GUIDE D'INSTALLATION ET D'ADMINISTRATION

SYNOVEX

Guide d'installation et d'administration

Matériel : Raspberry Pi 5

Éditions : Essential, Professional, Enterprise

Public : Administrateurs système et réseau, responsables infrastructure, équipes de sécurité



SYNOVEX — SIREN 884 713 009

Table des matières

Informations sur le document 5

Chapitre 1 — Architecture de la sonde 8
- 1.1 Principes d'architecture 8
- 1.2 Vue d'ensemble 8
- 1.3 Composants de la sonde 11
- 1.4 Stockage et conservation des données 14
- 1.5 Administration de la sonde 14
- 1.6 Modes de fonctionnement 15
- 1.7 Sécurité intégrée 16

Chapitre 2 — Prérequis 18
- 2.1 Matériel compatible 18
- 2.2 Alimentation électrique 20
- 2.3 Carte microSD 21
- 2.4 Refroidissement et boîtier 23
- 2.5 Réseau 23
- 2.6 Prérequis de sécurité et de gouvernance 26
- 2.7 Poste d'administration 27
- 2.8 Conditions d'installation physique 27
- 2.9 Liste de vérification avant démarrage 28

Chapitre 3 — Installation physique 30
- 3.1 Vue d'ensemble de la procédure 31
- 3.2 Précautions de manipulation 32
- 3.3 Identification du matériel 33
- 3.4 Assemblage avec la microSD préconfigurée 35
- 3.5 Mise en place du boîtier complet 40
- 3.6 Choix de l'emplacement 43
- 3.7 Connexion Ethernet 44
- 3.8 Branchement de l'alimentation et démarrage 45
- 3.9 Vérifications initiales 45
- 3.10 Erreurs fréquentes lors de l'installation 47

Chapitre 4 — Premier démarrage et mise en service 49
- 4.1 Les deux méthodes de mise en service 49
- 4.2 Déroulement de l'initialisation 52
- 4.3 Mise en service par fichier de provisionnement (méthode A) 53
- 4.4 Mise en service par l'assistant web (méthode B) 62
- 4.5 Édition de la sonde 67
- 4.6 Vérifier la disponibilité de la sonde 68
- 4.7 Premier contrôle de supervision 70
- 4.8 Vérifier la remontée des résultats 72
- 4.9 Checklist de fin de mise en service 72

Chapitre 5 — Configuration réseau et sécurité 74
- 5.1 Principes de sécurité de la sonde 74
- 5.2 Adressage IP 74
- 5.3 Résolution DNS 85
- 5.4 Synchronisation de l'heure 85
- 5.5 Proxy sortant 86
- 5.6 Flux réseau et pare-feu 88

5.7 Certificats et protocoles sécurisés 90
5.8 Identifiants, secrets et comptes techniques 92
5.9 Sécurisation des accès administrateur 94
5.10 Segmentation et positionnement réseau 96
5.11 Sécurité physique 99
5.12 Journalisation et audit 99
5.13 Recommandations aux RSSI 100

Chapitre 6 — Administration de la sonde 102
6.1 Moyens d'administration 102
6.2 Interface d'administration 104
6.3 API REST : principes 105
6.4 Utilisateurs et rôles 111
6.5 Jetons d'API 114
6.6 Gestion des contrôles 116
6.7 Scripts de scénarios 119
6.8 Secrets 120
6.9 Paramètres de la sonde 123
6.10 Journal d'audit 126
6.11 Événements en temps réel 127
6.12 Sauvegarde et restauration de la configuration 127
6.13 Automatisation 129
6.14 Gestion centralisée de plusieurs sondes 133

Chapitre 7 — Éditions et périmètre fonctionnel 134
7.1 Périmètre de la solution 134

Chapitre 8 — Maintenance et mises à jour 136
8.1 Répartition des responsabilités 136
8.2 Arrêt et redémarrage 136
8.3 Protection du support de stockage 138
8.4 Mises à jour 141
8.5 Sauvegarde et restauration de la configuration 168
8.6 Remplacer une carte microSD ou une sonde 169
8.7 Surveillance de la santé de la sonde 172
8.8 Rotation des secrets et des jetons 173
8.9 Maintenance des scénarios et des contrôles 174
8.10 Réinitialisation aux paramètres d'usine 175
8.11 Plan de maintenance préventive 178
8.12 Entretien physique 178
8.13 Fin de vie et effacement sécurisé 179

Chapitre 9 — Diagnostic et assistance 180
9.1 Méthode générale de diagnostic 180
9.2 Outils de diagnostic disponibles 182
9.3 Démarrage et matériel 186
9.4 Mise en service 189
9.5 Réseau 191
9.6 Stockage 193
9.7 Mises à jour 194
9.8 Types d'erreur et actions de premier niveau 196
9.9 Préparer une demande au support 197

Chapitre 10 — Références d'administration 200
10.1 Récapitulatif des prérequis 200
10.2 Checklist de mise en service 201

10.3 Tableau des flux réseau 203
10.4 Référence des configurations 205
10.5 Assistance et contacts 210

SYNOVEX

Guide d'installation et d'administration

Sonde de supervision applicative autonome pour Raspberry Pi 5

Information	Valeur
Document	Guide d'installation et d'administration — identifiant SYN-DOC-02
Révision documentaire	B
Public	Administrateurs système et réseau, responsables infrastructure, équipes de sécurité
Produit	SYNOVEX
Matériel pris en charge	Raspberry Pi 5
Éditions couvertes	SYNOVEX Essential, SYNOVEX Professional, SYNOVEX Enterprise
Éditeur	SYNOVEX — SIREN 884 713 009
Documentation en ligne	`https://docs-synovex.incitypark.fr` (après l'annonce de sa mise en service)
Langue	Français

Mentions légales

Éditeur

Cette documentation est éditée par SYNOVEX, SIREN 884 713 009. SYNOVEX est aussi le nom commercial de la gamme de sondes de supervision décrite.

Propriété intellectuelle et diffusion

© SYNOVEX. Tous droits réservés. Les textes, schémas, illustrations et exemples de cette documentation sont protégés par le droit d'auteur.

Cette documentation est réservée aux clients titulaires d'un droit d'utilisation du produit SYNOVEX. Le client peut la reproduire et la diffuser à l'intérieur de son organisation, et la communiquer aux prestataires qui interviennent pour son compte, pour les seuls besoins de l'installation, de l'exploitation et de la maintenance de ses sondes. Toute autre reproduction, diffusion ou mise à disposition, totale ou partielle, requiert l'accord écrit préalable de SYNOVEX.

Les fichiers d'exemple fournis avec la documentation (scénarios, règles d'alerte, tableau de bord, schémas JSON) peuvent être copiés et adaptés par le client pour l'exploitation de ses sondes.

Limitation de responsabilité

Les informations de cette documentation peuvent être modifiées sans préavis. L'éditeur s'efforce d'en assurer l'exactitude, mais ne peut être tenu responsable des erreurs ou omissions, ni des conséquences de l'utilisation des exemples fournis. Les exemples de configuration et de scénarios sont **fictifs** et doivent être adaptés à votre environnement, puis validés, avant tout usage. Cette documentation ne constitue pas un engagement contractuel : les engagements de l'éditeur, notamment de garantie, de support et de maintenance, résultent exclusivement de votre contrat.

Marques

SYNOVEX est un nom commercial de l'éditeur. Raspberry Pi est une marque de Raspberry Pi Ltd. Orange Pi est une marque de Shenzhen Xunlong Software Co., Ltd. Google Chrome est une marque de Google LLC ; Chromium et Puppeteer sont des projets open source de Google LLC. Java, OpenJDK, Oracle et MySQL sont des marques d'Oracle et/ou de ses filiales. Node.js est une marque de l'OpenJS Foundation. Prometheus et OpenTelemetry sont des marques de The Linux Foundation. Grafana est une marque de Grafana Labs. Datadog est une marque de Datadog, Inc. Dynatrace est une marque de Dynatrace LLC. Nagios est une marque de Nagios Enterprises, LLC. Centreon est une marque de Centreon. Microsoft et SQL Server sont des marques du groupe Microsoft. PostgreSQL est une marque de PostgreSQL Community Association of Canada. MariaDB est une marque de MariaDB plc. Les autres noms de produits et de sociétés cités peuvent être des marques de leurs propriétaires respectifs. Leur mention dans cette documentation n'implique aucun partenariat ni aucune approbation.

Logiciels tiers

La sonde intègre des logiciels libres et des composants tiers, distribués selon leurs propres licences. Les principaux composants et leurs licences sont listés au § 11.1 de la référence technique et API ; l'inventaire complet des composants accompagne chaque version du logiciel.

Matériel et fin de vie

Le Raspberry Pi 5 et ses accessoires officiels sont fabriqués par Raspberry Pi Ltd, qui en publie les déclarations de conformité. Avec l'offre microSD préconfigurée, le matériel est choisi et assemblé par vos soins. Avec l'offre boîtier complet, les informations de conformité applicables figurent dans les documents joints au produit. En fin de vie, la sonde relève de la collecte des déchets d'équipements électriques et électroniques : ne la jetez pas avec les déchets ordinaires et confiez-la à une filière de collecte agréée, après avoir effacé ses données (§ 8.13).

À propos de ce guide

Ce guide réunit tout ce dont un administrateur a besoin pour installer, sécuriser, administrer et maintenir une sonde SYNOVEX : architecture de la sonde, prérequis, installation physique, mise en service (assistant web ou fichier de provisionnement), configuration réseau et sécurité (adressage IPv4 et IPv6, DNS, heure, 802.1X, proxy, pare-feu, certificats), administration (comptes, rôles, jetons d'API, secrets, paramètres, sauvegarde), éditions, maintenance et mises à jour (mécanisme A/B, retour arrière, réinitialisation, remplacement), diagnostic et références.

Il ne nécessite pas de lire les chapitres consacrés au développement des scénarios Puppeteer, traités dans le guide de développement des scénarios (SYN-DOC-04). La création des contrôles et l'interprétation des résultats sont traitées dans le guide d'utilisation et de supervision (SYN-DOC-03), l'intégration aux plateformes d'observabilité dans le guide d'intégration et d'observabilité (SYN-DOC-05).

La bibliothèque documentaire SYNOVEX

La documentation SYNOVEX se compose d'un manuel technique complet et de six guides spécialisés. Tous sont produits à partir des mêmes sources : un passage repris dans plusieurs documents y est rigoureusement identique.

Document	Identifiant	Public
Manuel technique complet	SYN-DOC-00	Tous publics : référence intégrale
Guide de démarrage rapide	SYN-DOC-01	Techniciens d'installation, nouveaux clients
Guide d'installation et d'administration	SYN-DOC-02	Administrateurs système et réseau, équipes de sécurité
Guide d'utilisation et de supervision	SYN-DOC-03	Équipes d'exploitation et de supervision
Guide de développement des scénarios	SYN-DOC-04	Développeurs, intégrateurs, équipes de qualité
Guide d'intégration et d'observabilité	SYN-DOC-05	Architectes, DevOps, SRE
Référence technique et API	SYN-DOC-06	Intégrateurs avancés, architectes, développeurs

Renvois. Dans un guide, un renvoi sans autre mention désigne une section, un chapitre ou une figure du même guide, avec la numérotation de ce guide. Lorsque le sujet est traité dans un autre guide, le renvoi nomme ce guide, par exemple « § 6.3 du guide d'installation et d'administration ». La numérotation est alors celle du guide cité. Chaque guide se lit ainsi sans le manuel technique complet, qui réunit l'intégralité de la documentation sous sa propre numérotation.

Services en ligne. L'ensemble de la bibliothèque est également publié sur `https://docs-synovex.incitypark.fr`, avec une recherche et une navigation par profil. Ce site, le portail de support et le service de distribution des mises à jour de l'éditeur sont accessibles après l'annonce de leur mise en service. Avant cette annonce, ou si l'un de ces services ne répond pas, utilisez le canal de contact prévu par votre contrat. Les adresses citées dans ce guide s'entendent sous cette réserve.

Chapitre 1 — Architecture de la sonde

1.1 Principes d'architecture

L'architecture de la sonde repose sur six principes. Ils expliquent la plupart des choix décrits dans la suite de la documentation.

Principe	Signification	Conséquence pour vous
Autonomie	La sonde planifie, exécute, évalue et conserve elle-même ses contrôles	Elle continue de superviser même si vos plateformes de supervision, votre accès Internet ou les services de l'éditeur sont indisponibles
Source de vérité locale	La configuration et l'historique des résultats sont stockés sur la sonde	Les plateformes externes reçoivent une copie des résultats ; la référence reste consultable localement
Connexions sortantes uniquement vers l'extérieur	Toute communication avec un service extérieur à votre réseau est initiée par la sonde	Aucune ouverture de port depuis Internet n'est nécessaire
Isolation de l'exécution	Les scénarios navigateur et les plugins s'exécutent dans un environnement séparé, sans accès à la configuration ni aux secrets non déclarés	Un script défectueux ou malveillant ne peut ni compromettre la sonde ni lire l'ensemble des identifiants
Standards ouverts	API REST documentée (OpenAPI), OpenTelemetry/OTLP, format Prometheus, codes retour Nagios	Intégration à vos outils sans connecteur propriétaire
Sobriété	Peu de composants, écritures disque maîtrisées, ressources réservées au navigateur	Fonctionnement fiable sur un ordinateur monocarte, 24 heures sur 24

1.2 Vue d'ensemble

La sonde est installée au point d'observation choisi : dans le réseau de votre organisation, à proximité des utilisateurs ou des applications dont vous souhaitez vérifier le service, ou à l'extérieur, sur un site distant, chez un client, un partenaire ou un sous-traitant, ou dans une autre région géographique (§ 1.2.1). Le schéma ci-dessous présente le cas d'une sonde installée dans le réseau de l'entreprise ; les mêmes catégories d'échanges s'appliquent aux autres emplacements. Elle échange avec quatre catégories d'interlocuteurs :

- les **ressources supervisées** : sites web, API, bases de données, serveurs, équipements, sur lesquels elle exécute ses contrôles ;
- les **administrateurs**, qui la configurent et consultent ses résultats depuis un navigateur ou par l'API ;
- les **plateformes de supervision et d'observabilité** (Prometheus, Grafana, Datadog, Dynatrace, Nagios, Centreon…), qui reçoivent ou collectent ses résultats ;
- les **services d'infrastructure** indispensables : DNS, heure (NTP) et, si vous les activez, dépôt de mises à jour de l'éditeur et proxy sortant.

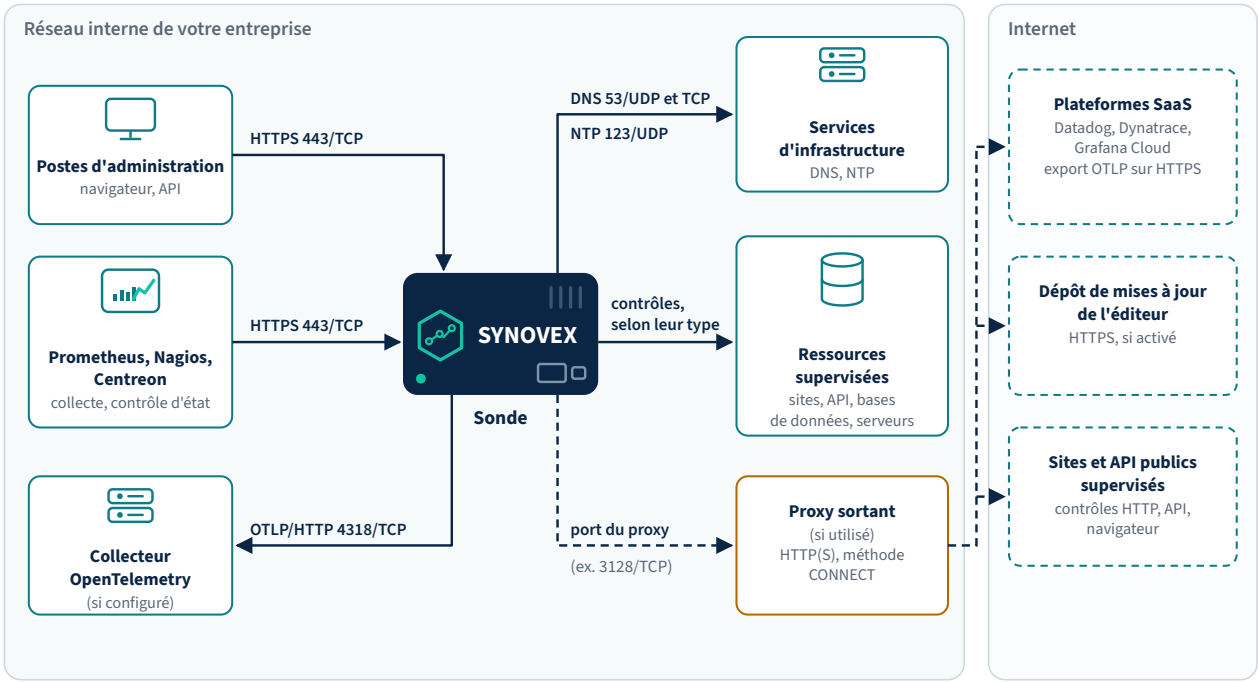


Figure 1-1 — Schéma d'implantation type : sonde dans le réseau interne, plateformes de supervision, accès Internet sortant via proxy

Les flèches indiquent le sens d'établissement des connexions. Les flux en pointillés sont facultatifs et dépendent de votre configuration. La sonde n'envoie aucune donnée de télémétrie à l'éditeur : ses seuls échanges avec lui sont la vérification et le téléchargement des mises à jour, si vous les activez.

1.2.1 Où placer la sonde ?

L'emplacement de la sonde détermine ce qu'elle mesure. Une sonde voit le service tel qu'il est perçu depuis son point d'observation : à travers les mêmes résolveurs DNS, pare-feu, proxys, opérateurs et liens que les utilisateurs ou les applications de ce réseau. Elle peut être installée dans tout environnement qui dispose des accès réseau nécessaires aux contrôles configurés, à l'intérieur comme à l'extérieur de votre organisation.

Emplacement	Ce que la sonde mesure	Usage typique
Réseau des utilisateurs d'un site	Le service tel que le perçoivent les collaborateurs de ce site, y compris les liens intersites et le proxy	Applications métier internes, services SaaS utilisés par l'entreprise
Centre de données, à proximité des serveurs	Le service sans les effets du réseau étendu	Distinguer un problème applicatif d'un problème de réseau
Zone d'accès externe ou réseau isolé vers Internet	Le service tel qu'il est vu depuis l'extérieur, en passant par l'accès Internet	Sites et API publics de l'entreprise
Site distant ou agence : filiale, entrepôt, magasin	Le service tel que le perçoivent les utilisateurs de ce site, à travers son réseau local, son accès opérateur et ses liaisons vers vos centres de données	Vérifier la disponibilité et les performances des applications centrales depuis chaque site
Réseau d'un client, avec son accord	Le service tel que le perçoivent les utilisateurs du client, à travers leur réseau, leur proxy et leur pare-feu	Vérifier que les services proposés par votre organisation sont réellement accessibles et fonctionnels depuis l'environnement du client

Emplacement	Ce que la sonde mesure	Usage typique
Réseau d'un partenaire ou d'un sous-traitant, avec son accord	Les échanges et les services tels qu'ils sont accessibles depuis cette organisation	Superviser un portail partenaire, une interconnexion ou des échanges entre organisations
Différentes régions géographiques	Le service tel qu'il est perçu dans chaque pays ou région : opérateur, liens internationaux, résolution DNS locale, éventuel réseau de diffusion de contenu (CDN)	Mesurer la latence et les temps de réponse par localisation, repérer une dégradation propre à une région ou à un opérateur

Plusieurs sondes placées à des endroits différents fournissent des **indices de localisation** d'un défaut. Si le même contrôle échoue depuis un site et réussit depuis le centre de données, l'écart oriente l'analyse vers ce qui distingue les deux points d'observation, souvent le chemin réseau du site. De même, un contrôle qui réussit depuis Paris mais échoue ou ralentit depuis Hô Chi Minh-Ville oriente l'analyse vers le chemin international, l'opérateur ou les services régionaux. Ces indices ne suffisent pas à conclure : un composant réseau commun peut affecter tous les sites, et une réponse qui dépend de la région, de l'identité du compte de test, du répartiteur de charge ou de la résolution DNS peut n'affecter qu'un seul point d'observation alors que la cause est applicative. Avant d'attribuer l'origine à l'application ou au réseau, comparez les chemins, les cibles effectivement jointes, les résolutions DNS, les politiques appliquées (proxy, filtrage) et les résultats détaillés des sondes. Chaque sonde rend compte de ce qu'elle observe depuis son emplacement ; elle n'identifie pas elle-même la cause d'une dégradation réseau, et chaque sonde fonctionne indépendamment des autres. Chaque sonde se voit attribuer un **nom de site** lors de sa mise en service (chapitre 4), repris dans tous ses résultats exportés : c'est lui qui permet de comparer les sondes entre elles dans vos tableaux de bord et vos alertes.

Les prérequis d'une sonde installée hors de vos locaux dépendent des services à superviser et de leur accessibilité depuis ce réseau. Prévoyez en particulier les points suivants :

- **accord du propriétaire du réseau** : installez-la uniquement avec l'autorisation écrite de l'organisation qui exploite le réseau, et convenez avec elle des cibles contrôlées, des flux ouverts et de la personne qui intervient physiquement sur l'appareil ;
- **transmission des résultats** : privilégiez l'envoi par OTLP (chapitre 2 du guide d'intégration et d'observabilité), qui n'utilise que des connexions sortantes, vers une plateforme joignable depuis ce site. La collecte par Prometheus ou par le plugin Nagios suppose au contraire que votre plateforme puisse joindre la sonde ;
- **administration** : l'interface et l'API ne doivent pas être exposées sur Internet (§ 1.5). Administrez la sonde depuis le réseau où elle est installée ou au travers d'un moyen d'accès sécurisé convenu avec l'exploitant de ce réseau. La sonde ne requiert aucune liaison permanente avec votre organisation pour exécuter ses contrôles ;
- **coupure de liaison** : la sonde continue d'exécuter ses contrôles et de conserver leur historique localement lorsque la liaison vers vos plateformes est interrompue. Les résultats exportés pendant la coupure ne sont pas renvoyés automatiquement ; l'historique local reste consultable (§ 2.12 du guide d'intégration et d'observabilité) ;
- **heure et réglementation locales** : vérifiez qu'un serveur NTP est joignable depuis le site et que l'installation respecte les règles locales applicables à l'équipement et aux données collectées.

1.3 Composants de la sonde

La sonde réunit un matériel, un système d'exploitation et deux moteurs logiciels.

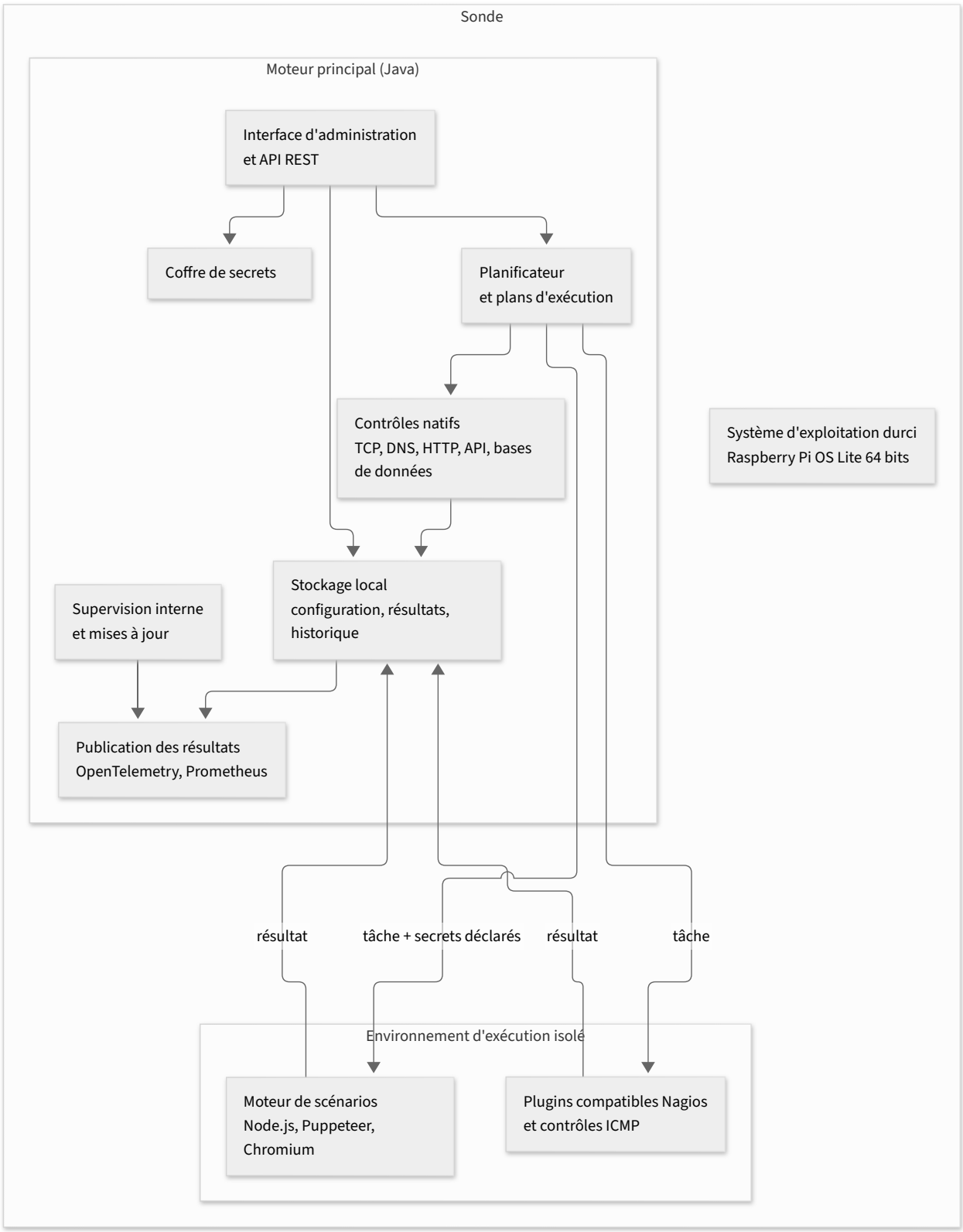


Schéma 1-1 — Composants de la sonde

1.3.1 Matériel et système

La sonde fonctionne sur un **Raspberry Pi 5**, ordinateur monocarte à processeur ARM 64 bits, avec une capacité mémoire adaptée à l'édition (chapitre 2). Le système d'exploitation est **Raspberry Pi OS Lite 64 bits**, distribution dérivée de Debian maintenue par le fabricant de la carte, installé sans interface graphique et durci : services inutiles retirés, accès distant SSH désactivé par défaut, comptes et droits limités au strict nécessaire. Le système est configuré pour limiter les écritures sur la carte microSD, dont la durée de vie dépend du volume écrit (chapitre 8).

La carte microSD porte deux **emplacements système** (A et B), dont un seul est actif. Le système y est monté en **lecture seule** : il n'est pas modifié en fonctionnement normal, de sorte qu'une coupure électrique n'interrompt aucune écriture du système. Cette disposition ne protège pas contre une défaillance du support lui-même (§ 8.3). Une mise à jour s'installe sur l'emplacement inactif, et la sonde revient automatiquement à l'emplacement précédent si la nouvelle version ne fonctionne pas correctement (§ 8.4.5). Les données de la sonde sont stockées sur une partition séparée de la microSD. Un **SSD NVMe** facultatif, monté sur la carte M.2 HAT+ officielle, peut accueillir les données les plus volumineuses ; la sonde continue de démarrer sur la microSD (§ 8.3.4).

1.3.2 Moteur principal

Le **moteur principal** est le cœur de la sonde. Développé en Java, il fonctionne en permanence et assure les fonctions suivantes.

Fonction	Description
Interface d'administration et API REST	Serveur HTTPS qui publie l'interface web et l'API documentée ; authentification des utilisateurs et des jetons, contrôle des droits, journal d'audit (chapitre 6). Le moteur d'authentification repose sur des fournisseurs interchangeables : la version actuelle utilise des comptes locaux, et l'ajout d'OpenID Connect est prévu dans une version ultérieure (§ 6.4)
Planification	Calcul des échéances de chaque contrôle et de chaque plan d'exécution, répartition dans le temps pour éviter les pics, limitation du nombre d'exécutions simultanées (chapitre 6 du guide d'utilisation et de supervision)
Contrôles natifs	Exécution directe des contrôles `tcp`, `dns`, `http`, `api` et `database`. Les connexions aux bases de données utilisent les pilotes standard JDBC de chaque éditeur de base (chapitre 5 du guide d'utilisation et de supervision)
Évaluation	Application des critères de réussite (assertions, seuils), des nouvelles tentatives et des règles de calcul de l'état (chapitre 3 du guide d'utilisation et de supervision)
Stockage local	Enregistrement de la configuration, des résultats, des étapes et des agrégats dans une base SQLite locale ; purge selon la durée de rétention
Coffre de secrets	Conservation chiffrée des mots de passe et jetons utilisés par les contrôles ; transmission limitée aux secrets déclarés par chaque contrôle
Publication	Production de métriques, traces et journaux au format OpenTelemetry ; export OTLP vers les destinations configurées ; endpoint Prometheus (chapitre 2 du guide d'intégration et d'observabilité)
Supervision interne	Surveillance de l'état de la sonde elle-même : mémoire, température, alimentation, espace disque, retards de planification, échecs d'export
Mises à jour	Vérification, téléchargement, contrôle de signature et installation des images système sur l'emplacement inactif, sans interrompre les contrôles ; canaux `security` (automatique par défaut) et `feature` (manuel par défaut) ; activation automatique dans une fenêtre de maintenance définie par le client, après préavis et drainage des exécutions, ou, par exception, à la demande d'un administrateur ou dès que possible pour un correctif critique si le client l'a choisi ; validation après redémarrage et retour arrière automatique (§ 8.4)

1.3.3 Environnement d'exécution isolé

Certains contrôles exécutent du code qui ne provient pas de l'éditeur : scripts de scénarios écrits par vos équipes, plugins compatibles Nagios. Ils s'exécutent dans un **environnement isolé**, distinct du moteur principal :

- un compte système dédié, sans accès en lecture à la base de configuration ni au coffre de secrets ;
- des limites de mémoire, de processeur et de nombre de processus, qui empêchent un scénario défaillant d'épuiser les ressources de la sonde ;
- un processus neuf pour chaque exécution, arrêté de force si le délai maximal est dépassé ;
- la réception, pour chaque exécution, des seuls secrets que le contrôle a explicitement déclarés.

Le **moteur de scénarios** fait partie de cet environnement. Il repose sur **Node.js**, environnement d'exécution JavaScript, sur **Puppeteer**, bibliothèque de pilotage du navigateur, et sur **Chromium** en mode headless. Pour chaque exécution d'un scénario, il démarre un navigateur neuf avec un profil vierge conservé en mémoire, exécute les étapes, mesure leur durée, réalise une capture d'écran en cas d'échec, puis ferme le navigateur. Aucune session, aucun cookie ni aucune donnée de navigation n'est conservé d'une exécution à l'autre. La version de Chromium est fournie et validée par l'éditeur avec la version de Puppeteer correspondante (chapitre 3 du guide de développement des scénarios).

Les **plugins compatibles Nagios** et les contrôles **ICMP** (ping), qui reposent sur des utilitaires système, s'exécutent dans ce même environnement isolé, quelle que soit l'édition. Les plugins sont lancés directement, sans interpréteur de commandes, ce qui empêche toute injection de commande par leurs arguments.

> **Information** — Cette séparation explique pourquoi la création de scénarios scriptés et l'ajout de plugins personnalisés sont réservés aux administrateurs : ces opérations reviennent à exécuter du code sur le réseau où la sonde est installée. Le chapitre 6 détaille les rôles.

1.3.4 Répartition des types de contrôles

Type de contrôle	Composant d'exécution	Édition minimale
`icmp` (ping)	Environnement isolé, utilitaire système	Essential
`tcp`, `dns`, `http`	Moteur principal	Essential
`nagios`, plugins fournis	Environnement isolé	Essential
`nagios`, plugins personnalisés	Environnement isolé	Professional
`api`	Moteur principal	Professional
`database`	Moteur principal (JDBC)	Professional
`browser` (scénarios déclaratifs et scriptés)	Moteur de scénarios	Enterprise

Chaque famille d'exécution dispose de sa propre limite de simultanéité. Un parcours navigateur long ne retarde donc pas les contrôles réseau, qui s'exécutent en parallèle dans leur propre file. Par défaut, un seul parcours navigateur s'exécute à la fois, car Chromium est le composant le plus consommateur de mémoire. Les plans d'exécution permettent d'enchaîner plusieurs scénarios sans les faire se chevaucher (chapitre 6 du guide d'utilisation et de supervision).

1.4 Stockage et conservation des données

La sonde conserve localement toutes les informations nécessaires à son fonctionnement et à son exploitation.

Donnée	Contenu	Conservation par défaut
Configuration	Contrôles, plans d'exécution, destinations d'export, paramètres, comptes, jetons (sous forme d'empreinte)	Permanente, avec sauvegarde automatique quotidienne (trois générations)
Secrets	Mots de passe et jetons utilisés par les contrôles, chiffrés	Permanente, jusqu'à suppression
Exécutions détaillées	Résultat, état, durée, étapes, erreur, mesures de chaque exécution	14 jours
Agrégats horaires	Nombre d'exécutions, d'échecs, durées représentatives, par contrôle et par heure	400 jours
Artefacts	Captures d'écran, journaux de console du navigateur, sorties de plugins, produits en cas d'échec	7 jours, dans la limite de 500 Mo
Journal d'audit	Opérations d'administration	365 jours
Journaux système	Messages techniques des composants	En mémoire, effacés au redémarrage (par défaut)

Ces données sont stockées sur la partition de données de la microSD. Si un SSD NVMe est activé, les exécutions détaillées, les agrégats, les artefacts, la file d'attente d'export et les journaux persistants y sont placés ; la configuration, les secrets et le certificat d'édition restent sur la microSD (§ 8.3.4). Ces durées sont configurables dans les limites de l'espace disponible (chapitre 6). Le stockage est conçu pour limiter les effets d'une coupure électrique : une coupure peut faire perdre les derniers résultats enregistrés ; la configuration, enregistrée avec un niveau de durabilité supérieur, et la cohérence des bases sont préservées tant que le support de stockage fonctionne correctement, et la base est vérifiée à chaque démarrage. Une panne de la carte elle-même relève de la sauvegarde de la configuration. Le chapitre 8 détaille les mesures de protection de la carte microSD et les procédures de sauvegarde et de restauration.

1.5 Administration de la sonde

La sonde s'administre **localement**, depuis le réseau où elle est installée, sans dépendre d'un service extérieur.

Moyen	Usage	Chapitre
Assistant de mise en service	Configuration initiale : compte administrateur, réseau, heure, proxy, certificat, destinations d'export	chapitre 2
Fichier de provisionnement	Configuration initiale sans intervention interactive, préparée sur la carte microSD avant le premier démarrage ; adapté aux déploiements en nombre	chapitre 2
Interface d'administration web	Consultation des états et des résultats, gestion des contrôles, des plans d'exécution, des utilisateurs, des secrets, des destinations d'export, des paramètres	chapitre 4
API REST	Automatisation de toutes les opérations de l'interface : intégration à vos outils de déploiement, gestion en masse, synchronisation avec vos référentiels	chapitre 4 et chapitre 4 du guide d'utilisation et de supervision
Accès SSH	Maintenance avancée, désactivé par défaut et activable par un administrateur	chapitre 3 et chapitre 3 du guide d'utilisation et de supervision

L'interface d'administration utilise exclusivement l'API REST : tout ce que vous faites dans l'interface peut donc être automatisé. Tous les échanges sont chiffrés en HTTPS. Les accès sont authentifiés par compte nominatif ou par jeton d'API, et soumis à quatre rôles : administrateur (`admin`), opérateur (`operator`), lecteur (`viewer`) et collecte de métriques (`metrics`) (chapitre 6). Chaque opération d'administration est consignée dans un journal d'audit.

→ **Évolution prévue** — L'authentification par OpenID Connect, pour se connecter avec les comptes de l'annuaire de l'entreprise, est prévue dans une version ultérieure. Elle s'ajoutera comme un nouveau fournisseur d'authentification, avec une correspondance entre les groupes de l'annuaire et les rôles de la sonde, sans modification des rôles ni de l'API.

! **Avertissement** — L'interface d'administration et l'API ne doivent jamais être exposées directement sur Internet. La sonde est conçue pour être administrée depuis le réseau où elle est installée ; l'accès à distance passe par un moyen d'accès sécurisé à ce réseau, celui de votre organisation ou celui convenu avec l'exploitant du réseau d'accueil.

1.6 Modes de fonctionnement

La sonde connaît trois modes de fonctionnement successifs, auxquels s'ajoutent un mode restreint lié au certificat d'édition et un état temporaire de maintenance, propre à l'activation des mises à jour.

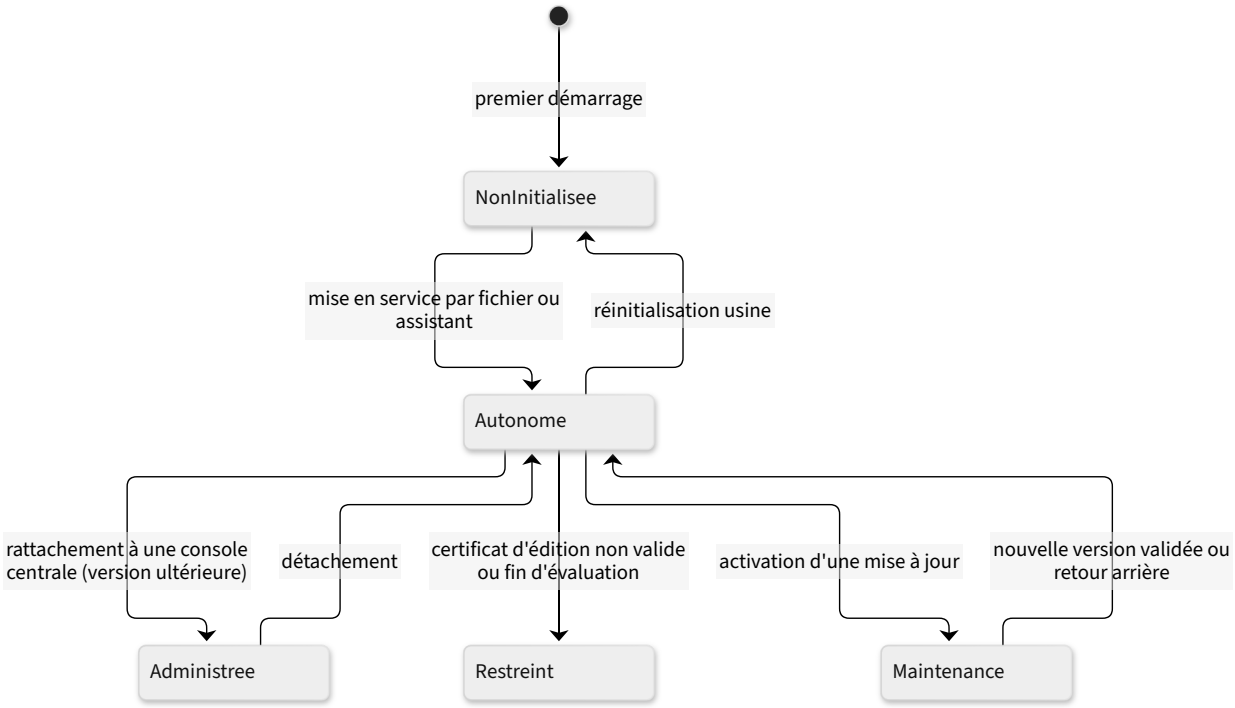


Schéma 1-2 — Modes de fonctionnement de la sonde

Mode	Description
Non initialisée	État à la sortie de l'emballage, ou après une réinitialisation. La sonde n'exécute aucun contrôle et attend sa mise en service, par fichier de provisionnement ou par l'assistant protégé par un code d'installation (chapitre 4).
Autonome	Mode nominal. La configuration est gérée localement par l'interface ou l'API ; les résultats sont conservés localement et publiés vers les destinations configurées.

Mode	Description
Administrée	Mode prévu avec la console centrale. La configuration est définie dans la console et appliquée par la sonde, qui continue de fonctionner avec la dernière configuration reçue si la console devient injoignable.
Maintenance	État temporaire de l'activation d'une mise à jour, dans une fenêtre définie par le client, à la demande d'un administrateur ou, pour un correctif critique avec `criticalPolicy: asap`, dès que possible et hors fenêtre. La sonde **draine** d'abord ses exécutions : aucune nouvelle exécution ne démarre et celles en cours se terminent dans un délai limité. Elle **redémarre** ensuite sur la nouvelle version, qui s'autoteste ; en cas d'échec, elle revient à la version précédente. Cet état est exposé par `/health` (`MAINTENANCE`) et par les métriques de la sonde (§ 8.4).
Restreint	Mode appliqué lorsque le certificat d'édition est absent, invalide ou propre à une autre carte, ou au terme des 30 jours d'évaluation d'une carte de démonstration prêtée. Aucun contrôle n'est exécuté ; la consultation, l'export de la configuration et l'archive de diagnostic restent disponibles. La cause est indiquée dans l'état de santé (§ 4.5).

Une sonde ne supervise pas pendant son propre redémarrage. Lorsque la continuité de la supervision est critique, déployez au moins deux sondes par site, exécutant les mêmes contrôles avec des fenêtres de maintenance qui ne se chevauchent pas, séparées d'un écart supérieur à la durée totale mesurée d'une activation, et fondez vos alertes sur l'ensemble des sondes du site (§ 8.4). Cet espacement réduit le risque que deux sondes du même site soient en maintenance en même temps sans l'exclure : il ne coordonne ni les activations manuelles ni celles d'un correctif critique en mode `asap`, qui ont lieu hors fenêtre. Pour ces dernières, un décalage fixe propre à chaque sonde (`security.criticalStagger`) échelonne les activations, sans vérifier l'état des autres sondes : les sondes étant autonomes, rien ne garantit l'absence de redémarrage simultané (§ 8.4.11 et § 8.4.12). N'activez jamais manuellement deux sondes d'un même site en même temps.

> → **Évolution prévue** — La **console centrale multi-sondes**, hébergée par l'éditeur ou installée dans votre infrastructure, permettra de gérer un parc de sondes depuis un point unique : inventaire, configuration commune, synthèse des états. La sonde s'y connectera par une liaison sortante chiffrée et authentifiée par certificat. Cette console restera facultative : une sonde administrée continue de fonctionner sans elle, et une sonde autonome n'en a jamais besoin. L'adresse de la console hébergée par l'éditeur, `https://fleet-synovex.incitypark.fr`, est réservée dans le plan de nommage ; la sonde ne la contacte pas.

1.7 Sécurité intégrée

La sécurité est prise en compte à tous les niveaux. Le tableau ci-dessous résume les mesures, détaillées au chapitre 5 (réseau et sécurité) et au chapitre 6 (comptes, rôles et secrets).

Domaine	Mesures
Mise en service	Aucun mot de passe par défaut ; assistant protégé par un code d'installation propre à la carte ; certificat HTTPS propre à chaque sonde, généré au premier démarrage
Accès	HTTPS uniquement ; comptes nominatifs ; jetons d'API à portée limitée, révocables ; quatre rôles ; protection contre les tentatives répétées ; SSH désactivé par défaut
Secrets	Chiffrés au repos ; jamais relisibles par l'API ; transmis aux seuls contrôles qui les déclarent ; masqués dans les journaux
Exécution	Environnement isolé pour les scénarios et plugins ; compte système dédié ; limites de ressources ; navigateur neuf à chaque exécution ; pas d'interpréteur de commandes pour les plugins
Réseau	Aucune ouverture entrante depuis Internet ; flux sortants limités et documentés ; prise en charge d'un proxy ; IPv4, IPv6 activable ; authentification 802.1X par certificat (EAP-TLS) sur le port Ethernet (chapitre 5)
Traçabilité	Journal d'audit des opérations d'administration, exportable vers votre outil de gestion des événements de sécurité

Domaine	Mesures
Mises à jour	Images système signées par l'éditeur, installées sur un emplacement A/B avec retour arrière automatique (§ 8.4.5) ; système en lecture seule ; version de Chromium validée ; correctifs de sécurité pendant toute la période de support, sur un canal distinct des versions fonctionnelles et installés automatiquement par défaut (désactivable) ; activation automatique dans les fenêtres choisies par le client, avec préavis et report possible ; exceptions documentées : activation manuelle et correctif critique en mode `asap` (chapitre 8)

Chapitre 2 — Prérequis

Ce chapitre recense tout ce qui doit être réuni **avant** l'installation de la sonde : matériel, alimentation, carte microSD, raccordement réseau, autorisations de flux, comptes de test, poste d'administration et conditions d'installation. Il se termine par une liste de vérification à compléter avant le premier démarrage (§ 2.9).

> ✓ **Conseil** — Transmettez ce chapitre à vos équipes réseau et sécurité dès la commande de la sonde. Les demandes d'ouverture de flux et la création de comptes de test demandent souvent plusieurs jours ; les anticiper évite de retarder la mise en service.

2.1 Matériel compatible

2.1.1 Carte supportée

La sonde fonctionne **exclusivement sur Raspberry Pi 5**. La carte microSD contient un système préparé pour ce seul modèle ; son fonctionnement sur un autre modèle de Raspberry Pi ou sur une carte d'un autre fabricant n'est ni pris en charge ni garanti.

> ! **Attention** — N'insérez pas la carte microSD de la sonde dans un Raspberry Pi 4, un Raspberry Pi 400, un Compute Module ou une carte Orange Pi. Le système de la sonde contrôle le modèle de carte au tout début de son démarrage, avant tout montage d'une partition en écriture et avant l'extension de la partition de données (§ 4.2). Sur un matériel autre qu'un Raspberry Pi 5, deux cas se présentent. Si le microprogramme (*firmware*) de la carte parvient à charger le système, celui-ci s'arrête sans monter de partition en écriture et affiche un message sur l'écran HDMI éventuellement raccordé. Si le microprogramme d'un autre modèle ne charge pas l'image, aucun composant de la sonde ne s'exécute et aucun message ne peut s'afficher ; cela n'établit pas à lui seul qu'aucune écriture n'a eu lieu, le comportement du microprogramme tiers n'étant pas maîtrisé par la sonde. Dans les deux cas, la sonde ne démarre pas ; ce contrôle vise à préserver la carte pour qu'elle reste utilisable ensuite sur le bon matériel, sans que sa conservation puisse être garantie lorsque le microprogramme d'une autre carte a manipulé le support. La prise en charge d'autres cartes est une évolution envisagée, non disponible actuellement.

2.1.2 Capacité mémoire selon l'édition

Le Raspberry Pi 5 existe en plusieurs capacités de mémoire vive. La capacité requise dépend de l'édition, principalement parce que le navigateur Chromium utilisé par les scénarios de l'édition Enterprise est gourmand en mémoire.

Édition	Mémoire minimale	Mémoire recommandée	Justification
Essential	2 Go	4 Go	Contrôles réseau, HTTP et plugins : faible consommation. La marge de 4 Go facilite une évolution ultérieure vers Professional
Professional	4 Go	4 Go ou plus	Pilotes de bases de données et suites de requêtes API
Enterprise	**8 Go**	8 Go	Chromium consomme, à titre indicatif, plusieurs centaines de mégaoctets par parcours en cours d'exécution

La capacité de mémoire est indiquée sur l'emballage du Raspberry Pi 5 ; après la mise en service, elle est également affichée dans l'état de santé de la sonde (chapitre 4), et la réponse de `GET /api/v1/system` l'indique dans le champ `resources.memoryTotalBytes`, en octets. Pour l'offre « boîtier complet », le Raspberry Pi 5 livré a la capacité de mémoire requise par l'édition.

> **Information** — Le changement d'édition se fait par échange de la carte microSD contre une carte de l'édition supérieure, avec transfert de la configuration (§ 8.6). Si vous envisagez de passer à l'édition Enterprise, prévoyez dès le départ un Raspberry Pi 5 de 8 Go.

2.1.3 Composition des offres

Élément	Offre « microSD préconfigurée »	Offre « boîtier complet »
Carte microSD préconfigurée	Fournie	Fournie, déjà insérée
Raspberry Pi 5	À fournir par vous (capacité selon § 2.1.2)	Fourni
Boîtier	À fournir par vous (§ 2.4)	Fourni, assemblé
Refroidissement	À fournir par vous (§ 2.4)	Fourni, monté
Alimentation USB-C	À fournir par vous (§ 2.2)	Selon la composition de l'offre, indiquée sur la liste de colisage de votre commande ; à défaut, à fournir par vous (§ 2.2)
Câble Ethernet	À fournir par vous	Selon la composition de l'offre, indiquée sur la liste de colisage de votre commande ; à défaut, à fournir par vous
Carte M.2 HAT+ officielle et SSD NVMe (facultatifs, § 2.3.3)	À fournir par vous, si vous choisissez cette option	Selon votre commande ; à défaut, à fournir par vous si vous choisissez cette option
Encart d'identification de la carte (édition, numéro de série, code d'installation)	Fourni	Fourni
Étiquette d'identification du boîtier (numéro de série, adresse MAC, nom d'hôte par défaut, code d'installation, édition et capacité mémoire)	Non	Fournie
Accessoires de fixation (montage en baie, fixation murale)	Non	Selon votre commande

La liste de colisage exacte et les références des composants sont fournies avec votre commande.

> **Information** — Ne présumez pas qu'un accessoire est fourni s'il ne figure pas sur la liste de colisage de votre commande. Avant l'installation, vérifiez en particulier l'alimentation (§ 2.2), le câble Ethernet et, le cas échéant, la carte M.2 HAT+ et le SSD. Seuls les éléments qui définissent chaque offre sont toujours présents : la carte microSD et son encart pour l'offre « microSD préconfigurée » ; le Raspberry Pi 5 en boîtier, son refroidissement et la carte insérée pour l'offre « boîtier complet ».

2.1.4 Écran, clavier et souris

La sonde n'a besoin ni d'écran, ni de clavier, ni de souris : elle s'administre par le réseau. Lors du premier démarrage, l'empreinte du certificat doit toutefois être vérifiée par un canal indépendant du réseau : un écran raccordé au port micro-HDMI de la carte, ou la lecture du fichier `setup-code.txt` sur la microSD (§ 4.4.4). L'écran est aussi utile pour

lire le code d'installation et l'empreinte du certificat de la sonde, et suivre le démarrage (chapitre 4), ou lors d'un dépannage. Le Raspberry Pi 5 dispose de ports **micro-HDMI** : prévoyez un câble ou un adaptateur micro-HDMI vers HDMI si nécessaire.

2.1.5 Compatibilité avec d'autres ordinateurs monocartes

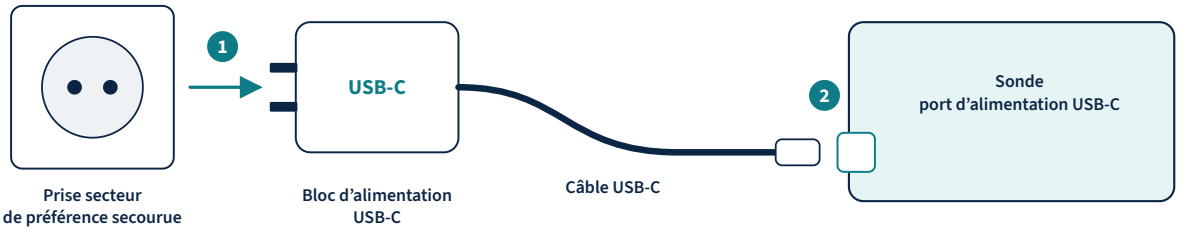
SYNOVEX est conçu et documenté pour Raspberry Pi 5. Son architecture logicielle peut permettre une utilisation sur d'autres ordinateurs monocartes, notamment certains modèles Orange Pi. Toutefois, ces plateformes n'ont pas fait l'objet d'une validation officielle et leur fonctionnement n'est pas garanti.

La carte microSD livrée contient une image système propre au Raspberry Pi 5 : chargeur d'amorçage, noyau et mécanismes de démarrage et de mise à jour de cette carte. Elle ne peut pas être utilisée telle quelle sur une carte Orange Pi ou sur un autre ordinateur monocarte, ni passer d'un modèle de carte à l'autre (§ 2.1.1). Les procédures, les valeurs et les exigences de cette documentation concernent le seul Raspberry Pi 5.

2.2 Alimentation électrique

2.2.1 Caractéristiques requises

La qualité de l'alimentation est la première cause d'instabilité des ordinateurs monocartes : une alimentation insuffisante provoque des redémarrages inopinés, des erreurs d'écriture et, à terme, la corruption de la carte microSD.



Ordre de branchement

1. Brancher le bloc d'alimentation sur la prise secteur.
2. Brancher le connecteur USB-C sur la sonde, en dernier.

Raspberry Pi 5 : exigences (§ 2.2.1)	
Recommandée	Alimentation officielle Raspberry Pi 27 W USB-C (5,1 V, 5 A)
Alternative	Alimentation USB-C 5 V / 3 A de qualité : courant limité sur les ports USB Non admise avec un SSD NVMe
Avec un SSD NVMe	Alimentation officielle de 27 W obligatoire
À proscrire	Chargeurs de téléphone génériques, ports USB d'ordinateur ou d'écran, câbles USB-C longs ou de faible section, multiprises non protégées

Représentation schématique, non à l'échelle

Figure 2-1 — Raccordement de l'alimentation du Raspberry Pi 5 : prise, bloc d'alimentation USB-C, câble et sonde

Caractéristique	Valeur
Alimentation recommandée	**Alimentation officielle Raspberry Pi 27 W USB-C** (5,1 V, 5 A)
Connecteur	USB-C

Caractéristique	Valeur
Alternative	Alimentation USB-C 5 V / 3 A de qualité : la carte fonctionne, mais limite le courant disponible sur ses ports USB (comportement documenté par Raspberry Pi). **Non admise avec un SSD NVMe** (§ 2.3.3)
À proscrire	Chargeurs de téléphone génériques, ports USB d'ordinateur ou d'écran, câbles USB-C longs ou de faible section, multiprises non protégées

> **Attention** — Une alimentation sous-dimensionnée peut sembler fonctionner pendant des jours avant de provoquer des incidents difficiles à diagnostiquer. La sonde détecte les épisodes de sous-tension et les signale dans sa supervision interne (chapitre 7 du guide d'utilisation et de supervision), mais seule une alimentation conforme les évite. Pour l'édition Enterprise, l'alimentation officielle de 27 W est fortement recommandée. Elle est **obligatoire** lorsque la sonde est équipée d'un SSD NVMe (§ 2.3.3).

2.2.2 Continuité électrique

La sonde est conçue pour qu'une coupure électrique n'affecte pas sa configuration, tant que le support de stockage fonctionne correctement (§ 1.4). Les coupures répétées augmentent néanmoins le risque d'usure et de corruption de la carte microSD.

> **Information** — Une coupure brutale peut faire perdre les toutes dernières écritures (résultats d'exécution, événements encore en attente d'envoi). Les bases sont conçues pour rester cohérentes, seules les dernières transactions pouvant manquer, à condition que la carte respecte les écritures synchrones. Une panne du support lui-même (carte défaillante) relève de la sauvegarde de configuration (chapitre 8).

Situation	Recommandation
Installation en salle informatique ou en baie	Raccorder l'alimentation à une prise ondulée (alimentation sans interruption, ASI)
Installation dans un local sans ondulation	Accepter le risque, ou prévoir un petit onduleur ; programmer des sauvegardes de configuration (chapitre 8)
Coupures programmées (travaux électriques)	Arrêter proprement la sonde avant la coupure (chapitre 8)

2.3 Carte microSD

2.3.1 Carte fournie

La carte microSD fournie contient le système d'exploitation, le moteur principal, le moteur de scénarios, Chromium et l'ensemble des composants nécessaires. Elle est prête à l'emploi : aucune installation de logiciel n'est nécessaire.

Caractéristique	Valeur
Capacité	32 Go minimum
Classe	A2 / U3
Type	« High Endurance », conçu pour des écritures continues, recommandé
Contenu	Image système de la sonde ; sa version est indiquée dans les notes de version et, après la mise en service, par `GET /api/v1/system` (champ `version`)

> **Avertissement** — Ne reformatez pas la carte et ne modifiez pas ses partitions. La seule opération prévue sur la carte avant le premier démarrage est le dépôt facultatif d'un fichier de provisionnement sur sa partition `SVA-BOOT` (chapitre 4). Avec le mécanisme de mise à jour A/B, d'autres partitions de la carte peuvent apparaître sur votre poste : ne les modifiez pas. Toute autre modification peut rendre la sonde inutilisable.

2.3.2 Conservation et manipulation

Conservez la carte dans son étui jusqu'à l'installation. Évitez de toucher ses contacts dorés, de la plier, de l'exposer à l'humidité, à la chaleur ou à l'électricité statique. Notez son numéro de série ou la référence de commande avant l'insertion si votre gestion de parc l'exige.

2.3.3 Stockage sur SSD

Les cartes microSD ont une durée de vie limitée par le volume de données écrites. La **carte microSD reste le support principal** de la sonde et **suffit à un usage standard**, quelle que soit l'édition. Un **SSD NVMe** (*Non-Volatile Memory Express*, disque à mémoire flash raccordé par le bus PCI Express) peut la compléter. Il est **facultatif** et surtout recommandé pour l'édition Enterprise, dont les scénarios navigateur produisent davantage d'écritures.

Le SSD sert uniquement de **volume de données** :

Support	Contenu
Carte microSD (toujours)	Partition de démarrage, deux emplacements système (mécanisme de mise à jour, chapitre 8), certificat d'édition, configuration et secrets
SSD NVMe (s'il est activé)	Historique des exécutions, agrégats, artefacts (captures d'écran), file d'attente d'export, journaux persistants

La sonde démarre toujours sur la microSD : l'ordre de démarrage du Raspberry Pi 5 n'est pas modifié. Le droit d'utilisation reste attaché à la carte microSD. Si le SSD devient absent ou défaillant, les contrôles continuent de s'exécuter, l'historique local est conservé sur la microSD en mode réduit et l'état de santé `storage` passe en `CRITICAL` (§ 8.3.4).

Si vous retenez cette option, réunissez le matériel suivant :

Élément	Exigence
Carte d'extension	**Carte M.2 HAT+ officielle de Raspberry Pi**. Elle fonctionne en PCIe 2.0 x1 (environ 500 Mo/s). Le mode PCIe Gen 3, non certifié par Raspberry Pi, n'est pas utilisé par la sonde
SSD	SSD NVMe au format M.2 **2230 ou 2242**, figurant dans la liste des modèles pris en charge, publiée dans les notes de version
Alimentation	**Alimentation officielle Raspberry Pi 27 W USB-C**, obligatoire avec un SSD (§ 2.2.1)
Refroidissement	Compatible avec le refroidisseur actif officiel (*Active Cooler*), qui doit être **installé en premier**, avant la carte M.2 HAT+ (chapitre 3)
Boîtier	Le boîtier officiel Raspberry Pi 5 n'est utilisable **que sans son couvercle ni son ventilateur**. Avec un autre boîtier, vérifiez auprès de son fabricant qu'il accepte une carte M.2 HAT+

Le montage du matériel est décrit au chapitre 3 (§ 3.4.6) et l'activation du SSD par la sonde au chapitre 8 (§ 8.3.4).

> **Attention** — L'activation **formate entièrement** le SSD. N'utilisez pas un SSD qui contient des données à conserver.

2.3.4 Carte de rechange

Pour les sondes dont la disponibilité est critique, il est recommandé de disposer d'une carte microSD préconfigurée de rechange et d'une sauvegarde récente de la configuration. La remise en service consiste alors à remplacer la carte, à effectuer la mise en service puis à restaurer la configuration (chapitre 8).

2.4 Refroidissement et boîtier

Le processeur du Raspberry Pi 5 réduit automatiquement sa fréquence lorsqu'il chauffe. Ce bridage thermique ralentit les contrôles, notamment les parcours navigateur, et fausse les mesures de durée.

Édition	Refroidissement
Essential, Professional	Refroidisseur actif officiel ou boîtier ventilé **recommandé**
Enterprise	Refroidisseur actif officiel ou boîtier ventilé **obligatoire**

Pour l'offre microSD préconfigurée, choisissez un boîtier qui :

- laisse accessibles le lecteur de carte microSD, le port Ethernet, le connecteur USB-C d'alimentation et, si possible, le bouton d'alimentation ;
- assure une circulation d'air suffisante ou intègre un ventilateur ;
- protège la carte des contacts accidentels et de la poussière ;
- se fixe de manière stable dans votre environnement : étagère, baie, support mural.

La sonde surveille la température de son processeur et signale tout bridage thermique (chapitre 7 du guide d'utilisation et de supervision).

> **Information** — Si la sonde reçoit un SSD NVMe (§ 2.3.3), le refroidisseur actif officiel reste utilisable : il s'installe en premier, sous la carte M.2 HAT+. Le boîtier officiel Raspberry Pi 5 ne peut alors être utilisé que sans son couvercle ni son ventilateur.

2.5 Réseau

2.5.1 Raccordement

La sonde se raccorde **exclusivement en Ethernet filaire**. Le Raspberry Pi 5 dispose d'un port Ethernet Gigabit RJ45.

Élément	Exigence
Câble	Câble Ethernet catégorie 5e ou supérieure, longueur adaptée
Prise réseau	Port de commutateur actif, dans le réseau ou le VLAN choisi pour la sonde
Débit	100 Mbit/s suffisent ; 1 Gbit/s pris en charge
Alimentation par Ethernet (PoE)	Non prise en charge : la carte d'extension officielle PoE+ (HAT PoE+) n'est pas prévue pour la sonde. Alimentez la sonde par son port USB-C (§ 2.2)
Contrôle d'accès au réseau (802.1X)	Pris en charge par certificat (méthode EAP-TLS) (§ 5.2.6) ; exception par adresse MAC (MAB) possible en alternative. Prérequis ci-dessous

Si le port de raccordement est protégé par le contrôle d'accès **802.1X**, norme selon laquelle un équipement doit s'authentifier auprès du commutateur avant d'obtenir l'accès au réseau, préparez avec votre équipe réseau :

- un **serveur RADIUS** (*Remote Authentication Dial-In User Service*, serveur qui valide les authentifications transmises par le commutateur) acceptant la méthode **EAP-TLS**, c'est-à-dire l'authentification par certificat ;
- un **certificat client** pour la sonde, émis par votre infrastructure de gestion de clés (IGC), avec l'identité que la sonde présentera au serveur RADIUS. Il est recommandé de faire générer la clé et la demande de certificat (CSR) par la sonde elle-même, après une première mise en service sur un port non contrôlé : la clé privée ne quitte alors jamais l'appareil. Si la sonde doit s'authentifier dès son premier démarrage, prévoyez à la place un fichier PKCS#12 (clé et certificat) et son mot de passe, déposés sur la microSD avec le fichier de provisionnement (chapitre 4) ;
- le certificat de l'**autorité de certification (AC)** qui a émis le certificat du serveur RADIUS, au format PEM ;
- à défaut, ou pour la seule mise en service, une **exception par adresse MAC** (MAB, *MAC Authentication Bypass*) sur le port de la sonde ;
- de préférence, la **pile officielle de l'horloge temps réel** (RTC, *Real-Time Clock*) du Raspberry Pi 5, installée sur la carte. La vérification des certificats EAP-TLS dépend de l'heure, alors que les serveurs NTP ne sont joignables qu'après l'authentification : la pile conserve l'heure lorsque la sonde est hors tension. Sans elle, l'heure de départ est la dernière heure enregistrée par la sonde ou, à défaut, la date de construction de l'image (§ 5.2.6).

La procédure complète figure au chapitre 5 (§ 5.2.6).

> **Attention** — La sonde ne prend en charge ni l'étiquetage VLAN (IEEE 802.1Q) sur la prise de la sonde, ni la méthode PEAP (authentification 802.1X par identifiant et mot de passe). Raccordez la sonde à un port d'accès configuré dans le VLAN choisi.

> **Évolution prévue** — La connexion Wi-Fi n'est pas prise en charge. Le Wi-Fi et le Bluetooth intégrés au Raspberry Pi 5 sont désactivés dans le système de la sonde, par une surcouche de l'arbre des périphériques (*device tree overlay*).

2.5.2 Choix de l'emplacement réseau

L'emplacement de la sonde détermine ce qu'elle mesure (§ 1.2.1). Avant l'installation, déterminez :

1. le **réseau ou VLAN** de raccordement, en fonction des services à superviser et du point de vue souhaité (utilisateurs d'un site, centre de données, accès Internet, site distant ou à l'étranger, réseau d'un client ou d'un partenaire) ;
2. le **mode d'adressage** : adresse attribuée par DHCP (par défaut) ou adresse IP fixe. Une adresse fixe, ou une réservation DHCP, est recommandée pour qu'administrateurs et plateformes de supervision joignent toujours la sonde à la même adresse. L'IPv4 est obligatoire ; l'IPv6 est facultatif et désactivé par défaut. Activez-le si des ressources à superviser ne sont joignables qu'en IPv6, ou si vous souhaitez contrôler leur accès en IPv6 (§ 5.2.5) ;
3. les **serveurs DNS** que la sonde doit utiliser. Ils déterminent les noms qu'elle sait résoudre ; utilisez les mêmes que les utilisateurs dont vous voulez reproduire le point de vue ;
4. les **serveurs NTP**. Une heure exacte est indispensable à la cohérence des résultats, des certificats et des exports ;
5. le **proxy sortant** éventuel, nécessaire si la sonde doit joindre des sites externes, une plateforme SaaS ou le dépôt de mises à jour et que votre réseau impose un proxy.

Si vous choisissez une adresse fixe, préparez les informations suivantes :

Paramètre	Exemple fictif	Votre valeur
Adresse IP et masque	`192.0.2.50/24`	

Paramètre	Exemple fictif	Votre valeur
Passerelle	`192.0.2.1`	
Adresse IPv6 et passerelle IPv6, si l'IPv6 est activé en mode statique	`2001:db8:10::50/64`, `2001:db8:10::1`	
Serveurs DNS	`192.0.2.10`, `192.0.2.11`	
Domaine de recherche DNS	`example.internal`	
Serveurs NTP	`ntp1.example.internal`	
Proxy sortant et exclusions	`http://proxy.example.internal:3128`, sauf `.example.internal`	
Nom d'hôte souhaité	`sonde-paris-01`	
Nom de site	`paris-dc1`	

2.5.3 Résumé des flux réseau

Les flux nécessaires sont détaillés au chapitre 5 et récapitulés dans le tableau des flux réseau du chapitre 10, à transmettre à vos équipes réseau et sécurité. En synthèse :

Sens	Flux	Obligatoire
Entrant vers la sonde	HTTPS (TCP 443) depuis les postes d'administration et, le cas échéant, depuis Prometheus, Nagios ou Centreon	Oui, depuis le réseau d'administration
Entrant vers la sonde	HTTP (TCP 80), redirection vers HTTPS uniquement	Non : facultatif, désactivable
Entrant vers la sonde	mDNS (UDP 5353), découverte du nom `.local` sur le réseau local	Non : désactivable
Entrant vers la sonde	SSH (TCP 22) depuis les postes d'administration	Non : désactivé par défaut
Sortant	DHCP, DNS, NTP	Oui (DHCP si utilisé)
Entrant et sortant	ICMPv6 de découverte des voisins, sur le réseau local de la sonde	Si l'IPv6 est activé
Couche 2, entre la sonde et le commutateur	EAPOL (authentification 802.1X), sans flux IP	Si le port est protégé par 802.1X
Sortant	Vers chaque ressource supervisée, selon les contrôles : ICMP, ports TCP, HTTP(S), ports des bases de données	Oui
Sortant	Vers les destinations d'export : collecteur OpenTelemetry, agent Datadog, plateformes SaaS	Selon votre configuration
Sortant	Vers le service de distribution des mises à jour de l'éditeur, en HTTPS : `https://updates-synovex.incitypark.fr` (adresse par défaut, inscrite dans le profil éditeur), ou vers votre miroir interne. Sans ce service, les images signées s'importent hors ligne, après leur transmission par le canal convenu dans votre contrat (§ 8.4.4 ; § 10.5)	Si mises à jour en ligne

Lorsque l'IPv6 est activé, ces flux s'entendent en IPv4 et en IPv6. Aucun flux entrant depuis Internet n'est nécessaire.

> ✓ **Conseil** — Placez la sonde dans un réseau d'où elle peut atteindre les ressources supervisées, mais limitez ses flux entrants aux seuls postes et serveurs qui en ont besoin. La sonde manipule des identifiants de comptes de test : traitez-la comme un équipement d'infrastructure sensible.

2.6 Prérequis de sécurité et de gouvernance

La sonde agit dans votre système d'information comme un utilisateur automatisé. Son déploiement doit être validé et préparé comme celui de tout compte de service.

2.6.1 Accord des équipes concernées

Avant le déploiement, obtenez l'accord :

- de l'**équipe sécurité**, sur l'installation d'un équipement dans le réseau, les flux, le stockage de secrets et l'usage de comptes de test ;
- des **responsables des applications supervisées**, qui doivent savoir que des transactions automatisées seront exécutées régulièrement, pour ne pas les confondre avec une attaque ou du trafic anormal ;
- de l'**équipe réseau**, pour le raccordement, l'adressage et les ouvertures de flux.

> ! **Attention** — Les contrôles répétés, en particulier les tentatives de connexion, peuvent déclencher des protections : blocage de compte après échecs, limitation de débit, détection d'intrusion, pare-feu applicatif. Faites déclarer l'adresse de la sonde auprès des équipes concernées et prévoyez si nécessaire des exceptions.

2.6.2 Comptes et données de test

Chaque contrôle qui s'authentifie doit utiliser un **compte de test dédié**, jamais un compte personnel ni un compte d'administration.

Exigence	Raison
Compte nominatif « supervision », distinct pour chaque application	Traçabilité ; un compte compromis n'ouvre pas l'accès aux autres applications
Droits minimaux : lecture seule lorsque c'est possible	Limiter l'impact d'une erreur de scénario ou d'une fuite de secret
Mot de passe non soumis à expiration automatique, ou procédure de rotation planifiée	Éviter les fausses alertes à l'expiration du mot de passe
Pas d'authentification multifacteur interactive, ou mécanisme adapté aux comptes de service validé par votre équipe sécurité	Un scénario automatisé ne peut pas saisir un code reçu par téléphone
Données de test identifiables : articles, clients, commandes marqués comme fictifs	Éviter que les actions des scénarios faussent l'activité réelle ou les statistiques
Pour les bases de données : compte en **lecture seule** limité aux tables nécessaires	Une requête de contrôle ne doit jamais pouvoir modifier des données

> ! **Avertissement** — Un scénario qui ajoute un produit au panier, passe une commande ou effectue un paiement agit réellement sur l'application. N'exécutez ces scénarios en production qu'avec des articles et des moyens de paiement de test prévus à cet effet, et avec l'accord des équipes métier. Le chapitre 5 du guide de développement des scénarios présente les précautions applicables à chaque exemple.

2.6.3 Secrets

Recensez les secrets dont la sonde aura besoin : mots de passe des comptes de test, jetons d'API des applications supervisées, mots de passe des comptes de base de données, clés d'API des plateformes d'observabilité. Ils seront saisis dans le coffre de secrets de la sonde (chapitre 6) et ne doivent jamais figurer en clair dans la définition d'un contrôle, un script ou un fichier de provisionnement. Prévoyez qui les détient, comment ils sont transmis à l'administrateur de la sonde et à quel rythme ils sont renouvelés.

2.6.4 Certificats

La sonde génère au premier démarrage un certificat autosigné pour son interface HTTPS. Si votre politique impose des certificats émis par votre autorité de certification interne, préparez la demande de certificat (nom d'hôte, éventuellement adresse IP) ; la procédure de remplacement figure au chapitre 5. Si les applications supervisées utilisent des certificats émis par une autorité interne, préparez le certificat de cette autorité pour l'importer dans la sonde, faute de quoi les contrôles HTTPS échoueront avec une erreur de certificat.

2.6.5 Édition et droit d'utilisation

L'édition acquise est inscrite sur la carte microSD lors de sa préparation (certificat d'édition, § 4.5). Elle est vérifiée localement par la sonde, sans connexion à un serveur de l'éditeur. **Aucune clé de licence n'est à préparer ni à saisir** : vérifiez simplement que l'édition indiquée sur l'encart ou l'étiquette correspond à votre commande.

2.7 Poste d'administration

L'administration s'effectue depuis un poste de travail raccordé à un réseau autorisé à joindre la sonde en HTTPS.

Élément	Exigence
Navigateur	Chrome, Edge, Firefox ou Safari, dans l'une de leurs deux dernières versions majeures, ou Firefox ESR
Accès réseau	Accès HTTPS (TCP 443) à l'adresse de la sonde
Lecteur de carte	Lecteur de carte microSD, ou adaptateur SD, si vous utilisez le fichier de provisionnement, si vous devez lire le code d'installation sur la carte, ou, sans écran, pour lire l'empreinte du certificat dans `setup-code.txt` (§ 4.4.4)
Outils facultatifs	Client en ligne de commande pour l'API (par exemple `curl`), client SSH pour la maintenance avancée
Développement de scénarios (Enterprise)	Node.js et Puppeteer installés sur le poste pour tester les scénarios avant déploiement, avec le lanceur local fourni avec les exemples (chapitre 5 du guide de développement des scénarios) ; éditeur de code

2.8 Conditions d'installation physique

Critère	Recommandation
Local	Local technique, baie ou bureau fermé, à accès contrôlé : la carte microSD contient des secrets chiffrés et la configuration de la sonde
Température ambiante	Plage de température de fonctionnement indiquée par Raspberry Pi Ltd dans la fiche produit du Raspberry Pi 5 ; éviter la proximité de sources de chaleur et l'exposition directe au soleil
Humidité, poussière	Environnement sec et propre, sans condensation
Ventilation	Laisser plusieurs centimètres libres autour des ouïes du boîtier

Critère	Recommandation
Fixation	Surface stable, plane, non conductrice, ou fixation prévue par le boîtier ; câbles sans tension
Accès	Accès possible au lecteur de carte microSD, au bouton d'alimentation et aux voyants pour la maintenance
Alimentation	Prise à proximité, de préférence ondulée
Étiquetage	Étiqueter la sonde avec son nom d'hôte, son adresse IP et le contact de l'équipe responsable

> **Avertissement** — La protection physique de la sonde fait partie de sa sécurité. Une personne disposant d'un accès physique peut retirer la carte microSD. Les secrets y sont chiffrés, mais la meilleure protection reste un emplacement à accès restreint (chapitre 5).

2.9 Liste de vérification avant démarrage

Complétez cette liste avant de procéder à l'installation physique (chapitre 3). Une version imprimable figure au chapitre 10.

N°	Vérification	Responsable	Fait
1	Édition acquise connue et conforme à la commande (encart ou étiquette)	Chef de projet	[ ]
2	Raspberry Pi 5 de capacité mémoire conforme à l'édition (§ 2.1.2), ou boîtier complet reçu	Technicien	[ ]
3	Alimentation USB-C conforme (§ 2.2), prise de préférence ondulée	Technicien	[ ]
4	Refroidissement et boîtier conformes (§ 2.4)	Technicien	[ ]
5	Carte microSD préconfigurée en bon état, version notée	Technicien	[ ]
6	Emplacement physique choisi et conforme (§ 2.8)	Technicien	[ ]
7	Port réseau actif dans le VLAN choisi ; câble Ethernet disponible	Équipe réseau	[ ]
8	Mode d'adressage décidé : DHCP avec réservation ou IP fixe ; paramètres réseau réunis (§ 2.5.2)	Équipe réseau	[ ]
9	Serveurs DNS et NTP accessibles depuis le réseau de la sonde	Équipe réseau	[ ]
10	Proxy sortant identifié, le cas échéant	Équipe réseau	[ ]
11	Flux entrants HTTPS autorisés depuis les postes d'administration	Équipe sécurité	[ ]
12	Flux sortants vers les ressources supervisées autorisés	Équipe sécurité	[ ]
13	Flux vers les destinations d'export et le dépôt de mises à jour autorisés, si utilisés	Équipe sécurité	[ ]
14	Accord des responsables des applications supervisées ; adresse de la sonde déclarée	Chef de projet	[ ]
15	Comptes de test créés, avec droits minimaux (§ 2.6.2)	Responsables applicatifs	[ ]
16	Secrets recensés et circuit de transmission défini (§ 2.6.3)	Équipe sécurité	[ ]
17	Certificat d'autorité interne disponible, si des applications utilisent une AC interne (§ 2.6.4)	Équipe sécurité	[ ]
18	Mode de mise en service choisi : fichier de provisionnement ou assistant (chapitre 4)	Administrateur	[ ]
19	Poste d'administration avec navigateur récent et accès au réseau de la sonde (§ 2.7)	Administrateur	[ ]
20	Lecteur de carte microSD disponible, si nécessaire (§ 2.7)	Administrateur	[ ]

N°	Vérification	Responsable	Fait
21	Premiers contrôles à créer identifiés, avec leurs critères de réussite	Responsables applicatifs	[ ]
22	Destinataires des alertes et plateforme de supervision cible identifiés (chapitre 2 du guide d'intégration et d'observabilité)	Exploitation	[ ]
23	Si le port est protégé par 802.1X : serveur RADIUS, certificat client ou exception MAB, certificat de l'AC du serveur RADIUS préparés ; pile officielle de l'horloge temps réel (RTC) recommandée (§ 2.5.1)	Équipe réseau	[ ]
24	Si un SSD NVMe est prévu : carte M.2 HAT+ officielle, SSD pris en charge et alimentation de 27 W réunis (§ 2.3.3)	Technicien	[ ]

Lorsque toutes les lignes sont cochées, vous pouvez procéder à l'installation physique décrite au chapitre 3.

Chapitre 3 — Installation physique

Ce chapitre décrit l'installation matérielle de la sonde, depuis l'ouverture du colis jusqu'au premier allumage. Deux parcours sont proposés, selon l'offre acquise :

- **Offre microSD préconfigurée** : vous fournissez le Raspberry Pi 5 et ses accessoires, puis vous assemblez l'ensemble ;
- **Offre boîtier complet**, prêt à l'emploi : la sonde vous est livrée assemblée ; il suffit de l'installer et de la raccorder.

Les § 3.1 à § 3.3 concernent les deux offres. Le § 3.4 est propre à l'offre microSD préconfigurée, le § 3.5 à l'offre boîtier complet. Les § 3.6 à § 3.10 s'appliquent de nouveau aux deux.

> **Information** — Ce chapitre traite uniquement du matériel et du raccordement. La configuration logicielle (adresse IP, compte administrateur, vérification de l'édition) fait l'objet du chapitre 4. Il est recommandé de lire le chapitre 4 **avant** d'allumer la sonde : selon la méthode de mise en service choisie, un fichier de provisionnement doit parfois être déposé sur la microSD avant le premier démarrage (voir § 4.3).

3.1 Vue d'ensemble de la procédure

Le schéma suivant résume l'enchaînement des opérations.

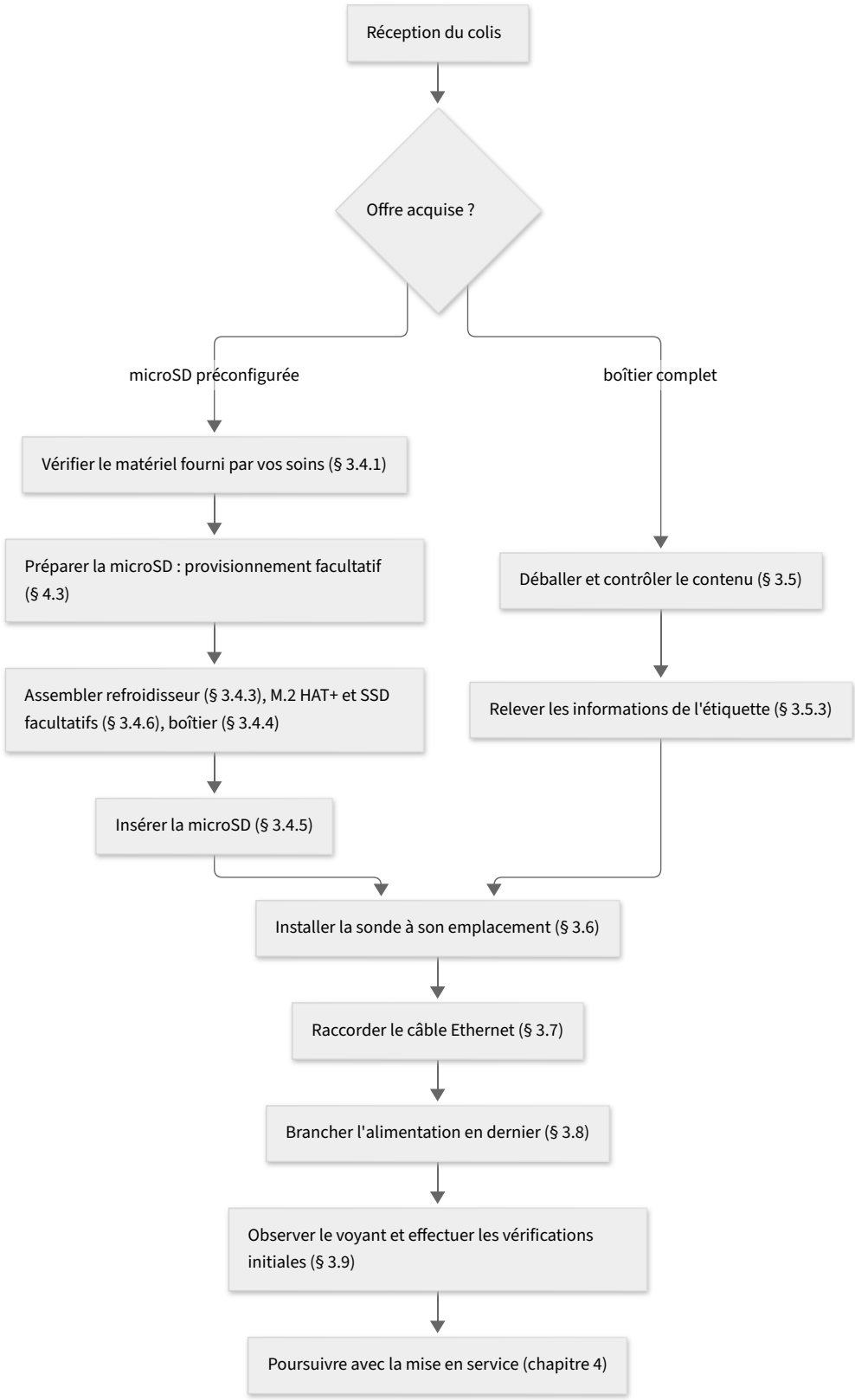


Schéma 3-1 — Enchaînement des opérations d'installation physique

Durée indicative : 10 minutes pour le boîtier complet, 20 à 30 minutes pour la microSD préconfigurée, hors préparation éventuelle du fichier de provisionnement.

3.2 Précautions de manipulation

Le Raspberry Pi 5 est une carte électronique nue. Comme tout équipement de ce type, il est sensible aux décharges électrostatiques, aux contraintes mécaniques et à l'humidité.

> **Avertissement** — Ne manipulez jamais la carte, la microSD ou les accessoires lorsque l'alimentation est branchée. Débranchez toujours le câble d'alimentation USB-C avant toute intervention à l'intérieur du boîtier.

3.2.1 Protection contre les décharges électrostatiques

Une décharge électrostatique (ESD, *ElectroStatic Discharge*) est le transfert brutal de charges électriques accumulées sur le corps humain vers un composant électronique. Elle est souvent imperceptible pour l'opérateur, mais peut endommager durablement un composant.

Appliquez les règles suivantes :

1. Travaillez sur une surface non conductrice et dégagée (table en bois ou tapis antistatique). Évitez la moquette et les vêtements en laine ou en fibres synthétiques.
2. Avant de saisir la carte, touchez une partie métallique reliée à la terre (châssis d'une baie raccordée à la terre, par exemple) ou portez un bracelet antistatique relié à la terre.
3. Tenez la carte **par ses bords**. Ne touchez ni les composants, ni les broches du connecteur GPIO, ni les contacts dorés de la microSD.
4. Conservez la carte dans son sachet antistatique d'origine jusqu'au moment de l'assemblage.

3.2.2 Précautions mécaniques

- N'exercez aucune pression sur les composants lors de la pose du refroidisseur ou de la fermeture du boîtier.
- N'insérez ni ne retirez la microSD en forçant : elle n'entre que dans un seul sens (voir § 3.4.5).
- Ne pliez pas les nappes ou câbles fins (câble du ventilateur notamment) à angle vif.
- Ne posez pas d'objet sur la sonde une fois installée : la circulation d'air doit rester libre.

3.2.3 Précautions liées à l'environnement

- N'installez pas la sonde dans un lieu humide, poussiéreux ou exposé aux projections de liquide.
- Ne l'exposez pas au rayonnement direct du soleil ni à proximité d'une source de chaleur.
- Respectez la plage de température ambiante de fonctionnement indiquée par Raspberry Pi Ltd dans la fiche produit du Raspberry Pi 5 (§ 2.8).
- Laissez le matériel s'acclimater environ une heure s'il a été transporté par temps froid, afin d'éviter toute condensation lors de la mise sous tension.

3.3 Identification du matériel

3.3.1 Le Raspberry Pi 5

La sonde repose exclusivement sur le **Raspberry Pi 5**. Aucun autre modèle n'est pris en charge par l'image fournie : son fonctionnement sur un Raspberry Pi 4 ou sur une autre carte n'est ni pris en charge ni garanti (§ 2.1.1).

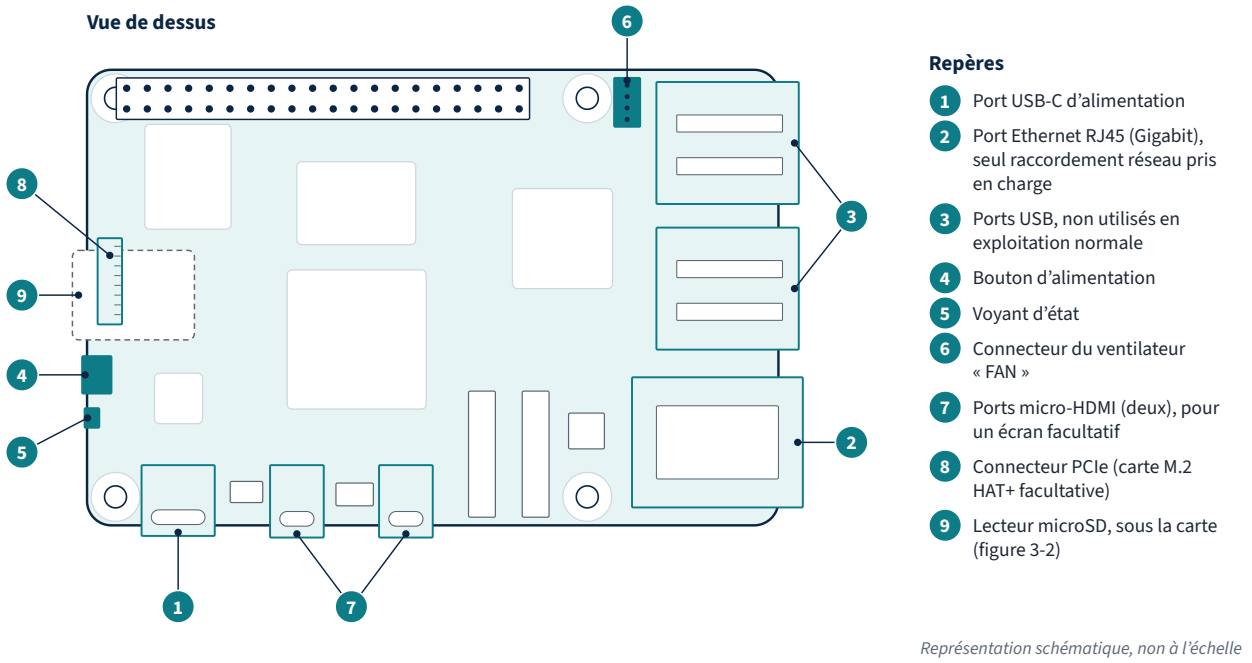


Figure 3-1 — Vue de dessus du Raspberry Pi 5 avec repérage des éléments utiles : port USB-C d'alimentation, port Ethernet, ports USB, bouton d'alimentation, voyant d'état, connecteur du ventilateur, ports micro-HDMI

Le tableau suivant recense les éléments de la carte utilisés lors de l'installation.

Élément	Emplacement	Usage pour la sonde
Port USB-C	Grand côté de la carte, à côté des deux ports micro-HDMI	Alimentation électrique
Port Ethernet RJ45 (Gigabit)	Petit côté de la carte, avec les ports USB	Raccordement au réseau — **seul mode de connexion pris en charge**
Lecteur de carte microSD	**Face inférieure** de la carte, sur le petit côté opposé aux ports Ethernet et USB	Accueille la microSD contenant le système
Bouton d'alimentation	Bord de la carte (repère sur l'figure 3-1)	Mise en marche et arrêt. Comportement standard de Raspberry Pi OS sur Raspberry Pi 5 : sonde arrêtée, un appui la démarre ; sonde en fonctionnement, un appui bref déclenche l'arrêt propre et un appui long force la coupure
Voyant d'état	Bord de la carte (repère sur l'figure 3-1)	Indique l'état d'alimentation et l'activité (voir § 3.9.1)
Connecteur du ventilateur (marqué « FAN »)	Face supérieure (repère sur l'figure 3-1)	Raccordement du refroidisseur actif ou du ventilateur du boîtier
Ports micro-HDMI (deux)	Même côté que le port USB-C	Facultatif : affichage du code d'installation et de l'empreinte du certificat sur un écran (voir § 4.4.3)

Élément	Emplacement	Usage pour la sonde
Ports USB	Côté du port Ethernet	Non utilisés en exploitation normale

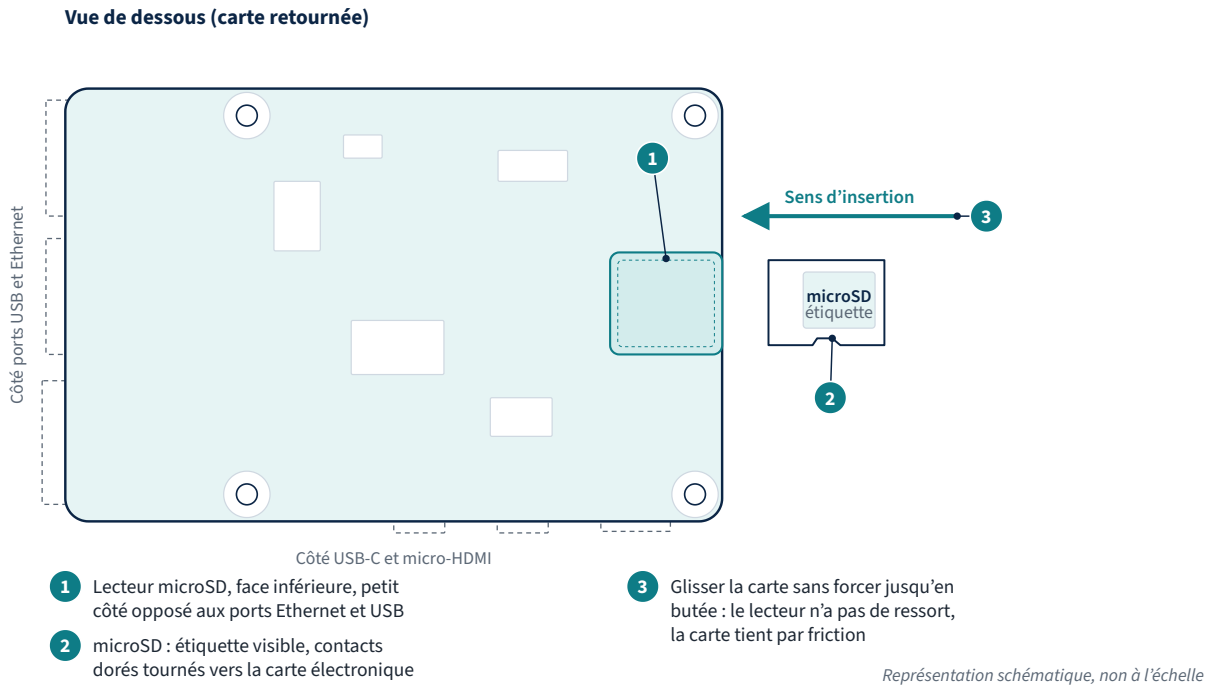


Figure 3-2 — Vue de dessous du Raspberry Pi 5 : emplacement du lecteur microSD, flèche indiquant le sens d'insertion de la carte

3.3.2 La quantité de mémoire

Le Raspberry Pi 5 existe en plusieurs capacités de mémoire vive (RAM). La capacité requise dépend de l'édition de la sonde.

Édition	RAM minimale	RAM recommandée
Essential	2 Go	4 Go
Professional	4 Go	4 Go ou plus
Enterprise	**8 Go**	8 Go

La capacité est indiquée sur l'emballage de la carte ; après la mise en service, elle est également visible dans l'état de santé de la sonde (§ 4.6) : la réponse de `GET /api/v1/system` l'indique dans le champ `resources.memoryTotalBytes`, en octets. Les raisons de ces exigences, liées notamment au navigateur Chromium utilisé par les scénarios de l'édition Enterprise, sont détaillées au chapitre 2.

3.3.3 La microSD préconfigurée

La microSD fournie contient le système de la sonde. Elle porte son numéro de série et est accompagnée d'un **encart d'identification** qui indique l'édition acquise, le numéro de série du produit et le **code d'installation** (§ 4.4.3). Conservez cet encart en lieu sûr : le code d'installation donne accès à la mise en service. La référence du produit figure sur votre bon de commande ; la version de l'image est indiquée dans les notes de version et, après la mise en service, par `GET /api/v1/system` (champ `version`).

> ! **Attention** — Ne reformatez pas la microSD et n'y installez pas d'autre système. Si vous ouvrez la carte sur un ordinateur pour y déposer un fichier de provisionnement (§ 4.3), votre système d'exploitation peut proposer de « formater » une partition qu'il ne sait pas lire : **refusez systématiquement**. Seule la partition de dépôt, au format FAT32 et étiquetée `SVA-BOOT`, est destinée à être ouverte depuis un poste de travail. Avec le mécanisme de mise à jour A/B, d'autres partitions de la carte peuvent apparaître sur votre poste : ne les modifiez pas.

3.4 Assemblage avec la microSD préconfigurée

3.4.1 Matériel à réunir

Objectif : disposer de tous les éléments nécessaires avant de commencer l'assemblage.

Le tableau suivant liste le matériel que vous devez fournir. Les exigences détaillées figurent au chapitre 2.

Élément	Exigence	Remarque
Raspberry Pi 5	RAM selon l'édition (§ 3.3.2)	Modèle 5 exclusivement
Alimentation	Alimentation officielle Raspberry Pi 27 W USB-C (5,1 V, 5 A) recommandée	Une alimentation 5 V / 3 A fonctionne, mais limite le courant disponible sur les ports USB ; c'est un comportement documenté du Raspberry Pi 5
Refroidissement	Refroidisseur actif officiel (*Active Cooler*) ou boîtier équipé d'un ventilateur	**Obligatoire pour l'édition Enterprise**, recommandé pour les autres
Boîtier	Boîtier compatible Raspberry Pi 5, ventilé, laissant accès au lecteur microSD, au port Ethernet et au port USB-C	Le boîtier officiel Raspberry Pi 5 intègre un ventilateur
Câble Ethernet	Catégorie 5e minimum, longueur adaptée	Câble droit standard
microSD préconfigurée	Fournie	Ne pas la remplacer par une autre carte
Facultatif	Écran HDMI + câble micro-HDMI vers HDMI	Pour lire le code d'installation et l'empreinte du certificat à l'écran (§ 4.4.3)
Facultatif	Carte M.2 HAT+ officielle de Raspberry Pi et SSD NVMe M.2 2230 ou 2242 pris en charge	Volume de données complémentaire, surtout utile pour l'édition Enterprise (§ 2.3.3). Exige l'alimentation officielle de 27 W
Facultatif	Pile officielle de l'horloge temps réel (RTC) du Raspberry Pi 5	Recommandée si le port réseau est protégé par 802.1X : elle conserve l'heure hors tension, nécessaire à la vérification des certificats avant tout accès NTP (§ 2.5.1, § 5.2.6)

> ✓ **Conseil** — Le boîtier officiel Raspberry Pi 5 et le refroidisseur actif officiel ne s'utilisent généralement pas ensemble, le boîtier disposant de son propre ventilateur. Suivez la notice du fabricant de votre boîtier pour savoir quel refroidissement installer. Si vous installez la carte M.2 HAT+ et un SSD (§ 3.4.6), le boîtier officiel n'est utilisable que **sans son couvercle ni son ventilateur** : le refroidissement est alors assuré par le refroidisseur actif officiel, installé en premier.

3.4.2 Préparer la microSD (facultatif)

Si vous avez choisi la mise en service par **fichier de provisionnement** (méthode A du chapitre 4), préparez la microSD **maintenant**, avant de l'insérer dans la carte. La procédure est décrite au § 4.3. Si le port réseau de la sonde est protégé par 802.1X et que la sonde doit s'y authentifier dès son premier démarrage, déposez à cette étape, à côté du fichier de provisionnement, le fichier PKCS#12 de la sonde et le certificat de l'AC du serveur RADIUS (§ 4.3.3 et § 5.2.6). Si vous utilisez l'assistant web (méthode B), passez directement au § 3.4.3.

3.4.3 Installer le refroidissement

Objectif : assurer une dissipation thermique suffisante pour un fonctionnement permanent.

Prérequis : carte hors tension et hors de son sachet ; précautions ESD appliquées (§ 3.2.1).

Étapes (refroidisseur actif officiel) :

1. Posez la carte sur une surface plane, face supérieure visible.
2. Retirez les films de protection des pastilles thermiques situées sous le refroidisseur.
3. Positionnez le refroidisseur au-dessus de la carte en alignant ses deux tiges de fixation sur les deux trous de montage prévus à cet effet.
4. Enfoncez les tiges de fixation en appuyant **sur les tiges elles-mêmes**, et non sur le corps du refroidisseur, jusqu'au clic.
5. Branchez le câble du ventilateur sur le connecteur marqué « FAN », en respectant le détrompeur.
6. Vérifiez que le câble ne touche pas les pales du ventilateur.

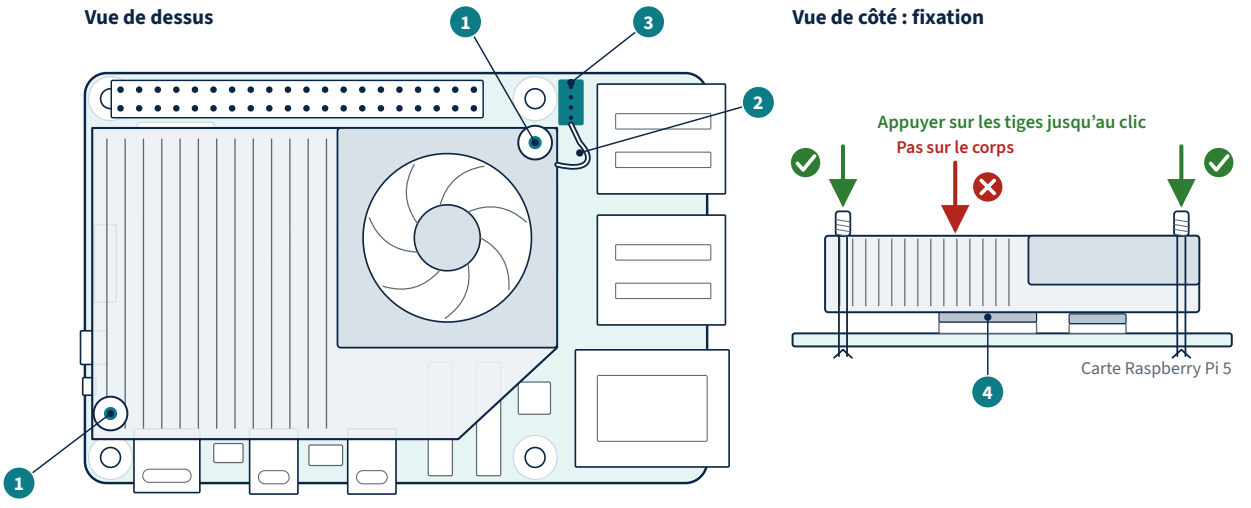


Figure 3-3 — Pose du refroidisseur actif officiel : alignement des tiges de fixation et branchement sur le connecteur FAN

Résultat attendu : le refroidisseur est fermement maintenu, sans jeu ; le câble est branché.

Vérification : la mise en rotation du ventilateur sera observée au premier démarrage. Le ventilateur peut ne pas tourner en permanence : sa vitesse est pilotée selon la température.

Avec un boîtier ventilé : suivez la notice du fabricant ; raccordez son ventilateur au connecteur « FAN » s'il est prévu pour cela.

> **Attention** — Un refroidisseur ne se repose pas : les pastilles thermiques perdent leur efficacité une fois décollées. Ne retirez le refroidisseur qu'en cas de nécessité.

3.4.4 Installer la carte dans le boîtier

Objectif : protéger la carte et faciliter son installation.

Prérequis : refroidissement installé (§ 3.4.3) ; si vous avez retenu l'option SSD, carte M.2 HAT+ et SSD déjà montés (§ 3.4.6).

Étapes :

1. Ouvrez le boîtier selon la notice du fabricant. Suivez aussi ses éventuelles instructions propres au refroidissement (dissipateur fourni avec le boîtier, par exemple), sans les cumuler avec le refroidisseur actif officiel si la notice l'exclut.
2. Placez la carte dans le fond du boîtier en alignant les ports avec les ouvertures correspondantes.
3. Fixez la carte si le boîtier le prévoit (vis ou ergots), sans serrage excessif.
4. Si le boîtier est équipé d'un ventilateur, raccordez-le au connecteur « FAN ».
5. **Ne refermez pas encore le boîtier** s'il masque le lecteur microSD : certains boîtiers exigent l'insertion de la carte avant fermeture. Dans ce cas, réalisez d'abord le § 3.4.5.
6. Refermez le boîtier.

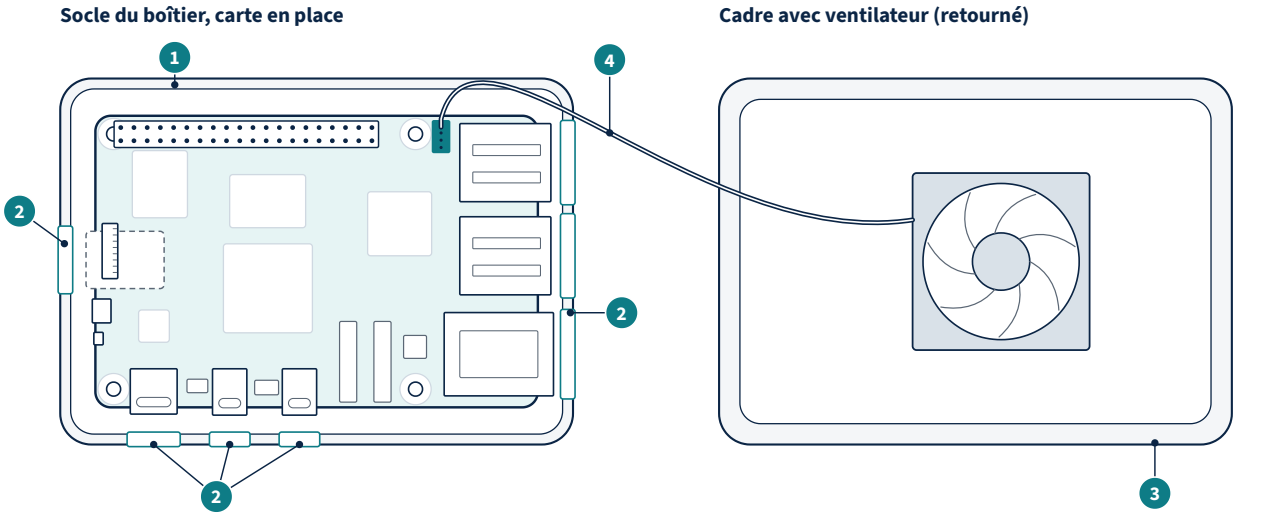


Figure 3-4 — Carte installée dans le boîtier officiel Raspberry Pi 5 : alignement des ports et raccordement du ventilateur

Résultat attendu : la carte est maintenue ; le port USB-C, le port Ethernet et le lecteur microSD restent accessibles.

3.4.5 Insérer la microSD

Objectif : installer le support contenant le système de la sonde.

Prérequis : carte **hors tension** ; microSD préparée si vous utilisez la méthode A (§ 4.3).

Étapes :

1. Repérez le lecteur microSD sur la **face inférieure** de la carte, sur le petit côté opposé aux ports Ethernet et USB (figure 3-2).
2. Tenez la microSD par ses bords, **contacts dorés tournés vers la carte électronique** : lorsque vous regardez la face inférieure de la carte retournée, c'est l'étiquette de la microSD qui est visible.
3. Faites glisser la microSD dans le lecteur, sans forcer, jusqu'à ce qu'elle soit entièrement insérée. Le lecteur du Raspberry Pi 5 n'a pas de mécanisme à ressort : la carte est maintenue par friction.
4. Vérifiez que la carte ne dépasse que légèrement du bord de la carte électronique ou de l'ouverture du boîtier.

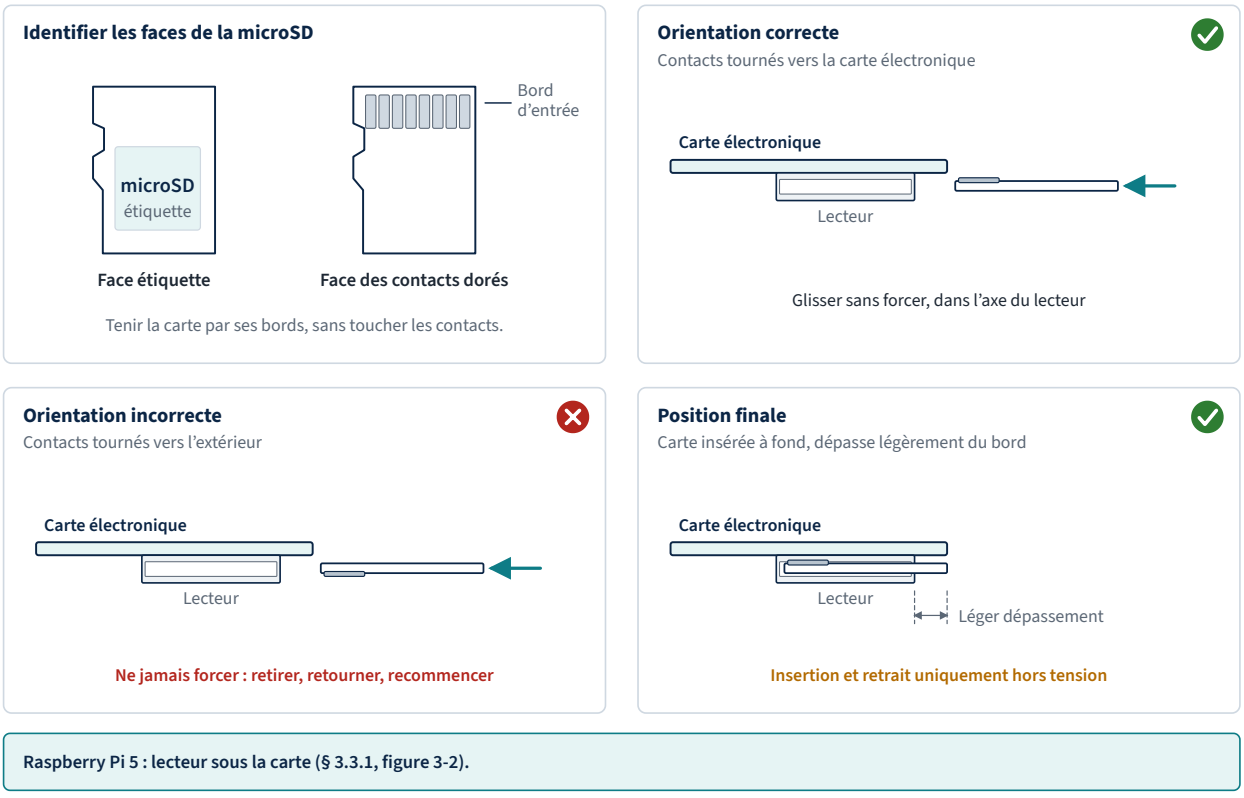


Figure 3-5 — Insertion de la microSD : orientation correcte (contacts vers la carte) et position finale

Résultat attendu : la microSD est insérée à fond et ne bouge pas lorsqu'on effleure son bord.

En cas de problème : si la carte n'entre pas, retirez-la, vérifiez son orientation et recommencez. Ne forcez jamais.

> ! **Attention** — N'insérez et ne retirez jamais la microSD lorsque la sonde est alimentée. Un retrait à chaud peut corrompre le système de fichiers et rendre la sonde inutilisable.

3.4.6 Monter la carte M.2 HAT+ et le SSD NVMe (facultatif)

Cette opération ne concerne que les sondes équipées du SSD NVMe facultatif (§ 2.3.3). Dans l'ordre d'assemblage, elle se place **après** la pose du refroidisseur actif (§ 3.4.3) et **avant** la mise en boîtier (§ 3.4.4). Elle se limite au montage physique : la sonde n'utilise le SSD qu'après son activation, décrite au chapitre 8 (§ 8.3.4).

Objectif : raccorder un SSD NVMe au Raspberry Pi 5 par la carte M.2 HAT+ officielle.

Prérequis :

- carte hors tension, câble d'alimentation USB-C débranché ; précautions ESD appliquées (§ 3.2.1) ;
- refroidisseur actif officiel déjà installé, s'il est utilisé (§ 3.4.3) ;
- carte M.2 HAT+ officielle de Raspberry Pi, avec les accessoires de montage et la notice fournis par le fabricant ;
- SSD NVMe au format M.2 2230 ou 2242, figurant dans la liste des modèles pris en charge (§ 2.3.3) ;
- alimentation officielle Raspberry Pi 27 W USB-C, qui sera utilisée au § 3.8.

Étapes :

1. Vérifiez que le refroidisseur actif, si vous l'utilisez, est déjà en place : il ne peut pas être posé après la carte M.2 HAT+.
2. Installez les entretoises fournies avec la carte M.2 HAT+, ainsi que l'embase GPIO empilable si elle est fournie, selon la notice du fabricant.
3. Raccordez la nappe PCIe au connecteur PCIe du Raspberry Pi 5 (connecteur plat, repère sur l'figure 3-6) : soulevez délicatement le verrou du connecteur, insérez la nappe à fond dans l'orientation indiquée par la notice, puis rabattez le verrou.
4. Placez la carte M.2 HAT+ sur les entretoises et fixez-la avec les vis fournies, sans serrage excessif.
5. Raccordez l'autre extrémité de la nappe au connecteur de la carte M.2 HAT+ : verrou soulevé, nappe insérée à fond, verrou rabattu. L'orientation des contacts de ce côté est celle qu'indique la notice du M.2 HAT+ ; elle n'est pas nécessairement la même qu'à l'étape précédente.
6. Insérez le SSD dans l'emplacement M.2 de la carte, en biais, contacts en premier, puis abaissez-le et fixez-le avec la vis prévue, à la position qui correspond à sa longueur (2230 ou 2242).
7. Vérifiez que la nappe n'est pas pliée à angle vif et qu'elle ne touche pas les pales du ventilateur.
8. Poursuivez avec la mise en boîtier (§ 3.4.4). Avec le boîtier officiel Raspberry Pi 5, n'installez ni son couvercle ni son ventilateur.

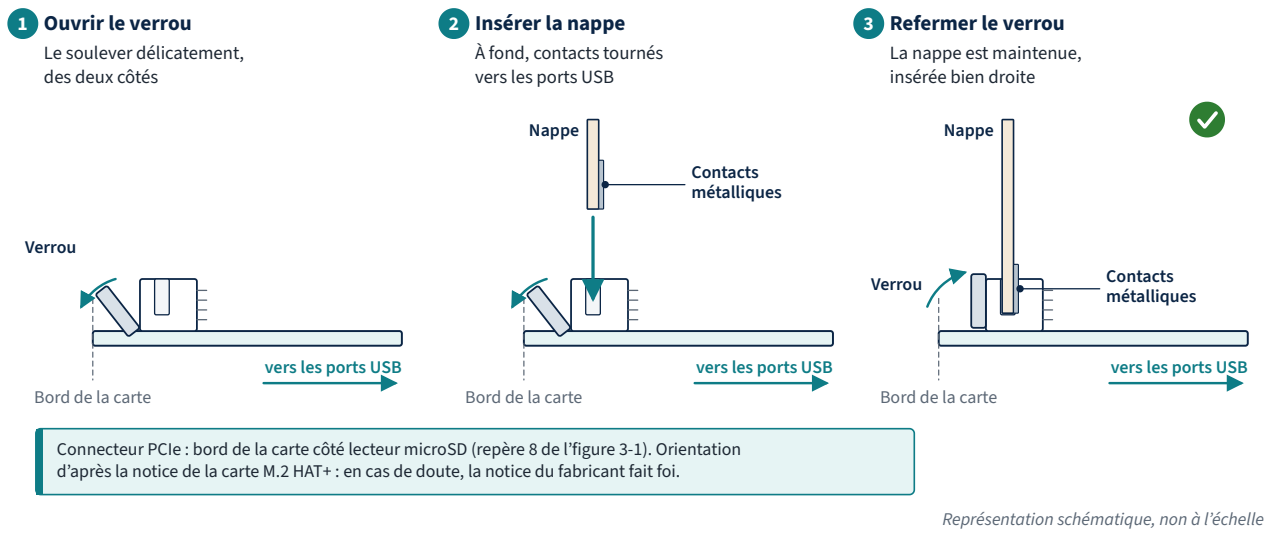


Figure 3-6 — Raccordement de la nappe PCIe au connecteur PCIe du Raspberry Pi 5 : verrou ouvert, orientation de la nappe, verrou refermé

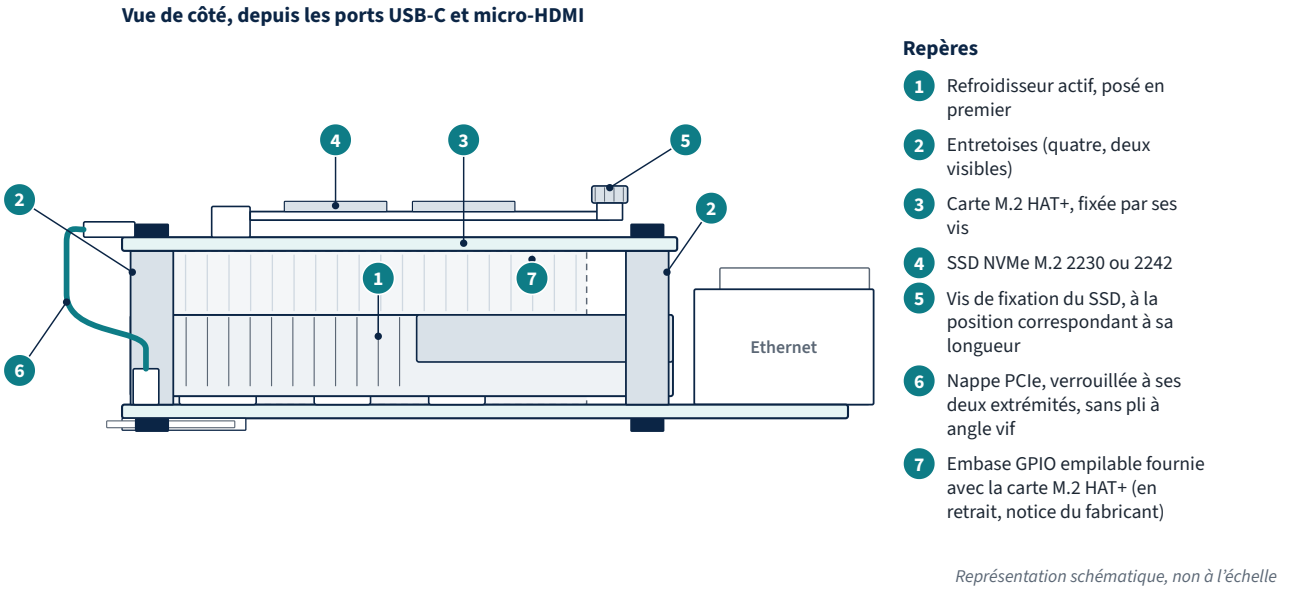


Figure 3-7 — Ensemble monté : refroidisseur actif, carte M.2 HAT+ sur ses entretoises, SSD fixé par sa vis

Résultat attendu : la carte M.2 HAT+ est fixée sans jeu ; la nappe est verrouillée à ses deux extrémités ; le SSD est inséré à fond et maintenu par sa vis.

Vérification : contrôle visuel à ce stade. La détection du SSD par la sonde se vérifie lors de son activation (§ 8.3.4).

Erreurs possibles : si le SSD n'est pas détecté lors de l'activation, les causes habituelles sont une nappe mal insérée ou inversée, un SSD absent de la liste des modèles pris en charge ou une alimentation non conforme. Arrêtez proprement la sonde, débranchez l'alimentation, puis vérifiez le montage.

Précautions :

- La nappe PCIe est fragile : ne la pliez pas à angle vif et ne tirez pas dessus pour la retirer ; ouvrez toujours le verrou du connecteur.
- Ne modifiez aucun fichier système de la microSD, en particulier la configuration de démarrage du Raspberry Pi (`config.txt`), ni pour activer le mode PCIe Gen 3, ni pour changer l'ordre de démarrage : seule la partition `SVA-BOOT` reçoit vos fichiers, et uniquement ceux que décrit cette documentation ; la sonde n'utilise pas le mode Gen 3 et démarre toujours sur la microSD.
- N'installez aucun système sur le SSD et n'y copiez pas l'image de la sonde : le système, la configuration et les secrets restent sur la microSD.
- L'activation du SSD le **formate entièrement** : n'utilisez pas un SSD contenant des données à conserver.

> **Information** — Dans l'offre boîtier complet, la présence d'un SSD dépend de votre commande : reportez-vous à la liste de colisage.

3.5 Mise en place du boîtier complet

3.5.1 Déballage

Objectif : sortir le matériel sans l'endommager et vérifier son état.

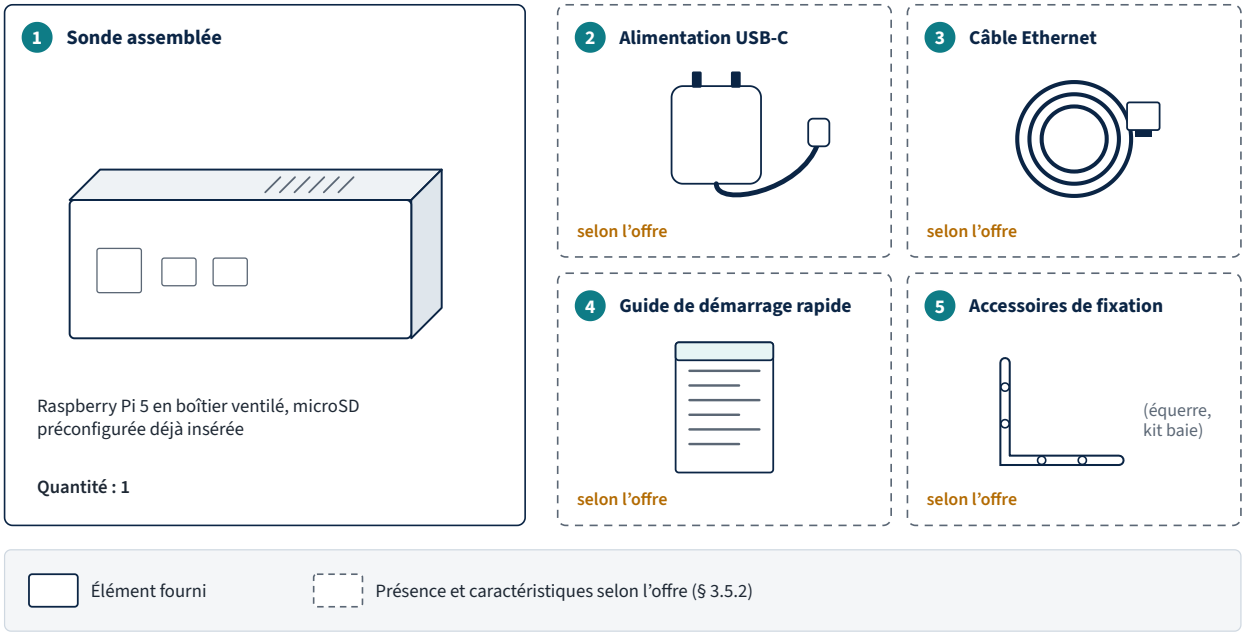
Étapes :

1. Inspectez l'emballage extérieur. En cas de choc visible ou d'emballage endommagé, photographiez-le avant ouverture et signalez-le au transporteur.
2. Ouvrez le colis et sortez les éléments un par un.
3. Conservez l'emballage d'origine : il est recommandé pour tout retour de matériel.
4. Contrôlez visuellement le boîtier : absence de fissure, de pièce mobile à l'intérieur (bruit en inclinant légèrement le boîtier), de connecteur endommagé.

3.5.2 Contenu du colis

Offre boîtier complet.

Élément	Quantité	Vérifié
Sonde assemblée (Raspberry Pi 5 en boîtier ventilé, microSD préconfigurée insérée)	1	[ ]
Alimentation USB-C	Selon la liste de colisage de votre commande ; à défaut, voir § 2.2	[ ]
Câble Ethernet	Selon la liste de colisage de votre commande ; à défaut, à fournir par vous (§ 2.5.1)	[ ]
Guide de démarrage rapide	Selon la liste de colisage de votre commande	[ ]
Accessoires de fixation (équerre, kit baie)	Selon la liste de colisage de votre commande	[ ]



Représentation schématique, non à l'échelle

Figure 3-8 — Contenu du colis de l'offre boîtier complet

Offre microSD préconfigurée (§ 3.4). Le colis contient les éléments suivants ; tout autre élément est fourni par vos soins (§ 3.4.1).

Élément	Quantité	Vérifié
Carte microSD contenant le système et le logiciel de la sonde, portant son numéro de série (§ 3.3.3)	1	[ ]
Encart d'identification : édition acquise, numéro de série du produit et code d'installation (§ 3.3.3)	1	[ ]

En cas d'élément manquant ou endommagé, contactez le support avant toute installation (coordonnées au chapitre 10).

> **Information** — Dans l'offre boîtier complet, la microSD est déjà insérée. Il n'est pas nécessaire d'ouvrir le boîtier. Si vous souhaitez utiliser un fichier de provisionnement (§ 4.3), retirez la microSD selon les indications jointes au boîtier livré ou, à défaut, communiquées par le support ; ne forcez jamais sur le lecteur.

3.5.3 Étiquette d'identification

Le boîtier porte une étiquette d'identification. Relevez ses informations **avant** l'installation, car l'étiquette peut devenir difficile d'accès une fois la sonde placée en baie.

Information	Usage
Numéro de série	Identification auprès du support
Adresse MAC de l'interface Ethernet	Réservation DHCP, recherche de la sonde sur le réseau (§ 4.4.2)
Nom d'hôte par défaut	De la forme `sva-XXXXXX`, où `XXXXXX` correspond aux six derniers caractères hexadécimaux de l'adresse MAC
Code d'installation	Accès à l'assistant de mise en service (§ 4.4.3)
Édition et capacité mémoire	Vérification de la conformité de la commande

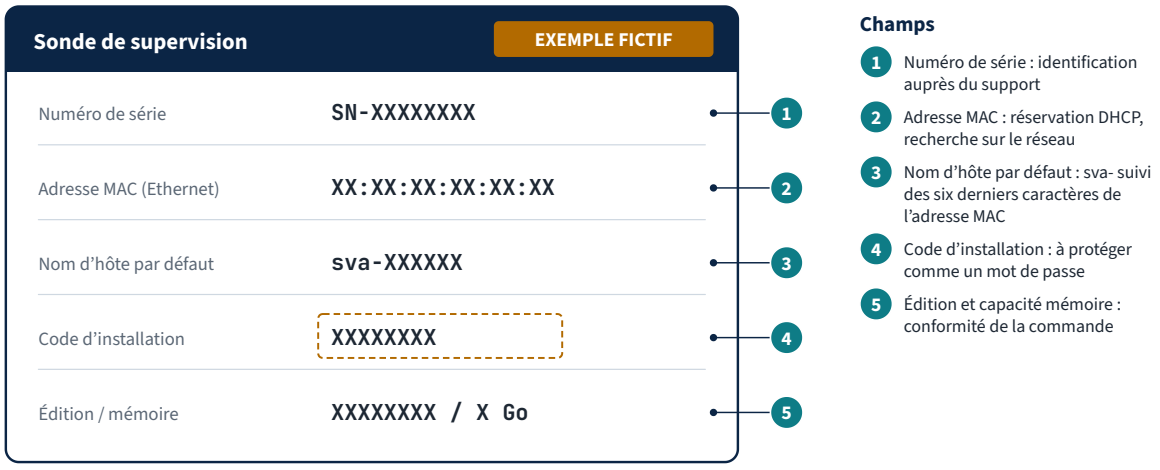


Figure 3-9 — Exemple d'étiquette d'identification du boîtier complet, avec repérage de chaque champ

> **Avertissement** — Le code d'installation permet de prendre le contrôle d'une sonde non encore configurée. Ne le diffusez pas et ne le photographiez pas sur un support partagé. Il ne permet plus d'ouvrir l'assistant après la mise en service, mais il reste exigé pour récupérer le compte administrateur (§ 8.10.2) et redevient valide après une réinitialisation usine : conservez l'encart ou l'étiquette pendant toute la vie du produit.

> **Conseil** — Recopiez l'adresse MAC et le numéro de série dans la fiche de mise en service (chapitre 10) et transmettez l'adresse MAC à l'équipe réseau si une réservation DHCP est souhaitée (§ 5.2).

3.6 Choix de l'emplacement

Objectif : installer la sonde dans un lieu qui garantit sa fiabilité, sa sécurité et la pertinence de ses mesures.

3.6.1 Critères techniques

Critère	Recommandation
Position réseau	La sonde mesure ce qu'elle « voit » depuis son emplacement. Placez-la sur le segment réseau dont vous voulez évaluer l'expérience : réseau des utilisateurs pour mesurer l'accès à une application, réseau du centre de données pour superviser des services internes. Voir § 5.10
Sécurité physique	Local fermé, baie verrouillée ou local technique. La microSD contient la configuration et les secrets chiffrés de la sonde : un accès physique non contrôlé constitue un risque (§ 5.11)
Ventilation	Espace libre d'au moins quelques centimètres autour des ouïes d'aération ; pas d'empilement contre un équipement chaud
Alimentation	Prise secourue (onduleur) recommandée : une coupure électrique brutale est l'une des principales causes d'usure et de corruption des cartes microSD
Câblage	Prise réseau ou port de commutateur disponible à proximité ; longueur de câble Ethernet inférieure à 100 m
Accès	Accès possible pour la maintenance (retrait de la microSD, observation du voyant)

3.6.2 Installation en baie

La sonde n'est pas un équipement au format rack 19 pouces. Pour une installation en baie, posez-la sur une **tablette** fixe ou utilisez un **support** adapté, notamment l'accessoire de montage éventuellement prévu par votre commande. Ne la posez pas directement sur le capot d'un serveur, dont la chaleur dégraderait son refroidissement.

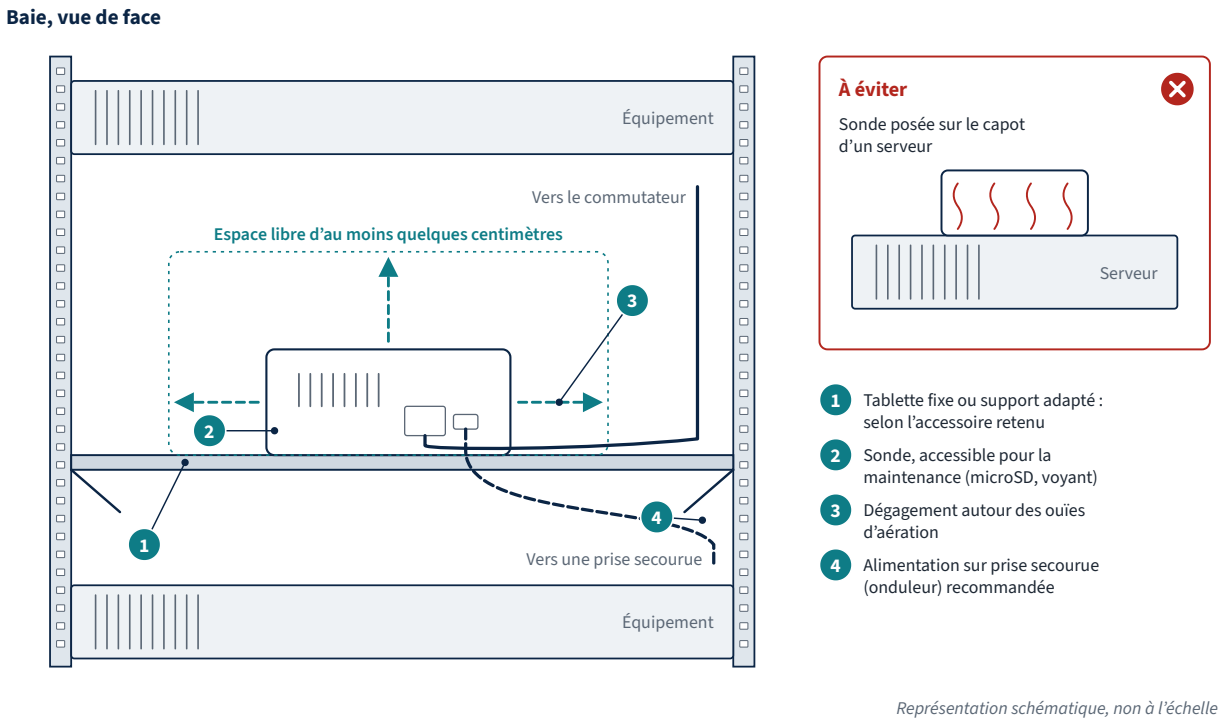


Figure 3-10 — Exemple d'installation sur tablette en baie, avec dégagement pour la ventilation

3.7 Connexion Ethernet

Objectif : raccorder la sonde au réseau choisi pour son implantation (§ 2.5.2).

Prérequis :

- port de commutateur ou prise murale active, sur le réseau prévu (VLAN de supervision, par exemple, voir § 5.10) ;
- si le port est protégé par le contrôle d'accès 802.1X, la sonde s'authentifie par certificat (EAP-TLS). Deux possibilités, à arrêter avec l'équipe réseau (§ 2.5.1 et § 5.2.6) : le fichier PKCS#12 de la sonde et le certificat de l'AC du serveur RADIUS ont été déposés sur la microSD avec le fichier de provisionnement (§ 3.4.2), ou le port est provisoirement non contrôlé ou autorisé par adresse MAC (MAB) pour la mise en service, 802.1X étant activé ensuite ;
- si la sonde doit obtenir une adresse par DHCP, un serveur DHCP doit être actif sur ce réseau ; sinon, une configuration statique doit être fournie par le fichier de provisionnement (§ 4.3).

Étapes :

1. Branchez une extrémité du câble Ethernet sur le port RJ45 de la sonde, jusqu'au clic du loquet.
2. Branchez l'autre extrémité sur le port du commutateur ou la prise murale.
3. Ne branchez pas encore l'alimentation.

Résultat attendu : le câble est verrouillé aux deux extrémités.

Vérification : les voyants du port Ethernet de la sonde et du commutateur s'allumeront après la mise sous tension (§ 3.9.2).

> **Information** — La sonde fonctionne exclusivement en Ethernet. Le Wi-Fi et le Bluetooth intégrés au Raspberry Pi 5 sont désactivés dans le système de la sonde, par une surcouche de l'arbre des périphériques (*device tree overlay*).

→ **Évolution prévue** — La prise en charge du Wi-Fi est envisagée dans une version ultérieure.

3.8 Branchement de l'alimentation et démarrage

Objectif : mettre la sonde sous tension dans de bonnes conditions.

Prérequis : microSD insérée ; boîtier fermé ; câble Ethernet branché ; méthode de mise en service choisie (chapitre 4).

Étapes :

1. Branchez l'alimentation sur la prise secteur (de préférence secourue).
2. Branchez le connecteur USB-C sur le port d'alimentation de la sonde. **L'alimentation doit être branchée en dernier.**
3. La sonde démarre automatiquement dès qu'elle est alimentée. Il n'est normalement pas nécessaire d'appuyer sur le bouton d'alimentation.
4. Ne débranchez pas la sonde pendant le premier démarrage, qui comporte des opérations d'initialisation (extension du système de fichiers, génération des clés de sécurité). Sa durée est indiquée au § 4.2.

Résultat attendu : le voyant d'état s'allume, puis traduit l'activité du système (§ 3.9.1).

! **Attention** — Ne coupez jamais l'alimentation d'une sonde en fonctionnement en débranchant le câble, sauf en dernier recours. Utilisez la procédure d'arrêt propre décrite au chapitre 8. Une coupure brutale peut provoquer une perte des dernières données et, de manière répétée, une corruption de la microSD.

i **Information** — Si l'alimentation utilisée ne fournit pas le courant attendu par le Raspberry Pi 5 (alimentation 5 V / 3 A, par exemple), la carte peut fonctionner avec un courant USB limité. La sonde surveille les situations de sous-tension et les signale dans ses indicateurs de santé (chapitre 7 du guide d'utilisation et de supervision et chapitre 9).

3.9 Vérifications initiales

3.9.1 Voyant d'état

Le Raspberry Pi 5 dispose d'un voyant d'état unique, bicolore. D'après la documentation du fabricant, sa couleur indique l'état d'alimentation de la carte :

Observation	Signification (comportement général du Raspberry Pi 5)	Action
Aucun voyant allumé	Cause probable : la carte n'est pas alimentée (à recouper avec l'écran HDMI éventuel et les voyants Ethernet, encadré ci-dessous)	Vérifier l'alimentation, le câble et la prise (§ 3.10)
Rouge fixe	La carte est alimentée mais le système est arrêté ou en veille	Appuyer brièvement sur le bouton d'alimentation pour démarrer ; si la situation persiste, voir § 3.10
Vert, clignotant de façon irrégulière	Le système fonctionne ; le clignotement traduit l'activité de lecture et d'écriture	Situation normale

Observation	Signification (comportement général du Raspberry Pi 5)	Action
Clignotements répétitifs selon un motif régulier (séquences de flashs longs et courts)	Code d'erreur du chargeur d'amorçage, documenté par Raspberry Pi (par exemple, microSD illisible ou système introuvable)	Noter le motif, consulter la documentation Raspberry Pi et le chapitre 9

La sonde ne définit aucune signalisation propre : le voyant ne présente que les comportements standard du Raspberry Pi 5 décrits ci-dessus. En particulier, il n'indique ni la fin de l'initialisation ni l'état de configuration de la sonde ; ces informations se vérifient sur l'écran HDMI éventuel ou par le réseau (chapitre 4).

> **Information** — Les couleurs et clignotements du voyant sont des **indices matériels** : leur comportement exact dépend du microprogramme (*firmware*) du Raspberry Pi 5, de sa configuration et de l'étape du démarrage. Un voyant vert actif signale une activité de lecture et d'écriture sur le support de stockage ; il ne confirme ni que le logiciel de la sonde fonctionne, ni qu'il est correctement configuré. Pour établir l'état de la sonde, recoupez toujours le voyant avec la console de l'écran HDMI éventuellement raccordé (adresse IP, empreinte du certificat, état de la mise en service) et, dès que la sonde est joignable, avec l'adresse `/health` (§ 4.6.2).

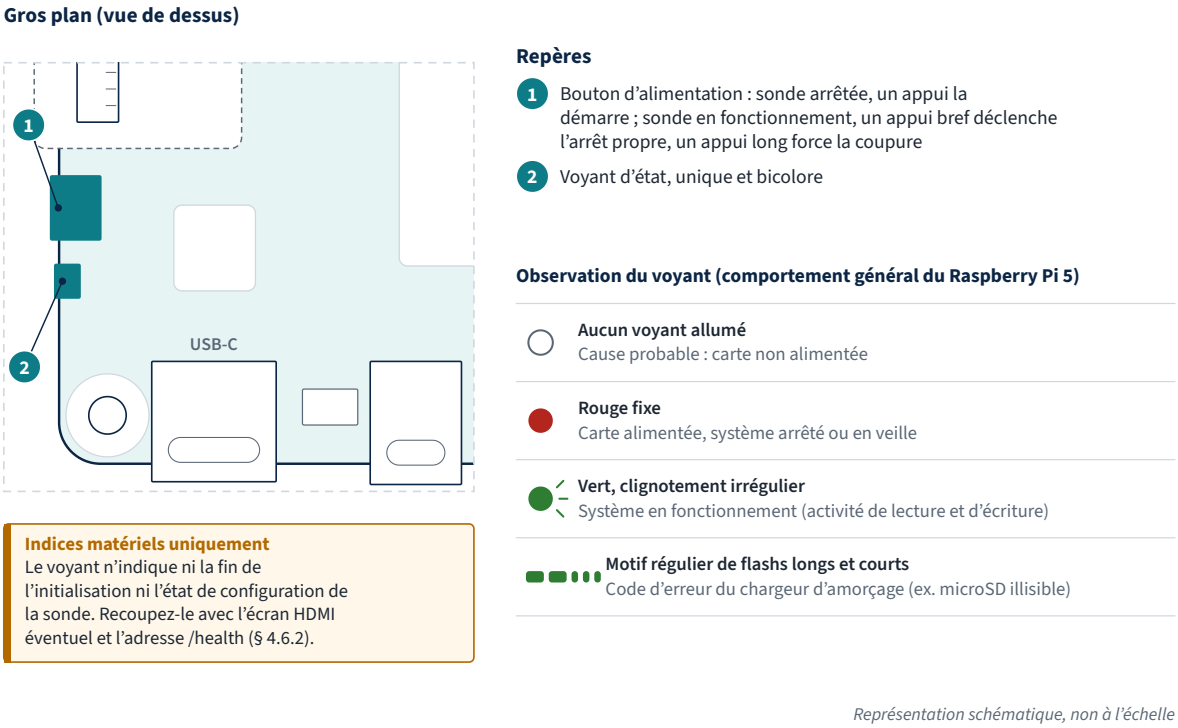


Figure 3-11 — Emplacement du voyant d'état et du bouton d'alimentation du Raspberry Pi 5

3.9.2 Voyants du port Ethernet

Le port Ethernet comporte deux voyants intégrés :

Observation	Signification
Voyant de liaison allumé	Une liaison physique est établie avec le commutateur
Voyant d'activité clignotant	Des trames circulent sur le lien
Aucun voyant	Pas de liaison : câble, port de commutateur ou prise murale à vérifier

Vérifiez également, côté commutateur, que le port est actif et affecté au bon VLAN. L'équipe réseau peut confirmer qu'une adresse MAC correspondant à la sonde est apprise sur le port.

3.9.3 Ventilateur

Le ventilateur peut tourner brièvement à pleine vitesse au démarrage, puis ralentir ou s'arrêter selon la température. Un ventilateur qui ne tourne jamais, alors que la sonde est très chaude au toucher, doit être vérifié (branchement sur le connecteur « FAN »).

3.9.4 Liste de vérification de fin d'installation physique

Point de contrôle	Vérifié
Matériel conforme à l'édition (RAM, refroidissement)	[ ]
Refroidissement installé et raccordé	[ ]
microSD insérée à fond, sonde hors tension lors de l'insertion	[ ]
Emplacement ventilé, sécurisé, alimentation secourue si possible	[ ]
Câble Ethernet verrouillé, voyants de liaison allumés	[ ]
Alimentation branchée en dernier	[ ]
Voyant d'état vert avec activité	[ ]
Adresse MAC et numéro de série relevés	[ ]
Si SSD prévu : carte M.2 HAT+ et SSD montés, nappe verrouillée, alimentation de 27 W utilisée (§ 3.4.6)	[ ]

L'installation physique est terminée. Poursuivez avec la mise en service au chapitre 4.

3.10 Erreurs fréquentes lors de l'installation

Symptôme	Causes possibles	Vérifications et actions
Aucun voyant	Alimentation non branchée ou défectueuse ; prise sans courant	Tester la prise avec un autre appareil ; essayer une autre alimentation conforme
Voyant rouge fixe, pas de démarrage	Système arrêté ; alimentation insuffisante	Appui bref sur le bouton d'alimentation ; utiliser l'alimentation recommandée (§ 3.4.1)
Motif de clignotement répétitif	microSD absente, mal insérée, endommagée ou ne contenant pas l'image de la sonde	Mettre hors tension, réinsérer la microSD à fond ; vérifier qu'il s'agit bien de la carte fournie ; voir chapitre 9
Voyant vert actif mais pas de voyant Ethernet	Câble non verrouillé ou défectueux ; port de commutateur inactif	Changer de câble ; tester un autre port ; vérifier la configuration du port avec l'équipe réseau
Ventilateur bruyant en permanence	Température élevée ; emplacement mal ventilé	Améliorer la ventilation ; vérifier l'absence de source de chaleur proche

Symptôme	Causes possibles	Vérifications et actions
La sonde redémarre de façon répétée	Alimentation insuffisante ; microSD défectueuse	Utiliser l'alimentation recommandée ; contacter le support si le problème persiste
Voyant de liaison Ethernet allumé, mais la sonde n'obtient pas d'adresse, sur un port protégé par 802.1X	Authentification 802.1X refusée, ou sonde sans identifiant client	Consulter l'état affiché sur l'écran HDMI éventuel et le journal du serveur RADIUS ; voir § 5.2.6 et chapitre 9
Aucun démarrage, avec ou sans message sur l'écran HDMI, sur une carte autre qu'un Raspberry Pi 5	Modèle de carte non pris en charge (Raspberry Pi 4, Raspberry Pi 400, Compute Module, Orange Pi…)	Le système vérifie le modèle au tout début du démarrage, avant tout montage en écriture et avant l'extension de la partition ; s'il a pu démarrer, il s'arrête sans monter de partition en écriture et affiche un message sur l'écran HDMI. Si le microprogramme de la carte ne charge pas l'image, aucun composant de la sonde ne s'exécute et aucun message ne peut s'afficher. Dans les deux cas, le contrôle vise à préserver la microSD, sans que sa conservation puisse être garantie lorsque le microprogramme d'une autre carte a manipulé le support (§ 2.1.1). Mettez hors tension et installez la carte dans un Raspberry Pi 5 (§ 2.1.1).
La microSD a été « formatée » par un ordinateur	Acceptation d'une proposition de formatage du système d'exploitation du poste	Le formatage a effacé le système et le certificat d'édition, qui ne peut pas être réinscrit par vos soins : la carte doit être remplacée. Contactez le support avec le numéro de série du produit (§ 8.6.4)

Le diagnostic détaillé de ces situations est traité au chapitre 9.

Chapitre 4 — Premier démarrage et mise en service

Ce chapitre décrit les opérations qui transforment une sonde neuve, tout juste raccordée, en sonde opérationnelle : initialisation du système, configuration initiale, vérification de l'édition, vérifications et exécution d'un premier contrôle.

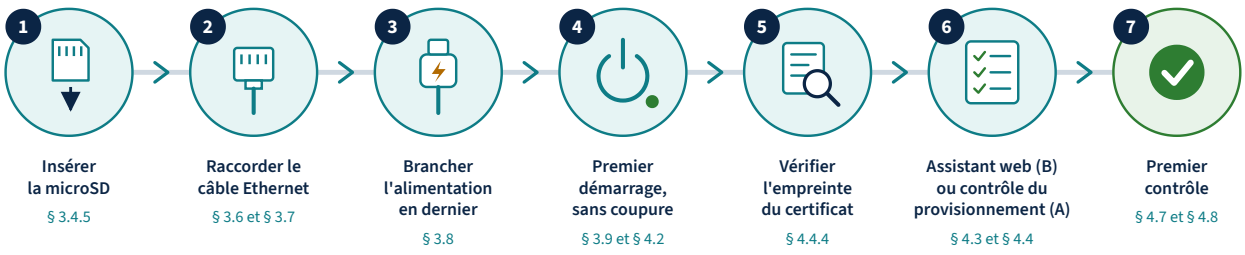
À l'issue de ce chapitre, la sonde :

- dispose d'une adresse IP connue et d'un nom d'hôte ;
- est protégée par un compte administrateur qui vous est propre ;
- a produit un code de récupération de ce compte, que vous avez enregistré dans le coffre-fort de votre organisation ;
- présente un certificat dont vous avez vérifié l'empreinte ;
- a son édition vérifiée ;
- a exécuté un premier contrôle dont le résultat est consultable.

> **Information** — Les exemples de ce chapitre utilisent des adresses et des noms fictifs, réservés à la documentation : réseau `192.0.2.0/24`, domaine `example.internal`, sonde `sonde-paris-01`. Remplacez-les par les valeurs de votre environnement.

4.1 Les deux méthodes de mise en service

La sonde ne contient **aucun mot de passe par défaut**. Tant qu'elle n'est pas configurée, elle n'accepte qu'une seule forme d'accès protégée. Deux méthodes sont proposées.



Offre boîtier complet : déballer et contrôler le contenu (§ 3.5) remplace l'étape 1.
Méthode A : le fichier provision.yaml est déposé sur la microSD avant l'étape 1 et appliqué au premier démarrage (§ 4.3).
Étape 5 : comparer l'empreinte affichée par le navigateur à celle de l'écran HDMI ou du fichier setup-code.txt, avant toute saisie (§ 4.4.4).

Figure 4-1 — Les étapes de la mise en service, de l'insertion de la microSD au premier contrôle

	Méthode A — Fichier de provisionnement	Méthode B — Assistant web
Principe	Un fichier `provision.yaml`, préparé sur un poste de travail, est déposé sur la microSD avant le premier démarrage. La sonde l'applique automatiquement	Après le démarrage, un assistant web, protégé par un code d'installation, guide la configuration

	Méthode A — Fichier de provisionnement	Méthode B — Assistant web
Adaptée à	Déploiements en série ; réseaux sans DHCP (adresse statique dès le premier démarrage) ; ports soumis à l'authentification 802.1X ; automatisation	Installation unitaire ; utilisateurs préférant une interface guidée
Nécessite	Un poste capable de lire une microSD ; l'empreinte d'un mot de passe (§ 4.3.4)	Un serveur DHCP sur le réseau de la sonde ; l'accès au code d'installation ; un écran micro-HDMI ou un lecteur de microSD pour vérifier l'empreinte du certificat (§ 4.4.4)
Intervention après démarrage	Vérification, puis relevé du code de récupération à la première connexion (§ 4.4.6)	Parcours de l'assistant (durée indicative : une dizaine de minutes, selon les options choisies)

✓ **Conseil** — Sur un réseau sans serveur DHCP, utilisez la méthode A : sans adresse IP, la sonde ne pourrait pas être jointe par l'assistant web. Il en va de même sur un port de commutateur soumis à l'authentification 802.1X : seule la méthode A permet de fournir à la sonde son identifiant 802.1X avant tout accès au réseau (§ 4.3.3). À défaut, effectuez la mise en service sur un port non contrôlé ou autorisé par adresse MAC, puis activez 802.1X (chapitre 5).

Les deux méthodes aboutissent au même résultat. Un fichier de provisionnement valide suffit à configurer la sonde : les sections qu'il ne contient pas prennent leurs valeurs par défaut (§ 4.3.3). Si le fichier est refusé, la sonde reste non initialisée et la mise en service peut se poursuivre avec l'assistant.

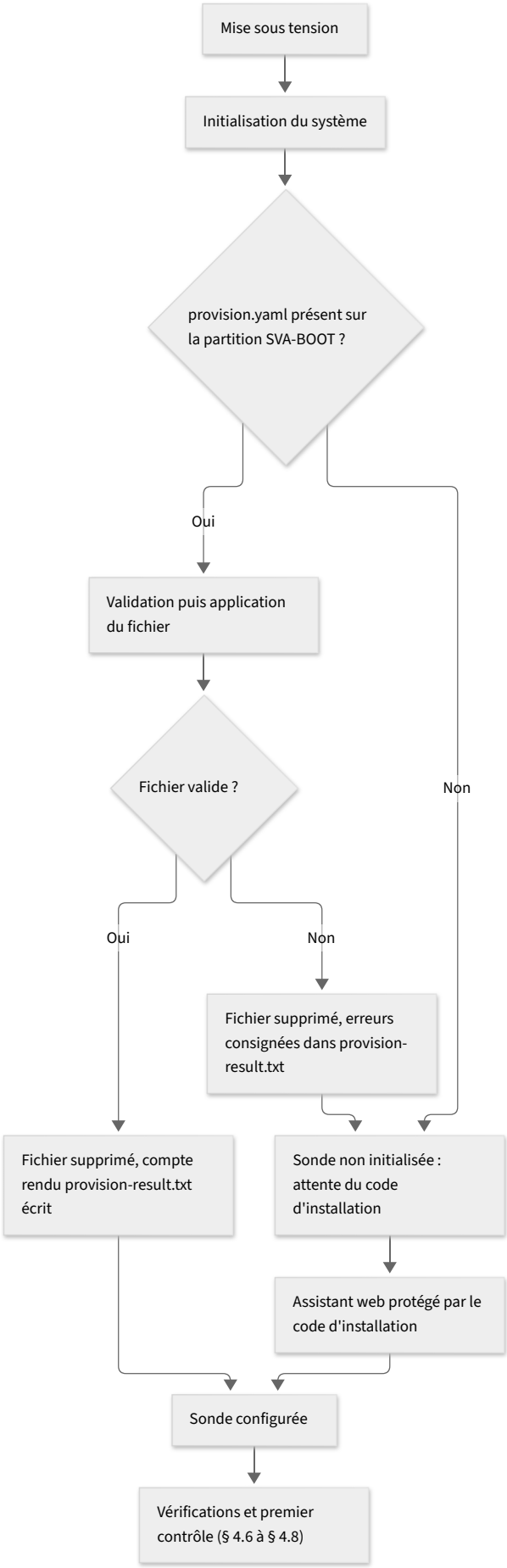


Schéma 4-1 — Premier démarrage et choix de la méthode de mise en service

> **Attention** — La validation du fichier est **atomique** : soit le fichier est entièrement valide et tous ses paramètres sont appliqués, soit aucun ne l'est. Dans les deux cas, le fichier est supprimé, car il contient des données sensibles, et le motif d'un refus est consigné, sans aucun secret, dans `provision-result.txt`. Consultez ce compte rendu après chaque provisionnement.

4.2 Déroulement de l'initialisation

Au premier démarrage, la sonde exécute des opérations qui ne se reproduiront pas lors des démarrages suivants :

Ordre	Opération	Effet visible
1	Démarrage du système Raspberry Pi OS	Voyant vert, activité intense
2	Extension de la partition de données à la capacité restante de la microSD (les emplacements système A/B, en lecture seule, ne sont pas modifiés)	Activité disque soutenue
3	Génération des identifiants propres à l'appareil : identifiant unique de sonde, clés SSH (même si SSH reste désactivé), clé privée et certificat TLS autosigné, clé de chiffrement des secrets	Aucun
4	Lecture du fichier de provisionnement s'il est présent	Écriture de `provision-result.txt`
5	Si le fichier de provisionnement contient une section `dot1x` : authentification 802.1X (EAP-TLS) sur la prise Ethernet, **avant** la configuration réseau. Puis configuration réseau : DHCP par défaut, ou paramètres du provisionnement ; IPv6 seulement s'il est activé	Voyants Ethernet actifs ; requête DHCP visible côté serveur. En cas d'échec de l'authentification 802.1X : nouvelles tentatives, état affiché sur la console HDMI
6	Démarrage du moteur principal et du moteur de scénarios	Interface d'administration accessible
7	Si la sonde n'est pas configurée : attente de la mise en service	Code d'installation (inscrit sur la carte lors de sa préparation) et empreinte du certificat affichés sur l'écran HDMI éventuel, avec l'adresse IP et le nom mDNS ; code et empreinte écrits dans `setup-code.txt`. Contrairement aux autres opérations du tableau, l'écriture de ce fichier se répète à chaque démarrage ; le code en disparaît une fois la sonde initialisée (encadré ci-dessous)

> **Information** — Le fichier `setup-code.txt` de la partition `SVA-BOOT` n'est pas propre à l'attente de mise en service : la sonde le **réécrit à chaque démarrage**, qu'elle soit configurée ou non, avec l'empreinte SHA-256 du certificat qu'elle présente à ce moment. Le code d'installation n'y figure que tant que la sonde n'est pas initialisée ; une fois la mise en service terminée, le fichier ne contient plus que l'empreinte. De même, la console de l'écran HDMI affiche l'empreinte courante à chaque démarrage. Ces deux canaux, indépendants du réseau, sont donc disponibles quel que soit le parcours de mise en service, y compris le provisionnement sans écran (§ 4.3).

Le premier démarrage est plus long que les suivants, en raison de l'extension du système de fichiers et de la génération des clés. À titre indicatif, comptez quelques minutes. Les démarrages suivants sont plus rapides.

> **Attention** — Ne coupez pas l'alimentation pendant le premier démarrage. Une interruption pendant l'extension du système de fichiers ou la génération des clés peut rendre la carte inutilisable ; elle se remplace alors selon le § 8.6.4.

> **Information** — Les clés et le certificat sont générés **sur la sonde**, au premier démarrage. Deux sondes issues de la même image ne partagent donc aucun secret. C'est aussi la raison pour laquelle il ne faut pas dupliquer une microSD déjà mise en service pour en équiper une autre sonde (voir chapitre 8).

4.3 Mise en service par fichier de provisionnement (méthode A)

4.3.1 Principe

La microSD comporte une petite **partition de dépôt** au format FAT32, étiquetée `SVA-BOOT`, lisible depuis Windows, macOS et Linux ; dans cette documentation, l'expression « partition de démarrage » désigne cette partition. Avec le mécanisme de mise à jour A/B, d'autres partitions peuvent apparaître sur votre poste : ne les modifiez pas. Si un fichier nommé `provision.yaml` est présent à la racine de cette partition au démarrage d'une sonde non encore initialisée, la sonde :

1. le lit et valide son contenu ;
2. applique l'ensemble de ses paramètres si le fichier est entièrement valide, et aucun dans le cas contraire (validation atomique) ;
3. **supprime** le fichier dans tous les cas, afin qu'aucune information sensible ne reste lisible sur la carte ;
4. écrit, au même emplacement, un compte rendu `provision-result.txt` qui ne contient aucun secret.

Le format YAML (*YAML Ain't Markup Language*) est un format texte structuré par l'indentation. Il est lisible et modifiable avec tout éditeur de texte.

4.3.2 Prérequis

- Un poste de travail équipé d'un lecteur de cartes microSD (ou d'un adaptateur USB).
- Un éditeur de texte brut (Bloc-notes, TextEdit en mode texte brut, Visual Studio Code, vi…). **N'utilisez pas** un traitement de texte, qui ajouterait une mise en forme.
- Les paramètres réseau de la sonde si l'adresse doit être statique : adresse et masque, passerelle, serveurs DNS, serveurs NTP.
- L'empreinte du mot de passe administrateur (§ 4.3.4).
- Si l'IPv6 doit être activé en adressage statique : adresse IPv6 et longueur de préfixe, passerelle IPv6.
- Si le port de commutateur est soumis à l'authentification 802.1X : l'identité à présenter, l'identifiant client de la sonde sous forme de fichier PKCS#12 et son mot de passe, ainsi que le certificat, au format PEM, de l'autorité de certification (AC) du serveur RADIUS. Ces éléments sont fournis par l'équipe en charge du contrôle d'accès réseau.

4.3.3 Référence des champs

Le tableau suivant décrit les champs reconnus par la version 1 du format.

Champ	Obligatoire	Description	Exemple
`version`	Oui	Version du format du fichier ; vaut `1`	`1`

Champ	Obligatoire	Description	Exemple
`hostname`	Non	Nom d'hôte de la sonde : lettres minuscules, chiffres et tirets, 63 caractères maximum. Par défaut : `sva-XXXXXX`	`sonde-paris-01`
`site`	Non, recommandé	Emplacement logique de la sonde ; repris comme attribut de toutes les données exportées (chapitre 2 du guide d'intégration et d'observabilité)	`paris-dc1`
`admin.username`	Oui	Identifiant du premier compte administrateur	`admin`
`admin.passwordHash`	Oui	**Empreinte** du mot de passe, jamais le mot de passe en clair (§ 4.3.4)	—
`network.mode`	Non	`dhcp` (par défaut) ou `static`	`static`
`network.address`	Si `static`	Adresse IPv4 et longueur de préfixe	`192.0.2.50/24`
`network.gateway`	Si `static`	Passerelle par défaut	`192.0.2.1`
`network.dns`	Si `static`	Liste de serveurs DNS (deux recommandés), en IPv4 ou en IPv6	`[192.0.2.10, 192.0.2.11]`
`network.ntp`	Non, recommandé	Liste de serveurs NTP. Par défaut : serveurs fournis par DHCP (option 42), sinon une zone fournisseur du *NTP Pool*, indiquée dans les notes de version	`[ntp1.example.internal]`
`network.ipv6.enabled`	Non	Active l'IPv6, en complément de l'IPv4 qui reste toujours actif. Par défaut : `false`	`true`
`network.ipv6.mode`	Si l'IPv6 est activé	`slaac` (configuration automatique par les annonces du routeur) ou `static`. Valeur par défaut : `slaac`	`static`
`network.ipv6.address`	Si `ipv6.mode` vaut `static`	Adresse IPv6 et longueur de préfixe (notation CIDR)	`2001:db8:10::50/64`
`network.ipv6.gateway`	Si `ipv6.mode` vaut `static`	Passerelle IPv6 par défaut	`2001:db8:10::1`
`proxy.url`	Non	Proxy HTTP(S) sortant	`http://proxy.example.internal:3128`

Champ	Obligatoire	Description	Exemple
`proxy.noProxy`	Non	Destinations joignables sans proxy : suffixes de domaine, adresses, plages	`[".example.internal", "192.0.2.0/24"]`
`dot1x.identity`	Si la section `dot1x` est présente	Identité présentée au serveur RADIUS lors de l'authentification 802.1X (EAP-TLS) sur la prise Ethernet. La présence de la section `dot1x` déclenche l'authentification avant tout accès au réseau	`sonde-paris-01.example.internal`
`dot1x.pkcs12File`	Si la section `dot1x` est présente	Nom du fichier PKCS#12 (clé privée et certificat client de la sonde), déposé à la racine de la partition `SVA-BOOT`. Supprimé après traitement	`sonde-paris-01.p12`
`dot1x.caFile`	Si la section `dot1x` est présente	Nom du fichier contenant le certificat de l'AC du serveur RADIUS, au format PEM, déposé à la racine de la partition `SVA-BOOT`. Supprimé après traitement	`radius-ca.pem`
`dot1x.pkcs12Password`	Si la section `dot1x` est présente	Mot de passe du fichier PKCS#12. **Seul secret admis dans ce fichier**, supprimé avec lui après traitement	—
`ssh.locked`	Non	`true` verrouille **définitivement** l'accès SSH : il ne pourra plus être activé, jusqu'à une réinitialisation usine (§ 5.9.4). Par défaut : `false`	`true`
`updates.security.mode`	Non, recommandé	Mode du canal des correctifs de sécurité : `automatic` (par défaut) ou `manual`. En mode `automatic`, les correctifs sont téléchargés et installés sur l'emplacement inactif dès leur disponibilité, puis activés dans une fenêtre de maintenance	`automatic`

Champ	Obligatoire	Description	Exemple
`updates.security.criticalPolicy`	Non	Activation d'un correctif de sécurité critique (vulnérabilité activement exploitée) : `next-window` (par défaut : au début de la première fenêtre qui commence au moins 15 minutes après l'annonce) ou `asap` (choix explicite : 15 minutes après l'annonce, augmentées de `criticalStagger`, même hors fenêtre)	`next-window`
`updates.security.criticalStagger`	Non	Décalage fixe, propre à la sonde, ajouté au préavis de 15 minutes d'un correctif critique en mode `asap`, de `0` à `4h`, pour échelonner les sondes d'un même site (§ 8.4.11)	`0`
`updates.feature.mode`	Non	Mode du canal des versions fonctionnelles : `manual` (par défaut) ou `automatic`	`manual`
`updates.windows`	Non, recommandé	Liste de 0 à 7 fenêtres de maintenance, chacune avec `days` (jours parmi `mon`, `tue`, `wed`, `thu`, `fri`, `sat`, `sun`), `start` (heure de début au format `HH:MM`, **entre guillemets**) et `duration`. **Aucune fenêtre par défaut**	`[{days: [tue], start: "22:00", duration: 2h}]`
`updates.notice`	Non	Préavis minimal annoncé avant toute activation automatique, de `0` à `7d` (activation manuelle et correctif critique : § 8.4.2). Par défaut : `24h`	`24h`
`updates.drainTimeout`	Non	Délai accordé aux exécutions en cours pour se terminer au début d'une activation, `30m` au maximum. Par défaut : `5m`	`5m`

Les champs ci-dessus constituent le format version 1, y compris les sections `dot1x`, `network.ipv6`, `ssh.locked` et `updates`.

Section `updates`. Elle fixe la politique de mises à jour dès le premier démarrage (chapitre 8). Une mise à jour est téléchargée et installée sur l'emplacement système inactif sans interrompre les contrôles ; son **activation**, c'est-à-dire le redémarrage sur la nouvelle version, n'a lieu que dans l'une des fenêtres que vous définissez. Si le fichier ne contient pas de section `updates`, la sonde applique les valeurs par défaut du tableau, **sans aucune fenêtre** : aucune mise à jour n'est alors activée automatiquement, et l'état de santé `updates` reste en `WARNING` tant qu'aucune fenêtre n'est définie. Un administrateur active alors chaque mise à jour par l'interface ou par l'API (`POST /api/v1/updates/apply`, chapitre 8). Aucune plage horaire n'est imposée : choisissez des créneaux compatibles avec vos plans d'exécution (chapitre 6 du guide d'utilisation et de supervision).

Exemple de section `updates` (valeurs fictives, à ajouter au fichier de provisionnement) :

```yaml
# Politique de mises à jour — exemple fictif
updates:
  security:
    mode: automatic             # automatic (par défaut) | manual
    criticalPolicy: next-window # next-window (par défaut) | asap
    criticalStagger: "0"      # décalage des activations asap, de 0 à 4h
  feature:
    mode: manual                # manual (par défaut) | automatic
  windows:                      # aucune fenêtre par défaut ; 7 fenêtres au maximum
    - days: [tue, thu]
      start: "22:00"            # format HH:MM, toujours entre guillemets
      duration: 2h
  notice: 24h                   # préavis avant activation, de 0 à 7d
  drainTimeout: 5m              # 30m au maximum
```

Information — Le choix des fenêtres et du préavis relève de votre organisation : le règlement européen sur la cyberrésilience (CRA) n'impose ni horaire ni calendrier particulier. Une sonde unique ne supervise pas pendant son propre redémarrage ; pour les environnements critiques, le chapitre 8 décrit le déploiement de plusieurs sondes par site avec des fenêtres qui ne se chevauchent pas. Les autres réglages (destinations d'export, authentification du proxy, certificat fourni par votre organisation, domaine de recherche DNS, activation temporaire de SSH) se configurent après la mise en service, dans l'interface ou par l'API : plusieurs d'entre eux font appel à des secrets, qui n'ont pas leur place dans ce fichier. Seule exception, le mot de passe du fichier PKCS#12 (`dot1x.pkcs12Password`) : il est indispensable pour que la sonde s'authentifie auprès du commutateur avant de disposer d'un accès au réseau.

Avertissement — Ne placez **aucun secret applicatif** (mot de passe d'un compte de test, jeton d'une plateforme d'observabilité) dans le fichier de provisionnement. Même si le fichier est supprimé après lecture, il a pu être copié ou rester dans la corbeille du poste qui l'a préparé. Les secrets se saisissent dans l'interface d'administration ou par l'API (chapitre 6).

Avertissement — La section `dot1x` place sur la microSD le mot de passe du fichier PKCS#12, le fichier PKCS#12 lui-même, qui contient la clé privée de la sonde, et le certificat de l'AC. La sonde supprime ces fichiers et ce mot de passe après traitement, comme `provision.yaml`. Préparez-les sur un poste de confiance, supprimez-en toute copie (y compris dans la corbeille) une fois la carte préparée, et ne laissez pas la carte sans surveillance avant son insertion dans la sonde. Lorsque c'est possible, préférez une première mise en service sur un port non contrôlé ou autorisé par adresse MAC, suivie d'une génération de la clé et de la demande de certificat sur la sonde elle-même (chapitre 5) : la clé privée ne quitte alors jamais la sonde. La suppression des fichiers par la sonde ne vaut pas effacement physique de la mémoire flash : les précautions qui en découlent (certificat dédié et de courte durée, carte traitée comme un support sensible, révocation en cas de perte) sont détaillées au § 4.3.5.

> **Information** — L'authentification 802.1X dès le premier démarrage repose sur la section `dot1x` du fichier de provisionnement : elle a lieu avant la configuration réseau et, en cas d'échec, la sonde renouvelle ses tentatives et affiche l'état de l'authentification sur la console HDMI (§ 4.2).

> **Attention** — Le verrouillage de SSH (`ssh.locked: true`) est **irréversible** : seule une réinitialisation usine permet de le lever. Le support de l'éditeur ne pourra plus intervenir par SSH sur la sonde. La procédure de récupération du compte administrateur (§ 8.10.2) reste possible.

4.3.4 Empreinte du mot de passe administrateur

Une **empreinte** (ou *hash*) est le résultat d'une fonction cryptographique à sens unique appliquée au mot de passe. La sonde peut vérifier qu'un mot de passe saisi correspond à l'empreinte, mais l'empreinte ne permet pas de retrouver le mot de passe. Le fichier de provisionnement ne contient ainsi jamais le mot de passe lui-même.

La sonde accepte une empreinte calculée avec l'algorithme **Argon2id**, au format PHC (*Password Hashing Competition*), de la forme `$argon2id$v=19$m=…,t=…,p=…$<sel>$<empreinte>`. Toute bibliothèque standard d'Argon2 peut la produire.

L'exemple suivant utilise la bibliothèque publique Python `argon2-cffi`, installée dans un environnement virtuel sur le poste de préparation (Linux ou macOS ; sous Windows, remplacez `argon2-env/bin/` par `argon2-env\Scripts\`) :

```bash
# Créer un environnement virtuel et y installer la bibliothèque argon2-cffi
python3 -m venv argon2-env
argon2-env/bin/pip install argon2-cffi

# Saisir le mot de passe sans affichage, puis afficher son empreinte Argon2id au format PHC
argon2-env/bin/python -c "import getpass; from argon2 import PasswordHasher;
    print(PasswordHasher().hash(getpass.getpass('Mot de passe : ')))"
```

La commande affiche une ligne commençant par `$argon2id$v=19$` : c'est la valeur à reporter dans le champ `admin.passwordHash`, **entre guillemets** (§ 4.3.6). Le sel étant tiré au hasard, deux exécutions pour le même mot de passe produisent des empreintes différentes, toutes deux valides.

Règles à respecter :

1. Choisissez un mot de passe de 12 à 128 caractères, unique et non utilisé ailleurs. Aucune règle de composition n'est imposée : privilégiez une phrase de passe longue.
2. Générez l'empreinte sur un poste de confiance, avec l'outil indiqué ci-dessus.
3. Conservez le mot de passe dans le coffre-fort de mots de passe de votre organisation.
4. Ne transmettez jamais le mot de passe par messagerie ; seule l'empreinte figure dans le fichier.

4.3.5 Procédure

Objectif : configurer la sonde automatiquement dès son premier démarrage.

Prérequis : § 4.3.2 ; sonde **non encore initialisée** avec cette microSD (le fichier est lu à chaque démarrage tant que la sonde n'est pas initialisée, puis ignoré : une fois la sonde en service, sa configuration ne peut plus être écrasée par un fichier déposé sur la carte).

Étapes :

1. Insérez la microSD dans le lecteur de votre poste de travail.

2. Ouvrez la partition FAT32 étiquetée `SVA-BOOT` : c'est la seule partition de dépôt, qui reçoit tous les fichiers décrits dans cette documentation et ceux que produit la sonde. Avec le mécanisme de mise à jour A/B, d'autres partitions de la carte peuvent apparaître sur votre poste : **ne les modifiez pas**. Si la partition `SVA-BOOT` contient d'autres fichiers que ceux décrits dans cette documentation, **ne les modifiez pas et ne les supprimez pas**.
3. Si le système de votre poste propose de formater une autre partition illisible, **refusez** (§ 3.3.3).
4. Créez à la racine de cette partition un fichier texte nommé exactement `provision.yaml`. Sous Windows, vérifiez que l'extension `.txt` n'a pas été ajoutée automatiquement (affichez les extensions de fichiers dans l'explorateur).
5. Saisissez le contenu en vous appuyant sur l'exemple ci-dessous et sur le tableau du § 4.3.3. Si vous utilisez la section `dot1x`, copiez aussi à la racine de la partition les deux fichiers désignés par `pkcs12File` et `caFile`.
6. Enregistrez le fichier en encodage **UTF-8**.
7. Vérifiez la syntaxe YAML (§ 4.3.6).
8. Éjectez proprement la microSD avec la fonction d'éjection de votre système, puis retirez-la.
9. Insérez la microSD dans la sonde (§ 3.4.5) et mettez la sonde sous tension (§ 3.8).

Exemple de fichier (valeurs fictives) pour une adresse statique :

```yaml
# Fichier de provisionnement — exemple fictif
version: 1
hostname: sonde-paris-01
site: paris-dc1
admin:
  username: admin
  # Empreinte du mot de passe (jamais le mot de passe en clair)
  passwordHash: "<empreinte Argon2id générée selon le § 4.3.4>"
network:
  mode: static            # dhcp | static
  address: 192.0.2.50/24
  gateway: 192.0.2.1
  dns: [192.0.2.10, 192.0.2.11]
  ntp: [ntp1.example.internal]
proxy:
  url: http://proxy.example.internal:3128
  noProxy: [".example.internal", "192.0.2.0/24"]
```

Exemple minimal, en adressage DHCP :

```yaml
# Fichier de provisionnement minimal — exemple fictif
version: 1
hostname: sonde-lyon-01
site: lyon-siege
admin:
  username: admin
  passwordHash: "<empreinte Argon2id générée selon le § 4.3.4>"
```

Exemple pour un port soumis à l'authentification 802.1X, avec IPv6 activé et SSH verrouillé (valeurs fictives ; les fichiers `sonde-marseille-01.p12` et `radius-ca.pem` sont déposés à côté de `provision.yaml`) :

```yaml
# Fichier de provisionnement avec 802.1X et IPv6 — exemple fictif
version: 1
hostname: sonde-marseille-01
site: marseille-agence
admin:
  username: admin
  passwordHash: "<empreinte Argon2id générée selon le § 4.3.4>"
network:
  mode: dhcp
  ipv6:
    enabled: true          # IPv6 en complément de l'IPv4 (désactivé par défaut)
    mode: static           # slaac | static
    address: 2001:db8:10::50/64
    gateway: 2001:db8:10::1
dot1x:
  identity: sonde-marseille-01.example.internal
  pkcs12File: sonde-marseille-01.p12   # clé privée et certificat client de la sonde
  caFile: radius-ca.pem                # AC du serveur RADIUS, au format PEM
  # Seul secret admis dans ce fichier ; supprimé après traitement
  pkcs12Password: "<mot de passe du fichier PKCS#12>"
ssh:
  locked: true             # Irréversible jusqu'à une réinitialisation usine
```

Résultat attendu : après le premier démarrage, la sonde est joignable à l'adresse prévue et vous pouvez vous connecter à l'interface d'administration avec le compte défini. Lors de cette première connexion, l'interface affiche une seule fois le code de récupération du compte administrateur : enregistrez-le immédiatement (§ 4.4.6). Si une section `dot1x` a été fournie, `provision.yaml`, le fichier PKCS#12 et le certificat de l'AC ont disparu de la partition `SVA-BOOT`.

Vérification : § 4.3.7, puis § 4.6.

> **Attention — Vérifiez l'empreinte du certificat avant la première connexion**, selon la procédure du § 4.4.4 : le provisionnement s'achève sans passer par l'assistant, mais cette vérification reste obligatoire avant toute saisie d'identifiants et avant toute transmission d'un jeton d'API. Sans écran HDMI, relevez l'empreinte courante dans `setup-code.txt` lorsque vous retirez la microSD pour lire `provision-result.txt` (§ 4.3.7). Si les empreintes diffèrent, n'allez pas plus loin.

> **Avertissement — Effacement du fichier PKCS#12.** La suppression du fichier PKCS#12, du certificat de l'AC et du mot de passe par la sonde est une suppression **logique** : sur une mémoire flash, elle ne garantit pas l'effacement physique des données, dont des fragments peuvent subsister sur la carte. Pour cette raison :
>
> - préférez la voie qui génère la clé sur la sonde (voie CSR du § 5.2.6) chaque fois qu'un port non contrôlé ou autorisé par MAB peut être utilisé, même temporairement : la clé privée ne quitte alors jamais la sonde et ne transite jamais par la partition `SVA-BOOT` ;
> - si la voie du provisionnement est indispensable, faites émettre pour la sonde un **certificat client dédié** à ce seul usage, de **courte durée de validité**, puis remplacez-le dès que possible par un certificat obtenu à partir d'une clé générée sur la sonde (renouvellement décrit au § 5.2.6) ;
> - traitez la microSD comme un **support sensible** pendant toute sa vie, y compris lors de son remplacement ou de sa mise au rebut (effacement sécurisé, § 8.13) ;
> - en cas de perte ou de vol de la carte, faites **révoquer** sans délai le certificat client par votre IGC et retirez son autorisation du serveur RADIUS.

> ! **Attention — Heure de la sonde et EAP-TLS au premier démarrage.** Sur un port 802.1X, la sonde n'accède au serveur NTP qu'après l'authentification, alors que la vérification des certificats exige une heure correcte. Les chemins de pré-réglage de l'horloge, sous votre contrôle, et leurs limites sont décrits au § 5.2.6. Si aucun d'eux n'est possible, la réussite de l'authentification EAP-TLS au premier démarrage ne peut pas être garantie.

4.3.6 Erreurs de syntaxe à éviter

Le YAML est sensible à l'indentation. Les erreurs les plus fréquentes sont les suivantes.

Erreur	Exemple incorrect	Correction
Tabulation au lieu d'espaces	Indentation par la touche Tab	Utiliser deux espaces par niveau
Indentation incohérente	`address` aligné différemment de `gateway`	Aligner les clés d'un même bloc
Espace manquant après les deux-points	`mode:static`	`mode: static`
Caractère spécial non protégé	Valeur contenant `#` ou `:` sans guillemets	Entourer la valeur de guillemets
Extension erronée	`provision.yaml.txt`	Renommer en `provision.yaml`
Heure non protégée	`start: 22:00` (peut être lu comme un nombre)	`start: "22:00"`

> ✓ **Conseil** — Faites valider le fichier par un outil de vérification YAML (extension de votre éditeur, ou validateur en ligne de commande) avant de le copier sur la carte. N'utilisez pas de validateur en ligne public : ce fichier contient l'empreinte du mot de passe administrateur, la configuration de votre réseau et, le cas échéant, le mot de passe du fichier PKCS#12.

4.3.7 Lire le compte rendu `provision-result.txt`

Objectif : vérifier que le provisionnement a été appliqué intégralement.

Étapes :

1. Si la sonde est joignable, consultez de préférence le résultat dans le journal d'audit (interface d'administration, ou `GET /api/v1/audit-events`) : le provisionnement y est enregistré comme un événement, avec son résultat.
2. Sinon, arrêtez proprement la sonde (chapitre 8), retirez la microSD et ouvrez la partition `SVA-BOOT` sur votre poste.
3. Ouvrez `provision-result.txt`.

Le compte rendu est un fichier texte UTF-8 qui contient : la date et l'heure de traitement, le résultat global (appliqué ou refusé), la liste des sections appliquées et, en cas de refus, chaque erreur avec son numéro de ligne et son motif. Il ne contient aucune valeur sensible.

En cas de problème : corrigez les erreurs signalées. Si la sonde n'a pas été initialisée, elle attend une mise en service par l'assistant (méthode B) : vous pouvez soit poursuivre avec l'assistant, soit déposer un fichier corrigé sur la partition `SVA-BOOT` et redémarrer la sonde : le fichier est lu à chaque démarrage tant que la sonde n'est pas initialisée.

Si la sonde reste injoignable alors que le provisionnement comporte une section `dot1x`, l'authentification 802.1X a probablement échoué : la sonde réessaie et affiche l'état de l'authentification sur la console HDMI. Vérifiez avec l'équipe réseau l'identité, la validité du certificat client, l'AC du serveur RADIUS et la configuration du port (§ 9.5).

4.4 Mise en service par l'assistant web (méthode B)

La méthode B, décrite dans cette section, consiste à configurer la sonde après son démarrage, dans un assistant web protégé par le code d'installation. La méthode A désigne l'autre parcours : le provisionnement par fichier, décrit au § 4.3, où un fichier `provision.yaml` déposé sur la microSD configure la sonde dès son premier démarrage.

4.4.1 Prérequis

- Sonde installée et démarrée (chapitre 3), sans fichier de provisionnement.
- Serveur DHCP actif sur le réseau de la sonde.
- Port de commutateur sans authentification 802.1X, ou autorisé par adresse MAC (MAB, *MAC Authentication Bypass*) : l'assistant ne permet pas de fournir un identifiant 802.1X. Sur un port contrôlé, utilisez la méthode A, ou activez 802.1X après la mise en service (chapitre 5).
- Poste d'administration sur un réseau autorisé à joindre la sonde en HTTPS (port TCP 443), équipé d'un navigateur récent.
- Accès au code d'installation (§ 4.4.3).
- Paramètres à saisir : nom d'hôte et site souhaités, serveurs DNS et NTP, proxy éventuel ; l'adresse IP définitive est obtenue par une réservation DHCP, et non saisie dans l'assistant.

4.4.2 Trouver l'adresse IP de la sonde

La sonde obtient son adresse du serveur DHCP. Plusieurs moyens permettent de la retrouver.

> ! **Avertissement** — N'utilisez pas d'outil de balayage réseau (*scan*) sans l'accord de votre équipe sécurité : ce type d'outil peut déclencher des alertes de détection d'intrusion.

Moyen	Procédure	Remarque
Table des baux DHCP	Rechercher, dans la console du serveur DHCP, le bail associé à l'**adresse MAC** de la sonde (étiquette du boîtier complet) ou au nom d'hôte `sva-XXXXXX`	Méthode la plus fiable
Réservation DHCP préalable	Créer avant le démarrage une réservation associant l'adresse MAC à une adresse choisie	Recommandé : l'adresse ne changera pas
Nom mDNS	Saisir `https://sva-XXXXXX.local/` dans le navigateur, `XXXXXX` correspondant aux six derniers caractères hexadécimaux de l'adresse MAC	Annonce mDNS active par défaut, désactivable dans la section `network` des paramètres. Fonctionne uniquement si le poste est sur le même segment réseau et si mDNS n'est pas filtré
Écran HDMI	Brancher un écran sur un port micro-HDMI : la console locale affiche l'adresse IP, le nom mDNS, l'empreinte du certificat et, tant que la sonde n'est pas initialisée, le code d'installation	Utile en l'absence d'accès au serveur DHCP
Table des adresses MAC du commutateur, table ARP du routeur	Rechercher l'adresse MAC sur le port de raccordement, puis l'adresse IP associée	Nécessite l'équipe réseau

> i **Information** — mDNS (*multicast DNS*) est un mécanisme de résolution de noms sans serveur, limité au réseau local. Les noms se terminent par `.local`. Il est souvent filtré entre VLAN.

4.4.3 Obtenir le code d'installation

Le code d'installation est un code propre à la carte, qui protège l'assistant : il est généré lors de la préparation de la carte et imprimé sur l'encart ou l'étiquette qui accompagne le produit. Il empêche qu'une autre personne présente sur le réseau ne s'approprie la sonde avant vous. Il devient invalide dès la fin de l'assistant.

Offre	Où trouver le code
Boîtier complet	Étiquette d'identification du boîtier (§ 3.5.3)
microSD préconfigurée	Encart d'identification qui accompagne la carte (§ 3.3.3)
Secours (les deux offres)	Écran branché en micro-HDMI au démarrage (console locale, avec l'empreinte du certificat), ou fichier `setup-code.txt` de la partition `SVA-BOOT`. Ce fichier contient aussi l'empreinte SHA-256 du certificat de la sonde, utile au § 4.4.4 ; il est réécrit à chaque démarrage avec l'empreinte courante (§ 4.2)

Si vous ne disposez plus de l'encart ou de l'étiquette, lisez `setup-code.txt` sans écran :

1. Laissez la sonde terminer son premier démarrage (§ 4.2).
2. Arrêtez-la proprement. Si l'interface n'est pas encore accessible, un appui bref sur le bouton d'alimentation déclenche l'arrêt propre (comportement standard de Raspberry Pi OS sur Raspberry Pi 5 ; un appui long force la coupure et doit être évité) ; attendez que le voyant passe au rouge fixe.
3. Débranchez l'alimentation, retirez la microSD et lisez le fichier `setup-code.txt` sur votre poste.
4. Réinsérez la microSD et redémarrez la sonde.

Le code d'installation reste valide d'un démarrage à l'autre tant que la sonde n'est pas initialisée : le code relevé reste donc valide après ce redémarrage. Il est invalidé à la fin de l'assistant, puis redevient valide après une réinitialisation usine (§ 8.10). Il est aussi exigé, avec le code de récupération, par la procédure de récupération du compte administrateur (§ 4.4.6) : conservez l'encart ou l'étiquette pendant toute la vie du produit.

> **Avertissement** — Traitez le code d'installation comme un mot de passe. Toute personne qui le détient, et qui peut joindre la sonde sur le réseau, peut en prendre le contrôle tant que la mise en service n'est pas terminée. Effectuez la mise en service sans délai après le premier démarrage.

4.4.4 Se connecter et vérifier le certificat

La sonde présente un **certificat TLS autosigné**, généré à son premier démarrage. Un certificat autosigné n'est pas émis par une autorité de certification reconnue par votre navigateur : celui-ci affiche donc un avertissement de sécurité. Cet avertissement est attendu lors de la mise en service. Il ne doit cependant être accepté qu'après vérification de l'**empreinte** du certificat, qui garantit que vous êtes bien connecté à votre sonde et non à un équipement intercalé.

Cette section est la procédure de référence de la vérification d'empreinte, quel que soit le parcours de mise en service (méthode A ou B) et quel que soit l'outil utilisé ensuite (navigateur, `curl`, Prometheus, Nagios). Les autres sections de la documentation y renvoient.

Objectif : établir une connexion chiffrée et authentifiée avec la sonde.

Prérequis : l'empreinte SHA-256 courante du certificat, relevée par un canal indépendant du réseau (tableau ci-dessous).

Étapes :

1. Saisissez dans le navigateur `https://<adresse-ip-de-la-sonde>/` (exemple : `https://192.0.2.50/`).
2. Le navigateur signale que le certificat n'est pas reconnu. N'acceptez pas encore.

3. Affichez le détail du certificat (icône à gauche de la barre d'adresse, puis détail du certificat ; le libellé varie selon le navigateur). Relevez son **empreinte SHA-256**.
4. Comparez cette empreinte avec celle communiquée par la sonde par un canal indépendant du réseau : écran HDMI ou fichier `setup-code.txt` de la partition `SVA-BOOT` (§ 4.4.3). Seule cette comparaison hors réseau protège contre une interception : l'empreinte affichée ensuite par l'assistant ou par l'interface transite par la même connexion que celle que vous cherchez à vérifier.
5. Si les empreintes concordent, acceptez l'exception de sécurité pour cette adresse.
6. Si elles diffèrent, **interrompez la procédure** et contactez votre équipe sécurité : une interception de la connexion est possible.

> **Attention** — La vérification de l'empreinte est **obligatoire avant toute saisie d'identifiants** (code d'installation, compte administrateur) **et avant toute transmission d'un jeton d'API**. Elle se refait chaque fois que le certificat change (changement de nom ou d'adresse, renouvellement, réinitialisation usine), avec l'empreinte **courante** : une empreinte relevée avant un redémarrage ou un changement de certificat n'est plus une référence sûre.

Canal indépendant du réseau selon le parcours. L'empreinte courante est réécrite dans `setup-code.txt` à chaque démarrage et affichée sur la console HDMI (§ 4.2).

Parcours	Canal indépendant du réseau disponible
Provisionnement sans écran (méthode A)	Fichier `setup-code.txt`, lu en retirant la microSD après le premier démarrage (§ 4.4.3)
Assistant web (méthode B)	Console de l'écran HDMI, ou fichier `setup-code.txt` (§ 4.4.3)
Certificat émis par l'AC de votre entreprise (§ 5.7.2)	La chaîne de certification de votre entreprise, vérifiée par le navigateur ou par `curl` : aucune exception de sécurité n'est alors nécessaire
Après régénération ou renouvellement du certificat autosigné	Empreinte reçue par une connexion déjà vérifiée (§ 5.2.3) ; à défaut, console HDMI ou fichier `setup-code.txt`

Vérification en ligne de commande. Pour interroger la sonde avec `curl` ou un outil de supervision **sans désactiver la vérification TLS**, ces outils ont besoin du certificat de la sonde au format PEM. Récupérez-le, soit en l'exportant depuis votre navigateur après la vérification ci-dessus, soit par l'adresse `GET /api/v1/system/certificate`, puis vérifiez son empreinte avant de l'enregistrer, par exemple sous le nom `sonde-paris-01.pem` :

```bash
# Récupérer le certificat puis afficher son empreinte SHA-256 pour la comparer à celle de setup-code.txt
curl --insecure --silent https://192.0.2.50/api/v1/system/certificate -o sonde-paris-01.pem
openssl x509 -in sonde-paris-01.pem -noout -fingerprint -sha256
```

L'option `--insecure` n'est admise ici que pour ce téléchargement unique, effectué sans jeton et suivi obligatoirement de la comparaison d'empreinte. Supprimez le fichier si les empreintes diffèrent. Une alternative consiste à afficher l'empreinte du certificat présenté par le serveur avec OpenSSL :

```bash
# Afficher l'empreinte SHA-256 du certificat présenté par la sonde
openssl s_client -connect 192.0.2.50:443 </dev/null 2>/dev/null \
  | openssl x509 -noout -fingerprint -sha256
```

L'empreinte affichée doit être identique à celle relevée par le canal indépendant du réseau.

> **Information** — Le certificat autosigné couvre, dans son extension *Subject Alternative Name*, le nom d'hôte, le nom mDNS et l'adresse IPv4 de la sonde, ainsi que son adresse IPv6 statique lorsqu'elle est configurée. Si l'un de ces éléments change et qu'aucun certificat importé n'est en place, la sonde régénère son certificat : le fichier PEM enregistré n'est plus valable. Récupérez-le et vérifiez-le de nouveau comme ci-dessus.

> **Conseil** — À l'issue de la mise en service, il est recommandé de remplacer le certificat autosigné par un certificat émis par l'autorité de certification interne de votre organisation. Les navigateurs et outils de votre parc le reconnaîtront alors sans exception de sécurité (§ 5.7).

4.4.5 Parcourir l'assistant

L'assistant comporte les étapes suivantes, dans cet ordre. Les intitulés du tableau décrivent le contenu de chaque étape ; ils ne reproduisent pas nécessairement les libellés des écrans.

Étape	Contenu	Remarques
1. Code d'installation	Saisie du code (§ 4.4.3)	Après 5 saisies erronées, la saisie est bloquée pendant 15 minutes ; cette durée double à chaque nouvelle série d'échecs. Chaque échec est journalisé
2. Édition	Affichage de l'édition inscrite sur la carte (Essential, Professional, Enterprise) ; aucune saisie	Voir § 4.5
3. Compte administrateur	Identifiant et mot de passe du premier administrateur	Mot de passe de 12 à 128 caractères, sans règle de composition ni expiration périodique
4. Réseau	Nom d'hôte, site, mode DHCP ou statique, adresse, passerelle, DNS ; activation facultative de l'IPv6 (désactivé par défaut), en mode SLAAC ou statique (adresse IPv6, passerelle IPv6)	Ne changez pas l'adresse IP dans l'assistant ; utilisez une réservation DHCP (§ 5.2.1). Un changement d'adresse ou de nom d'hôte impose une réauthentification à la nouvelle adresse dans les 120 secondes (procédure après le tableau). L'IPv4 reste toujours actif ; les serveurs DNS peuvent être IPv4 ou IPv6
5. Heure	Serveurs NTP, fuseau horaire d'affichage	La sonde vérifie la synchronisation (§ 5.4)
6. Proxy	Proxy sortant éventuel et exclusions	Facultatif
7. Certificat	Affichage de l'empreinte SHA-256 ; option d'import d'un certificat de votre AC	L'import peut être réalisé plus tard (§ 5.7)
8. Destinations d'export	Configuration facultative d'une première destination (Prometheus, OTLP…)	Peut être reportée au chapitre 2 du guide d'intégration et d'observabilité
9. Mises à jour	Choix du mode de chaque canal (correctifs de sécurité : `automatic` ou `manual` ; versions fonctionnelles : `manual` ou `automatic`), politique des correctifs critiques, puis définition d'**au moins une fenêtre de maintenance** (jours, heure de début, durée), ou choix explicite du **mode manuel** (chaque activation est alors décidée par un administrateur) ; préavis et délai de drainage	**Aucune fenêtre n'est proposée par défaut** : l'étape ne peut être validée sans un choix explicite. Sans fenêtre, aucune mise à jour n'est activée automatiquement et l'état de santé `updates` reste en `WARNING` (chapitre 8)
10. Récapitulatif	Relecture et validation	Le code d'installation est invalidé à la validation
11. Code de récupération	Affichage **unique** du code de récupération du compte administrateur	À enregistrer immédiatement dans le coffre-fort de l'organisation (§ 4.4.6) ; il ne pourra plus être affiché

Résultat attendu : la sonde affiche la page d'accueil de l'interface d'administration ; vous êtes connecté avec le compte administrateur créé.

> ! **Attention** — Ne changez pas l'adresse IP dans l'assistant ; utilisez une réservation DHCP (§ 5.2.1). Si un changement d'adresse ou de nom d'hôte est indispensable à l'étape 4, vous devez vous réauthentifier à la nouvelle adresse dans les **120 secondes**, faute de quoi la sonde revient automatiquement à la configuration précédente : suivez la procédure ci-dessous.

Changement d'adresse ou de nom d'hôte à l'étape 4 (déconseillé). Après validation de l'étape 4, la sonde devient joignable à sa nouvelle adresse. La session d'administration est liée à l'adresse d'origine (cookie de session et protection contre la falsification de requêtes, CSRF) : à la nouvelle adresse, le navigateur ouvre une **nouvelle session**, et la confirmation n'est émise qu'après votre réauthentification. L'interface émet alors pour vous la confirmation `POST /api/v1/settings/network/confirm` décrite au § 5.2.3. Procédez ainsi :

1. Dans les 120 secondes, ouvrez la nouvelle adresse. Pendant ce délai, la sonde présente encore l'**ancien certificat**, celui dont vous avez vérifié l'empreinte au § 4.4.4 : le navigateur affiche la **même empreinte**, que vous reconnaissez avant d'accepter l'exception pour cette adresse.
2. Authentifiez-vous de nouveau : la confirmation est alors émise.
3. Lorsque le nom d'hôte ou l'adresse change, le certificat autosigné est régénéré pour les inclure, et son empreinte change. Après la confirmation, l'assistant affiche l'empreinte SHA-256 du nouveau certificat, reçue par la connexion déjà vérifiée, qui en fait une source de confiance ; le nouveau certificat est mis en service 30 secondes plus tard. Relevez cette empreinte.
4. Après la bascule, comparez l'empreinte présentée par le navigateur à celle relevée à l'étape 3, avant d'accepter l'exception. Aucune vérification hors réseau n'est nécessaire dans ce délai.

Sans confirmation, la sonde revient d'elle-même à la configuration précédente au bout de 120 secondes. La nouvelle empreinte s'affiche aussi sur la console HDMI, figure dans le journal d'audit et est écrite dans le fichier `setup-code.txt` de la partition `SVA-BOOT` au plus tard au démarrage suivant ; jusqu'à ce démarrage, ce fichier peut donc encore contenir l'empreinte précédente. Si la politique de votre navigateur interdit l'exception de sécurité, si la réponse de confirmation est perdue ou si vous ne savez pas si la confirmation a été enregistrée, appliquez les recours du § 5.2.3. Un certificat émis par l'AC de votre entreprise ne dispense de l'exception que s'il couvre le nom ou l'adresse que vous utilisez pour joindre la sonde après le changement (§ 5.7.2).

4.4.6 Conserver le code de récupération du compte administrateur

Le **code de récupération** permet de redéfinir le mot de passe d'un compte administrateur si plus aucun administrateur ne peut se connecter, sans perdre la configuration de la sonde. Il comporte 24 caractères et est généré à la fin de la mise en service, quelle que soit la méthode :

- méthode B : il est affiché à la dernière étape de l'assistant (§ 4.4.5) ;
- méthode A : il est affiché à la première connexion à l'interface d'administration d'une sonde provisionnée.

La sonde ne conserve qu'une empreinte Argon2id de ce code (§ 4.3.4) : elle ne peut donc plus jamais l'afficher. La procédure de récupération exige à la fois un accès physique à la carte microSD, le code d'installation imprimé (§ 4.4.3) et ce code de récupération. Elle est décrite au § 8.10.

Objectif : conserver le code de récupération de façon sûre et durable.

Prérequis : accès en écriture au coffre-fort de mots de passe de votre organisation, ouvert sur le poste d'administration avant la fin de la mise en service.

Étapes :

1. Lorsque le code de récupération s'affiche, ne quittez pas l'écran.

2. Enregistrez le code dans le coffre-fort de votre organisation, dans une entrée qui identifie la sonde (nom d'hôte, numéro de série).
3. Relisez l'entrée enregistrée et comparez-la au code affiché, caractère par caractère.
4. Quittez l'écran seulement ensuite.

Résultat attendu : le code de récupération est enregistré dans le coffre-fort et nulle part ailleurs.

Vérification : l'entrée du coffre-fort contient un code de 24 caractères, rattaché à la bonne sonde.

Erreurs possibles :

Situation	Conséquence	Action
Écran fermé avant l'enregistrement du code	Le code ne peut plus être affiché	Un administrateur génère un nouveau code depuis l'interface ou par `POST /api/v1/system/recovery-code` (rôle `admin`, saisie de son mot de passe exigée) : le nouveau code s'affiche une seule fois et l'ancien est invalidé. Tant qu'aucun code n'est disponible, la perte du dernier compte administrateur n'est réparable que par une réinitialisation usine (§ 8.10)
Code consommé par une récupération	Un nouveau code est affiché à l'issue de la récupération	Remplacer l'ancien code par le nouveau dans le coffre-fort

> **Avertissement** — Le code de récupération donne, avec le code d'installation et un accès physique à la carte, le contrôle d'un compte administrateur. Ne le conservez ni sur l'encart du produit, ni sur la sonde, ni dans un courriel. Ne le transmettez jamais au support de l'éditeur.

4.5 Édition de la sonde

L'édition détermine les types de contrôles disponibles.

Édition	Types de contrôles disponibles
Essential	ICMP, TCP, DNS, HTTP/HTTPS (y compris vérification du contenu), plugins Nagios fournis
Professional	Essential + suites de requêtes API, contrôles de bases de données et indicateurs métier, plugins Nagios personnalisés
Enterprise	Professional + scénarios navigateur (déclaratifs et scriptés) avec Puppeteer et Chromium

L'édition acquise est inscrite sur la carte microSD lors de sa préparation, sous la forme d'un **certificat d'édition** : un fichier signé par l'éditeur et lié à l'identifiant matériel de cette carte. La sonde le vérifie **localement** à chaque démarrage, sans connexion à un serveur de l'éditeur. Il n'y a ni clé à saisir, ni activation en ligne, ni date d'expiration : le droit d'utilisation du logiciel intégré est perpétuel. Seule une carte de démonstration, prêtée par l'éditeur pour une évaluation, est limitée à 30 jours (§ 10.1 de la référence technique et API). Le certificat d'édition ne change pas lors des mises à jour et il est conservé lors d'une réinitialisation usine.

Vous pouvez changer librement de Raspberry Pi 5 compatible : l'édition suit la carte. En revanche, une copie du système sur une autre carte n'est associée à aucune édition.

Objectif : vérifier que l'édition active correspond à votre commande.

Étapes :

1. Lisez l'édition affichée à l'étape 2 de l'assistant, ou dans l'état de santé de la sonde.
2. Comparez-la à l'édition indiquée sur l'encart ou l'étiquette du produit.

Vérification : la ressource `GET /api/v1/system` indique l'édition active (§ 4.6.3).

En cas de problème : l'édition dépend du seul certificat d'édition de la carte. Si l'édition affichée n'est pas celle commandée, contactez le support ; si une fonction de l'édition semble limitée, vérifiez aussi que la capacité mémoire du Raspberry Pi 5 respecte les exigences de l'édition (§ 3.3.2), puis contactez le support en indiquant le numéro de série du produit.

> **Information** — Si le certificat d'édition est absent, invalide ou ne correspond pas à la carte (par exemple, système copié sur une autre carte), la sonde démarre en **mode restreint** : aucun contrôle n'est exécuté, mais l'interface et l'API restent accessibles pour consulter l'état, exporter la configuration et produire une archive de diagnostic. L'état de santé indique la cause : champ `editionCertificateStatus` de `GET /api/v1/system`, lisible avec le rôle `viewer` ; le détail figure dans `GET /api/v1/settings/license` (rôle `admin`). Une carte d'origine défectueuse est remplacée selon le § 8.6.

4.6 Vérifier la disponibilité de la sonde

4.6.1 Consulter l'état depuis l'interface d'administration

La page d'accueil de l'interface présente l'état de santé de la sonde : version, édition, durée de fonctionnement, état des moteurs, utilisation des ressources, synchronisation horaire, état des destinations d'export.

Les mêmes informations sont disponibles par l'API, avec la ressource `GET /api/v1/system` (§ 4.6.3).

4.6.2 Vérifier la vivacité avec `/health`

L'adresse `/health` répond sans authentification et indique uniquement si la sonde est en fonctionnement. Elle ne révèle aucune information sensible. Elle convient à une vérification rapide ou à une supervision de premier niveau.

La commande suivante utilise le fichier `sonde-paris-01.pem`, récupéré et vérifié selon le § 4.4.4 (vérification en ligne de commande) :

```bash
# Vérifier la vivacité de la sonde (exemple fictif)
# --cacert : fait confiance au certificat exporté de la sonde, et à lui seul
curl --cacert sonde-paris-01.pem https://192.0.2.50/health
```

Résultat attendu : un code HTTP `200`. La réponse est `{"status": "OK"}`.

> **Avertissement** — L'option `-k` (ou `--insecure`) de `curl` désactive toute vérification du certificat : elle expose vos jetons d'API à une interception. Ne l'utilisez pas, même pour un test ponctuel, en dehors du téléchargement initial du certificat décrit au § 4.4.4.

4.6.3 Créer un jeton d'API et consulter l'état du système

Les appels à l'API, hors `/health` et `GET /api/v1/system/certificate`, exigent un **jeton d'API**. Un jeton d'API est une chaîne aléatoire, associée à un rôle, qui authentifie un outil ou un script auprès de la sonde. La gestion des jetons est décrite au chapitre 6.

Étapes :

1. Dans l'interface d'administration, créez un jeton de rôle `viewer` à usage de vérification (chapitre 6).
2. Copiez-le immédiatement : il n'est affiché qu'une seule fois.

3. Enregistrez-le une seule fois dans un fichier d'en-tête protégé, `$HOME/.sva/entete-auth`, lisible par vous seul, avec la commande ci-dessous (procédure détaillée au § 6.3.3). Le jeton n'apparaît ainsi ni dans l'historique du shell ni dans les arguments des commandes, visibles dans la liste des processus : `curl` lit l'en-tête dans le fichier.

   Sur un poste Linux ou macOS (shell bash ou zsh), la commande suivante rend le répertoire `$HOME/.sva` privé, crée le fichier vide en mode `600`, puis y écrit le jeton, saisi au clavier sans affichage (collez-le, puis appuyez sur Entrée) :

   ```bash
   (
     umask 077
     mkdir -p "$HOME/.sva" && chmod 700 "$HOME/.sva" &&
     rm -f "$HOME/.sva/entete-auth" &&
     : > "$HOME/.sva/entete-auth" && chmod 600 "$HOME/.sva/entete-auth" &&
     IFS= read -rs SONDE_TOKEN &&
     printf 'Authorization: Bearer %s\n' "$SONDE_TOKEN" > "$HOME/.sva/entete-auth"
   )
   ```

   N'activez pas la trace du shell (`set -x`) pendant cette opération : elle afficherait le jeton. Pour remplacer le jeton, recréez simplement le fichier avec la même commande.

```bash
# Consulter l'état du système
# L'en-tête d'authentification est lu dans le fichier protégé créé selon le § 6.3.3
curl --cacert sonde-paris-01.pem \
     -H @"$HOME/.sva/entete-auth" \
     https://192.0.2.50/api/v1/system
```

Résultat attendu : une réponse JSON indiquant notamment la version, l'édition, l'état des modules et des exports. Le détail des champs figure au § 7.9.1 du guide d'utilisation et de supervision.

4.6.4 Contrôler le fonctionnement des services

La sonde repose sur deux composants logiciels principaux : le **moteur principal**, qui planifie et exécute les contrôles et sert l'interface, et le **moteur de scénarios**, qui exécute les scénarios navigateur et les plugins dans un environnement isolé (chapitre 1).

Vérification	Où	Résultat attendu
Moteur principal actif	Page d'état de santé ; `GET /api/v1/system`	État nominal
Moteur de scénarios actif	Idem	État nominal. Hors édition Enterprise, les scénarios navigateur ne sont pas disponibles, mais l'environnement isolé reste toujours actif, quelle que soit l'édition, car il exécute les contrôles ICMP (`fping`) et les plugins. Chromium est présent sur la carte de toutes les éditions, qui partagent le même système, mais il n'est activé que par le certificat d'édition Enterprise (§ 4.5)
Heure synchronisée	Idem	Synchronisation NTP établie
Espace de stockage	Idem	Occupation faible sur une sonde neuve
Alimentation	Idem	Aucune alerte de sous-tension
Mises à jour (composant `updates`)	Idem	`OK` sur une sonde neuve dotée d'au moins une fenêtre de maintenance ; `WARNING` tant qu'aucune fenêtre n'est définie en mode automatique (§ 4.3.3 ; état de santé : § 7.9.1 du guide d'utilisation et de supervision)

> **Information** — L'accès SSH est désactivé par défaut. Les vérifications courantes ne le nécessitent pas. L'activation temporaire de SSH pour un diagnostic avancé (durée limitée, 4 heures par défaut et 72 heures au maximum, désactivation automatique à l'échéance) est décrite au § 5.9.4.

> **Information** — Si votre sonde est équipée d'un SSD NVMe facultatif (carte M.2 HAT+), celui-ci n'intervient pas dans la mise en service : la sonde démarre et fonctionne sur la microSD, qui reste son support de démarrage. Le SSD s'active **après** la mise en service, par un administrateur ; ses données (historique, artefacts, file d'export, journaux persistants) y sont alors migrées (chapitre 8).

4.7 Premier contrôle de supervision

Objectif : vérifier de bout en bout que la sonde exécute un contrôle, en enregistre le résultat et le restitue.

Prérequis : une cible HTTPS joignable depuis la sonde. L'exemple utilise une application fictive, `https://intranet.example.internal/`. Choisissez une page de votre intranet, accessible sans authentification.

4.7.1 Créer le contrôle depuis l'interface d'administration

Étapes :

1. Ouvrez la gestion des contrôles et créez un contrôle de type **HTTP**.
2. Renseignez :
   - identifiant : `intranet-accueil` ;
   - nom : « Intranet : page d'accueil » ;
   - URL : `https://intranet.example.internal/` ;
   - fréquence : 5 minutes ;
   - délai maximal (*timeout*) : 10 secondes ;
   - vérification : code de réponse égal à 200.
3. Enregistrez puis déclenchez une exécution immédiate.
4. Ouvrez le détail de l'exécution.

Le détail de l'exécution indique l'état du contrôle, sa durée et les phases de la requête. La même opération par l'API est décrite au § 4.7.2.

4.7.2 Créer le contrôle par l'API

Le même contrôle peut être créé par l'API, avec un jeton de rôle `operator` ou `admin` : le jeton `viewer` du § 4.6.3 ne suffit pas. Préparez d'abord ce jeton :

1. Dans l'interface d'administration, ouvrez la gestion des jetons et créez un jeton nommé explicitement (par exemple `mise-en-service`), de rôle `operator`, avec une date d'expiration proche (§ 6.5.2).
2. Copiez sa valeur immédiatement : elle n'est affichée qu'une seule fois.
3. Remplacez le jeton `viewer` par ce jeton dans le fichier d'en-tête protégé `$HOME/.sva/entete-auth`, en exécutant de nouveau la commande du § 4.6.3 (fichier recréé en mode `600`, jeton saisi sans affichage).

L'exemple suppose que le fichier `intranet-accueil.json` contient la définition suivante :

```json
{
  "id": "intranet-accueil",
  "name": "Intranet : page d'accueil",
  "type": "http",
  "schedule": { "interval": "5m" },
  "timeout": "10s",
  "http": {
    "method": "GET",
    "url": "https://intranet.example.internal/",
    "assertions": [
      { "kind": "status", "operator": "eq", "value": 200 }
    ]
  }
}
```

```bash
# 1. Créer le contrôle
curl --cacert sonde-paris-01.pem \
     -H @"$HOME/.sva/entete-auth" \
     -H "Content-Type: application/json" \
     --data @intranet-accueil.json \
     https://192.0.2.50/api/v1/checks

# 2. Déclencher une exécution immédiate (réponse 202 Accepted + en-tête Location)
curl --cacert sonde-paris-01.pem -i -X POST \
     -H @"$HOME/.sva/entete-auth" \
     https://192.0.2.50/api/v1/checks/intranet-accueil/runs

# 3. Consulter le dernier état du contrôle
curl --cacert sonde-paris-01.pem \
     -H @"$HOME/.sva/entete-auth" \
     https://192.0.2.50/api/v1/checks/intranet-accueil/status
```

Résultat attendu :

- la création renvoie le contrôle enregistré ;
- le déclenchement renvoie `202 Accepted` et l'adresse de l'exécution dans l'en-tête `Location` ;
- après quelques secondes, l'état vaut `OK`.

Le modèle complet des contrôles est décrit aux chapitres 3 et 4 du guide d'utilisation et de supervision.

> **Information** — L'état d'un contrôle (`GET /api/v1/checks/{id}/status` , commande 3 de l'exemple) se lit avec un jeton de rôle `metrics` ou supérieur : `metrics` est le rôle minimal indiqué pour cette ressource (§ 6.6, chapitre 10). Chaque jeton possède un rôle unique (§ 6.4.1) ; le jeton `operator` utilisé ici convient donc pour les trois commandes, et un jeton `metrics` suffit pour la seule commande 3, par exemple pour Nagios ou Centreon.

En cas de problème :

État obtenu	Cause probable	Action
`CRITICAL` avec `error.type` = `dns_error`	Nom non résolu par les serveurs DNS de la sonde	Vérifier la configuration DNS (§ 5.3)
`CRITICAL` avec `connection_refused` ou `timeout`	Flux bloqué par un pare-feu, ou proxy nécessaire	Vérifier les flux (§ 5.6) et le proxy (§ 5.5)

État obtenu	Cause probable	Action
`CRITICAL` avec `tls_error`	Certificat de la cible émis par une AC interne inconnue de la sonde	Importer l'AC interne (§ 5.7.3)
`CRITICAL` avec `http_status`	Code de réponse différent de 200 (redirection vers une page d'authentification, par exemple)	Choisir une page publique ou adapter l'assertion

4.8 Vérifier la remontée des résultats

Les résultats sont conservés **localement** par la sonde, qui fonctionne de manière autonome : aucune plateforme externe n'est nécessaire pour les consulter.

Vérification	Méthode	Résultat attendu
Historique local	Interface : historique du contrôle ; API : `GET /api/v1/runs?checkId=intranet-accueil`	Les exécutions planifiées apparaissent toutes les 5 minutes
Destination d'export (si configurée)	Interface : état des destinations ; API : `POST /api/v1/exporters/{id}/test`	Envoi de test réussi
Métriques Prometheus (si utilisé)	Collecte de `/metrics` par votre serveur Prometheus	La série de l'état du contrôle est présente (chapitre 2 du guide d'intégration et d'observabilité)

La configuration des destinations d'export (Prometheus, Grafana, Datadog, Dynatrace, Nagios/Centreon) est décrite au chapitre 2 du guide d'intégration et d'observabilité ; l'interprétation des résultats, au chapitre 7 du guide d'utilisation et de supervision.

> ✓ **Conseil** — Une fois le premier contrôle validé, révoquez (supprimez) les jetons `viewer` et `operator` créés pour ces vérifications, ou créez-les dès le départ avec une date d'expiration (`expiresAt`) (§ 6.5).

4.9 Checklist de fin de mise en service

Point de contrôle	Référence	Vérifié
Premier démarrage terminé sans interruption	§ 4.2	[ ]
Provisionnement appliqué sans erreur (méthode A) ou assistant terminé (méthode B)	§ 4.3, § 4.4	[ ]
Empreinte du certificat vérifiée et consignée	§ 4.4.4	[ ]
Compte administrateur personnel créé ; mot de passe stocké dans le coffre-fort de l'organisation	§ 4.3.4, § 4.4.5	[ ]
Code de récupération du compte administrateur enregistré dans le coffre-fort de l'organisation ; encart ou étiquette portant le code d'installation conservé	§ 4.4.6 ; § 8.10.2	[ ]
Authentification 802.1X établie, si le port est contrôlé	§ 4.3.3 ; chapitre 5	[ ]
Adresse IP définitive confirmée (réservation DHCP ou adresse statique)	§ 5.2	[ ]
Nom d'hôte et site renseignés	§ 4.3.3	[ ]
Heure synchronisée par NTP	§ 5.4	[ ]
Édition affichée conforme à la commande	§ 4.5	[ ]

Point de contrôle	Référence	Vérifié
Moteurs en fonctionnement, aucune alerte de santé	§ 4.6.4	[ ]
Premier contrôle exécuté avec l'état `OK`	§ 4.7	[ ]
Résultats consultables localement	§ 4.8	[ ]
Jetons `viewer` et `operator` créés pour les vérifications révoqués, ou dotés d'une date d'expiration (`expiresAt`)	§ 4.8 ; § 6.5	[ ]
Destinations d'export configurées et testées (si prévu)	Chapitre 2 du guide d'intégration et d'observabilité	[ ]
Fichier de provisionnement et, le cas échéant, fichiers 802.1X (PKCS#12, certificat de l'AC) supprimés de la carte et du poste de préparation	§ 4.3	[ ]
SSH toujours désactivé (sauf besoin justifié), ou verrouillé si votre politique de sécurité l'exige	§ 4.3.3, § 5.9.4	[ ]
Politique de mises à jour définie : mode de chaque canal et au moins une fenêtre de maintenance, ou mode manuel assumé avec une procédure d'activation par un administrateur ; état de santé `updates` vérifié	§ 4.3.3, § 4.4.5 ; chapitre 8	[ ]
SSD NVMe éventuel activé une fois la mise en service terminée	Chapitre 8	[ ]
Fiche de mise en service complétée (chapitre 10)	Chapitre 10	[ ]

La sonde est opérationnelle. Le chapitre 5 détaille la configuration réseau et les mesures de sécurité à appliquer pour une exploitation durable.

Chapitre 5 — Configuration réseau et sécurité

La sonde s'installe dans le réseau qui correspond au point d'observation choisi : réseau de votre organisation, site distant, ou réseau d'un client, d'un partenaire ou d'un sous-traitant (§ 1.2.1). Elle accède à des applications métier, parfois avec des comptes de test, et transmet des données vers vos outils de supervision. Sa configuration réseau et sa sécurisation conditionnent donc à la fois la **pertinence des mesures** et la **sécurité du système d'information** qui l'accueille.

Ce chapitre s'adresse aux administrateurs réseau et système ainsi qu'aux responsables de la sécurité des systèmes d'information (RSSI). Il complète la mise en service (chapitre 4) et précède l'administration courante (chapitre 6).

> **Information** — Les adresses, noms de domaine et comptes utilisés dans ce chapitre sont fictifs : réseau `192.0.2.0/24`, domaine `example.internal`.

5.1 Principes de sécurité de la sonde

La conception de la sonde repose sur les principes suivants, qui guident l'ensemble des recommandations de ce chapitre.

Principe	Mise en œuvre
Aucun secret par défaut	Pas de mot de passe par défaut ; clés et certificat générés sur chaque sonde au premier démarrage (§ 4.2)
Connexions sortantes privilégiées	La sonde initie elle-même ses échanges avec les plateformes externes. Les flux entrants se limitent à l'administration et à l'API en HTTPS (443/TCP), à la redirection HTTP vers HTTPS (80/TCP, désactivable), à l'annonce mDNS (5353/UDP, désactivable), à SSH (22/TCP) s'il est activé, et à la collecte par Prometheus ou l'interrogation par Nagios et Centreon, en HTTPS (§ 5.6.1)
Chiffrement des échanges	Interface d'administration et API exclusivement en HTTPS ; exports vers les plateformes en HTTPS. L'export OTLP en HTTP non chiffré reste admis vers un collecteur ou un agent interne (§ 5.6.1)
Moindre privilège	Rôles distincts pour les utilisateurs et les jetons ; comptes de test dédiés et limités ; exécution des scénarios et plugins dans un environnement isolé, sans accès aux secrets non déclarés
Autonomie	La sonde n'exige aucun accès à Internet pour fonctionner ; chaque flux externe est facultatif et explicite
Traçabilité	Journal d'audit des opérations d'administration

> **Avertissement** — La sonde n'est pas conçue pour être exposée sur Internet. N'ouvrez jamais l'accès à son interface d'administration ou à son API depuis l'extérieur du réseau où elle est installée, même temporairement. Pour une administration à distance, utilisez un moyen d'accès sécurisé à ce réseau (VPN d'administration, bastion), celui de votre organisation ou celui convenu avec l'exploitant du réseau d'accueil.

5.2 Adressage IP

La sonde utilise une seule interface réseau, l'interface Ethernet. Elle fonctionne en IPv4, toujours actif, et peut fonctionner en double pile : l'IPv6 est activable et désactivé par défaut (§ 5.2.5). L'accès à un port protégé par 802.1X est décrit au § 5.2.6.

5.2.1 DHCP et réservation

Par défaut, la sonde obtient son adresse par **DHCP** (*Dynamic Host Configuration Protocol*), le protocole qui attribue automatiquement une adresse IP, une passerelle et des serveurs DNS aux équipements d'un réseau.

L'adresse d'une sonde doit cependant rester **stable**, car vos outils l'interrogent : serveur Prometheus, Nagios ou Centreon, postes d'administration, règles de pare-feu. Deux solutions sont possibles :

Solution	Avantages	Inconvénients
Réservation DHCP (adresse fixe associée à l'adresse MAC)	Configuration centralisée sur le serveur DHCP ; aucune intervention sur la sonde ; changement d'adressage maîtrisé par l'équipe réseau	Dépend de la disponibilité du serveur DHCP au démarrage
Adresse statique configurée sur la sonde	Indépendante du DHCP	Configuration à maintenir sur chaque sonde ; risque de conflit d'adresse si la plage n'est pas réservée

> ✓ **Conseil** — Privilégiez la réservation DHCP lorsque votre organisation en a l'usage. Réservez l'adresse statique aux réseaux sans DHCP, comme certains réseaux de serveurs.

5.2.2 Adresse statique

Une configuration statique comprend :

- l'adresse IPv4 et la longueur de préfixe (exemple : `192.0.2.50/24`) ;
- la passerelle par défaut (exemple : `192.0.2.1`) ;
- un ou plusieurs serveurs DNS (deux recommandés) ;
- éventuellement un ou plusieurs domaines de recherche DNS (propriété `searchDomains` de la section `network`).

Elle peut être définie :

- dès le premier démarrage, par le fichier de provisionnement (§ 4.3) ;
- lors de la mise en service, par l'assistant (§ 4.4.5) ;
- à tout moment ensuite, par l'interface d'administration ou par l'API (§ 5.2.4).

5.2.3 Mécanisme de confirmation des changements réseau

Une erreur de configuration réseau (adresse incorrecte, passerelle erronée) peut rendre une sonde injoignable, et imposer une intervention physique. Pour éviter cette situation, la sonde applique tout changement de configuration réseau selon un principe de **confirmation obligatoire** :

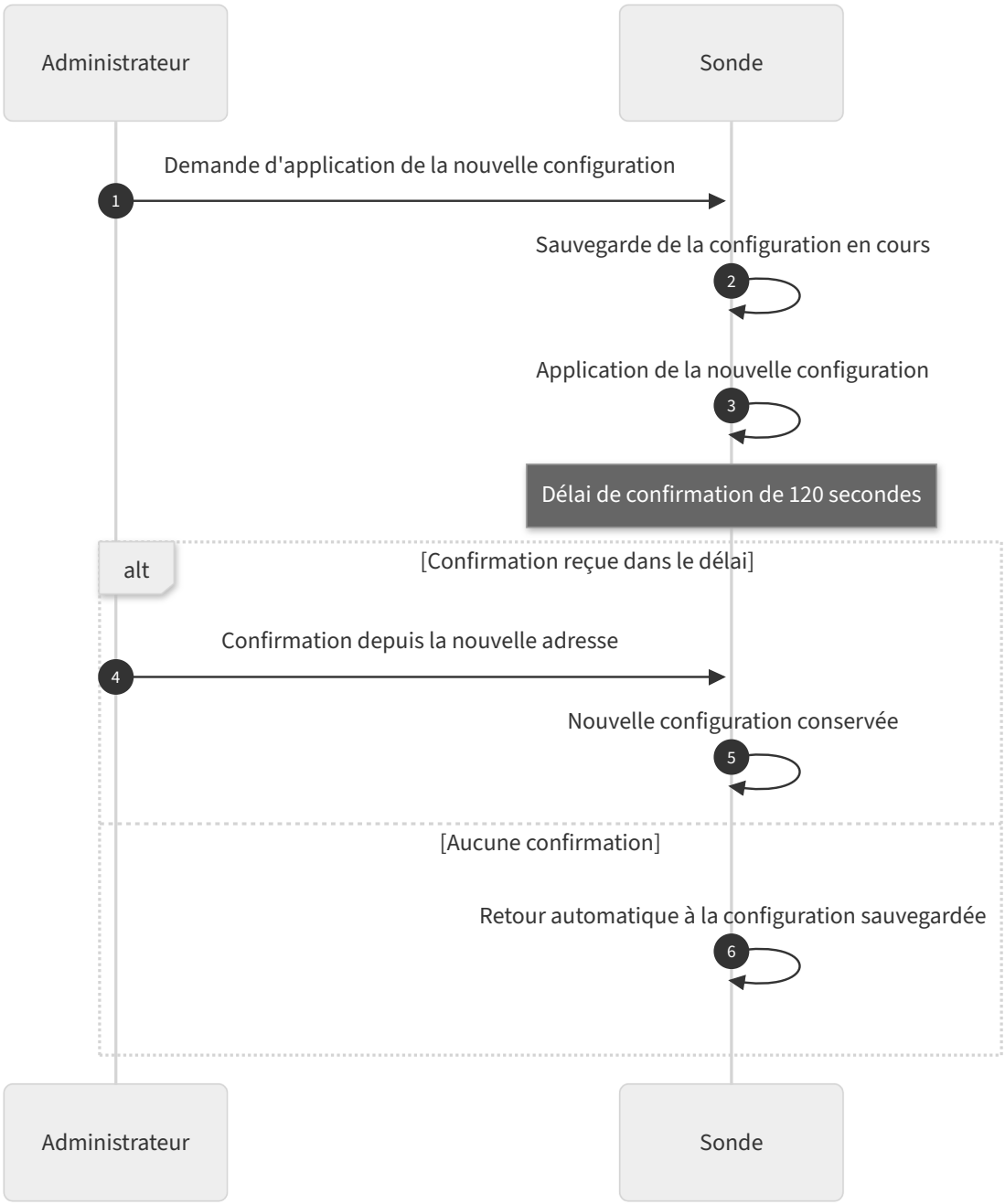


Schéma 5-1 — Confirmation obligatoire d'un changement réseau

Conséquences pratiques :

1. Après l'application, la sonde peut changer d'adresse : reconnectez-vous à la **nouvelle** adresse.
2. Confirmez dans les **120 secondes**.

3. Si vous ne parvenez pas à joindre la nouvelle adresse, attendez : au terme du délai, la sonde revient d'elle-même à l'ancienne configuration.

L'application (`POST /api/v1/settings/network/apply`) renvoie un identifiant de changement. La confirmation s'effectue par l'appel `POST /api/v1/settings/network/confirm`, émis **depuis la nouvelle adresse** de la sonde, ce qui prouve qu'elle reste joignable. L'interface d'administration émet cette confirmation lorsque, dans le délai, vous vous êtes reconnecté à la nouvelle adresse et authentifié de nouveau (paragraphe « Confirmation depuis un navigateur » ci-dessous).

Certificat pendant et après la confirmation. Pendant la fenêtre de 120 secondes, la sonde présente encore l'**ancien certificat**, celui dont vous avez déjà vérifié l'empreinte. Vous confirmez donc à la nouvelle adresse en reconnaissant la même empreinte (interface d'administration), ou en indiquant à curl l'ancien certificat et l'ancien nom (API, § 5.2.4). Si le changement entraîne la régénération du certificat autosigné (encadré du § 5.2.4), la réponse à la confirmation contient le **nouveau certificat** : champ `certificate` (format PEM), champ `fingerprint` (empreinte SHA-256) et champ `activatesAt` (instant de la mise en service, 30 secondes après la confirmation). Transmis par la connexion déjà vérifiée, ce certificat est une source de confiance : aucune vérification hors réseau n'est nécessaire dans le délai. L'interface d'administration affiche la nouvelle empreinte avant la bascule.

Confirmation depuis un navigateur. La session d'administration est liée à l'origine, c'est-à-dire à l'adresse ou au nom saisi dans le navigateur : son cookie et le jeton de protection contre la falsification de requêtes (CSRF, *Cross-Site Request Forgery*) ne sont pas valables à la nouvelle adresse. Après avoir reconnu l'empreinte à la nouvelle adresse, **authentifiez-vous de nouveau** ; la confirmation n'est émise qu'ensuite. Tenez compte de ce temps de reconnexion dans le délai de 120 secondes.

Recours lorsque le parcours ne se déroule pas comme prévu.

Situation	Conduite à tenir
La politique du navigateur interdit l'exception de sécurité à la nouvelle adresse (navigateur géré par l'organisation, par exemple)	Laissez la sonde revenir à l'ancienne configuration (120 secondes), puis effectuez le changement par l'API, avec `curl` (§ 5.2.4). Pour éviter ce cas, préférez une réservation DHCP (§ 5.2.1), qui ne modifie pas la configuration de la sonde, ou installez au préalable un certificat émis par l'AC de votre entreprise (§ 5.7.2)
La réponse de confirmation est perdue (coupure, fermeture de l'onglet, échec de l'écriture du fichier `confirmation.json`)	Récupérez le certificat par `GET /api/v1/system/certificate` (sans authentification, § 4.4.4), puis vérifiez son empreinte par un canal indépendant du réseau : de préférence la console de l'écran HDMI. Le fichier `setup-code.txt` de la partition `SVA-BOOT` n'est réécrit qu'au démarrage : il peut encore porter l'empreinte de l'ancien certificat tant que la sonde n'a pas redémarré (§ 4.2). Ne transmettez aucun jeton et ne saisissez aucun identifiant tant que cette vérification n'est pas faite
Vous ne savez pas si la confirmation a été enregistrée	Attendez la fin du délai de 120 secondes : la sonde est alors joignable à la nouvelle adresse si la confirmation a été enregistrée, à l'ancienne dans le cas contraire. Le journal d'audit l'indique
Aucune confirmation dans le délai	La sonde revient automatiquement à la configuration précédente au bout de 120 secondes : c'est la sécurité du mécanisme. Recommencez l'opération

> ✓ **Conseil** — Ne changez l'adresse ou le nom d'hôte d'une sonde qu'en cas de nécessité. Pour stabiliser une adresse, préférez une réservation DHCP (§ 5.2.1), qui ne modifie pas la configuration de la sonde.

5.2.4 Modifier la configuration réseau

Objectif : modifier l'adressage d'une sonde en service sans risque de perte d'accès.

Prérequis :

- compte ou jeton de rôle `admin` ;

- nouveaux paramètres validés avec l'équipe réseau ;
- règles de pare-feu mises à jour pour la nouvelle adresse (accès d'administration, collecte Prometheus, Nagios) ;
- poste d'administration capable de joindre la nouvelle adresse.

Étapes (interface d'administration) :

1. Ouvrez les paramètres réseau de l'interface d'administration.
2. Saisissez les nouveaux paramètres.
3. Appliquez.
4. Reconnectez-vous à la nouvelle adresse dans les 120 secondes : l'interface confirme alors la configuration.

Étapes (API) : la section `network` des paramètres se consulte et se modifie par `GET` et `PUT /api/v1/settings/network`, puis s'applique par `POST /api/v1/settings/network/apply` et se confirme par `POST /api/v1/settings/network/confirm` (§ 5.2.3). Le format de la section `network` est le suivant.

JSON
```
{
  "hostname": "sonde-paris-01",
  "mode": "static",
  "address": "192.0.2.50/24",
  "gateway": "192.0.2.1",
  "dns": ["192.0.2.10", "192.0.2.11"]
}
```

BASH
```
# Préparation du poste selon le § 6.3.3 : fichier d'en-tête $HOME/.sva/entete-auth
# (jeton de rôle admin), variable CA (certificat vérifié de la sonde) et fonction
# sapi. SONDE désigne ici l'ancienne adresse de la sonde, présente dans son
# certificat (exemple fictif).
SONDE=https://192.0.2.50

# 1. Lire la configuration courante et son ETag (en-têtes affichés par -i)
sapi -i "$SONDE/api/v1/settings/network"

# 2. Enregistrer la nouvelle configuration (If-Match : ETag relevé à l'étape 1)
sapi -X PUT -H 'Content-Type: application/json' \
     -H 'If-Match: "<etag>"' \
     --data @network.json \
     "$SONDE/api/v1/settings/network"

# 3. Appliquer : la réponse contient l'identifiant du changement, à confirmer
#    dans les 120 secondes par POST /api/v1/settings/network/confirm,
#    appelé depuis la nouvelle adresse de la sonde (§ 5.2.3)
sapi -X POST "$SONDE/api/v1/settings/network/apply"

# 4. Confirmer depuis la nouvelle adresse (exemple fictif : 192.0.2.60), dans les
#    120 secondes. La sonde présente encore l'ancien certificat : curl le vérifie
#    avec l'ancien fichier de confiance ($CA) et l'ancien nom (ici l'ancienne
#    adresse, 192.0.2.50), et se connecte à la nouvelle adresse grâce à --connect-to.
#    <id> : identifiant renvoyé à l'étape 3
sapi --connect-to 192.0.2.50:443:192.0.2.60:443 \
     -X POST -H 'Content-Type: application/json' \
     --data '{"id":"<id>"}' \
     -o confirmation.json \
     "$SONDE/api/v1/settings/network/confirm"
```

Si le certificat autosigné est régénéré, la réponse de l'étape 4 (fichier `confirmation.json`) contient les champs `certificate`, `fingerprint` et `activatesAt` (§ 5.2.3). Enregistrez le contenu du champ `certificate` comme **nouveau fichier de confiance** (par exemple `sonde-paris-01-nouveau.pem`, avec l'outil standard `jq` : `jq -r`

`.certificate confirmation.json > sonde-paris-01-nouveau.pem`) et relevez l'empreinte `fingerprint`. À partir de l'instant `activatesAt`, utilisez ce nouveau fichier dans vos appels (variable `CA` du § 6.3.3, option `--cacert`) et fournissez-le à vos outils (Prometheus, Nagios, Centreon).

Si la commande de l'étape 4 n'a pas produit de fichier `confirmation.json` exploitable, appliquez les recours du § 5.2.3 : récupération du certificat par `GET /api/v1/system/certificate`, puis vérification de son empreinte sur la console HDMI ou dans `setup-code.txt`, avant tout nouvel appel muni du fichier d'en-tête.

> **Information** — Dans l'étape 4, `--connect-to` dirige la connexion vers la nouvelle adresse tout en conservant l'ancien nom pour la vérification du certificat, qui contient encore ce nom. Le nom utilisé dans l'URL doit figurer dans l'ancien certificat (nom d'hôte, nom mDNS ou ancienne adresse IPv4, comme dans l'exemple).

> **Attention** — `PUT /api/v1/settings/network` **remplace la section entière** : un champ absent du corps reprend sa valeur par défaut ou disparaît. Partez donc toujours du résultat du `GET` de l'étape 1, et conservez dans `network.json` les champs que vous ne modifiez pas, notamment `mdns`, `searchDomains` et `ipv6`. Les exemples ci-dessus ne montrent que les champs de l'adressage IPv4.

> **Information** — Les serveurs NTP ne font pas partie de la section `network` des paramètres : le champ `network.ntp` du fichier de provisionnement (§ 4.3.3) correspond à la section `time` des paramètres (§ 5.4).

L'en-tête `If-Match` garantit que la configuration n'a pas été modifiée par un autre administrateur entre la lecture et l'écriture : en cas de conflit, la sonde répond `412 Precondition Failed`.

Résultat attendu : la sonde est joignable à sa nouvelle adresse ; la configuration est confirmée.

Vérification : page d'état de santé ; exécution correcte des contrôles ; collecte Prometheus ou interrogation Nagios rétablie.

En cas de problème : sans confirmation, la sonde revient à l'ancienne configuration au bout de 120 secondes. Si elle reste injoignable au-delà, voir chapitre 9.

> **Attention** — Le certificat autosigné de la sonde contient son nom d'hôte, son nom mDNS, son adresse IPv4 et, si l'IPv6 est activé en mode statique, son adresse IPv6. Si l'un de ces éléments change et qu'aucun certificat importé n'est en place, la sonde régénère automatiquement son certificat autosigné ; le nouveau certificat apparaît sur la console HDMI et dans le journal d'audit. Pendant la fenêtre de confirmation, la sonde présente encore l'ancien certificat ; le nouveau est transmis dans la réponse de la confirmation, par la connexion déjà vérifiée, puis mis en service 30 secondes plus tard (§ 5.2.3). Son empreinte change : les outils auxquels vous avez fourni l'ancien certificat (curl, Prometheus) refusent alors la connexion jusqu'à ce que vous leur fournissiez le nouveau, enregistré à partir de la réponse de la confirmation (étape 4 ci-dessus). Utilisez un nom DNS stable plutôt qu'une adresse IP dans vos configurations, et de préférence un certificat de votre AC interne (§ 5.7.2).

5.2.5 IPv6

La sonde fonctionne en **double pile** : l'IPv4 est toujours actif et obligatoire, l'IPv6 est facultatif et **désactivé par défaut**. Une fois activé, il permet d'administrer la sonde et de superviser des cibles en IPv6, en complément de l'IPv4.

Paramètres. L'IPv6 se règle dans la section `network`, par l'objet `ipv6` :

Champ	Description	Exemple fictif
`ipv6.enabled`	Active l'IPv6. Valeur par défaut : `false`	`true`
`ipv6.mode`	`slaac` : adresse obtenue automatiquement à partir des annonces du routeur (*StateLess Address AutoConfiguration*) ; `static` : adresse fixe	`static`
`ipv6.address`	Adresse IPv6 et longueur de préfixe, en notation CIDR. Obligatoire en mode `static`	`2001:db8:10::50/64`
`ipv6.gateway`	Passerelle IPv6 par défaut. Obligatoire en mode `static`	`2001:db8:10::1`

Les serveurs DNS de la sonde (propriété `dns`) peuvent indifféremment être des adresses IPv4 ou IPv6.

Exemple de section `network` avec IPv4 et IPv6 statiques (valeurs fictives) :

```json
{
  "hostname": "sonde-paris-01",
  "mode": "static",
  "address": "192.0.2.50/24",
  "gateway": "192.0.2.1",
  "dns": ["192.0.2.10", "2001:db8:10::53"],
  "ipv6": {
    "enabled": true,
    "mode": "static",
    "address": "2001:db8:10::50/64",
    "gateway": "2001:db8:10::1"
  }
}
```

En mode `slaac`, l'objet se réduit à `{"enabled": true, "mode": "slaac"}`.

Effets de l'activation.

Domaine	Comportement
Contrôles	Le paramètre commun `ipFamily` de chaque contrôle choisit la famille d'adresses : `auto` (par défaut) utilise l'IPv6 si celui-ci est activé et si la cible possède une adresse AAAA, l'IPv4 sinon ; `ipv4` et `ipv6` imposent une famille (chapitre 3 du guide d'utilisation et de supervision). Les contrôles ICMP utilisent alors ICMPv6 (outil `fping`)
Pare-feu local	Les règles du pare-feu local (§ 5.6.3) s'appliquent de façon identique en IPv6
Certificat autosigné	S'il est en place, il inclut l'adresse IPv6 statique de la sonde
Flux réseau	Le flux ICMPv6 de découverte des voisins doit être autorisé sur le réseau local de la sonde (§ 5.6.1)

Procédure.

Objectif : activer l'IPv6 sur une sonde en service.

Prérequis :

- compte ou jeton de rôle `admin` ;
- réseau de la sonde routé en IPv6, avec annonces de routeur en mode `slaac`, ou adresse et passerelle IPv6 attribuées par l'équipe réseau en mode `static` ;
- règles de pare-feu réseau mises à jour pour l'IPv6 : accès d'administration, collecte Prometheus, Nagios, flux des contrôles, ICMPv6 de découverte des voisins.

Étapes :

1. Ajoutez l'objet `ipv6` à la section `network`, dans l'interface d'administration ou par l'API (§ 5.2.4). L'IPv6 peut aussi être activé dès la mise en service, par le fichier de provisionnement (§ 4.3.3).
2. Appliquez la configuration, puis confirmez-la dans les 120 secondes (§ 5.2.3).
3. Pour chaque contrôle dont la cible doit être jointe dans une famille précise, réglez `ipFamily` (chapitre 3 du guide d'utilisation et de supervision).

Résultat attendu : la sonde dispose d'une adresse IPv6 et reste joignable en IPv4.

Vérification : la configuration effective, lue par `GET /api/v1/settings/network` ou sur la page d'état de santé, présente l'adresse IPv6 ; un contrôle de test réglé sur `"ipFamily": "ipv6"` vers une cible IPv6 connue réussit.

Erreurs possibles :

Symptôme	Cause probable	Action
Aucune adresse IPv6 en mode `slaac`	Pas d'annonce de routeur sur le réseau de la sonde ; ICMPv6 filtré	Vérifier la configuration du routeur avec l'équipe réseau ; autoriser ICMPv6 de découverte des voisins
Contrôles en échec après l'activation, alors qu'ils réussissaient en IPv4	Les cibles ont une adresse AAAA, mais le chemin IPv6 est filtré ou non routé. La règle `auto` ne prévoit pas de repli sur l'IPv4	Corriger le routage ou le filtrage IPv6, ou fixer `"ipFamily": "ipv4"` sur les contrôles concernés
Interface d'administration inaccessible en IPv6	Pare-feu réseau ; liste des réseaux autorisés de la sonde (§ 5.6.3)	Ouvrir l'accès HTTPS en IPv6 depuis le réseau d'administration ; ajuster la liste des réseaux autorisés

> **Attention** — Une liste de réseaux autorisés (§ 5.6.3) qui ne contient que des préfixes IPv4 ne laisse pas passer l'administration en IPv6. La liste accepte des préfixes IPv4 et IPv6 en notation CIDR (par exemple `2001:db8:10::/64`) : ajoutez-y les préfixes IPv6 de vos postes d'administration.

5.2.6 Authentification 802.1X

Le contrôle d'accès **802.1X** impose à un équipement de s'authentifier auprès du commutateur avant d'obtenir l'accès au réseau. Le commutateur, appelé « authentificateur », transmet l'authentification à un **serveur RADIUS**, qui l'accepte ou la refuse. Tant que l'authentification n'a pas réussi, le port ne laisse passer que les échanges d'authentification (trames EAPOL, *EAP over LAN*).

La sonde prend en charge 802.1X sur sa prise Ethernet, avec la méthode **EAP-TLS** : elle s'authentifie par un **certificat client**, et vérifie elle-même le certificat du serveur RADIUS. Le client 802.1X de la sonde est `wpa_supplicant`, en mode filaire.

Élément	Prise en charge
EAP-TLS (authentification par certificat)	Oui
Exception par adresse MAC (MAB, *MAC Authentication Bypass*)	Oui, configurée sur le commutateur : la sonde n'a rien à paramétrer
PEAP (identifiant et mot de passe)	Non
Étiquetage VLAN (IEEE 802.1Q) sur la prise de la sonde	Non : la sonde se raccorde à un port d'accès

Paramètres. La section `dot1x` des paramètres contient :

Champ	Description
`enabled`	Active l'authentification 802.1X sur la prise Ethernet
`identity`	Identité présentée au serveur RADIUS
`caRef`	Identifiant (`id`) de l'autorité dans la section `trust` : celle qui a émis le certificat du serveur RADIUS (§ 5.7.3)

Exemple fictif :

```json
{
  "enabled": true,
  "identity": "sonde-paris-01.example.internal",
  "caRef": "ac-radius-example"
}
```

L'**identifiant client** (clé privée et certificat) ne figure pas dans cette section. Il s'obtient de deux manières :

Méthode	Appel	Remarque
Génération de la clé et de la demande de certificat (CSR) sur la sonde	`POST /api/v1/system/dot1x/csr`	**Recommandée** : la clé privée ne quitte jamais la sonde
Import d'un fichier PKCS#12 (clé et certificat)	`PUT /api/v1/system/dot1x/credential`	Écriture seule : l'identifiant importé ne peut pas être relu

Ces opérations sont réservées au rôle `admin` et enregistrées dans le journal d'audit.

> **Information** — Les trames EAPOL circulent uniquement entre la sonde et le commutateur, au niveau de la liaison Ethernet : elles ne nécessitent aucune ouverture de flux IP. Les échanges RADIUS ont lieu entre le commutateur et le serveur RADIUS, sans passer par la sonde.

Choisir une voie de mise en œuvre. Un port contrôlé par 802.1X n'offre aucun accès au réseau avant l'authentification : la sonde doit donc disposer de son identifiant avant de pouvoir être jointe. Deux voies sont possibles.

Voie	Principe	À privilégier lorsque
PKCS#12 — Provisionnement	L'identifiant (fichier PKCS#12 et son mot de passe) et le certificat de l'AC du serveur RADIUS sont déposés sur la microSD, avec la section `dot1x` du fichier de provisionnement. La sonde s'authentifie dès son premier démarrage, avant tout accès au réseau	Aucun port non contrôlé ni exception MAB n'est disponible, même temporairement
CSR — Activation après la mise en service	La sonde est mise en service sur un port non contrôlé ou autorisé par MAB, puis 802.1X est activé par l'interface ou l'API, avec une clé générée sur la sonde	Dans les autres cas : c'est la voie recommandée, car la clé privée ne quitte jamais la sonde

Procédure — voie PKCS#12 (provisionnement).

Objectif : obtenir l'accès à un port contrôlé par 802.1X dès le premier démarrage.

Prérequis : prérequis du § 4.3.2 ; fichier PKCS#12 contenant la clé privée et le certificat client de la sonde, émis par votre IGC, et son mot de passe ; certificat de l'AC du serveur RADIUS au format PEM ; identité attendue par le serveur RADIUS.

Étapes :

1. Copiez le fichier PKCS#12 et le certificat de l'AC à la racine de la partition `SVA-BOOT` de la microSD.

2. Ajoutez au fichier `provision.yaml` la section `dot1x` (champs détaillés au § 4.3.3) :

```yaml
# Section 802.1X du fichier de provisionnement — exemple fictif
dot1x:
  identity: sonde-paris-01.example.internal
  pkcs12File: sonde-paris-01.p12      # fichier déposé à la racine de la partition SVA-BOOT
  caFile: radius-ca.pem               # AC du serveur RADIUS, format PEM
  pkcs12Password: "<mot de passe du fichier PKCS#12>"   # seul secret admis dans ce fichier
```

3. Terminez la préparation de la microSD (§ 4.3.5), installez la sonde et raccordez-la au port contrôlé (chapitre 3).

Résultat attendu : au premier démarrage, la sonde s'authentifie, puis obtient sa configuration réseau. Le fichier PKCS#12, le certificat de l'AC et le mot de passe sont supprimés de la microSD après traitement, comme `provision.yaml`.

Vérification : `provision-result.txt` (§ 4.3.7) ; port autorisé sur le commutateur ; sonde joignable à son adresse.

> **Avertissement** — La suppression du fichier PKCS#12 par la sonde ne vaut pas effacement physique de la mémoire flash. Préférez la voie CSR ; si la voie PKCS#12 est indispensable, appliquez les précautions détaillées au chapitre 4 (§ 4.3.5), puis remplacez le certificat dès que possible selon les étapes 3 à 5 de la voie CSR.

> **Avertissement** — Le mot de passe du fichier PKCS#12 est le **seul secret admis** dans le fichier de provisionnement. Entre la préparation de la carte et le premier démarrage, la microSD contient la clé privée de la sonde et ce mot de passe : préparez les fichiers sur un poste de confiance, supprimez-en toute copie, et ne laissez pas la carte sans surveillance (§ 4.3.3).

> **Attention** — L'authentification EAP-TLS vérifie la validité des certificats, ce qui suppose une heure correcte. Or, au premier démarrage sur un port 802.1X, le serveur NTP n'est joignable qu'après l'authentification. Sans pile pour son horloge temps réel, la sonde part de la dernière heure enregistrée ou, à défaut, de la date de construction de l'image. Pour un déploiement 802.1X, équipez le Raspberry Pi 5 de la pile officielle de l'horloge temps réel (§ 5.4). Une pile neuve ne donne l'heure juste qu'après un premier réglage de l'horloge, c'est-à-dire après un démarrage au cours duquel la sonde a accès à un serveur NTP (par exemple sur un port non contrôlé ou autorisé par MAB).

Pré-régler l'horloge avant un premier démarrage sur un port 802.1X. Les chemins suivants restent sous votre contrôle :

Chemin	Principe	Condition
Premier démarrage sur un port non contrôlé	Avec la pile officielle de l'horloge temps réel installée, démarrez une première fois la sonde sur un port sans 802.1X, depuis lequel le flux NTP (UDP 123) est autorisé ; la sonde règle son horloge, qui conserve ensuite l'heure hors tension. Arrêtez-la proprement, puis raccordez-la au port contrôlé	Un port non contrôlé, même temporaire, sur un réseau qui donne accès à un serveur NTP
Exception MAB temporaire	L'équipe réseau autorise provisoirement le port par l'adresse MAC de la sonde (MAB), le temps d'un premier démarrage avec accès NTP, puis retire l'exception	Une politique de sécurité qui admet une exception MAB limitée dans le temps

Si aucun de ces chemins n'est possible, la réussite de l'authentification EAP-TLS au premier démarrage **ne peut pas être garantie** : elle dépend de l'écart entre l'heure de départ de la sonde (dernière heure enregistrée ou date de construction de l'image) et les périodes de validité des certificats, notamment celle du certificat du serveur RADIUS,

que la sonde vérifie. La sonde ne désactive jamais la vérification des périodes de validité TLS pour contourner ce cas. En cas d'échec, la console de l'écran HDMI affiche l'état de l'authentification et permet de distinguer une heure incorrecte des autres causes.

Procédure — voie CSR (activation après la mise en service).

Objectif : basculer une sonde en service vers un port contrôlé par 802.1X, avec une clé générée sur la sonde.

Prérequis :

- sonde mise en service sur un port non contrôlé ou autorisé par MAB (chapitre 4) ;
- compte ou jeton de rôle `admin` ;
- certificat de l'AC du serveur RADIUS au format PEM ;
- accès à votre IGC pour faire signer une demande de certificat client ;
- heure de la sonde synchronisée (§ 5.4) : la validité des certificats en dépend.

Étapes :

1. Importez le certificat de l'AC du serveur RADIUS dans le magasin de confiance de la sonde, section `trust` (§ 5.7.3), et notez l'identifiant (`id`) sous lequel il est enregistré.
2. Renseignez la section `dot1x` **sans l'activer** : `identity` et `caRef`, avec `enabled` à `false`, dans l'interface d'administration ou par `PUT /api/v1/settings/dot1x`, avec l'en-tête `If-Match` (§ 5.2.4). L'identité doit être enregistrée avant la demande de certificat, dont elle constitue le sujet.

   ```json
   {
     "enabled": false,
     "identity": "sonde-paris-01.example.internal",
     "caRef": "ac-radius-example"
   }
   ```

3. Générez la clé et la demande de certificat sur la sonde (`POST /api/v1/system/dot1x/csr`). La clé privée est générée sur la sonde et ne la quitte jamais. Le sujet de la demande reprend l'identité 802.1X (`dot1x.identity`). Le type de clé se choisit dans le corps de la requête : `{"keyType": "ec-p256"}` (par défaut) ou `{"keyType": "rsa-2048"}` pour un serveur RADIUS plus ancien. La réponse contient la demande au format PEM.
4. Faites signer la demande par votre IGC, sous la forme d'un certificat d'authentification client reconnu par votre serveur RADIUS.
5. Importez le certificat signé sur la sonde par `PUT /api/v1/system/dot1x/credential`, au format PEM (certificat et chaîne) : la sonde l'associe à la clé générée lors de la demande. Si votre organisation fournit plutôt un fichier PKCS#12, importez-le par `PUT /api/v1/system/dot1x/credential`.
6. Une fois le certificat installé seulement, activez l'authentification : passez `enabled` à `true` dans la section `dot1x` (interface d'administration, ou `PUT /api/v1/settings/dot1x` avec l'en-tête `If-Match`), en conservant `identity` et `caRef`. Le corps correspond alors à l'exemple fictif ci-dessus.
7. Faites activer 802.1X sur le port de la sonde par l'équipe réseau, ou déplacez la sonde vers le port contrôlé prévu.

Résultat attendu : le commutateur autorise le port après l'authentification de la sonde ; la sonde reste joignable à son adresse.

Vérification : l'indicateur de santé `network` est à l'état `OK` ; le commutateur indique le port comme authentifié ; le journal du serveur RADIUS enregistre l'acceptation ; la métrique `sva.dot1x.certificate.expiry` est publiée (chapitre 7 du guide d'utilisation et de supervision).

Erreurs possibles (deux voies) : en cas d'échec de l'authentification, la sonde effectue de nouvelles tentatives, affiche l'état de l'authentification sur la console HDMI et le signale par l'indicateur de santé `network`. Les causes habituelles sont une identité inconnue du serveur RADIUS, un certificat client non reconnu, expiré ou dépourvu de l'usage

d'authentification client, une AC du serveur RADIUS mal référencée (`caRef`) ou une heure incorrecte. Le diagnostic détaillé figure au chapitre 9 (§ 9.5).

Surveillance de l'expiration. Un certificat client expiré coupe l'accès de la sonde au réseau. La sonde publie la date d'expiration de son certificat client par la métrique `sva.dot1x.certificate.expiry` et émet un avertissement **30 jours** avant l'échéance. Renouvelez le certificat avant cette date, en reprenant les étapes 3 à 5 de la voie CSR. Pendant un renouvellement, l'identifiant en cours reste utilisé jusqu'à l'import du nouveau certificat : la nouvelle clé est conservée à part et ne remplace l'ancienne qu'à ce moment, sans interruption de l'accès au réseau. Intégrez cette échéance à vos alertes (chapitre 7 du guide d'utilisation et de supervision).

Exception par adresse MAC (MAB). Lorsque 802.1X par certificat n'est pas envisageable, l'équipe réseau peut autoriser le port à partir de l'adresse MAC de la sonde. Pour l'offre boîtier complet, cette adresse figure sur l'étiquette du boîtier (§ 3.5.3). Pour l'offre microSD préconfigurée, elle dépend du Raspberry Pi 5 que vous fournissez : relevez-la sur le commutateur (adresse apprise sur le port) ou dans la table du serveur DHCP, lors d'un premier raccordement à un port non contrôlé. Aucun réglage n'est nécessaire sur la sonde.

> **Attention** — Une adresse MAC peut être usurpée par tout équipement raccordé au même port. Réservez MAB à la mise en service ou aux réseaux où votre politique de sécurité l'admet, et limitez les droits réseau associés au port (VLAN de supervision, § 5.10.2).

5.3 Résolution DNS

Le DNS (*Domain Name System*) traduit les noms de domaine en adresses IP. La sonde l'utilise :

- pour joindre les ressources supervisées par leur nom ;
- pour joindre les destinations d'export, les serveurs NTP et le dépôt de mises à jour ;
- dans les contrôles de type `dns`, qui vérifient eux-mêmes le bon fonctionnement de la résolution (chapitre 4 du guide d'utilisation et de supervision).

Recommandations :

1. Configurez **deux serveurs DNS** au moins, pour que la défaillance de l'un n'entraîne pas une cascade de faux incidents.
2. Utilisez les **mêmes serveurs DNS que les utilisateurs** dont vous souhaitez reproduire l'expérience. Une sonde qui résout les noms autrement que les postes utilisateurs peut indiquer `OK` alors que les utilisateurs rencontrent un problème, ou l'inverse.
3. Si votre organisation utilise un DNS différent selon les zones (« split DNS »), vérifiez que les noms internes et externes à superviser sont résolus comme attendu depuis le réseau de la sonde.

> **Information** — Un contrôle de type `dns` peut interroger des serveurs DNS précis, différents de ceux configurés pour la sonde. C'est utile pour superviser individuellement chaque serveur DNS de l'organisation (chapitre 4 du guide d'utilisation et de supervision).

5.4 Synchronisation de l'heure

L'heure exacte est indispensable au bon fonctionnement de la sonde :

Usage	Conséquence d'une heure incorrecte
Horodatage des résultats	Historique incohérent ; corrélation impossible avec les journaux des applications

Usage	Conséquence d'une heure incorrecte
Planification des contrôles par expression cron et fenêtres d'activité	Contrôles exécutés aux mauvais moments
Fenêtres de maintenance des mises à jour (§ 8.4.8)	Activation d'une mise à jour en dehors de la plage prévue
Vérification des certificats TLS	Rejet de certificats valides, ou acceptation de certificats expirés
Vérification de la fraîcheur des mises à jour en ligne (date d'expiration des métadonnées, § 8.4.5)	Refus de métadonnées valides, ou acceptation de métadonnées expirées
Export vers les plateformes d'observabilité	Données rejetées ou mal placées dans le temps
Journal d'audit	Traçabilité compromise

Le Raspberry Pi 5 intègre une horloge temps réel. Sans pile optionnelle, elle ne conserve pas l'heure lorsque la carte est hors tension. La sonde s'appuie donc sur le protocole **NTP** (*Network Time Protocol*) pour obtenir l'heure à chaque démarrage, puis la maintenir. Sur un port soumis à 802.1X, l'accès NTP n'existe qu'après l'authentification EAP-TLS, qui exige elle-même une heure correcte : les chemins de pré-réglage de l'horloge sont décrits au § 5.2.6.

Recommandations :

1. Configurez au moins deux serveurs NTP internes de votre organisation. À défaut de configuration, la sonde utilise les serveurs NTP fournis par DHCP (option 42), sinon une zone fournisseur du *NTP Pool*, indiquée dans les notes de version.
2. Autorisez le flux UDP 123 de la sonde vers ces serveurs (§ 5.6).
3. Vérifiez l'état de synchronisation sur la page d'état de santé après toute modification.

La sonde enregistre et exporte toutes les dates en temps universel coordonné (UTC). Le fuseau horaire configuré sert uniquement à l'affichage et à l'interprétation des **fenêtres de maintenance des mises à jour**, exprimées en heure locale de la sonde (§ 8.4.8). Les expressions cron et les plages d'activité des contrôles ne dépendent pas de ce réglage : elles sont interprétées dans le fuseau indiqué par leur propre planification (propriété `timezone`, UTC par défaut, § 6.2.3 du guide d'utilisation et de supervision).

> **Information** — Une modification du fuseau horaire recalcule les activations de mises à jour déjà planifiées dans une fenêtre de maintenance, dont les bornes sont des heures locales, et les annonce de nouveau. Si, après ce recalcul, le préavis restant devient insuffisant, l'activation est reportée à la fenêtre de maintenance suivante. Une activation manuelle programmée par `scheduledAt` désigne un instant absolu, exprimé en UTC (RFC 3339) : elle reste fixée à cet instant, qui n'est ni recalculé ni reporté. Configurez vos outils de mise en sourdine des alertes dans le même fuseau que la sonde (§ 8.4.10).

> **Attention** — Une sonde dont l'heure n'est pas synchronisée le signale dans ses indicateurs de santé : l'indicateur `clock` reste à l'état `WARNING` jusqu'à la synchronisation. Au démarrage, les contrôles attendent la synchronisation de l'heure pendant 5 minutes au plus, puis s'exécutent même si elle n'est pas obtenue ; leurs vérifications TLS peuvent alors échouer.

5.5 Proxy sortant

De nombreuses organisations imposent un **proxy** pour les flux sortants vers Internet. Un proxy est un serveur intermédiaire qui relaie les requêtes web pour le compte des postes et des serveurs.

La sonde prend en charge un proxy HTTP(S) utilisant la méthode `CONNECT`, avec une authentification Basic facultative, et une **liste d'exclusions** pour les destinations joignables directement.

5.5.1 Quels flux passent par le proxy ?

Flux	Passage par le proxy
Exports vers des plateformes SaaS (Datadog, Dynatrace, Grafana Cloud)	Oui, sauf exclusion
Dépôt de mises à jour de l'éditeur	Oui, sauf exclusion
Contrôles HTTP et API, scénarios navigateur	Oui, sauf exclusion ; c'est souvent le comportement souhaité pour reproduire l'accès des utilisateurs à Internet. Chaque contrôle `http`, `api` ou `browser` peut contourner le proxy global (`"proxy": "none"`), mais pas en définir un autre
Contrôles ICMP, TCP, DNS, bases de données	Non : ces protocoles ne transitent pas par un proxy HTTP
NTP, DNS de la sonde	Non

5.5.2 Configurer la liste d'exclusions

La liste d'exclusions doit contenir toutes les destinations internes joignables directement : domaines internes (sous forme de suffixe, par exemple `.example.internal`), plages d'adresses internes, collecteur OpenTelemetry interne.

Exemple (fichier de provisionnement) :

```yaml
proxy:
  url: http://proxy.example.internal:3128
  noProxy: [".example.internal", "192.0.2.0/24", "198.51.100.0/24"]
```

✓ **Conseil** — Pour superviser une application interne **telle que la voient les utilisateurs**, reproduisez leur chemin réseau. Si les postes utilisateurs passent par le proxy pour joindre cette application, la sonde doit y passer aussi.

5.5.3 Inspection TLS par le proxy

Certains proxys déchiffrent les flux HTTPS pour les inspecter (« inspection TLS »). Ils présentent alors à la sonde des certificats émis par une autorité de certification interne. Pour que la sonde accepte ces certificats, importez cette autorité dans le magasin de confiance de la sonde (§ 5.7.3). Sinon, les contrôles et les exports échouent avec une erreur `tls_error`.

! **Attention** — Si le proxy authentifie ses utilisateurs, créez un compte technique dédié à la sonde (§ 5.8.3). Le mot de passe de ce compte est un secret : ne le placez pas dans le fichier de provisionnement (§ 4.3.3). Enregistrez-le comme secret de la sonde (chapitre 6) ; la configuration du proxy le référence par son nom (propriété `passwordSecret`), sans jamais contenir sa valeur.

5.6 Flux réseau et pare-feu

5.6.1 Matrice des flux

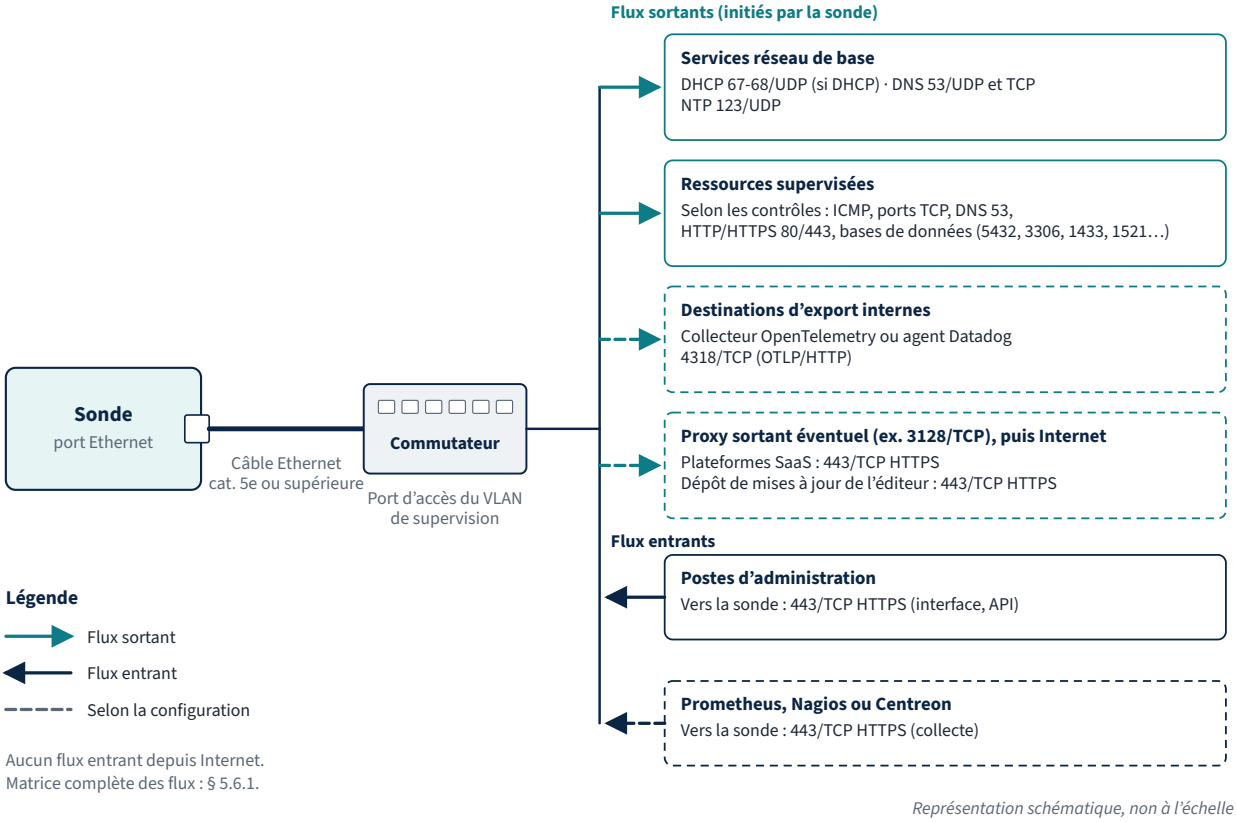


Figure 5-1 — Raccordement réseau de la sonde et principaux flux (le détail figure dans la matrice des flux ci-dessous)

Le tableau suivant recense l'ensemble des flux de la sonde. Transmettez-le à l'équipe chargée des pare-feu. La colonne « Obligatoire » distingue les flux indispensables des flux liés à une fonction facultative.

Sens	Source	Destination	Port / protocole	Usage	Obligatoire
Entrant	Postes d'administration	Sonde	443/TCP (HTTPS)	Interface d'administration, API	Oui
Entrant	Serveur Prometheus	Sonde	443/TCP (HTTPS)	Collecte de `/metrics`	Si Prometheus en mode collecte
Entrant	Serveur Nagios ou Centreon	Sonde	443/TCP (HTTPS)	Plugin `check_sva`	Si Nagios ou Centreon
Entrant	Postes d'administration	Sonde	80/TCP (HTTP)	Redirection permanente vers HTTPS, aucun contenu servi	Non (désactivable)
Entrant	Postes du réseau local	Sonde	5353/UDP (mDNS)	Résolution du nom `.local` de la sonde ; annonce active par défaut	Non (désactivable dans la section `network`)
Entrant	Postes d'administration autorisés	Sonde	22/TCP (SSH)	Maintenance avancée	Non : désactivé par défaut ; activation temporaire, 4 heures par défaut, 72 heures au maximum (§ 5.9.4)

Sens	Source	Destination	Port / protocole	Usage	Obligatoire
Couche 2 (sans flux IP)	Sonde	Commutateur (authentificateur 802.1X)	EAPOL (*EAP over LAN*) : trames Ethernet de type 0x888E, aucun port ni adresse IP	Authentification 802.1X EAP-TLS du port ; le commutateur relaie vers le serveur RADIUS	Si le port est contrôlé par 802.1X (§ 5.2.6)
Entrant et sortant	Sonde	Routeurs et voisins du lien local	ICMPv6 (découverte des voisins, NDP, dont les annonces de routeur utilisées en mode `slaac`)	Adressage et résolution d'adresses IPv6	Si l'IPv6 est activé (§ 5.2.5)
Sortant	Sonde	Serveurs DHCP	67-68/UDP	Adressage	Si DHCP
Sortant	Sonde	Serveurs DNS	53/UDP et 53/TCP	Résolution de noms	Oui
Sortant	Sonde	Serveurs NTP	123/UDP	Synchronisation de l'heure	Oui
Sortant	Sonde	Dépôt de mises à jour de l'éditeur, ou miroir interne	443/TCP (HTTPS)	Mises à jour en ligne : vérification et téléchargement des images signées ; adresse par défaut `https://updates-synovex.incitypark.fr`, inscrite dans le profil éditeur	Si mises à jour en ligne
Sortant	Sonde	Proxy de l'entreprise	Port du proxy (par exemple 3128/TCP)	Relais des flux HTTP(S) sortants (§ 5.5)	Si proxy
Sortant	Sonde	Plateformes SaaS (Datadog, Dynatrace, Grafana Cloud)	443/TCP (HTTPS, OTLP/HTTP)	Export OpenTelemetry	Si configurées
Sortant	Sonde	Collecteur OpenTelemetry ou Agent Datadog du client	4318/TCP (OTLP/HTTP) ou 4317/TCP (OTLP/gRPC), selon le protocole de la destination (§ 2.1.4 du guide d'intégration et d'observabilité)	Export OpenTelemetry	Si configurés
Sortant	Sonde	Proxy inverse placé devant le récepteur OTLP de Prometheus	Port du proxy inverse (par exemple 443/TCP, HTTPS)	Export des métriques en mode envoi (§ 2.5.3 du guide d'intégration et d'observabilité)	Si configuré
Sortant	Sonde	Ressources supervisées	Selon les contrôles : ICMP ou ICMPv6 ; ports TCP des services ; 53 ; 80 et 443 ; SGBD : 5432 (PostgreSQL), 3306 (MySQL/MariaDB), 1433 (SQL Server), 1521 (Oracle)	Contrôles	Oui, selon les contrôles
Sortant	Sonde	Console centrale	443/TCP (HTTPS, authentification mutuelle mTLS)	Gestion multi-sondes	Non : évolution prévue, facultative

Lorsque l'IPv6 est activé, les flux de ce tableau s'entendent en IPv4 et en IPv6, selon la famille d'adresses utilisée.

> **Information** — L'édition est vérifiée hors ligne, à partir du certificat d'édition inscrit sur la carte : aucun flux vers un serveur de licences n'est nécessaire. La sonde n'envoie **aucune donnée à l'éditeur** (pas de télémétrie) : ses seuls échanges avec lui sont la vérification et le téléchargement des mises à jour, si vous les activez.

> **Évolution prévue** — La console centrale facultative (§ 6.14) utilisera une connexion sortante initiée par la sonde, sans ouverture entrante. Aucun flux vers elle n'est nécessaire aujourd'hui.

5.6.2 Règles recommandées

1. **Entrant** : limitez l'accès au port 443 de la sonde aux seuls postes d'administration, serveur Prometheus et serveur Nagios/Centreon. Refusez tout le reste.
2. **Sortant vers les ressources supervisées** : ouvrez uniquement les destinations et ports utilisés par vos contrôles. Une ouverture large (« tout le réseau interne ») facilite la configuration mais accroît l'impact d'une éventuelle compromission de la sonde.
3. **Sortant vers Internet** : limitez-le aux destinations nécessaires (plateformes SaaS, dépôt de mises à jour), de préférence via le proxy.
4. **ICMP** : si vous utilisez des contrôles de type `icmp`, autorisez les requêtes et réponses ICMP *Echo* entre la sonde et les cibles concernées, ainsi que leurs équivalents ICMPv6 pour les cibles jointes en IPv6. Si l'IPv6 est activé, ne filtrez pas l'ICMPv6 de découverte des voisins sur le réseau local de la sonde.
5. Journalisez les flux refusés depuis et vers la sonde : ces journaux sont précieux pour diagnostiquer un contrôle en échec (chapitre 9).

5.6.3 Pare-feu local de la sonde

En complément de vos pare-feu réseau, la sonde dispose d'un pare-feu local (nftables), **actif par défaut**. Il n'autorise en entrée que les ports nécessaires : 443/TCP, 80/TCP (redirection vers HTTPS, § 5.7.1), 5353/UDP (mDNS), et 22/TCP lorsque SSH est activé. Une liste facultative de réseaux autorisés, en notation CIDR (par exemple `192.0.2.0/24`), peut être configurée dans les paramètres de sécurité (section `security`) ; elle s'applique aux ports 443 et 22. Lorsque l'IPv6 est activé, le pare-feu local applique les mêmes règles en IPv6 (§ 5.2.5).

> → **Évolution prévue** — Pour l'édition Enterprise, la spécification prévoit un filtrage des connexions sortantes de l'environnement d'exécution des scénarios, limitant celles-ci aux destinations déclarées par l'administrateur.

5.7 Certificats et protocoles sécurisés

5.7.1 Protocoles utilisés

Échange	Protocole	Protection
Administration, API, `/metrics`	HTTPS	TLS 1.2 minimum, TLS 1.3 privilégié
Export vers les plateformes	HTTPS (OTLP/HTTP) ou OTLP/gRPC	TLS ; HTTP non chiffré accepté uniquement vers un collecteur interne si vous le configurez ainsi
Accès de maintenance	SSH	Chiffré ; authentification par clé publique uniquement, mot de passe interdit
Mises à jour	HTTPS	TLS, et signature de l'image de mise à jour par l'éditeur, vérifiée avant installation (chapitre 8)
Contrôles	Ceux des ressources supervisées	La sonde vérifie les certificats des cibles HTTPS par défaut

Le port HTTP 80 sert uniquement à une redirection permanente vers HTTPS : aucun contenu n'y est servi. Cette redirection peut être désactivée.

5.7.2 Remplacer le certificat de la sonde

Le certificat autosigné généré au premier démarrage protège les échanges, mais n'est reconnu par aucun navigateur ni outil. Il impose une vérification manuelle de l'empreinte (§ 4.4.4) et la diffusion du certificat aux outils qui interrogent la sonde. Il est donc recommandé de le remplacer par un certificat émis par l'**autorité de certification (AC) interne** de votre organisation.

Objectif : faire reconnaître la sonde par les navigateurs et outils de votre parc.

Prérequis :

- nom DNS de la sonde enregistré (exemple : `sonde-paris-01.example.internal`) ;
- accès à l'AC interne de votre organisation ;
- compte ou jeton de rôle `admin`.

Étapes :

1. Obtenez un certificat serveur pour le nom DNS de la sonde, en incluant ce nom dans l'extension *Subject Alternative Name*. Deux modes sont proposés : la **génération de la clé et de la demande de certificat (CSR) sur la sonde**, recommandée car la clé privée ne quitte jamais l'appareil, ou l'import d'une clé privée générée ailleurs.
2. Importez le certificat, la chaîne de certification et, le cas échéant, la clé privée, depuis l'interface ou par l'API. Si la demande a été générée sur la sonde (`POST /api/v1/system/certificate/csr`), seul le certificat signé et sa chaîne sont à importer. L'import se fait par `PUT /api/v1/system/certificate`. Formats acceptés : PEM (certificat, chaîne et clé), ou PKCS#12 protégé par un mot de passe.
3. Reconnectez-vous à l'interface en utilisant le nom DNS.

Résultat attendu : le navigateur affiche une connexion sécurisée sans avertissement.

Vérification : `curl https://sonde-paris-01.example.internal/health` réussit sans option `--cacert` sur un poste qui fait confiance à votre AC interne.

> ! **Attention** — Anticipez l'expiration du certificat : une sonde dont le certificat a expiré reste fonctionnelle, mais les outils qui la collectent (Prometheus, Nagios) échoueront. Planifiez son renouvellement dans vos processus habituels.

5.7.3 Faire confiance à une AC interne pour les contrôles et les exports

Indépendamment de son propre certificat, la sonde doit pouvoir **vérifier** les certificats des services qu'elle contacte : applications supervisées, collecteur OpenTelemetry interne, proxy avec inspection TLS. Si ces certificats sont émis par une AC interne, importez le certificat de cette AC, au format PEM, dans le magasin de confiance de la sonde, géré dans la section `trust` des paramètres (§ 6.9). Ce magasin s'ajoute au magasin système et s'applique aux contrôles `http`, `api`, `tcp` (avec TLS) et `browser`, ainsi qu'aux exports.

Les AC importées s'appliquent par défaut à tous les contrôles concernés. Un contrôle HTTP peut en outre restreindre sa confiance à une seule AC importée (propriété `tls.caRef`, chapitre 4 du guide d'utilisation et de supervision).

> ! **Avertissement** — La désactivation de la vérification des certificats (`tls.verify: false` dans un contrôle, `insecureSkipVerify` dans une destination d'export) doit rester exceptionnelle, temporaire et documentée. Elle supprime la protection contre l'interception des échanges, y compris des identifiants des comptes de test.

5.8 Identifiants, secrets et comptes techniques

5.8.1 Ce que la sonde doit connaître

Pour superviser vos applications en profondeur, la sonde a besoin d'identifiants : comptes de test pour se connecter aux applications web, comptes de lecture pour interroger les bases de données, jetons pour appeler les API, clés d'API des plateformes d'observabilité. Ces informations sont des **secrets**.

La sonde protège les secrets de la manière suivante :

Mesure	Effet
Stockage chiffré	Les secrets sont chiffrés sur la microSD
Écriture seule	Un secret enregistré ne peut jamais être relu, ni par l'interface ni par l'API ; il peut seulement être remplacé ou supprimé
Déclaration par contrôle	Chaque contrôle déclare les secrets qu'il utilise ; seuls ceux-ci lui sont transmis lors de l'exécution
Référencement	Les configurations ne contiennent jamais la valeur d'un secret, mais une référence de la forme `${secret:NOM}`
Masquage	Les valeurs des secrets sont masquées dans les journaux et les messages d'erreur
Exclusion des exports	Les exports de configuration excluent les secrets, ou les chiffrent par une phrase de passe

La procédure de création, de rotation et de suppression des secrets est décrite au chapitre 6.

> **Attention** — Sans composant matériel de sécurité, la clé qui protège les secrets réside sur la même microSD que les secrets eux-mêmes. Le chiffrement protège contre la copie de la base de données, mais **pas contre le vol de la microSD entière**. La sécurité physique de la sonde (§ 5.11) et le moindre privilège des comptes (§ 5.8.2) restent donc essentiels.

> **Attention** — Les captures d'écran produites en cas d'échec d'un scénario (chapitre 7 du guide d'utilisation et de supervision) peuvent afficher des données présentes à l'écran. Les champs de mot de passe sont masqués par le navigateur, mais une page peut réafficher une donnée sensible. Utilisez des comptes de test sans données réelles.

5.8.2 Principe du moindre privilège

Le **principe du moindre privilège** consiste à n'accorder à un compte que les droits strictement nécessaires à sa fonction. Appliqué à la sonde, il limite les conséquences d'une fuite d'identifiants ou d'une erreur de configuration.

Usage	Recommandation
Comptes de test applicatifs (scénarios navigateur, API)	Comptes **dédiés à la supervision**, nominativement identifiables (par exemple `test-supervision@example.com`), sans droits d'administration, sans accès à des données réelles, sans moyen de paiement réel
Comptes de bases de données	Compte **en lecture seule**, limité aux tables ou vues nécessaires ; idéalement, une vue dédiée qui expose uniquement les indicateurs à contrôler
Jetons d'API des applications	Portée minimale (lecture seule), durée de validité limitée
Clés d'API des plateformes d'observabilité	Clés limitées à l'**ingestion** des données (par exemple, pour Dynatrace, un jeton disposant uniquement des droits d'ingestion des signaux exportés)

Usage	Recommandation
Comptes d'accès à la sonde	Rôle minimal adapté à chaque usage (§ 5.9.1)

Exemple de compte en lecture seule pour un contrôle de base de données PostgreSQL (fictif) :

```sql
-- Compte de supervision en lecture seule, limité à une vue dédiée (exemple PostgreSQL)
CREATE ROLE supervision_ro LOGIN PASSWORD '********';
CREATE VIEW reporting.v_supervision_commandes AS
  SELECT count(*) AS nb_commandes_jour
  FROM ventes.commandes
  WHERE created_at >= current_date;
GRANT USAGE ON SCHEMA reporting TO supervision_ro;
GRANT SELECT ON reporting.v_supervision_commandes TO supervision_ro;
```

Information — Exposer une vue plutôt que les tables évite de donner à la sonde l'accès aux données détaillées : elle ne lit que l'indicateur agrégé dont elle a besoin. Les contrôles de bases de données sont décrits au chapitre 5 du guide d'utilisation et de supervision.

5.8.3 Comptes techniques dédiés

Créez des comptes techniques distincts pour chaque usage et chaque sonde lorsque c'est possible :

- un compte par application supervisée, plutôt qu'un compte partagé entre toutes ;
- un compte de proxy dédié à la sonde ;
- une clé d'API d'ingestion par plateforme et par site.

Vous pourrez ainsi révoquer un accès sans interrompre les autres, et identifier précisément l'origine des connexions dans les journaux de vos applications.

Conseil — Informez les équipes applicatives de l'existence des comptes de test de la sonde. Elles éviteront de les désactiver lors d'une revue des comptes, et pourront exclure leur activité des statistiques métier.

5.8.4 Rotation des secrets

Renouvelez les secrets selon la politique de votre organisation, et immédiatement en cas de suspicion de compromission. La sonde conserve la date de dernière rotation de chaque secret (chapitre 6). Pour une rotation sans interruption de la supervision :

1. Créez le nouveau mot de passe dans l'application cible (ou un second jeton).
2. Remplacez la valeur du secret dans la sonde.
3. Déclenchez une exécution immédiate des contrôles concernés et vérifiez leur état.
4. Désactivez l'ancien mot de passe ou jeton dans l'application cible.

5.9 Sécurisation des accès administrateur

5.9.1 Comptes et rôles

L'accès à la sonde est contrôlé par des **rôles**. Chaque compte utilisateur et chaque jeton d'API reçoit un rôle.

Rôle	Droits	Usage type
`admin`	Tous les droits : utilisateurs, jetons, secrets, réseau, mises à jour, scripts et plugins personnalisés	Administrateurs de la sonde (2 personnes au moins, comptes nominatifs)
`operator`	Création et modification des contrôles déclaratifs et des plans, activation, désactivation, exécution immédiate, consultation. Ni code exécutable ; référence d'un secret existant possible, sans le lire, le créer ni le modifier	Équipe d'exploitation
`viewer`	Lecture seule des états, résultats et artefacts	Équipes applicatives, support
`metrics`	Lecture de `/metrics` et de l'état des contrôles uniquement	Serveur Prometheus, plugin Nagios/Centreon

Recommandations :

1. Créez des **comptes nominatifs**, un par personne. N'utilisez pas de compte partagé.
2. Limitez le nombre d'administrateurs, en en conservant au moins deux pour éviter une perte d'accès.
3. Le téléversement de scripts et de plugins personnalisés est réservé au rôle `admin`, car il revient à exécuter du code sur le réseau où la sonde est installée.
4. Revoyez périodiquement la liste des comptes et des jetons.

La gestion des comptes est décrite au chapitre 6. Les comptes sont **locaux** à la sonde : l'authentification par l'annuaire d'entreprise (LDAP, Active Directory) ou par un service d'authentification unique n'est pas disponible.

> → **Évolution prévue** — L'authentification par OpenID Connect est prévue dans une version ultérieure (§ 6.4.2).

5.9.2 Jetons d'API

Les outils (Prometheus, Nagios, scripts d'automatisation) s'authentifient par **jeton d'API**. Bonnes pratiques :

- un jeton par outil et par usage, avec le rôle minimal (`metrics` pour Prometheus et Nagios) ;
- une date d'expiration ;
- un stockage dans le coffre-fort ou le gestionnaire de secrets de l'outil, jamais dans un dépôt de code ;
- une révocation immédiate en cas de doute.

Le jeton n'est affiché qu'une fois, à sa création ; la sonde n'en conserve qu'une empreinte.

5.9.3 Protection de l'interface d'administration

Mesure	Description
HTTPS uniquement	Aucune donnée d'authentification ne transite en clair
Protection contre les tentatives répétées	Après 5 échecs de connexion consécutifs, blocage pendant 15 minutes, par compte et par adresse source
Sessions sécurisées	Cookies de session protégés ; expiration après 30 minutes d'inactivité, et en tout état de cause après 12 heures

Mesure	Description
Restriction réseau	Filtrage par pare-feu (§ 5.6.2) et liste d'adresses autorisées (§ 5.6.3)
Poste d'administration	Utiliser un poste maîtrisé, à jour, de préférence un poste d'administration dédié

5.9.4 Accès SSH

L'accès SSH (*Secure Shell*) donne un accès en ligne de commande au système de la sonde. Il n'est **pas nécessaire** à l'exploitation courante : toutes les opérations prévues sont disponibles dans l'interface d'administration et par l'API. Il est donc **désactivé par défaut**.

Il peut être activé temporairement pour un diagnostic avancé, par exemple à la demande du support. L'éditeur ne dispose d'**aucun accès permanent** à la sonde et ne peut pas ouvrir cet accès lui-même : seul un administrateur de la sonde (rôle `admin`) peut l'activer, et toujours pour une **durée limitée**.

Objectif : ouvrir un accès SSH temporaire et maîtrisé.

Prérequis : compte de rôle `admin` ; paire de clés SSH de l'intervenant ; règle de pare-feu autorisant le port 22/TCP depuis le seul poste de l'intervenant ; accord du RSSI selon votre politique.

Étapes :

1. Activez l'accès SSH dans les paramètres de la sonde, section `ssh` : rubrique « Accès de maintenance SSH » de l'interface d'administration, ou `PUT /api/v1/settings/ssh` (champs `enabled`, `enabledUntil` et `authorizedKeys`, avec l'en-tête `If-Match`, § 5.2.4). La date de fin `enabledUntil` est **obligatoire** à l'activation : la durée est de 4 heures par défaut et de 72 heures au maximum.
2. Déposez la clé publique de l'intervenant. L'authentification par mot de passe est interdite : seule l'authentification par clé publique est acceptée. Compte système utilisé : un compte dédié, non privilégié, dont toute élévation de droits est journalisée ; nom du compte : `sva-maint`.
3. Réalisez l'intervention.
4. **Désactivez SSH** dès la fin de l'intervention, sans attendre l'échéance, et retirez la clé publique.
5. Supprimez la règle de pare-feu temporaire.

Exemple de section `ssh` pour une activation temporaire (valeurs fictives) :

```json
{
  "enabled": true,
  "enabledUntil": "2025-11-20T18:00:00Z",
  "authorizedKeys": [
    "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIExempleFictifDeCleIntervenant intervenant@example.internal"
  ]
}
```

Résultat attendu : SSH est accessible avec la clé déposée, depuis le seul poste autorisé, jusqu'à la date `enabledUntil`. À cette échéance, la sonde **désactive automatiquement** SSH et **ferme les sessions en cours**.

Vérification : le journal d'audit contient l'activation de SSH, chaque connexion SSH et la désactivation, manuelle ou automatique.

Erreurs possibles : connexion refusée si la clé présentée ne figure pas dans `authorizedKeys`, si le pare-feu réseau ou la liste des réseaux autorisés (§ 5.6.3) bloque le port 22, si la date `enabledUntil` est dépassée ou si SSH a été verrouillé définitivement (ci-dessous). Le diagnostic par SSH est traité au chapitre 9 (§ 9.2.4).

> **Avertissement** — Une intervention en ligne de commande peut modifier le système en dehors des mécanismes de la sonde et compromettre sa stabilité, sa sécurité ou ses mises à jour. N'effectuez que les opérations documentées par l'éditeur ou demandées par le support.

Verrouillage définitif de SSH. Si votre politique de sécurité interdit tout accès en ligne de commande, vous pouvez verrouiller définitivement SSH. Une fois verrouillé, SSH ne peut plus être activé, ni par l'interface ni par l'API, jusqu'à une réinitialisation usine (§ 8.10).

Objectif : supprimer durablement toute possibilité d'activer SSH sur la sonde.

Prérequis : compte ou jeton de rôle `admin` ; décision validée par le RSSI ; nom d'hôte exact de la sonde.

Étapes :

1. Dès la mise en service, ajoutez au fichier de provisionnement la ligne `locked: true` dans la section `ssh` (§ 4.3.3) ; ou, sur une sonde en service, appelez `POST /api/v1/settings/ssh/lock` en confirmant l'opération par le nom d'hôte de la sonde :

   ```bash
   # Verrouillage définitif de SSH (rôle admin). Le champ confirm doit contenir
   # le nom d'hôte exact de la sonde ; sinon la demande est refusée.
   # Préparation du poste (SONDE, CA, fonction sapi) : § 6.3.3
   sapi -X POST -H 'Content-Type: application/json' \
        --data '{"confirm": "sonde-paris-01"}' \
        "$SONDE/api/v1/settings/ssh/lock"
   ```

2. Vérifiez le résultat (ci-dessous).

Résultat attendu : la propriété `locked` de la section `ssh` vaut `true` ; toute demande d'activation de SSH est refusée.

Vérification : `GET /api/v1/settings/ssh` ; le journal d'audit enregistre le verrouillage.

Erreurs possibles : demande refusée si le nom d'hôte transmis dans `confirm` ne correspond pas exactement à celui de la sonde, ou si le compte n'a pas le rôle `admin`.

> **Avertissement** — Le verrouillage de SSH est **irréversible** : seule une réinitialisation usine, qui efface la configuration, permet de le lever. Une fois SSH verrouillé, le support ne pourra plus intervenir sur la sonde par SSH ; les diagnostics passeront uniquement par l'interface, l'API et l'archive de diagnostic (chapitre 9). La récupération du compte administrateur par code de récupération reste possible (chapitre 8).

5.10 Segmentation et positionnement réseau

5.10.1 Où placer la sonde ?

La sonde mesure ce qu'elle « voit » depuis son point de raccordement. Son emplacement dépend de la question à laquelle elle doit répondre.

Objectif	Positionnement recommandé
Mesurer l'expérience des utilisateurs d'un site	Réseau des postes utilisateurs de ce site, mêmes DNS, même proxy
Superviser des services internes au centre de données	Réseau d'administration ou de supervision du centre de données

Objectif	Positionnement recommandé
Comparer la disponibilité depuis plusieurs sites	Une sonde par site, chacune avec un attribut `site` distinct (chapitre 2 du guide d'intégration et d'observabilité)
Vérifier l'accès à une application exposée sur Internet	Réseau disposant de l'accès Internet standard de l'organisation

✓ **Conseil** — Le déploiement de deux sondes sur des sites différents fournit des indices pour localiser une panne : un échec vu depuis les deux sites oriente vers l'application ou vers un composant commun, un échec vu depuis un seul vers ce qui est propre à ce site. Ces indices ne suffisent pas à conclure. Un composant réseau commun peut affecter les deux sites, et une réponse qui dépend de la région, de l'identité, du répartiteur de charge ou du DNS peut n'affecter qu'un seul point d'observation. Comparez les chemins, les cibles, les résolutions DNS, les politiques appliquées et les résultats détaillés des deux sondes avant d'attribuer l'origine à l'application ou au réseau (§ 1.2.1).

5.10.2 VLAN de supervision

Lorsque votre réseau est segmenté, il est recommandé de placer la sonde dans un **VLAN** (réseau local virtuel) dédié à la supervision, ou dans le VLAN d'administration existant. Les échanges avec les ressources supervisées sont alors contrôlés par les règles de filtrage entre VLAN (§ 5.6.2).

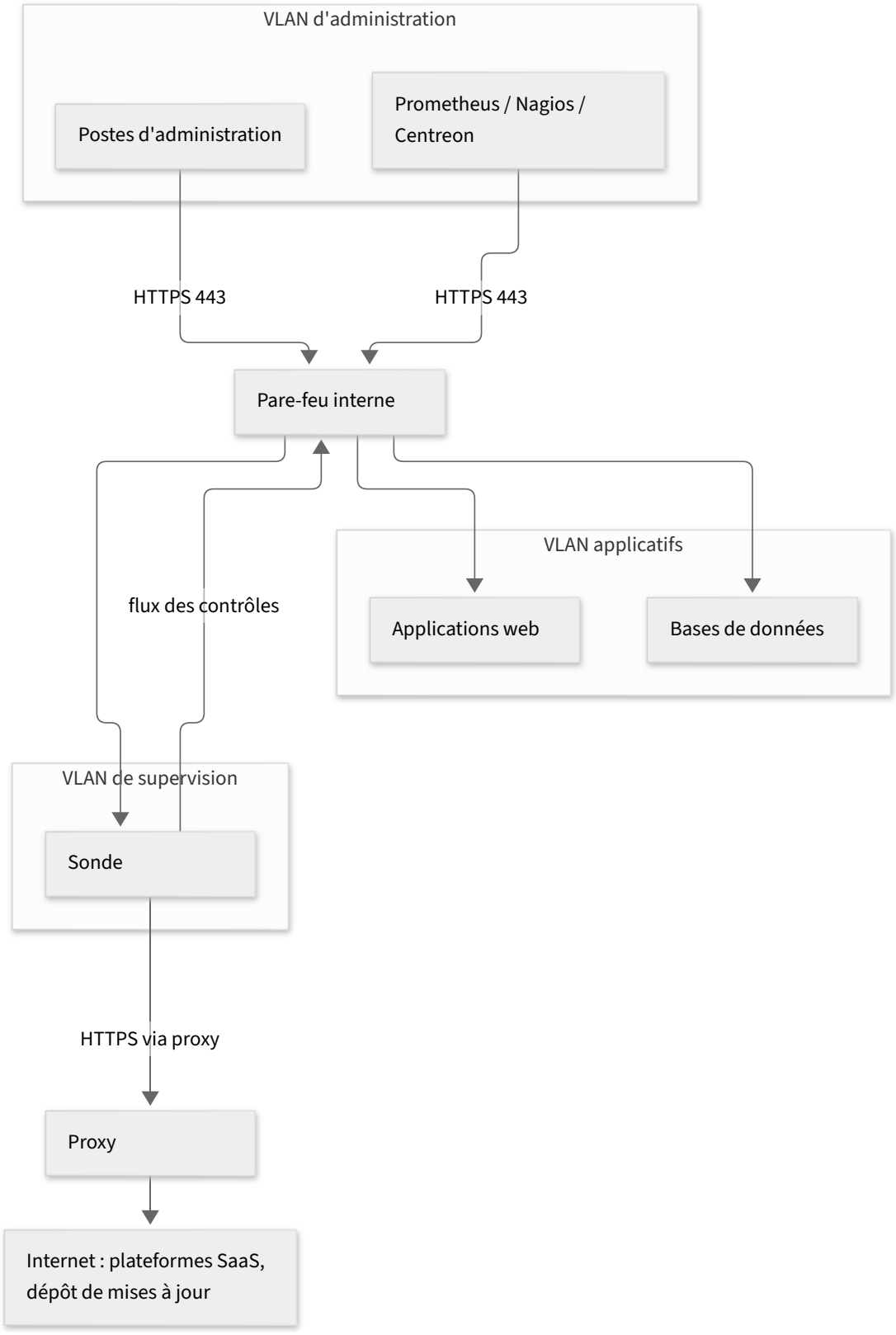


Schéma 5-2 — Sonde placée dans un VLAN de supervision

Ce découpage offre trois avantages :

- les flux d'administration et de collecte sont limités aux seuls outils autorisés ;
- les flux des contrôles sont explicitement autorisés, cible par cible ;
- une compromission éventuelle de la sonde ne donne pas un accès direct à l'ensemble du réseau.

> **Attention** — Le cloisonnement réseau modifie le chemin des flux. Vérifiez que la sonde, placée dans un VLAN dédié, mesure toujours l'expérience que vous souhaitez observer (§ 5.10.1). Si nécessaire, raccordez une seconde sonde dans le réseau des utilisateurs.

5.11 Sécurité physique

La microSD contient le système, la configuration et les secrets chiffrés de la sonde. Une personne ayant un accès physique à la sonde peut retirer la carte et en faire une copie.

Recommandations :

1. Installez la sonde dans un local ou une baie à accès contrôlé.
2. Ne laissez pas d'écran ni de clavier raccordé en permanence.
3. Tenez un inventaire des sondes (numéro de série, emplacement, adresse MAC).
4. En cas de vol ou de perte d'une sonde ou d'une microSD : changez sans délai **tous les secrets** que la sonde connaissait (comptes de test, comptes de bases de données, clés d'API d'ingestion), révoquez les jetons d'API et, s'il a été émis par votre AC interne, le certificat de la sonde ; révoquez le certificat client 802.1X de la sonde auprès de votre AC et retirez son exception MAB éventuelle ; puis retirez ses règles de pare-feu.
5. Avant de mettre au rebut ou de retourner une microSD, effacez-la de manière sécurisée ou détruisez-la (chapitre 8).

5.12 Journalisation et audit

5.12.1 Journal d'audit

La sonde tient un **journal d'audit** des opérations d'administration. Chaque événement comporte l'horodatage, l'auteur (compte ou jeton), l'adresse source, l'action, la ressource concernée et le résultat. Les modifications de configuration y figurent sans la valeur des secrets.

Événements journalisés :

- connexions réussies et échouées ;
- création, modification et suppression de contrôles, plans d'exécution, destinations d'export, comptes et jetons ;
- création, rotation et suppression de secrets (sans leur valeur) ;
- téléversement de scripts et de plugins ;
- modifications des paramètres réseau et de sécurité, activation, désactivation et verrouillage de SSH, connexions SSH ;
- gestion de l'identifiant client 802.1X ;
- mises à jour, réinitialisations, imports et exports de configuration.

Le journal est consultable par les administrateurs dans l'interface et par l'API (`GET /api/v1/audit-events`). Durée de conservation par défaut : 365 jours.

5.12.2 Centralisation dans le SIEM

Pour une conservation conforme à votre politique et une corrélation avec les autres événements de sécurité, transmettez les événements d'audit à votre SIEM (*Security Information and Event Management*). La sonde peut exporter ses journaux, y compris les événements d'audit, au format OpenTelemetry (chapitre 2 du guide d'intégration et d'observabilité). L'export des événements d'audit, sous forme de logs OTLP, est facultatif et désactivé par défaut ; il s'active destination par destination (`logs.audit: true`). Pour une extraction ponctuelle, `GET /api/v1/audit-events` accepte les filtres `from`, `to`, `actor` et `action`.

5.12.3 Journaux système

Les journaux système de la sonde sont conservés **en mémoire** par défaut, afin de limiter l'usure de la microSD : ils sont perdus au redémarrage. Pour un diagnostic portant sur une période incluant un redémarrage, la conservation sur disque peut être activée temporairement, par le paramètre `logging.persistentUntil`, qui fixe sa date de fin ; elle est désactivée automatiquement au bout de 72 heures au plus. Le diagnostic est traité au chapitre 9.

5.13 Recommandations aux RSSI

Le tableau suivant synthétise les points à valider avec la fonction sécurité avant la mise en production.

Domaine	Recommandation	Référence
Exposition	Aucun accès depuis Internet ; port 443 de la sonde ouvert aux seuls outils et postes autorisés	§ 5.1, § 5.6
Segmentation	Sonde dans un VLAN de supervision ou d'administration ; flux sortants limités aux cibles	§ 5.10
Contrôle d'accès au réseau	802.1X par certificat (EAP-TLS), clé générée sur la sonde ; MAB limité aux cas admis ; suivi de l'expiration du certificat client	§ 5.2.6
Certificats	Certificat de la sonde émis par l'AC interne ; vérification des certificats des cibles conservée	§ 5.7
Comptes	Comptes nominatifs ; rôles minimaux ; deux administrateurs au moins ; revue périodique	§ 5.9.1
Jetons	Un jeton par outil, rôle `metrics` pour la collecte, expiration, stockage en coffre-fort	§ 5.9.2
SSH	Désactivé ; activation temporaire (72 heures au plus), tracée et justifiée ; verrouillage définitif si la politique de sécurité l'exige	§ 5.9.4
Comptes de test	Dédiés, sans privilèges, sans données réelles ni moyens de paiement réels	§ 5.8.2
Bases de données	Comptes en lecture seule, vues dédiées	§ 5.8.2
Secrets	Rotation planifiée ; procédure de révocation en cas de perte de la sonde	§ 5.8.4, § 5.11
Scripts	Téléversement réservé aux administrateurs ; relecture des scripts avant mise en service	§ 5.9.1, chapitre 6 du guide de développement des scénarios
Traçabilité	Journal d'audit transmis au SIEM	§ 5.12
Mises à jour	Mode automatique ou processus manuel régulier ; suivi des correctifs de sécurité	Chapitre 8
Physique	Local à accès contrôlé ; inventaire ; procédure de mise au rebut	§ 5.11

Domaine	Recommandation	Référence
Données personnelles	Captures d'écran limitées aux échecs, rétention courte, comptes de test sans données réelles	§ 5.8.1

Information — Les caractéristiques de sécurité détaillées du produit (isolation de l'exécution, chiffrement, signature des mises à jour) sont décrites au chapitre 1. Pour toute question relative à la sécurité du produit, contactez le support de l'éditeur (chapitre 10).

Chapitre 6 — Administration de la sonde

Ce chapitre décrit comment administrer la sonde au quotidien :

- les deux moyens d'administration : l'interface web et l'API REST ;
- la gestion des comptes, des jetons d'API et des secrets ;
- la création et le pilotage des contrôles ;
- les paramètres, le journal d'audit et la sauvegarde de la configuration ;
- l'automatisation de ces opérations.

Il suppose que la mise en service décrite au chapitre 4 est terminée : un compte administrateur existe, et la sonde est joignable en HTTPS depuis votre poste.

Les noms d'hôtes, adresses et identifiants des exemples sont fictifs. La sonde y est désignée par `sonde-paris-01.example.internal`, et l'adresse `192.0.2.50` est réservée à la documentation.

> **Information** — L'interface d'administration et l'API sont décrites ici par leurs fonctions. Les écrans de l'interface ne sont pas reproduits en détail : chaque opération est aussi décrite par la requête REST correspondante.

6.1 Moyens d'administration

6.1.1 Vue d'ensemble

La sonde s'administre **localement**, depuis le réseau où elle est installée, sans dépendre d'aucun service extérieur. Deux moyens sont disponibles, et ils offrent les mêmes possibilités.

Moyen	Adresse	Destiné à	Authentification
Interface d'administration	`https://<adresse-de-la-sonde>/`	Mise en service, consultation, opérations courantes	Identifiant et mot de passe d'un compte local
API REST	`https://<adresse-de-la-sonde>/api/v1`	Automatisation, intégration à vos outils, administration en masse	Jeton d'API

L'interface d'administration s'appuie elle-même exclusivement sur l'API REST. Toute opération réalisable dans l'interface l'est donc aussi par l'API, avec les mêmes règles de droits et de validation.

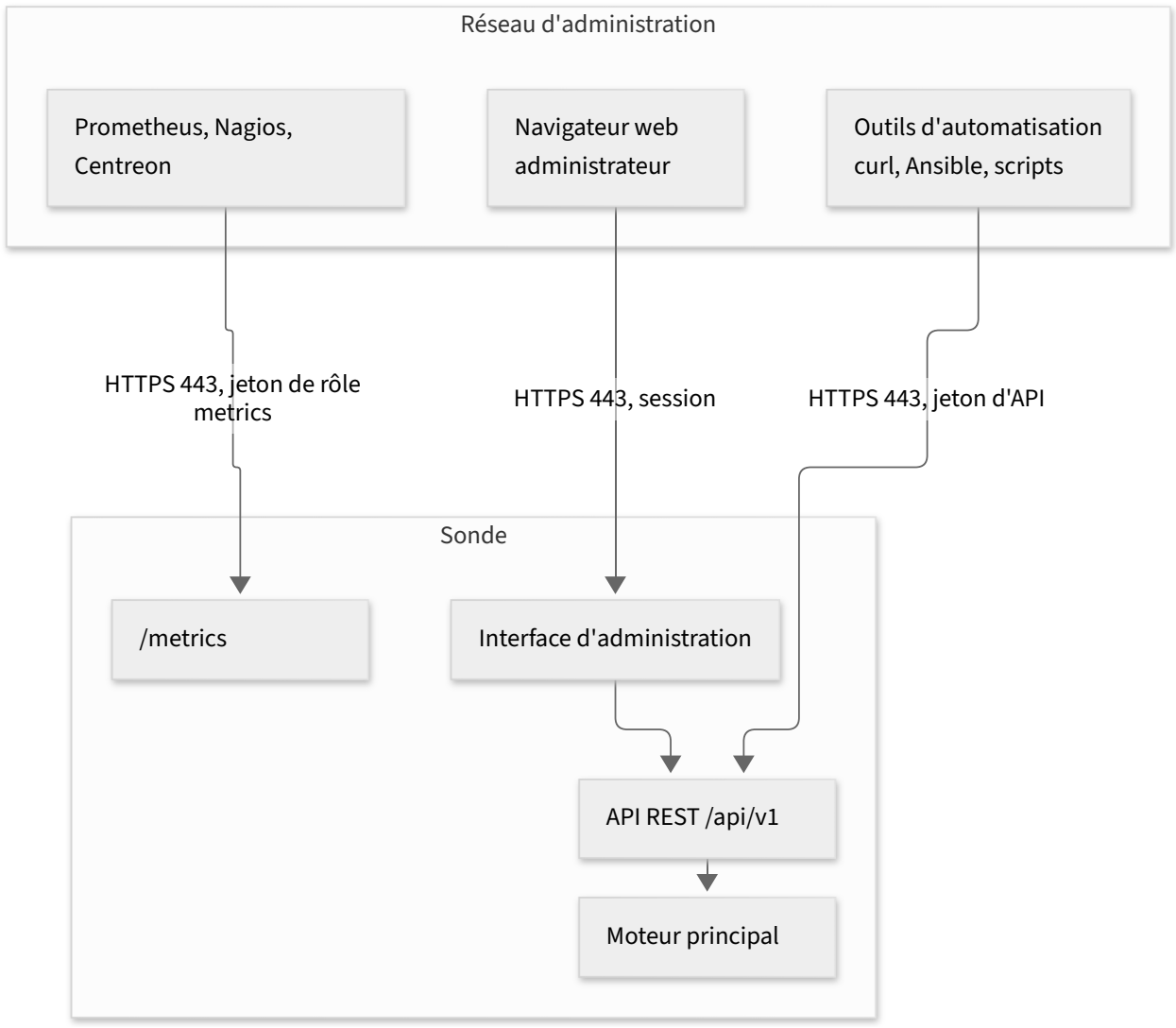


Schéma 6-1 — Interface d'administration et API REST

> **Avertissement** — L'interface d'administration et l'API sont conçues pour être utilisées depuis le réseau où la sonde est installée. N'exposez jamais la sonde directement sur Internet, par exemple via une redirection de port. L'administration à distance doit passer par un moyen d'accès sécurisé à ce réseau (accès d'administration, bastion, VPN), celui de votre organisation ou celui convenu avec l'exploitant du réseau d'accueil. Le chapitre 5 précise les flux à autoriser.

6.1.2 Accès SSH

L'accès SSH au système de la sonde est **désactivé par défaut**. Il n'est pas nécessaire à l'administration courante, qui se fait entièrement par l'interface et l'API. Un administrateur peut l'activer pour une opération de maintenance avancée ou à la demande du support (chapitre 5). Désactivez-le dès la fin de l'intervention.

L'activation est toujours **temporaire** : elle exige une date de fin (`enabledUntil`), fixée à 4 heures par défaut et à 72 heures au maximum. À l'échéance, SSH se désactive automatiquement et les sessions ouvertes sont fermées. Seul un compte `admin` de la sonde peut l'activer ; l'éditeur ne dispose d'aucun accès permanent. Activation, connexions et

désactivation sont enregistrées dans le journal d'audit (§ 6.10). Si votre politique de sécurité l'exige, SSH peut aussi être **verrouillé définitivement** (§ 6.9.3).

6.2 Interface d'administration

6.2.1 Accès

Objectif : ouvrir une session sur l'interface d'administration.

Prérequis : la sonde est mise en service (chapitre 4) ; vous disposez d'un compte et de l'empreinte du certificat de la sonde, ou le certificat de la sonde a été remplacé par un certificat de votre autorité de certification (chapitre 5).

Étapes :

1. Dans votre navigateur, saisissez l'adresse `https://<adresse-de-la-sonde>/`, par exemple `https://sonde-paris-01.example.internal/`.
2. Si la sonde utilise encore son certificat autosigné, le navigateur affiche un avertissement de sécurité. Consultez le certificat présenté et comparez son empreinte SHA-256 avec celle notée lors de la mise en service. Poursuivez uniquement si elles sont identiques.
3. Saisissez votre identifiant et votre mot de passe.

Résultat attendu : le tableau de bord des états des contrôles s'affiche.

> ! **Avertissement** — Un avertissement de certificat dont l'empreinte ne correspond pas à celle de la sonde peut signaler une interception du trafic. Dans ce cas, ne saisissez pas vos identifiants et alertez votre équipe sécurité. Pour supprimer durablement l'avertissement, installez sur la sonde un certificat émis par l'autorité de certification de l'entreprise (chapitre 5).

6.2.2 Fonctions disponibles

Domaine	Fonctions	Rôle minimal
Tableau de bord	État courant de tous les contrôles, filtres par type, état et étiquette	`viewer`
Résultats	Historique des exécutions, détail d'une exécution (étapes, erreur, mesures), captures d'écran et journaux	`viewer`
Contrôles	Création, modification, suppression, activation, désactivation, exécution immédiate et exécution d'essai	`operator`. Pour un contrôle scripté ou à plugin personnalisé : création, remplacement complet (`PUT`) et tout changement de code (`browser.mode`, `browser.scriptRef`, plugin) réservés à `admin` ; activation, désactivation, exécutions, réglages par `PATCH` et suppression restent ouverts à `operator`
Plans d'exécution	Création, modification, activation, désactivation, exécution immédiate	`operator`
Scripts	Téléversement des scénarios scriptés	`admin`
Secrets	Création, rotation, suppression (valeurs jamais affichées)	`admin`
Destinations d'export	Configuration et test des destinations OpenTelemetry et Prometheus	`admin`

Domaine	Fonctions	Rôle minimal
Paramètres	Réseau (dont IPv6 et 802.1X), heure, proxy, rétention, sécurité, SSH, mises à jour, licence, justificatif de maintenance, certificat, stockage SSD	`admin`
Comptes et jetons	Gestion des utilisateurs et des jetons d'API	`admin` (changement de son propre mot de passe : tout utilisateur authentifié)
Journal d'audit	Consultation des opérations d'administration	`admin`
Santé de la sonde	Version, édition, ressources, état des composants et des exports	`viewer`
Sauvegarde	Export et import de la configuration	`admin`

Les fonctions non autorisées pour votre rôle ne sont pas proposées.

6.2.3 Session

La session est maintenue par un cookie sécurisé, transmis uniquement en HTTPS et inaccessible aux scripts de la page. Elle expire après 30 minutes d'inactivité, et dans tous les cas 12 heures après la connexion. Pensez à vous déconnecter explicitement sur un poste partagé.

Après 5 tentatives de connexion infructueuses consécutives, le compte et l'adresse d'origine sont bloqués pendant 15 minutes. Toutes les tentatives, réussies ou non, sont enregistrées dans le journal d'audit (§ 6.10).

6.3 API REST : principes

6.3.1 Base et format

Élément	Règle
Adresse de base	`https://<adresse-de-la-sonde>/api/v1`
Version	Indiquée dans le chemin (`v1`). Une future version majeure coexistera au moins 12 mois avec la précédente
Format	JSON encodé en UTF-8 (`Content-Type: application/json`)
Dates	RFC 3339, en UTC. Exemple : `2025-11-19T09:15:02Z`
Durées dans les résultats	En millisecondes, dans des champs suffixés `Ms` (`durationMs`)
Durées dans la configuration	Chaînes `500ms`, `30s`, `5m`, `1h`
Identifiants	Choisis par vous pour les objets de configuration (`portail-accueil`) ; générés par la sonde (ULID) pour les exécutions
Description de l'API	Document OpenAPI 3.1 disponible à l'adresse `GET /api/v1/openapi.json`

Le document OpenAPI décrit toutes les ressources, leurs paramètres et leurs schémas. Il peut être importé dans un outil de test d'API ou servir à générer un client dans le langage de votre choix.

Deux adresses se situent hors de l'arborescence `/api/v1` :

Adresse	Usage	Authentification
`GET /health`	Vérifier que la sonde répond (vivacité). Ne renvoie aucune information sensible. Réponse `{"status": "OK"}` (code `200`) ; pendant l'**état de maintenance** qui ouvre l'activation d'une mise à jour, `{"status": "MAINTENANCE"}` (code `503`) (§ 8.4.9)	Aucune
`GET /metrics`	Métriques au format Prometheus (chapitre 2 du guide d'intégration et d'observabilité)	Jeton de rôle `metrics`

6.3.2 Authentification

Chaque appel à l'API, hors `GET /api/v1/system/certificate` (téléchargement du certificat de la sonde, sans authentification), doit présenter un **jeton d'API** dans l'en-tête HTTP `Authorization` :

```http
GET /api/v1/checks HTTP/1.1
Host: sonde-paris-01.example.internal
Authorization: Bearer <jeton>
Accept: application/json
```

Le jeton détermine l'identité de l'appelant et son rôle (§ 6.4). Un appel sans jeton, ou avec un jeton invalide, expiré ou révoqué, reçoit la réponse `401 Unauthorized`. Un appel authentifié mais non autorisé pour le rôle du jeton reçoit `403 Forbidden`.

> → **Évolution prévue** — L'authentification par certificat client (mTLS) n'est pas disponible actuellement : elle est prévue dans une version ultérieure, avec la console centrale (§ 6.14).

6.3.3 Préparer son poste : certificat et jeton

Les exemples de ce chapitre utilisent l'outil en ligne de commande `curl`, disponible sur Linux, macOS et Windows. Ils suivent deux règles de sécurité :

- **le certificat de la sonde est toujours vérifié**, grâce à l'option `--cacert`. L'option `-k` (`--insecure`) désactive cette vérification et ne doit pas être utilisée ;
- **le jeton n'apparaît jamais dans la ligne de commande**, où il serait visible dans l'historique du shell et la liste des processus. Il est lu depuis un fichier protégé.

Objectif : préparer un poste Linux ou macOS pour appeler l'API de façon sûre.

Prérequis : `curl` et `openssl` installés ; un jeton d'API (§ 6.5) ; l'empreinte SHA-256 du certificat de la sonde.

Étapes :

1. Créez un répertoire de travail accessible à vous seul :

   ```bash
   mkdir -p "$HOME/.sva" && chmod 700 "$HOME/.sva"
   ```

2. Si la sonde utilise son certificat autosigné, récupérez-le, soit par l'adresse `GET /api/v1/system/certificate` (§ 4.4.4), soit avec `openssl` :

   ```bash
   openssl s_client -connect sonde-paris-01.example.internal:443 \
     -servername sonde-paris-01.example.internal </dev/null 2>/dev/null \
     | openssl x509 -outform PEM > "$HOME/.sva/sonde-paris-01.pem"
   ```

3. Affichez son empreinte et **comparez-la** avec celle relevée lors de la mise en service :

```bash
openssl x509 -in "$HOME/.sva/sonde-paris-01.pem" -noout -fingerprint -sha256
```

   Si les empreintes diffèrent, supprimez le fichier et n'allez pas plus loin.

   Si la sonde utilise un certificat émis par l'autorité de certification de l'entreprise, utilisez à la place le certificat de cette autorité.

4. Créez le fichier d'en-tête d'authentification `entete-auth` une fois, puis recréez-le de la même manière à chaque rotation du jeton. Le répertoire `$HOME/.sva` est d'abord rendu privé ; un éventuel ancien fichier est supprimé, car un masque de permissions (`umask`) ne s'applique qu'à la création et ne resserre pas les droits d'un fichier existant ; le nouveau fichier est créé vide en mode `600` **avant** que le jeton n'y soit écrit. La commande `read -rs`, propre à bash et à zsh, lit le jeton au clavier sans l'afficher ; les parenthèses limitent le masque et la variable à cette seule opération :

```bash
(
  umask 077
  mkdir -p "$HOME/.sva" && chmod 700 "$HOME/.sva" &&
  rm -f "$HOME/.sva/entete-auth" &&
  : > "$HOME/.sva/entete-auth" && chmod 600 "$HOME/.sva/entete-auth" &&
  IFS= read -rs SONDE_TOKEN &&
  printf 'Authorization: Bearer %s\n' "$SONDE_TOKEN" > "$HOME/.sva/entete-auth"
)
```

   Si le jeton vous a été remis dans un fichier, par exemple `$HOME/.sva/jeton`, la forme suivante est équivalente (`printf` est une commande interne du shell : le jeton ne figure dans les arguments d'aucun processus) :

```bash
(
  umask 077
  mkdir -p "$HOME/.sva" && chmod 700 "$HOME/.sva" &&
  rm -f "$HOME/.sva/entete-auth" &&
  : > "$HOME/.sva/entete-auth" && chmod 600 "$HOME/.sva/entete-auth" &&
  printf 'Authorization: Bearer %s\n' "$(cat "$HOME/.sva/jeton")" > "$HOME/.sva/entete-auth"
)
```

   Supprimez ensuite le fichier `jeton` s'il n'a plus d'usage.

5. Définissez des variables de confort pour la session :

```bash
SONDE=https://sonde-paris-01.example.internal
CA="$HOME/.sva/sonde-paris-01.pem"
```

Information — Pourquoi cette méthode protège le jeton :

- le répertoire `$HOME/.sva` est ramené aux droits `700` et l'ancien fichier `entete-auth` éventuel est supprimé, car `umask` ne modifie pas les droits d'un fichier existant ; le nouveau fichier naît vide avec les droits `600` (lecture et écriture pour vous seul), et le jeton n'y est écrit qu'ensuite : il n'existe aucun instant où le jeton serait lisible par un autre compte. Chaque commande est enchaînée par `&&` : si l'une échoue, le jeton n'est pas écrit ;
- `read` et `printf` sont des **commandes internes** du shell (bash ou zsh ; l'option `-s` de `read` n'existe pas dans le shell POSIX `sh`) : elles ne créent aucun processus, et le jeton n'apparaît donc ni dans la liste des processus (`ps`), ni dans l'historique du shell. Dans la seconde forme, le processus `cat` ne reçoit que le **chemin** du fichier, jamais le jeton. Vous pouvez le vérifier avec `type printf`, qui doit répondre `printf is a shell builtin`. N'appelez pas `/usr/bin/printf` ou `env printf`, qui seraient des programmes externes ;
- `curl -H @"$HOME/.sva/entete-auth"` lit ensuite l'en-tête dans le fichier : le jeton ne figure pas dans les arguments de `curl`.

N'activez pas la trace du shell (`set -x`) pendant ces opérations : elle afficherait le jeton. Pour renouveler un jeton (§ 6.5), recréez simplement le fichier selon l'étape 4.

Vérification : interrogez l'état de la sonde.

```bash
curl --fail-with-body -sS --cacert "$CA" -H @"$HOME/.sva/entete-auth" \
  "$SONDE/api/v1/system"
```

Résultat attendu : une réponse JSON décrivant la sonde (version, édition, ressources, état des composants). Sa forme est définie par le schéma `system.schema.json`, et ses champs sont commentés au § 7.9 du guide d'utilisation et de supervision.

Information — `-H @fichier` demande à `curl` de lire les en-têtes dans un fichier. L'option `--fail-with-body` fait échouer la commande sur une erreur HTTP tout en affichant le détail renvoyé par la sonde. Ces options requièrent une version récente de `curl` : 7.55 ou ultérieure pour `-H @fichier`, 7.76 ou ultérieure pour `--fail-with-body`.

Dans la suite du chapitre, les commandes supposent ces variables définies. Pour alléger les exemples, nous utilisons la fonction suivante :

```bash
# Appel authentifié à l'API de la sonde, certificat vérifié
sapi() {
  curl --fail-with-body -sS --cacert "$CA" -H @"$HOME/.sva/entete-auth" \
       -H 'Accept: application/json' "$@"
}
```

L'outil `jq`, cité dans plusieurs exemples, met en forme et filtre les réponses JSON. Son usage est facultatif.

6.3.4 Codes de réponse et erreurs

Code	Signification	Cas typique
`200 OK`	Succès avec contenu	Lecture, modification
`201 Created`	Objet créé ; l'en-tête `Location` indique son adresse	Création d'un contrôle

Code	Signification	Cas typique
`202 Accepted`	Action acceptée et lancée en arrière-plan ; l'en-tête `Location` indique où suivre son avancement	Exécution manuelle, test d'une destination d'export
`204 No Content`	Succès sans contenu	Suppression, activation
`304 Not Modified`	Ressource inchangée depuis la version que vous détenez	Lecture conditionnelle
`400 Bad Request`	Requête mal formée	JSON invalide
`401 Unauthorized`	Jeton absent, invalide, expiré ou révoqué	—
`403 Forbidden`	Rôle insuffisant, fonction non incluse dans l'édition, ou mot de passe actuel erroné lors du changement de son propre mot de passe. Ces cas se distinguent par le champ `type` de l'erreur : `/api/v1/problems/edition-feature-unavailable` pour une fonction absente de l'édition, `/api/v1/problems/current-password-invalid` pour un mot de passe actuel erroné (§ 6.4.2)	Rôle `operator` qui téléverse un script ; contrôle `browser` créé sur une sonde Professional ; `PUT /api/v1/users/me/password` avec un mot de passe actuel erroné
`404 Not Found`	Objet inexistant	Identifiant erroné
`405 Method Not Allowed`	Méthode non admise par la ressource	`PUT /api/v1/settings/license`, section en lecture seule
`409 Conflict`	Opération incompatible avec l'état actuel	Création d'un identifiant déjà utilisé ; suppression d'un secret référencé par un contrôle
`410 Gone`	Ressource qui n'est plus disponible	Curseur de pagination expiré, plus de 24 heures après sa délivrance (§ 6.3.6)
`412 Precondition Failed`	Condition de l'en-tête `If-Match` ou `If-None-Match` non satisfaite (§ 6.3.5)	Objet modifié depuis votre dernière lecture ; création d'un secret qui existe déjà
`422 Unprocessable Content`	Contenu valide en JSON, mais non conforme au schéma ou aux règles	Champ obligatoire manquant, durée invalide
`428 Precondition Required`	Ni `If-Match` ni `If-None-Match` dans une requête qui en exige un (§ 6.3.5)	`PUT` ou `DELETE` sans en-tête conditionnel
`429 Too Many Requests`	Limite de débit atteinte	Boucle d'automatisation trop rapide
`5xx`	Erreur interne de la sonde	À signaler au support si elle persiste

Les erreurs sont décrites au format **Problem Details** (RFC 9457), type de contenu `application/problem+json`. Exemple de refus de validation (fictif) :

```json
{
  "type": "/api/v1/problems/validation",
  "title": "Configuration invalide",
  "status": 422,
  "detail": "Le contrôle 'portail-accueil' ne respecte pas le schéma.",
  "errors": [
    { "pointer": "/schedule", "detail": "Indiquer 'interval' ou 'cron', mais pas les deux." },
    { "pointer": "/timeout", "detail": "Format de durée invalide : '15 secondes'." }
  ]
}
```

Le champ `type` est une adresse relative de la forme `/api/v1/problems/{code}`, servie par la sonde. Il permet à un outil de distinguer les causes d'un même code HTTP : un refus `403` lié à l'édition porte ainsi le type `/api/v1/problems/edition-feature-unavailable`, et un refus pour mot de passe actuel erroné le type `/api/v1/problems/current-password-invalid`, et non celui d'un rôle insuffisant.

6.3.5 Modifications concurrentes : ETag et If-Match

Plusieurs administrateurs, ou un administrateur et un outil d'automatisation, peuvent modifier le même objet. Pour éviter qu'une modification n'en écrase silencieusement une autre, la sonde applique un **contrôle de concurrence optimiste** :

1. Chaque lecture d'un objet de configuration renvoie un en-tête `ETag`, qui identifie sa version. Pour un secret ou un compte, cette lecture est la lecture individuelle : `GET /api/v1/secrets/{name}` (§ 6.4.4) ou `GET /api/v1/users/{id}` (§ 6.4.2), réservées au rôle `admin`.
2. Toute modification (`PUT`, `PATCH`) ou suppression (`DELETE`) d'un objet existant doit présenter cette valeur dans l'en-tête `If-Match`.
3. Une ressource **créée** par `PUT`, comme un secret (`PUT /api/v1/secrets/{name}`, § 6.8.2), n'a pas encore d'`ETag` : la création présente l'en-tête `If-None-Match: *`, qui signifie « uniquement si la ressource n'existe pas ». Si elle existe déjà, la sonde répond `412 Precondition Failed` : il s'agit alors d'un remplacement, qui exige `If-Match`.
4. Une requête `PUT`, `PATCH` ou `DELETE` qui ne présente ni `If-Match` ni `If-None-Match` est refusée avec le code `428 Precondition Required`.
5. Si l'objet a changé entre-temps, la sonde refuse l'opération avec le code `412 Precondition Failed`. Relisez alors l'objet, réappliquez votre modification sur la version actuelle et renvoyez-la.

Portée. Cette règle s'applique aux ressources de configuration : contrôles, plans, scripts, destinations d'export, secrets, comptes et sections de paramètres (`/api/v1/settings/{section}`). Les requêtes d'action et d'import en écriture seule, qui ne modifient pas une ressource relue au préalable (`PUT /api/v1/system/maintenance`, `PUT /api/v1/system/certificate`, `PUT /api/v1/system/dot1x/credential`), n'en relèvent pas.

Exception. Le changement de son propre mot de passe, `PUT /api/v1/users/me/password` (§ 6.4.2), n'exige ni `If-Match` ni `If-None-Match` : la preuve demandée est le mot de passe actuel, et non la version du compte. Cette requête ne reçoit donc jamais le code `428`.

```bash
# Lecture : afficher l'ETag renvoyé
sapi -D - -o /dev/null "$SONDE/api/v1/checks/portail-accueil" | grep -i '^etag'
```

6.3.6 Pagination et filtres

Les listes potentiellement longues, comme l'historique des exécutions, sont **paginées par curseur**. La réponse contient les éléments et, s'il en reste, un curseur vers la page suivante :

```json
{
  "items": [ { "id": "01M7SJ4Q8R2V6X9Z3B5D7F1H0K", "checkId": "portail-accueil", "status": "OK" } ],
  "nextCursor": "eyJpZCI6IjAxSkRCNUs4UjJYN1E5TjNWNFQ2VzhZMFpBIn0"
}
```

Pour obtenir la page suivante, renvoyez la même requête avec le paramètre `cursor`. Le paramètre `limit` fixe la taille de page (100 par défaut, 1 000 au maximum). Le curseur est une valeur opaque, encodée en base64url : il se transmet tel quel, sans encodage supplémentaire.

Cohérence de la pagination. Pour l'historique des exécutions, les règles suivantes s'appliquent :

Règle	Conséquence pour vous
Les éléments sont rangés selon un **ordre total** : date de début (`startedAt`), puis identifiant (`id`) pour départager deux exécutions de même date	Aucun élément n'est lu deux fois ni sauté du fait d'un ex æquo
Le curseur encode la **dernière position lue** et reste valide **24 heures**	Au-delà, la sonde répond `410 Gone` : relancez la lecture depuis la première page
Les exécutions enregistrées pendant la lecture n'apparaissent dans les pages suivantes que si leur date de début les place après la dernière position lue ; sinon, elles manquent à la lecture en cours	Pour un **export reproductible**, fixez toujours une borne `to` dans le passé : les exécutions commencées après elle sont exclues. Une exécution commencée avant `to` mais enregistrée plus tard reste dans la période : deux lectures successives ne donnent le même ensemble que si `to` est assez ancienne pour qu'aucune exécution de la période ne soit encore en cours (§ 7.3.2 du guide d'utilisation et de supervision), et sous réserve de la règle suivante
La sonde ne fournit **pas d'instantané** : les exécutions purgées par la rétention (§ 3.12 du guide d'utilisation et de supervision) pendant la lecture disparaissent des pages suivantes	Pour un export complet, choisissez une borne `from` nettement plus récente que la limite de rétention, ou lisez les périodes anciennes en priorité

```bash
# Exécutions en échec d'un contrôle sur une période donnée
sapi "$SONDE/api/v1/runs?checkId=portail-accueil&status=CRITICAL&from=2025-11-18T00:00:00Z&to=2025-
    11-19T00:00:00Z&limit=50"
```

6.4 Utilisateurs et rôles

6.4.1 Les rôles

Les droits sont attribués par **rôle**. Chaque utilisateur et chaque jeton d'API possède un rôle unique.

Rôle	Droits	Usage recommandé
`admin`	Toutes les opérations, y compris comptes, jetons, secrets, réseau, mises à jour (politique, activation immédiate ou programmée, report), scripts et plugins personnalisés	Administrateurs de la sonde, en nombre limité

Rôle	Droits	Usage recommandé
`operator`	Créer et modifier les contrôles et plans **non scriptés**, activer, désactiver, déclencher, consulter. Peut **référencer** un secret existant dans un contrôle, sans pouvoir le lire, le créer, le modifier ni changer ses hôtes autorisés (`allowedHosts` , § 6.8). Pas de code exécutable : un `POST` , `PUT` ou `PATCH` d'un `operator` qui crée, modifie ou retire un scénario scripté (`browser.mode: script` ou `browser.scriptRef`) ou un plugin personnalisé est refusé avec `403` . Pas de paramètres système	Équipe d'exploitation, référents applicatifs
`viewer`	Lecture seule des états, résultats et artefacts, dont l'état de santé `updates` de la sonde (`GET /api/v1/system`)	Équipes support, consultation
`metrics`	Uniquement `/metrics` et l'état des contrôles (`GET /api/v1/checks/{id}/status`)	Prometheus, Nagios, Centreon

Information — Le téléversement de scripts de scénarios et de plugins personnalisés est réservé au rôle `admin` , parce qu'il revient à exécuter du code sur le réseau où la sonde est installée. Pour la même raison, seul un `admin` peut faire **désigner** un code par un contrôle : choisir ou changer le script d'un scénario (`scriptRef`) revient à décider du code exécuté. Un utilisateur `operator` peut créer des scénarios **déclaratifs** (chapitre 4 du guide de développement des scénarios), qui ne contiennent pas de code, et activer, désactiver ou déclencher un contrôle scripté existant.

Information — L'usage d'un secret est contrôlé **par la sonde**, et non par le seul rôle de l'auteur du contrôle. Chaque secret porte une liste obligatoire d'hôtes autorisés (`allowedHosts`), fixée par un `admin` (§ 6.8.1) : un `operator` qui référence un secret dans un contrôle ne peut le faire parvenir qu'à ces hôtes.

6.4.2 Gérer les comptes

Les comptes de l'interface d'administration sont des **comptes locaux** de la sonde. Le compte administrateur initial est créé lors de la mise en service (chapitre 4).

L'authentification repose uniquement sur ces comptes locaux. L'authentification par l'annuaire de l'entreprise (LDAP, SAML, OpenID Connect) n'est pas disponible.

Évolution prévue — L'authentification par **OpenID Connect** est prévue dans une version ultérieure. Le moteur d'authentification de la sonde repose sur des fournisseurs interchangeables (comptes locaux, puis OpenID Connect) : l'ajout de ce fournisseur, avec une correspondance entre les groupes de l'annuaire et les rôles de la sonde, ne modifiera ni les rôles décrits au § 6.4.1 ni l'API.

Objectif : créer un compte nominatif pour un membre de l'équipe d'exploitation.

Prérequis : rôle `admin` .

Étapes (interface d'administration) :

1. Ouvrez la gestion des comptes.
2. Créez un compte en indiquant l'identifiant, le rôle (`operator`) et un mot de passe initial conforme à la politique de mot de passe : 12 caractères au minimum et 128 au maximum, sans règle de composition imposée ni expiration périodique.
3. Transmettez le mot de passe initial par un canal sûr. Son changement est imposé à la première connexion, puisque le compte a été créé par un autre administrateur.

Étapes (API) : la création s'effectue par `POST /api/v1/users`, avec les champs `username`, `role` et `password`, décrits par le schéma `user.schema.json`. Dans l'exemple ci-dessous, le mot de passe est lu depuis l'entrée standard pour ne pas apparaître dans la ligne de commande.

```bash
read -rs MDP && printf '%s' "$MDP" | jq -Rs \
  '{username: "j.martin", role: "operator", password: .}' \
  | sapi -X POST -H 'Content-Type: application/json' --data @- \
      "$SONDE/api/v1/users"; unset MDP
```

Vérification : le compte apparaît dans `GET /api/v1/users`, et la création figure dans le journal d'audit.

Modifier le rôle ou le mot de passe d'un compte. Un administrateur modifie un compte existant par `PATCH /api/v1/users/{id}` (rôle `admin`), en indiquant le champ `role`, le champ `password`, ou les deux ; l'identifiant de connexion (`username`) ne se modifie pas. L'identifiant `{id}` du compte figure dans la réponse de `GET /api/v1/users`. Comme toute modification, la requête présente l'en-tête `If-Match` (§ 6.3.5), avec l'`ETag` obtenu par la lecture individuelle du compte, `GET /api/v1/users/{id}` (rôle `admin`). Cette lecture renvoie l'identifiant, l'identifiant de connexion et le rôle du compte, jamais son mot de passe ni l'empreinte de celui-ci. Exemple : réinitialiser le mot de passe d'un compte, lu sans affichage :

```bash
# 1. Lire l'ETag courant du compte
ETAG=$(sapi -D - -o /dev/null "$SONDE/api/v1/users/<id>" \
       | awk 'tolower($1)=="etag:" {print $2}' | tr -d '\r')

# 2. Définir le nouveau mot de passe
read -rs MDP && printf '%s' "$MDP" | jq -Rs '{password: .}' \
  | sapi -X PATCH -H 'Content-Type: application/merge-patch+json' \
      -H "If-Match: $ETAG" --data @- \
      "$SONDE/api/v1/users/<id>"; unset MDP
```

Dans cet exemple, `<id>` est l'identifiant du compte ; la première commande lit son `ETag` dans les en-têtes de la réponse de `GET /api/v1/users/{id}`. Le nouveau mot de passe respecte la même politique qu'à la création.

Effets d'une modification sur les sessions et les jetons du compte :

Modification	Sessions de l'interface du compte	Jetons d'API du compte
Changement de rôle (`role`)	Fermées immédiatement : l'utilisateur se reconnecte et obtient son nouveau rôle	**Inchangés** : chaque jeton conserve le rôle fixé à sa création, car le rôle est propre au jeton (§ 6.5.1)
Changement de mot de passe par un administrateur (`password`)	Fermées, à l'exception de la session depuis laquelle la requête est émise si elle appartient au compte modifié	Inchangés
Changement de son propre mot de passe (`PUT /api/v1/users/me/password`)	Les autres sessions sont fermées ; la session courante est conservée	Inchangés

> **Attention** — Abaisser le rôle d'un compte ne réduit pas les droits des jetons qu'il a créés. Si la modification doit s'appliquer aussi aux outils qui utilisent ces jetons, créez de nouveaux jetons du rôle voulu, puis révoquez les anciens (§ 6.5.4). De même, après un changement de mot de passe motivé par une compromission, révoquez les jetons du compte qui ont pu être exposés.

Changer son propre mot de passe. Tout utilisateur authentifié, quel que soit son rôle, change son propre mot de passe par `PUT /api/v1/users/me/password`, avec les champs `currentPassword` (mot de passe actuel) et `newPassword` (nouveau mot de passe, conforme à la politique ci-dessus). La saisie du mot de passe actuel empêche

qu'une session laissée ouverte suffise à changer le mot de passe. L'interface d'administration propose la même opération. Cette requête obéit aux règles suivantes :

- elle n'exige pas l'en-tête `If-Match` : la preuve demandée est le mot de passe actuel (exception au § 6.3.5) ;
- si le mot de passe actuel est erroné, la sonde répond `403 Forbidden` avec le type d'erreur `/api/v1/problems/current-password-invalid` (§ 6.3.4), et le mot de passe n'est pas modifié ;
- après le changement, les autres sessions de l'interface ouvertes pour ce compte sont fermées, la session courante est conservée, et les jetons d'API du compte ne sont pas modifiés.

```bash
read -rs ACTUEL && read -rs NOUVEAU \
  && printf '%s\n%s\n' "$ACTUEL" "$NOUVEAU" \
  | jq -Rn '[inputs] | {currentPassword: .[0], newPassword: .[1]}' \
  | sapi -X PUT -H 'Content-Type: application/json' --data @- \
      "$SONDE/api/v1/users/me/password"; unset ACTUEL NOUVEAU
```

Les deux mots de passe sont saisis l'un après l'autre, sans affichage, puis transmis à `jq` par l'entrée standard : comme dans les exemples précédents, ils n'apparaissent ni dans l'historique ni dans les arguments d'un processus.

Supprimer un compte. Utilisez `DELETE /api/v1/users/{id}`. Les sessions et jetons de l'utilisateur supprimé sont révoqués immédiatement.

6.4.3 Bonnes pratiques

- **Un compte par personne** : n'utilisez pas de compte partagé. Le journal d'audit n'a de valeur que si chaque action est rattachée à une personne.
- **Moindre privilège** : attribuez le rôle le plus restreint suffisant. La plupart des intervenants n'ont besoin que de `viewer` ou `operator`.
- **Au moins deux administrateurs** : pour éviter toute perte d'accès en cas d'absence ou d'oubli de mot de passe.
- **Code de récupération** : conservez dans le coffre-fort de l'organisation le code de récupération affiché une seule fois à la fin de la mise en service. Avec le code d'installation et un accès physique à la carte, il permet de redéfinir le mot de passe d'un compte `admin` sans perdre la configuration (chapitre 8). Sans lui, seule la réinitialisation usine permet de retrouver un accès administrateur.
- **Revue périodique** : supprimez les comptes des personnes ayant quitté l'équipe.

6.5 Jetons d'API

6.5.1 Principe

Un **jeton d'API** est une chaîne aléatoire qui authentifie un outil ou un script auprès de l'API. Il possède :

- un **rôle** qui limite ses droits (§ 6.4.1) ;
- un **nom** descriptif, qui indique son usage ;
- une **date d'expiration** facultative ;
- un **propriétaire**, l'utilisateur qui l'a créé.

La sonde ne conserve qu'une **empreinte** du jeton. La valeur en clair n'est affichée **qu'une seule fois**, au moment de la création : notez-la immédiatement dans un coffre-fort de mots de passe ou dans le gestionnaire de secrets de l'outil qui l'utilisera.

Un jeton est **immuable** : son nom, son rôle et sa date d'expiration ne se modifient plus après sa création, et l'API ne propose ni `PUT` ni `PATCH` sur les jetons. Pour changer l'un d'eux, ou pour renouveler un jeton qui arrive à expiration, créez un nouveau jeton, mettez à jour l'outil qui l'utilise, puis révoquez l'ancien (§ 6.5.4).

6.5.2 Créer un jeton

Objectif : créer un jeton en lecture seule pour le serveur Prometheus.

Prérequis : rôle `admin`.

Étapes :

1. Dans l'interface d'administration, ouvrez la gestion des jetons, ou utilisez `POST /api/v1/tokens`.
2. Indiquez un nom explicite (`prometheus-prod`), le rôle `metrics` et une date d'expiration conforme à votre politique de sécurité.
3. Copiez la valeur affichée et enregistrez-la dans l'outil destinataire.

Exemple par l'API (champs `name`, `role` et `expiresAt`) :

```bash
sapi -X POST -H 'Content-Type: application/json' \
  -d '{"name": "prometheus-prod", "role": "metrics", "expiresAt": "2026-11-30T00:00:00Z"}' \
  "$SONDE/api/v1/tokens"
```

Résultat attendu : la réponse contient la valeur du jeton, visible cette seule fois. Les champs de la requête et de la réponse sont décrits par le schéma `token.schema.json`.

Vérification : le jeton apparaît dans `GET /api/v1/tokens`, sans sa valeur.

6.5.3 Choisir le rôle et la durée de vie

Usage	Rôle	Expiration conseillée
Prometheus (collecte `/metrics`)	`metrics`	12 mois, renouvellement planifié
Nagios, Centreon (`check_sva`)	`metrics`	12 mois
Tableau de bord interne en lecture	`viewer`	12 mois
Outil d'automatisation créant des contrôles	`operator`	3 à 6 mois
Outil d'automatisation complet (déploiement de scripts, secrets)	`admin`	Courte ; à réserver à des outils de confiance

6.5.4 Révoquer un jeton

Révoquez immédiatement un jeton par `DELETE /api/v1/tokens/{id}` ou depuis l'interface lorsque :

- l'outil qui l'utilisait est retiré ;
- le jeton a pu être exposé (fichier partagé par erreur, dépôt de code, capture d'écran) ;
- son propriétaire quitte l'équipe.

La révocation est effective immédiatement : les appels suivants reçoivent `401 Unauthorized`.

> ! **Avertissement** — Ne stockez jamais un jeton d'API dans un dépôt de code source, un fichier de configuration lisible par tous ou un ticket. Utilisez le gestionnaire de secrets de votre outil d'automatisation (coffre Ansible, gestionnaire de secrets de votre chaîne d'intégration continue, coffre-fort d'entreprise).

6.6 Gestion des contrôles

Cette section décrit les opérations sur les contrôles. Les options propres à chaque type sont détaillées :

- au chapitre 4 du guide d'utilisation et de supervision pour `icmp`, `tcp`, `dns`, `http` et `nagios` ;
- au chapitre 5 du guide d'utilisation et de supervision pour `api` et `database` ;
- au chapitre 4 du guide de développement des scénarios pour `browser`.

6.6.1 Opérations disponibles

Opération	Méthode et chemin	Rôle minimal
Lister les contrôles	`GET /api/v1/checks` (filtres `type`, `enabled`, `tag`, `status`)	`viewer`
Lire un contrôle	`GET /api/v1/checks/{id}`	`viewer`
Créer	`POST /api/v1/checks`	`operator` ; `admin` pour un scénario scripté ou un contrôle qui utilise un plugin personnalisé
Remplacer	`PUT /api/v1/checks/{id}`	`operator` pour un contrôle non scripté ; `admin` si le contrôle existant ou la nouvelle définition est un scénario scripté ou utilise un plugin personnalisé, même si son code reste inchangé (un `operator` ajuste la planification ou les seuils d'un tel contrôle par `PATCH`)
Modifier partiellement	`PATCH /api/v1/checks/{id}` (JSON Merge Patch)	`operator` ; `admin` si la modification crée, change ou retire `browser.mode: script`, `browser.scriptRef` ou un plugin personnalisé
Supprimer	`DELETE /api/v1/checks/{id}`	`operator`
Activer, désactiver	`POST /api/v1/checks/{id}/enable`, `POST /api/v1/checks/{id}/disable`	`operator`
Exécuter immédiatement	`POST /api/v1/checks/{id}/runs`	`operator`
Exécution d'essai	`POST /api/v1/checks/{id}/runs?dryRun=true`	`operator`
État courant	`GET /api/v1/checks/{id}/status`	`metrics`

> **Attention** — Un `operator` peut ajuster la planification, les seuils ou les étiquettes d'un scénario scripté par `PATCH`, mais toute requête de sa part qui touche au code exécuté (passage en mode `script`, changement ou retrait de `scriptRef`, ajout, changement ou retrait d'un plugin personnalisé) est refusée avec `403`. Le choix du code exécuté relève toujours d'un `admin` (§ 6.4.1).

6.6.2 Créer un contrôle

Objectif : créer un contrôle HTTP vérifiant la page d'accueil d'un portail.

Prérequis : rôle `operator` ; édition Essential ou supérieure ; la cible est joignable depuis la sonde (§ 3.2.2 du guide d'utilisation et de supervision).

Étapes :

1. Rédigez la définition du contrôle dans un fichier `portail-accueil.json` :

```json
{
  "id": "portail-accueil",
  "name": "Portail client : page d'accueil",
  "type": "http",
  "enabled": false,
  "tags": { "application": "portail", "environment": "production" },
  "schedule": { "interval": "1m", "jitter": "10s" },
  "timeout": "15s",
  "retry": { "attempts": 1, "interval": "20s" },
  "thresholds": { "warningDuration": "3s" },
  "http": {
    "method": "GET",
    "url": "https://portail.example.com/",
    "assertions": [
      { "kind": "status", "operator": "eq", "value": 200 },
      { "kind": "body", "operator": "contains", "value": "Espace client" }
    ]
  }
}
```

   Le contrôle est créé **désactivé** (`"enabled": false`) pour pouvoir être testé avant d'entrer en service.

2. Envoyez-le à la sonde :

```bash
sapi -X POST -H 'Content-Type: application/json' \
  --data @portail-accueil.json "$SONDE/api/v1/checks"
```

3. Lancez une exécution d'essai (§ 6.6.5) et vérifiez son résultat.
4. Activez le contrôle (§ 6.6.4).

Résultat attendu : réponse `201 Created` ; le contrôle apparaît dans la liste et dans l'interface.

En cas de problème : une réponse `422` détaille les champs non conformes (§ 6.3.4) ; une réponse `409` indique que l'identifiant existe déjà ; une réponse `403` signale un rôle insuffisant ou, avec le type d'erreur `/api/v1/problems/edition-feature-unavailable`, un type de contrôle non inclus dans votre édition (§ 6.3.4).

Dans l'interface d'administration, la même opération s'effectue par un formulaire. Celui-ci applique les mêmes règles de validation que l'API (§ 6.3.4).

6.6.3 Modifier un contrôle

Deux méthodes sont possibles :

- `PUT` remplace la définition complète. C'est la méthode à privilégier lorsque la définition de référence est conservée dans un fichier, par exemple dans un dépôt de configuration ;
- `PATCH` ne modifie que les champs fournis (format JSON Merge Patch, RFC 7396). C'est la méthode la plus pratique pour un ajustement ponctuel.

Exemple : porter la fréquence à 2 minutes, en respectant le contrôle de concurrence (§ 6.3.5).

```bash
# 1. Lire l'ETag courant
ETAG=$(sapi -D - -o /dev/null "$SONDE/api/v1/checks/portail-accueil" \
       | awk 'tolower($1)=="etag:" {print $2}' | tr -d '\r')

# 2. Appliquer la modification partielle
sapi -X PATCH -H 'Content-Type: application/merge-patch+json' \
  -H "If-Match: $ETAG" \
  -d '{"schedule": {"interval": "2m", "jitter": "15s"}}' \
  "$SONDE/api/v1/checks/portail-accueil"
```

Chaque modification incrémente la **révision** du contrôle. Le numéro de révision est enregistré dans chaque résultat d'exécution : vous savez ainsi quelle version de la configuration a produit un résultat donné.

> **Information** — Avec JSON Merge Patch, les objets sont fusionnés champ par champ, mais un **tableau** fourni remplace intégralement le tableau existant. Pour modifier une seule assertion d'un contrôle HTTP, renvoyez donc la liste complète des assertions. Une propriété fixée à `null` est **supprimée** : `{"schedule": null}` retire ainsi la planification propre d'un contrôle, qui ne s'exécute plus que par un plan d'exécution ou manuellement (chapitre 6 du guide d'utilisation et de supervision).

6.6.4 Activer et désactiver

Désactiver un contrôle suspend ses exécutions planifiées sans le supprimer, et conserve son historique. C'est la méthode à utiliser pendant une intervention planifiée sur l'application supervisée, pour éviter des alertes inutiles.

```bash
sapi -X POST "$SONDE/api/v1/checks/portail-accueil/disable"
sapi -X POST "$SONDE/api/v1/checks/portail-accueil/enable"
```

> **Conseil** — Notez dans votre procédure de changement de **réactiver** les contrôles à la fin de l'intervention. Un contrôle oublié en état désactivé ne supervise plus rien. La liste `GET /api/v1/checks?enabled=false` permet de les repérer.

> **Évolution prévue** — Des fenêtres de maintenance planifiées, suspendant automatiquement des contrôles sur une période donnée, sont prévues dans une version ultérieure (§ 6.8 du guide d'utilisation et de supervision).

6.6.5 Exécution immédiate et exécution d'essai

	Exécution immédiate	Exécution d'essai (`dryRun`)
Appel	`POST /api/v1/checks/{id}/runs`	`POST /api/v1/checks/{id}/runs?dryRun=true`
Contrôle désactivé	Autorisé, par exemple pour mettre au point un contrôle avant de l'activer	Autorisé
Effet sur l'état courant	Oui	Non
Export vers les plateformes	Oui	Non

	Exécution immédiate	Exécution d'essai (`dryRun`)
Conservation du résultat	Dans l'historique	Consultable, marqué `dryRun`
Usage	Confirmer un incident ou la résolution d'un incident, rejouer un contrôle	Mettre au point un nouveau contrôle ou une modification sans perturber la supervision

L'exécution étant asynchrone, la sonde répond `202 Accepted` avec un en-tête `Location` vers la ressource d'exécution. Il suffit de suivre cette ressource jusqu'à la fin de l'exécution :

```bash
# Lancer une exécution d'essai et récupérer l'adresse de suivi
LOC=$(sapi -X POST -D - -o /dev/null \
      "$SONDE/api/v1/checks/portail-accueil/runs?dryRun=true" \
      | awk 'tolower($1)=="location:" {print $2}' | tr -d '\r')

# Consulter le résultat (répéter jusqu'à la fin de l'exécution)
sapi "$SONDE$LOC" | jq '{status, durationMs, error}'
```

L'en-tête `Location` de la réponse `202 Accepted` désigne la ressource de l'exécution, de la forme `/api/v1/runs/{runId}`.

> ✓ **Conseil** — Réalisez systématiquement une exécution d'essai après toute création ou modification significative d'un contrôle. Elle valide en une opération la configuration, l'accès réseau à la cible et les assertions.

6.6.6 Supprimer un contrôle

```bash
ETAG=$(sapi -D - -o /dev/null "$SONDE/api/v1/checks/portail-accueil" \
       | awk 'tolower($1)=="etag:" {print $2}' | tr -d '\r')
sapi -X DELETE -H "If-Match: $ETAG" "$SONDE/api/v1/checks/portail-accueil"
```

La suppression est définitive pour la configuration. L'historique des exécutions reste consultable jusqu'à l'échéance de sa durée de rétention. La suppression d'un contrôle référencé par un plan d'exécution est refusée (`409 Conflict`) ; la réponse liste les plans concernés. Retirez d'abord le contrôle de ces plans.

> ! **Attention** — Recréer ultérieurement un contrôle avec le même identifiant le rattache, dans les plateformes d'observabilité, à l'historique de l'ancien contrôle. Si la nouvelle définition vérifie autre chose, choisissez un nouvel identifiant.

6.7 Scripts de scénarios

Les scénarios **scriptés** (édition Enterprise) sont des modules JavaScript Puppeteer, décrits au chapitre 4 du guide de développement des scénarios. Le script est téléversé séparément du contrôle, puis référencé par celui-ci.

6.7.1 Téléverser un script

Le téléversement d'un script se fait par l'interface d'administration ou par `POST /api/v1/scripts` (rôle `admin`, édition Enterprise). La procédure complète de mise en service d'un scénario scripté, du téléversement à l'activation du contrôle, figure au § 4.16.2 du guide de développement des scénarios. Les règles propres à l'administration sont les suivantes :

- chaque requête transmet un seul module `.mjs`, avec le type de contenu `text/javascript`, dans la limite de 1 Mo. Les scénarios déclaratifs ne passent pas par cette ressource : leurs étapes figurent dans la définition du contrôle (`POST /api/v1/checks`, type `application/json`) ;
- la sonde valide le script, calcule son empreinte SHA-256 et renvoie une **référence** de la forme `nom@sha256:empreinte`, par exemple `boutique-connexion@sha256:4f1c9e2ab7d3` (empreinte abrégée dans les exemples de cette documentation : une référence réelle comporte les 64 caractères hexadécimaux de l'empreinte), à indiquer dans la propriété `browser.scriptRef` du contrôle ;
- le téléversement d'un script et toute création, modification ou suppression de `browser.scriptRef` dans un contrôle sont réservés au rôle `admin` : la même requête émise par un `operator` est refusée avec `403` (§ 6.4.1 et § 6.6.1).

Vérification : `GET /api/v1/scripts/{name}` liste les versions téléversées.

6.7.2 Pourquoi une référence par empreinte

La référence désigne **une version précise et immuable** du script. Téléverser une nouvelle version ne modifie donc pas les contrôles existants : le changement n'intervient qu'au moment où vous mettez à jour `scriptRef` dans le contrôle. Ce mécanisme apporte trois garanties :

- aucune modification involontaire d'un scénario en production ;
- la possibilité de revenir à la version précédente en rétablissant l'ancienne référence ;
- la traçabilité : le journal d'audit indique qui a téléversé quelle version, et quand.

> ✓ **Conseil** — Conservez vos scripts dans un système de gestion de versions (Git), et faites figurer l'empreinte renvoyée par la sonde dans le message de version. Le lien entre le code source et ce qui s'exécute sur la sonde reste ainsi vérifiable.

6.8 Secrets

6.8.1 Principe

Un **secret** est une valeur sensible dont un contrôle a besoin : mot de passe d'un compte de test, jeton d'une API, mot de passe d'une base de données. La sonde stocke les secrets **chiffrés** et applique quatre règles :

1. **Écriture seule** : un secret peut être créé, remplacé ou supprimé, mais sa valeur ne peut jamais être relue, ni par l'interface ni par l'API, quel que soit le rôle.
2. **Déclaration explicite** : un contrôle ne reçoit que les secrets qu'il déclare dans sa propriété `secrets`.
3. **Masquage** : la valeur d'un secret est masquée dans les messages d'erreur, les journaux, les sorties de plugins et la console du navigateur enregistrée.
4. **Destinations autorisées** : chaque secret porte une liste **obligatoire** d'hôtes autorisés, `allowedHosts` (noms d'hôtes ou motifs de noms, avec un port éventuel), fixée par un `admin`. La sonde n'injecte un secret que dans une requête, une connexion ou une page dont l'hôte figure dans cette liste.

Cette quatrième règle protège contre le détournement d'un secret : un contrôle non scripté modifié pour envoyer le secret vers un autre serveur ne le reçoit pas ; le cas des scénarios scriptés est précisé ci-dessous. Elle s'applique ainsi :

Situation	Comportement de la sonde
L'hôte de la requête, de la connexion ou de la page figure dans `allowedHosts`	Le secret est injecté
L'hôte n'y figure pas	Le secret n'est pas injecté ; l'exécution échoue
Redirection HTTP vers un **autre hôte**	Les en-têtes porteurs d'un secret (par exemple `Authorization`) ne sont **pas retransmis** à la destination de la redirection. Une redirection étant une nouvelle requête, la règle d'injection s'applique à sa destination pour **tout élément porteur d'un secret** (en-tête, corps renvoyé lors d'une redirection `307` ou `308`, paramètre d'adresse), et aucun n'est transmis à un hôte absent de la liste
Hôte inscrit avec un port (par exemple `db.example.internal:5432`)	Le secret n'est injecté que vers ce port
Changement de destination (URL ou hôte modifié dans le contrôle, navigation vers une autre page)	La vérification porte sur la destination de chaque requête, connexion ou page au moment de l'injection : un contrôle modifié pour viser un hôte absent de la liste ne reçoit pas le secret
Scénario scripté (`browser.mode=script`)	Le script reçoit la valeur dans l'objet `secrets` (chapitre 4 du guide de développement des scénarios) : la sonde ne peut pas garantir à elle seule que le code ne la transmet pas ailleurs . C'est l'une des raisons pour lesquelles ces scénarios sont réservés au rôle `admin`
Un `operator` crée ou modifie un contrôle	Il peut référencer un secret existant ; il ne peut ni lire sa valeur ni modifier `allowedHosts`
Import d'une configuration (§ 6.12.3)	Les références aux secrets sont **revérifiées** : secret existant, déclaration dans le contrôle, hôtes autorisés
Import d'une archive antérieure à `allowedHosts` (secret sans liste)	Le secret est importé mais reste **inutilisable**, c'est-à-dire jamais injecté, tant qu'un `admin` n'a pas défini sa liste ; le compte rendu d'import le signale

Les scénarios scriptés restent réservés au rôle `admin` (§ 6.4.1).

Les noms de secrets s'écrivent en majuscules, chiffres et tirets bas, et commencent par une lettre (`BOUTIQUE_PASSWORD`, `API_STOCK_TOKEN`).

6.8.2 Créer ou remplacer un secret

Objectif : enregistrer le mot de passe du compte de test de la boutique.

Prérequis : rôle `admin`.

Étapes :

1. Dans l'interface d'administration, ouvrez la gestion des secrets et créez le secret `BOUTIQUE_PASSWORD`, ou utilisez l'API, `PUT /api/v1/secrets/{name}`, avec un corps de la forme `{"value": …, "allowedHosts": [ … ]}`. La liste `allowedHosts` est obligatoire et contient au moins un hôte : ici, le seul site de la boutique de test (nom fictif). Pour une **création**, la requête porte l'en-tête `If-None-Match: *` (§ 6.3.5) : si un secret de même nom existe déjà, la sonde répond `412 Precondition Failed` au lieu de l'écraser. Exemple, la valeur étant lue sans affichage :

```bash
read -rs VAL && printf '%s' "$VAL" \
  | jq -Rs '{value: ., allowedHosts: ["recette.boutique.example.com"]}' \
  | sapi -X PUT -H 'Content-Type: application/json' -H 'If-None-Match: *' \
      --data @- "$SONDE/api/v1/secrets/BOUTIQUE_PASSWORD"; unset VAL
```

2. Vérifiez sa présence : `GET /api/v1/secrets` (rôle `admin`) liste les noms et les métadonnées des secrets, jamais leurs valeurs. Ces métadonnées comprennent la date de rotation et la liste `allowedHosts` de chaque secret. Pour un seul secret, `GET /api/v1/secrets/{name}` (rôle `admin`) renvoie ses métadonnées, dont `allowedHosts`, et son `ETag`, nécessaires à sa rotation (§ 6.8.4) ; cette lecture ne renvoie jamais la valeur du secret.

Corps de requête correspondant (valeur fictive) :

```json
{ "value": "********", "allowedHosts": ["recette.boutique.example.com"] }
```

Résultat attendu : le secret est disponible pour les contrôles qui le déclarent, et uniquement vers les hôtes autorisés.

6.8.3 Utiliser un secret dans un contrôle

Un secret s'utilise en deux temps :

1. il est **déclaré** dans la liste `secrets` du contrôle ;
2. il est **référencé** à l'endroit voulu par la syntaxe `${secret:NOM}`. Dans un scénario scripté, il est lu dans l'objet `secrets` (chapitre 4 du guide de développement des scénarios).

```json
{
  "id": "api-stock",
  "name": "API de stock : article témoin",
  "type": "http",
  "schedule": { "interval": "2m" },
  "timeout": "10s",
  "secrets": ["API_STOCK_TOKEN"],
  "http": {
    "method": "GET",
    "url": "https://api.example.com/v1/stock/ARTICLE-TEMOIN",
    "headers": { "Authorization": "Bearer ${secret:API_STOCK_TOKEN}" },
    "assertions": [ { "kind": "status", "operator": "eq", "value": 200 } ]
  }
}
```

Dans cet exemple, le secret `API_STOCK_TOKEN` doit avoir été créé avec `"allowedHosts": ["api.example.com"]` : l'hôte de l'URL du contrôle figure dans la liste, le secret est donc injecté dans l'en-tête `Authorization`.

Un contrôle qui référence un secret non déclaré, ou un secret inexistant, est refusé à la création (`422`). La suppression d'un secret encore référencé par un contrôle est refusée (`409`).

6.8.4 Rotation

Remplacer la valeur d'un secret suffit : tous les contrôles qui l'utilisent emploient la nouvelle valeur dès leur prochaine exécution. Le remplacement utilise la même requête qu'à la création (§ 6.8.2), mais avec l'en-tête `If-Match` portant l'`ETag` du secret, et non `If-None-Match: *` (§ 6.3.5). Chaque `PUT` exige en outre la liste `allowedHosts` en même temps que la valeur. Lisez donc d'abord le secret par `GET /api/v1/secrets/{name}` (rôle `admin`) : la réponse contient ses métadonnées, dont la liste `allowedHosts`, et l'en-tête `ETag`, mais jamais sa valeur. Renvoyez la liste à l'identique, sauf modification voulue, pour ne pas restreindre ni étendre par mégarde les destinations autorisées. La date de rotation est enregistrée et visible dans la liste des secrets.

Exemple de rotation, la nouvelle valeur étant lue sans affichage (nom de secret fictif) :

```bash
# 1. Lire les métadonnées et l'ETag du secret (la valeur n'est jamais renvoyée)
ENTETES=$(mktemp)
META=$(sapi -D "$ENTETES" "$SONDE/api/v1/secrets/BOUTIQUE_PASSWORD")
ETAG=$(awk 'tolower($1)=="etag:" {print $2}' "$ENTETES" | tr -d '\r'); rm -f "$ENTETES"

# 2. Remplacer la valeur en renvoyant à l'identique la liste allowedHosts relue
read -rs VAL && printf '%s' "$VAL" \
  | jq -Rs --argjson hotes "$(jq -c '.allowedHosts' <<<"$META")" \
      '{value: ., allowedHosts: $hotes}' \
  | sapi -X PUT -H 'Content-Type: application/json' -H "If-Match: $ETAG" \
      --data @- "$SONDE/api/v1/secrets/BOUTIQUE_PASSWORD"; unset VAL
```

Si un autre administrateur a modifié le secret entre la lecture et le remplacement, la sonde répond `412 Precondition Failed` : relisez le secret et recommencez.

Procédure de rotation sans interruption d'un mot de passe de compte de test :

1. Prévenez les équipes concernées et choisissez un moment hors période critique.
2. Modifiez le mot de passe du compte de test dans l'application supervisée.
3. Remplacez immédiatement la valeur du secret sur la sonde (exemple ci-dessus).
4. Lancez une exécution immédiate des contrôles concernés (§ 6.6.5) pour confirmer le bon fonctionnement.

Entre les étapes 2 et 3, une exécution peut échouer avec le type d'erreur `auth_failed`. Si l'application le permet, désactivez temporairement les contrôles concernés pendant l'opération.

6.8.5 Supprimer un secret

`DELETE /api/v1/secrets/{name}` supprime un secret, avec l'en-tête `If-Match` portant l'`ETag` renvoyé par `GET /api/v1/secrets/{name}` (§ 6.3.5). La suppression est refusée (`409 Conflict`) tant qu'un contrôle le référence.

> **Avertissement** — Utilisez des **comptes de test dédiés** à la supervision, dotés des droits strictement nécessaires, et jamais des comptes nominatifs ou des comptes à privilèges. Pour les bases de données, privilégiez un compte en **lecture seule**. Une sonde est un équipement installé dans votre réseau : limiter ce que ses identifiants permettent limite les conséquences d'une compromission.

6.9 Paramètres de la sonde

Les paramètres système sont regroupés en sections, consultables et modifiables par un administrateur dans l'interface ou par `GET` et `PUT /api/v1/settings/{section}`.

Section	Contenu	Détail
`network`	Nom d'hôte, adressage DHCP ou statique, passerelle, serveurs DNS (IPv4 ou IPv6), publication mDNS, domaines de recherche DNS (`searchDomains`) ; objet `ipv6` : `enabled` (`false` par défaut), `mode` (`slaac` ou `static`), `address` (notation CIDR), `gateway`	Chapitre 5
`dot1x`	Authentification 802.1X de la prise Ethernet par certificat (EAP-TLS) : `enabled`, `identity`, `caRef` (autorité de certification du serveur RADIUS, importée dans la section `trust`). L'identifiant client (clé et certificat) se gère par les opérations du § 6.9.3	Chapitre 5
`time`	Serveurs NTP, fuseau horaire d'affichage	Chapitre 5

Section	Contenu	Détail
`proxy`	Proxy HTTP(S) sortant, authentification, exclusions	Chapitre 5
`retention`	Durées de conservation des exécutions, agrégats, artefacts, audit	Ci-dessous
`security`	Politique de session, verrouillage après échecs, liste des réseaux autorisés à administrer (`allowedNetworks`, IPv4 ou IPv6), redirection du port 80 (`httpRedirect`)	Chapitre 5
`ssh`	Activation temporaire du service SSH : `enabled`, `enabledUntil` (obligatoire à l'activation ; 4 h par défaut, 72 h au maximum), `authorizedKeys` (clés publiques autorisées), `locked` (verrouillage définitif : voir § 6.9.3)	Chapitre 5
`updates`	Politique de mises à jour : `security.mode` (`automatic` par défaut, ou `manual`) et `security.criticalPolicy` (`next-window` par défaut, ou `asap`) pour les correctifs de sécurité, avec `security.criticalStagger` (décalage fixe des activations `asap`, `0` par défaut, `4h` au maximum, § 8.4.11) ; `feature.mode` (`manual` par défaut, ou `automatic`) pour les versions fonctionnelles ; `windows` : 0 à 7 fenêtres de maintenance (`days`, `start` au format `HH:MM`, `duration`), **aucune par défaut** ; `notice` : préavis avant activation (`24h` par défaut, de `0` à `7d`) ; `drainTimeout` : délai de drainage (`5m` par défaut, `30m` au maximum) ; `repositoryUrl` : miroir interne facultatif	§ 8.4.2 et § 8.4.8
`license`	Lecture seule : édition, numéro de série, état du certificat d'édition ; aucune clé à saisir	§ 4.5
`trust`	Autorités de certification internes reconnues par la sonde (format PEM)	§ 5.7.3
`logging`	Persistance temporaire des journaux système (`persistentUntil`, 72 h au plus)	Chapitre 9

6.9.1 Modifier la configuration réseau : confirmation obligatoire

Une erreur de configuration réseau peut rendre la sonde injoignable. Pour éviter cette situation, une nouvelle configuration réseau s'applique en deux temps :

1. Enregistrez les paramètres (`PUT /api/v1/settings/network`), puis demandez leur application (`POST /api/v1/settings/network/apply`), qui renvoie un identifiant.
2. Reconnectez-vous à la sonde, à sa nouvelle adresse le cas échéant, et **confirmez** la configuration dans un délai de **120 secondes**.

Sans confirmation dans ce délai, la sonde revient automatiquement à la configuration précédente. Par l'API, la confirmation s'effectue par `POST /api/v1/settings/network/confirm`, appelé **depuis la nouvelle adresse** ; l'interface d'administration l'envoie automatiquement. La procédure complète figure au chapitre 5.

6.9.2 Rétention des données

Les durées de conservation par défaut sont présentées au § 3.12.1 du guide d'utilisation et de supervision. Elles se règlent dans la section `retention`. Exemple :

```json
{
  "runs": "30d",
  "hourlyAggregates": "400d",
  "artifacts": { "maxAge": "7d", "maxSize": "500MB" },
  "audit": "365d"
}
```

> **Attention** — Allonger la rétention des exécutions détaillées augmente l'espace occupé et le volume d'écritures sur la carte microSD. Avant de dépasser 30 jours, vérifiez l'espace disponible dans l'état de santé de la sonde (chapitre 8). Pour une analyse de long terme, préférez les agrégats horaires ou une plateforme d'observabilité (chapitre 2 du guide d'intégration et d'observabilité).

6.9.3 Opérations système

Certaines opérations d'administration ne modifient pas une section de paramètres : elles déclenchent une action ou importent un élément signé. Elles sont toutes réservées au rôle `admin` et enregistrées dans le journal d'audit (§ 6.10). Le tableau suivant les recense ; leurs procédures complètes figurent dans les chapitres indiqués.

Opération	Appel	Détail
Consulter l'état des mises à jour : version de chaque emplacement système, emplacement actif, mises à jour disponibles, fin de la période de support (`supportEndsAt`) et du justificatif de maintenance (`maintenanceEndsAt`) ; état de la mise à jour en attente (`state`), activation annoncée (`scheduledActivation`) et report en cours (`postponedUntil`)	`GET /api/v1/updates`	Chapitre 8
Activer la mise à jour installée sur l'emplacement inactif, immédiatement, ou à une heure choisie avec le corps facultatif `{"scheduledAt": "<date RFC 3339>"}`	`POST /api/v1/updates/apply`	§ 8.4.3
Reporter l'activation prévue jusqu'à une date donnée : corps `{"until": "<date RFC 3339>"}` ; 30 jours au plus pour un correctif ordinaire, 7 jours au plus pour un correctif critique	`POST /api/v1/updates/postpone`	§ 8.4.2
Importer le justificatif de maintenance, fichier signé distinct du certificat d'édition	`PUT /api/v1/system/maintenance`	Chapitre 8
Activer le SSD NVMe facultatif (§ 8.3.4) . Le corps de la requête confirme l'opération par le nom d'hôte de la sonde : `{"confirm": "<nom d'hôte>"}`	`POST /api/v1/system/storage/ssd`	Chapitre 8
Générer sur la sonde la clé et la demande de certificat (CSR) de l'identifiant client 802.1X (méthode recommandée)	`POST /api/v1/system/dot1x/csr`	Chapitre 5
Installer le certificat client signé (PEM) émis pour la dernière CSR, ou importer un PKCS#12 protégé (écriture seule : l'identifiant ne peut pas être relu)	`PUT /api/v1/system/dot1x/credential`	Chapitre 5
Verrouiller définitivement SSH, avec confirmation par le nom d'hôte : `{"confirm": "<nom d'hôte>"}`	`POST /api/v1/settings/ssh/lock`	Chapitre 5

> **Attention** — L'activation du SSD **formate** le SSD raccordé, migre les données de la sonde, puis la redémarre. Prévoyez une interruption des contrôles pendant la migration et le redémarrage. Le démarrage reste sur la microSD.

> **Avertissement** — Le verrouillage de SSH est **irréversible** : il ne peut être levé que par une réinitialisation usine, qui efface la configuration. Une fois SSH verrouillé, le support ne pourra plus intervenir par SSH ; la récupération du compte administrateur par code de récupération (§ 6.4.3) reste possible. Le verrouillage peut aussi être demandé dès la mise en service, par le fichier de provisionnement (`ssh.locked: true` , chapitre 4).

> **Information** — L'activation d'une mise à jour, c'est-à-dire le redémarrage sur la nouvelle version, n'a lieu que dans une fenêtre de maintenance définie dans la section `updates`, ou à la demande d'un administrateur (`POST /api/v1/updates/apply`, immédiatement ou à l'heure `scheduledAt`). Elle commence par un **état de maintenance** : aucune exécution nouvelle ne démarre, celles en cours disposent du délai `drainTimeout`, puis sont interrompues en `UNKNOWN` avec le type d'erreur `maintenance`, et `GET /health` répond `{"status": "MAINTENANCE"}` (code `503`). Cet état ne suffit pas à neutraliser les alertes de vos plateformes, car la sonde est injoignable pendant son redémarrage. Procédures complètes : chapitre 8 (§ 8.4.3, § 8.4.8 à § 8.4.10) ; neutralisation des alertes : chapitre 2 du guide d'intégration et d'observabilité.

6.10 Journal d'audit

Le **journal d'audit** enregistre toutes les opérations d'administration, avec pour chacune :

- la date ;
- l'auteur, utilisateur ou jeton ;
- l'adresse d'origine ;
- l'action, l'objet concerné et le résultat ;
- pour une modification, la différence entre l'ancienne et la nouvelle configuration, **sans les valeurs des secrets**.

Événements enregistrés :

Catégorie	Exemples
Authentification	Connexions réussies et échouées, blocages
Configuration	Création, modification, suppression de contrôles, plans, destinations d'export, paramètres
Secrets	Création, rotation, suppression (sans valeur)
Code exécutable	Téléversement de scripts et de plugins
Comptes et jetons	Création, suppression, révocation
Système	Mises à jour, réinitialisation, activation, désactivation et verrouillage de SSH, connexions SSH, import de configuration, import du justificatif de maintenance, activation du SSD, gestion de l'identifiant 802.1X, récupération d'un compte administrateur
Mises à jour et maintenance	Modification de la section `updates` ; annonce d'une activation (événement `update.scheduled`), qu'elle provienne d'une fenêtre ou d'une demande d'un administrateur (`scheduledAt`) ; report d'une activation (`POST /api/v1/updates/postpone`) ; début et fin de l'état de maintenance ; résultat de l'activation, retour arrière compris

Le journal se consulte dans l'interface ou par `GET /api/v1/audit-events` (rôle `admin`). Il est conservé 365 jours par défaut. Il peut aussi être transmis sous forme de logs à votre plateforme d'observabilité ou à votre outil de gestion des événements de sécurité (SIEM), par une destination d'export OpenTelemetry dont l'option `logs.audit` est fixée à `true` (chapitre 2 du guide d'intégration et d'observabilité). Cet export est désactivé par défaut.

```bash
# Opérations de la dernière journée (filtres disponibles : from, to, actor, action)
sapi "$SONDE/api/v1/audit-events?from=2025-11-18T00:00:00Z&limit=100" | jq '.items[]'
```

6.11 Événements en temps réel

L'adresse `GET /api/v1/events` diffuse les événements de la sonde en temps réel, selon le protocole **Server-Sent Events** (SSE). Une connexion HTTP reste ouverte, et la sonde y envoie chaque événement dès qu'il se produit.

Événement	Émis quand
`run.started`	Une exécution démarre
`run.finished`	Une exécution se termine, avec son état
`check.status.changed`	L'état courant d'un contrôle change, par exemple de `OK` à `CRITICAL`
`system.alert`	La sonde signale une anomalie la concernant : espace disque, mémoire, défaillance d'un composant, échec d'export

Exemple d'écoute depuis un terminal (l'option `-N` désactive la mise en mémoire tampon) :

```bash
sapi -N -H 'Accept: text/event-stream' "$SONDE/api/v1/events"
```

L'interface d'administration utilise ce flux pour actualiser le tableau de bord sans rechargement. Il peut aussi alimenter un écran de supervision local ou un outil interne.

> **Information** — Ce flux est destiné à l'observation en direct. Il n'est pas conçu pour l'archivage : un événement émis pendant une déconnexion n'est pas renvoyé. Pour l'historique, utilisez `GET /api/v1/runs` ou une plateforme d'observabilité.

6.12 Sauvegarde et restauration de la configuration

6.12.1 Ce qui est sauvegardé

La sonde réalise **automatiquement** une sauvegarde quotidienne de sa configuration et en conserve trois générations. Ces sauvegardes, stockées sur la sonde, lui permettent de se rétablir seule en cas de corruption de sa base (chapitre 8). Elles ne protègent pas contre la perte ou la panne de la carte microSD : réalisez donc aussi des **exports** conservés hors de la sonde.

Contenu de l'export	Inclus
Contrôles, plans d'exécution, scripts	Oui
Destinations d'export	Oui
Paramètres (heure, proxy, rétention, sécurité, autorités de certification `trust`, mises à jour, journaux, SSH)	Oui, **sauf** la section `network`, propre à chaque appareil ; le verrouillage SSH (`ssh.locked`) est ignoré à l'import
Comptes utilisateurs	Inclus, sous forme d'empreintes, uniquement avec une phrase de passe
Secrets	**Exclus**, ou inclus **chiffrés** (AES-256-GCM, clé dérivée par Argon2id) avec une phrase de passe que vous fournissez. Chaque secret y est conservé avec sa liste `allowedHosts`, restaurée à l'import
Historique des exécutions et artefacts	Non

6.12.2 Exporter

Objectif : conserver une copie de la configuration hors de la sonde.

Prérequis : rôle `admin`.

Étapes :

1. Lancez l'export depuis l'interface, ou par l'API :

   ```bash
   sapi -o "sonde-paris-01-config-$(date +%Y%m%d).json" \
     "$SONDE/api/v1/config/export"
   ```

   Pour inclure les comptes et les secrets, chiffrés, envoyez la demande d'export en `POST` avec la phrase de passe dans l'en-tête `X-Config-Passphrase`, comme pour l'import (§ 6.12.3), et jamais dans l'adresse, qui peut être journalisée. La phrase de passe est lue sans affichage, puis placée dans un fichier d'en-tête temporaire, lisible par vous seul et supprimé aussitôt, pour ne figurer dans les arguments d'aucune commande (même méthode qu'au § 6.3.3) :

   ```bash
   (
     umask 077
     ENTETE=$(mktemp) && trap 'rm -f "$ENTETE"' EXIT &&
     IFS= read -rs PHRASE &&
     printf 'X-Config-Passphrase: %s\n' "$PHRASE" > "$ENTETE" &&
     unset PHRASE &&
     sapi -X POST -H @"$ENTETE" \
       -o "sonde-paris-01-config-$(date +%Y%m%d).json" \
       "$SONDE/api/v1/config/export"
   )
   ```

2. Stockez le fichier dans un emplacement sauvegardé et à accès restreint.

Fréquence recommandée : après chaque série de modifications importantes, et au minimum une fois par mois.

> **Avertissement** — Un export contenant des secrets chiffrés n'est protégé que par la robustesse de sa phrase de passe. Choisissez une phrase longue, conservez-la séparément du fichier, par exemple dans le coffre-fort de mots de passe de l'équipe.

6.12.3 Restaurer ou dupliquer une configuration

L'import permet de :

- restaurer une configuration sur une sonde réinstallée (chapitre 8) ;
- dupliquer une configuration vers une nouvelle sonde ;
- déployer une configuration de référence sur plusieurs sondes.

Étapes :

1. **Validez** d'abord l'import sans l'appliquer :

   ```bash
   sapi -X POST -H 'Content-Type: application/json' \
     --data-binary @sonde-paris-01-config-20261119.json \
     "$SONDE/api/v1/config/import?dryRun=true"
   ```

L'archive importée a le même format JSON que l'export. Si elle contient des comptes et des secrets chiffrés, transmettez la phrase de passe dans l'en-tête `X-Config-Passphrase`, selon la méthode du § 6.12.2 : reprenez la commande d'export en remplaçant l'appel à `config/export` par la commande d'import ci-dessus, complétée de l'option `-H @"$ENTETE"`. Comme à l'export, la phrase de passe ne doit jamais figurer dans l'adresse, qui peut être journalisée. Pour appliquer la configuration à une sonde qui fonctionnera en parallèle de la sonde d'origine, ajoutez le paramètre `newIdentity=true` (§ 8.5.3). La réponse est un compte rendu JSON qui liste les objets qui seraient créés, modifiés ou supprimés, ainsi que les éventuelles erreurs (fonction absente de l'édition, secret manquant…).

2. Si le rapport est conforme, relancez la même commande sans `?dryRun=true`.
3. Si les secrets n'étaient pas inclus, recréez-les (§ 6.8.2). Tant qu'un secret référencé par un contrôle est absent de la sonde, chaque exécution de ce contrôle se termine en `UNKNOWN` avec le type d'erreur `secret_missing` (§ 8.1 de la référence technique et API). Si l'archive est antérieure à la liste `allowedHosts`, définissez la liste de chaque secret signalé par le compte rendu d'import avant de compter sur les contrôles qui l'utilisent (§ 6.8.1).
4. Vérifiez par quelques exécutions d'essai que les contrôles fonctionnent.

> **Attention** — L'export n'inclut pas la section `network` (nom d'hôte, adresse IP, DNS) : la sonde cible conserve ses propres paramètres réseau. Lors d'une duplication, vérifiez en revanche les paramètres propres à chaque site (rattachement, attributs de ressource), et utilisez `newIdentity=true` pour que les deux sondes restent distinctes dans les plateformes d'observabilité.

6.13 Automatisation

6.13.1 Principe de la configuration en tant que code

Pour un parc de plusieurs sondes, ou pour une configuration soumise à revue, il est recommandé de gérer les définitions de contrôles comme du **code** :

1. les fichiers JSON des contrôles et des plans sont conservés dans un dépôt Git ;
2. toute modification fait l'objet d'une revue ;
3. un outil d'automatisation applique les définitions sur les sondes par l'API.

Cette approche garantit la traçabilité, la reproductibilité et le retour arrière.

6.13.2 Exemple avec un script shell

Le script suivant, illustratif, crée ou remplace tous les contrôles décrits dans un répertoire `controles/` (un fichier JSON par contrôle). Il s'appuie sur la préparation du § 6.3.3 (variables `SONDE` et `CA`, fichier d'en-tête `entete-auth`), mais définit sa propre fonction d'appel : contrairement à `sapi`, elle récupère le code HTTP de chaque réponse pour décider de la suite.

```bash
#!/usr/bin/env bash
# Déploiement idempotent des contrôles d'un répertoire sur une sonde (exemple)
# Prérequis (§ 6.3.3) : variables SONDE et CA définies, fichier "$HOME/.sva/entete-auth".
set -euo pipefail
shopt -s nullglob                    # motif sans correspondance => liste vide

fichiers=(controles/*.json)
if [ "${#fichiers[@]}" -eq 0 ]; then
  echo "Aucun fichier controles/*.json : rien à déployer." >&2
  exit 1
fi
```

```
tmp=$(mktemp -d)
trap 'rm -rf "$tmp"' EXIT

# Appel de l'API. Positionne deux variables, à tester dans cet ordre :
#   rc   : statut de sortie de curl (0 = transfert complet ; sinon transfert
#          interrompu, erreur TLS, sonde injoignable ou erreur d'écriture locale) ;
#   code : code HTTP reçu (000 si aucun). Un code peut avoir été reçu avant
#          l'interruption du transfert : il n'est fiable que si rc vaut 0.
# Les en-têtes et le corps de la réponse sont conservés dans $tmp.
appel() {
  rm -f "$tmp/entetes" "$tmp/corps"
  rc=0
  code=$(curl -sS --cacert "$CA" -H @"$HOME/.sva/entete-auth" \
              -H 'Accept: application/json' \
              -D "$tmp/entetes" -o "$tmp/corps" -w '%{http_code}' "$@") || rc=$?
}

# Arrêt du déploiement avec le détail renvoyé par la sonde
echec() {
  echo "ERREUR : $1" >&2
  [ -s "$tmp/corps" ] && cat "$tmp/corps" >&2
  exit 1
}

for f in "${fichiers[@]}"; do
  id=$(jq -er '.id' "$f") || echec "$f : identifiant (.id) absent ou JSON invalide"

  # 1. Lecture : transfert d'abord, puis 200 = le contrôle existe, 404 = il n'existe pas
  appel "$SONDE/api/v1/checks/$id"
  [ "$rc" -eq 0 ] ||
    echec "$id : lecture inachevée (curl $rc, HTTP $code) : sonde injoignable, TLS refusé ou
    transfert interrompu ; rien n'a été écrit"
  case "$code" in
    200)
      etag=$(awk 'tolower($1)=="etag:" {print $2}' "$tmp/entetes" | tr -d '\r')
      [ -n "$etag" ] || echec "$id : lecture réussie mais en-tête ETag absent"
      echo "Mise à jour : $id"
      appel -X PUT -H 'Content-Type: application/json' \
            -H "If-Match: $etag" --data-binary @"$f" \
            "$SONDE/api/v1/checks/$id"
      ;;
    404)
      echo "Création   : $id"
      appel -X POST -H 'Content-Type: application/json' \
            --data-binary @"$f" "$SONDE/api/v1/checks"
      ;;
    *) echec "$id : lecture refusée ou impossible (HTTP $code)" ;;
  esac

  # 2. Résultat de l'écriture : transfert d'abord, code HTTP ensuite.
  # Transfert inachevé : l'écriture a pu être appliquée ou non. Arrêt sans
  # réessai ; relisez le contrôle avant de relancer (voir ci-dessous).
  [ "$rc" -eq 0 ] ||
    echec "$id : résultat de l'écriture indéterminé (curl $rc, HTTP $code) ; relisez le contrôle
    avant tout nouvel essai"
  case "$code" in
    2??) ;;                                  # 200, 201 ou 204 : succès
    409) echec "$id : conflit (409), voir la conduite à tenir ci-dessous" ;;
    412) echec "$id : modifié depuis la lecture (412) ; relancez le script" ;;
    *)   echec "$id : écriture refusée (HTTP $code)" ;;
  esac
done
```

Le script distingue explicitement les réponses de la sonde, au lieu de déduire l'absence d'un contrôle d'un échec quelconque de la lecture :

Réponse à la lecture (`GET`)	Conduite du script
`200 OK`	Le contrôle existe. L'en-tête `ETag` est **exigé** ; il est renvoyé dans `If-Match` avec le `PUT` (§ 6.3.5). Son absence arrête le script
`404 Not Found`	Le contrôle n'existe pas : il est créé par `POST`
Transfert inachevé (statut de sortie de `curl` non nul : sonde injoignable, certificat refusé, transfert interrompu, erreur d'écriture locale), **même si un code HTTP a été reçu**	Arrêt immédiat. Le code reçu n'est pas exploité : un `200` ou un `404` suivi d'une interruption ne prouve rien. Aucune écriture n'est tentée
`401`, `403`, `429`, `5xx` ou tout autre code, transfert complet	Arrêt immédiat, avec le détail renvoyé par la sonde. Aucune création n'est tentée
Aucun fichier `controles/*.json`	Arrêt avec un message : grâce à l'option `nullglob`, le motif n'est jamais traité comme un nom de fichier littéral

Pour l'écriture (`PUT` ou `POST`), le script examine aussi le transfert **avant** le code HTTP. Si le transfert est inachevé, le résultat est **indéterminé** : la sonde a pu appliquer l'écriture sans que la réponse soit reçue en entier, ou ne pas l'avoir reçue. Le script s'arrête alors sans réessai et sans compter l'écriture comme réussie. Avant de relancer, relisez le contrôle (`GET /api/v1/checks/{id}`) et comparez-le au fichier du dépôt, ou consultez le journal d'audit (§ 6.10) : vous saurez ainsi si l'écriture a eu lieu. La relance du script reste sûre dans les deux cas, puisqu'elle relit le contrôle avant d'écrire.

Conduite à tenir après un refus de l'écriture :

- **`409 Conflict`** : l'opération est incompatible avec l'état de la sonde. Lors d'une création, l'identifiant a pu être créé entre la lecture et l'écriture, par une autre personne ou un autre outil : relancez le script, qui empruntera alors le chemin de mise à jour. Si le conflit persiste, lisez le détail (`application/problem+json`) : il désigne l'objet en cause, par exemple une référence incompatible avec l'état actuel de la configuration. Corrigez la définition dans le dépôt avant de relancer ;
- **`412 Precondition Failed`** : le contrôle a été modifié entre la lecture et l'écriture. Consultez le journal d'audit (§ 6.10) pour identifier cette modification. Si elle doit être conservée, reportez-la dans le fichier du dépôt ; sinon, relancez simplement le script, qui relit le contrôle et obtient un nouvel `ETag`. Ne contournez jamais ce refus en supprimant l'en-tête `If-Match` ;
- **`422 Unprocessable Content`** : la définition n'est pas conforme au schéma ; corrigez le fichier.

> ! **Attention** — Le script s'arrête à la première erreur : les contrôles traités avant l'erreur restent déployés. Comme il est idempotent, il suffit de le relancer après correction. Les codes de réponse attendus en cas de succès (`200`, `201`, `204`) sont ceux du § 6.3.4.

6.13.3 Exemple avec Ansible

Avec Ansible, le module standard `ansible.builtin.uri` permet d'appeler l'API. L'exemple ci-dessous, illustratif, crée un contrôle s'il n'existe pas. Le jeton est conservé dans un coffre Ansible (`ansible-vault`) et le certificat de la sonde est vérifié.

```yaml
# Exemple illustratif : création d'un contrôle sur les sondes de l'inventaire
- name: Contrôles de supervision
  hosts: sondes
  gather_facts: false
```

```
vars:
  sonde_url: "https://{{ inventory_hostname }}"
  sonde_ca: "files/ca-sondes.pem"          # certificat de l'AC ou de la sonde
  sonde_token: "{{ vault_sonde_token }}"    # jeton chiffré par ansible-vault
tasks:
  - name: Vérifier si le contrôle existe
    no_log: true                            # la tâche manipule le jeton
    ansible.builtin.uri:
      url: "{{ sonde_url }}/api/v1/checks/portail-accueil"
      headers: { Authorization: "Bearer {{ sonde_token }}" }
      ca_path: "{{ sonde_ca }}"
      status_code: [200, 404]
    delegate_to: localhost
    register: existant

  - name: Créer le contrôle
    no_log: true                            # la tâche manipule le jeton
    ansible.builtin.uri:
      url: "{{ sonde_url }}/api/v1/checks"
      method: POST
      headers: { Authorization: "Bearer {{ sonde_token }}" }
      ca_path: "{{ sonde_ca }}"
      body_format: json
      body: "{{ lookup('ansible.builtin.file', 'controles/portail-accueil.json') | from_json }}"
      status_code: 201
    delegate_to: localhost
    when: existant.status == 404
```

Les appels sont délégués au poste de contrôle Ansible (`delegate_to: localhost`) : la sonde est administrée par son API, et non par SSH, qui reste désactivé.

> **Attention** — Le jeton est chiffré dans le coffre Ansible, mais il est déchiffré en mémoire pour construire l'en-tête `Authorization`. Sans précaution, Ansible peut l'afficher en clair dans ses sorties : résultat d'une tâche en échec, mode verbeux (`-v` à `-vvvv`), variable enregistrée par `register` et affichée par `debug`, journal configuré par `log_path`, ou greffon de rappel (*callback*) qui transmet les résultats à un outil tiers. C'est pourquoi **chaque tâche qui manipule le jeton porte `no_log: true`**. Cette option masque aussi le détail des erreurs : pour diagnostiquer un échec, rejouez l'appel avec `curl` selon la méthode du § 6.3.3, plutôt que de retirer `no_log`. N'affichez jamais la variable `existant` avec le module `debug`.

6.13.4 Règles pour une automatisation sûre

Règle	Raison
Utiliser un jeton dédié, de rôle `operator` si possible	Limiter les conséquences d'une fuite du jeton
Vérifier le certificat de la sonde	Éviter l'interception du jeton
Ne jamais placer le jeton dans les arguments d'une commande : fichier d'en-tête protégé (§ 6.3.3), `no_log: true` dans Ansible (§ 6.13.3)	Éviter sa divulgation dans la liste des processus, l'historique ou les journaux
Respecter `If-Match`	Ne pas écraser une modification manuelle concurrente
Valider avec `dryRun` avant d'appliquer à grande échelle	Détecter les erreurs avant leur déploiement
Limiter le rythme des appels	Éviter les réponses `429`
Conserver les secrets hors du dépôt	Les créer par un canal séparé (§ 6.8)

6.14 Gestion centralisée de plusieurs sondes

La console centrale est une évolution prévue et facultative du produit (§ 7.1.4) : elle n'est pas disponible dans la version actuelle, et aucune fonction décrite dans cette documentation n'en dépend. Cette section en présente le principe pour vous permettre d'anticiper son intégration.

> → **Évolution prévue** — Une **console centrale** facultative permettra, dans une version ultérieure, de gérer un parc de sondes depuis un point unique : inventaire, déploiement de configurations, vue consolidée des états. Elle sera proposée au choix en service hébergé (SaaS), à l'adresse réservée `https://fleet-synovex.incitypark.fr`, ou installée sur l'infrastructure du client.

Les principes retenus pour cette console sont les suivants :

Principe	Conséquence
La console est **facultative**	Une sonde sans console fonctionne exactement comme décrit dans cette documentation
La sonde **initie la connexion**, en HTTPS sortant, avec authentification mutuelle par certificat (mTLS)	Aucun port entrant à ouvrir depuis Internet ; compatibilité avec les proxys d'entreprise
La sonde **récupère périodiquement** sa configuration de référence et la valide avant de l'appliquer	Une configuration invalide est rejetée ; la précédente reste en vigueur
La console injoignable **n'interrompt pas** la supervision	La sonde continue avec la dernière configuration appliquée
Les résultats détaillés **restent sur la sonde** et dans vos plateformes d'observabilité	La console ne reçoit qu'une synthèse

D'ici là, la gestion d'un parc repose sur l'API de chaque sonde et sur vos outils d'automatisation (§ 6.13).

Chapitre 7 — Éditions et périmètre fonctionnel

7.1 Périmètre de la solution

7.1.1 Éditions

Les fonctions disponibles dépendent de l'édition acquise : SYNOVEX Essential, SYNOVEX Professional ou SYNOVEX Enterprise. Dans les tableaux de cette documentation, les éditions sont désignées par leur seul nom (Essential, Professional, Enterprise). Toutes les éditions partagent le même système. L'édition est inscrite sur la carte microSD lors de sa préparation, sous la forme d'un **certificat d'édition** qui active les modules correspondants : aucune clé n'est à saisir et aucune activation en ligne n'est nécessaire. Le droit d'utilisation du logiciel intégré est perpétuel : il ne nécessite ni abonnement ni renouvellement. Chaque version majeure bénéficie d'une période de support d'au moins cinq ans, dont la date de fin vous est indiquée à l'achat : pendant cette période, les correctifs de sécurité sont publiés pour toutes les sondes. Un contrat de maintenance facultatif donne en outre accès aux nouvelles versions fonctionnelles ; son échéance n'affecte aucune fonction acquise (§ 8.4.7). Pour passer à une édition supérieure, vous remplacez la carte par une carte de cette édition et vous y transférez votre configuration (§ 8.6), sous réserve que le Raspberry Pi 5 corresponde aux exigences de l'édition visée (chapitre 2).

Fonction	Essential	Professional	Enterprise
Contrôles ICMP, TCP, DNS	Oui	Oui	Oui
Contrôles HTTP/HTTPS, y compris vérification du contenu et du certificat	Oui	Oui	Oui
Plugins compatibles Nagios fournis avec la sonde	Oui	Oui	Oui
Plugins compatibles Nagios personnalisés	—	Oui	Oui
Contrôles d'API (suites de requêtes, extraction de valeurs)	—	Oui	Oui
Contrôles de bases de données (PostgreSQL, MySQL/MariaDB, SQL Server, Oracle) et indicateurs métier	—	Oui	Oui
Scénarios navigateur déclaratifs et scriptés (Puppeteer, Chromium headless)	—	—	Oui
Interface d'administration, API REST, planification, plans d'exécution, historique local	Oui	Oui	Oui
Export OpenTelemetry (OTLP), endpoint Prometheus, plugin Nagios/Centreon	Oui	Oui	Oui

Aucune édition n'impose de limite technique au nombre de contrôles ou de scénarios navigateur. La capacité réelle dépend du matériel, de la fréquence et de la durée des contrôles : la méthode de dimensionnement (calcul de la charge, seuils à respecter, surveillance dans la durée) figure au § 6.6 du guide d'utilisation et de supervision, et le § 10.1 récapitule, sous forme d'aide-mémoire, les prérequis et la configuration matérielle minimale.

7.1.2 Offres matérielles

La sonde est proposée sous deux formes :

Offre	Contenu	Ce que vous fournissez
microSD préconfigurée	Carte microSD contenant le système et le logiciel de la sonde	Raspberry Pi 5 de capacité mémoire adaptée à l'édition, alimentation, refroidissement, boîtier, câble Ethernet

Offre	Contenu	Ce que vous fournissez
Boîtier complet	Raspberry Pi 5 assemblé dans son boîtier, refroidissement, carte microSD installée	Alimentation et câble Ethernet, sauf mention contraire de la liste de colisage jointe au boîtier et de votre bon de commande ; emplacement d'installation

Un SSD NVMe facultatif, monté sur la carte d'extension M.2 HAT+ officielle de Raspberry Pi, peut compléter la carte microSD comme volume de données. Il est surtout utile pour l'édition Enterprise ; la carte microSD reste le support principal et suffit à un usage standard (§ 8.3.4).

Le contenu exact de chaque offre et les références de matériel sont détaillés au chapitre 2.

> **Information** — SYNOVEX est conçu et documenté pour Raspberry Pi 5. Son architecture logicielle peut permettre une utilisation sur d'autres ordinateurs monocartes, notamment certains modèles Orange Pi. Toutefois, ces plateformes n'ont pas fait l'objet d'une validation officielle et leur fonctionnement n'est pas garanti. SYNOVEX est pris en charge exclusivement sur **Raspberry Pi 5** raccordé en **Ethernet** (§ 2.1.5).

7.1.3 Ce que la sonde fait et ne fait pas

La sonde **observe depuis l'extérieur** le comportement des services, à la manière d'un utilisateur ou d'une application cliente. Elle n'installe aucun agent sur les serveurs supervisés et n'a pas besoin d'accès privilégié à ces serveurs. En contrepartie, elle ne mesure pas l'utilisation du processeur, de la mémoire ou des disques des serveurs : cette supervision des ressources reste du ressort de vos outils existants, que la sonde complète sans les remplacer (chapitre 1 du guide d'utilisation et de supervision).

La sonde n'est pas non plus un outil de test de charge. Ses contrôles sont volontairement peu fréquents et légers, pour ne pas perturber les services observés. Elle n'est pas davantage un outil de mesure de l'expérience des utilisateurs réels : elle mesure des parcours représentatifs, reproduits à l'identique, ce qui la rend complémentaire des solutions de mesure en conditions réelles (§ 1.6.3 du guide d'utilisation et de supervision).

7.1.4 Évolutions prévues

Les évolutions suivantes sont envisagées pour des versions ultérieures. Elles ne font pas partie des fonctions actuelles de la sonde : ne les prenez pas en compte pour préparer un déploiement.

- **Console centrale.** Une console centrale facultative permettra de gérer plusieurs sondes depuis un point unique. Elle sera hébergée par l'éditeur ou installée dans votre infrastructure, au choix. La sonde restera pleinement autonome : la console ne sera jamais nécessaire à son fonctionnement. L'adresse de la console hébergée par l'éditeur est réservée (`https://fleet-synovex.incitypark.fr`) ; la sonde ne l'utilise pas.
- **Connexion Wi-Fi.** La sonde se raccorde aujourd'hui exclusivement en Ethernet ; une connexion Wi-Fi est à l'étude.

Chapitre 8 — Maintenance et mises à jour

Une sonde de supervision fonctionne en continu, sans surveillance directe, souvent pendant plusieurs années. Sa fiabilité dépend de quelques opérations simples mais régulières : arrêter l'appareil proprement, protéger son support de stockage, appliquer les mises à jour, sauvegarder la configuration, renouveler les secrets et adapter les scénarios aux évolutions des applications.

Ce chapitre décrit ces opérations et propose, au § 8.11, un plan de maintenance préventive.

> **Information** — Les exemples de ce chapitre utilisent des noms et adresses fictifs (`sonde-paris-01.example.internal`) et suivent la convention du chapitre 6 (§ 6.3.3) : la variable `SONDE` contient l'adresse de la sonde, la variable `CA` le chemin de son certificat, récupéré et vérifié selon le chapitre 4 (§ 4.4.4), et la fonction `sapi` appelle l'API avec ce certificat et le jeton lu dans le fichier d'en-tête protégé `$HOME/.sva/entete-auth`. Le jeton n'apparaît ainsi jamais dans la ligne de commande.

8.1 Répartition des responsabilités

Domaine	Éditeur	Client
Système d'exploitation, moteur principal, moteur de scénarios, Chromium	Publie des images système signées et validées ; publie les correctifs de sécurité pendant toute la période de support (§ 8.4.6)	Choisit le mode de chaque canal, définit les fenêtres de maintenance et le préavis, active ou laisse activer les mises à jour (§ 8.4.2)
Matériel	Garantie du boîtier complet, selon les conditions de votre contrat	Environnement d'installation, alimentation, refroidissement ; matériel fourni par le client dans l'offre microSD préconfigurée
Configuration (contrôles, plans, destinations)	—	Conception, sauvegarde, évolution
Scénarios	Exemples et documentation	Maintenance au rythme des évolutions applicatives
Secrets et comptes de test	—	Création, rotation, révocation
Sauvegardes	Sauvegarde automatique locale de la configuration	Export régulier hors de la sonde

8.2 Arrêt et redémarrage

8.2.1 Pourquoi un arrêt propre est indispensable

La sonde écrit en permanence sur son support de stockage : résultats, historique, journaux d'exécution. Couper l'alimentation sans arrêt préalable interrompt ces écritures. Les mécanismes de la sonde (base de données transactionnelle, écritures atomiques des fichiers de configuration, récupération automatique au démarrage) limitent fortement le risque, mais ne l'éliminent pas. Des coupures répétées peuvent abîmer le système de fichiers ou la carte microSD elle-même.

> **Avertissement** — Ne débranchez jamais l'alimentation d'une sonde en fonctionnement, sauf en cas d'urgence (fumée, odeur de brûlé, liquide renversé). Arrêtez d'abord la sonde, puis attendez l'extinction complète avant de débrancher.

8.2.2 Arrêter la sonde

Objectif : mettre la sonde hors tension sans risque pour les données.

Prérequis : compte de rôle `admin` (arrêt par l'API ou l'interface).

Étapes

1. Informez les équipes qui exploitent les alertes : pendant l'arrêt, la sonde n'exécute plus aucun contrôle et peut apparaître `STALE` dans les plateformes de supervision.
2. Si votre plateforme le permet, planifiez une période de maintenance pour éviter les fausses alertes.
3. Déclenchez l'arrêt par l'une des méthodes suivantes :
   - depuis l'interface d'administration, fonction d'arrêt de la sonde ;
   - par l'API : `POST /api/v1/system/shutdown` (réponse `202 Accepted`, l'arrêt suit dans les secondes qui viennent) ;
   - par un appui bref sur le bouton d'alimentation du Raspberry Pi 5, qui déclenche l'arrêt propre (comportement standard de Raspberry Pi OS Lite). Un appui long force la coupure sans arrêt propre : réservez-le aux situations où le système ne répond plus ;
   - en dernier recours, par SSH (si activé) : `sudo systemctl poweroff`.
4. Attendez que le voyant d'état cesse de clignoter et reste allumé en rouge fixe, signe que le système est arrêté (comportement standard du Raspberry Pi 5 : le voyant passe au rouge en veille basse consommation ; l'image de la sonde n'ajoute aucune signalisation propre).
5. Débranchez l'alimentation.

Résultat attendu : la sonde est éteinte et ne répond plus à `GET /health`.

Vérification : au redémarrage suivant, aucun message de récupération de base n'apparaît dans le journal d'audit.

8.2.3 Redémarrer la sonde

Le redémarrage est utile après certaines mises à jour, ou pour rétablir un fonctionnement normal après une saturation de ressources.

1. Déclenchez le redémarrage depuis l'interface d'administration, par l'API (`POST /api/v1/system/reboot`, rôle `admin`) ou, si SSH est activé, par `sudo systemctl reboot`.
2. Attendez le retour de la sonde : `GET /health` répond de nouveau en `200`.
3. Vérifiez dans le tableau de bord que les contrôles reprennent. Après un redémarrage, la sonde recalcule les échéances avec un léger décalage aléatoire, pour ne pas lancer tous les contrôles en même temps. Les exécutions manquées pendant l'arrêt ne sont pas rattrapées.

> **Information** — Une exécution en cours au moment du redémarrage est close avec l'état `UNKNOWN` et le type d'erreur `agent_restart`. Ce n'est pas un incident de la ressource supervisée.

8.2.4 Redémarrages automatiques

La sonde redémarre ses services automatiquement en cas de défaillance logicielle, et l'appareil complet en cas de blocage système (chien de garde matériel). Ces redémarrages sont visibles dans les métriques et le journal d'audit. S'ils se répètent, recherchez une cause matérielle (alimentation, chaleur, carte) avec le chapitre 9.

8.2.5 Coupures électriques

Après une coupure secteur, la sonde redémarre automatiquement dès le retour du courant et reprend ses contrôles sans intervention. Au démarrage, elle vérifie l'intégrité de sa base de données et la restaure si nécessaire à partir de la dernière sauvegarde de configuration (§ 8.5.1).

> ✓ **Conseil** — Branchez la sonde sur une alimentation secourue (onduleur) partagée avec les équipements réseau qui la desservent. C'est la mesure la plus efficace pour préserver la carte microSD, et la sonde continue de superviser pendant les micro-coupures.

8.3 Protection du support de stockage

8.3.1 Comprendre l'usure d'une carte microSD

Une carte microSD utilise de la mémoire flash, dont chaque cellule supporte un nombre limité de cycles d'écriture. Une carte conçue pour un appareil photo n'est pas prévue pour des écritures continues 24 heures sur 24. La sonde réduit volontairement ses écritures :

Mesure intégrée	Effet
Système installé sur une partition en **lecture seule**, données placées sur une partition séparée (ou sur le SSD, § 8.3.4)	Aucune écriture sur la partition système en fonctionnement normal : une coupure n'interrompt aucune écriture du système. Cette protection ne couvre ni une défaillance du support lui-même, ni les écritures légitimes d'une mise à jour sur l'emplacement inactif ; les données restent sur une partition écrite en continu (§ 8.2.5)
Journaux système conservés en mémoire par défaut	Supprime la principale source d'écritures continues
Profil et cache de Chromium en mémoire, détruits après chaque exécution	Aucune écriture disque liée à la navigation
Fichiers temporaires en mémoire	Idem
Regroupement des écritures de résultats	Moins d'opérations d'écriture
Captures d'écran produites seulement en cas d'échec, avec quota	Volume maîtrisé
Purge automatique selon la rétention	Pas de saturation

8.3.2 Recommandations

Recommandation	Justification
Utiliser exclusivement la carte fournie par l'éditeur ; toute carte de remplacement s'obtient selon le § 8.6.4 (une carte achetée ailleurs démarrerait en mode restreint)	La carte fournie, de type « High Endurance », est conçue pour les écritures continues et porte le certificat d'édition

Recommandation	Justification
Pour l'édition Enterprise avec des parcours navigateur fréquents, envisager un SSD NVMe facultatif (carte M.2 HAT+ officielle) comme volume de données. La microSD reste le support principal et suffit à un usage standard	Le SSD reçoit les écritures les plus volumineuses (historique, captures, journaux) et soulage la microSD. Le système continue de démarrer sur la microSD. Activation : § 8.3.4
Protéger l'alimentation (onduleur)	Les coupures sont la première cause de corruption
Ne pas allonger inutilement la rétention	Moins d'écritures et de volume
Ne pas activer durablement les journaux persistants	Réservés aux diagnostics ponctuels
Conserver une carte de rechange préparée (voir § 8.6)	Réduit la durée d'interruption

8.3.3 Durée de vie

La durée de vie d'une carte dépend du nombre de contrôles, de leur fréquence et de la rétention. Elle n'est pas garantie : surveillez les signes d'usure ci-dessous et évaluez chaque année le remplacement préventif de la carte selon l'usage (§ 8.11). Signes d'une carte en fin de vie : erreurs d'entrée/sortie dans les journaux du noyau, redémarrages spontanés, partition de données remontée en lecture seule (la partition système, elle, est en lecture seule par conception), lenteurs inexpliquées (§ 9.3 et § 9.6).

8.3.4 Activer un SSD NVMe

Un SSD NVMe peut compléter la microSD, et dans toutes les éditions. Il est surtout utile pour l'édition Enterprise, dont les scénarios navigateur produisent davantage d'écritures. Il est **facultatif** : la microSD reste le support principal et suffit à un usage standard.

Rôle du SSD. Le SSD sert exclusivement de **volume de données**. La répartition est la suivante :

Support	Contenu
SSD NVMe (s'il est activé)	Historique des exécutions, agrégats, artefacts (captures d'écran), file d'attente d'export, journaux persistants
microSD (toujours)	Partition de démarrage, deux emplacements système (§ 8.4.5), certificat d'édition, configuration et secrets

La sonde démarre toujours sur la microSD : l'activation du SSD ne modifie pas l'ordre de démarrage du Raspberry Pi 5. Le certificat d'édition reste attaché à la carte microSD et le mécanisme de mise à jour est inchangé.

Objectif : déplacer les données volumineuses de la sonde sur un SSD NVMe.

Prérequis

- Matériel monté selon le chapitre 3 : carte M.2 HAT+ officielle de Raspberry Pi, SSD M.2 au format 2230 ou 2242 figurant dans la liste des modèles pris en charge, indiquée dans les notes de version, alimentation officielle de 27 W. Le refroidisseur actif (*Active Cooler*), s'il est utilisé, est installé en premier. Le boîtier officiel n'est utilisable que sans couvercle ni ventilateur.
- Rôle `admin`.
- Export récent de la configuration (§ 8.5.2).
- Une période de maintenance planifiée dans vos plateformes de supervision : la sonde redémarre à la fin de l'opération.

> **Information** — La carte M.2 HAT+ fonctionne en PCIe 2.0 x1 (environ 500 Mo/s). Le mode PCIe Gen 3, non certifié par Raspberry Pi, n'est pas utilisé par la sonde. Ce débit est largement suffisant pour le rôle de volume de données.

> **Avertissement** — Le SSD est **entièrement formaté** lors de l'activation. Toute donnée qu'il contient est définitivement perdue. N'utilisez pas un SSD contenant des données à conserver.

Étapes

1. Arrêtez proprement la sonde (§ 8.2.2), montez la carte M.2 HAT+ et le SSD (chapitre 3), puis remettez la sonde sous tension.
2. Lancez l'activation depuis l'interface d'administration ou par l'API. Le corps de la requête reprend le nom d'hôte de la sonde, ce qui évite d'agir sur la mauvaise sonde :

```bash
# Active le SSD comme volume de données (rôle admin requis).
# Le champ "confirm" doit contenir le nom d'hôte exact de la sonde.
sapi -X POST \
     -H "Content-Type: application/json" \
     -d '{"confirm": "sonde-paris-01"}' \
     "$SONDE/api/v1/system/storage/ssd"
```

3. La sonde formate le SSD, y migre les données concernées (historique, agrégats, artefacts, file d'export, journaux persistants), puis redémarre. Ne coupez pas l'alimentation pendant cette opération.
4. Attendez le retour de la sonde : `GET /health` répond de nouveau en `200`.

Résultat attendu : la sonde fonctionne normalement ; l'historique antérieur est consultable ; les nouvelles données sont écrites sur le SSD.

Vérification : dans la page de santé de l'interface ou dans `GET /api/v1/system`, l'état de santé `storage` est `OK`. Vérifiez que les contrôles ont repris et que l'historique antérieur reste consultable.

Erreurs possibles

Symptôme	Cause probable	Action
Requête refusée	Nom d'hôte incorrect dans `confirm` ; rôle insuffisant	Corriger le nom d'hôte ; utiliser un compte `admin`
SSD non détecté	Nappe PCIe mal insérée ; SSD absent de la liste des modèles pris en charge ; alimentation insuffisante	Arrêter la sonde, vérifier le montage (chapitre 3) et l'alimentation de 27 W
État de santé `storage` en `CRITICAL` après l'activation	SSD défaillant ou déconnecté	Voir le comportement en cas de défaillance ci-dessous

Comportement en cas d'absence ou de défaillance du SSD. Si le SSD activé devient absent ou défaillant, la sonde **continue d'exécuter ses contrôles**. L'historique local est alors conservé sur la microSD, en mode réduit, et l'état de santé `storage` passe en `CRITICAL`. Remplacez le SSD dès que possible ou contactez le support. Surveillez cet état de santé dans vos plateformes (§ 8.7).

> **Attention** — En mode réduit, toutes les écritures se reportent sur la microSD. Ne laissez pas durablement une sonde dans cet état : l'usure de la carte s'accélère.

8.4 Mises à jour

8.4.1 Ce qui est mis à jour

Les mises à jour publiées par l'éditeur couvrent :

- le système d'exploitation (correctifs de sécurité) ;
- le moteur principal et le moteur de scénarios ;
- Chromium et la bibliothèque Puppeteer, toujours livrés **ensemble**, dans des versions testées conjointement par l'éditeur ;
- l'interface d'administration ;
- la liste des plugins Nagios fournis.

Ces éléments ne sont pas mis à jour séparément. Une mise à jour est une **image système complète**, signée par l'éditeur (*bundle*). La sonde vérifie la signature avant toute installation et refuse une image dont la signature est invalide. L'image s'installe sur un second emplacement système, distinct de celui qui fonctionne : en cas d'échec, la sonde revient automatiquement à la version précédente (§ 8.4.5).

Les mises à jour sont publiées sur deux canaux :

Canal	Contenu	Accès
`security`	Correctifs de sécurité, y compris ceux de Chromium	Sans condition, pendant toute la période de support (§ 8.4.6)
`feature` (versions fonctionnelles)	Nouvelles fonctions et évolutions	Réservé aux sondes disposant d'un justificatif de maintenance en cours de validité (§ 8.4.7)

Les deux canaux sont indépendants : leurs images sont distinctes et chacun dispose de son propre mode, `automatic` par défaut pour le canal `security` et `manual` par défaut pour le canal `feature` (§ 8.4.2). Un correctif de sécurité n'exige jamais d'installer une version fonctionnelle.

Une seule image en attente. L'emplacement inactif ne peut contenir qu'**une seule image préparée** à la fois, quel que soit son canal. Les règles suivantes s'appliquent :

Règle	Comportement
Préemption	Une image `security` **préempte** une image `feature` déjà préparée : l'image fonctionnelle est abandonnée, le correctif est installé à sa place, puis la version fonctionnelle est retéléchargée plus tard
Images cumulatives	Une version fonctionnelle contient tous les correctifs de sécurité publiés avant elle
Ligne de versions	Une image `security` s'applique à la ligne de versions installée sur la sonde
Niveau de correctifs	Aucun changement de canal ne peut abaisser le niveau de correctifs déjà installé
Report	Un report vaut pour une version donnée ; une nouvelle image critique est réévaluée, avec un report de 7 jours au plus (§ 8.4.2)

L'image préparée est identifiée dans le champ `staged` de `GET /api/v1/updates` : version, canal et caractère critique.

> **Information** — Chromium n'est jamais mis à jour indépendamment de Puppeteer. Une version de Chromium non validée pourrait modifier le comportement des scénarios. L'éditeur publie les correctifs de sécurité de Chromium après les avoir validés avec la version de Puppeteer embarquée. Il se fixe pour **objectifs**, à compter de la disponibilité du correctif publié par le projet Chromium : 14 jours pour une vulnérabilité critique ou activement exploitée, 30 jours pour une vulnérabilité de gravité élevée. Ces objectifs ne sont pas des engagements contractuels. Les engagements contractuels éventuels relèvent de votre contrat de maintenance.

Le délai qui sépare une vulnérabilité de sa correction effective sur votre sonde comprend plusieurs étapes, qui relèvent de responsabilités distinctes :

Étape	Ce qu'elle recouvre	Responsable
Disponibilité du correctif	Publication de l'image corrigée sur le canal `security` (objectifs ci-dessus, à compter du correctif amont)	Éditeur
Notification	Avis de sécurité publié et joint à la mise à jour ; état de santé `updates` et métrique `sva.update.pending` (§ 8.4.9, § 8.4.11)	Éditeur et sonde
Déploiement	Installation immédiate sur l'emplacement inactif, puis activation selon vos fenêtres, votre préavis et vos éventuels reports (§ 8.4.2, § 8.4.8)	Client
Mesures compensatoires	Dispositions prises en attendant l'activation, par exemple la suspension des scénarios navigateur qui visitent des applications exposées (§ 8.4.11)	Client

Les objectifs de l'éditeur ne portent que sur la première étape. La durée totale dépend aussi de vos fenêtres et de vos reports : plus vos fenêtres sont espacées, plus les mesures compensatoires prennent d'importance.

8.4.2 Choisir un mode de mise à jour

Une mise à jour se déroule en deux temps bien distincts :

Temps	Ce qui se passe	Effet sur la supervision
Installation	Téléchargement de l'image signée, vérification de sa signature et écriture sur l'emplacement système inactif (§ 8.4.5)	Aucun : les contrôles continuent de s'exécuter normalement
Activation	Annonce, avec un préavis qui dépend du cas d'activation (matrice ci-dessous), passage en état de maintenance, drainage des exécutions, redémarrage sur le nouvel emplacement, autotest et, si nécessaire, retour arrière (§ 8.4.9)	Interruption de la supervision assurée par cette sonde, le temps du drainage, du redémarrage et de l'autotest

Un mode par canal. Chacun des deux canaux (§ 8.4.1) dispose de son propre mode :

Canal	Paramètre	Par défaut	Mode `automatic`	Mode `manual`
`security`	`security.mode`	`automatic`	La sonde installe chaque correctif dès qu'il est disponible, sans interrompre les contrôles, puis l'active dans une fenêtre de maintenance, après préavis ; un correctif critique suit `security.criticalPolicy` (§ 8.4.11)	La sonde signale les correctifs disponibles ; un administrateur décide quand les appliquer (§ 8.4.3)
`feature`	`feature.mode`	`manual`	Même fonctionnement pour les versions fonctionnelles auxquelles la sonde a accès (§ 8.4.7)	La sonde signale les versions disponibles ; un administrateur décide quand les appliquer (§ 8.4.3)

Le mode automatique convient aux sondes standard, aux parcs importants et aux équipes qui souhaitent limiter l'exploitation. Le mode manuel convient aux environnements soumis à une gestion des changements stricte et aux sondes pilotes. L'installation automatique des correctifs de sécurité est le réglage par défaut recommandé ; vous pouvez passer le canal `security` en mode `manual` à tout moment, par un simple changement de paramètre.

Fenêtres de maintenance. Une activation automatique ordinaire, ou celle d'un correctif critique en mode `next-window` (réglage par défaut), n'a lieu que dans une **fenêtre de maintenance** définie par vos soins : un créneau récurrent (jours, heure de début, durée) pendant lequel la sonde est autorisée à redémarrer. Vous pouvez définir de 0 à 7 fenêtres. **Aucune fenêtre n'est définie par défaut** et aucune plage horaire n'est imposée. Lors d'une mise en service par l'assistant web, l'étape consacrée aux mises à jour impose un choix explicite : au moins une fenêtre, ou le mode manuel (§ 4.4.5). Dans le fichier `provision.yaml`, la section `updates` est en revanche facultative : en son absence, ou si elle ne contient aucune fenêtre, la sonde n'active aucune mise à jour automatiquement et l'état de santé `updates` reste en `WARNING` jusqu'à la définition d'une fenêtre (§ 4.3.3). La méthode de choix des fenêtres est décrite au § 8.4.8.

Sans fenêtre définie, la sonde n'active d'elle-même ni une mise à jour ordinaire ni un correctif critique en mode `next-window`. La mise à jour reste en attente : l'état de santé `updates` passe en `WARNING`, ou en `CRITICAL` pour un correctif critique, et un administrateur l'active depuis l'interface ou par `POST /api/v1/updates/apply`, immédiatement ou à une heure donnée (§ 8.4.3). Seule exception : un correctif critique en mode `asap`, réglage que vous choisissez explicitement (§ 8.4.11), est activé à l'instant annoncé, même sans fenêtre.

Matrice des activations. Une activation relève toujours de l'un des six cas suivants. Cette matrice fait foi pour l'ensemble de la documentation : les règles de préavis, de fenêtre et de report décrites ailleurs en sont des extraits.

Cas	Déclenchement	Instant de l'activation	Préavis minimal
Manuelle immédiate	Administrateur : `POST /api/v1/updates/apply` sans `scheduledAt`, après confirmation explicite	Aussitôt, dans une fenêtre ou non	Aucun : `update.scheduled` et `maintenance.started` sont émis ensemble
Manuelle programmée	Administrateur : `POST /api/v1/updates/apply` avec `scheduledAt`	`scheduledAt`, dans une fenêtre ou non	1 minute : une date plus proche ou passée est refusée (`422`)
Automatique ordinaire	Sonde, canal en mode `automatic`	Début de la première fenêtre qui commence au moins `notice` après l'annonce	`notice` (24 heures par défaut)
Critique `next-window` (par défaut)	Sonde, canal `security` en mode `automatic`	Début de la première fenêtre qui commence au moins 15 minutes après l'annonce. Une fenêtre plus proche, ou déjà commencée, n'est pas admissible : l'activation attend la fenêtre admissible suivante	15 minutes
Critique `asap` (choix explicite)	Sonde, canal `security` en mode `automatic`	15 minutes après l'annonce, augmentées du décalage `security.criticalStagger`, dans une fenêtre ou non, y compris sans fenêtre définie	15 minutes, augmentées du décalage
Critique, canal en mode `manual`	Administrateur uniquement	Celui que choisit l'administrateur, comme pour une activation manuelle	Celui du cas manuel retenu

Cas	Sans fenêtre définie	Après un report (`postpone`)	Fin prévue (`windowEnd`)
Manuelle immédiate	Possible	Sans objet : l'activation a commencé	`null`

Cas	Sans fenêtre définie	Après un report (`postpone`)	Fin prévue (`windowEnd`)
Manuelle programmée	Possible	Replanifiée selon le mode du canal, comme une activation non programmée	Fin de la fenêtre qui contient `scheduledAt` ; sinon `null`
Automatique ordinaire	Aucune activation : mise à jour en attente	Première fenêtre qui commence après `until` et au moins `notice` après la réannonce ; report de 30 jours au plus	Fin de la fenêtre retenue
Critique `next-window`	Aucune activation automatique : correctif en attente d'un administrateur	Première fenêtre qui commence après `until` et au moins 15 minutes après la réannonce ; report de 7 jours au plus	Fin de la fenêtre retenue
Critique `asap`	Activation à l'instant annoncé	À `until`, ou 15 minutes après la réannonce si `until` est plus proche, sans nouveau décalage ; report de 7 jours au plus	`null`
Critique, canal en mode `manual`	Aucune activation automatique	Sans objet tant qu'aucune activation n'est programmée	Selon le cas manuel retenu

Règles communes à tous les cas :

- **signalement du préavis** : `noticeReduced` vaut `true` dès que le préavis effectif est inférieur à `notice`, dans la réponse de `POST /api/v1/updates/apply`, dans `scheduledActivation` et dans l'attribut `sva.update.notice_reduced` de l'annonce ;
- **réannonce** : toute activation déplacée (report, nouvelle date, activation manuelle qui avance une activation annoncée, changement de fuseau) est annoncée de nouveau, avec le même identifiant d'activation et un numéro d'annonce plus grand. Lorsqu'aucun instant ne peut être déterminé, par exemple après un report sans fenêtre définie, l'activation est annulée (événement `update.cancelled`) et la mise à jour reste en attente (§ 8.4.9) ;
- **état de santé `updates`** : `CRITICAL` tant qu'un correctif critique n'est pas actif, quel que soit le cas ; sinon `WARNING` lorsqu'une mise à jour attend sans activation planifiée, après un report, ou lorsqu'un canal est en mode `automatic` sans aucune fenêtre définie (configuration incomplète), et `OK` dans les autres cas. Pendant l'activation, `/health` répond `MAINTENANCE` (§ 8.4.9) ;
- **notification des plateformes** : chaque annonce, annulation, début et fin de maintenance est transmis aux destinations d'export (événements `update.scheduled`, `update.cancelled`, `maintenance.started`, `maintenance.ended`, métriques du § 8.4.9). Les activations sans fin prévue (`windowEnd` à `null`) demandent une préparation particulière de vos plateformes (§ 8.4.10) ;
- **activation immédiate** : un administrateur peut toujours autoriser explicitement une activation immédiate, y compris pour un correctif critique qui attend une fenêtre admissible.

Préavis. Le préavis `notice` (24 heures par défaut, de `0` à `7d`) s'applique aux activations automatiques ordinaires : si la prochaine fenêtre commence avant son expiration, l'activation passe à la fenêtre suivante. Les correctifs critiques suivent le préavis de 15 minutes de la matrice, et les activations demandées par un administrateur les règles de priorité ci-dessous. Les moyens par lesquels l'activation est annoncée sont décrits au § 8.4.9.

Priorité des activations. Lorsque plusieurs règles peuvent s'appliquer, la sonde les combine ainsi :

Situation	Comportement
Activation automatique ordinaire	Respecte le préavis `notice` ; sinon, elle passe à la fenêtre suivante
Correctif critique (`next-window` ou `asap`)	Respecte le préavis de 15 minutes de la matrice ci-dessus, augmenté du décalage en mode `asap`

Situation	Comportement
`POST /api/v1/updates/apply` **sans** `scheduledAt`	Activation manuelle **immédiate, sans préavis**. L'interface affiche ses conséquences (interruption de la supervision assurée par la sonde, passage en état de maintenance) et demande une confirmation explicite. Les événements `update.scheduled` et `maintenance.started` sont émis aussitôt
`POST /api/v1/updates/apply` **avec** `scheduledAt` à une date passée ou à moins d'une minute	Demande refusée : `422 Unprocessable Content`
`POST /api/v1/updates/apply` avec `scheduledAt` antérieur à l'expiration du préavis	Activation acceptée à la date demandée ; la réponse porte `noticeReduced: true` pour signaler que le préavis habituel n'est pas respecté
Activation manuelle alors qu'un report est en cours	L'activation manuelle **prime** sur le report

> **Attention** — Une intégration qui attend le préavis `notice` avant toute maintenance peut recevoir `update.scheduled` et `maintenance.started` presque simultanément lors d'une activation manuelle immédiate. Planifiez une période de maintenance ponctuelle dans vos plateformes avant de lancer une telle activation (§ 8.4.10).

Report. Un administrateur peut reporter une activation annoncée, par l'interface ou par `POST /api/v1/updates/postpone`, en indiquant la date limite du report dans le champ `until`. L'activation est ensuite replanifiée et réannoncée selon son cas (matrice ci-dessus). Le report est limité à **30 jours** pour un correctif ordinaire et à **7 jours** pour un correctif de sécurité critique (§ 8.4.11). Chaque report est consigné dans le journal d'audit. Un report vaut pour **une version donnée** : si une nouvelle image critique arrive pendant le report, elle est réévaluée et ne peut être reportée que de 7 jours au plus. Une activation manuelle (§ 8.4.3) prime sur le report en cours.

```bash
# Reporte l'activation de la mise à jour en attente (rôle admin requis).
# Date fictive, exprimée en UTC comme toutes les dates de l'API.
sapi -X POST \
     -H "Content-Type: application/json" \
     -d '{"until": "2026-12-01T00:00:00Z"}' \
     "$SONDE/api/v1/updates/postpone"
```

Drainage. Au début de l'activation, la sonde ne lance plus aucune exécution et laisse celles en cours se terminer pendant au plus `drainTimeout` (5 minutes par défaut, 30 minutes au maximum), avant de redémarrer (§ 8.4.9).

Paramètres. La politique se règle dans les paramètres de la sonde, section `updates` (interface d'administration, ou `GET` / `PUT /api/v1/settings/updates`) :

Champ	Description	Valeur par défaut
`security.mode`	Mode du canal `security` : `automatic` ou `manual`	`automatic`
`security.criticalPolicy`	Activation d'un correctif de sécurité critique : `next-window` (au début de la première fenêtre qui commence au moins 15 minutes après l'annonce) ou `asap` (15 minutes après l'annonce, augmentées de `security.criticalStagger`, même hors fenêtre), § 8.4.11	`next-window`
`security.criticalStagger`	Décalage fixe, propre à la sonde, ajouté au préavis réduit d'une activation critique en mode `asap`, de `0` à `4h` ; sert à échelonner les sondes d'un même site (§ 8.4.11)	`0` (aucun décalage)
`feature.mode`	Mode du canal `feature` : `manual` ou `automatic`	`manual`

Champ	Description	Valeur par défaut
`windows`	Liste de 0 à 7 fenêtres de maintenance	Aucune fenêtre
`windows[].days`	Jours de la semaine où la fenêtre s'applique, parmi `mon`, `tue`, `wed`, `thu`, `fri`, `sat`, `sun`	—
`windows[].start`	Heure de début de la fenêtre, au format `HH:MM`	—
`windows[].duration`	Durée de la fenêtre, au format des autres durées (par exemple `2h` ou `90m`)	—
`notice`	Préavis minimal d'une activation automatique ordinaire, de `0` à `7d` ; les autres cas suivent la matrice ci-dessus	`24h`
`drainTimeout`	Délai accordé aux exécutions en cours pour se terminer au début d'une activation, `30m` au maximum	`5m`
`repositoryUrl`	Adresse du dépôt de mises à jour. Facultatif : par défaut, l'adresse du service de distribution de l'éditeur, `https://updates-synovex.incitypark.fr`, lue dans le profil éditeur. Renseignez-le pour utiliser un miroir interne à votre organisation	Dépôt de l'éditeur

Exemple de section `updates` (valeurs fictives, à adapter à votre organisation selon le § 8.4.8) :

JSON

```
{
  "security": {
    "mode": "automatic",
    "criticalPolicy": "next-window"
  },
  "feature": {
    "mode": "manual"
  },
  "windows": [
    { "days": ["mon", "wed"], "start": "21:30", "duration": "90m" }
  ],
  "notice": "24h",
  "drainTimeout": "5m"
}
```

BASH

```
# Applique la politique de mises à jour contenue dans le fichier updates.json (rôle admin requis).
# 1. Lire la version courante de la section (en-tête ETag)
ETAG=$(sapi -D - -o /dev/null "$SONDE/api/v1/settings/updates" | awk 'tolower($1)=="etag:" {print
    $2}' | tr -d '\r')
# 2. Enregistrer la nouvelle politique (If-Match : version lue à l'étape 1)
sapi -X PUT \
     -H "If-Match: $ETAG" \
     -H "Content-Type: application/json" \
     --data-binary @updates.json \
     "$SONDE/api/v1/settings/updates"
```

Les heures de `windows[].start` sont interprétées dans le fuseau horaire de la section `time` (fuseau choisi à la mise en service, UTC par défaut) ; elles suivent l'heure légale de ce fuseau. Le traitement des changements d'heure, y compris la fin d'une fenêtre traversée par une bascule, est décrit au § 8.4.8. Choisissez une fenêtre suffisamment longue : elle doit couvrir le drainage (`drainTimeout`), le redémarrage, la période de validation de 10 minutes et, le cas échéant, un retour arrière (§ 8.4.5).

> **Information** — Le règlement européen sur la cyberrésilience (CRA) demande que les mises à jour de sécurité automatiques soient, *le cas échéant*, installées dans un délai approprié et activées par défaut, avec un mécanisme de désactivation clair et simple, la notification des mises à jour disponibles et la possibilité de les reporter temporairement. Il demande aussi de séparer les correctifs de sécurité des mises à jour fonctionnelles lorsque c'est techniquement possible. La sonde met en œuvre ces principes par le canal `security` en mode automatique par défaut, désactivable par le paramètre `security.mode`, par l'annonce de chaque activation (§ 8.4.9) et par le report (`POST /api/v1/updates/postpone`). Le règlement n'impose **ni horaire ni calendrier** particulier : le choix des fenêtres relève entièrement de votre organisation.

> **Conseil** — Dans un parc de plusieurs sondes, laissez une ou deux **sondes pilotes** en mode manuel et appliquez-y chaque nouvelle version quelques jours avant les autres. Vérifiez que tous les scénarios restent `OK`, puis généralisez.

> **Information** — Les adresses de l'éditeur utilisées par la sonde (dépôt de mises à jour, documentation en ligne, support) ne sont pas inscrites dans le logiciel. Elles figurent dans un **profil éditeur signé**, livré avec l'image et actualisé par le canal `security`. Un changement d'adresse ne nécessite donc pas de nouvelle version du logiciel. Valeurs du profil : distribution des mises à jour `https://updates-synovex.incitypark.fr`, documentation `https://docs-synovex.incitypark.fr`, support `https://support-synovex.incitypark.fr`, site commercial `https://synovex.incitypark.fr` ; l'adresse de la console centrale prévue, `https://fleet-synovex.incitypark.fr`, y est seulement réservée et n'est jamais contactée par la sonde autonome. Le paramètre `repositoryUrl` permet en outre de pointer vers un miroir interne : comme chaque image est signée par l'éditeur et vérifiée avant installation, un miroir préserve l'authenticité des images ; leur fraîcheur dépend en revanche de la synchronisation du miroir (encadré suivant).

> **Attention** — Avec un miroir, l'**intégrité** et l'authenticité des images restent garanties par leur signature, toujours vérifiée. Leur **fraîcheur** n'est assurée que si les métadonnées du miroir sont à jour : les métadonnées du dépôt sont signées et portent une date d'expiration (`validUntil`, 7 jours). Une sonde refuse des métadonnées expirées, ce qui la protège contre un miroir figé au-delà de cette échéance ; avant celle-ci, un miroir en retard peut encore lui présenter des métadonnées valides qui ne mentionnent pas les correctifs publiés depuis sa dernière synchronisation. Synchronisez donc votre miroir nettement plus souvent que cette échéance, par exemple chaque jour. L'effet de métadonnées expirées sur l'état de santé `updates` est précisé dans les notes de version. Les règles de confiance sont décrites au § 8.4.5.

8.4.3 Appliquer une mise à jour manuellement

Objectif : installer et activer une mise à jour disponible ou en attente, au moment choisi par un administrateur : sonde dont le canal concerné est en mode manuel, sonde sans fenêtre de maintenance, ou activation à avancer (correctif critique, § 8.4.11).

Prérequis : rôle `admin` ; accès HTTPS sortant vers le dépôt de l'éditeur (`https://updates-synovex.incitypark.fr` ou votre miroir interne), ou, à défaut, image signée importée hors ligne (§ 8.4.4) ; sauvegarde récente de la configuration (§ 8.5).

Étapes

1. Consultez les mises à jour disponibles dans l'interface ou par l'API :

   ```bash
   sapi "$SONDE/api/v1/updates"
   ```

   Le champ `scheduledActivation` indique, le cas échéant, l'activation déjà planifiée.
2. Lisez les notes de version (documentation en ligne, ou document transmis par le canal convenu dans votre contrat, § 10.5) : changements de comportement, nouvelle version de Chromium et de Puppeteer, actions requises.
3. Exportez la configuration (§ 8.5.2).
4. Planifiez une période de maintenance dans vos plateformes de supervision (§ 8.4.10).
5. Lancez l'activation depuis l'interface ou par l'API, immédiatement :

   ```bash
   sapi -X POST \
        "$SONDE/api/v1/updates/apply"
   ```

   ou à une heure donnée, par le champ facultatif `scheduledAt` (date fictive, exprimée en UTC) :

   ```bash
   sapi -X POST \
        -H "Content-Type: application/json" \
        -d '{"scheduledAt": "2026-11-24T21:00:00Z"}' \
        "$SONDE/api/v1/updates/apply"
   ```

   L'activation **immédiate** (sans `scheduledAt`) a lieu **sans préavis** : dans l'interface, elle n'est lancée qu'après l'affichage de ses conséquences et une confirmation explicite. Ce message rappelle que la sonde cessera de superviser jusqu'à son retour et, sur un site redondant, que la supervision du site sera entièrement interrompue si une autre sonde est déjà en maintenance ou hors service. Le décalage `security.criticalStagger` ne s'applique pas à une activation manuelle (§ 8.4.11). Avec `scheduledAt`, une date passée ou située à moins d'une minute est refusée (`422`) ; une date antérieure à l'expiration du préavis `notice` est acceptée, et la réponse porte alors `noticeReduced: true`. Une activation manuelle prime sur un report en cours (§ 8.4.2).

   > **Attention** — Sur un site équipé de plusieurs sondes redondantes, n'activez **jamais manuellement deux sondes du même site en même temps** : attendez la fin de maintenance de la première (événement `maintenance.ended`, retour arrière éventuel compris) avant d'activer la suivante (§ 8.4.12).

   La réponse `202 Accepted` indique que l'opération a démarré. Elle porte l'identifiant de l'activation (`activationId`), l'instant retenu (`at`) et `noticeReduced` ; conservez l'identifiant pour la vérification de l'étape 7. L'en-tête `Location` désigne la ressource de suivi. Si l'image n'est pas encore installée, elle l'est d'abord sur l'emplacement système inactif, pendant que la sonde continue de superviser.
6. Ne coupez pas l'alimentation. Au moment de l'activation, la sonde passe en état de maintenance et draine ses exécutions (§ 8.4.9), redémarre une fois sur le nouvel emplacement, puis vérifie son propre fonctionnement pendant 10 minutes au plus (§ 8.4.5).
7. Une fois la sonde revenue, vérifiez dans `GET /api/v1/updates` que `lastResult.activationId` est l'identifiant renvoyé à l'étape 5, que `lastResult.outcome` vaut `succeeded` et que l'emplacement actif porte la nouvelle version, puis confirmez la version dans `GET /api/v1/system`. Un `lastResult` qui porte un autre identifiant concerne une tentative antérieure (§ 8.4.12).

Résultat attendu : la sonde fonctionne avec la nouvelle version, validée par son autotest, et les contrôles ont repris. Si la validation a échoué, la sonde est revenue automatiquement à la version précédente : l'emplacement actif porte l'ancienne version et l'événement figure dans le journal d'audit.

Vérification : lancez une exécution d'essai des scénarios les plus importants (`POST /api/v1/checks/{id}/runs?dryRun=true`) et comparez leurs durées avec celles observées avant la mise à jour.

En cas de problème : § 9.7.

8.4.4 Mise à jour hors ligne

Pour une sonde sans accès au dépôt de l'éditeur, un administrateur importe le **même fichier d'image signé** que celui distribué en ligne. Il le télécharge depuis un poste disposant d'un accès Internet, sur le service de distribution de l'éditeur (`https://updates-synovex.incitypark.fr`), ou le reçoit par le canal convenu dans votre contrat tant que ce service n'est pas disponible (§ 10.5). Il l'importe ensuite par l'interface ou par l'API, puis l'applique comme au § 8.4.3 :

```bash
# Importe un fichier d'image signé téléchargé au préalable (nom fictif).
# TYPE_IMAGE : type de contenu de l'image, indiqué dans les notes de version.
sapi -X POST \
     -H "Content-Type: $TYPE_IMAGE" \
     --data-binary @sva-image-exemple.bundle \
     "$SONDE/api/v1/updates/upload"
```

La sonde vérifie la signature du fichier de la même manière qu'en ligne et refuse un fichier altéré. L'installation, le redémarrage, l'autotest et le retour arrière éventuel se déroulent ensuite exactement comme pour une mise à jour en ligne (§ 8.4.5). Les correctifs du canal `security` peuvent être importés de cette façon pendant toute la période de support, sans justificatif de maintenance.

Un fichier importé hors ligne n'est pas accompagné des métadonnées du dépôt : il ne fait donc l'objet d'**aucun contrôle de fraîcheur**. La règle **anti-retour en arrière** s'applique en revanche : un fichier dont la version est inférieure à la version installée est refusé (§ 8.4.5). Il vous appartient de vérifier, avant l'import, que vous disposez de la dernière image publiée pour votre ligne de versions.

> **Information** — Le nom du fichier ci-dessus est fictif. Utilisez le fichier tel qu'il a été téléchargé, sans le renommer ni le décompresser.

8.4.5 Déroulement d'une mise à jour et retour arrière automatique

La carte microSD contient **deux emplacements système**, A et B. Un seul est actif à un instant donné. Le système y est installé en **lecture seule** : il ne peut pas être modifié en fonctionnement. Les données de la sonde (configuration, résultats, historique) sont stockées sur une partition séparée, ou sur le SSD s'il est activé (§ 8.3.4) : elles sont

communes aux deux emplacements.

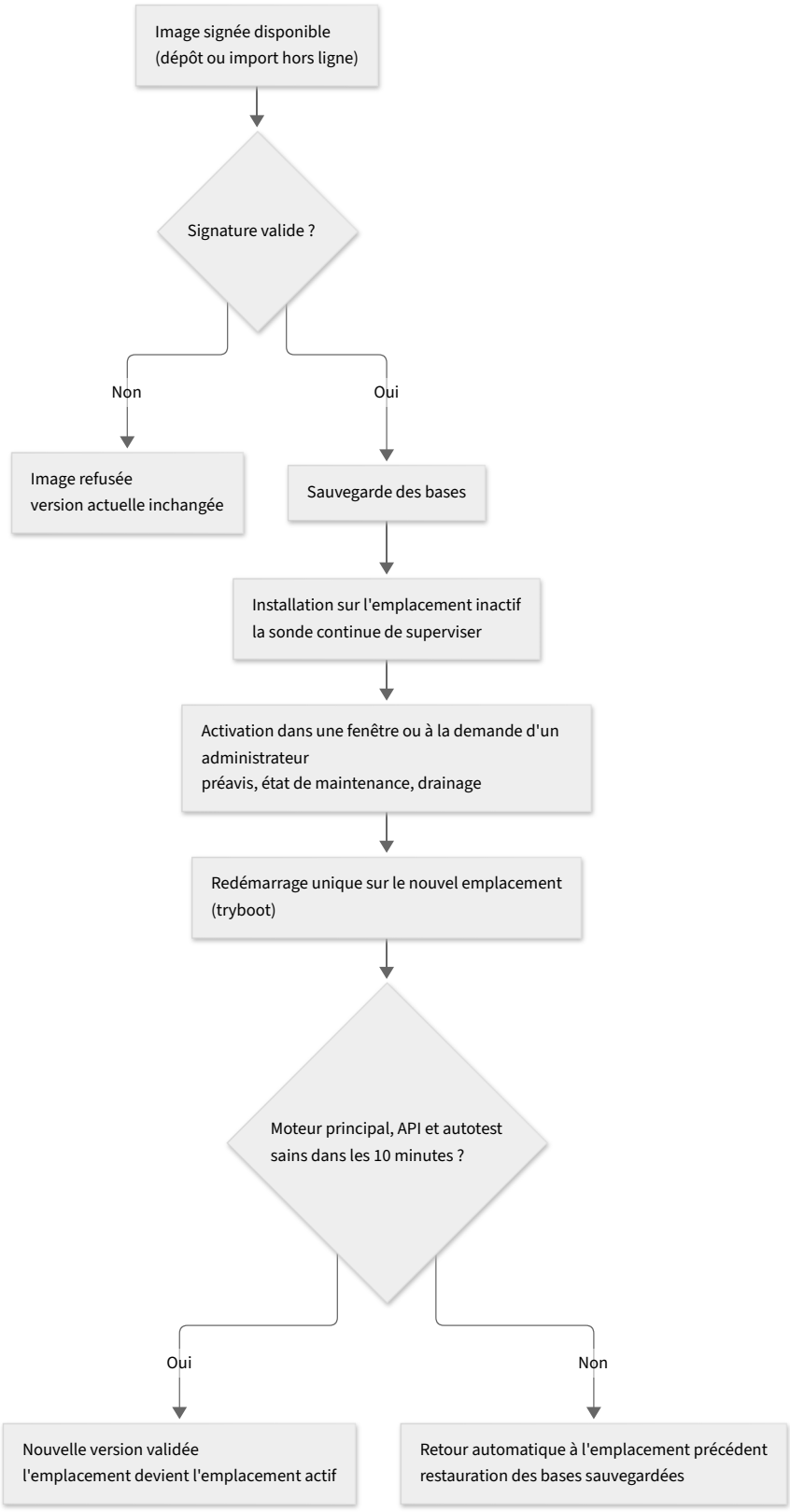


Schéma 8-1 — Déroulement d'une mise à jour et retour arrière automatique

1. **Vérification.** La sonde vérifie la signature de l'image avant toute installation. Pour une image obtenue en ligne, elle vérifie aussi la signature et la date d'expiration des métadonnées du dépôt ; elle refuse une image de version inférieure à la version installée (règles de confiance ci-dessous).

2. **Sauvegarde.** Les bases de données sont sauvegardées avant toute migration de leur structure.
3. **Installation.** L'image est écrite sur l'emplacement inactif, dès qu'elle est disponible pour un canal en mode automatique, ou à la demande d'un administrateur. L'emplacement actif n'est pas modifié et la sonde continue d'exécuter ses contrôles.
4. **Redémarrage d'essai.** Au moment de l'activation, dans une fenêtre de maintenance ou à la demande d'un administrateur, et après le préavis et le drainage des exécutions (§ 8.4.9), la sonde redémarre **une seule fois** sur le nouvel emplacement, au moyen du mécanisme *tryboot* du chargeur d'amorçage du Raspberry Pi : si ce démarrage échoue, le démarrage suivant se fait automatiquement sur l'emplacement précédent. L'indicateur *tryboot* est **à usage unique** : il ne vaut que pour ce démarrage. Le chien de garde du chargeur d'amorçage puis le chien de garde matériel du Raspberry Pi surveillent le démarrage, de sorte qu'un blocage du système avant le démarrage des services provoque une réinitialisation de la carte sans intervention. La surveillance du chargeur d'amorçage (paramètre `BOOT_WATCHDOG_TIMEOUT`) prend fin au démarrage du processeur ARM, d'après la documentation du fabricant ; le chien de garde matériel est ensuite armé par le système. **Toute réinitialisation pendant l'essai** (blocage, coupure électrique, chien de garde) ramène la sonde sur l'emplacement précédent.
5. **Validation.** Le moteur principal, l'API et un autotest doivent être sains dans les **10 minutes**. Dans ce cas, la nouvelle version est validée et devient définitive. Ces 10 minutes sont le délai accordé à l'autotest, et non la durée d'un retour en fonctionnement : si le système se bloque sans que l'autotest puisse conclure, le retour à l'emplacement précédent suppose un redémarrage effectif, provoqué par un chien de garde ou, à défaut, par une remise sous tension ; la durée totale dépend alors de ces mécanismes (étape 4). Le **point de validation définitive** est la réussite de l'autotest : c'est seulement à ce moment que le fichier de configuration du chargeur d'amorçage `autoboot.txt` est mis à jour pour faire du nouvel emplacement l'emplacement de démarrage par défaut. Avant ce point, tout redémarrage ramène à l'emplacement précédent.
6. **Retour arrière.** Dans le cas contraire, la sonde **revient automatiquement** à l'emplacement précédent et restaure les bases sauvegardées. Aucune intervention n'est nécessaire. Comme les données sont communes aux deux emplacements, la restauration des bases sauvegardées à l'étape 2 annule les migrations de structure éventuellement effectuées par la nouvelle version pendant l'essai.

`GET /api/v1/updates` indique la version installée sur chaque emplacement, l'emplacement actif, les mises à jour disponibles, la date de fin de la période de support (`supportEndsAt`) et la date de fin du justificatif de maintenance (`maintenanceEndsAt`). Le champ `staged` identifie l'image préparée sur l'emplacement inactif (version, canal, caractère critique ; § 8.4.1).

Règles de confiance et de fraîcheur des images

Règle	Comportement
Signature des images	Chaque image est signée par l'éditeur ; une signature invalide entraîne le refus de l'image
Métadonnées du dépôt	Signées, avec une date d'expiration (`validUntil`, 7 jours). Des métadonnées expirées sont refusées, ce qui protège contre le gel d'un dépôt ou d'un miroir
Anti-retour en arrière	Une image de version inférieure à la version installée est refusée. Seule exception : le retour arrière A/B local vers l'emplacement précédent (étape 6)
Import hors ligne	Pas de contrôle de fraîcheur (pas de métadonnées du dépôt) ; la règle anti-retour en arrière s'applique (§ 8.4.4)
Clés	La clé racine de confiance est incluse dans l'image. La rotation des clés de signature et la liste de révocation sont distribuées par le canal `security`, dans le profil éditeur signé (§ 8.4.2)
Heure non synchronisée	La date d'expiration des métadonnées ne peut être vérifiée qu'avec une heure fiable (§ 5.4). Le traitement des métadonnées et du profil éditeur tant que l'indicateur `clock` est en `WARNING` est précisé dans les notes de version ; rétablissez d'abord une heure fiable

Règle	Comportement
Sonde hors ligne ou longtemps déconnectée	Une image signée importée hors ligne apporte le profil éditeur de sa version, si la sonde peut la vérifier avec les clés qu'elle détient. Les autres moyens d'actualiser la chaîne de confiance sont précisés dans les notes de version
Métadonnées ou profil expirés, clé révoquée	Refus ; la sonde conserve son profil précédent, n'installe aucune mise à jour en ligne et continue d'exécuter ses contrôles. Pour la récupération, contactez le support (§ 10.5)

Ces règles s'inspirent des principes de The Update Framework (TUF), cadre public de sécurisation des systèmes de mise à jour.

La durée d'indisponibilité d'une activation (drainage, redémarrage, autotest) et celle d'un retour arrière automatique s'observent sur vos sondes entre les événements `maintenance.started` et `maintenance.ended` (§ 8.4.9).

> **Information** — Le redémarrage interrompt les contrôles exécutés par la sonde. Avant de redémarrer, la sonde draine ses exécutions ; celles qui ne sont pas terminées à l'issue du délai `drainTimeout` sont closes en `UNKNOWN` avec le type d'erreur `maintenance` (§ 8.4.9). Pour éviter les fausses alertes, alignez les périodes de maintenance de vos plateformes sur vos fenêtres (§ 8.4.10) ; pour maintenir la supervision pendant ce redémarrage, voir § 8.4.12.

> **Attention** — Un retour arrière automatique signale un problème de la nouvelle version sur votre sonde. Consultez le journal d'audit, puis contactez le support en joignant une archive de diagnostic (§ 9.9). Ne relancez pas la même mise à jour avant l'avis du support.

8.4.6 Période de support

Chaque version majeure du logiciel bénéficie d'une **période de support** d'au moins **5 ans** à compter de sa mise sur le marché. Cette durée est allongée si la durée d'utilisation prévisible du produit ou la réglementation l'exige : la période retenue est d'**au moins 5 ans, ajustée à la durée d'utilisation prévisible** du produit. Pendant cette période, l'éditeur publie les correctifs de sécurité sur le canal `security`, accessibles à toutes les sondes, avec ou sans contrat de maintenance.

La date de fin de la période de support (mois et année) est indiquée à l'achat. La sonde l'expose dans le champ `supportEndsAt` de `GET /api/v1/system` (et de `GET /api/v1/updates`).

Après cette date, la sonde **continue de fonctionner** avec toutes ses fonctions, mais ne reçoit plus de nouveau correctif. L'état de santé `support` passe alors en `WARNING` pour vous le signaler. Anticipez cette échéance en contactant l'éditeur ou le support (§ 10.5).

8.4.7 Contrat de maintenance et justificatif

Le contrat de maintenance est **facultatif**. Il donne accès aux **nouvelles versions fonctionnelles** du logiciel. Il n'est pas nécessaire pour recevoir les correctifs de sécurité, qui restent accessibles sans contrat pendant toute la période de support (§ 8.4.6). Ses conditions sont celles de votre contrat de maintenance.

Le contrat se matérialise sur la sonde par un **justificatif de maintenance** : un fichier signé par l'éditeur, distinct du certificat d'édition, qui porte une date de fin. Il s'importe hors ligne, sans connexion à un service de l'éditeur.

Objectif : permettre à la sonde d'installer les versions fonctionnelles couvertes par votre contrat.

Prérequis : rôle `admin` ; fichier de justificatif remis par l'éditeur selon les modalités prévues par votre contrat.

Étapes

1. Importez le justificatif depuis l'interface d'administration ou par l'API :

```bash
# Importe le justificatif de maintenance (nom de fichier fictif).
# TYPE_JUSTIFICATIF : type de contenu du justificatif, indiqué dans les notes de version.
sapi -X PUT \
     -H "Content-Type: $TYPE_JUSTIFICATIF" \
     --data-binary @justificatif-maintenance-exemple \
     "$SONDE/api/v1/system/maintenance"
```

2. Vérifiez la date de fin du justificatif dans le champ `maintenanceEndsAt` de `GET /api/v1/updates`.

Résultat attendu : les versions fonctionnelles couvertes par le contrat apparaissent parmi les mises à jour disponibles.

Erreurs possibles : un justificatif dont la signature est invalide est refusé ; la sonde conserve alors son état antérieur. Vérifiez que vous importez le fichier tel qu'il vous a été remis, sans modification.

> **Information** — L'échéance du justificatif de maintenance n'affecte **aucune fonction acquise** : la sonde continue de fonctionner avec la version installée et de recevoir les correctifs de sécurité jusqu'à la fin de la période de support. Seul l'accès aux nouvelles versions fonctionnelles cesse.

8.4.8 Définir les fenêtres de maintenance et le préavis

Une fenêtre de maintenance est le créneau récurrent pendant lequel la sonde est autorisée à activer une mise à jour, c'est-à-dire à interrompre sa supervision le temps d'un redémarrage. Ce choix vous appartient : la sonde ne propose aucun créneau par défaut, car le meilleur moment dépend de l'activité de votre organisation et des applications supervisées.

Objectif : définir des fenêtres de maintenance et un préavis adaptés à votre organisation, afin que les mises à jour soient activées sans perturber la supervision des périodes importantes.

Prérequis

- Rôle `admin`.
- La liste des plans d'exécution et des contrôles les plus importants de la sonde (chapitre 6 du guide d'utilisation et de supervision).
- Les créneaux de changement de votre organisation (calendrier de gestion des changements, périodes de gel, astreintes).
- Pour un site équipé de plusieurs sondes, l'inventaire des sondes qui exécutent les mêmes contrôles (§ 8.4.12).

Étapes

1. **Identifiez les périodes creuses propres à votre organisation** : les créneaux où les applications supervisées sont le moins utilisées et où une courte interruption de la supervision a le moins de conséquences. Il n'existe pas de créneau universel : une nuit de semaine convient à une application de bureau, mais pas à un site de commerce en ligne dont l'activité culmine le soir, ni à une application qui exécute des traitements par lots la nuit.
2. **Confrontez ces créneaux à vos plans d'exécution** (chapitre 6 du guide d'utilisation et de supervision) : évitez les créneaux où s'exécutent les contrôles les plus importants, par exemple le contrôle d'un traitement par lots ou d'un indicateur métier calculé à heure fixe.
3. **Dimensionnez la durée de chaque fenêtre** : elle doit couvrir le drainage (`drainTimeout`), le redémarrage, la période de validation de 10 minutes et, par précaution, un retour arrière éventuel, qui ajoute un redémarrage. Ces durées s'observent sur vos sondes, par exemple sur une sonde pilote, entre les événements `maintenance.started` et `maintenance.ended` (§ 8.4.5, § 8.4.9).

4. **Choisissez la fréquence** : une ou deux fenêtres par semaine suffisent en général. Davantage de fenêtres réduit le délai entre la publication d'un correctif et son activation ; vous pouvez en définir 7 au plus.
5. **Choisissez le préavis** (`notice`) : il doit laisser à vos équipes le temps de prendre connaissance de l'annonce, de reporter l'activation si nécessaire et de vérifier les périodes de maintenance de leurs plateformes. La valeur par défaut, 24 heures, convient à la plupart des organisations ; la valeur maximale est `7d`. Une valeur de `0` supprime le délai d'annonce : réservez-la aux sondes de test.
6. **Pour plusieurs sondes redondantes d'un même site**, attribuez à chacune des fenêtres qui ne se chevauchent pas, séparées par un écart suffisant pour que la première sonde ait terminé son activation, retour arrière compris, avant que la suivante ne commence (§ 8.4.12). Cet écart doit **dépasser la durée totale mesurée d'une activation** : drainage, redémarrage, autotest et retour arrière éventuel (§ 8.4.5). Des fenêtres disjointes ne suffisent pas si une activation commencée en fin de fenêtre déborde sur la fenêtre de l'autre sonde.
7. **Enregistrez la politique** dans l'interface d'administration ou par `PUT /api/v1/settings/updates` (exemple au § 8.4.2).
8. **Alignez les périodes de maintenance de vos plateformes de supervision** sur ces fenêtres (§ 8.4.10), puis consignez les fenêtres retenues dans votre référentiel de gestion des changements.

Résultat attendu : la section `updates` de la sonde contient vos fenêtres et votre préavis ; l'état de santé `updates` n'est plus en `WARNING` faute de fenêtre.

Vérification

- `GET /api/v1/settings/updates` renvoie les fenêtres et le préavis enregistrés.
- La page de santé de l'interface ou `GET /api/v1/system` n'indique plus d'avertissement lié à l'absence de fenêtre pour l'état de santé `updates`.
- À la prochaine mise à jour ordinaire, le champ `scheduledActivation` de `GET /api/v1/updates` indique une activation située dans l'une de vos fenêtres, annoncée au moins `notice` à l'avance (15 minutes au moins pour un correctif critique).

Erreurs possibles

Situation	Cause probable	Action
Paramètres refusés	Heure de début hors du format `HH:MM` ; plus de 7 fenêtres ; préavis supérieur à `7d` ; `drainTimeout` supérieur à `30m`	Corriger la valeur. Dans `provision.yaml`, écrire l'heure entre guillemets (chapitre 4)
Activation repoussée à une fenêtre ultérieure	La prochaine fenêtre commençait avant l'expiration du préavis : l'activation passe alors à la fenêtre suivante	Comportement normal. Ajouter une fenêtre ou réduire le préavis si ce délai est trop long
Deux sondes du même site redémarrent en même temps	Fenêtres qui se chevauchent ; écart entre fenêtres inférieur à la durée totale d'une activation ; activations manuelles simultanées	Décaler les fenêtres (étape 6) ; activer manuellement les sondes l'une après l'autre (§ 8.4.3)
Fausses alertes pendant la fenêtre	Périodes de maintenance des plateformes non alignées sur les fenêtres	§ 8.4.10 et chapitre 2 du guide d'intégration et d'observabilité

Précautions

- Une fenêtre trop courte peut ne pas laisser le temps d'un retour arrière ; préférez une marge confortable.
- Après un changement d'heure légale ou de fuseau horaire, vérifiez que vos fenêtres et les périodes de maintenance de vos plateformes restent alignées.
- Lors des changements d'heure légale, une fenêtre qui commence dans l'heure **inexistante** (passage à l'heure d'été) démarre à la première minute valide qui suit ; une fenêtre qui commence dans l'heure **répétée** (passage à l'heure d'hiver) n'a lieu qu'une seule fois, à la **première occurrence** de cette heure (heure d'été). Configurez les

outils de mise en sourdine de vos plateformes **dans le même fuseau** que la sonde : c'est nécessaire pour éviter un décalage d'une heure à chaque bascule, mais cela ne garantit pas que l'outil résout une heure inexistante ou répétée comme la sonde, chacun appliquant ses propres règles. Vérifiez la correspondance lors de la première bascule, ou évitez de placer le début d'une fenêtre entre 2 h et 3 h du matin.

- Lorsqu'une bascule intervient pendant une fenêtre, sa fin dépend de la sémantique de `windows[].duration` : la durée est un temps écoulé, compté depuis le début effectif de la fenêtre, de sorte que la fenêtre couvre toujours la durée choisie ; sa fin, exprimée en heure locale, se décale alors d'une heure par rapport au calcul « début plus durée » en heure civile. Un outil de sourdine défini par deux bornes civiles peut alors différer d'une heure de la fenêtre de la sonde cette nuit-là.
- Une modification du fuseau de la section `time` recalcule et réannonce les activations planifiées dans une fenêtre, dont les bornes sont des heures locales. Si le préavis devient insuffisant au regard de la nouvelle heure, l'activation passe à la fenêtre suivante. Une activation manuelle programmée par `scheduledAt` désigne un instant absolu en UTC : elle reste fixée à cet instant (§ 5.4).
- Revoyez les fenêtres lorsque l'activité supervisée change (nouvelle application, nouveaux horaires d'ouverture, nouveaux traitements par lots).

> ✓ **Conseil** — Pour un site équipé de deux sondes, une disposition simple consiste à placer leurs fenêtres le même jour de faible activité, à plusieurs heures d'intervalle, ou à des jours différents. Pendant les activations automatiques, la supervision du site reste ainsi assurée par au moins une sonde, à condition que l'écart dépasse la durée totale mesurée d'une activation ; les activations manuelles et `asap` ne sont pas coordonnées par ces fenêtres (§ 8.4.12).

8.4.9 Notification, drainage et état de maintenance

Une activation suit toujours la même chronologie, qu'elle ait lieu dans une fenêtre de maintenance ou à la demande d'un administrateur.

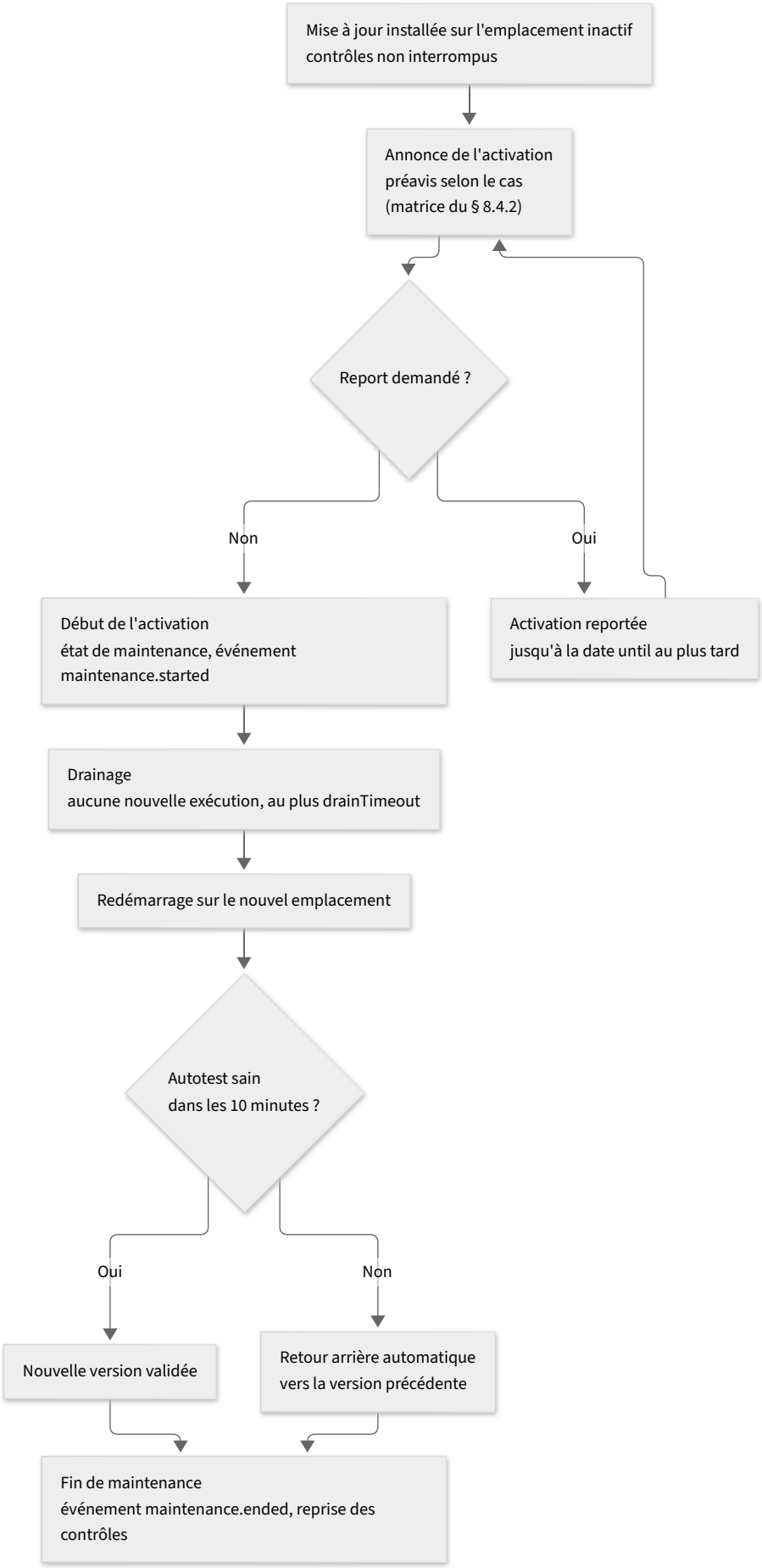


Schéma 8-2 — Chronologie d'une activation : notification, drainage, maintenance

1. Annonce. Dès qu'une activation est planifiée ou replanifiée, la sonde l'annonce par les moyens suivants, avec le préavis que fixe la matrice du § 8.4.2 pour son cas : au moins `notice` pour une activation automatique ordinaire, 15 minutes pour un correctif critique (augmentées du décalage en mode `asap`), le délai choisi pour une activation manuelle programmée, aucun pour une activation manuelle immédiate. Un préavis effectif inférieur à `notice` est signalé par `noticeReduced: true` :

Moyen	Contenu
Interface d'administration	Bandeau indiquant la mise à jour et l'heure prévue de son activation
`GET /api/v1/updates`	Champ `scheduledActivation` : activation planifiée
Journal d'audit	Planification de l'activation, puis report éventuel
Événement OTLP `update.scheduled`	Transmis aux destinations d'export (chapitre 2 du guide d'intégration et d'observabilité), à chaque planification et à chaque replanification
Événement OTLP `update.cancelled`	Activation annoncée qui n'aura pas lieu sous cet identifiant : report sans instant déterminable, image remplacée par une autre, canal passé en mode `manual` ou fenêtres supprimées, image retirée
Métrique `sva.update.pending` (unité `{state}`, attributs `sva.update.channel` et `sva.update.critical`)	Mise à jour en attente d'activation, avec son canal et son caractère critique
Métriques `sva.maintenance.next_start` et `sva.maintenance.next_end` (unité `s`, horodatages)	Début et fin **prévue** de la prochaine maintenance planifiée

Ces signaux permettent à vos équipes et à vos plateformes d'anticiper l'activation : vérifier les périodes de maintenance, prévenir les équipes concernées ou reporter l'activation (§ 8.4.2).

Identification et ordre des annonces. Chaque activation planifiée reçoit un **identifiant d'activation** unique (`activationId` dans l'API, attribut `sva.update.activation.id` des événements). Il reste le même tant que la même image doit être activée : report, nouvelle date, activation manuelle qui avance l'activation annoncée, recalcul après un changement de fuseau. Une nouvelle image reçoit un nouvel identifiant, et l'activation de l'image remplacée est annulée par `update.cancelled`. Chaque annonce porte en outre un **numéro d'annonce** (`sva.update.announcement.sequence`, repris par `scheduledActivation.sequence`), strictement croissant pour une même sonde, toutes activations confondues. Ce numéro ne régresse ni après un redémarrage, ni après un retour arrière, ni après une restauration de configuration. Il est dérivé de l'heure de la sonde : après le remplacement d'une sonde qui reprend l'identité de la précédente (§ 8.6), sa croissance n'est assurée que si l'heure de la nouvelle sonde est fiable (indicateur `clock` à `OK`, § 5.4).

Pour un automatisme qui reçoit ces événements, la règle est simple : pour une sonde donnée, **seule compte l'annonce de plus grand numéro**. Une annonce reçue en double, ou après une annonce de numéro supérieur, est ignorée. Le § 2.15.4 du guide d'intégration et d'observabilité en donne une mise en œuvre pour Alertmanager.

Les attributs de ces quatre événements (`update.scheduled`, `update.cancelled`, `maintenance.started`, `maintenance.ended`) sont décrits au § 2.3.6 du guide d'intégration et d'observabilité, qui fait référence : identifiant d'activation, numéro d'annonce, cas d'activation, canal, caractère critique, version, préavis réduit, bornes de maintenance, motif d'annulation et résultat.

Valeurs selon le mode d'activation. L'instant de l'annonce et la borne de fin dépendent du mode d'activation. Dans le tableau suivant, l'**annonce** est l'événement `update.scheduled` ; le **début annoncé** est la valeur de `scheduledActivation.at` et de `sva.maintenance.next_start` ; la **fin prévue** est celle de `windowEnd` et de `sva.maintenance.next_end`.

Mode d'activation	Annonce	`noticeReduced`	Début annoncé	Fin prévue
Automatique ordinaire	Au moins `notice` avant le début de la fenêtre retenue	`false`	Début de la fenêtre retenue	Fin de cette fenêtre
Manuelle immédiate (`POST /api/v1/updates/apply` sans `scheduledAt`)	Au début de l'activation, avec `maintenance.started`	`true`	Heure de réception de la demande (champ `at` de la réponse)	Aucune fenêtre : `windowEnd` vaut `null`
Manuelle à date fixe (`scheduledAt`)	À l'acceptation de la demande	`true` si `scheduledAt` précède l'expiration du préavis `notice` , `false` sinon	`scheduledAt`	Hors fenêtre : `windowEnd` vaut `null` . Date située dans une fenêtre : fin de cette fenêtre
Correctif critique, `criticalPolicy: asap`	Dès l'installation, au moins 15 minutes avant l'activation (§ 8.4.11)	`true` si 15 minutes augmentées du décalage restent inférieures à `notice`	Instant annoncé : 15 minutes après l'annonce, augmentées du décalage `security.criticalStagger` de la sonde (§ 8.4.11)	Aucune fenêtre : `windowEnd` vaut `null`
Correctif critique, `criticalPolicy: next-window`	Dès l'installation, au moins 15 minutes avant le début de la fenêtre retenue	`true` si le délai jusqu'à la fenêtre retenue est inférieur à `notice`	Début de la première fenêtre qui commence au moins 15 minutes après l'annonce	Fin de cette fenêtre

Lorsque `windowEnd` vaut `null` , la métrique `sva.maintenance.next_end` vaut `0` alors que `sva.maintenance.next_start` porte le début annoncé, et l'attribut `sva.maintenance.end` est **absent** de `update.scheduled` : aucune fin n'est annoncée, et la durée de la maintenance se prépare comme indiqué au paragraphe suivant. Sans fenêtre ni activation planifiée, les deux métriques valent `0` .

La **fin prévue** est une borne de planification. La **reprise réelle** est signalée par l'événement `maintenance.ended` (autotest réussi ou retour arrière terminé) : elle peut précéder la fin prévue ou la dépasser, par exemple lorsqu'une activation commencée en fin de fenêtre déborde (§ 8.4.8). Pour une activation hors fenêtre, dimensionnez la période de maintenance de vos plateformes sur une **durée maximale** que vous fixez d'après la durée totale observée d'une activation sur vos sondes, retour arrière compris (§ 8.4.5), puis levez-la dès la reprise vérifiée de la sonde (§ 8.4.12).

2. Début de l'activation et drainage. Au début de l'activation, la sonde passe en **état de maintenance** et émet l'événement `maintenance.started` . Aucune exécution nouvelle ne démarre. Les exécutions en cours disposent du délai `drainTimeout` (5 minutes par défaut, 30 minutes au maximum) pour se terminer normalement. Au-delà, elles sont interrompues et closes avec l'état `UNKNOWN` et le type d'erreur `maintenance` .

3. Redémarrage et autotest. La sonde redémarre sur le nouvel emplacement, puis vérifie son fonctionnement pendant 10 minutes au plus. En cas d'échec, elle revient automatiquement à la version précédente (§ 8.4.5).

4. Fin de maintenance. La sonde émet l'événement `maintenance.ended` , quitte l'état de maintenance et reprend ses contrôles à leur prochaine échéance. Cet événement est émis lorsque l'autotest a réussi, ou lorsque le retour arrière est terminé ; son attribut `sva.update.result` indique lequel. Il signale la fin de la maintenance, pas à lui seul le bon fonctionnement des contrôles : la reprise se vérifie comme au § 8.4.12.

Exposition de l'état de maintenance. Tant que la sonde répond, son état de maintenance est visible par les moyens suivants :

Moyen	Valeur pendant la maintenance
`GET /health`	`{"status": "MAINTENANCE"}`, avec le code HTTP `503`
Métrique `sva.agent.maintenance` (unité `{state}`, Prometheus `sva_agent_maintenance`)	`1`
Événements OTLP	`maintenance.started` au début, `maintenance.ended` à la fin
Plugin `check_sva` (Nagios, Centreon)	Code de retour `3` (`UNKNOWN`), avec le texte `MAINTENANCE` (§ 2.10 du guide d'intégration et d'observabilité)

> **Attention** — Pendant le redémarrage proprement dit, la sonde ne répond plus du tout : ni `/health`, ni les métriques, ni `check_sva` ne sont disponibles. L'état de maintenance ne peut donc pas, à lui seul, éviter les alertes de vos plateformes (§ 8.4.10).

Conséquences pour les contrôles

Situation	Conséquence
Exécution en cours au début de l'activation	Se termine normalement si elle s'achève dans le délai `drainTimeout` ; sinon, close en `UNKNOWN` avec le type d'erreur `maintenance`
Exécution prévue pendant la maintenance	Non lancée ; elle n'est pas rattrapée après la reprise (§ 8.2.3)
État `STALE`	Son calcul est suspendu pendant la maintenance et pendant un intervalle de planification de chaque contrôle après la reprise : une maintenance ne rend aucun contrôle `STALE`

> **Information** — Le type d'erreur `maintenance` signale une exécution interrompue par la sonde elle-même pour activer une mise à jour. Comme `agent_restart` (§ 8.2.3), il ne traduit aucun incident de la ressource supervisée. Vous pouvez l'exclure de vos calculs de disponibilité, selon la méthode convenue avec vos parties prenantes (chapitre 7 du guide d'utilisation et de supervision).

8.4.10 Éviter les fausses alertes pendant une maintenance

L'état de maintenance (§ 8.4.9) informe vos plateformes que la sonde va redémarrer, mais il **ne suffit pas à supprimer les alertes**. Pendant le redémarrage, la sonde est injoignable : Prometheus constate l'échec de la collecte, les métriques `sva.agent.up` cessent d'arriver, et `check_sva` ne reçoit aucune réponse. Sans précaution, vos plateformes déclenchent alors les alertes « sonde injoignable » ou « sonde muette », alors qu'il s'agit d'une opération planifiée.

Objectif : éviter que l'activation d'une mise à jour ne déclenche de fausses alertes, sans masquer une véritable panne.

Prérequis : fenêtres de maintenance définies (§ 8.4.8) ; accès à la configuration des alertes de vos plateformes.

Étapes

1. Dans chaque plateforme qui reçoit les données de la sonde, configurez une période de maintenance récurrente **alignée sur chacune des fenêtres** de la sonde (mêmes jours, même heure de début, même durée, même fuseau horaire). Les mécanismes à utiliser sont décrits au § 2.15 du guide d'intégration et d'observabilité : intervalles de temps d'Alertmanager, règles excluant les sondes en maintenance (`sva_agent_maintenance == 1`), temps d'arrêt programmés récurrents de Datadog, fenêtres de maintenance de Dynatrace, temps d'arrêt récurrents de Centreon, temps d'arrêt programmés de Nagios.

2. Limitez cette période aux alertes qui concernent **la sonde en maintenance** et les contrôles qu'elle exécute. Ne neutralisez pas les alertes des autres sondes du site, qui continuent de superviser (§ 8.4.12).
3. Pour une activation hors fenêtre, c'est-à-dire une activation manuelle (§ 8.4.3) ou un correctif critique en mode `asap` (§ 8.4.11), planifiez une période de maintenance ponctuelle limitée à la sonde concernée : **avant** de lancer une activation manuelle immédiate, car son annonce arrive au moment où elle commence ; **dès l'annonce** dans les autres cas, le préavis étant alors de 15 minutes au moins. Fixez sa durée maximale d'après la durée totale observée d'une activation, retour arrière compris, et levez-la après la reprise vérifiée de la sonde (§ 8.4.12). Une automatisation par événement est décrite au § 2.15.4 du guide d'intégration et d'observabilité.
4. Conservez une alerte qui se déclenche si la sonde n'est pas revenue **après la fin de la fenêtre** ou, sans fenêtre, après la durée maximale retenue (§ 8.7.1, alerte « maintenance anormalement longue ») : c'est elle qui révèle une activation qui a mal tourné.

Résultat attendu : une activation dans une fenêtre, ou couverte par une période ponctuelle, ne produit aucune alerte ; une sonde qui ne revient pas après la fin de la fenêtre ou de la période déclenche une alerte.

Vérification : lors de la première activation qui suit la configuration, contrôlez dans vos plateformes qu'aucune alerte n'a été déclenchée pendant la fenêtre, et que les événements `maintenance.started` et `maintenance.ended` ont bien été reçus.

Erreurs possibles

Situation	Cause probable	Action
Alerte « sonde injoignable » pendant la fenêtre	Période de maintenance de la plateforme absente, décalée ou exprimée dans un autre fuseau horaire	Réaligner la période sur la fenêtre de la sonde
Aucune alerte alors que la sonde n'est jamais revenue	Période de maintenance plus longue que la fenêtre, ou alerte de maintenance anormalement longue absente	Limiter la période à la fenêtre ; ajouter l'alerte du § 8.7.1

> **Avertissement** — Une période de maintenance trop large masque les véritables pannes. Ne neutralisez jamais durablement les alertes d'une sonde au motif qu'elle se met à jour.

Les configurations détaillées propres à chaque plateforme figurent au § 2.15.2 à § 2.15.5 du guide d'intégration et d'observabilité.

8.4.11 Correctifs de sécurité critiques

Un correctif est dit **critique** lorsqu'il corrige une vulnérabilité activement exploitée. Il suit un traitement accéléré :

1. **Installation immédiate.** Dès sa publication, le correctif est téléchargé et installé sur l'emplacement inactif, sans interrompre les contrôles. Lorsque le canal `security` est en mode `manual`, le correctif n'est jamais activé automatiquement : l'état de santé `updates` passe en `CRITICAL`, la notification est émise, et l'administrateur décide de l'activation.
2. **Avis de sécurité.** L'éditeur publie un avis de sécurité qui décrit la vulnérabilité et le correctif sur le site de l'éditeur ; l'avis est aussi joint à la mise à jour dans `GET /api/v1/updates`.
3. **Signalement sur la sonde.** L'état de santé `updates` passe en `CRITICAL` et la métrique `sva.update.pending` porte l'attribut `sva.update.critical` égal à `true`.
4. **Activation** selon le paramètre `security.criticalPolicy` :

Valeur	Activation	Préavis	Recommandé pour
`next-window` (par défaut)	Au début de la première fenêtre de maintenance qui commence au moins 15 minutes après l'annonce ; une fenêtre plus proche, ou déjà commencée, n'est pas admissible et l'activation attend la suivante	15 minutes au moins	La plupart des organisations : l'interruption reste dans un créneau maîtrisé
`asap`	15 minutes après l'annonce, augmentées du décalage `security.criticalStagger` éventuel de la sonde, sans attendre une fenêtre, y compris si aucune fenêtre n'est définie	15 minutes, augmentées du décalage	Sondes exposées à un risque élevé, ou organisations dont les fenêtres sont espacées

Dans tous les cas, l'activation est annoncée et précédée du drainage des exécutions (§ 8.4.9). **Aucun redémarrage immédiat n'est imposé, et aucun redémarrage hors de vos fenêtres n'a lieu par défaut** : le mode `asap` résulte toujours d'un choix explicite d'un administrateur. Sans fenêtre définie, un correctif critique en mode `next-window` reste en attente, avec l'état de santé `updates` en `CRITICAL`, jusqu'à ce qu'un administrateur l'active (§ 8.4.3) ; en mode `asap`, il est activé à l'instant annoncé. L'activation peut être reportée de **7 jours au plus** (§ 8.4.2), et un administrateur peut toujours l'avancer en l'activant lui-même.

> **Information** — Avec `criticalPolicy: asap`, l'activation peut avoir lieu **hors de vos fenêtres**. C'est, avec l'activation manuelle (§ 8.4.3), l'une des deux exceptions documentées à la règle selon laquelle une activation commence dans l'une des fenêtres que vous avez choisies (§ 8.4.12). Si vous retenez `asap`, prévoyez dans vos plateformes une neutralisation des alertes adaptée à une maintenance non planifiée (§ 8.4.10), sans masquer les alertes des autres sondes du site.

Échelonner les sondes d'un même site (`security.criticalStagger`). Un correctif critique est publié pour toutes les sondes en même temps. En mode `asap`, sans précaution, les sondes d'un même site l'activeraient donc à quelques instants d'intervalle, et la supervision du site serait interrompue. Pour l'éviter, le paramètre `security.criticalStagger` retarde l'activation d'une durée **fixe, propre à chaque sonde** :

- l'activation a lieu 15 minutes après l'annonce, augmentées de ce décalage ; l'instant obtenu est annoncé dès l'installation du correctif, comme toute activation (§ 8.4.9) ;
- la valeur est **déterministe** : elle est choisie par l'administrateur, sans tirage aléatoire, et donne toujours le même ordre d'activation ;
- elle va de `0` (valeur par défaut, aucun décalage) à `4h`. Les métadonnées signées d'un correctif peuvent imposer un plafond inférieur lorsque son urgence l'exige ;
- le décalage est calculé **une seule fois** pour une image préparée. Il ne se renouvelle pas et ne se cumule pas avec un report : un correctif critique n'est jamais retardé indéfiniment, et son report reste limité à 7 jours (§ 8.4.2) ;
- il ne s'applique ni au mode `next-window`, ni au mode `manual`, ni à une activation manuelle.

Sur un site équipé de deux sondes, laissez par exemple `0` sur la première et attribuez à la seconde un décalage supérieur à la durée totale mesurée d'une activation, retour arrière compris (§ 8.4.8), telle que vous l'observez entre les événements `maintenance.started` et `maintenance.ended` (§ 8.4.9).

> **Attention** — Un décalage temporel **ne garantit pas** que l'autre sonde soit opérationnelle. Les sondes sont autonomes : aucune ne connaît l'état des autres. Le décalage ne vérifie ni que la première sonde a terminé son activation, ni qu'elle n'est pas en retour arrière, ni qu'elle n'était pas déjà hors service. Deux activations peuvent encore se recouvrir si l'écart entre les décalages est trop court, ou en cas d'activation manuelle. La sonde ne garantit donc pas l'absence de redémarrage simultané. Pour les environnements critiques, appliquez les recommandations du § 8.4.12.

Objectif : traiter un correctif critique dans les meilleurs délais, en maîtrisant l'interruption de la supervision.

Prérequis : rôle `admin` ; alerte « correctif critique en attente » configurée (§ 8.7.1).

Étapes

1. À réception de l'alerte ou de l'avis de sécurité, consultez `GET /api/v1/updates` : version du correctif, champ `scheduledActivation`.
2. Lisez l'avis de sécurité et évaluez l'exposition de la sonde.
3. Choisissez l'une des options suivantes :
   - laisser l'activation se faire à l'instant annoncé ;
   - l'avancer en l'activant vous-même, immédiatement ou à une heure donnée (§ 8.4.3), après avoir planifié une période de maintenance dans vos plateformes (§ 8.4.10) ;
   - la reporter, pour une raison justifiée (période critique pour l'activité), de 7 jours au plus (`POST /api/v1/updates/postpone`).

   Tant que le correctif n'est pas actif, appliquez si nécessaire des **mesures compensatoires**, par exemple suspendre les scénarios navigateur qui visitent des applications exposées à Internet ou des contenus que vous ne maîtrisez pas, ou restreindre temporairement les flux sortants de la sonde (chapitre 5). Levez-les une fois le correctif actif.
4. Après l'activation, vérifiez la version active dans `GET /api/v1/updates` et le retour de l'état de santé `updates` à `OK` .

Résultat attendu : le correctif est actif ; l'état de santé `updates` n'est plus en `CRITICAL` .

Erreurs possibles : un report au-delà de 7 jours est refusé ; un retour arrière automatique laisse le correctif inactif et doit être signalé au support (§ 8.4.5).

Cas urgents. Lorsque l'avis de sécurité signale une exploitation active susceptible de toucher la sonde elle-même, et que votre prochaine fenêtre est lointaine :

1. Appliquez immédiatement les mesures compensatoires décrites à l'étape 3.
2. Planifiez une période de maintenance ponctuelle dans vos plateformes (§ 8.4.10).
3. Activez le correctif manuellement, immédiatement ou à une heure proche (§ 8.4.3). Sur un site équipé de plusieurs sondes, traitez-les l'une après l'autre, jamais simultanément (§ 8.4.12).
4. Vérifiez la version active et l'état de santé `updates` , puis levez les mesures compensatoires.

Pour un traitement durable, envisagez `criticalPolicy: asap` ou des fenêtres plus rapprochées.

> **Avertissement** — Une sonde qui exécute des scénarios navigateur visite des applications web avec Chromium. Un correctif critique de Chromium réduit un risque réel : ne reportez son activation que pour une raison précise, et jamais par défaut.

8.4.12 Continuité de service et redondance

Une sonde unique **ne supervise pas pendant son propre redémarrage**. Pendant l'activation d'une mise à jour (§ 8.4.9), les contrôles qu'elle exécute sont suspendus : une panne survenant à ce moment ne serait détectée qu'après son retour. Pour la plupart des usages, cette interruption brève et planifiée est acceptable. Pour les environnements critiques, elle ne l'est pas.

Architecture recommandée pour les environnements critiques

Principe	Mise en œuvre
Au moins **deux sondes par site**	Chaque sonde exécute les mêmes contrôles, sur les mêmes cibles

Principe	Mise en œuvre
Fenêtres **qui ne se chevauchent pas**	L'écart entre les fenêtres des sondes d'un même site dépasse la durée totale mesurée d'une activation, retour arrière compris (§ 8.4.8), afin que leurs activations automatiques ne se recouvrent pas ; elles ne sont jamais activées manuellement en même temps (§ 8.4.3). Cet espacement ne coordonne pas les activations `asap`, qui ont lieu hors fenêtre (§ 8.4.11)
Activations critiques **échelonnées**	Avec `criticalPolicy: asap`, un décalage `security.criticalStagger` différent sur chaque sonde du site (§ 8.4.11). Le décalage réduit le risque d'activations simultanées sans le supprimer : il ne vérifie pas l'état des autres sondes
Retour en service **vérifié**	Pour les environnements critiques : fenêtres distinctes avec `criticalPolicy: next-window`, ou orchestration externe qui n'active une sonde qu'après le retour vérifié de la précédente (ci-dessous)
Alertes fondées sur **l'ensemble des sondes** du site	Une alerte ne dépend jamais d'une seule sonde : elle est évaluée à partir des résultats de toutes les sondes qui répondent
Indépendance matérielle	Si possible, alimentations et raccordements réseau distincts (commutateurs différents), pour qu'un même incident local n'affecte pas toutes les sondes

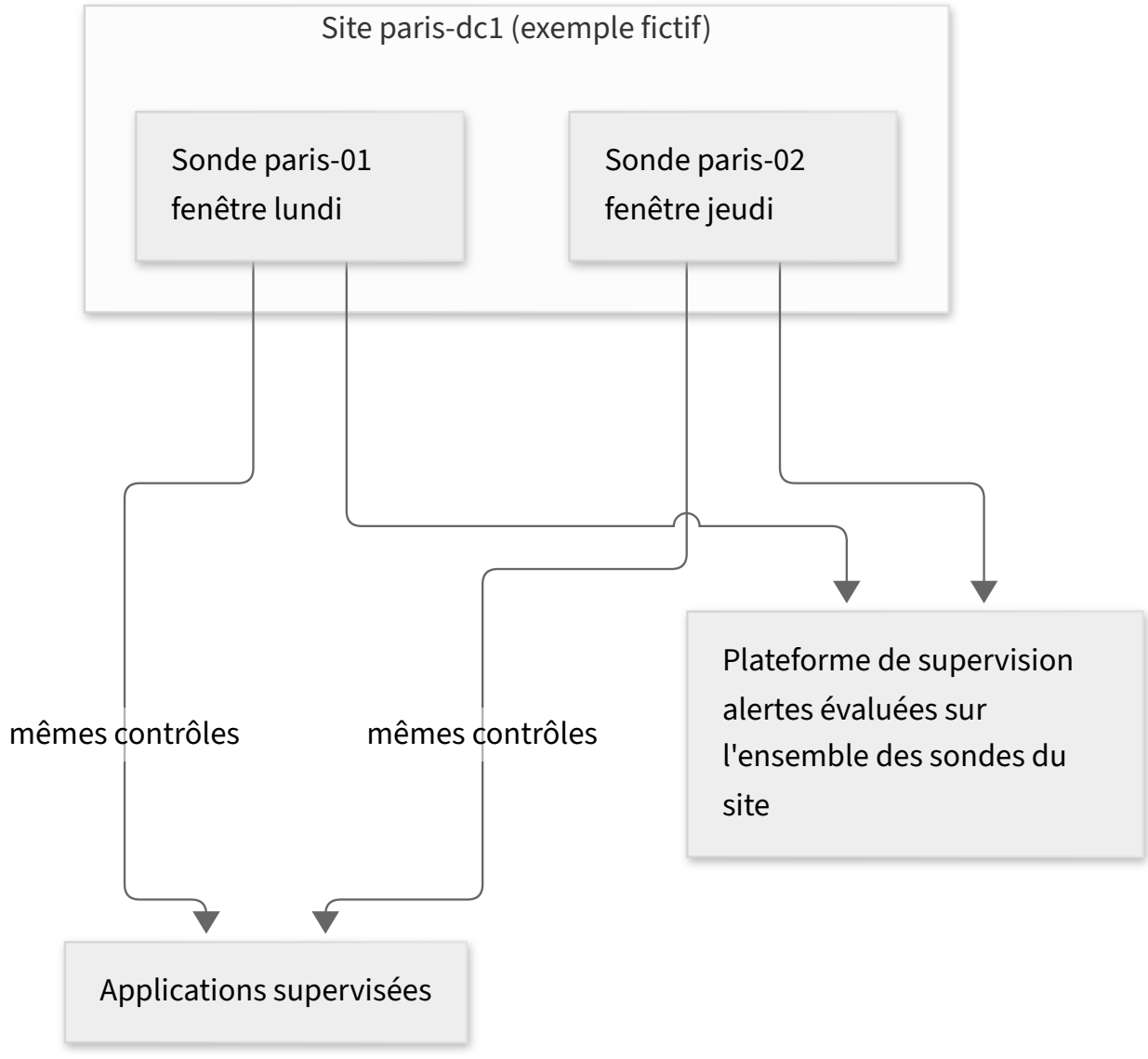


Schéma 8-3 — Redondance : plusieurs sondes sur un même site

Objectif : maintenir la supervision d'un site pendant la maintenance de l'une de ses sondes.

Prérequis

- Au moins deux sondes installées sur le site (chapitres 3 et 4), chacune avec sa propre carte microSD de l'édition requise, et le même paramètre `site`.
- Une plateforme de supervision capable d'agréger les résultats de plusieurs sondes (chapitre 2 du guide d'intégration et d'observabilité).

Étapes

1. Installez et mettez en service la seconde sonde, avec le même paramètre `site` que la première (chapitre 4).
2. Exportez la configuration de la première sonde (§ 8.5.2), puis importez-la sur la seconde avec le paramètre `newIdentity=true` (§ 8.5.3) : les deux sondes exécutent les mêmes contrôles, avec les mêmes identifiants de contrôle, tout en restant distinctes dans vos plateformes.
3. Attribuez à chaque sonde des fenêtres de maintenance qui ne se chevauchent pas (§ 8.4.8). L'import ayant recopié la section `updates`, modifiez les fenêtres de la seconde sonde.
4. Créez des règles d'alerte fondées sur l'ensemble des sondes du site (règles d'alerte de site ci-dessous ; groupe `sondes-site` du § 2.15.6 du guide d'intégration et d'observabilité), en complément des alertes de santé propres à chaque sonde (§ 8.7.1).
5. Configurez les périodes de maintenance de vos plateformes sonde par sonde (§ 8.4.10).
6. Si vous retenez `criticalPolicy: asap`, attribuez à chaque sonde un décalage `security.criticalStagger` différent (§ 8.4.11).

Orchestration externe des activations (environnements critiques). Les sondes ne se coordonnent pas entre elles. Lorsque l'interruption simultanée de la supervision d'un site n'est pas acceptable, confiez l'enchaînement des activations à votre propre outil d'automatisation, avec l'API existante :

1. Placez le canal `security` des sondes du site en mode `manual` : aucune activation n'a lieu sans votre outil.
2. Activez la première sonde (`POST /api/v1/updates/apply`, § 8.4.3).
3. Conservez l'identifiant `activationId` renvoyé par la réponse de l'activation, ainsi que la version attendue (`staged.version` de `GET /api/v1/updates`, relevée avant l'activation).
4. Attendez son retour en service effectif, et non un simple délai. Interrogez `GET /api/v1/updates` à intervalles réguliers, jusqu'à un délai maximal que vous fixez d'après la durée totale observée d'une activation, retour arrière compris. La sonde n'est revenue en service que si **toutes** les conditions suivantes sont réunies :
   - `lastResult` n'est pas `null` et `lastResult.activationId` est égal à l'identifiant conservé à l'étape 3 ;
   - `lastResult.outcome` vaut `succeeded` ;
   - la version de l'emplacement actif (`slots` et `activeSlot`) est la version attendue ;
   - `state` ne vaut pas `maintenance` ;
   - `/health` répond `OK` (§ 4.6.2) ;
   - votre plateforme de supervision reçoit de cette sonde des résultats d'exécution postérieurs à `lastResult.finishedAt`.
5. Seulement alors, activez la sonde suivante.

Interprétez les autres situations ainsi :

Situation observée	Signification	Action
`lastResult` à `null`, ou `activationId` différent de celui de l'étape 3	Le résultat ne concerne pas votre activation : elle n'a pas encore produit de résultat, ou il s'agit d'une tentative antérieure	Continuer d'attendre, jusqu'au délai maximal

Situation observée	Signification	Action
`outcome` à `in_progress`, ou `state` à `maintenance`	Activation en cours (drainage, redémarrage ou autotest)	Continuer d'attendre, jusqu'au délai maximal
`outcome` à `rolled_back`	Retour arrière automatique : l'ancienne version est active	Arrêter l'enchaînement et traiter l'incident (§ 9.7)
`outcome` à `failed`	Échec avant redémarrage : l'emplacement actif est inchangé	Arrêter l'enchaînement et traiter l'incident
`outcome` à `succeeded`, mais version active différente de la version attendue	Incohérence : une autre image a été activée	Arrêter l'enchaînement et vérifier `GET /api/v1/updates` et le journal d'audit
Conditions réunies, sauf l'arrivée de résultats récents	La sonde a redémarré mais ne supervise pas, ou ses résultats ne parviennent pas à la plateforme	Ne pas poursuivre ; vérifier les destinations d'export et les contrôles de la sonde
Délai maximal dépassé	Sonde injoignable ou activation bloquée	Arrêter l'enchaînement ; intervenir sur la sonde (chapitre 9)

Un succès antérieur ne prouve jamais la reprise : `lastResult` désigne la **dernière tentative**, quelle que soit l'activation. La jauge `sva.update.last_result` peut servir de signal complémentaire dans vos tableaux de bord, mais elle ne porte ni la version ni l'identifiant d'activation : elle ne suffit pas à valider une étape d'orchestration. De même, le décalage `security.criticalStagger` (§ 8.4.11) réduit le risque d'activations simultanées, mais ne vérifie pas le retour des autres sondes.

> ! **Attention** — En mode `manual`, la sonde n'active jamais d'elle-même un correctif critique (§ 8.4.11). La priorité du correctif repose alors sur votre procédure : l'état de santé `updates` reste en `CRITICAL` et l'alerte « correctif critique en attente » (§ 8.7.1) reste active jusqu'à l'activation. Fixez dans votre procédure un délai maximal de traitement, afin que la coordination ne retarde jamais indéfiniment un correctif de sécurité.

> → **Évolution prévue** — La console de gestion centralisée prévue (§ 1.6) doit permettre d'orchestrer **séquentiellement** les mises à jour des sondes d'un même site : chaque activation ne serait engagée qu'après le retour vérifié de la précédente à un état sain, avec un délai maximal au-delà duquel un correctif critique serait activé malgré tout. Elle est prévue dans une version ultérieure ; la sonde ne dépendra jamais de cette console pour fonctionner.

Règles d'alerte de site. Deux alertes distinctes sont nécessaires, car un échec applicatif et une perte de couverture appellent des réactions différentes. Une sonde est dite **évaluable** pour un contrôle lorsqu'elle en fournit un résultat `OK`, `WARNING` ou `CRITICAL` et qu'elle n'est pas en maintenance.

Alerte	Se déclenche lorsque	Signification
`ParcoursEnEchecSurLeSite`	Toutes les sondes évaluables du site voient le contrôle en `CRITICAL`, au moins une sonde étant évaluable	Incident probable de l'application ou du parcours supervisé
`CouvertureInsuffisanteSurLeSite`	Le nombre de sondes évaluables est inférieur à l'effectif attendu du site, y compris lorsqu'aucune sonde ne fournit plus de résultat évaluable	Perte de couverture : la supervision du site repose sur moins de sondes que prévu, ou n'est plus assurée

Ces deux alertes forment le groupe de règles Prometheus `sondes-site`, fourni prêt à charger dans le fichier `exemples/prometheus/sva-regles-alerte.yml`. Leurs expressions PromQL, le seul paramètre à adapter (l'effectif attendu de chaque site, `sva:site_effectif_attendu`), leurs limites, l'extension facultative `sondes-site-controles` et l'adaptation au mode envoi (label `sva_site`) sont décrits au § 2.15.6 du guide d'intégration et d'observabilité.

> **Information** — L'alerte de couverture se déclenche aussi pendant la maintenance planifiée d'une sonde, puisque celle-ci n'est plus évaluable. Choisissez pour elle un délai `for` supérieur à la durée totale mesurée d'une activation (§ 8.4.5), ou neutralisez cette seule alerte pendant les fenêtres des sondes du site (§ 8.4.10). Ne neutralisez jamais `ParcoursEnEchecSurLeSite` : c'est elle qui détecte un incident pendant la maintenance d'une sonde.

Résultat attendu : pendant la maintenance d'une sonde, la supervision du site reste assurée par les autres, et les alertes restent fondées sur leurs résultats.

Vérification : activez une mise à jour sur l'une des sondes (§ 8.4.3), ou attendez sa fenêtre, et vérifiez que l'autre continue de publier ses résultats et que la règle reste évaluée.

Erreurs possibles

Situation	Cause probable	Action
Alerte déclenchée pendant la maintenance d'une sonde	Règle fondée sur une seule sonde ; label `site` (ou `sva_site`) absent	Réécrire la règle sur l'ensemble des sondes ; vérifier les labels
Aucune supervision pendant une fenêtre	Fenêtres des sondes qui se chevauchent ; activation qui déborde sur la fenêtre de l'autre sonde ; activations manuelles simultanées	Décaler les fenêtres en tenant compte de la durée totale d'une activation (§ 8.4.8) ; activer les sondes l'une après l'autre
`CouvertureInsuffisanteSurLeSite` à chaque activation planifiée	Délai `for` inférieur à la durée d'une activation	Allonger le délai `for` ou neutraliser cette seule alerte pendant les fenêtres du site
Résultats divergents entre les sondes	Configurations différentes, ou accès réseau différents	Réimporter la configuration ; comparer les flux réseau des deux sondes (chapitre 5)

> **Information** — La durée pendant laquelle une sonde ne supervise pas lors d'une activation s'observe entre les événements `maintenance.started` et `maintenance.ended` (§ 8.4.5, § 8.4.9). Pour les sites qui ne disposent que d'une sonde, cette durée est la seule interruption planifiée de la supervision. Une activation **automatique** commence dans l'une des fenêtres que vous avez choisies, mais elle peut se prolonger au-delà de la fin de la fenêtre lorsque sa durée totale, retour arrière éventuel compris, dépasse le temps restant dans la fenêtre (§ 8.4.8). L'activation manuelle par un administrateur (§ 8.4.3) et l'activation d'un correctif critique avec `criticalPolicy: asap` (§ 8.4.11) peuvent en outre intervenir hors fenêtre. Sur un site redondant, l'espacement des fenêtres ne coordonne pas les activations `asap` : un même correctif critique publié pour toutes les sondes du site peut les activer à des instants proches, sauf si vous leur attribuez des décalages `security.criticalStagger` différents (§ 8.4.11), qui réduisent ce risque sans l'exclure.

8.5 Sauvegarde et restauration de la configuration

8.5.1 Sauvegarde automatique locale

La sonde sauvegarde automatiquement sa configuration une fois par jour et conserve les **trois dernières générations**. Cette sauvegarde lui sert à se restaurer elle-même si sa base de données est corrompue. Elle est stockée sur la même carte que la sonde : elle ne protège donc **pas** contre la perte ou la panne de la carte.

8.5.2 Exporter la configuration

Objectif : conserver hors de la sonde une copie de sa configuration, pour la restaurer sur une nouvelle carte ou une nouvelle sonde.

Prérequis : rôle `admin`.

Étapes

1. Lancez l'export depuis l'interface d'administration ou par l'API :

   ```bash
   sapi -o sonde-paris-01-config-2026-11-19.json \
        "$SONDE/api/v1/config/export"
   ```

   L'archive est un document JSON. Sans autre option, elle ne contient ni les comptes ni les secrets.

2. Choisissez le traitement des secrets :
   - **sans les secrets** (recommandé pour l'archivage courant) : il faudra les ressaisir lors d'une restauration ;
   - **avec les secrets chiffrés par une phrase de passe** : l'export se demande alors en `POST`, avec la phrase de passe dans l'en-tête `X-Config-Passphrase`, comme pour l'import, et jamais dans l'adresse, qui peut être journalisée. La phrase de passe est lue sans affichage et placée dans un fichier d'en-tête temporaire, lisible par vous seul et supprimé aussitôt (même méthode qu'au § 6.12.2) :

     ```bash
     (
       umask 077
       ENTETE=$(mktemp) && trap 'rm -f "$ENTETE"' EXIT &&
       IFS= read -rs PHRASE &&
       printf 'X-Config-Passphrase: %s\n' "$PHRASE" > "$ENTETE" &&
       unset PHRASE &&
       sapi -X POST -H @"$ENTETE" \
         -o "sonde-paris-01-config-$(date +%Y%m%d).json" \
         "$SONDE/api/v1/config/export"
     )
     ```

     L'archive inclut les comptes (empreintes des mots de passe) et les secrets, chiffrés en AES-256-GCM avec une clé dérivée de la phrase de passe par Argon2id. À l'import, la phrase de passe est transmise de la même manière (§ 8.5.3). Conservez-la dans votre coffre-fort de mots de passe, jamais à côté de l'archive.

3. Rangez l'archive dans un espace de stockage sécurisé de votre entreprise, avec un nom indiquant la sonde et la date.

Résultat attendu : une archive contenant les contrôles, plans d'exécution, scripts, destinations d'export et paramètres, à l'exception de la section `network`. Les comptes et les secrets n'y figurent, chiffrés, que si une phrase de passe a été fournie.

> ✓ **Conseil** — Exportez la configuration après chaque modification importante et au moins une fois par mois. Pour les équipes qui gèrent la supervision « as code », l'archive ou ses composants peuvent être versionnés dans un dépôt de gestion de configuration, à condition d'en exclure les secrets.

8.5.3 Restaurer une configuration

1. Sur la sonde cible (mise en service effectuée, compte administrateur créé), validez d'abord l'archive **sans l'appliquer** :

   ```bash
   sapi -X POST \
        -H "Content-Type: application/json" \
        --data-binary @sonde-paris-01-config-2026-11-19.json \
        "$SONDE/api/v1/config/import?dryRun=true"
   ```

   L'archive est transmise telle qu'elle a été exportée, au même format JSON. La réponse est un compte rendu JSON qui indique les éléments qui seraient créés ou modifiés, et les erreurs éventuelles (par exemple, un type de contrôle non couvert par l'édition de la sonde cible).

2. Corrigez les erreurs signalées, puis relancez l'import sans `dryRun=true` :

   ```bash
   # Import effectif. Pour une archive chiffrée par une phrase de passe (§ 8.5.2),
   # transmettez aussi l'en-tête X-Config-Passphrase par un fichier d'en-tête temporaire
   # (-H @"$ENTETE"), créé comme pour l'export, jamais par une valeur en argument.
   sapi -X POST \
        -H "Content-Type: application/json" \
        --data-binary @sonde-paris-01-config-2026-11-19.json \
        "$SONDE/api/v1/config/import"
   ```

3. Ressaisissez les secrets si l'archive n'en contenait pas (chapitre 6).
4. Vérifiez les destinations d'export avec leur fonction de test.
5. Lancez une exécution d'essai des contrôles principaux.

> ! **Attention** — L'archive ne contient pas la section `network` : les paramètres réseau de la sonde cible sont conservés. En revanche, l'identifiant de la sonde (`service.instance.id`) est restauré par défaut. Pour appliquer la configuration à une sonde destinée à fonctionner en parallèle de la sonde d'origine, ajoutez le paramètre `newIdentity=true` à la requête d'import, afin que les deux sondes restent distinctes dans les plateformes d'observabilité.

8.6 Remplacer une carte microSD ou une sonde

8.6.1 Cas d'usage

- Carte microSD défaillante ou en fin de vie (§ 9.3 et § 9.6).
- Raspberry Pi 5 défaillant.
- Remplacement préventif programmé.
- Changement d'édition : la nouvelle édition est livrée sur une nouvelle carte (§ 8.6.5). Si l'édition visée exige plus de mémoire, remplacez aussi le Raspberry Pi 5 (par exemple, un modèle de 8 Go pour l'édition Enterprise).

8.6.2 Procédure

Prérequis : une nouvelle carte microSD préparée par l'éditeur, de l'édition voulue, avec son encart (code d'installation). Chaque carte porte son propre certificat d'édition : une image écrite par vos soins sur une autre carte démarrerait en mode restreint (§ 4.5). Vous avez aussi besoin du dernier export de configuration (§ 8.5.2) et des secrets si l'export n'en contient pas. La carte se commande auprès de l'éditeur, selon les conditions de votre contrat.

Étapes

1. Si l'ancienne sonde fonctionne encore, exportez sa configuration et arrêtez-la proprement (§ 8.2.2).
2. Débranchez l'alimentation, retirez l'ancienne carte (chapitre 3) et étiquetez-la « à effacer ».
3. Insérez la nouvelle carte. Pour retrouver rapidement l'adresse et l'identité précédentes, déposez au préalable un fichier `provision.yaml` reprenant le nom d'hôte, le site et la configuration réseau d'origine (chapitre 4).
4. Mettez sous tension et effectuez la mise en service (chapitre 4).
5. Importez la configuration (§ 8.5.3) et ressaisissez les secrets si nécessaire.
6. Installez le certificat de l'entreprise si l'ancienne sonde en utilisait un (chapitre 5).
7. **Révoquez** les jetons d'API de l'ancienne sonde qui ne sont plus utilisés, puis créez-en de nouveaux pour Prometheus, Nagios ou Centreon et vos automatisations. Mettez à jour ces outils.
8. Vérifiez que les plateformes d'observabilité reçoivent de nouveau les données, et que la politique de mises à jour (section `updates`, restaurée par l'import) convient toujours : fenêtres de maintenance, et décalage par rapport aux autres sondes du site (§ 8.4.8, § 8.4.12).
9. Effacez de manière sécurisée l'ancienne carte (§ 8.13).

> **Information** — L'identifiant unique de la sonde (`service.instance.id` dans la télémétrie) est généré au premier démarrage. Lors de l'import de la configuration (étape 5), il est **restauré par défaut** : la sonde remplacée conserve son identifiant. La portée de cette continuité dépend du mode de transmission :
>
> - **en mode envoi (OTLP)**, `service.instance.id` restauré est une condition de la continuité des séries dans les plateformes d'observabilité, mais il ne suffit pas à l'assurer : l'identité finale d'une série dépend aussi des autres attributs de ressource exportés (nom d'hôte, site, version), de ceux que la destination promeut en labels ou en dimensions, et des règles propres à chaque destination. Vérifiez sur votre plateforme que les séries de la sonde remplacée se poursuivent ;
> - **en mode collecte (Prometheus)**, le label `instance` est dérivé de l'adresse de la cible collectée, et non de `service.instance.id` : les séries ne se poursuivent sous le même label que si la cible déclarée dans Prometheus reste identique : même nom d'hôte si la cible est déclarée par son nom, même adresse IP si elle l'est par son adresse (fichier de provisionnement, étape 3).
>
> Dans les deux cas, les **compteurs repartent de zéro** sur la nouvelle sonde ; les fonctions `increase()` et `rate()` de PromQL traitent cette réinitialisation sans erreur. **Mettez l'ancienne sonde hors service avant de réutiliser son identité** : deux sondes qui émettent le même identifiant en même temps mélangent leurs séries. Le nom d'hôte et le site (`sva.site`), repris par le fichier de provisionnement, complètent cette continuité. Si vous n'importez pas de configuration, ou si vous ajoutez le paramètre `newIdentity=true` (§ 8.5.3), la sonde apparaît sous un nouvel identifiant : prévoyez alors de supprimer l'ancienne instance de vos inventaires.

> **Information** — L'historique des exécutions n'est pas inclus dans l'export de configuration. Il est perdu lors d'un remplacement de carte. L'historique transmis aux plateformes d'observabilité reste disponible dans celles-ci. Si la sonde utilise un SSD (§ 8.3.4), l'historique est stocké sur celui-ci et non sur la microSD ; il n'est pas repris par la nouvelle carte : l'activation du SSD par celle-ci (§ 8.3.4) le reformate. Une réinitialisation usine efface également le SSD.

8.6.3 Carte de rechange

Pour les sondes critiques, conservez une carte de rechange de la même édition, acquise auprès de l'éditeur, accompagnée d'un `provision.yaml` prêt à l'emploi et du dernier export de configuration. Le remplacement prend alors quelques minutes. Le fichier de provisionnement contient des informations sensibles : conservez la carte de rechange dans un lieu sécurisé.

8.6.4 Remplacer une carte défectueuse

Le droit d'utilisation du logiciel intégré est attaché à la carte livrée. Si cette carte devient défectueuse, elle est **remplacée par une carte de la même édition, sans rachat du produit**. La nouvelle carte porte un nouveau certificat d'édition.

Prérequis : numéro de série du produit (encart, étiquette, ou état de santé `GET /api/v1/system` si la sonde démarre encore) ; description des symptômes (§ 9.3 et § 9.6) ; si possible, un export récent de la configuration (§ 8.5.2).

Étapes

1. Contactez le support (§ 10.5) en indiquant le numéro de série et les symptômes. Si la sonde démarre encore, joignez une archive de diagnostic (§ 9.9).
2. Après confirmation du défaut, le support vous adresse une carte de remplacement de la même édition, avec son encart.
3. Retournez la carte défectueuse selon les instructions du support, ou détruisez-la selon la procédure qu'il vous indique. Une carte défectueuse contient encore vos secrets chiffrés et leur clé de chiffrement. **Si elle ne peut plus être effacée** (carte illisible), vous n'êtes pas tenu de la retourner : vous pouvez la conserver dans un lieu sécurisé, ou la détruire physiquement et fournir au support une **attestation de destruction** à la place du retour. Le remplacement reste acquis dans ce cas. Pour toute carte retournée, joignez une preuve d'effacement (§ 8.13). Demandez au support le modèle d'attestation de destruction et ses modalités de transmission.
4. Installez la carte de remplacement en suivant la procédure du § 8.6.2.

Les conditions de remplacement, pendant et après la période de garantie, sont celles de votre contrat.

> ✓ **Conseil** — La rapidité d'un remplacement dépend surtout de la fraîcheur de votre dernier export de configuration. Exportez la configuration après chaque modification importante (§ 8.5).

8.6.5 Changer d'édition

Une édition supérieure est livrée sur une **nouvelle carte microSD**. Votre configuration, vos scénarios et vos secrets y sont transférés par un export suivi d'un import. L'ancienne carte reste un produit utilisable dans son édition d'origine, sauf si vous la restituez dans le cadre d'une offre de reprise, selon les conditions de votre contrat.

Prérequis : la carte de la nouvelle édition et son encart ; rôle `admin` sur la sonde actuelle ; un Raspberry Pi 5 dont la capacité mémoire convient à la nouvelle édition (§ 2.1.2).

> ℹ **Information** — Si la sonde utilise un SSD NVMe (§ 8.3.4), il reste en place : le changement d'édition ne concerne que la carte microSD, qui porte le certificat d'édition, la configuration et les secrets. L'historique des exécutions, stocké sur le SSD, suit la règle du § 8.6.2.

Étapes

1. Exportez la configuration **avec une phrase de passe**, afin d'inclure les comptes et les secrets, chiffrés (§ 8.5.2). Choisissez une phrase de passe longue et conservez-la dans votre coffre-fort de mots de passe, séparément de l'archive.

2. Arrêtez proprement la sonde (§ 8.2.2), puis remplacez la carte. Pour retrouver le même nom d'hôte et la même adresse, déposez au préalable sur la nouvelle carte un `provision.yaml` reprenant ces paramètres (chapitre 4).
3. Mettez la sonde sous tension et terminez la mise en service. Vérifiez que l'édition affichée est la nouvelle édition (§ 4.5).
4. Validez l'import sans l'appliquer (`dryRun=true`), en transmettant la phrase de passe dans l'en-tête `X-Config-Passphrase` (§ 8.5.3), puis appliquez-le. L'identifiant de la sonde est restauré ; cette restauration ne suffit pas, à elle seule, à assurer la continuité des séries de métriques dans vos plateformes : ses conditions sont précisées au § 8.6.2 (encadré qui suit la procédure). Vérifiez sur vos plateformes que les séries de la sonde se poursuivent.
5. Créez de nouveaux jetons d'API pour Prometheus, Nagios, Centreon et vos automatisations : les jetons ne font pas partie de l'export. Mettez à jour ces outils.
6. Vérifiez les destinations d'export avec leur fonction de test, puis lancez une exécution d'essai des contrôles principaux.
7. Supprimez l'archive d'export des emplacements temporaires utilisés pour le transfert.
8. Si vous restituez l'ancienne carte, réinitialisez-la d'abord aux paramètres d'usine (§ 8.10) afin qu'elle ne contienne plus aucune donnée de votre organisation, puis suivez les instructions de restitution.

Résultat attendu : la sonde fonctionne avec la nouvelle édition, avec la même configuration, le même identifiant et les mêmes secrets. Les fonctions propres à la nouvelle édition sont disponibles.

> ! **Avertissement** — L'archive exportée avec une phrase de passe contient vos secrets, chiffrés. Ne la transmettez jamais par courriel ou par messagerie, et ne conservez jamais la phrase de passe à côté de l'archive.

8.7 Surveillance de la santé de la sonde

8.7.1 Indicateurs à suivre

La sonde publie des métriques sur sa propre santé (chapitre 2 du guide d'intégration et d'observabilité). Les alertes suivantes sont recommandées dans votre plateforme de supervision.

Alerte	Condition indicative	Signification
Sonde muette	Absence de `sva.agent.up` pendant 5 minutes	Sonde éteinte, injoignable ou export interrompu (équivalent de l'état `STALE` de la sonde)
Sous-tension	`sva.hw.throttled` égal à 1 avec l'attribut `sva.hw.reason` = `undervoltage`	Alimentation insuffisante : risque de corruption
Surchauffe	`sva.hw.throttled` égal à 1 avec `sva.hw.reason` = `thermal`, ou `sva.hw.temperature` durablement élevée	Refroidissement à vérifier
Stockage	Occupation d'un système de fichiers de la sonde (`system.filesystem.usage`, état `used`) au-delà de 80 % de sa capacité pendant 30 minutes ; le détail par zone est donné par `sva.storage.usage`	Rétention à réduire ou support à remplacer (§ 8.6.4)
Saturation	`sva.agent.scheduler.lag` en hausse durable	Trop de contrôles pour la sonde
Échecs de Chromium	Hausse de `sva.browser.launches` en échec	Problème du moteur de scénarios
Export	`sva.export.failures` ou `sva.export.dropped` en hausse	Destination d'export en erreur

Alerte	Condition indicative	Signification
Récupération de base	Incrément de `sva.storage.recoveries`	Coupure ayant corrompu la base : examiner l'alimentation
Mise à jour en attente sans fenêtre	État de santé `updates` en `WARNING`, ou `sva.update.pending` égal à 1 depuis plus de 24 heures sans maintenance planifiée (`sva.maintenance.next_start` égal à `0` ; une série absente traduit une perte de collecte, pas l'absence de planification)	Aucune fenêtre de maintenance : la mise à jour ne sera pas activée sans intervention (§ 8.4.2, § 8.4.8)
Correctif critique en attente	État de santé `updates` en `CRITICAL`, ou `sva.update.pending` égal à 1 avec l'attribut `sva.update.critical` = `true`	Vulnérabilité activement exploitée : décider de l'activation (§ 8.4.11)
Mise à jour en échec	`sva.update.last_result` porte `rolled_back` ou `failed` (`lastResult` de `GET /api/v1/updates`)	Retour arrière automatique ou échec avant redémarrage : la version précédente reste active ; consulter le journal d'audit et le § 9.7
Maintenance anormalement longue	`sva.agent.maintenance` égal à 1 au-delà de la durée de la fenêtre, ou sonde muette après la fin de la fenêtre de maintenance (`sva.maintenance.next_end` dépassé) ou, pour une activation sans fin prévue (`sva.maintenance.next_end` à `0`), après la durée maximale que vous avez retenue	Activation bloquée ou sonde non revenue après son redémarrage : consulter le journal d'audit et le § 9.7

Les noms des métriques utilisent le préfixe stable `sva.`. Leur traduction au format Prometheus et des exemples de requêtes figurent au chapitre 2 du guide d'intégration et d'observabilité.

8.7.2 Vérification manuelle

En complément des alertes, consultez périodiquement la page de santé de l'interface ou `GET /api/v1/system` : version, ressources, état des modules et des destinations d'export. Trois états de santé concernent particulièrement la maintenance : `storage`, qui passe en `CRITICAL` si le SSD activé est absent ou défaillant (§ 8.3.4) ; `support`, qui passe en `WARNING` à la fin de la période de support (§ 8.4.6) ; `updates`, qui passe en `WARNING` lorsqu'une mise à jour attend sans activation planifiée ou après un report (§ 8.4.2) et en `CRITICAL` tant qu'un correctif critique n'est pas actif (§ 8.4.11).

8.8 Rotation des secrets et des jetons

Élément	Rotation recommandée	Procédure
Mots de passe des comptes de test des applications	Selon la politique de l'entreprise, et au moins une fois par an	Changer le mot de passe dans l'application, puis remplacer immédiatement le secret dans la sonde (`PUT /api/v1/secrets/{name}`). Le secret ne peut jamais être relu, seulement remplacé
Comptes des bases de données (lecture seule)	Idem	Idem
Clés d'ingestion des plateformes (Datadog, Dynatrace, Grafana)	Selon la politique de la plateforme	Créer la nouvelle clé, mettre à jour le secret, tester la destination, puis révoquer l'ancienne clé
Jetons d'API de la sonde	Au moins une fois par an ; immédiatement au départ d'un collaborateur ou en cas de doute	Créer un nouveau jeton, mettre à jour l'outil qui l'utilise, révoquer l'ancien

Élément	Rotation recommandée	Procédure
Mots de passe des comptes de l'interface	Selon la politique de l'entreprise	Changement par l'utilisateur ou par un administrateur
Certificat TLS de la sonde	Avant expiration (certificat émis par l'autorité de l'entreprise)	Téléverser le nouveau certificat (chapitre 5)

✓ **Conseil** — Pour éviter qu'une rotation de mot de passe ne provoque une alerte, coordonnez-la avec la mise à jour du secret : changez le mot de passe dans l'application, puis mettez à jour le secret dans les minutes qui suivent. La date de rotation de chaque secret est visible dans l'interface. Consultez-la lors de la revue trimestrielle (§ 8.11).

! **Avertissement** — Lorsqu'un secret est supprimé ou remplacé, révoquez également l'ancienne valeur dans le système qui l'a émise. Supprimer un secret de la sonde ne le rend pas invalide pour l'application concernée.

8.9 Maintenance des scénarios et des contrôles

Les applications supervisées évoluent : nouvelles versions, changement de charte graphique, nouveaux parcours, nouvelles règles de sécurité. Un scénario non entretenu finit par échouer alors que l'application fonctionne. Il produit alors de fausses alertes et décrédibilise la supervision.

8.9.1 Intégrer la supervision au cycle de livraison

1. **Avant une mise en production**, l'équipe applicative informe le responsable de la supervision des changements visibles : libellés, structure des pages, parcours, authentification.
2. **Sur l'environnement de recette**, une sonde (ou un contrôle dédié) exécute les scénarios sur la nouvelle version. Les écarts sont corrigés avant la mise en production.
3. **Pendant la mise en production**, les contrôles concernés sont suspendus ou placés en période de maintenance, si la plateforme le permet.
4. **Après la mise en production**, une exécution d'essai de chaque scénario concerné confirme son fonctionnement.

✓ **Conseil** — Demandez aux équipes de développement d'ajouter des attributs stables dédiés aux tests (`data-testid`) sur les éléments utilisés par les scénarios. C'est la mesure qui réduit le plus la maintenance des scénarios (chapitre 6 du guide de développement des scénarios).

8.9.2 Revue périodique des contrôles

Une fois par trimestre, passez en revue l'ensemble des contrôles :

- contrôles désactivés depuis longtemps : à supprimer ou à réactiver ;
- contrôles en bagotage fréquent : seuils ou nouvelles tentatives à ajuster (§ 8.2 du guide d'utilisation et de supervision) ;
- scénarios dont la durée augmente régulièrement : dérive de performance à signaler ;
- applications retirées du service : contrôles à supprimer ;
- nouvelles applications : contrôles à créer ;
- comptes de test : toujours valides, droits minimaux, pas de données réelles.

8.10 Réinitialisation aux paramètres d'usine

La réinitialisation efface la configuration, les résultats, les comptes, les jetons et les secrets, puis ramène la sonde à l'état « non initialisée » : le code d'installation imprimé sur l'encart ou l'étiquette du produit redevient valide pour une nouvelle mise en service. Le certificat d'édition est conservé.

Méthode	Description
Par l'interface ou l'API	Action réservée au rôle `admin` : `POST /api/v1/system/factory-reset` avec le corps `{"confirm": "<nom d'hôte de la sonde>"}`. La confirmation par le nom d'hôte évite une réinitialisation de la mauvaise sonde.
Sans accès administrateur	Procédure physique par fichier déposé sur la partition `SVA-BOOT` de la microSD, confirmée en deux temps par un code aléatoire (§ 8.10.1). Si seul le mot de passe administrateur est perdu, préférez la récupération sans perte de configuration (§ 8.10.2)
Réécriture de la carte	Remplacement par une carte neuve préconfigurée (§ 8.6)

> **Avertissement** — La réinitialisation est irréversible. Exportez la configuration au préalable si elle doit être réutilisée. Pensez à révoquer, côté applications et plateformes, les identifiants qui étaient stockés sur la sonde si celle-ci change de main.

> **Information** — La réinitialisation usine lève le verrouillage définitif de SSH (`ssh.locked` , chapitre 5) : c'est le seul moyen de le lever. Après la réinitialisation, SSH est de nouveau désactivé par défaut, comme à la sortie de l'emballage.

8.10.1 Réinitialiser sans accès administrateur (procédure physique)

Objectif : ramener aux paramètres d'usine une sonde dont aucun compte administrateur n'est plus utilisable, par exemple une sonde récupérée sans ses identifiants.

La procédure exige un **accès physique** à la carte microSD et une **confirmation en deux temps** : le premier démarrage ne fait que produire un code aléatoire, et rien n'est effacé tant que ce code n'a pas été recopié. Le numéro de série de la sonde, qui figure sur l'étiquette et l'encart, ne suffit jamais à autoriser une réinitialisation.

Prérequis : accès physique à la sonde ; un poste de travail capable de lire la partition de démarrage de la microSD, au format FAT32 et étiquetée `SVA-BOOT` (§ 4.3.5) ; facultativement, un écran raccordé en micro-HDMI.

> **Avertissement** — Avant d'engager cette procédure, vérifiez si la récupération du compte administrateur (§ 8.10.2) est possible : elle conserve toute la configuration. La réinitialisation, elle, efface définitivement la configuration, les résultats, les comptes, les jetons et les secrets.

Étapes — premier temps : demande

1. Arrêtez la sonde par un appui bref sur le bouton d'alimentation (§ 8.2.2), attendez l'extinction, puis débranchez l'alimentation.
2. Retirez la carte microSD (chapitre 3) et ouvrez sur votre poste sa partition de démarrage, étiquetée `SVA-BOOT`. Avec le mécanisme de mise à jour A/B, d'autres partitions de la carte peuvent apparaître sur le poste : ne les modifiez pas. Ne modifiez aucun autre fichier de la partition `SVA-BOOT`.
3. Créez à la racine de cette partition un fichier texte nommé `factory-reset.txt` (le fichier peut être vide : son contenu est ignoré à ce stade). Vérifiez que votre système n'a pas ajouté d'extension masquée (par exemple `factory-reset.txt.txt`).

4. Éjectez proprement la carte, réinsérez-la dans la sonde et mettez celle-ci sous tension.
5. Au démarrage, la sonde **n'efface rien**. Elle écrit sur la partition `SVA-BOOT` un fichier `factory-reset-challenge.txt` contenant un **code aléatoire de 8 caractères**, valable **24 heures**, et un avertissement sur les conséquences de l'opération. Elle affiche aussi ce code sur la console HDMI et consigne la demande dans le journal.

Étapes — second temps : confirmation

6. Relevez le code sur la console HDMI ou, après un nouvel arrêt propre et le retrait de la carte, dans le fichier `factory-reset-challenge.txt`. Lisez l'avertissement qu'il contient.
7. Remplacez le contenu de `factory-reset.txt` par la seule ligne suivante, où `<code>` est le code relevé :

```
EFFACER <code>
```

8. Réinsérez la carte et redémarrez la sonde avant l'expiration du délai de 24 heures.

Résultat attendu : si le code est exact et encore valide, la sonde se réinitialise et revient à l'état « non initialisée ». Le certificat d'édition est conservé et le code d'installation imprimé sur l'encart ou l'étiquette redevient valide. Le verrouillage de SSH éventuel est levé.

Vérification : la sonde attend une nouvelle mise en service ; la console HDMI et le fichier `setup-code.txt` de la partition `SVA-BOOT` affichent de nouveau le code d'installation (§ 4.4.3).

Erreurs possibles

Situation	Conséquence	Action
Code inexact	Aucune réinitialisation	Relire le code dans `factory-reset-challenge.txt` ou sur la console HDMI ; corriger la ligne `EFFACER <code>`
Code expiré (plus de 24 heures)	Aucune réinitialisation	Recommencer la procédure au premier temps pour obtenir un nouveau code
Fichier mal nommé ou placé dans un sous-dossier	La demande n'est pas prise en compte	Placer `factory-reset.txt` à la racine de la partition `SVA-BOOT`, sans extension supplémentaire ; ne pas l'écrire sur une autre partition de la carte

Précautions : la carte microSD contient vos secrets chiffrés et leur clé (§ 8.13). Ne la confiez pas à un tiers pour réaliser cette procédure. Après la réinitialisation, procédez à une nouvelle mise en service (chapitre 4) ou, si la sonde quitte votre organisation, poursuivez avec le § 8.13.

8.10.2 Récupérer l'accès administrateur sans perte de configuration

Objectif : définir un nouveau mot de passe pour un compte `admin` existant lorsque plus aucun administrateur ne peut se connecter (départ d'un collaborateur, mot de passe perdu), **sans perdre la configuration** de la sonde.

Prérequis

- Accès physique à la sonde et un poste capable de lire la partition de démarrage de la microSD, au format FAT32 et étiquetée `SVA-BOOT`.
- Le **code d'installation** imprimé sur l'encart ou l'étiquette du produit.
- Le **code de récupération** : code de 24 caractères, à usage unique, généré à la fin de la mise en service et affiché une seule fois, dans l'assistant ou, pour une sonde provisionnée par fichier, à la première connexion (§ 4.4.6). Il doit avoir été conservé dans le coffre-fort de mots de passe de votre organisation. La sonde n'en conserve qu'une empreinte (Argon2id) : ni la sonde ni le support de l'éditeur ne peuvent le retrouver.
- L'adresse de la sonde sur le réseau (§ 4.4.2).

> **Attention** — Sans code de récupération, cette procédure est impossible : seule la réinitialisation usine reste disponible (§ 8.10.1), avec perte de la configuration. Conservez le code de récupération et l'encart dès la mise en service.

Étapes

1. Arrêtez la sonde par un appui bref sur le bouton d'alimentation (§ 8.2.2), puis débranchez l'alimentation.
2. Retirez la carte microSD et créez, à la racine de sa partition de démarrage étiquetée `SVA-BOOT`, un fichier texte nommé `recovery.txt` (le fichier peut être vide : son contenu est ignoré). D'autres partitions de la carte peuvent apparaître sur le poste : ne les modifiez pas.
3. Réinsérez la carte et mettez la sonde sous tension.
4. Au démarrage, la sonde ouvre une **page de récupération** pendant **30 minutes** (`https://<adresse de la sonde>/recovery`). Connectez-vous-y depuis un poste du réseau où la sonde est installée, en vérifiant le certificat de la sonde comme au chapitre 4 (§ 4.4.4).
5. Saisissez le **code d'installation** et le **code de récupération**. Vous disposez de **3 essais au plus** par ouverture de la page.
6. Choisissez le compte `admin` existant à récupérer et définissez son nouveau mot de passe.
7. **Relevez le nouveau code de récupération** affiché par la page : l'ancien vient d'être consommé. Rangez-le immédiatement dans votre coffre-fort de mots de passe. Il ne sera plus affiché.
8. Connectez-vous à l'interface avec le compte récupéré.

Résultat attendu

- Le compte `admin` dispose de son nouveau mot de passe ; toutes ses sessions et tous ses jetons d'API ont été révoqués.
- La configuration, les contrôles, les secrets, les résultats et les autres comptes sont **conservés**.
- Un nouveau code de récupération a été émis ; le fichier `recovery.txt` a été supprimé par la sonde.

Vérification : le journal d'audit contient l'événement de récupération ; `recovery.txt` n'est plus présent sur la partition `SVA-BOOT` ; les contrôles s'exécutent normalement.

Erreurs possibles

Situation	Cause probable	Action
Page de récupération inaccessible	Délai de 30 minutes écoulé ; fichier mal nommé ou mal placé	Redéposer `recovery.txt` à la racine de la partition `SVA-BOOT` (et non sur une autre partition de la carte) et redémarrer la sonde
Codes refusés, page fermée après 3 essais	Faute de frappe ; code d'une autre sonde ; code de récupération déjà consommé	Vérifier l'encart de **cette** sonde et le dernier code de récupération conservé ; recommencer depuis l'étape 1
Code de récupération introuvable	Code non conservé lors de la mise en service	Réinitialisation usine (§ 8.10.1)

Précautions

- Recréez les jetons d'API utilisés par vos outils (Prometheus, Nagios, Centreon, automatisations) s'ils appartenaient au compte récupéré, puis mettez ces outils à jour.
- Si la perte d'accès fait suite au départ d'un collaborateur, revoyez aussi les autres comptes et jetons (chapitre 6).
- La récupération reste possible même lorsque SSH a été verrouillé définitivement (chapitre 5).

8.11 Plan de maintenance préventive

Fréquence	Opération	Référence
Quotidienne (automatisée)	Vérifier par des alertes que la sonde émet (`sva.agent.up`) et que les exports fonctionnent	§ 8.7
	Traiter les contrôles en `CRITICAL` , `UNKNOWN` ou `STALE`	Chapitre 7 du guide d'utilisation et de supervision et chapitre 9
Hebdomadaire	Consulter la page de santé : ressources, température, sous-tension, stockage	§ 8.7.2
	Vérifier les mises à jour disponibles ou en attente (canal en mode manuel, absence de fenêtre, report en cours), les activations annoncées, et lire les notes de version	§ 8.4
Mensuelle	Exporter la configuration hors de la sonde	§ 8.5.2
	Examiner les tendances de durée des scénarios principaux	Chapitre 7 du guide d'utilisation et de supervision
	Consulter le journal d'audit à la recherche d'opérations inattendues	Chapitre 6
Trimestrielle	Revue des contrôles et des scénarios	§ 8.9.2
	Revue des comptes de l'interface, des rôles et des jetons d'API (révoquer l'inutile)	Chapitre 6
	Vérifier l'ancienneté des secrets	§ 8.8
	Vérifier la date d'expiration du certificat de la sonde	Chapitre 5
	Revoir les fenêtres de maintenance, leur alignement avec les périodes de maintenance des plateformes et leur décalage entre sondes d'un même site	§ 8.4.8, § 8.4.10, § 8.4.12
Annuelle	Rotation des secrets et des jetons	§ 8.8
	Test de restauration de la configuration sur une carte de rechange	§ 8.5.3, § 8.6
	Inspection physique et dépoussiérage	§ 8.12
	Évaluation du remplacement préventif de la carte microSD selon l'usage	§ 8.3.3
	Vérifier les dates de fin de la période de support (`supportEndsAt`) et du justificatif de maintenance (`maintenanceEndsAt`), et la conservation du code de récupération	§ 8.4.6, § 8.4.7, § 8.10.2

8.12 Entretien physique

> **Avertissement** — Manipulez la carte Raspberry Pi 5 par ses bords, après vous être déchargé de l'électricité statique (contact avec une partie métallique reliée à la terre). Ne touchez pas les composants ni les contacts de la carte microSD.

1. Arrêtez la sonde proprement avant toute intervention physique (§ 8.2.2).
2. Vérifiez que les aérations du boîtier ne sont pas obstruées et que le ventilateur tourne librement.
3. Retirez la poussière à l'air sec (bombe d'air pour matériel électronique), en immobilisant le ventilateur pour ne pas le faire tourner à grande vitesse. N'utilisez ni liquide ni aspirateur.

4. Vérifiez l'état du câble d'alimentation, du connecteur USB-C et du câble Ethernet : absence de pliure, de traction ou d'échauffement.
5. Vérifiez que la sonde reste fixée et protégée des chocs, de l'humidité et des sources de chaleur.

8.13 Fin de vie et effacement sécurisé

La carte microSD et, le cas échéant, le SSD d'une sonde contiennent des informations sensibles : secrets chiffrés et leur clé de chiffrement, configuration du réseau interne, noms et adresses des applications supervisées, captures d'écran, historique. Une sonde retirée du service doit être traitée comme un support de données confidentielles.

Étapes

1. Exportez la configuration si elle doit être réutilisée (§ 8.5.2).
2. Révoquez, côté applications et plateformes, tous les identifiants stockés sur la sonde : comptes de test, comptes de base de données, clés d'ingestion. Révoquez aussi les jetons d'API de la sonde utilisés par vos outils.
3. Effectuez une réinitialisation usine (§ 8.10). Elle ne garantit pas, à elle seule, l'effacement physique des données sur une mémoire flash.
4. Effacez ensuite le support selon la politique de sécurité de votre entreprise. Sur une mémoire flash (microSD, SSD), un simple formatage ne suffit pas. En cas de doute, la **destruction physique** de la carte est la méthode la plus sûre. Pour un SSD NVMe, utilisez la fonction d'effacement sécurisé du constructeur.
5. Retirez la sonde de vos inventaires, des cibles Prometheus, des services Nagios ou Centreon et des tableaux de bord.
6. Recyclez le matériel électronique via une filière agréée (déchets d'équipements électriques et électroniques).

> **Information** — Pour un support retourné à l'éditeur (remplacement, reprise, fin de prêt), joignez une **preuve d'effacement** conforme à la politique de votre entreprise, ou, si le support a été détruit, une **attestation de destruction**. Une carte défectueuse impossible à effacer n'a pas à être retournée : vous pouvez la conserver ou la détruire physiquement, et son remplacement reste acquis (§ 8.6.4).

> **Avertissement** — Ne revendez pas et ne réaffectez pas une carte microSD de sonde sans effacement sécurisé préalable. Les secrets y sont chiffrés, mais la clé de chiffrement se trouve sur le même support (chapitres 5 et 6).

Chapitre 9 — Diagnostic et assistance

9.1 Méthode générale de diagnostic

9.1.1 Principe

Un incident de supervision peut avoir trois origines distinctes, qu'il faut séparer avant toute action :

1. **La ressource supervisée** : l'application, l'API, la base ou le service surveillé est réellement défaillant. C'est le cas nominal : la sonde remplit son rôle en le signalant.
2. **Le chemin entre la sonde et la ressource** : réseau, résolution DNS, pare-feu, proxy, certificat. La ressource fonctionne peut-être pour ses utilisateurs, mais pas depuis l'emplacement de la sonde.
3. **La sonde elle-même** : alimentation, stockage, mémoire, configuration du contrôle, script de scénario devenu obsolète.

L'état `UNKNOWN` est réservé aux situations où la sonde n'a pas pu évaluer le contrôle (troisième cas). Un état `CRITICAL` signale en principe un problème de la ressource ou du chemin réseau (premier et deuxième cas). Cette distinction, décrite au chapitre 3 du guide d'utilisation et de supervision, est le premier indice à exploiter.

9.1.2 Démarche recommandée

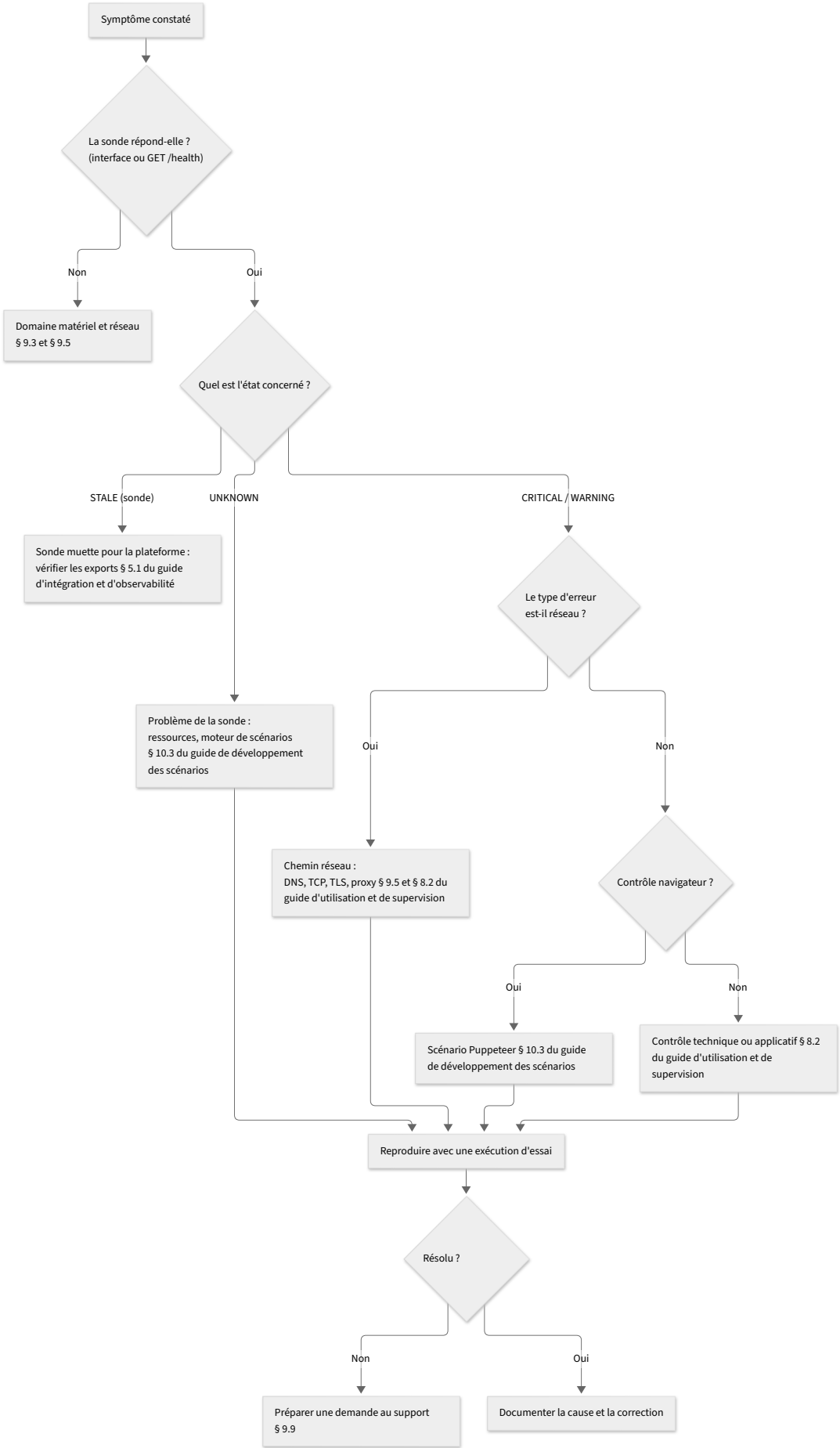


Schéma 9-1 — Démarche de diagnostic

En pratique :

1. **Qualifier le symptôme** : quel contrôle, depuis quand, sur quelle sonde, avec quel état et quel type d'erreur (`error.type`).
2. **Consulter le détail de la dernière exécution en échec** : étape concernée, message, capture d'écran et journal de console pour un scénario navigateur (voir chapitre 7 du guide d'utilisation et de supervision).
3. **Comparer avec l'historique** : un échec isolé, un bagotage ou une rupture nette n'appellent pas la même analyse.
4. **Vérifier si plusieurs contrôles sont touchés en même temps**. Si tous les contrôles d'une même sonde échouent simultanément, la cause se trouve probablement côté sonde ou réseau local, et non dans les applications supervisées.
5. **Reproduire** avec une exécution d'essai (`POST /api/v1/checks/{id}/runs?dryRun=true`). Elle n'enregistre pas d'état et n'exporte rien, ce qui évite de fausser l'historique pendant le diagnostic.
6. **Corriger, puis vérifier** par une nouvelle exécution d'essai avant de réactiver le contrôle ou d'attendre la prochaine échéance.

> ✓ **Conseil** — Notez systématiquement l'heure UTC de l'exécution en échec et son identifiant (`runId`). Ces deux informations permettent de retrouver l'événement dans les journaux, les traces OpenTelemetry et les plateformes d'observabilité.

9.2 Outils de diagnostic disponibles

9.2.1 Interface d'administration

L'interface d'administration (chapitre 6) est l'outil de premier niveau. Elle permet de :

- consulter l'état de chaque contrôle et l'historique des exécutions ;
- ouvrir le détail d'une exécution : étapes, durée de chaque étape, type d'erreur, message, artefacts (capture d'écran, journal de console) ;
- déclencher une exécution manuelle ou d'essai ;
- consulter l'état de santé de la sonde : ressources, modules, destinations d'export ;
- consulter le journal d'audit (rôle `admin`).

9.2.2 API REST

L'API offre les mêmes informations sous une forme exploitable par script. Les appels les plus utiles en diagnostic sont les suivants.

Appel	Rôle minimal	Utilité en diagnostic
`GET /health`	aucun	Vérifie que le moteur principal répond. Ne donne aucune information sensible
`GET /api/v1/system`	`viewer`	Version, édition, ressources, état des modules et des destinations d'export
`GET /api/v1/checks/{id}/status`	`metrics`	Dernier état consolidé d'un contrôle
`GET /api/v1/runs?checkId=…&status=CRITICAL`	`viewer`	Historique des échecs d'un contrôle
`GET /api/v1/runs/{runId}`	`viewer`	Détail complet d'une exécution

Appel	Rôle minimal	Utilité en diagnostic
`GET /api/v1/runs/{runId}/artifacts/{name}`	`viewer`	Téléchargement d'une capture ou d'un journal de console
`POST /api/v1/checks/{id}/runs?dryRun=true`	`operator`	Exécution d'essai
`POST /api/v1/exporters/{id}/test`	`admin`	Test d'une destination d'export avec diagnostic détaillé
`GET /api/v1/audit-events`	`admin`	Modifications récentes de configuration

Exemple : vérifier que la sonde répond, puis afficher son état de santé. Dans cet exemple fictif, le jeton d'API n'apparaît pas dans la ligne de commande : il est lu dans le fichier d'en-tête protégé `$HOME/.sva/entete-auth`, créé une fois selon le chapitre 6 (§ 6.3.3). Le certificat de la sonde, récupéré puis vérifié selon le chapitre 4 (§ 4.4.4), est enregistré dans `sonde-ca.pem`.

```bash
# Vivacité du moteur principal (aucune authentification requise)
curl --cacert sonde-ca.pem https://sonde-paris-01.example.internal/health

# État de santé détaillé (rôle viewer)
curl --cacert sonde-ca.pem \
     -H @"$HOME/.sva/entete-auth" \
     https://sonde-paris-01.example.internal/api/v1/system
```

Exemple : lister les dernières exécutions en échec d'un contrôle.

```bash
curl --cacert sonde-ca.pem \
     -H @"$HOME/.sva/entete-auth" \
     "https://sonde-paris-01.example.internal/api/v1/runs?checkId=boutique-
    connexion&status=CRITICAL&limit=20"
```

> **Attention** — N'utilisez pas l'option `curl -k` (`--insecure`, vérification du certificat désactivée) pour vos appels courants : elle supprime la protection contre l'interception, y compris celle de votre jeton d'API. Utilisez l'option `--cacert`, avec le certificat de la sonde ou celui de l'autorité de certification de votre entreprise (chapitres 4 et 5).

9.2.3 Journaux

La sonde produit trois catégories de traces :

Source	Contenu	Accès
Journal de chaque exécution	Étapes, messages `log.info` des scénarios, sortie des plugins Nagios, erreurs (secrets masqués)	Interface, `GET /api/v1/runs/{runId}`
Journal d'audit	Opérations d'administration : connexions, modifications, téléversements, mises à jour	Interface (`admin`), `GET /api/v1/audit-events`
Journaux système	Messages des services de la sonde et du système d'exploitation	SSH (si activé), export OTLP des logs vers votre plateforme

> **Information** — Par défaut, les journaux système sont conservés **en mémoire** pour limiter l'usure de la microSD (voir chapitre 8). Ils sont donc perdus à chaque redémarrage. Pour analyser un incident ayant entraîné un redémarrage, exportez les logs vers une plateforme d'observabilité (chapitre 2 du guide d'intégration et d'observabilité) ou activez temporairement la conservation persistante avec le paramètre `logging.persistentUntil`, qui fixe l'échéance de la persistance. La sonde revient automatiquement aux journaux en mémoire à cette échéance, et au plus tard 72 heures après l'activation.

9.2.4 Accès SSH (diagnostic avancé)

L'accès SSH est **désactivé par défaut**. Seul un administrateur (rôle `admin`) de la sonde peut l'activer, depuis l'interface d'administration ou dans la section `ssh` des paramètres, et toujours pour une durée limitée : l'échéance (`enabledUntil`) est obligatoire, de 4 heures par défaut et de 72 heures au maximum. À l'échéance, SSH se désactive automatiquement et les sessions ouvertes sont fermées. L'activation, les connexions et la désactivation sont enregistrées dans le journal d'audit (voir § 5.9.4). Il est destiné aux administrateurs système expérimentés et au support de l'éditeur. Si SSH a été verrouillé (`ssh.locked`), il ne peut plus être activé avant une réinitialisation usine.

> **Avertissement** — Une session SSH donne un accès étendu au système de la sonde. Ne modifiez pas les fichiers du produit et n'installez pas de logiciels supplémentaires : ces opérations ne sont pas prises en charge et peuvent être annulées par une mise à jour, le système étant installé en lecture seule. Désactivez SSH à la fin de l'intervention, sans attendre l'échéance automatique.

Les commandes ci-dessous sont des commandes Linux standard, disponibles sur Raspberry Pi OS. Elles ne modifient rien.

Commande	Objet
`systemctl status sva-agent sva-runner`	État des services du moteur principal et du moteur de scénarios
`journalctl -u sva-agent --since "1 hour ago"`	Journal du moteur principal sur la dernière heure
`journalctl -u sva-runner -n 200`	200 dernières lignes du journal du moteur de scénarios
`journalctl -k -b`	Messages du noyau depuis le dernier démarrage
`dmesg --level=err,warn`	Erreurs et avertissements du noyau (carte microSD, mémoire, USB)
`ip addr show eth0`	Adresse IP de l'interface Ethernet
`ip route`	Passerelle par défaut
`getent hosts www.example.com`	Résolution d'un nom selon la configuration du système
`dig www.example.com`	Interrogation DNS détaillée (outil présent dans l'image de la sonde)
`ping -c 4 192.0.2.1`	Joignabilité ICMP
`curl -v https://www.example.com/`	Requête HTTPS détaillée (DNS, TLS, réponse)
`timedatectl`	Heure système et état de la synchronisation NTP
`df -h`	Espace disque par partition
`free -h`	Mémoire disponible
`uptime`	Durée de fonctionnement et charge
`vcgencmd get_throttled`	Indicateurs de sous-tension et de bridage thermique (Raspberry Pi)
`vcgencmd measure_temp`	Température du processeur (Raspberry Pi)

> **Information** — Les services de la sonde s'appellent `sva-agent` (moteur principal) et `sva-runner` (moteur de scénarios et environnement isolé). Ces noms techniques sont stables. Le chemin du répertoire de données de la sonde est indiqué dans les notes de version.

Interpréter `vcgencmd get_throttled`

La commande renvoie une valeur hexadécimale, par exemple `throttled=0x50005`. Chaque bit a une signification documentée par Raspberry Pi :

Bit	Valeur	Signification
0	`0x1`	Sous-tension **actuellement** détectée
1	`0x2`	Fréquence du processeur actuellement plafonnée
2	`0x4`	Processeur actuellement bridé
3	`0x8`	Limite thermique logicielle actuellement atteinte
16	`0x10000`	Sous-tension survenue depuis le démarrage
17	`0x20000`	Plafonnement de fréquence survenu depuis le démarrage
18	`0x40000`	Bridage survenu depuis le démarrage
19	`0x80000`	Limite thermique logicielle atteinte depuis le démarrage

La valeur `0x0` indique qu'aucun problème n'a été détecté depuis le démarrage. Toute autre valeur appelle une vérification de l'alimentation ou du refroidissement (§ 9.3).

9.2.5 Métriques de supervision interne

La sonde publie des métriques sur sa propre santé (voir chapitre 2 du guide d'intégration et d'observabilité). Elles sont souvent l'indice le plus rapide :

Métrique	Ce qu'elle révèle
`sva.agent.up`	Absence de signal : sonde éteinte, injoignable ou export interrompu
`sva.agent.scheduler.lag`	Retard de la planification : sonde saturée
`sva.agent.queue.depth`	Contrôles en attente d'exécution
`sva.browser.launches` (issue en échec)	Problèmes de lancement de Chromium
`sva.export.failures`, `sva.export.dropped`	Destinations d'export en erreur, données perdues
`sva.storage.usage`	Remplissage de la base et des artefacts
`sva.dot1x.certificate.expiry`	Échéance du certificat client 802.1X ; un avertissement est émis 30 jours avant son expiration
`sva.hw.temperature`, `sva.hw.throttled`	Surchauffe, sous-tension

9.3 Démarrage et matériel

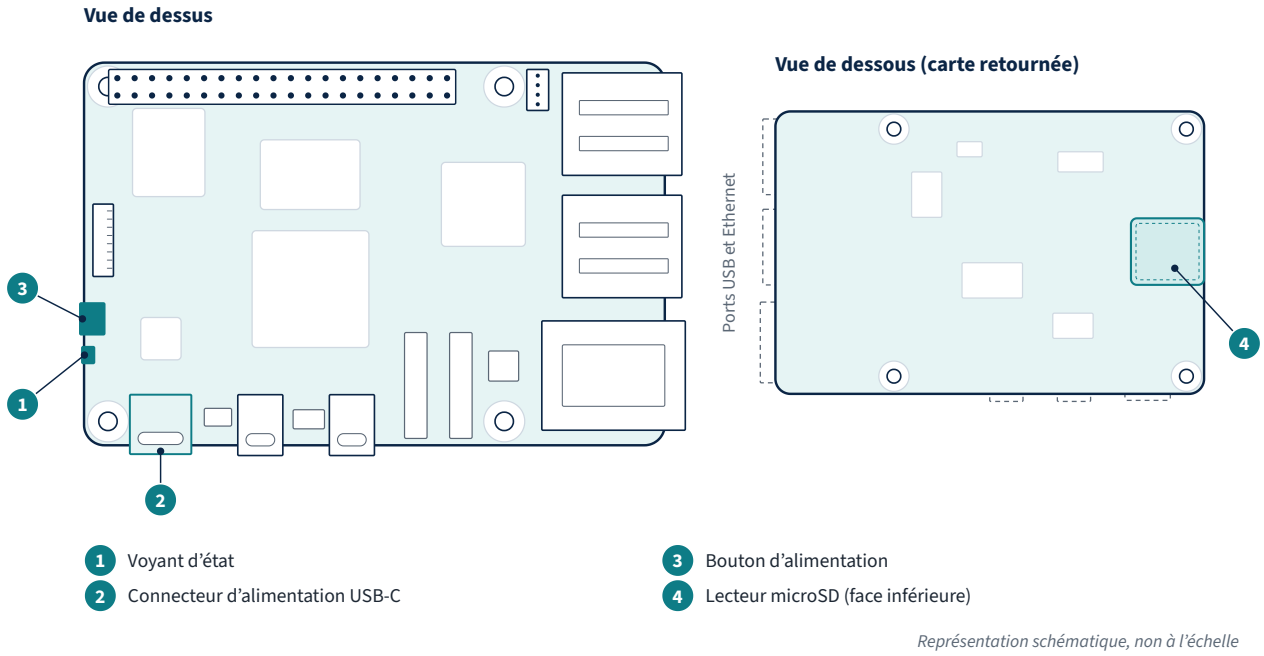


Figure 9-1 — Raspberry Pi 5 : emplacement du voyant d'état, du connecteur d'alimentation USB-C, du bouton d'alimentation et du lecteur microSD

Symptôme	Causes possibles	Vérifications	Actions correctives
Aucun voyant allumé à la mise sous tension	Alimentation absente ou défectueuse ; câble USB-C endommagé ; prise électrique sans courant. L'absence de voyant n'implique pas forcément l'absence d'alimentation : le comportement du voyant dépend aussi du micrologiciel, de la configuration et de l'état de démarrage	Tester la prise avec un autre appareil ; vérifier que le connecteur USB-C est bien enfoncé ; essayer une autre alimentation conforme ; brancher un écran HDMI pour vérifier si la console de démarrage s'affiche ; interroger `/health` si la sonde est déjà connue sur le réseau	Utiliser l'alimentation recommandée (27 W USB-C, 5,1 V / 5 A, chapitre 2) ; remplacer le câble
Le voyant s'allume mais la sonde n'apparaît jamais sur le réseau	Carte microSD absente, mal insérée ou illisible ; premier démarrage encore en cours ; câble Ethernet débranché	Vérifier l'insertion de la carte (chapitre 3) ; patienter le temps du premier démarrage, de l'ordre de quelques minutes à titre indicatif ; vérifier les voyants du port Ethernet et du commutateur	Réinsérer la carte hors tension ; brancher le câble avant la mise sous tension ; voir § 9.4 et § 9.5
Carte microSD non reconnue (la sonde ne démarre pas, comportement de voyant indiquant une absence de système)	Carte mal insérée, contacts sales, carte défaillante, image corrompue	Retirer la carte hors tension et l'inspecter ; la lire sur un poste de travail : la partition de démarrage, étiquetée `SVA-BOOT`, doit apparaître	Nettoyer délicatement les contacts ; réinsérer ; si la partition n'est pas lisible, remplacer la carte (§ 8.6)

Symptôme	Causes possibles	Vérifications	Actions correctives
Clignotements répétitifs du voyant d'état	Code de diagnostic du chargeur d'amorçage du Raspberry Pi (par exemple, image système introuvable)	Compter la séquence de clignotements longs et courts et la comparer aux codes publiés par Raspberry Pi	Selon le code (tableau ci-dessous) : réinsérer ou remplacer la carte, vérifier l'alimentation. L'image de la sonde n'ajoute aucune signalisation propre : seuls les codes standard du Raspberry Pi s'appliquent
La sonde redémarre spontanément	Sous-tension ; surchauffe ; watchdog déclenché par un blocage ; alimentation instable (multiprise surchargée)	`vcgencmd get_throttled` (bit 16) ; `journalctl -k -b -1` si les journaux sont persistants ; métrique `sva.hw.throttled`	Remplacer l'alimentation ; brancher la sonde sur un circuit protégé, idéalement un onduleur ; voir surchauffe ci-dessous
Sous-tension signalée (`sva.hw.throttled` avec `sva.hw.reason` = `undervoltage` , bit `0x1` ou `0x10000`)	Alimentation non conforme ; câble trop long ou de section insuffisante ; périphériques USB gourmands	`vcgencmd get_throttled`	Utiliser l'alimentation officielle 27 W et le câble d'origine ; débrancher les périphériques USB inutiles
Surchauffe ou bridage thermique (`sva.hw.temperature` élevée, bit `0x8` ou `0x80000`)	Refroidissement absent ou ventilateur bloqué ; boîtier confiné ; local trop chaud ; parcours navigateur très nombreux	`vcgencmd measure_temp` ; inspection visuelle du ventilateur ; température du local	Installer le refroidisseur actif officiel ou un boîtier ventilé (obligatoire pour l'édition Enterprise, recommandé pour les autres, chapitre 2) ; dégager les aérations ; déplacer la sonde ; réduire la concurrence navigateur (chapitre 6 du guide d'utilisation et de supervision)
Performances dégradées sans alerte matérielle	Mémoire saturée ; carte microSD lente ou en fin de vie ; trop de contrôles pour l'édition et la carte	`free -h` ; `sva.agent.scheduler.lag` ; `dmesg` (erreurs d'entrée/sortie `mmc`)	Réduire la fréquence des contrôles ; répartir sur une seconde sonde ; demander une carte de remplacement (§ 8.6.4) ou ajouter un SSD NVMe (§ 8.3.4), recommandé surtout pour l'édition Enterprise
Erreurs d'entrée/sortie dans `dmesg` (`mmc0: … error` , `I/O error` , `EXT4-fs error`)	Carte microSD en fin de vie ou corrompue après coupure ; carte autre que celle fournie par l'éditeur	`dmesg --level=err`	Sauvegarder immédiatement la configuration (§ 8.5) ; demander une carte de remplacement (§ 8.6.4)

Information — Les couleurs et clignotements du voyant d'état sont des **indices matériels** produits par le Raspberry Pi et son chargeur d'amorçage. Ils ne renseignent pas sur l'état de l'application : une activité du voyant liée aux accès au stockage ne prouve pas que le moteur de supervision fonctionne. Recoupez toujours ces indices avec la console HDMI (messages de démarrage, adresse et empreinte affichées) et avec la réponse de `GET /health` (§ 9.2.2). L'image de la sonde n'ajoute aucune signalisation propre au voyant.

Le tableau suivant reprend les codes de clignotement standard publiés par Raspberry Pi dans sa documentation officielle (section *LED warning flash codes*). Un code se lit comme un nombre de clignotements longs suivi d'un nombre de clignotements courts. En cas de doute, la documentation officielle de Raspberry Pi fait foi.

Longs	Courts	Signification
0	3	Échec générique du démarrage
0	4	Fichier `start*.elf` introuvable
0	7	Image du noyau introuvable
0	8	Défaillance de la mémoire vive (SDRAM)
0	9	Mémoire vive (SDRAM) insuffisante
0	10	Système à l'arrêt (état HALT)
1	2	Surintensité détectée sur la carte microSD
2	1	Partition qui n'est pas au format FAT
2	2	Échec de lecture de la partition
2	3	Partition étendue qui n'est pas au format FAT
2	4	Signature ou empreinte de fichier non conforme
3	1	Erreur de l'EEPROM SPI
3	2	EEPROM SPI protégée en écriture
3	3	Erreur I2C
3	4	Configuration de démarrage sécurisé invalide
4	3	Composant RP1 introuvable
4	4	Type de carte non pris en charge
4	5	Erreur fatale du micrologiciel
4	6	Défaillance d'alimentation de type A
4	7	Défaillance d'alimentation de type B

> **Avertissement** — Ne retirez jamais la carte microSD et ne débranchez jamais l'alimentation pendant le fonctionnement de la sonde. Arrêtez-la proprement d'abord (§ 8.2). Un retrait à chaud peut corrompre la carte.

9.4 Mise en service

Symptôme	Causes possibles	Vérifications	Actions correctives
Impossible de trouver l'adresse IP de la sonde	DHCP inactif sur le réseau ; port de commutateur désactivé ou dans un autre VLAN ; nom mDNS non résolu par le poste	Rechercher l'adresse MAC dans la table de baux DHCP ; tester `sva-XXXXXX.local` depuis un poste du même réseau (l'annonce mDNS est active par défaut, sauf si elle a été désactivée dans la section `network`) ; brancher un écran HDMI, qui affiche l'adresse IP et le nom mDNS	Réserver une adresse DHCP pour l'adresse MAC ; ou provisionner une adresse statique via `provision.yaml` (chapitre 4)
Le navigateur affiche un avertissement de sécurité à la connexion	Comportement normal : le certificat de la sonde est autosigné	Comparer l'empreinte SHA-256 affichée par le navigateur avec celle du fichier `setup-code.txt` ou de l'écran HDMI (§ 4.4.4)	Accepter le certificat après vérification de l'empreinte ; ensuite, installer un certificat émis par l'autorité de certification de l'entreprise (chapitre 5)
L'empreinte du certificat ne correspond pas	Connexion à un autre équipement (erreur d'adresse) ; interception par un proxy d'inspection TLS ; tentative d'usurpation	Vérifier l'adresse saisie ; contourner le proxy du poste pour l'adresse de la sonde	Ne pas poursuivre tant que l'empreinte ne correspond pas ; exclure l'adresse de la sonde de l'inspection TLS
Code d'installation refusé	Faute de frappe (confusion entre caractères proches) ; code d'une autre sonde (encart ou étiquette d'un autre produit) ; assistant déjà terminé ; blocage temporaire après 5 saisies erronées : 15 minutes, durée doublée à chaque nouvelle série d'échecs	Relire `setup-code.txt` sur la partition `SVA-BOOT` de la microSD ou l'écran HDMI, qui affiche le code tant que la sonde n'est pas initialisée ; en cas de blocage, attendre la fin du délai avant de saisir de nouveau le code ; vérifier si un compte administrateur existe déjà	Utiliser le code actuel ; si l'assistant a déjà été terminé, se connecter avec le compte administrateur créé ; en cas de perte, voir réinitialisation (§ 8.10)
L'assistant ne s'affiche pas, la page de connexion apparaît directement	La sonde a été provisionnée par `provision.yaml` ou l'assistant a déjà été terminé	Lire `provision-result.txt` sur la partition `SVA-BOOT` de la microSD	Se connecter avec le compte défini dans le fichier de provisionnement
Le provisionnement n'a pas été appliqué	Fichier mal nommé (extension masquée par l'explorateur, par exemple `provision.yaml.txt`) ; fichier placé dans un sous-dossier ou sur une autre partition que `SVA-BOOT` ; erreur de syntaxe YAML ; valeur invalide	Mettre la sonde hors tension, lire la carte sur un poste : présence et contenu de `provision-result.txt` , qui indique le motif du refus sans aucun secret	Corriger le fichier selon le compte rendu ; valider la syntaxe YAML (indentation par espaces, jamais de tabulation) ; recopier le fichier complet à la racine de la partition `SVA-BOOT` (ne modifier aucune autre partition de la carte), car un fichier refusé est supprimé ; redémarrer : le fichier est relu à chaque démarrage tant que la sonde n'est pas initialisée
Le fichier entier est refusé alors qu'une seule valeur est en cause	Comportement normal : la validation est atomique. Une seule erreur entraîne le refus de tout le fichier, et aucune section n'est appliquée	`provision-result.txt`	Corriger la valeur signalée et redéposer le fichier complet. Les sections absentes d'un fichier valide sont demandées par l'assistant de mise en service

Symptôme	Causes possibles	Vérifications	Actions correctives
Édition inattendue, ou sonde en mode restreint (aucun contrôle exécuté)	Carte d'une autre édition que celle commandée ; système copié sur une autre carte ; carte d'origine défectueuse ; carte de démonstration dont la période d'évaluation est terminée	Édition et cause affichées dans l'état de santé (`GET /api/v1/system`) ; numéro de série sur l'encart ou l'étiquette	Remettre la carte d'origine. Si elle est défectueuse, demander son remplacement (§ 8.6). Si l'édition ne correspond pas à la commande, contacter le service commercial (§ 10.5)
Mot de passe administrateur perdu	—	Existence d'un autre compte `admin` ; disponibilité du code de récupération (coffre-fort de l'organisation, § 4.4.6) et du code d'installation (encart ou étiquette)	Un autre administrateur peut réinitialiser le mot de passe. Sinon, procédure de récupération du compte administrateur (§ 8.10.2) : dépôt de `recovery.txt` sur la partition `SVA-BOOT`, puis page de récupération ouverte pendant 30 minutes au démarrage, qui exige le code d'installation et le code de récupération. La configuration est conservée. Sans code de récupération, seule la réinitialisation usine reste possible
Page de récupération refusant les codes, ou fermée	Faute de saisie ; code de récupération déjà consommé par une récupération précédente (un nouveau code a alors été affiché) ; 3 essais épuisés pour cette ouverture ; délai de 30 minutes dépassé	Code de récupération le plus récent dans le coffre-fort ; code d'installation de l'encart ou de l'étiquette ; journal d'audit après récupération	Déposer de nouveau `recovery.txt` et redémarrer pour rouvrir la page ; saisir le code de récupération le plus récent. Sans code valide : réinitialisation usine (§ 8.10)
Réinitialisation usine physique (`factory-reset.txt`) sans effet	Comportement normal au premier redémarrage : la réinitialisation se confirme en deux temps et rien n'est effacé à la première étape ; ligne de confirmation absente ou mal saisie ; code de confirmation erroné ou expiré (validité de 24 heures)	Présence de `factory-reset-challenge.txt` sur la partition `SVA-BOOT`, qui contient le code aléatoire de 8 caractères ; code affiché sur la console HDMI ; journal d'audit	Écrire dans `factory-reset.txt` la ligne `EFFACER <code>` avec le code en cours de validité, puis redémarrer. Si le code a expiré, recommencer la première étape. Le numéro de série ne suffit jamais à autoriser la réinitialisation (§ 8.10)

Avertissement — Après un provisionnement réussi, vérifiez que `provision.yaml` a bien disparu de la partition `SVA-BOOT`, ainsi que les fichiers 802.1X désignés par `pkcs12File` et `caFile` s'il y en avait. Si l'un de ces fichiers subsiste, supprimez-le : il peut contenir des informations sensibles (empreinte du mot de passe, paramètres réseau et de proxy, mot de passe et clé privée de l'identifiant 802.1X).

9.5 Réseau

Symptôme	Causes possibles	Vérifications	Actions correctives
La sonde n'obtient pas d'adresse IP	Câble défectueux ; port désactivé ; contrôle d'accès réseau 802.1X sur le port ; serveur DHCP saturé	Voyants du port Ethernet ; journal du commutateur ; table DHCP	Changer de câble ou de port ; configurer l'authentification 802.1X de la sonde (chapitre 5), ou autoriser son adresse MAC dans le contrôle d'accès réseau (MAB) ; configurer une adresse statique
Échec de l'authentification 802.1X : la sonde reste sans accès au réseau	Certificat client expiré ou révoqué ; AC du serveur RADIUS différente de celle configurée (`dot1x.caRef` , ou `caFile` du provisionnement) ; identité (`dot1x.identity`) inconnue du serveur RADIUS ; port du commutateur non configuré pour 802.1X, ou dans un autre mode (PEAP, étiquetage VLAN, non pris en charge)	État de l'authentification affiché sur la console HDMI ; état de santé `network` dans `GET /api/v1/system` si la sonde reste joignable ; métrique `sva.dot1x.certificate.expiry` ; journaux du serveur RADIUS et du commutateur	La sonde réessaie automatiquement. Renouveler le certificat client (nouvelle demande générée sur la sonde ou import PKCS#12, chapitre 5) ; corriger l'AC ou l'identité ; faire configurer le port en EAP-TLS. Pour reprendre la main, raccorder temporairement la sonde à un port non contrôlé ou autorisé par adresse MAC (MAB)
Avertissement d'expiration du certificat 802.1X	Certificat client à moins de 30 jours de son expiration	`sva.dot1x.certificate.expiry` ; état de santé	Renouveler le certificat avant l'échéance (chapitre 5) : à expiration, la sonde perdrait l'accès au réseau
La sonde n'est pas joignable en IPv6 ; aucune adresse IPv6	IPv6 désactivé (valeur par défaut) ; mode `slaac` sans annonce de routeur sur le segment ; adresse ou passerelle statique erronée ; ICMPv6 (découverte des voisins) filtré	Section `network` , objet `ipv6` (`enabled` , `mode` , `address` , `gateway`) ; `ip -6 addr show eth0` et `ip -6 route` en SSH	Activer l'IPv6 et corriger ses paramètres (chapitre 5) ; autoriser ICMPv6 (découverte des voisins) sur le segment. L'IPv4 reste toujours actif et suffit à l'administration
Un contrôle vers une cible IPv6 utilise l'IPv4, ou l'inverse	Paramètre `ipFamily` à `auto` (valeur par défaut) : l'IPv6 n'est utilisé que si l'IPv6 de la sonde est activé **et** si la cible a une adresse AAAA ; sinon l'IPv4 est utilisé	`ipFamily` du contrôle ; contrôle `dns` avec `dns.recordType` à `AAAA` sur le nom de la cible	Fixer `ipFamily` à `ipv6` ou `ipv4` pour imposer la famille d'adresses (§ 3.1.3 du guide d'utilisation et de supervision ; chapitre 4 du guide d'utilisation et de supervision) ; faire publier l'enregistrement AAAA

Symptôme	Causes possibles	Vérifications	Actions correctives
`dns_error` sur un contrôle dont `ipFamily` vaut `ipv6`	Le nom de la cible n'a pas d'adresse IPv6 (enregistrement AAAA absent)	Contrôle `dns` avec `dns.recordType` à `AAAA`	Faire publier l'enregistrement AAAA, ou revenir à `ipFamily: auto`
Contrôles en IPv6 en échec (`timeout`, `connection_refused`) alors qu'ils réussissent en IPv4	Enregistrement AAAA absent ou erroné ; pare-feu ou routage IPv6 incomplet entre la sonde et la cible ; règles de filtrage différentes entre IPv4 et IPv6	Contrôle `dns` avec `dns.recordType` à `AAAA` ; contrôle `tcp` ou `icmp` avec `ipFamily: ipv6` ; règles des pare-feu intermédiaires	Faire corriger l'enregistrement AAAA ; faire ouvrir les flux en IPv6 comme en IPv4 (§ 10.3). Le pare-feu local de la sonde applique les mêmes règles en IPv6 qu'en IPv4
SSH impossible à activer	SSH verrouillé définitivement (`ssh.locked: true`, par le fichier de provisionnement ou par `POST /api/v1/settings/ssh/lock`) ; compte sans rôle `admin`	Section `ssh` des paramètres (`locked`) ; journal d'audit	Le verrouillage est irréversible jusqu'à une réinitialisation usine. Transmettre une archive de diagnostic au support (§ 9.9) plutôt qu'un accès SSH. La récupération du compte administrateur reste possible
Session SSH fermée, SSH désactivé de lui-même	Comportement normal : l'échéance `enabledUntil` est atteinte (4 heures par défaut, 72 heures au maximum) ; les sessions ouvertes sont alors fermées	Section `ssh` (`enabled`, `enabledUntil`) ; journal d'audit (activation, connexions, désactivation)	Réactiver SSH avec une nouvelle échéance adaptée à l'intervention (§ 5.9.4)
Perte de l'accès après une modification de la configuration réseau	Erreur d'adresse, de masque ou de passerelle	Attendre 120 secondes : sans confirmation, la sonde revient automatiquement à la configuration précédente	Recommencer avec les bonnes valeurs ; confirmer dans le délai (chapitre 5)
Les noms ne sont pas résolus (`error.type = dns_error` sur de nombreux contrôles)	Serveurs DNS injoignables ou mal configurés ; nom interne non résolu par un DNS public	`getent hosts <nom>` en SSH ; contrôle `dns` de test (chapitre 4 du guide d'utilisation et de supervision)	Corriger les serveurs DNS ; utiliser les serveurs DNS internes pour les noms internes
Heure incorrecte ; erreurs TLS généralisées (« certificat pas encore valide ») ; horodatages incohérents dans les plateformes	Synchronisation NTP impossible : flux UDP 123 bloqué, serveur NTP injoignable. Sans pile, l'horloge du Raspberry Pi 5 ne conserve pas l'heure hors tension	`timedatectl` ; état NTP dans `GET /api/v1/system`	Ouvrir le flux UDP 123 vers les serveurs NTP configurés ; utiliser le serveur NTP interne de l'entreprise
Accès Internet impossible malgré un proxy configuré	Adresse ou port du proxy erronés ; authentification refusée ; proxy n'autorisant pas `CONNECT` sur le port de destination	Message d'erreur des contrôles HTTP (`407 Proxy Authentication Required`) ; journaux du proxy	Corriger les paramètres (chapitre 5) ; autoriser l'adresse IP de la sonde ; ajouter les destinations internes dans la liste d'exclusions

Symptôme	Causes possibles	Vérifications	Actions correctives
Les ressources internes échouent alors que les ressources Internet fonctionnent	Requêtes internes envoyées au proxy	Liste d'exclusions du proxy	Ajouter les domaines et plages internes à la liste d'exclusions
L'interface d'administration est inaccessible depuis certains postes	Pare-feu entre le poste et la sonde ; liste d'adresses autorisées configurée sur la sonde	Test `curl -v https://<sonde>/health` depuis le poste ; paramètres de sécurité de la sonde	Ouvrir le port TCP 443 depuis le réseau d'administration ; ajuster la liste d'adresses autorisées
Les contrôles vers une zone réseau précise échouent tous (`connection_refused`, `timeout`)	Règles de pare-feu entre la zone de la sonde et la zone cible ; routage	`ping`, `curl -v`, contrôle `tcp` sur le port concerné	Faire ouvrir les flux nécessaires (§ 10.3)
Contrôles en erreur après déplacement de la sonde	Nouveau réseau, nouveau VLAN, nouveaux serveurs DNS ou proxy	Configuration réseau effective	Mettre à jour la configuration réseau, DNS et proxy

9.6 Stockage

Symptôme	Causes possibles	Vérifications	Actions correctives
Alerte d'espace disque, `sva.storage.usage` élevé	Rétention trop longue pour le nombre de contrôles ; nombreux artefacts ; carte de faible capacité	`df -h` ; paramètres de rétention	Réduire la rétention des exécutions détaillées ou des artefacts (chapitre 6) ; la sonde purge automatiquement les données les plus anciennes avant saturation
Disque plein	Purge insuffisante ; fichiers anormaux	`df -h`	La sonde poursuit les contrôles et supprime en priorité les artefacts les plus anciens ; si la situation persiste, contacter le support
Message signalant une récupération de la base au démarrage, historique des résultats vide	La sonde a détecté une base corrompue (généralement après une coupure électrique) et l'a restaurée à partir de la dernière sauvegarde de configuration	Journal d'audit et métrique `sva.storage.recoveries`	La configuration est préservée, l'historique récent est perdu. Identifier la cause de la coupure (onduleur, alimentation) ; envisager le remplacement de la carte si l'incident se répète
La sonde démarre en mode « non initialisée » après un incident	Aucune sauvegarde de configuration valide n'a pu être restaurée	Interface : message d'incident	Importer le dernier export de configuration (§ 8.5) ou relancer la mise en service
Erreurs en lecture seule (« read-only file system »)	Le système a remonté une partition en lecture seule après des erreurs : carte défaillante	`dmesg` ; `mount`	Exporter la configuration si l'interface répond encore ; remplacer la carte (§ 8.6)

Symptôme	Causes possibles	Vérifications	Actions correctives
État de santé `storage` en `CRITICAL` sur une sonde équipée d'un SSD NVMe	SSD absent, mal enfiché, non détecté ou défaillant ; carte M.2 HAT+ mal raccordée ; alimentation insuffisante (l'alimentation officielle de 27 W est requise)	État de santé `storage` dans `GET /api/v1/system` ; `dmesg --level=err,warn` (erreurs `nvme` ou PCIe) ; `vcgencmd get_throttled`	Les contrôles continuent : l'historique local est conservé sur la microSD en mode réduit, et la configuration, les secrets et le système, qui résident sur la microSD, ne sont pas affectés. Arrêter proprement la sonde, vérifier le raccordement de la carte M.2 HAT+ et du SSD, puis redémarrer. Si le SSD est défaillant, le remplacer par un modèle de la liste des modèles pris en charge, publiée dans les notes de version, et l'activer de nouveau (chapitre 8)
Historique plus court que prévu, artefacts moins nombreux	Fonctionnement en mode réduit sur la microSD après la perte du SSD	État de santé `storage`	Rétablir ou remplacer le SSD (ligne précédente). L'historique conservé sur le SSD défaillant peut être perdu

9.7 Mises à jour

Symptôme	Causes possibles	Vérifications	Actions correctives
Aucune mise à jour proposée	Mode manuel sans vérification récente ; dépôt injoignable (proxy, pare-feu) ; période de support terminée (`supportEndsAt` dépassée : plus aucun correctif, état de santé `support` en `WARNING`) ; pour une version fonctionnelle seulement, justificatif de maintenance absent ou échu (`maintenanceEndsAt`) : les correctifs de sécurité restent proposés sans justificatif	État des mises à jour (`GET /api/v1/updates`, champs `supportEndsAt` et `maintenanceEndsAt`) ; flux HTTPS vers le dépôt (`https://updates-synovex.incitypark.fr` par défaut, ou votre miroir interne)	Ouvrir le flux sortant ; vérifier le proxy ; importer un justificatif de maintenance en cours de validité (`PUT /api/v1/system/maintenance`, chapitre 8) pour accéder aux versions fonctionnelles
Image refusée alors que sa signature est valide	Métadonnées du dépôt ou du miroir expirées (`validUntil`, 7 jours) : miroir interne non synchronisé ; image de version inférieure à la version installée (règle anti-retour en arrière, y compris pour un import hors ligne)	Message d'erreur ; date de dernière synchronisation du miroir ; version installée dans `GET /api/v1/updates`	Synchroniser le miroir ou revenir au dépôt de l'éditeur ; importer une image de version égale ou supérieure (§ 8.4.4 et § 8.4.5)
Activation programmée refusée (`422`)	Date `scheduledAt` passée ou située à moins d'une minute	Corps de la requête ; heure du poste (dates en UTC)	Indiquer une date future, à plus d'une minute ; une date antérieure à l'expiration du préavis est acceptée avec `noticeReduced: true` (§ 8.4.2)
Échec de vérification de signature	Image de mise à jour (*bundle*) altérée ou incomplète, téléchargée ou téléversée (`POST /api/v1/updates/upload`) ; heure système incorrecte	`timedatectl` ; message d'erreur	Ne pas forcer l'installation ; corriger l'heure ; relancer le téléchargement ; contacter le support si l'erreur persiste
Les scénarios échouent après une mise à jour	Nouvelle version de Chromium ou de Puppeteer modifiant un comportement	Notes de version ; comparaison avant/après	Consulter les notes de version ; adapter les scénarios concernés ; signaler la régression au support

Symptôme	Causes possibles	Vérifications	Actions correctives
La sonde ne redémarre pas correctement après une mise à jour	Coupure pendant l'installation ; incident logiciel de la nouvelle version ; blocage du système avant le démarrage des services	Accès à `/health` ; écran HDMI	Patienter sans couper l'alimentation : l'autotest dispose de 10 minutes ; s'il échoue, la sonde revient automatiquement à l'emplacement système précédent (ligne suivante). Ces 10 minutes ne sont pas une durée garantie de retour : si le système est bloqué, le retour suppose un redémarrage effectif. Un blocage avant le démarrage des services est traité par le chien de garde du chargeur d'amorçage puis par le chien de garde matériel, qui réinitialisent la carte (§ 8.4.5) ; toute réinitialisation pendant le démarrage d'essai ramène la sonde sur l'emplacement précédent, car l'indicateur *tryboot* est à usage unique (§ 8.4.5). Si la sonde reste injoignable au-delà, contacter le support
Mise à jour annulée par retour arrière automatique : la version précédente est de nouveau active	La nouvelle version n'a pas été jugée saine dans les 10 minutes suivant son démarrage (moteur principal, API ou autotest en échec) ; la sonde est revenue à l'emplacement précédent et a restauré les bases sauvegardées avant la migration	`GET /api/v1/updates` : version de chaque emplacement et emplacement actif ; journal d'audit (installation, redémarrage, retour arrière)	Aucune action urgente : la sonde fonctionne sur la version précédente, avec sa configuration. Ne pas relancer la même mise à jour en boucle ; préparer une archive de diagnostic et contacter le support (§ 9.9)
Mise à jour activée en dehors de la période souhaitée	Fenêtres de maintenance mal réglées : jours, heure de début ou durée erronés, ou fuseau horaire de la sonde différent de celui retenu pour définir les fenêtres ; correctif critique activé dès que possible (`updates.security.criticalPolicy: asap`) ; activation déclenchée ou programmée par un administrateur (`POST /api/v1/updates/apply`, éventuellement avec `scheduledAt`)	Section `updates` des paramètres : `windows` (`days`, `start` au format `HH:MM`, `duration`) et `security.criticalPolicy` ; fuseau horaire de la sonde (chapitre 5) ; journal d'audit ; événement `update.scheduled`	Corriger les fenêtres ou le fuseau horaire ; revenir à `criticalPolicy: next-window` si nécessaire ; passer un canal en mode `manual` si votre organisation l'exige (chapitre 8)

Symptôme	Causes possibles	Vérifications	Actions correctives
Mise à jour installée mais qui ne s'active pas (état de santé `updates` en `WARNING` ou `CRITICAL`)	Aucune fenêtre de maintenance définie : sans fenêtre, aucune activation automatique ordinaire ni aucun correctif critique en mode `next-window` n'est activé ; activation reportée (`POST /api/v1/updates/postpone`, jusqu'à la date `until`) ; préavis non respecté : une activation automatique ordinaire doit être annoncée au moins `updates.notice` avant son début (24 heures par défaut), un correctif critique au moins 15 minutes avant le début de la fenêtre retenue, sinon l'activation passe à la fenêtre suivante ; canal concerné en mode `manual`	`GET /api/v1/updates` (champ `scheduledActivation`) ; métriques `sva.update.pending`, `sva.maintenance.next_start` et `sva.maintenance.next_end` ; section `updates` (`windows`, `notice`, `security.mode`, `security.criticalPolicy`, `feature.mode`) ; journal d'audit (report) ; événement `update.cancelled` (motif de l'annulation)	Définir au moins une fenêtre de maintenance ; ou activer la mise à jour par `POST /api/v1/updates/apply`, immédiatement ou à une heure donnée (`scheduledAt`) ; vérifier l'échéance d'un report ; pour un correctif critique (`CRITICAL`), ne pas différer l'activation au-delà du nécessaire : le report est limité à 7 jours (chapitre 8)
Contrôles en `UNKNOWN` avec le type d'erreur `maintenance`	Exécutions interrompues par le drainage au début de l'activation d'une mise à jour : elles ne se sont pas terminées dans le délai `updates.drainTimeout` (5 minutes par défaut)	Heure des exécutions comparée aux fenêtres de maintenance ; événements `maintenance.started` et `maintenance.ended` ; journal d'audit	Aucune action si le phénomène est ponctuel et coïncide avec une activation. S'il touche régulièrement les mêmes plans ou scénarios longs, allonger `drainTimeout` (30 minutes au maximum) ou déplacer les fenêtres hors des créneaux de ces plans (chapitre 6 du guide d'utilisation et de supervision)
Alertes reçues pendant la maintenance de la sonde (sonde injoignable, absence de données de la sonde dans la plateforme)	L'état de maintenance ne suffit pas à supprimer les alertes : la sonde est injoignable pendant son redémarrage ; périodes de maintenance non déclarées dans la plateforme, ou non alignées sur les fenêtres de la sonde	Heure des alertes comparée à `sva.maintenance.next_start` et `sva.maintenance.next_end` ; métrique `sva.agent.maintenance`	Configurer dans la plateforme des périodes de maintenance alignées sur les fenêtres de la sonde (Alertmanager, Datadog, Dynatrace, Centreon, Nagios) et, pour Prometheus, exclure la sonde en maintenance des règles d'alerte (chapitre 2 du guide d'intégration et d'observabilité) ; pour une supervision sans interruption, déployer plusieurs sondes par site avec des fenêtres qui ne se chevauchent pas (chapitre 8)

9.8 Types d'erreur et actions de premier niveau

Le tableau suivant reprend la liste fermée des types d'erreur que la sonde associe à une exécution (champ `error.type`). Le § 8.1 de la référence technique et API en donne une description complète.

Type d'erreur	État habituel	Origine probable	Première action
`timeout`	`CRITICAL`	Ressource lente ou flux filtré	Vérifier la ressource et le flux ; ajuster le timeout
`dns_error`	`CRITICAL`	Nom ou DNS	Contrôle `dns` ; configuration DNS
`connection_refused`	`CRITICAL`	Service arrêté, mauvais port	Contrôle `tcp`

Type d'erreur	État habituel	Origine probable	Première action
`connection_reset`	`CRITICAL`	Coupure par le serveur, un pare-feu ou un équipement intermédiaire	Journaux du serveur et des équipements réseau
`tls_error`	`CRITICAL`	Autorité, nom ou protocole TLS	Autorité de certification interne, nom exact
`certificate_expired`	`CRITICAL`	Certificat serveur expiré	Renouvellement du certificat
`http_status`	`CRITICAL`	Code HTTP inattendu	Code, redirections, authentification
`assertion_failed`	`CRITICAL`	Contenu différent de l'attendu	Comparer réel et attendu
`element_not_found`	`CRITICAL`	Sélecteur obsolète, élément tardif	Capture d'écran ; sélecteur
`navigation_error`	`CRITICAL`	Navigation impossible	Réseau ; URL
`script_error`	`CRITICAL`	Erreur dans un scénario scripté	Corriger et tester le script
`browser_crash`	`UNKNOWN`	Chromium défaillant	Mémoire, redémarrage
`plugin_error`	`UNKNOWN`	Plugin Nagios qui n'a pas pu s'exécuter jusqu'à son terme, ou code retour en dehors de 0 à 3	Sortie du plugin, nom et arguments
`secret_missing`	`UNKNOWN`	Secret référencé par le contrôle mais absent de la sonde (non créé, supprimé, mal orthographié, configuration importée sans ses secrets)	Un administrateur crée le secret, avec ses hôtes autorisés (§ 6.8)
`database_error`	`CRITICAL`	Connexion ou requête SQL	Paramètres, pilote, requête
`no_data`	`UNKNOWN` (selon `onEmpty`)	Requête `database` sans aucune ligne renvoyée	Réécrire la requête pour qu'elle renvoie toujours une ligne (chapitre 5 du guide d'utilisation et de supervision)
`auth_failed`	`CRITICAL`	Identifiants refusés	Secret, état du compte
`resource_exhausted`	`UNKNOWN`	Sonde à court de ressources	Concurrence, RAM
`runner_crash`	`UNKNOWN`	Moteur de scénarios interrompu	Redémarrage automatique ; si répété, support
`agent_restart`	`UNKNOWN`	Moteur principal redémarré pendant l'exécution	Cause du redémarrage (mise à jour, coupure)
`maintenance`	`UNKNOWN`	Exécution interrompue par le drainage au début de l'activation d'une mise à jour	Aucune si ponctuel ; sinon ajuster `updates.drainTimeout` ou les fenêtres (§ 9.7)
`unknown`	`UNKNOWN`	Erreur non classée	Message ; support si répété

9.9 Préparer une demande au support

Une demande complète réduit fortement le délai de résolution. Avant de contacter le support (coordonnées en § 10.5), rassemblez les informations suivantes.

Information	Où la trouver
Version du produit, édition, version de Chromium et de Puppeteer	`GET /api/v1/system` ou page de santé de l'interface

Information	Où la trouver
Numéro de série ou adresse MAC de la sonde	Étiquette du boîtier complet ou `GET /api/v1/system`
Offre matérielle (microSD préconfigurée ou boîtier complet), modèle et RAM du Raspberry Pi 5, alimentation utilisée	Inventaire
Description du symptôme, date et heure (UTC) de début, fréquence	Votre constat, historique des exécutions
Identifiants des exécutions concernées (`runId`) et des contrôles (`checkId`)	Interface, `GET /api/v1/runs`
Détail des exécutions en échec (étapes, type d'erreur, message)	`GET /api/v1/runs/{runId}`
Captures d'écran et journaux de console des scénarios en échec	Artefacts (après vérification de leur contenu, voir ci-dessous)
Résultat du test de la destination d'export, le cas échéant	`POST /api/v1/exporters/{id}/test`
Résultat de `vcgencmd get_throttled` et température	SSH ou métriques
Modifications récentes : configuration, réseau, mise à jour, évolution de l'application supervisée	Journal d'audit, gestion des changements
Actions déjà tentées et leur effet	Votre historique
Archive de diagnostic : version, état de santé, configuration sans les secrets et journaux récents	`POST /api/v1/system/diagnostics` (rôle `admin`) : téléchargez l'archive, vérifiez son contenu (captures, journaux), puis transmettez-la vous-même au support par le canal qu'il vous indique

Avertissement — Ne transmettez jamais de secret au support : mots de passe des comptes de test, jetons d'API, clés d'ingestion, empreintes de mot de passe, clés privées. Avant de joindre une capture d'écran, un journal de console ou un export de configuration, vérifiez qu'il ne contient ni donnée personnelle ni donnée sensible. Les exports de configuration doivent être produits **sans les secrets** (§ 8.5).

Attention — Avant de transmettre l'archive de diagnostic, ouvrez-la et vérifiez son contenu. Les journaux et les captures d'écran peuvent contenir des données personnelles ou un secret réaffiché par une application supervisée : le masquage automatique des valeurs connues ne couvre pas ces cas. Retirez ou masquez tout élément sensible. Transmettez l'archive uniquement par le canal indiqué par le support. La durée de conservation des archives par l'éditeur est définie dans sa politique de support, selon les conditions de votre contrat, et indiquée sur le portail du support (`https://support-synovex.incitypark.fr`).

Information — Modalités d'intervention à distance du support :

- L'éditeur ne dispose d'**aucun accès permanent** à la sonde : aucun compte, aucune clé ni aucun canal ne lui est réservé.
- La sonde n'envoie **aucune donnée** à l'éditeur (pas de télémétrie). Ses seuls échanges avec l'éditeur sont la vérification et le téléchargement des mises à jour, si vous les avez activés.
- Le mode d'intervention privilégié est l'**archive de diagnostic**, que vous produisez (`POST /api/v1/system/diagnostics`), vérifiez et transmettez vous-même au support.
- Si une intervention en ligne de commande est nécessaire, seul un administrateur de votre organisation peut activer un **accès SSH temporaire** (§ 9.2.4 ; § 5.9.4) : échéance obligatoire, de 4 heures par défaut et de 72 heures au maximum, désactivation automatique à l'échéance avec fermeture des sessions, et enregistrement de l'activation, des connexions et de la désactivation dans le journal d'audit. Déposez la clé publique fournie par le support et désactivez SSH dès la fin de l'intervention.
- Si SSH a été verrouillé (`ssh.locked`), aucune intervention SSH n'est possible : le support travaille alors à partir de l'archive de diagnostic.

Les conditions contractuelles d'intervention (délais, horaires) sont définies dans votre contrat de maintenance.

Chapitre 10 — Références d'administration

10.1 Récapitulatif des prérequis

Le détail figure au chapitre 2.

> **Information** — Cette annexe est un aide-mémoire des prérequis et de la configuration matérielle minimale de chaque édition. Elle ne dimensionne pas une sonde : la méthode de calcul de la charge, les seuils et le nombre de contrôles qu'une sonde peut exécuter sont décrits au § 6.6 du guide d'utilisation et de supervision (« Charge et dimensionnement »).

10.1.1 Matériel

Élément	Essential	Professional	Enterprise
Carte	Raspberry Pi 5	Raspberry Pi 5	Raspberry Pi 5
Mémoire vive	2 Go minimum, 4 Go recommandés	4 Go minimum	8 Go minimum
Stockage	microSD préconfigurée 32 Go, High Endurance, fournie par l'éditeur	Idem	Idem
Stockage complémentaire (facultatif)	SSD NVMe M.2 2230 ou 2242 de la liste des modèles pris en charge, sur carte M.2 HAT+ officielle de Raspberry Pi	Idem	Idem ; surtout utile pour cette édition
Alimentation	Officielle 27 W USB-C (5,1 V, 5 A) recommandée ; obligatoire avec un SSD NVMe	Idem	Officielle 27 W fortement recommandée ; obligatoire avec un SSD NVMe
Refroidissement	Refroidisseur actif officiel ou boîtier ventilé recommandé	Idem	Refroidisseur actif officiel ou boîtier ventilé **obligatoire**
Réseau	Port Ethernet et câble RJ45	Idem	Idem
Boîtier	Recommandé	Recommandé	Recommandé, ventilé

Dans l'offre « boîtier complet », le Raspberry Pi 5, le boîtier, le refroidissement et la carte microSD sont fournis et assemblés. Les autres éléments (alimentation, câble Ethernet, accessoires, SSD) ne sont fournis que s'ils figurent sur la liste de colisage de votre commande (§ 2.1.3).

Avec un SSD, l'alimentation officielle de 27 W est requise. Le refroidisseur actif (*Active Cooler*) est compatible avec la carte M.2 HAT+ et s'installe en premier. Le boîtier officiel du Raspberry Pi 5 n'est alors utilisable que sans couvercle ni ventilateur. La liste des modèles de SSD pris en charge figure dans les notes de version. Voir chapitres 2 et 3.

10.1.2 Réseau

Élément	Exigence
Adressage	Serveur DHCP, ou adresse IP statique réservée avec masque, passerelle et serveurs DNS. IPv4 obligatoire

Élément	Exigence
IPv6 (facultatif)	Désactivé par défaut. Si activé : autoconfiguration (SLAAC) sur le lien, ou adresse statique (notation CIDR) et passerelle ; ICMPv6 autorisé pour la découverte des voisins
Port de commutateur	Port d'accès dans le VLAN de supervision : la sonde n'étiquette pas ses trames
802.1X (si le port est contrôlé)	Serveur RADIUS acceptant EAP-TLS ; certificat client émis pour la sonde (demande générée sur la sonde, recommandé, ou fichier PKCS#12) ; certificat de l'autorité de certification du serveur RADIUS. À défaut, port non contrôlé ou exception par adresse MAC (MAB) pour la première mise en service
DNS	Serveurs, en IPv4 ou en IPv6, capables de résoudre les noms des ressources supervisées
NTP	Accès à au moins un serveur NTP (UDP 123)
Proxy	Adresse, port et éventuels identifiants si les flux sortants passent par un proxy
Pare-feu	Flux du § 10.3 ouverts
Poste d'administration	Navigateur récent, sur un réseau autorisé à joindre la sonde en HTTPS

10.1.3 Organisation et sécurité

Élément	Exigence
Édition	Édition indiquée sur l'encart ou l'étiquette, conforme à la commande
Comptes de test	Un compte dédié par application, sans données réelles, droits minimaux, sans authentification multifacteur dans l'environnement supervisé
Comptes de base de données	Lecture seule, limités aux objets interrogés
Clés d'ingestion	Pour chaque plateforme d'observabilité retenue, avec les droits d'ingestion requis
Certificat (facultatif)	Certificat émis par l'autorité de l'entreprise pour le nom de la sonde
Code de récupération	Coffre-fort de mots de passe de l'organisation prêt à recevoir le code de récupération, affiché une seule fois à la fin de la mise en service
Contrat de maintenance (facultatif)	Justificatif de maintenance fourni par l'éditeur, à importer sur la sonde pour accéder aux nouvelles versions fonctionnelles
Lieu d'installation	Local technique ou baie, ventilé, à l'abri de l'humidité, idéalement sur alimentation secourue

10.2 Checklist de mise en service

Cochez chaque point au fur et à mesure. Les renvois indiquent la procédure détaillée.

Avant l'installation

- [ ] Édition acquise conforme à la commande ; encart ou étiquette (code d'installation) disponible (chapitre 4)
- [ ] Matériel conforme à l'édition, ou boîtier complet reçu (chapitre 2, § 10.1)
- [ ] Emplacement choisi : ventilation, alimentation secourue, port réseau disponible (chapitre 3)
- [ ] Port de commutateur configuré en mode accès dans le bon VLAN (chapitre 5)
- [ ] Si le port est soumis à 802.1X : certificat client (ou demande à générer sur la sonde) et certificat de l'AC du serveur RADIUS préparés, ou port non contrôlé / exception MAB prévus pour la première mise en service (chapitre 5)

- [ ] Décision prise sur l'activation d'IPv6 et, le cas échéant, paramètres définis : SLAAC ou adresse statique (chapitre 5)
- [ ] Adresse IP réservée en DHCP ou attribuée en statique (chapitre 5)
- [ ] Flux réseau ouverts conformément au § 10.3
- [ ] Paramètres de proxy connus, le cas échéant (chapitre 5)
- [ ] Comptes de test et comptes de base de données créés (chapitre 6 et chapitre 5 du guide d'utilisation et de supervision)
- [ ] Méthode de mise en service choisie : fichier de provisionnement ou assistant (chapitre 4)
- [ ] Le cas échéant, `provision.yaml` préparé, validé et copié à la racine de la partition de démarrage, avec les fichiers 802.1X qu'il désigne (chapitres 4 et 5)
- [ ] Coffre-fort de l'organisation prêt à recevoir le code de récupération (chapitre 4)

Installation physique

- [ ] Carte microSD insérée hors tension, contacts tournés vers la carte (chapitre 3)
- [ ] Refroidisseur et boîtier installés (chapitre 3)
- [ ] Le cas échéant, SSD NVMe monté sur la carte M.2 HAT+, après le refroidisseur actif ; boîtier officiel sans couvercle ni ventilateur (chapitre 3)
- [ ] Câble Ethernet branché avant la mise sous tension (chapitre 3)
- [ ] Alimentation conforme branchée (chapitre 3)
- [ ] Voyants conformes au comportement attendu (chapitre 3)

Mise en service

- [ ] Adresse de la sonde identifiée (chapitre 4)
- [ ] Empreinte du certificat vérifiée à la première connexion (chapitre 4)
- [ ] Assistant terminé ou provisionnement confirmé par `provision-result.txt` (chapitre 4)
- [ ] `provision.yaml` absent de la partition de démarrage après provisionnement, ainsi que les fichiers 802.1X (`pkcs12File`, `caFile`) (chapitre 4)
- [ ] Le cas échéant, authentification 802.1X réussie : état de santé `network` normal (chapitre 5)
- [ ] Édition correcte affichée (chapitre 4)
- [ ] Heure correcte et synchronisation NTP active (chapitre 5)
- [ ] Compte administrateur nominatif créé ; second administrateur prévu (chapitre 6)
- [ ] Certificat de l'entreprise installé, le cas échéant (chapitre 5)
- [ ] SSH laissé désactivé, sauf besoin justifié ; verrouillage définitif décidé selon votre politique de sécurité (chapitre 5)
- [ ] Code de récupération affiché à la fin de la mise en service, conservé dans le coffre-fort de l'organisation (chapitre 4)
- [ ] Le cas échéant, SSD activé et état de santé `storage` normal (chapitre 8)

Configuration de la supervision

- [ ] Secrets enregistrés (chapitre 6)
- [ ] Premier contrôle créé et exécution immédiate réussie (chapitre 4)
- [ ] Contrôles techniques configurés (chapitre 4 du guide d'utilisation et de supervision)
- [ ] Contrôles applicatifs et métier configurés (chapitre 5 du guide d'utilisation et de supervision)

- [ ] Scénarios navigateur testés en exécution d'essai (chapitres 4 et 5 du guide de développement des scénarios)
- [ ] Plans d'exécution et fenêtres d'activité définis (chapitre 6 du guide d'utilisation et de supervision)
- [ ] Seuils, timeouts et nouvelles tentatives ajustés (chapitre 3 du guide d'utilisation et de supervision)

Intégration et exploitation

- [ ] Destinations d'export créées et testées (chapitre 2 du guide d'intégration et d'observabilité)
- [ ] Données visibles dans la ou les plateformes (chapitre 2 du guide d'intégration et d'observabilité)
- [ ] Tableaux de bord et alertes créés ou importés, par exemple à partir des modèles Grafana et Prometheus fournis (chapitre 2 du guide d'intégration et d'observabilité)
- [ ] Alerte « sonde muette » configurée (chapitre 8)
- [ ] Services Nagios ou Centreon `check_sva` configurés, le cas échéant (chapitre 2 du guide d'intégration et d'observabilité)
- [ ] Politique de mises à jour définie : mode de chaque canal (correctifs de sécurité, versions fonctionnelles) et fenêtres de maintenance compatibles avec vos plans d'exécution, ou mode manuel assumé ; état de santé `updates` vérifié (chapitre 8)
- [ ] Alertes neutralisées pendant les fenêtres de maintenance sur vos plateformes (Alertmanager, Datadog, Dynatrace, Centreon, Nagios) ; pour un environnement critique, plusieurs sondes par site avec des fenêtres sans chevauchement (chapitre 2 du guide d'intégration et d'observabilité et chapitre 8)
- [ ] Date de fin de la période de support relevée (`supportEndsAt`) ; justificatif de maintenance importé si un contrat a été souscrit (chapitre 8)
- [ ] Premier export de configuration réalisé et archivé hors de la sonde (chapitre 8)
- [ ] Sonde inscrite à l'inventaire : emplacement, adresse, numéro de série, édition, responsable
- [ ] Contacts du support connus des équipes d'exploitation (§ 10.5)

10.3 Tableau des flux réseau

Ce tableau reprend, à l'identique, la matrice des flux de la configuration réseau, pour la transmettre à l'équipe chargée des pare-feu.

Sens	Source	Destination	Port / protocole	Usage	Obligatoire
Entrant	Postes d'administration	Sonde	443/TCP (HTTPS)	Interface d'administration, API	Oui
Entrant	Serveur Prometheus	Sonde	443/TCP (HTTPS)	Collecte de `/metrics`	Si Prometheus en mode collecte
Entrant	Serveur Nagios ou Centreon	Sonde	443/TCP (HTTPS)	Plugin `check_sva`	Si Nagios ou Centreon
Entrant	Postes d'administration	Sonde	80/TCP (HTTP)	Redirection permanente vers HTTPS, aucun contenu servi	Non (désactivable)
Entrant	Postes du réseau local	Sonde	5353/UDP (mDNS)	Résolution du nom `.local` de la sonde ; annonce active par défaut	Non (désactivable dans la section `network`)
Entrant	Postes d'administration autorisés	Sonde	22/TCP (SSH)	Maintenance avancée	Non : désactivé par défaut ; activation temporaire, 4 heures par défaut, 72 heures au maximum (§ 5.9.4)

Sens	Source	Destination	Port / protocole	Usage	Obligatoire
Couche 2 (sans flux IP)	Sonde	Commutateur (authentificateur 802.1X)	EAPOL (*EAP over LAN*) : trames Ethernet de type 0x888E, aucun port ni adresse IP	Authentification 802.1X EAP-TLS du port ; le commutateur relaie vers le serveur RADIUS	Si le port est contrôlé par 802.1X (§ 5.2.6)
Entrant et sortant	Sonde	Routeurs et voisins du lien local	ICMPv6 (découverte des voisins, NDP, dont les annonces de routeur utilisées en mode `slaac`)	Adressage et résolution d'adresses IPv6	Si l'IPv6 est activé (§ 5.2.5)
Sortant	Sonde	Serveurs DHCP	67-68/UDP	Adressage	Si DHCP
Sortant	Sonde	Serveurs DNS	53/UDP et 53/TCP	Résolution de noms	Oui
Sortant	Sonde	Serveurs NTP	123/UDP	Synchronisation de l'heure	Oui
Sortant	Sonde	Dépôt de mises à jour de l'éditeur, ou miroir interne	443/TCP (HTTPS)	Mises à jour en ligne : vérification et téléchargement des images signées ; adresse par défaut `https://updates-synovex.incitypark.fr`, inscrite dans le profil éditeur	Si mises à jour en ligne
Sortant	Sonde	Proxy de l'entreprise	Port du proxy (par exemple 3128/TCP)	Relais des flux HTTP(S) sortants (§ 5.5)	Si proxy
Sortant	Sonde	Plateformes SaaS (Datadog, Dynatrace, Grafana Cloud)	443/TCP (HTTPS, OTLP/HTTP)	Export OpenTelemetry	Si configurées
Sortant	Sonde	Collecteur OpenTelemetry ou Agent Datadog du client	4318/TCP (OTLP/HTTP) ou 4317/TCP (OTLP/gRPC), selon le protocole de la destination (§ 2.1.4 du guide d'intégration et d'observabilité)	Export OpenTelemetry	Si configurés
Sortant	Sonde	Proxy inverse placé devant le récepteur OTLP de Prometheus	Port du proxy inverse (par exemple 443/TCP, HTTPS)	Export des métriques en mode envoi (§ 2.5.3 du guide d'intégration et d'observabilité)	Si configuré
Sortant	Sonde	Ressources supervisées	Selon les contrôles : ICMP ou ICMPv6 ; ports TCP des services ; 53 ; 80 et 443 ; SGBD : 5432 (PostgreSQL), 3306 (MySQL/MariaDB), 1433 (SQL Server), 1521 (Oracle)	Contrôles	Oui, selon les contrôles
Sortant	Sonde	Console centrale	443/TCP (HTTPS, authentification mutuelle mTLS)	Gestion multi-sondes	Non : évolution prévue, facultative

Information — Les ports des SGBD indiqués sont les ports par défaut. Ils peuvent différer dans votre environnement. Les ports des contrôles sont ceux que vous configurez. La sonde n'utilise aucun serveur de licences en ligne et n'envoie aucune télémétrie à l'éditeur.

Information — Si l'IPv6 est activé, les flux de ce tableau s'appliquent à l'identique en IPv6 : le pare-feu local de la sonde applique les mêmes règles dans les deux familles d'adresses. Les échanges RADIUS ont lieu entre le commutateur et le serveur RADIUS : ils ne partent pas de la sonde. Le mécanisme de mise à jour A/B ne crée aucun flux supplémentaire, et une mise à jour hors ligne n'en exige aucun vers l'éditeur.

10.4 Référence des configurations

Les tableaux ci-dessous résument les champs. Les schémas complets et les exemples figurent dans les chapitres indiqués.

10.4.1 Champs communs à tous les contrôles

Champ	Type	Obligatoire	Description
`id`	texte	Oui	Identifiant stable : minuscules, chiffres, tirets, 2 à 63 caractères
`name`	texte	Oui	Libellé lisible (120 caractères maximum)
`description`	texte	Non	Description libre
`type`	énumération	Oui	`icmp`, `tcp`, `dns`, `http`, `api`, `nagios`, `database`, `browser`
`enabled`	booléen	Non (`true`)	Activation
`tags`	objet	Non	8 étiquettes maximum
`schedule`	objet ou `null`	Non	`interval` (`5m`) **ou** `cron` + `timezone`, `jitter` ; `null` : exécution par un plan ou manuelle
`timeout`	durée	Non	Délai maximal de l'exécution
`retry`	objet	Non	`attempts` (0 à 5), `interval`
`thresholds`	objet	Non	`warningDuration`, `criticalDuration`
`secrets`	liste	Non	Noms des secrets autorisés (16 maximum)
`ipFamily`	énumération	Non (`auto`)	Famille d'adresses utilisée pour joindre la cible : `auto` (IPv6 si l'IPv6 est activé sur la sonde et si la cible a une adresse AAAA, sinon IPv4), `ipv4` ou `ipv6`

Durées : `500ms`, `30s`, `5m`, `1h`. Références : `${secret:NOM}`, `${param:nom}`, `${var:nom}`.

10.4.2 Champs propres à chaque type

Type	Champs principaux	Chapitre
`icmp`	`host`, `count` (1 à 20), `maxPacketLossPercent`, `warningRttMs`, `criticalRttMs`	chapitre 2 du guide d'utilisation et de supervision
`tcp`	`host`, `port`, `tls`, `send`, `expect`	chapitre 2 du guide d'utilisation et de supervision
`dns`	`name`, `recordType` (`A`, `AAAA`, `CNAME`, `MX`, `TXT`, `NS`, `SRV`, `PTR`, `SOA`), `servers`, `expect`	chapitre 2 du guide d'utilisation et de supervision
`http`	`method`, `url`, `headers`, `body`, `followRedirects`, `tls` (`verify`, `caRef`, `certificateExpiryWarningDays`, `certificateExpiryCriticalDays`), `proxy` (`"none"` pour contourner le proxy global), `assertions` (`kind` : `status`, `header`, `body`, `jsonPath`, `xpath`, `duration` ; `path`, `operator`, `value`)	chapitre 2 du guide d'utilisation et de supervision
`api`	`requests` (1 à 20) : champs de `http` + `name`, `extract` (`type` : `jsonpath`, `xpath`, `regex` ; `reveal` pour afficher la valeur, masquée par défaut)	chapitre 3 du guide d'utilisation et de supervision

Type	Champs principaux	Chapitre
`nagios`	`plugin` (nom sans chemin), `args`, `perfdataExport`	chapitre 2 du guide d'utilisation et de supervision
`database`	`engine` (`mysql`, `mariadb`, `postgresql`, `sqlserver`, `oracle`), `host`, `port`, `database`, `username`, `passwordSecret`, `query` **ou** `procedure`, `params`, `rules` (`column`, `operator` : `eq`, `ne`, `lt`, `lte`, `gt`, `gte` ; `value`, `severity`, `scope`), `onEmpty` (`UNKNOWN` par défaut), `exportValues` (première ligne), `tls`, `properties` (liste fermée de propriétés JDBC)	chapitre 3 du guide d'utilisation et de supervision
`browser`	`mode` (`steps` ou `script`), `steps` (50 maximum), `scriptRef`, `params`, `viewport`, `userAgentSuffix`, `captureOnFailure`, `blockDomains`	chapitre 2 du guide de développement des scénarios

Opérateurs d'assertion : `eq`, `ne`, `lt`, `lte`, `gt`, `gte`, `contains`, `notContains`, `matches`, `exists`.

Actions des scénarios déclaratifs : `goto`, `click`, `fill`, `select`, `press`, `hover`, `waitForSelector`, `waitForNavigation`, `assertVisible`, `assertHidden`, `assertText`, `assertUrl`, `assertTitle`. Propriétés d'une étape : `name`, `action`, `url`, `selector`, `frame`, `value`, `key`, `operator`, `timeout`, `waitForNavigation`.

10.4.3 Plan d'exécution

Champ	Description
`id`, `name`, `enabled`	Identification et activation
`schedule`	`interval` ou `cron` (obligatoire)
`activeWindows`	Liste de plages : `days` (`mon` à `sun`), `from`, `to` (`HH:MM`)
`stopOnFailure`	Arrêt du plan au premier échec
`maxDuration`	Durée maximale du plan
`items`	Liste ordonnée (1 à 50) : `checkId`, `continueOnFailure`

10.4.4 Destination d'export

Champ	Description
`id`, `kind` (`otlp` ou `prometheus`), `enabled`, `preset`	Identification ; préréglage : `otlp-generic`, `datadog-agent`, `datadog-agentless`, `dynatrace`, `grafana-cloud`, `prometheus-otlp`
`signals`	`metrics`, `traces`, `logs`
`endpoint` ou `signalEndpoints`	URL de base, ou URL complète par signal
`protocol`	`http/protobuf` (par défaut), `http/json`, `grpc`
`headers`	En-têtes ; les valeurs sensibles référencent un secret
`compression`, `timeout`, `tls`	`gzip` ou `none` ; délai ; `caRef`, `clientCertRef`, `insecureSkipVerify`
`metrics`	`temporality` (`cumulative` ou `delta`), `exportInterval`, `histogram`, `stepHistograms`
`logs`	`audit` : export du journal d'audit (`false` par défaut)
`retry`, `queue`	`maxElapsed` ; `maxBatches`
`path`, `requireToken`	Pour `kind: prometheus`

10.4.5 Fichier de provisionnement `provision.yaml` (chapitre 4)

Clé	Description
`version`	Version du format (`1`)
`hostname`	Nom d'hôte de la sonde
`site`	Nom du site (attribut `sva.site`)
`admin.username` , `admin.passwordHash`	Compte administrateur ; empreinte du mot de passe, jamais le mot de passe en clair. Format : Argon2id au format PHC (`$argon2id$v=19$m=…`)
`network.mode`	`dhcp` ou `static`
`network.address` , `network.gateway` , `network.dns` , `network.ntp`	Paramètres réseau ; les serveurs DNS peuvent être IPv4 ou IPv6
`network.ipv6.enabled` , `network.ipv6.mode` , `network.ipv6.address` , `network.ipv6.gateway`	IPv6 : activation (`false` par défaut), mode `slaac` ou `static` , adresse en notation CIDR et passerelle (mode `static`)
`dot1x.identity` , `dot1x.pkcs12File` , `dot1x.caFile` , `dot1x.pkcs12Password`	802.1X EAP-TLS avant tout accès au réseau : identité, fichier PKCS#12 de l'identifiant client et certificat de l'AC du serveur RADIUS, déposés sur la partition de démarrage, et mot de passe du fichier PKCS#12. Seul secret admis dans `provision.yaml` : fichiers et mot de passe sont supprimés après traitement
`ssh.locked`	`true` : verrouillage définitif de SSH, irréversible jusqu'à une réinitialisation usine
`updates.security.mode` , `updates.security.criticalPolicy` , `updates.security.criticalStagger` , `updates.feature.mode` , `updates.windows` , `updates.notice` , `updates.drainTimeout`	Politique de mises à jour dès le premier démarrage : mêmes champs et mêmes valeurs par défaut que la section `updates` (§ 10.4.7), **aucune fenêtre par défaut**
`proxy.url` , `proxy.noProxy`	Proxy sortant et exclusions

10.4.6 Valeurs par défaut

Paramètre	Valeur par défaut
Concurrence des contrôles légers	16, à titre indicatif
Concurrence plugins et bases de données	4, à titre indicatif
Concurrence navigateur	1 (2 configurable avec 8 Go), à titre indicatif
Intervalle entre nouvelles tentatives (`retry.interval`)	15 secondes
Durée maximale d'un plan d'exécution (`maxDuration`)	30 minutes
Export : `timeout` , `exportInterval`	10 secondes ; 60 secondes
Export : file d'attente (`queue.maxBatches`), taille d'un lot	100 lots ; 1 000 points par lot
Histogrammes par étape (`metrics.stepHistograms`)	Activés (`true`)
Scénarios : `viewport` , délai d'étape, délai de navigation	1366 × 768 ; 10 secondes ; 30 secondes
Contrôle `database` sans résultat (`onEmpty`)	`UNKNOWN` (`no_data`)
Pagination de l'API	100 éléments (1 000 au maximum)

Paramètre	Valeur par défaut
Rétention des exécutions détaillées	14 jours
Rétention des agrégats horaires	400 jours
Rétention des artefacts	7 jours et 500 Mo
Rétention du journal d'audit	365 jours
Sauvegarde automatique de la configuration	Quotidienne, 3 générations
Délai de confirmation d'une configuration réseau	120 secondes
Annonce mDNS	Active (désactivable dans la section `network`)
Pare-feu local	Actif : entrées 443/TCP, 80/TCP (redirection), 5353/UDP (mDNS), 22/TCP si SSH est activé ; mêmes règles en IPv6
Port 80	Redirection permanente vers HTTPS (désactivable)
Sessions de l'interface	Expiration après 30 minutes d'inactivité ; durée absolue de 12 heures
Blocage après échecs de connexion	15 minutes après 5 échecs consécutifs, par compte et par adresse source
Saisie du code d'installation	5 essais, puis blocage de 15 minutes, doublé à chaque nouvelle série
Mots de passe des comptes	12 caractères minimum, 128 maximum
Journaux système	En mémoire (volatils) ; persistance temporaire (`logging.persistentUntil`) de 72 heures au plus
Famille d'adresses des contrôles (`ipFamily`)	`auto`
IPv6 (`network.ipv6.enabled`)	Désactivé (`false`)
802.1X (`dot1x.enabled`)	Désactivé ; avertissement 30 jours avant l'expiration du certificat client
Durée d'activation de SSH (`ssh.enabledUntil`)	4 heures (72 heures au maximum)
Page de récupération du compte administrateur	Ouverte 30 minutes après le démarrage ; 3 essais au plus par ouverture
Code de réinitialisation usine (`factory-reset-challenge.txt`)	8 caractères, valable 24 heures
Activation des correctifs de sécurité (`updates.security.mode`)	`automatic`
Correctifs critiques (`updates.security.criticalPolicy`)	`next-window` (prochaine fenêtre)
Décalage des activations critiques (`updates.security.criticalStagger`)	`0` (aucun décalage)
Activation des versions fonctionnelles (`updates.feature.mode`)	`manual`
Fenêtres de maintenance (`updates.windows`)	Aucune : sans fenêtre, aucune activation automatique
Préavis avant activation (`updates.notice`)	24 heures (de 0 à 7 jours), pour une activation automatique ordinaire
Préavis d'un correctif critique	15 minutes (`next-window` et `asap`), augmentées du décalage `criticalStagger` en mode `asap`
Délai de drainage (`updates.drainTimeout`)	5 minutes (30 minutes au maximum)

Paramètre	Valeur par défaut
Report d'une activation (`POST /api/v1/updates/postpone`)	30 jours au plus ; 7 jours au plus pour un correctif critique
Autotest après mise à jour	10 minutes accordées à l'autotest ; à défaut, retour automatique à l'emplacement précédent, après un redémarrage effectif
Période de support (correctifs de sécurité)	Au moins 5 ans après la mise sur le marché de la version majeure

10.4.7 Sections de paramètres système : réseau IPv6, 802.1X, SSH et mises à jour (chapitres 5 et 8)

Ces sections se consultent et se modifient par `GET` et `PUT /api/v1/settings/{section}` (rôle `admin`). Le tableau ne reprend que les champs introduits par les fonctions correspondantes.

Section et champ	Description
`network.ipv6.enabled`	Activation de l'IPv6 (`false` par défaut) ; IPv4 reste toujours actif
`network.ipv6.mode`	`slaac` (autoconfiguration) ou `static`
`network.ipv6.address` , `network.ipv6.gateway`	Adresse en notation CIDR et passerelle, en mode `static` . Le certificat autosigné de la sonde inclut l'adresse IPv6 statique
`dot1x.enabled`	Activation de l'authentification 802.1X EAP-TLS sur la prise Ethernet
`dot1x.identity`	Identité présentée au serveur RADIUS
`dot1x.caRef`	Référence, dans la section `trust` , du certificat de l'AC du serveur RADIUS
`ssh.enabled`	Activation de SSH (seul un `admin` peut l'activer)
`ssh.enabledUntil`	Échéance de l'activation, obligatoire : 4 heures par défaut, 72 heures au maximum. À l'échéance, SSH se désactive et les sessions sont fermées
`ssh.authorizedKeys`	Clés publiques autorisées
`ssh.locked`	Verrouillage définitif, en lecture seule ici : il se pose par `provision.yaml` ou par `POST /api/v1/settings/ssh/lock`
`updates.security.mode`	Correctifs de sécurité : `automatic` (par défaut), activés dans une fenêtre de maintenance, ou `manual`
`updates.security.criticalPolicy`	Correctif d'une vulnérabilité activement exploitée : `next-window` (par défaut : au début de la première fenêtre qui commence au moins 15 minutes après l'annonce) ou `asap` (choix explicite : 15 minutes après l'annonce, augmentées de `criticalStagger` , même hors fenêtre) ; drainage dans les deux cas (§ 8.4.2)
`updates.security.criticalStagger`	Décalage fixe, propre à la sonde, ajouté au préavis de 15 minutes d'une activation `asap` , de `0` (par défaut) à `4h` : échelonne les sondes d'un même site, sans vérifier leur état (§ 8.4.11)
`updates.feature.mode`	Versions fonctionnelles, canal distinct : `manual` (par défaut) ou `automatic`
`updates.windows`	0 à 7 fenêtres de maintenance : `days` (`mon` à `sun`), `start` (`HH:MM`), `duration` . **Aucune fenêtre par défaut** : sans fenêtre, la mise à jour reste en attente et l'état de santé `updates` passe en `WARNING`
`updates.notice`	Préavis avant toute activation automatique : `24h` par défaut, de `0` à `7d` (activation manuelle et correctif critique : § 8.4.2 et § 8.4.11)
`updates.drainTimeout`	Délai de drainage : `5m` par défaut, `30m` au maximum

Section et champ	Description
`updates.repositoryUrl`	Facultatif : adresse d'un miroir interne du dépôt de mises à jour (HTTPS) ; les images restent signées et vérifiées

L'identifiant client 802.1X (clé privée et certificat) ne figure dans aucune section : il se génère par `POST /api/v1/system/dot1x/csr` ou s'importe par `PUT /api/v1/system/dot1x/credential`, en écriture seule.

10.5 Assistance et contacts

Rubrique	Information
Service, adresse électronique, téléphone, horaires et langues du support	Indiqués dans votre contrat ; le portail de support (voir ce tableau) centralise les demandes dès sa mise en service
Site commercial	`https://synovex.incitypark.fr`
Portail de support	`https://support-synovex.incitypark.fr`, après l'annonce de sa mise en service (encadré ci-dessous)
Niveaux de service	Délais de prise en charge définis par votre contrat, par niveau de gravité (§ 10.5.1) et par édition
Garantie et remplacement de carte	Durée, conditions et procédure de retour selon vos conditions de vente ; procédure technique de remplacement : § 8.6.4
Documentation en ligne et notes de version	`https://docs-synovex.incitypark.fr`, après l'annonce de sa mise en service (encadré ci-dessous)
Distribution des mises à jour	`https://updates-synovex.incitypark.fr` (utilisée par la sonde pour les mises à jour en ligne, après l'annonce de sa mise en service ; images signées)
Console de gestion centralisée	`https://fleet-synovex.incitypark.fr` : adresse réservée à la console centrale prévue ; non utilisée par la sonde
Signalement d'une vulnérabilité de sécurité	Canal dédié indiqué dans votre contrat, distinct des canaux ordinaires du support ; voir § 10.5.4
Service commercial (changement d'édition, reprise, remplacement de carte)	Coordonnées indiquées dans votre contrat ou votre bon de commande ; site commercial ci-dessus

> **Information** — Ces adresses constituent le plan de nommage officiel de l'éditeur ; les services correspondants sont mis en service progressivement. Une procédure qui s'appuie sur l'un de ces services (portail de support, documentation en ligne, téléchargement d'une image) ne s'applique qu'après l'annonce de sa mise en service par l'éditeur. Avant cette annonce, ou si un service ne répond pas, utilisez le canal de contact et de mise à disposition des images convenu dans votre contrat.

10.5.1 Niveaux de gravité proposés

Gravité	Définition	Exemple
1 — Bloquant	Sonde hors service, aucune supervision assurée	La sonde ne démarre plus
2 — Majeur	Fonction importante indisponible, sans contournement	Tous les scénarios navigateur en `UNKNOWN`
3 — Mineur	Fonction dégradée, contournement possible	Une destination d'export en erreur intermittente

Gravité	Définition	Exemple
4 — Demande	Question, demande d'information ou d'évolution	Conseil sur la conception d'un scénario

Les délais associés à chaque niveau sont définis par votre contrat.

10.5.2 Informations à préparer

Avant de contacter le support, rassemblez les informations listées au § 9.9 : version, édition, numéro de série ou adresse MAC, description et horodatage du symptôme, identifiants des exécutions, actions déjà tentées. Ne transmettez jamais de secret.

10.5.3 Ce que couvrent l'assistance et la maintenance

Service	Accès	Référence
Correctifs et avis de sécurité de la version acquise, pendant la période de support	Toute sonde, sans contrat	§ 8.4.6
Garantie et remplacement d'une carte défectueuse, sans rachat de l'édition acquise	Toute sonde, selon les conditions de vente	§ 8.6.4
Documentation et notes de version	Toute sonde	Ci-dessus
Nouvelles versions fonctionnelles	Sondes couvertes par un contrat de maintenance	§ 8.4.7
Assistance technique (diagnostic, conseil de configuration)	Sondes couvertes par un contrat de maintenance	Ce chapitre
Prestations : mise en service sur site, écriture de scénarios, formation, développement spécifique	Sur devis	Service commercial

Les conditions applicables, et notamment les délais de prise en charge, sont celles de vos conditions de vente et, le cas échéant, de votre contrat de maintenance. Aucun délai n'est garanti par cette documentation.

10.5.4 Signaler une vulnérabilité de sécurité

Si vous découvrez une vulnérabilité dans la sonde ou dans son logiciel intégré, signalez-la par le canal dédié indiqué dans votre contrat (tableau ci-dessus, rubrique « Signalement d'une vulnérabilité de sécurité »), et non par les canaux ordinaires du support. Votre contrat indique également où consulter la politique de divulgation coordonnée de l'éditeur, qui précise le traitement des signalements, ainsi que la clé de chiffrement à utiliser pour transmettre un signalement confidentiel.

Indiquez :

- la version et l'édition de la sonde ;
- la description de la vulnérabilité et son impact ;
- les étapes de reproduction.

Testez uniquement sur des sondes que vous possédez ou que vous êtes autorisé à tester, sans accéder aux données d'autrui ni perturber un service.

L'éditeur publie des avis de sécurité pour les vulnérabilités corrigées. Les correctifs sont diffusés par le canal `security` (§ 8.4).