Fiche mémo · Leçon 9 · 25 min

Les clés d'API, le .env et ce qui ne s'écrit jamais

Une clé d'API vit au coffre, jamais dans le code, un commit, un log ou la discussion. Nexus génère le .env du poste depuis le coffre : l'agent compare le gabarit .env.example à ce que le coffre sait poser, sans afficher une valeur. Le .env doit être ignoré par git, et la production ne descend jamais sur un poste.

Objectifs

- Écrire un gabarit .env.example et vérifier que git ignore le .env
- Faire générer le .env de développement depuis le coffre, en rangeant d'abord ce qui manque
- Réagir à une clé exposée en la révoquant chez le service, puis en mettant le coffre à jour

À retenir

- Une clé d'API vit au coffre, jamais dans le code, un commit, un log, le navigateur ou la discussion.
- Le .env.example dit les noms et se commite ; le .env porte les valeurs et git l'ignore, sinon Nexus refuse de l'écrire.
- Une variable descend dans le .env si son libellé au coffre est son nom, avec le type Variable d'environnement.
- La production ne descend jamais sur un poste, et en développement les courriels sont capturés.
- Une clé écrite une fois quelque part d'interdit est exposée : elle se révoque chez le service, puis se remplace au coffre.

Quels droits donner à une clé

Ce qu'elle peut faire \ Où elle circule	Un seul poste	Plusieurs outils
Écrire, envoyer	**À surveiller** — Clé d'envoi de courriels du site : rangée au coffre, révoquée au moindre doute.	**À éviter** — Une clé qui écrit et que trois outils emploient : séparez-la en clés dédiées.
Lire	**Sans souci** — Une clé de lecture sur votre poste, pour un script de suivi.	**Préférez** — Une clé de Nexus en lecture seule pour un tableau de bord : elle n'appelle que des outils de lecture.

Plus une clé circule, moins elle doit pouvoir faire.

La demande à recopier

Demande à recopier **Préparer le .env de développement**

```
Projet du site du négociant, environnement de développement.
1. Compare le gabarit .env.example à ce que le coffre sait poser, et dis-moi ce qui manque.
N'affiche aucune valeur.
2. Pour SESSION_SECRET : range-le au coffre en le faisant générer par Nexus, type Variable
d'environnement, environnement Développement.
3. Pour toute autre variable manquante : ne l'invente pas, dis-moi laquelle je dois ranger moi-
même.
4. Écris ensuite le .env de développement depuis le coffre, puis vérifie que git l'ignore.
Ne relis pas le .env pour m'en recopier les valeurs.
```

Note : Si la réponse contient une valeur, c'est une erreur à signaler : la clé exposée se change chez le service.

Le code à recopier

Le gabarit .env.example du site du négociant ENV

```
# Gabarit : les NOMS attendus, jamais les valeurs. Ce fichier se commite.

# Service d'envoi des courriels du formulaire de contact
EMAIL_API_KEY=
# Adresses qui reçoivent les demandes, séparées par des virgules
CONTACT_DESTINATAIRES=
# Secret de signature des sessions du site (généré, jamais choisi à la main)
SESSION_SECRET=
# SMTP : laissés vides en développement, Nexus pose un SMTP qui capture les courriels
SMTP_HOST=
SMTP_PORT=
SMTP_USER=
```

Les noms sont ceux de votre code : ils n'appartiennent ni à Nexus ni au service d'envoi.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Écrire la clé dans le code « juste pour tester », en se promettant de la retirer. Le test réussit, le fichier est commité avec le reste, et la clé vit dans l'historique pour toujours. La retirer ensuite ne l'efface pas.	Dès le premier essai, la clé passe par le coffre et le .env. Si elle a été commitée, elle se révoque chez le service.
Recopier dans la discussion les valeurs du .env pour « vérifier » qu'elles sont justes. La vérification affiche tous les secrets du poste dans une conversation conservée et transmise au fournisseur d'IA.	Demandez l'état : ce que le gabarit attend, ce que le coffre pose, ce qui manque. Les noms suffisent à vérifier.
Ranger une variable au coffre sous un libellé descriptif, « Clé Brevo du formulaire ». Pour descendre dans le .env, une variable d'environnement doit avoir pour libellé son nom exact. Le .env reste donc incomplet.	Libellé : EMAIL_API_KEY, le nom du gabarit. La description va dans les notes.
Copier le SMTP ou une clé de production dans le .env de son poste pour reproduire un bug. La production ne descend jamais sur un poste : un test envoie alors de vrais courriels à de vrais clients, et la clé quitte le coffre.	Reproduisez en préproduction avec ses propres accès, ou demandez à l'agent de lire les journaux de production en lecture seule.