Résoudre un 403 Nginx sans ouvrir les permissions à l'aveugle

Suivez le refus d'accès depuis la réponse HTTP jusqu'au fichier ou à la règle qui le bloque. Cette méthode permet de corriger une erreur 403 Forbidden ou « Permission denied » de façon ciblée.

Au sommaire

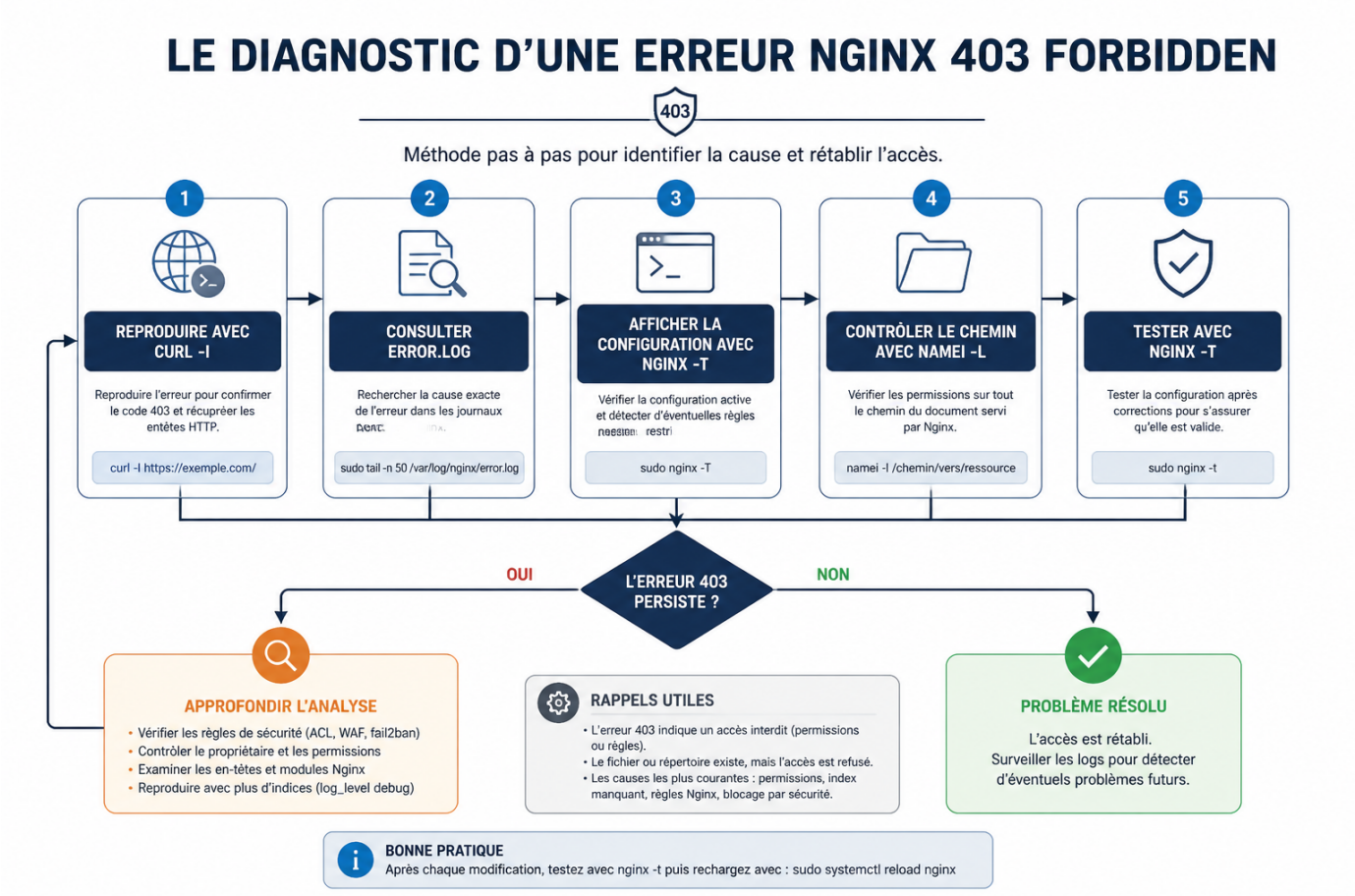
Le bon réflexe face à un 403

Un code 403 signifie que le serveur a compris la requête, mais en refuse l'accès.

Ne confondez pas 403 et 404 : un 403 désigne un problème d'autorisation, de règle ou de politique de sécurité.

Évitez chmod 777 : la correction doit préserver un accès minimal au contenu publié.

Commencez par les journaux Nginx avant de modifier les droits ou la configuration.



INFOGRAPHIE *Étapes de diagnostic Permission denied Nginx pour corriger une erreur 403 Forbidden.*

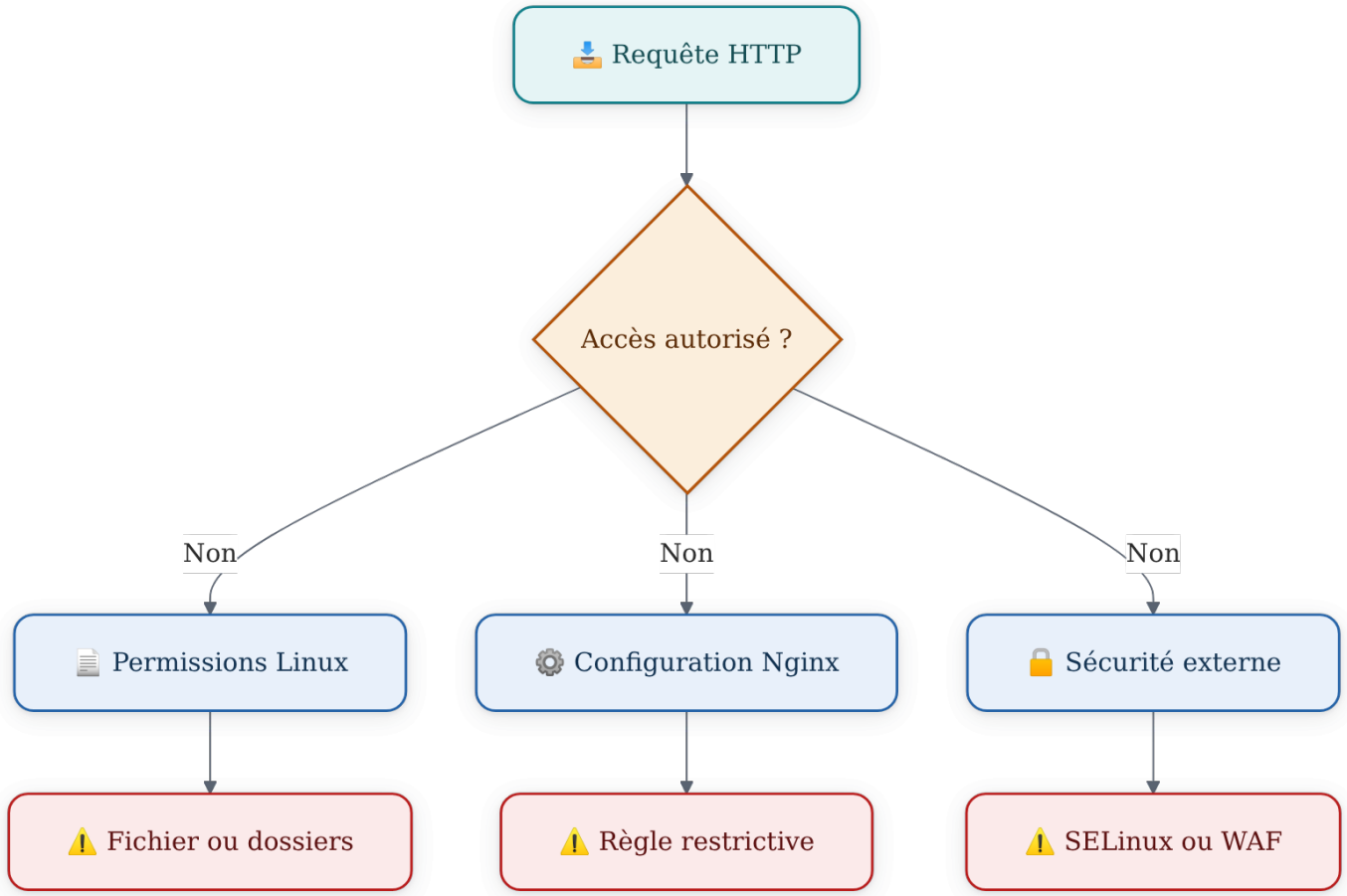
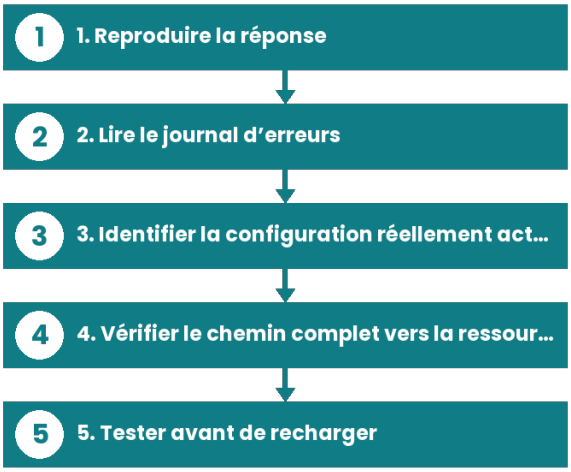


SCHÉMA *Les principales couches à contrôler lors d'une erreur Nginx 403 Forbidden.*

Diagnostic en 5 étapes



1 **1. Reproduire la réponse**
Utilisez curl -I https://exemple.fr/chemin pour confirmer le code HTTP, lire les en-têtes et repérer une éventuelle intervention d'un CDN ou d'un WAF.

2 **2. Lire le journal d'erreurs**
Consultez le fichier défini par error_log, souvent situé dans /var/log/nginx/error.log. Le message oriente la correction : « permission denied », « directory index is forbidden » et « access forbidden by rule » ne renvoient pas à la même cause.

3 **3. Identifier la configuration réellement active**
Exécutez sudo nginx -T pour retrouver le bloc server chargé, le server_name, la directive root et les règles incluses.

4 **4. Vérifier le chemin complet vers la ressource**
Contrôlez les droits du fichier demandé et de tous ses répertoires parents. Avec namei -l /chemin/vers/le/fichier, vérifiez que le processus Nginx peut traverser chaque dossier.

5 **5. Tester avant de recharger**
Après toute modification, lancez sudo nginx -t. Rechargez Nginx uniquement si le test de configuration est valide.

Contrôles système de fichiers

- [ ] **Identifier l'utilisateur exécutant Nginx**
  Vérifiez la directive user dans /etc/nginx/nginx.conf ; le compte dépend de la distribution.
- [ ] **Vérifier la lisibilité des fichiers publiés**
  Des droits 644 sont courants pour des fichiers publics, selon le propriétaire et le groupe.
- [ ] **Vérifier la traversée des répertoires parents**
  Des droits 755 sont courants pour les dossiers publics ; le droit d'exécution est nécessaire pour traverser un répertoire.
- [ ] **Contrôler propriétaire et groupe**
  Nginx n'a pas nécessairement besoin de posséder tous les fichiers : adaptez le modèle aux besoins du déploiement.
- [ ] **Examiner SELinux si les droits semblent corrects**
  Une politique système peut refuser l'accès malgré des permissions Linux apparemment valides.

Message observé : piste de correction

Indice dans le diagnostic	Contrôle prioritaire
permission denied	Permissions, propriétaire, groupe, traversée des répertoires parents et SELinux
directory index is forbidden	Présence du fichier d'index, directive index et comportement attendu pour le listing
access forbidden by rule	Directives allow, deny, auth_basic et règles héritées dans http, server ou location
403 avec une signature de CDN ou WAF	Règles de filtrage externes, blocage IP, CDN et pare-feu applicatif
Chemin servi inattendu	Directives root, alias et règles try_files du bloc concerné

Relecture de la configuration Nginx

- [ ] **Confirmer que root vise le répertoire réellement publié**
  Le chemin doit correspondre à l'emplacement des fichiers accessibles.
- [ ] **Vérifier la directive index**
  Elle doit contenir le fichier d'accueil attendu, par exemple index.html ou l'index utilisé par l'application.

Relire try_files
Cette directive peut orienter une requête vers un dossier ou une ressource sans index.

Rechercher les règles allow et deny
Contrôlez les niveaux http, server et location, car certaines règles peuvent être héritées.

Vérifier les protections d'authentification
Une directive auth_basic ou une politique applicative peut produire un refus d'accès.

> ! **À ne pas faire**
> Ne corrigez pas un 403 en appliquant chmod 777 à la racine web. Cette action élargit inutilement les droits et ne résout pas une directive deny, un index absent, un mauvais root, un WAF ou une politique SELinux.

Avant un rechargement, validez toujours la configuration avec nginx -t. Adaptez propriétaire, groupe et permissions au compte de service Nginx et à votre méthode de déploiement.