

ANCORIA

by Ancoris Solutions

SOUVERAINETÉ NUMÉRIQUE · GUIDE N° 05

Comprendre, essayer et décider

NixOS dans l'administration

Le socle Linux que la DINUM a choisi pour ses propres postes,
expliqué à ceux qui doivent rendre un plan à l'automne.

250

POSTES · LE PÉRIMÈTRE RÉEL ANNONCÉ
PAR LA DINUM

20 000

OPTIONS DÉCLARATIVES RECHERCHABLES
EN LIGNE

v0.19

SÉCURIX AU 31/08/2026 · TOUJOURS EN
ALPHA

OUVERTURE

À qui s'adresse ce guide

Aux DSI, RSSI et chargés de projet numérique d'une administration d'État ou d'une collectivité, qui doivent se prononcer sur l'avenir de leur poste de travail — et qui n'ont ni le temps ni l'envie de devenir experts d'un paradigme nouveau pour y arriver.

Le 8 avril 2026, un séminaire interministériel réuni par la DINUM avec l'ANSSI, la DAE et la DGE a posé une obligation nette : chaque ministère, opérateurs inclus, devra formaliser son plan de réduction des dépendances extra-européennes sur sept domaines, dont le poste de travail, d'ici l'automne 2026. Le texte n'impose aucune distribution — mais le seul socle de poste que l'État ait publié en open source est bâti sur NixOS.



Le communiqué du 8 avril 2026 sur numerique.gouv.fr. Il demande un **plan**, sur sept domaines — pas une distribution.

Chapitre	Ce que vous saurez faire	Temps
1. Pourquoi celle-là	Défendre le choix de la distribution, chiffres à l'appui	10 min
2. Le modèle déclaratif	Expliquer ce que NixOS change, sans jargon	10 min
3. Essayer	Faire tourner NixOS en machine virtuelle	30 min
4. La configuration	Lire et modifier <code>configuration.nix</code>	20 min
5. Le quotidien	Reconstruire, revenir en arrière, tester un logiciel	15 min
6. Sécurix	Lire une règle ANSSI écrite en code	15 min
7. Décider	Instruire le choix, et savoir quand renoncer	—

CE QUE CE GUIDE FAIT, ET CE QU'IL NE FAIT PAS

- **Il ne vous vend pas NixOS.** Le chapitre 7 donne autant d'arguments de renoncement que d'adoption.
- **Il vous fait manipuler.** Toutes les commandes sont celles du manuel officiel et se testent en machine virtuelle.
- **Il écarte deux chiffres très répandus** qui n'existent dans aucune source primaire — et vous dira lesquels.

CHAPITRE 1

Pourquoi celle-là, et pas une autre

Toutes les distributions GNU/Linux installent les mêmes logiciels libres. Ce qui les sépare n'est pas leur contenu, c'est la façon dont un parc tient dans le temps. Sur Debian, Ubuntu ou Red Hat, on standardise un parc avec un outil posé par-dessus — Ansible, Puppet, une image de référence. Sur NixOS, il n'y a pas d'outil par-dessus : la description du poste est le système. C'est la seule distribution répandue où la standardisation n'est pas une couche ajoutée, mais la propriété de base.

D'où l'intérêt annoncé à grande échelle : dix mille postes décrits par le même fichier sont dix mille postes identiques, et un correctif se pousse en modifiant une ligne. L'argument est solide — **et il doit être tenu avec prudence**. Personne n'exploite aujourd'hui NixOS sur des milliers de postes bureautiques ; la DINUM en a 40 en service. Pour piloter des parcs de cette taille, Ansible et Puppet ont vingt ans de terrain que l'écosystème Nix n'a pas encore.

Le second argument est celui de la dépendance à un éditeur

Distribution	Qui est derrière	Où	Modèle
NixOS	Stichting NixOS Foundation	Utrecht, Pays-Bas	Fondation sans but lucratif, sans capital
Ubuntu	Canonical Ltd	Londres, Royaume-Uni	Société commerciale, abonnements
RHEL	Red Hat, filiale d'IBM	Raleigh, États-Unis	Société commerciale, abonnements
SUSE	SUSE S.A.	Luxembourg / Nuremberg	Société commerciale, abonnements
Debian	Projet communautaire	—	Aucun éditeur

L'IDÉE REÇUE À CORRIGER AVANT DE L'ÉCRIRE DANS UNE NOTE

Ubuntu n'est pas américain : Canonical est une société britannique, hors Union européenne depuis le Brexit, mais pas américaine — et c'est sur Ubuntu que tourne le plus gros parc Linux de l'État français, les 103 164 postes de la Gendarmerie. SUSE, éditeur européen, existe aussi.

Ce qui distingue NixOS n'est donc pas d'être « moins américain » que les autres. C'est de **n'avoir aucun éditeur du tout** : personne avec qui négocier, aucun abonnement, aucun rachat possible. Le même fait supprime la dépendance et le support — voir le chapitre 6.

CHAPITRE 2

Ce que « déclaratif » change vraiment

Définition. NixOS est une distribution GNU/Linux dont la configuration complète — paquets installés, services actifs, comptes, réglages de sécurité — est décrite dans un fichier texte versionné, à partir duquel le système se reconstruit à l'identique sur n'importe quelle machine.

La différence avec un parc classique n'est pas cosmétique. Sur un poste ordinaire, l'état réel de la machine résulte de la sédimentation de centaines d'installations, de mises à jour et de correctifs manuels. Personne ne peut le décrire exactement. Ici, le fichier est la description.

Question	Parc classique	NixOS
Qu'y a-t-il sur ce poste ?	On inventorie, et on découvre des écarts	On lit le fichier de configuration
Deux postes sont-ils identiques ?	Rarement, et rien ne le signale	Oui si le fichier est le même
Une mise à jour casse tout	Restauration d'image, ou réparation à la main	Redémarrage sur la génération précédente
Prouver une règle de sécurité	Audit et entretien	Lecture du code, puis exécution d'un contrôle
Rejouer la config sur un poste neuf	Procédure documentée, appliquée par un humain	Même fichier, même résultat

L'IDÉE À RETENIR AVANT TOUTE DÉMONSTRATION

Le gain n'est pas « Linux au lieu de Windows », c'est « une description exécutable au lieu d'un état constaté ». Une administration qui n'a jamais su répondre à « que contient ce poste ? » gagne d'abord une réponse, avant de gagner des licences.

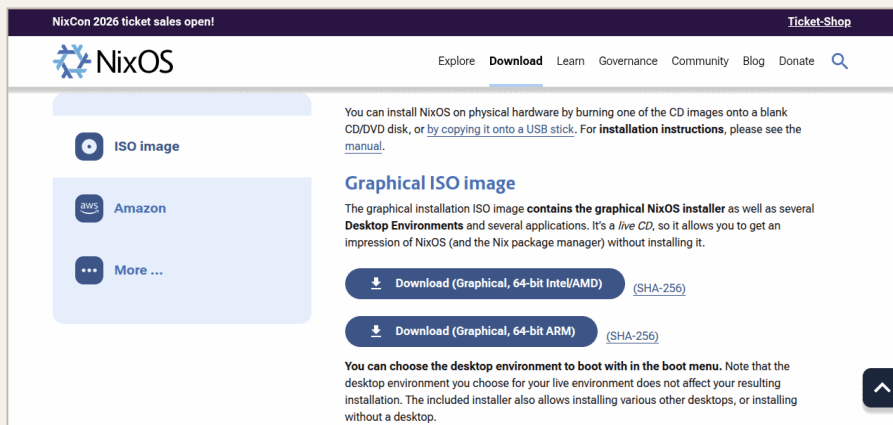
Et ce que le modèle ne résout pas

Il ne rend pas les applications métier compatibles : un logiciel qui n'existe que sous Windows n'existe toujours pas. Il ne remplace ni SELinux ni AppArmor, qui restent à activer et à écrire. Il ne supprime pas le besoin d'annuaire, il le déplace vers un dépôt Git. Et il coûte cher en apprentissage : le langage Nix déroute des administrateurs Linux expérimentés, parce que la difficulté n'est pas la syntaxe mais le renversement — on décrit un état voulu au lieu d'enchaîner des actions.

CHAPITRE 3

Essayer sans rien casser, en 30 minutes

La bonne première étape n'est pas d'installer NixOS sur un poste, mais de le faire tourner dans une machine virtuelle. L'image ISO est publiée sur le site officiel, en version graphique ou minimale.



nixos.org/download — l'ISO graphique installe un bureau complet ; l'ISO minimale suffit pour découvrir la configuration en ligne de commande.

Le chemin le plus court, dans VirtualBox ou GNOME Boxes :

1. Télécharger l'ISO graphique sur nixos.org/download.
2. Créer une VM de 4 Go de RAM et 30 Go de disque, démarrer dessus.
3. Lancer l'installateur graphique : il pose les mêmes questions que n'importe quelle distribution.
4. Redémarrer, puis ouvrir `/etc/nixos/configuration.nix`.

CONSEIL · CE QU'IL FAUT REGARDER EN PREMIER

Au redémarrage, ouvrez le menu de démarrage. Le manuel NixOS l'appelle une liste de *configurations disponibles* : chaque modification du système y ajoute une entrée. C'est la propriété la plus vendeuse auprès d'un exploitant, et elle se montre en dix secondes — bien avant tout discours sur la souveraineté.

Les six vérifications qui décident vraiment

Une VM ne dit rien du matériel ni du réseau. Ce qui se teste utilement, dans l'ordre de ce qui bloque le plus souvent :

- **Impression** — le pilote du parc d'imprimantes existe-t-il ?
- **Carte à puce et FIDO2** — lecteur reconnu, agent fonctionnel ?
- **VPN de l'administration** — client compatible, ou seulement Windows ?
- **Bureautique** — les modèles de documents survivent-ils à LibreOffice ?
- **Applications métier web** — quel navigateur est exigé, et pour quelle version ?
- **Visioconférence** — caméra, micro et partage d'écran, dans l'outil réellement utilisé.

CHAPITRE 4

Lire et modifier la configuration

Tout tient dans `/etc/nixos/configuration.nix`. Le fichier se lit sans connaître le langage Nix : ce sont des options nommées auxquelles on donne une valeur.

```
# /etc/nixos/configuration.nix – extrait commenté

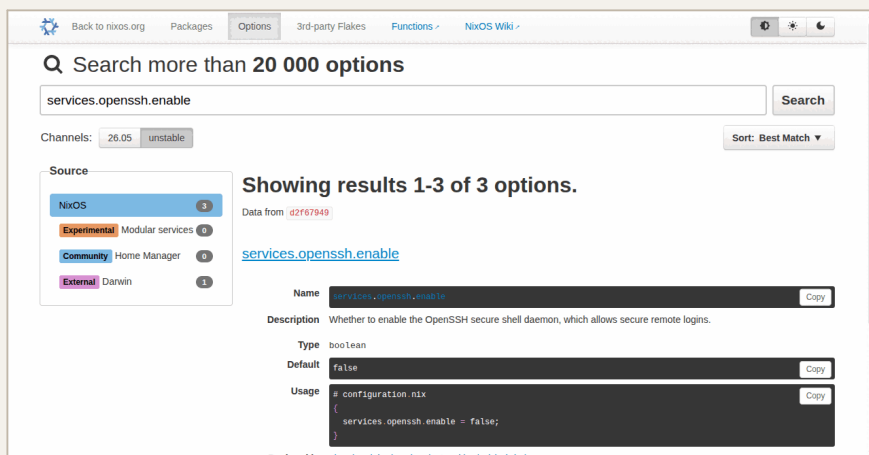
{ config, pkgs, ... }:
{
  # Nom de la machine sur le réseau
  networking.hostName = "poste-dsi-01";

  # Fuseau et clavier
  time.timeZone = "Europe/Paris";
  console.keyMap = "fr";

  # Un service : l'accès SSH, coupé par défaut
  services.openssh.enable = true;

  # Les logiciels installés pour tout le monde
  environment.systemPackages = with pkgs; [ firefox libreoffice ];
}
```

Chaque option est documentée et cherchable en ligne, avec son type, sa valeur par défaut et un exemple d'usage : plus de 20 000 options y sont indexées.



search.nixos.org/options — chaque option affiche sa description, son type, sa valeur par défaut et l'extrait de `configuration.nix` à recopier.

Le fichier se met sous Git comme n'importe quel code : l'historique du poste devient lisible, chaque changement a un auteur et une date, et une revue par un pair devient possible avant application.

CHAPITRE 5

Les trois gestes du quotidien

Modifier le fichier ne change rien tant qu'on n'a pas reconstruit le système. Trois commandes couvrent l'essentiel de l'exploitation, et elles se distinguent par ce qu'elles rendent permanent.

Commande	Ce qu'elle fait	Quand s'en servir
<code>nixos-rebuild switch</code>	Construit, applique tout de suite, et devient la configuration de démarrage	Changement validé
<code>nixos-rebuild test</code>	Applique sans devenir la configuration de démarrage	Essai réversible par simple redémarrage
<code>nixos-rebuild boot</code>	Devient la configuration de démarrage sans basculer maintenant	Changement à appliquer à la prochaine fenêtre
<code>nixos-rebuild build</code>	Construit seulement, ne touche pas au système	Vérifier que tout compile

Le shell jetable est l'autre geste à connaître. Il donne accès à un logiciel sans l'installer sur la machine : à la sortie du shell, il n'est plus là. C'est la réponse propre à « j'ai besoin de cet outil une fois ».

```
$ nix-shell -p cowsay lolcat

[nix-shell:~]$ exit
exit

$ cowsay no more
The program 'cowsay' is currently not installed.
```

POINTS CLÉS · CE QU'IL FAUT SAVOIR FAIRE

- Éditer `/etc/nixos/configuration.nix` et appliquer avec `nixos-rebuild switch`.
- Revenir en arrière en redémarrant sur la génération précédente.
- Chercher une option sur search.nixos.org/options plutôt que de deviner son nom.
- Essayer un logiciel avec `nix-shell -p` sans salir le poste.

Le revers : les générations occupent le disque

Chaque génération conservée garde ses paquets. Sur un poste très modifié, le disque se remplit. Le ménage est explicite, et c'est voulu : rien n'est supprimé dans votre dos.

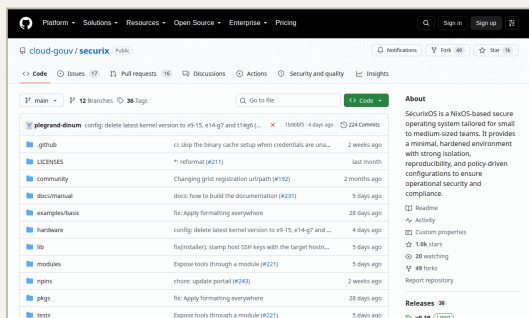
```
# Supprimer les générations anciennes et libérer le disque
$ sudo nix-collect-garbage -d

# Vérifier la version du système
$ nixos-version
```

CHAPITRE 6

Sécurix, le socle publié par l'État

La DINUM a publié son socle de poste durci sous licence MIT. C'est un dépôt vivant : au 31 août 2026, 224 commits, 36 versions publiées et environ un millier d'étoiles, pour une version v0.19.



github.com/cloud-gouv/secuirix — les répertoires `modules`, `lib` et `tests` portent les règles ANSSI et leurs contrôles.

L'idée transposable tient en une phrase : **chaque règle de durcissement ANSSI devient un module de code**, avec ses métadonnées (sévérité, catégorie), la configuration qui l'applique, et un script qui vérifie à l'exécution qu'elle l'est réellement. Et le README de ce module précise qu'il **peut être copié-collé hors de Sécurix pour vos propres besoins** : le travail de conformité se reprend sans adopter le socle entier.

`modules/anSSI/kernel-options.nix` — extrait réel, licence MIT

```
R8 = {
  anssiRef    = "R8 – Paramétrer les options de configuration mémoire";
  severity    = "intermediary";
  category    = "base";

  config = _: {
    # ce que la règle applique
    boot.kernelParams = [
      "l1tf=full,force" # L1 Terminal Fault, SMT désactivé
      "pti=on"          # Page Table Isolation, contre Meltdown
      "mds=full,nosmt"  # atténuation MDS complète
      # ... 8 autres paramètres
    ];
  };

  checkScript = pkgs: ... # ce qui vérifie qu'elle l'est
};
```

CE QUE LE DÉPÔT AVERTIT, ET QUE LES REPRISES TAISENT

- « Alpha, aucun support n'est proposé pour l'heure » — c'est écrit dans le README, ce n'est pas une précaution de style.
- Couverture partielle** : une dizaine de règles du guide ANSSI réellement codées sur une centaine.
- Pas de contrôle d'accès obligatoire** : Sécurix documente les règles ANSSI R37 et R45 à R49 comme non applicables. AppArmor existe pourtant dans NixOS (`security.apparmor.enable`, désactivé par défaut) — c'est un choix du socle, pas une limite de la distribution.
- Les contrôles ne tournent pas en intégration continue** : la preuve d'audit reste à construire.

CHAPITRE 7

Décider dans votre contexte

Le calendrier est le même pour tout le monde. Le support de Windows 10 a cessé le 14 octobre 2025, et 60 à 70 % des postes administratifs français fonctionnaient encore sous cette version. Pour une commune de 15 000 habitants, le renouvellement anticipé de 400 postes représente un budget de 300 000 à 400 000 euros.

	Sécurix / NixOS (DINUM)	GendBuntu / Ubuntu (Gendarmerie)
Parc déployé	~250 postes visés, 40 en service	~100 000 postes, la quasi-totalité du parc
Ancienneté	Alpha, v0.19	Lancé en 2008, 17 ans de recul
Gestion du parc	Déclaratif, dépôt Git, pas d'annuaire	Parc classique, outillage éprouvé
Économies	Non établies	Annoncées, jamais publiées par la Gendarmerie
Compétences	Rares, paradigme spécifique	Administration Linux courante

DEUX CHIFFRES À NE PAS PORTER DANS VOTRE NOTE

- « 2,5 millions de postes d'ici 2030 » — n'apparaît dans aucun texte officiel. Il circule de blog en blog.
- Les économies chiffrées de la Gendarmerie — « 500 M€ sur vingt ans », « 50 M€ depuis 2004 », « -40 % de TCO » : aucune n'est publiée par la Gendarmerie, et elles se contredisent entre elles. Le fait solide est le parc, pas le coût évité.

Les six questions à trancher avant d'inscrire NixOS dans un plan :

- Quelles applications métier n'existent que sous Windows ? C'est cet inventaire, pas la distribution, qui fixe le périmètre migrable.
- Qui forme les équipes, et sur quel budget ?
- Qui répond à 3 h du matin, sans contrat de support ?
- Le parc matériel supporte-t-il FIDO2 et TPM2 ?
- Qui maintient le fork une fois la DINUM partie sur autre chose ?
- Comment prouve-t-on la conformité tant que les contrôles ne tournent pas en CI ?

CONSEIL · LE SCÉNARIO RÉALISTE POUR UNE COLLECTIVITÉ

Ne pas migrer le parc. Prendre **un** usage homogène et sans application métier Windows — un poste de médiathèque, une salle de formation, un parc de bornes — et le décrire en code. On y gagne l'expérience du modèle déclaratif, un chiffrage réel du coût de montée en compétence, et un argument mesuré pour la suite. Sans risquer l'état civil un lundi matin.

POUR ALLER PLUS LOIN

Sources et documentation

Toutes les affirmations chiffrées de ce guide viennent des pages ci-dessous, relevées le 31 août 2026. Les commandes sont celles du manuel officiel.

Ce que vous y trouvez	Adresse
La décision du 8 avril 2026, dans son texte	numerique.gouv.fr — espace presse, souveraineté numérique
Manuel NixOS : installation et reconstruction	nixos.org/manual/nixos/stable
Les 20 000 options, avec exemples	search.nixos.org/options
Premiers pas guidés, shells jetables	nix.dev/tutorials/first-steps
Le socle de l'État, code et README	github.com/cloud-gouv/securix
Le poste bureautique qui en dérive	github.com/cloud-gouv/bureautix-exemple
Logiciels libres métiers utilisés par les collectivités	comptoir-du-libre.org (Adullact)
Entraide francophone	discourse.nixos.org — catégorie « Apprendre en Français »
Parc GendBuntu : un ordre de grandeur, sans source primaire	Presse spécialisée ; la Gendarmerie ne publie pas ce chiffre

Les huit mots que vous entendrez

Terme	Ce que ça veut dire
Nix	Le gestionnaire de paquets et le langage. NixOS est la distribution bâtie dessus.
nixpkgs	Le dépôt collectif de tous les paquets et de toutes les options.
Génération	Un état complet du système, conservé et redémarrable.
Canal	La série de versions suivie — par exemple 26.05, ou unstable.
Dérivation	La recette de construction d'un paquet, entrées comprises.
Flake	Un format qui fige les versions des dépendances d'une configuration.
Home Manager	L'extension qui applique le même principe au profil d'un utilisateur.
Sécurix / Bureautix	Les deux socles de la DINUM : poste d'administration, puis bureautique.

LA PHRASE À EMPORTER

Ce qui mérite d'être copié n'est pas la distribution, c'est la décision d'écrire une politique de sécurité sous une forme exécutable et vérifiable. Cette méthode ne demande ni budget de migration ni changement de système d'exploitation pour commencer — elle demande d'accepter que la conformité se prouve en s'exécutant, pas en se déclarant.