

# Nextcloud

## Plateforme collaborative auto-hébergée

Présentation, fonctionnalités techniques et provisionnement

Association LinuXMaine    Thierry GAYET  
Thierry.Gayet@gmail.com

Association LinuXMaine

2026



Nextcloud

# Plan I

- 1 Présentation générale
- 2 Architecture technique
- 3 Fonctionnalités & usages
- 4 Plugins d'usage en détail
- 5 Accès sécurisé à Nextcloud
- 6 Sécurité & conformité
- 7 Intégration Yubikey & 2FA matérielle
- 8 Connexion à Keycloak (SSO)
- 9 Coffres-forts numériques & Nextcloud
- 10 Installation manuelle (prérequis)
- 11 Provisionnement avec Ansible
- 12 Provisionnement avec OpenTofu
- 13 Exploitation & maintenance
- 14 Lexique
- 15 Liens de référence
- 16 Références bibliographiques

# Plan II

## 17 Conclusion

# Qu'est-ce que Nextcloud ?

- Plateforme **libre** de partage et de collaboration **auto-hébergée**
- **Fork de ownCloud** créé en 2016 par **Frank Karlitschek** (fondateur d'ownCloud)
- Écrit en **PHP** (8.x), avec une base de données relationnelle (MariaDB/MySQL/PostgreSQL/SQLite)
- **Alternative souveraine** aux services SaaS (Google Drive, Dropbox, Microsoft 365)
- Licence **AGPLv3** : code source ouvert, copyleft fort
- Déployé par +400 000 organisations : universités, ministères, hôpitaux, ONG
- Sigle communautaire : *Hub* car Nextcloud agrège fichiers, agenda, contacts, visio, mail, bureautique. . .

## Philosophie

*Reprendre le contrôle de ses données* : tout reste sur votre infrastructure (serveur privé, VPS, cloud souverain).

# Historique du projet

- **2010** : Naissance d'**ownCloud**, projet initial de Frank Karlitschek
- **Juin 2016** : **Fork de Nextcloud** après départ de plusieurs développeurs clés
- **2017** : Nextcloud Talk (visioconférence WebRTC intégrée)
- **2018** : Nextcloud Hub — agrégation Files + Talk + Groupware
- **2020** : Partenariat avec **IONOS** et l'État allemand pour la *Bundescloud*
- **2022** : Hub 3 — intégration de **Collabora Online** et **OnlyOffice**
- **2023** : Hub 5 — assistant IA (Ethical AI Rating), *Files Sync v3*
- **2024** : Hub 8 — assistant local (LocalAI, Llama), *Files End-to-End Encryption*
- **2025** : Hub 9 — nouveau *Files* (PWA), *Tables* renforcé, *Cospend*
- **2026** : Hub 10 (en cours) — IA souveraine, *Federation 2.0*, perfs PHP 8.4

# Rôle de Nextcloud

## Rôle fonctionnel : un *Hub* unifié de productivité

Nextcloud joue le rôle de **point d'entrée unique** pour toutes les données et les communications d'une organisation : fichiers, agendas, contacts, mails, visio, bureautique et tableaux collaboratifs sous une seule identité, une seule URL, un seul socle de droits.

## Rôle technique

- **Plateforme d'agrégation** : Files + Talk + Groupware + Office sur un même serveur PHP
- **Couche d'accès unifiée** aux stockages hétérogènes (S3, NFS, SMB, FTP...)
- **Passerelle fédérée** entre instances autonomes
- **Hub d'authentification** (LDAP, SAML, OIDC, 2FA)

## Rôle stratégique

- **Souveraineté numérique** : alternative crédible à Google Workspace / Microsoft 365
- **Conformité RGPD / HDS** sur infrastructure maîtrisée
- **Réduction du *vendor lock-in*** : code AGPLv3, données portables (WebDAV, CalDAV, CardDAV)
- **Outil de cohésion** pour les associations, collectivités et PME

# Écosystème & gouvernance

## Éditeur

- **Nextcloud GmbH** — Stuttgart (Allemagne)
- Modèle : open source + souscriptions entreprise
- Engagement *No Vendor Lock-in*

## Communauté

- +2 500 contributeurs sur GitHub
- +250 applications dans l'AppStore
- Forum, Matrix, conférence annuelle

## Adoption institutionnelle

- **France** : Ministère de l'Éducation (*Apps.education*), Gendarmerie
- **Allemagne** : Bundescloud (administration fédérale)
- **Pays-Bas** : SURF (universités)
- **Suisse** : EPFL, plusieurs cantons
- **Santé** : nombreux CHU (HDS-compatible)

## Souveraineté numérique

Nextcloud est cité par l'ANSSI et le Bundes-CIO comme brique de la *souveraineté numérique européenne*.

# Stack logicielle

## Couche serveur

- **PHP 8.1+** (recommandé 8.3 / 8.4)
- **Apache 2.4** ou **Nginx** + PHP-FPM
- **Base de données** : MariaDB 10.6+, MySQL 8, PostgreSQL 14+, SQLite (dev)
- **Cache** : Redis (sessions, file locking)
- **APCu** : cache mémoire local PHP

## Couche cliente

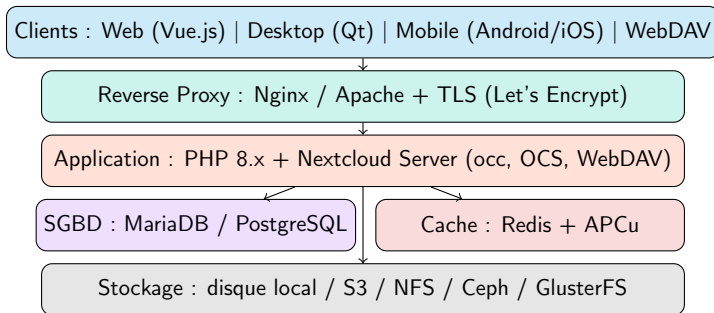
- **Web** : Vue.js 3 + interface responsive PWA
- **Desktop** : Qt6 (Linux, Windows, macOS)
- **Mobile** : Android (Kotlin), iOS (Swift)
- **CLI** : occ (commande de gestion)
- **API** : OCS REST + WebDAV

## Composants optionnels

**Collabora Online** (CODE) ou **OnlyOffice** pour la bureautique en ligne, **High Performance Backend** (HPB, Node.js) pour Talk, **Push Server** pour les notifications mobiles, **ClamAV** pour l'antivirus.



# Architecture en couches



# Stockage des données

- **Données utilisateurs** : arborescence `data/<user>/files/` (par défaut)
- **Backends supportés** : Local, **S3** (objet primaire), **Swift**, **Ceph**, **NFS**, **SMB/CIFS**, **FTP/SFTP**, **WebDAV**, **Google Drive** (External Storage)
- **Chiffrement** : module *Server-Side Encryption* (E2EE côté client pour les dossiers sensibles)
- **Versioning** : conservation automatique des versions de fichiers
- **Corbeille** : suppression différée, configurable par durée
- **Quotas** : par utilisateur, par groupe
- **Déduplication** : possible via le backend (ZFS, S3 versioning)

## Patterns de déploiement

Petits sites : disque local + MariaDB. Production : **S3 primary storage** + PostgreSQL + Redis Sentinel + HPB pour la montée en charge.

# API et intégrations

## API exposées

- **WebDAV** : accès fichier standard (RFC 4918)
- **OCS REST** : utilisateurs, groupes, partages
- **CardDAV** : contacts (RFC 6352)
- **CalDAV** : agendas (RFC 4791)
- **ActivityPub** : fédération sociale
- **Federation API** : partages entre instances

## Authentication

- Locale (LDAP-compatible)
- **LDAP / Active Directory**
- **SAML 2.0** (SSO entreprise)
- **OpenID Connect / OAuth2**
- **Kerberos / SPNEGO**
- **2FA** : TOTP, U2F/WebAuthn, matériel

# Nextcloud Files — Gestion documentaire

- **Synchronisation** multi-poste (clients desktop + mobiles), basée delta
- **Partage** : lien public, mot de passe, expiration, droits granulaires
- **Partage fédéré** entre instances Nextcloud (Federated Cloud Sharing)
- **Tags**, commentaires, activités, *favorites*
- **Workflow Engine** : règles automatisées (filigrane, blocage, anti-virus)
- **Files Lock** : verrouillage collaboratif (RFC compatible WOPI)
- **End-to-End Encryption** côté client pour les dossiers sensibles
- **Photos** : galerie avec reconnaissance faciale (*Memories, Recognize*)

# Nextcloud Talk — Visioconférence

- **WebRTC** natif — chiffrement *end-to-end* de la signalisation
- Conversations **1-1**, **groupe**, **public** (invités externes)
- **Partage d'écran**, **enregistrement** côté serveur
- **Sous-titres en direct** via STT (Whisper local)
- **Tableau blanc** collaboratif (Whiteboard)
- **Lobby**, salles d'attente, modération
- **Bots** : webhooks, intégration Matrix
- **HPB** (High Performance Backend, Node.js) requis  $\geq 5$  participants

## Souveraineté

Alternative directe à Zoom / Teams pour l'administration et l'éducation ; ne nécessite aucun service externe.

# Nextcloud Groupware — Mail / Calendar / Contacts

## Mail

- Webmail multi-comptes IMAP/SMTP
- Filtres Sieve, signatures, *thread view*
- Chiffrement OpenPGP (Mailvelope)

## Calendar

- CalDAV, invitations iMIP, ressources
- Planification disponibilité (Appointments)
- Synchro Thunderbird, iOS, Android

## Contacts

- CardDAV, carnets partagés
- Import/export vCard
- Cercles & équipes

## Deck

- Tableaux Kanban (à la Trello)
- Cartes, tags, échéances
- Intégration Talk & Files

# Bureautique en ligne

- **Nextcloud Office** (Collabora Online / CODE) : LibreOffice en ligne via WOPI
- Formats natifs : ODT, ODS, ODP — support DOCX, XLSX, PPTX
- **OnlyOffice Document Server** : alternative compatible MS Office
- **Édition collaborative** temps réel multi-curseur
- **Text** : éditeur Markdown collaboratif intégré
- **Notes** : prise de notes Markdown synchronisée
- **Tables** : feuilles de calcul collaboratives style *AirTable*
- **Forms** : formulaires en ligne (alternative à Google Forms)

# Applications additionnelles (AppStore)

## Productivité

- *Deck* (Kanban), *Tasks* (todo)
- *Notes*, *Polls*, *Forms*
- *Cospend* (gestion partagée de dépenses)
- *Bookmarks*, *News* (RSS)

## Sécurité & admin

- *Passwords*, *Passman*
- *Two-Factor* (TOTP, U2F, Email)
- *Suspicious Login*, *Brute-force Settings*

## Multimédia

- *Photos*, *Memories*, *Recognize* (IA locale)
- *Music*, *Audio Player*
- *Maps*, *Phonetrack*

## Intégrations

- *GitHub*, *GitLab*, *Mattermost*
- *LDAP/AD*, *SAML SSO*
- *Assistant* (LLM local : Llama, Mistral)



# Cas d'usage typiques

## Particuliers & associations

- Dropbox auto-hébergé
- Synchro multi-poste (PC, mobiles)
- Partage familial photos / vidéos
- Carnet d'adresses + agenda CalDAV

## TPE / PME

- GED collaborative
- Visio interne (Talk)
- Office 365 souverain (Collabora)

## Grandes organisations

- Plateforme *file sharing* fédérée
- Intégration AD / SAML
- Workflow Engine (*watermark*, DLP)
- HDS (santé), RGPD-compliant

## Éducation & recherche

- Apps.education (1.5M comptes)
- Kit pédagogique : Talk + Office + Forms

# Plugins d'usage — Productivité & collaboration

## Bureautique & édition

- **Nextcloud Office** (Collabora CODE) : LibreOffice en ligne, multi-curseur, ODT/DOCX/ODS/XLSX
- **OnlyOffice Document Server** : alternative compatible MS Office (*Track Changes*)
- **Text** : éditeur Markdown live, mentions @user
- **Notes** : prise de notes Markdown synchronisée avec l'app mobile

## Gestion de projet

- **Deck** : Kanban (à la Trello), intégration Talk/Files
- **Tasks** : todo CalDAV (RFC 5545 VTOD), compatible Thunderbird
- **Tables** : feuilles collaboratives style *AirTable*, 8 types de colonnes
- **Forms** : formulaires (alternative à Google Forms), export CSV
- **Polls** : sondages d'équipe (date + texte)

# Plugins d'usage — Communication & multimédia

## Communication

- **Talk** : visio WebRTC, salons, lobby, sous-titres en direct
- **Mail** : webmail multi-comptes IMAP/SMTP, filtres Sieve
- **Calendar** : CalDAV, *Appointments* (créneaux publics)
- **Contacts** : CardDAV, carnets partagés, cercles
- **Whiteboard** : tableau blanc collaboratif (Excalidraw-like)

## Multimédia & IA

- **Photos** : galerie, albums partagés, EXIF, géolocalisation
- **Memories** : timeline, *Faces*, *Places*
- **Recognize** : IA locale (TensorFlow), tags automatiques
- **Music** : streaming Subsonic-compatible
- **Maps** : OSM, traces GPX, *Phonetrack*
- **Assistant** (Hub 8+) : LLM local (Llama, Mistral), STT (Whisper)

# Plugins d'usage — Sécurité & administration

## Sécurité côté utilisateur

- **Passwords** : coffre-fort de mots de passe, partage, dossiers
- **End-to-End Encryption** : E2EE par dossier, clés privées client
- **Two-Factor TOTP** : code à 6 chiffres (Google Authenticator, FreeOTP)
- **Two-Factor WebAuthn** : Yubikey, Solokey, Titan, Touch ID
- **Two-Factor Email / SMS / Notification**

## Admin & gouvernance

- **User\_LDAP / SAML / OIDC** : fédération d'identité
- **Suspicious Login** : détection ML des connexions anormales
- **Brute-force Settings** : rate limit IP/utilisateur
- **Audit Log** : journal détaillé (qui, quoi, quand, depuis où)
- **Data Loss Prevention** : Workflow Engine + Files Access Control
- **Backup** : snapshot de l'instance complète

# Comment fonctionnent les plugins (apps) ?

## Format d'une app

- Code **PHP** (+ Vue.js côté UI), arborescence figgée
- Manifeste appinfo/info.xml (id, version, dépendances)
- Routage : appinfo/routes.php ou Routes.php
- Migrations BD : dossier lib/Migration/
- Permissions et rôles déclarés dans info.xml

## Sources

- **AppStore officiel** : apps.nextcloud.com (signature *Nextcloud GmbH*)
- **Dépôt manuel** : extraction de l'archive dans apps-extra/
- **Développement** : générateur nextcloud/app-skeleton
- +250 apps publiques, +50 apps Enterprise
- Ratings : *Featured, Stable, Beta, Alpha*

## Sécurité

Chaque app publiée sur l'AppStore est **signée** par son auteur et vérifiée par Nextcloud GmbH. Les administrateurs peuvent restreindre les apps autorisées via *App Bundles*.

# Installer et gérer les plugins

## Via l'interface web

- ❶ Connexion en tant qu'admin
- ❷ Menu *Apps* (icone en haut à droite)
- ❸ Catégories : *Featured, Files, Auth, Office...*
- ❹ Bouton *Activer / Désactiver / Désinstaller*
- ❺ Mises à jour : pastille rouge sur l'icône

## App Bundles prédéfinis

- *Hub Bundle, Education, Groupware*
- *Enterprise, Public Sector*

## Via la CLI occ

```
# Lister les apps installées
sudo -u www-data php occ app:list

# Installer une app
sudo -u www-data php occ app:install spread # Talk
sudo -u www-data php occ app:install deck

# Activer / Désactiver
sudo -u www-data php occ app:enable mail
sudo -u www-data php occ app:disable photos

# Mettre à jour toutes les apps
sudo -u www-data php occ app:update --all

# Désinstaller
sudo -u www-data php occ app:remove news

# Restreindre une app à un groupe
sudo -u www-data php occ app:enable \
  --groups admin --groups gestion deck
```

# Accès depuis un poste Linux

## Client officiel Nextcloud Desktop

- Application Qt 6 multi-distrib (ApplImage, Flatpak, paquets natifs)
- Synchronisation sélective (*Virtual Files* sous Linux : kernel 5.x + libfuse3)
- **TLS strict** : vérification certificat (refuse TLS < 1.2)
- **App Password** dédié par poste (révocable, distinct du mot de passe principal)
- Compatible 2FA via *App Passwords*

## Intégration système de fichiers

- **GNOME Files / Nautilus** : protocole `davs://` natif via GVFS
- **KDE Dolphin** : KIO Worker WebDAV
- **davfs2** : montage POSIX (`/etc/fstab`)
- **rclone** : sync scriptable, chiffrement côté client

# Accès Linux — exemples de commandes

```
# 1. Installation du client desktop officiel (Flatpak recommande)
flatpak install flathub com.nextcloud.desktopclient.nextcloud
flatpak run com.nextcloud.desktopclient.nextcloud # assistant graphique

# 2. Montage WebDAV via davfs2 (paquet : davfs2)
sudo apt install davfs2
echo "https://nextcloud.linuxmaine.fr/remote.php/dav/files/USER/  USER  APPPASS" \
| sudo tee -a /etc/davfs2/secrets
sudo chmod 600 /etc/davfs2/secrets
sudo mkdir /mnt/nc
sudo mount -t davfs https://nextcloud.linuxmaine.fr/remote.php/dav/files/USER/ /mnt/nc

# 3. rclone : configuration interactive
rclone config # type=webdav, vendor=nextcloud, user=USER, pass=APPPASS
rclone copy ~/Documents nc:Backup --progress --transfers=4

# 4. Accès ad-hoc via GVFS (GNOME)
gio mount davs://nextcloud.linuxmaine.fr/remote.php/dav/files/USER/
ls "/run/user/$UID/gvfs/dav:host=nextcloud.linuxmaine.fr,..."
```

## Bonne pratique

Toujours utiliser un **App Password** (Paramètres → Sécurité) plutôt que le mot de passe principal : révocable individuellement, indispensable si 2FA activé.



# Accès depuis un navigateur web

## Connexion sécurisée

- URL en **HTTPS** avec **HSTS** (Strict-Transport-Security)
- Vérification du certificat (Let's Encrypt, ZeroSSL ou CA interne)
- Cookies Secure, HttpOnly, SameSite=Lax
- En-têtes : CSP, X-Frame-Options, X-Content-Type-Options
- Session PHPSESSID chiffrée, expiration paramétrable

## Authentification utilisateur

- Mot de passe + **2FA** (TOTP / WebAuthn)
- SSO entreprise via SAML 2.0 ou OIDC
- **Trusted Domains** : limiter les domaines d'accès
- **Brute-force protection** active par défaut
- Déconnexion globale possible (*Logout everywhere*)

## Hardening navigateur recommandé

Activer la *HTTPS-Only Mode* (Firefox, Chrome), vérifier le verrou TLS, utiliser un gestionnaire de mots de passe + 2FA matériel (Yubikey).

# Téléchargement scriptable — curl & wget

## Principe

Tout fichier Nextcloud est accessible via WebDAV à l'URL :

`https://<host>/remote.php/dav/files/<user>/<chemin>/<fichier>`

Authentification HTTP *Basic* : utiliser un **App Password** (jamais le mot de passe principal).

```
# --- Variables ---
NC_URL="https://nextcloud.linuxmaine.fr"
NC_USER="thierry"
NC_PASS="xxxx-xxxx-xxxx-xxxx" # App Password genere depuis Parametres -> Securite
NC_DAV="$NC_URL/remote.php/dav/files/$NC_USER"

# --- 1. Telechargement avec curl ---
curl -u "$NC_USER:$NC_PASS" -o rapport.pdf "$NC_DAV/Documents/rapport.pdf"

# --- 2. Telechargement avec wget ---
wget --user="$NC_USER" --password="$NC_PASS" \
  -O rapport.pdf "$NC_DAV/Documents/rapport.pdf"

# --- 3. Lien public (partage non protege par mot de passe) ---
curl -L -o doc.pdf "https://nextcloud.linuxmaine.fr/s/AbCd1234/download"

# --- 4. Lien public protege par mot de passe ---
curl -u ":monMotDePassePartage" -L \
  -o doc.pdf "https://nextcloud.linuxmaine.fr/s/AbCd1234/download"

# --- 5. Upload (PUT WebDAV) ---
curl -u "$NC_USER:$NC_PASS" -T fichier.zip "$NC_DAV/Backup/fichier.zip"
```



# Bonnes pratiques de scripting

- Stocker l'**App Password** dans **libsecret** (`secret-tool`) ou un `.netrc` en mode 600
- **Ne jamais** exposer le mot de passe en argument `ps-visible` : préférer `-config` ou `stdin`
- Toujours **HTTPS** : `curl -proto-default https` et `wget -secure-protocol=TLSv1_3`
- Vérifier le certificat : `curl -cacert /etc/ssl/certs/ca-certificates.crt`
- Couverture des erreurs : `curl -fSL` (fail-silent + suivre redirections + log erreur)

```
# Stocker un App Password avec libsecret
secret-tool store --label="Nextcloud" service nc account thierry
secret-tool lookup service nc account thierry

# Utilisation dans un script (.netrc style)
cat > ~/.netrc <<EOF
machine nextcloud.linuxmaine.fr
login thierry
password xxxx-xxxx-xxxx-xxxx
EOF
chmod 600 ~/.netrc
curl -n -O "$NC_DAV/Documents/rapport.pdf"
```

# Sécurité par défaut

- **TLS** obligatoire (HSTS, A+ sur SSL Labs)
- **2FA** natif : TOTP, WebAuthn, U2F, Yubikey, SMS, Email
- **Server-Side Encryption** (AES-256) avec gestion de clés maîtres
- **End-to-End Encryption** côté client (clés privées jamais sur serveur)
- **Brute Force protection** : ralentissement progressif des IP suspectes
- **Rate limiting, CSRF tokens, CSP headers**
- **Audit log** : trace de toutes les actions sensibles
- **Sécurité *Scan*** : [nextcloud.com/security-scan/](https://nextcloud.com/security-scan/) (note A–F)
- Programme **Bug Bounty** (HackerOne)

# Conformité réglementaire

- **RGPD** : DPA disponible, journal de consentement, droit à l'oubli
- **HDS** (Hébergeur de Données de Santé, France) : architecture compatible
- **ISO 27001** : conformité des ESN qui hébergent
- **HIPAA** (USA, santé) : modules disponibles
- **C5** (Allemagne, BSI) : certification cloud fédéral
- **SecNumCloud** : compatible (hébergement sur OVHcloud, Outscale, Scaleway qualifiés)
- **eIDAS** : signature électronique (LibreSign, EIDEasy)

## Souveraineté

Code source AGPLv3, hébergement *on-premise* ou cloud souverain européen, audit possible à tout moment.

# Yubikey — principes

## Qu'est-ce qu'une Yubikey ?

- Clé matérielle USB / NFC fabriquée par **Yubico** (Suède / USA)
- Stocke des **secrets cryptographiques** sans jamais les exporter
- Résiste au phishing : la clé signe le *domaine* (ne fonctionne que sur le bon site)
- Modèles : Yubikey 5 (USB-A/C, NFC, Lightning), Security Key, Bio
- Alternatives libres : **Solokey**, **Nitrokey**, **OnlyKey**

## Protocoles supportés

- **FIDO2 / WebAuthn** : passkey, sans mot de passe (recommandé)
- **U2F** : second facteur historique (Universal 2nd Factor)
- **TOTP / HOTP** (OATH) : codes à 6 chiffres
- **OpenPGP** : signature et chiffrement de courriels
- **PIV** : carte à puce (X.509)
- **Yubikey OTP** : OTP propriétaire historique

# Activer la Yubikey sur Nextcloud

## Prérequis

Apps à activer (Paramètres → Apps → Sécurité) :

- **Two-Factor WebAuthn** : recommandé (FIDO2, passkey, biométrie)
- **Two-Factor U2F** (legacy, encore supporté)
- **Two-Factor TOTP** : si Yubikey utilisée en mode OATH

## Activation utilisateur (HTTPS obligatoire)

- 1 Paramètres → Sécurité → Authentification à deux facteurs
- 2 Cocher *WebAuthn* → bouton *Ajouter une clé*
- 3 Brancher la Yubikey, toucher le bouton doré quand le navigateur clignote
- 4 Donner un nom (ex : *Yubikey-USB-C-bureau*) et sauvegarder
- 5 Générer un **code de secours** (*Backup codes*) et le stocker hors ligne

```
# Activation forcée 2FA via occ (côté serveur)
sudo -u www-data php occ twofactorauth:enforce --on
sudo -u www-data php occ twofactorauth:state thierry
sudo -u www-data php occ twofactorauth:disable thierry totp # débloquer si perte
```

# Yubikey — usages avancés

## SSH avec Yubikey

- Clé SSH *résidente* sur la Yubikey (FIDO2)
- `ssh-keygen -t ed25519-sk -O resident`
- Toucher la clé à chaque connexion : protection anti-vol
- Compatible avec serveurs Nextcloud, GitLab, GitHub

## Chiffrement OpenPGP

- Stocker la sous-clé GPG dans la Yubikey
- Signer des fichiers déposés sur Nextcloud
- Compatible Mailvelope (chiffrer Mail Nextcloud)

## Linux : configuration

- Paquet `libfido2-1`, `yubikey-manager`, `yubico-piv-tool`
- Règles `udev` pour accès non-root
- `ykman info` : vérifier la clé
- `ykman fido credentials list`

## Sécurité opérationnelle

- Toujours **2 clés** (principale + secours)
- Stocker codes de récupération hors ligne
- Définir un **PIN** FIDO2 (limite les tentatives)



# Keycloak — l'IdP libre de référence

## Qu'est-ce que Keycloak ?

- **Fournisseur d'identité** (IdP) libre, lancé par **Red Hat** en 2014
- Donné à la **Cloud Native Computing Foundation** (CNCF) en 2023
- Écrit en Java (Quarkus), back-end relationnel (Postgres, MariaDB)
- Licence **Apache 2.0**
- Distribution entreprise : *Red Hat build of Keycloak* (anciennement RH-SSO)

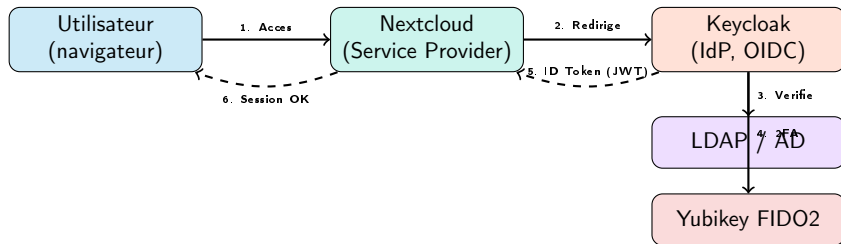
## Standards supportés

- **OpenID Connect** (OIDC) : recommandé pour Nextcloud
- **OAuth 2.0** : autorisation déléguée
- **SAML 2.0** : compatibilité legacy entreprise
- **LDAP / Active Directory** : federation back-end
- **Kerberos / SPNEGO, X.509, WebAuthn**
- **Brokering** : Google, GitHub, GitLab, France Connect

## Pourquoi Keycloak avec Nextcloud ?

**SSO unifié** pour Nextcloud + Passbolt + Bitwarden + GitLab + Mattermost + Jenkins... et délégation de la 2FA (TOTP, Yubikey/FIDO2) au seul IdP.

# Architecture Nextcloud + Keycloak



- Nextcloud joue le rôle de **Relying Party** (*client OIDC*)
- Keycloak joue le rôle de **Identity Provider** : centralise mots de passe, MFA, politiques
- L'utilisateur ne saisit **jamais** son mot de passe dans Nextcloud
- Provisionnement automatique des comptes via les *claims* OIDC

# Configuration côté Keycloak

- ❶ Créer un **Realm** (ex : linuxmaine)
- ❷ **Clients** → *Create client* : type OpenID Connect
- ❸ Client ID : nextcloud — Root URL : <https://nextcloud.linuxmaine.fr>
- ❹ Client authentication : ON (confidentiel) — Client secret : copier
- ❺ Valid Redirect URLs : [https://nextcloud.linuxmaine.fr/apps/user\\_oidc/code](https://nextcloud.linuxmaine.fr/apps/user_oidc/code)
- ❻ Valid Post Logout Redirect URLs : <https://nextcloud.linuxmaine.fr>
- ❼ **Mappers** : ajouter groups, email, preferred\_username, name
- ❽ **Authentication flow** : activer *WebAuthn Passwordless* (Yubikey) ou TOTP

```
# URLs OIDC (decouverte automatique)
https://keycloak.linuxmaine.fr/realms/linuxmaine/.well-known/openid-configuration

# Endpoints derives :
#   authorization_endpoint : .../protocol/openid-connect/auth
#   token_endpoint        : .../protocol/openid-connect/token
#   userinfo_endpoint     : .../protocol/openid-connect/userinfo
#   end_session_endpoint  : .../protocol/openid-connect/logout
#   jwks_uri              : .../protocol/openid-connect/certs
```

# Configuration côté Nextcloud (app user\_oidc)

Prérequis : installer l'app officielle

```
sudo -u www-data php occ app:install user_oidc (ou via l'AppStore)
```

## Configuration via l'interface

- Paramètres → Administration → *OpenID Connect*
- *Identifiant* : linuxmaine-keycloak
- *Discovery URL* : .../realms/linuxmaine/.well-known/openid-configuration
- *Client ID* : nextcloud — *Client Secret* : (copié depuis Keycloak)
- *Scope* : openid profile email roles groups

## Configuration en CLI (occ, automatisable)

```
# Provider OIDC complet
sudo -u www-data php occ user_oidc:provider linuxmaine-keycloak \
  --clientid="nextcloud" --clientsecret="$KC_SECRET" \
  --discoveryuri="https://keycloak.linuxmaine.fr/realms/linuxmaine/.well-known/openid-configuration" \
  --scope="openid profile email roles groups" \
  --mapping-uid="preferred_username" \
  --mapping-display-name="name" --mapping-email="email" \
  --mapping-groups="groups" --group-provisioning=1

# Forcer la connexion via Keycloak (desactiver auth locale)
sudo -u www-data php occ config:app:set user_oidc allow_multiple_user_back_ends --value="0"
sudo -u www-data php occ config:system:set auth.bruteforce.protection.enabled \
```



# Déploiement automatisé (Ansible)

```
# group_vars/nextcloud/keycloak.yml
keycloak_realm: "linuxmaine"
keycloak_url: "https://keycloak.linuxmaine.fr"
keycloak_client_id: "nextcloud"
keycloak_client_secret: "{{ vault_keycloak_client_secret }}" # Vault

# roles/nextcloud_oidc/tasks/main.yml
- name: Installer l'app user_oidc
  command: php occ app:install user_oidc
  args: { chdir: /var/www/nextcloud }
  become_user: www-data
  register: r
  changed_when: "'already installed' not in r.stdout"
  failed_when: r.rc != 0 and 'already installed' not in r.stdout

- name: Configurer le provider Keycloak
  command: >-
    php occ user_oidc:provider {{ keycloak_realm }}
    --clientid={{ keycloak_client_id }}
    --clientsecret={{ keycloak_client_secret }}
    --discoveryuri={{ keycloak_url }}/realms/{{ keycloak_realm }}/well-known/openid-configuration
    --scope="openid profile email roles groups"
    --mapping-uid=preferred_username
    --mapping-groups=groups
    --group-provisioning=1
  args: { chdir: /var/www/nextcloud }
  become_user: www-data
  no_log: true
```

# Bonnes pratiques Keycloak + Nextcloud

- **HTTPS obligatoire** sur les deux services + certificats valides (Let's Encrypt ou CA interne)
- **Trusted proxies** : configurer `trusted_proxies` dans `config.php` si reverse-proxy en tête
- **Synchronisation horloge** (NTP / chrony) : un décalage casse la vérification JWT
- **Session courte** côté Keycloak (1h-8h) + *Refresh Token* : révocation rapide
- **Mappage des groupes** : provisionner automatiquement les groupes Nextcloud depuis Keycloak (claim groups)
- **2FA centralisée** : activer WebAuthn (Yubikey) côté Keycloak, désactiver la 2FA Nextcloud (évite la double saisie)
- **Logout SSO** : `end_session_endpoint` pour fermer toutes les sessions
- **Sauvegarde Keycloak** : exporter les realms (`kc.sh export`) avant chaque mise à jour
- **Brokering** : permettre la connexion via France Connect ou ProConnect pour les services publics

# Alternatives à Keycloak

## IdP libres compatibles

- **Authentik** : Python/Django, UI moderne, BSL/MIT
- **Authelia** : portail SSO léger Go
- **Zitadel** : Go, multi-tenant, Apache 2.0
- **LemonLDAP::NG** : écosystème *gov.fr*, Perl
- **Gluu / Janssen Server** : enterprise grade

## IdP propriétaires

- Microsoft Entra ID (anciennement Azure AD)
- Okta, Auth0, OneLogin
- Google Identity Platform

## Fédérations sectorielles

- **ProConnect** (admin française)
- **eduGAIN** / RENATER (recherche)
- **France Connect** (citoyens)

Toutes ces solutions parlent OIDC ou SAML : Nextcloud reste compatible via `user_oidc` ou `user_saml`.

# Pourquoi un coffre-fort externe ?

- Nextcloud propose l'app **Passwords** (officielle) : suffisante pour un usage personnel
- En entreprise / équipe : préférer un **gestionnaire dédié** : audit, partage granulaire, politique de rotation, MFA
- Trois familles de coffres-forts compatibles avec Nextcloud :
  - **Passbolt** : spécialisé *partage en équipe*, OpenPGP natif
  - **Bitwarden** / **Vaultwarden** : multi-plateforme, libre, app mobile
  - **KeePassXC** : coffre local (.kdbx), synchronisé *via* Nextcloud
- Patterns d'intégration :
  - *Auth* : SSO commun (LDAP / SAML / OIDC) entre Nextcloud et le coffre
  - *Stockage* : fichier KeePass .kdbx dans Nextcloud
  - *Plugin* : navigateur ou app mobile remplit les champs Nextcloud
  - *Webhook* : automatisation rotation de mot de passe et App Password



# Passbolt — coffre-fort équipe

## Présentation

- Coffre-fort **libre** (AGPLv3), éditeur français/luxembourgeois
- Architecture : serveur PHP + extension navigateur + GPG
- **Chiffrement E2EE** : chaque secret chiffré avec la clé GPG du destinataire
- Partage granulaire (lecture, mise à jour, propriétaire)
- Audit & journal complet

## Intégration Nextcloud

- **SSO** commun via SAML / OIDC (Keycloak)
- App *External Sites* : ajouter Passbolt dans le menu Nextcloud
- Stockage des fichiers de clés GPG sur Nextcloud (chiffrement E2EE)
- **Yubikey FIDO2** pour le 2FA Passbolt (idem Nextcloud)
- Déploiement parallèle via Ansible / OpenTofu

Site officiel : <https://www.passbolt.com> — Déploiement Docker, Helm ou Ansible disponible.

# Bitwarden / Vaultwarden + Nextcloud

- **Bitwarden** : version officielle (cloud ou self-hosted, .NET)
- **Vaultwarden** : réimplémentation légère en Rust, même API
- Coffre-fort multi-plateforme : Web, Desktop, Android, iOS, extension navigateur, CLI bw
- **Compatibilité Yubikey** : 2FA U2F/WebAuthn ou TOTP
- Possibilité de stocker des *Secure Notes*, fichiers chiffrés, cartes bancaires

## Patterns d'intégration avec Nextcloud

- 1 **SSO unifié** : Keycloak (OIDC) authentifie Nextcloud + Bitwarden (même identité)
- 2 **App Password Nextcloud** stocké dans Bitwarden (champ dédié + URI)
- 3 **CLI bw** dans les scripts qui tapent l'API Nextcloud

```
# Recupérer un App Password Nextcloud depuis Bitwarden CLI
export BW_SESSION=$(bw unlock --raw)
NC_PASS=$(bw get password "Nextcloud LinuxMaine")
NC_USER=$(bw get username "Nextcloud LinuxMaine")
curl -u "$NC_USER:$NC_PASS" -O \
  "https://nextcloud.linuxmaine.fr/remote.php/dav/files/$NC_USER/Documents/rapport.pdf"
```

# KeePassXC + Nextcloud (*best of both worlds*)

## Principe

- **KeePassXC** : coffre-fort local libre, format .kdbx
- Le .kdbx est placé dans Documents/secrets.kdbx sur Nextcloud
- Synchronisation automatique entre tous les postes (Linux, Win, Mac, mobile)
- Mobile : **KeePassDX** (Android), **Strongbox** (iOS) avec WebDAV Nextcloud
- **Yubikey** en mode HMAC-SHA1 challenge-response (complément du mot de passe maître)

## Sécurité

- Coffre toujours chiffré (AES-256, ChaCha20, Argon2)
- Clé maître + Yubikey + fichier-clé (3 facteurs)
- Aucune confiance nécessaire dans le serveur Nextcloud (zero-knowledge)
- Versioning Nextcloud = historique de coffre
- Compatible **Browser-pass-through** (extension Firefox/Chrome)

## Recommandation LinuXMaine

Pour un usage individuel ou associatif : **KeePassXC + Nextcloud + Yubikey** = trio robuste, 100% libre, sans serveur de coffre supplémentaire à maintenir

# Synthèse — choix d'un coffre-fort

| Critère        | NC Passwords  | Passbolt          | Bitwarden / Vaultwarden | KeePassXC + NC       |
|----------------|---------------|-------------------|-------------------------|----------------------|
| Licence        | AGPLv3        | AGPLv3            | GPLv3 / AGPLv3          | GPLv3                |
| Type           | App Nextcloud | Serveur dédié     | Serveur dédié           | Local + sync NC      |
| Partage équipe | Basique       | Excellent (GPG)   | Bon (Organizations)     | Manuel               |
| Yubikey        | Oui (FIDO2)   | Oui (FIDO2)       | Oui (FIDO2/U2F)         | Oui (HMAC-SHA1)      |
| SSO            | Hérite NC     | SAML / OIDC       | SSO Premium             | N/A (local)          |
| Mobile         | App NC        | App dédiée        | App native              | KeePassDX, Strongbox |
| Cas idéal      | Solo / TPE    | Équipe <i>ops</i> | Toute taille            | Tech-savvy / asso    |

Pour LinuXMaine : Passbolt pour les secrets d'équipe (production), KeePassXC pour les bénévoles individuels.

# Prérequis système

## Matériel minimum

- 2 vCPU, 2 Go RAM (lab)
- 4 vCPU, 8 Go RAM (production  $\leq$  50 utilisateurs)
- 16 Go RAM + Redis HPB ( $\geq$  200 utilisateurs)
- Stockage : SSD recommandé

## Logiciel

- **OS** : Debian 12, Ubuntu 24.04, RHEL 9
- **PHP** 8.1 – 8.4 + extensions
- **Apache** 2.4 ou **Nginx** + PHP-FPM
- **MariaDB** 10.6+ / **PostgreSQL** 14+
- **Redis** 7+
- Certificat TLS (Let's Encrypt)

*# Extensions PHP requises (Debian/Ubuntu)*

```
sudo apt install php-{cli,fpm,mysql,gd,curl,xml,mbstring,zip,intl,bcmath,gmp,imagick,redis,apcu}
```

# Installation manuelle (archive officielle)

```
# 1. Télécharger la dernière version (Hub 10)
cd /var/www/
sudo curl -O https://download.nextcloud.com/server/releases/latest.zip
sudo unzip latest.zip && sudo chown -R www-data:www-data nextcloud/

# 2. Créer la base de données
sudo mysql -e "CREATE DATABASE nextcloud CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;"
sudo mysql -e "CREATE USER 'nc'@'localhost' IDENTIFIED BY 'CHANGE_ME';"
sudo mysql -e "GRANT ALL ON nextcloud.* TO 'nc'@'localhost'; FLUSH PRIVILEGES;"

# 3. Configurer Apache (vhost minimal)
sudo a2enmod rewrite headers env dir mime ssl

# 4. Lancer l'installation web ou en CLI via occ
sudo -u www-data php /var/www/nextcloud/occ maintenance:install \
  --database "mysql" --database-name "nextcloud" \
  --database-user "nc" --database-pass "CHANGE_ME" \
  --admin-user "admin" --admin-pass "CHANGE_ME"
```

Pour un déploiement reproductible, préférer Ansible ou OpenTofu (cf. sections suivantes).

# Déploiement Docker (alternative rapide)

```
# docker-compose.yml minimal Nextcloud + MariaDB + Redis
services:
  db:
    image: mariadb:10.11
    command: --transaction-isolation=READ-COMMITTED --binlog-format=ROW
    environment:
      MARIADB_ROOT_PASSWORD: root
      MARIADB_DATABASE: nextcloud
      MARIADB_USER: nextcloud
      MARIADB_PASSWORD: CHANGE_ME
    volumes: [db:/var/lib/mysql]

  redis:
    image: redis:7-alpine

  app:
    image: nextcloud:30-apache
    depends_on: [db, redis]
    ports: ["8080:80"]
    environment:
      MYSQL_HOST: db
      MYSQL_DATABASE: nextcloud
      MYSQL_USER: nextcloud
      MYSQL_PASSWORD: CHANGE_ME
      REDIS_HOST: redis
    volumes: [nc:/var/www/html]

volumes: { db: {}, nc: {} }
```

# Pourquoi Ansible pour Nextcloud ?

- **Sans agent** : un simple accès SSH suffit, pas de logiciel sur la cible
- **Idempotent** : relancer le playbook ne casse pas l'instance existante
- **Reproductible** : même code pour dev, staging, production
- **Versionnable** (Git) : chaque modification tracée, revue de code possible
- **Rôles communautaires** matures : `geerlingguy.nextcloud`, `nextcloud.admin`
- **Vault** : chiffrement des mots de passe BD et compte admin

## Architecture cible du playbook

Un hôte = Apache + PHP-FPM + MariaDB + Redis + Nextcloud configuré, certificat Let's Encrypt obtenu via certbot.



# Inventaire & vars du rôle

```
# inventory/hosts.yml
all:
  children:
    nextcloud:
      hosts:
        nc01:
          ansible_host: nextcloud.linuxmaine.fr
          ansible_user: deploy
```

```
# group_vars/nextcloud/main.yml
nextcloud_version: "30.0.2"
nextcloud_domain: "nextcloud.linuxmaine.fr"
nextcloud_admin_user: "admin"
nextcloud_admin_pass: "{{ vault_admin_pass }}" # Ansible Vault
nextcloud_db_engine: "mysql"
nextcloud_db_name: "nextcloud"
nextcloud_db_user: "nc"
nextcloud_db_pass: "{{ vault_db_pass }}"
nextcloud_trusted_domains:
  - "nextcloud.linuxmaine.fr"
nextcloud_redis_enabled: true
nextcloud_tls_email: "tgayet@tixeo.com"
```

# Playbook principal (extrait)

```
# playbooks/site.yml
- name: Deploiement Nextcloud
  hosts: nextcloud
  become: true
  pre_tasks:
    - name: Mise à jour APT
      apt: { update_cache: yes, cache_valid_time: 3600 }

  roles:
    - role: geerlingguy.mysql
    - role: geerlingguy.redis
    - role: geerlingguy.apache
    - role: geerlingguy.php
    vars:
      php_version: "8.3"
      php_packages_extra: [php-mysql, php-gd, php-curl, php-xml,
                           php-mbstring, php-zip, php-intl, php-bcmath, php-gmp,
                           php-imagick, php-redis, php-apcu]
    - role: nextcloud.admin
    - role: geerlingguy.certbot
    vars:
      certbot_create_if_missing: true
      certbot_certs:
        - email: "{{ nextcloud_tls_email }}"
          domains: ["{{ nextcloud_domain }}"]

  post_tasks:
    - name: Activer Redis dans config.php
      command: >
        sudo -u www-data php occ config:system:set memcache.locking
          --value="//OC\\Memcache\\Redis"
      args: { chdir: /var/www/nextcloud }
      changed_when: false
```

# Exécution & vérification

```
# Cloner le depot
git clone https://framagit.org/linuxmaine/formations.git
cd formations/devsecops/nextcloud/

# Installer les dependances Galaxy
ansible-galaxy install -r requirements.yml

# Chiffrer les secrets
ansible-vault edit group_vars/nextcloud/vault.yml

# Dry-run (verification)
ansible-playbook -i inventory/hosts.yml playbooks/site.yml --check --diff

# Application
ansible-playbook -i inventory/hosts.yml playbooks/site.yml --ask-vault-pass

# Verification post-deploiement
ansible nextcloud -m uri -a "url=https://nextcloud.linuxmaine.fr/status.php"
ansible nextcloud -a "sudo -u www-data php /var/www/nextcloud/occ status"
```

## Bonnes pratiques

Toujours tester avec `-check -diff` avant l'application réelle. Conserver un backup BD + dossier data/ avant toute montée de version.

# Pourquoi OpenTofu pour Nextcloud ?

- **OpenTofu** : fork open source de Terraform (Linux Foundation, MPL 2.0, 2023)
- Compatible à 100% avec les fichiers `.tf` et providers existants
- **Provisionnement de l'infrastructure** : VM, réseau, DNS, certificats, stockage S3
- **Déclaratif** : on décrit l'état cible, OpenTofu calcule le *plan*
- **State file** : suivi de l'infrastructure réelle (`terraform.tfstate`)
- **Multi-cloud** : OVH, Scaleway, Hetzner, AWS, Azure, GCP, Proxmox...
- Complémentaire d'Ansible : *Tofu provisionne le "socle", Ansible installe Nextcloud dessus*

## Pattern recommandé

- 1) OpenTofu crée la VM, le DNS, le bucket S3, le pare-feu.
- 2) Ansible installe et configure Nextcloud sur la VM.
- 3) Tout est versionné dans un même dépôt Git.

# Module Tofu : VM + DNS + S3 (Scaleway)

```

terraform {
  required_version = ">= 1.6"
  required_providers {
    scaleway = { source = "scaleway/scaleway", version = "~> 2.40" }
  }
  backend "s3" {
    bucket = "linuxmaine-tfstate"
    key    = "nextcloud/terraform.tfstate"
    region = "fr-par"
  }
}

provider "scaleway" {
  zone  = "fr-par-1"
  region = "fr-par"
}

# VM applicative
resource "scaleway_instance_server" "nextcloud" {
  name     = "nc-prod"
  type     = "DEVi-L"           # 4 vCPU, 8 Go RAM
  image    = "debian_bookworm"
  tags     = ["nextcloud", "linuxmaine"]
  ip_id    = scaleway_instance_ip.nextcloud.id
  user_data = { "cloud-init" = file("${path.module}/cloud-init.yaml") }
}

resource "scaleway_instance_ip" "nextcloud" {}

# Bucket S3 pour stockage primaire
resource "scaleway_object_bucket" "nc_data" {
  name     = "linuxmaine-nc-data"
  region   = "fr-par"
  versioning { enabled = true }
}

```



# Workflow OpenTofu + Ansible

```
# 1. Initialisation du backend (state distant)
tofu init

# 2. Plan (calcul du diff vs etat reel)
tofu plan -out=plan.tfplan

# 3. Application
tofu apply plan.tfplan

# 4. Recuperation de l'IP cree
NC_IP=$(tofu output -raw ip)
echo "Nextcloud IP: $NC_IP"

# 5. Mise a jour de l'inventaire Ansible
cat > inventory/hosts.yml <<EOF
all:
  children:
    nextcloud:
      hosts:
        nc01:
          ansible_host: $NC_IP
          ansible_user: deploy
EOF

# 6. Provisionnement applicatif
ansible-playbook -i inventory/hosts.yml playbooks/site.yml --ask-vault-pass

# 7. Destruction (lab uniquement !)
tofu destroy -auto-approve
```

# OpenTofu — bonnes pratiques

- **Backend distant** (S3, GCS, Postgres) : ne jamais committer le tfstate en clair
- **State locking** : verrouillage via DynamoDB / Postgres pour le travail en équipe
- **Modules** : factoriser les ressources (*module Nextcloud, module DNS, module storage*)
- **Workspaces** : un workspace par environnement (dev / staging / prod)
- **Lint** : tofu fmt, tofu validate, tflint
- **Security scan** : checkov, tfsec, trivy config
- **Secrets** : ne jamais en HCL en clair — utiliser *Vault, SOPS, AWS Secrets Manager*
- **CI/CD** : pipeline *plan* sur PR, *apply* après validation manuelle

# La commande occ

- Outil CLI officiel d'administration de Nextcloud (ownCloud Console)
- S'exécute en tant qu'utilisateur du serveur web (www-data)

```
# Status d'instance
sudo -u www-data php occ status

# Lister les utilisateurs
sudo -u www-data php occ user:list

# Créer un utilisateur (mot de passe via stdin)
echo "MotDePasse" | sudo -u www-data php occ user:add --password-from-env user1

# Mode maintenance (avant mise à jour)
sudo -u www-data php occ maintenance:mode --on

# Réparer l'index de fichiers
sudo -u www-data php occ files:scan --all

# Mise à jour majeure
sudo -u www-data php occ upgrade

# Lister les apps installées
sudo -u www-data php occ app:list
```



# Sauvegarde & restauration

## Éléments à sauvegarder

- Dossier config/
- Dossier data/ (données utilisateurs)
- Dossier apps/ (custom apps)
- **Base de données** (mysqldump, pg\_dump)
- Clés de chiffrement (si SSE activé)

## Outils

- borgbackup : sauvegarde incrémentale chiffrée
- restic : compatible S3
- **Snapshots** ZFS / LVM / Ceph
- App *Nextcloud Backup* (officielle)
- Snapshot S3 versioning

### Règle 3-2-1

3 copies, 2 supports différents, 1 hors-site — toujours tester la restauration périodiquement.

# Supervision & observabilité

- **Endpoint** /status.php : version, maintenance, installé (JSON)
- **Serverinfo API** : métriques détaillées (utilisateurs, stockage, apps)
- Exporters **Prometheus** : xperimental/nextcloud-exporter
- Tableaux **Grafana** : dashboard officiel ID 8693
- **Logs** : data/nextcloud.log (JSON), Audit log (audit.log)
- **Sentry / Loki** : agrégation des erreurs PHP
- **Healthchecks** HTTP : sondes Kubernetes / Docker compose
- **Notifications** sur incident : Pushover, Mattermost, Matrix, e-mail

# Lexique (1/3) — Nextcloud I

**App / Application** Module logiciel installé dans Nextcloud (Talk, Deck, Photos...), distribué via l'AppStore.

**AppStore** Catalogue officiel des applications additionnelles (*apps.nextcloud.com*).

**CalDAV** Protocole standard de synchronisation d'agendas (RFC 4791).

**CardDAV** Protocole standard de synchronisation de carnets d'adresses (RFC 6352).

**Cercle (Circle)** Groupe d'utilisateurs créé à la demande, partagé entre apps.

**Collabora Online** Suite bureautique en ligne basée sur LibreOffice, intégrée à Nextcloud via WOPI.

**E2EE (End-to-End Encryption)** Chiffrement côté client : seules les clés privées du client peuvent déchiffrer.

**Fédération** Partage transparent de fichiers entre instances Nextcloud distinctes.

**GED** Gestion Électronique de Documents.

**Hub** Nom de la distribution Nextcloud regroupant Files, Talk, Groupware, Office.

# Lexique (1/3) — Nextcloud II

**HPB (High Performance Backend)** Service Node.js qui décharge Nextcloud Talk pour la signalisation à grande échelle.

**occ** Commande CLI d'administration (*ownCloud Console*).

**OnlyOffice** Suite bureautique alternative à Collabora, compatible MS Office.

**SSE (Server-Side Encryption)** Chiffrement côté serveur, transparent pour l'utilisateur.

**Talk** Application de visioconférence WebRTC intégrée.

**WebDAV** Extension HTTP pour la gestion de fichiers à distance (RFC 4918).

**Workflow Engine** Moteur de règles automatisées (filigrane, blocage, anti-virus, DLP).

# Lexique (1/3) — Nextcloud III

## Lexique (2/3) — Provisionnement

**Ansible** Outil d'automatisation *push*, sans agent, en YAML.

**Ansible Galaxy** Dépôt communautaire de rôles et collections Ansible.

**Ansible Vault** Mécanisme de chiffrement des secrets dans les fichiers YAML.

**Cloud-init** Outil d'initialisation au premier boot d'une VM cloud (hostname, SSH, paquets).

**Collection (Ansible)** Paquet versionné de modules, rôles et plugins.

**Déclaratif** Paradigme : on décrit l'état cible, le moteur calcule les actions.

**Idempotence** Propriété d'une opération : la répéter ne change pas le résultat final.

**IaC (Infrastructure as Code)** Description de l'infrastructure dans des fichiers versionnés.

**Impératif** Paradigme : on décrit la séquence d'actions à exécuter.

**Inventory** Liste des machines cibles d'Ansible (statique INI/YAML ou dynamique).

**Jinja2** Moteur de templates Python utilisé par Ansible.

**OpenTofu** Fork open source (MPL 2.0) de Terraform, hébergé par la Linux Foundation.

# Lexique (1/3) — Nextcloud IV

**Playbook** Fichier YAML décrivant des tâches Ansible à appliquer sur un inventaire.

**Provider (Tofu/Terraform)** Plugin gérant un fournisseur cloud (AWS, OVH...).

**Pull** Modèle où le nœud cible récupère sa configuration (Puppet, Chef).

**Push** Modèle où le contrôleur pousse la configuration (Ansible, Tofu).

**Rôle (Ansible)** Structure réutilisable (tasks, handlers, vars, templates).

**State file** Fichier d'état OpenTofu/Terraform (`terraform.tfstate`).

**Workspace** Espace de travail isolé dans OpenTofu (un par environnement).

# Lexique (1/3) — Nextcloud V

## Lexique (3/3) — Infrastructure & sécurité

**2FA (Two-Factor Authentication)** Authentification à double facteur (mot de passe + code).

**App Password** Mot de passe dédié à un client Nextcloud (généré dans Paramètres → Sécurité), révocable, requis quand 2FA est activé.

**Bitwarden** Gestionnaire de mots de passe libre (édition serveur officielle .NET).

**davfs2** Pilote Linux qui monte une URL WebDAV comme un système de fichiers POSIX.

**FIDO2** Standard d'authentification fort sans mot de passe (passkey, Yubikey, WebAuthn).

**GVFS** Couche d'accès aux systèmes de fichiers virtuels de GNOME (davs://, sftp://...).

**HMAC-SHA1 challenge-response** Mode de la Yubikey utilisé par KeePassXC pour ajouter un facteur matériel au coffre.

**KeePassXC** Coffre-fort local libre au format .kdbx, synchronisable via Nextcloud.

**Keycloak** Fournisseur d'identité libre (CNCF, Apache 2.0) parlant OIDC et SAML, utilisé comme IdP central pour Nextcloud et autres services.

# Lexique (1/3) — Nextcloud V1

**IdP** *Identity Provider* : service qui authentifie les utilisateurs et délivre des jetons aux applications.

**ID Token** Jeton JWT émis par un IdP OIDC contenant l'identité de l'utilisateur.

**JWT** *JSON Web Token*, format compact de jeton signé (RFC 7519).

**Realm (Keycloak)** Espace de tenants isolé dans Keycloak (utilisateurs, clients, rôles).

**Relying Party** Application qui délègue l'authentification à un IdP (OIDC).

**user\_oidc** App officielle Nextcloud implémentant le client OIDC.

**user\_saml** App officielle Nextcloud implémentant le client SAML 2.0.

**Mailvelope** Extension navigateur OpenPGP, intégrée à Nextcloud Mail pour le chiffrement bout-en-bout des courriels.

**Passbolt** Coffre-fort équipe libre (AGPLv3), basé sur GPG, partage granulaire.

**passkey** Identifiant FIDO2 (clé privée dans un *authenticator*) qui remplace mot de passe + 2FA.

**PIV** *Personal Identity Verification*, support carte à puce X.509 sur Yubikey.



# Lexique (1/3) — Nextcloud VII

**rclone** Outil CLI de synchronisation multi-cloud (WebDAV Nextcloud, S3...).

**U2F** *Universal 2nd Factor*, ancêtre de FIDO2 pour le second facteur matériel.

**Vaultwarden** Serveur Bitwarden non officiel, léger (Rust), API compatible.

**WebAuthn** API navigateur W3C utilisant FIDO2 pour authentifier sans mot de passe.

**Yubikey** Clé matérielle d'authentification fabriquée par Yubico (FIDO2, OTP, OpenPGP, PIV).

**AGPLv3** Licence libre copyleft fort exigeant la publication du code en cas d'usage en réseau.

**ANSSI** Agence nationale de la sécurité des systèmes d'information (France).

**BSI** *Bundesamt für Sicherheit in der Informationstechnik* (Allemagne).

**C5** Référentiel de sécurité cloud du BSI (Allemagne).

**Federation** Capacité d'échange entre instances autonomes (mail, ActivityPub, Nextcloud).

**HDS** Hébergeur de Données de Santé (certification française, ASIP/ANS).

**HSTS** *HTTP Strict Transport Security* : impose HTTPS aux navigateurs.

**LDAP** Protocole d'annuaire (*Lightweight Directory Access Protocol*).

# Lexique (1/3) — Nextcloud VIII

**OAuth2** Protocole d'autorisation déléguée (RFC 6749).

**OIDC (OpenID Connect)** Couche d'identité au-dessus d'OAuth2.

**PWA** *Progressive Web App* : application web installable, offline-capable.

**Reverse Proxy** Serveur intermédiaire qui relaie les requêtes vers un backend (Nginx, HAProxy).

**RGPD** Règlement Général sur la Protection des Données (UE 2016/679).

**SAML 2.0** Protocole fédéré d'authentification (SSO entreprise).

**SecNumCloud** Qualification ANSSI pour les services cloud souverains.

**SSO (Single Sign-On)** Authentification unique pour plusieurs services.

**TLS** *Transport Layer Security*, successeur de SSL.

**WebRTC** API navigateur pour audio/vidéo/data en temps réel.

**WOPI** *Web Application Open Platform Interface* (Microsoft) : protocole d'édition collaborative.

# Liens utiles — Projet Nextcloud

- Site officiel : <https://nextcloud.com>
- Documentation : <https://docs.nextcloud.com>
- Code source : <https://github.com/nextcloud/server>
- AppStore : <https://apps.nextcloud.com>
- Forum : <https://help.nextcloud.com>
- Security Scanner : <https://scan.nextcloud.com>
- Changelogs : <https://nextcloud.com/changelog/>
- Bug Bounty (HackerOne) : <https://hackerone.com/nextcloud>
- Manuel admin : [https://docs.nextcloud.com/server/latest/admin\\_manual/](https://docs.nextcloud.com/server/latest/admin_manual/)
- Guide de *hardening* : [https://docs.nextcloud.com/server/latest/admin\\_manual/installation/harden\\_server.html](https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html)

# Liens utiles — Provisionnement

- Ansible : <https://docs.ansible.com>
- Rôle nextcloud.admin : <https://galaxy.ansible.com/nextcloud/admin>
- Rôle geerlingguy.nextcloud : <https://galaxy.ansible.com/geerlingguy/nextcloud>
- OpenTofu : <https://opentofu.org>
- Registre OpenTofu : <https://search.opentofu.org>
- Docker Hub Nextcloud : [https://hub.docker.com/\\_/nextcloud](https://hub.docker.com/_/nextcloud)
- Helm chart : <https://artifacthub.io/packages/helm/nextcloud/nextcloud>
- AIO (All-In-One) : <https://github.com/nextcloud/all-in-one>
- Apps.education (France) : <https://apps.education.fr>

## Liens utiles — 2FA, Yubikey & coffres-forts

- Yubico — documentation : <https://docs.yubico.com>
- Yubikey Manager : <https://www.yubico.com/products/yubikey-manager>
- FIDO Alliance : <https://fidoalliance.org>
- WebAuthn (W3C) : <https://www.w3.org/TR/webauthn-2/>
- Solokey (libre) : <https://solokeys.com>
- Nitrokey : <https://www.nitrokey.com>
- Passbolt : <https://www.passbolt.com>
- Bitwarden : <https://bitwarden.com>
- Vaultwarden (fork Rust) : <https://github.com/dani-garcia/vaultwarden>
- KeePassXC : <https://keepassxc.org>
- KeePassDX (Android) : <https://www.keepassdx.com>
- Strongbox (iOS) : <https://strongboxsafe.com>
- rclone : <https://rclone.org/webdav/>

# Liens utiles — SSO & Keycloak

- Keycloak : <https://www.keycloak.org>
- Documentation Keycloak : <https://www.keycloak.org/documentation>
- Code source : <https://github.com/keycloak/keycloak>
- App user\_oidc : [https://apps.nextcloud.com/apps/user\\_oidc](https://apps.nextcloud.com/apps/user_oidc)
- App user\_saml : [https://apps.nextcloud.com/apps/user\\_saml](https://apps.nextcloud.com/apps/user_saml)
- Doc OIDC Nextcloud : [https://docs.nextcloud.com/server/latest/admin\\_manual/configuration\\_user/oidc/](https://docs.nextcloud.com/server/latest/admin_manual/configuration_user/oidc/)
- OpenID Connect Core 1.0 : [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html)
- Authentik : <https://goauthentik.io>
- Authelia : <https://www.authelia.com>
- Zitadel : <https://zitadel.com>
- LemonLDAP::NG : <https://lemonldap-ng.org>
- ProConnect (admin FR) : <https://www.proconnect.gouv.fr>

# Liens utiles — LinuXMaine & écosystème

- LinuXMaine : <https://linuxmaine.org>
- Framagit LinuXMaine : <https://framagit.org/linuxmaine>
- Framasoft (Cloud souverain) : <https://framacloud.org>
- April (libertés numériques) : <https://april.org>
- ANSSI — Souveraineté : <https://www.ssi.gouv.fr>
- DINUM — BlueHats : <https://code.gouv.fr>
- Linux Foundation Europe : <https://linuxfoundation.eu>
- Bundes-CIO — Souveraineté numérique : <https://www.cio.bund.de>
- Open Source Observatory :  
<https://joinup.ec.europa.eu/collection/open-source-observatory-osor>

# Références bibliographiques (en français) I



**Frank Karlitschek.** *Naissance de Nextcloud : pourquoi un fork d'ownCloud ?*  
Billet de blog, juin 2016. <https://nextcloud.com/blog/>



**Équipe Nextcloud GmbH.** *Manuel d'administration Nextcloud (édition 2026).* Documentation officielle (traduction française communautaire). <https://docs.nextcloud.com>



**ANSSI.** *Chaîne d'approvisionnement numérique souveraine : recommandations pour les administrations.* Guide ANSSI-PA-079, dernière mise à jour 2025. <https://www.ssi.gouv.fr>



**CNLL (Conseil National du Logiciel Libre).** *Panorama du logiciel libre en France — édition 2024.* Rapport annuel, Paris, 2024.



**DINUM (Direction interministérielle du numérique).** *Politique logicielle de l'État : socle interministériel des logiciels libres.* Mission BlueHats, 2025. <https://code.gouv.fr>



**Ministère de l'Éducation Nationale.** *Apps.education.fr : retour d'expérience d'un Nextcloud à 1,5 million d'utilisateurs.* Conférence Capitoile du Libre, Toulouse, 2024.



**Kief Morris.** *Infrastructure as Code — Gérer ses serveurs comme du code.* Traduction française de l'édition O'Reilly (2e éd.), 2022.



# Références bibliographiques (en français) II



**Jeff Geerling.** *Ansible pour DevOps : automatiser ses serveurs avec Ansible.* Traduction française communautaire, 2023. <https://www.ansiblefordevops.com>



**Linux Foundation.** *Manifeste OpenTofu : pourquoi un fork de Terraform ?*  
Communiqué officiel, septembre 2023. <https://opentofu.org/manifesto/>

# Références bibliographiques (en français) III



**CNIL.** *Guide pratique RGPD pour hébergeurs de services collaboratifs.* Commission Nationale de l'Informatique et des Libertés, Paris, 2024. <https://www.cnil.fr>



**Agence du Numérique en Santé (ANS).** *Référentiel de certification HDS — version 2024.* <https://esante.gouv.fr>



**Commission européenne, OSOR.** *Open Source en Europe : panorama des déploiements Nextcloud dans le secteur public.* Open Source Observatory, Bruxelles, 2024.



**Red Hat.** *Ansible Automation Platform : guide d'architecture.* Documentation officielle (édition française), 2024.



**Salvatore Loreto, Simon Pietro Romano.** *Communications temps réel avec WebRTC — principes et applications.* Édition française, ENI éditions, 2021.



**OWASP Foundation.** *ASVS — Application Security Verification Standard, version 4.0.3 (traduction française).* Project ASVS, 2024. <https://owasp.org/www-project-application-security-verification-standard/>



**FIDO Alliance.** *FIDO2 et WebAuthn : guide de mise en œuvre (traduction française).* Livre blanc, 2024. <https://fidoalliance.org>

# Références bibliographiques (en français) IV



**Passbolt SA.** *Gestion déléguée des secrets en équipe : architecture Passbolt*. Livre blanc technique, Luxembourg, 2024. <https://www.passbolt.com>



**Bitwarden Inc.** *Audit de sécurité indépendant Cure53 (rapport synthèse française)*, 2023.



**Cloud Native Computing Foundation.** *Keycloak rejoint la CNCF : feuille de route 2024–2026 (synthèse française)*. Communiqué officiel, 2023. <https://www.cncf.io>



**Sakimura, Bradley, Jones et al.** *OpenID Connect Core 1.0 — traduction et commentaires en français*. OpenID Foundation, 2014. <https://openid.net>



**ANSSI.** *KeePass : coffre-fort certifié CSPN — recommandations d'usage*. Note technique, 2022. <https://www.ssi.gouv.fr>



**Association LinuxMaine.** *Atelier DevSecOps — Module Nextcloud*. Support de formation, Le Mans, 2026. <https://framagit.org/linuxmaine/formations>

# Synthèse

## Ce qu'il faut retenir

- Nextcloud = **plateforme libre auto-hébergée** : Files, Talk, Groupware, Office
- **Souveraineté** : code AGPLv3, données on-premise, conformité RGPD/HDS/SecNumCloud
- Architecture **PHP** + **base SQL** + **Redis**, scalable jusqu'à des dizaines de milliers d'utilisateurs
- Déploiement reproductible : **Tofu pour le socle** + **Ansible pour l'applicatif**
- Écosystème **vivant** : 250+ apps, communauté mondiale, adoption institutionnelle

## Ressources LinuxMaine

- Dépôt Framagit : <https://framagit.org/linuxmaine/formations>
- Site association : <https://linuxmaine.org>
- Contact auteur : [Thierry.Gayet@gmail.com](mailto:Thierry.Gayet@gmail.com)

# Merci



## Nextcloud

### Merci de votre attention

Questions & discussions

[Thierry.Gayet@gmail.com](mailto:Thierry.Gayet@gmail.com)

Association LinuXMaine — 2026