Galaxy Swiss Bourdin

Fiche de procédure :

Configuration de Nextcloud

Mise à jour : 10/05/2024

Auteur : Noah LOUINEAU

1. Sécurisation de Nextcloud

A. Système opérateur

I. **Contexte : Nextcloud utilise un générateur de nombres pseudo-aléatoires conforme à la RFC 4086 pour garantir la sécurité des opérations cryptographiques telles que la génération de clés de session et de jetons d'authentification. Ce générateur demande des nombres aléatoires à différentes sources pour produire des résultats robustes. L'accès à /dev/urandom est crucial car il fournit une source de nombres aléatoires de haute qualité sur les systèmes Linux.**

Rôle de /dev/urandom : /dev/urandom est un périphérique spécial dans les systèmes Linux qui fournit un flux de données aléatoires à la demande. Il utilise un générateur de nombres aléatoires cryptographiquement sécurisé pour produire des données aléatoires. /dev/urandom est essentiel pour les applications nécessitant des données aléatoires sécurisées, telles que la génération de clés cryptographiques.

Procédé de configuration pour que php puisse lire urandom

```
#nano /etc/php/8.2/cli/php.ini
open_basedir = /dev/urandom:/var/www/html/nexcloud
nano /etc/php/8.2/apache2/php.ini
open_basedir = /dev/urandom:/var/www/html/nexcloud
```

Vérification pour savoir si PHP peut lire urandom à l'aide d'un script php

```
<?php
$random_data = file_get_contents('/dev/urandom', false, null, 0, 10); // Lecture de 10 octets de /dev/urandom
echo bin2hex($random_data); // Afficher les données lues en tant que chaîne hexadécimale
?>
```

```
#php script-test.php
```

Résultat en sortie : c434c3071805f7aeeac6