

Novaxel CLOUD

FICHE TECHNIQUE

7 mai 2012



Think paperless



novaxel

Services offerts

Hébergement et sauvegarde de vos bibliothèques Novaxel

La **synchronisation** de vos données se fait à partir de votre poste. (à la demande, ou automatiquement)

Consultation de vos données à partir d'un navigateur et/ou de votre Smartphone (Android, iPhone, BlackBerry etc...)

Accès protégé :

- Accès aux sites WEB et mobile protégé par un certificat SSL et un cryptage 256 bits
- Cryptage de "bout en bout" des connexions
- Accès aux bibliothèques (WEB et mobiles) par mot de passe

Avantage :

Cette offre vous permet de sauvegarder vos données et d'avoir un accès sécurisé à distance via web.



Infrastructure

Serveurs dédiés à Novaxel (non mutualisé) chez un prestataire performant (OVH)

Datacenter haute performance (connexion électrique redondée, salle climatisée, situé en France, etc)

Bande passante réseau dédiée 200 Mbps pour l'ensemble de l'infrastructure (c'est à dire : partagée entre WEB et synchronisation Bibliothèques Novaxel)

Monitoring matériel (état matériel du serveur) et logiciel (services HTTPS et SSH actifs)

Infrastructure virtuelle (basée sur VMWare ESXi)

- 1 serveur dédié pour les accès WEB
- 1 serveur dédié pour les Bibliothèques Novaxel (Firebird)
- Montée en charge simple et souple (ajout de serveurs virtuels)

Cette infrastructure est totalement dédiée aux services proposés (aucun autre service n'est présent sur ces serveurs)



Sécurités

Sauvegarde des bibliothèques Novaxel chaque nuit :

- Une sauvegarde locale sur un disque dur spécifiquement dédié à cette tâche, pour reprise sur incident rapide
- Une sauvegarde distante sur un autre serveur pour une reprise sur incident plus complexe (dysfonctionnement d'un disque dur local par exemple)

Sauvegarde des configurations système chaque nuit sur un serveur distant

Synchronisation des bibliothèques

- Accès protégé par la mise en place d'un tunnel SSH (cryptage 256 bits)
- Procédure de synchronisation sécurisée à plusieurs niveaux (tests MD5 sur les fichiers envoyés, dialogue personnalisé entre client et serveur par échange de fichiers témoins, etc.)

Protection des systèmes eux-mêmes par la mise en place d'outil de détection d'intrusion réseau et actions d'exclusion associées (bannissement de l'adresse IP concernée)

Accès SSH : Tous les accès administratifs distants aux serveurs de l'infrastructure sont effectués en utilisant le protocole SSH et par des administrateurs approuvés et de confiance.

Les serveurs sont protégés par des pare-feux et seuls les services nécessaires aux clients sont accessibles à partir d'internet (services WEB et SSH)

