

Documentation

Mise en Place des Bonnes Pratiques



06 mai 2024

INFRA & SI

Aix Ynov Campus

Table of Contents

[Restrictions concernant le nom d'utilisateur : 2](#_Toc166340209)

[Restrictions concernant le mot de passe : 2](#_Toc166340210)

[Limitation de quota : 2](#_Toc166340211)

[Connexion HTTPS : 2](#_Toc166340212)

[Blocage automatique des comptes : 3](#_Toc166340213)

[Utilisation d’authentification multi facteur : 3](#_Toc166340214)

Dans ce document nous répertorions une liste des bonnes pratiques que nous avons mis en place et la raison de ces dernières.

## Restrictions concernant le nom d'utilisateur :

Le nom d'utilisateur n'est pas sensible à la casse et peut inclure de 1 à 64 caractères Unicode, mais ne peut pas contenir les symboles suivants :  
! " # $ % & ' ( ) \* + , / : ; < = > ? @ [ ] \ ^ ` { } | ~

Le premier caractère ne peut pas être le signe moins ou un espace, et le dernier caractère ne peut pas être un espace.

Les noms d'utilisateur suivants sont réservés pour le système : mailer-daemon, postmaster.

La description de l'utilisateur peut inclure jusqu'à 64 caractères Unicode affichables.

Cette restriction permet d’éviter des erreurs systèmes en rapport avec un mauvais traitement du nom de l’utilisateur.

## Restrictions concernant le mot de passe :

Afin d’augmenter notre sécurité face à des attaques de types Brute Force nous avons mis en place une politique de mot de passe avec les contraintes suivantes :

* Exclure du mot de passe le nom la description de l’utilisateur
* Inclure le mélange majuscule/minuscule
* Inclure les caractères numériques
* Inclure les caractères spéciaux
* Exclure un mot de passe faible
* Longueur minimale de mot de passe à 8

## Limitation de quota :

Le quota d'utilisation maximale du stockage qui peut être saisi pour chaque utilisateur est approximativement de 25 Go pour le dossier home (dossier personnel) cela permet d’éviter que les utilisateurs n’utilisent le dossier home pour stocker les fichiers plutôt que les dossiers partagés prévu à cet effet.

## Connexion HTTPS :

Nous avons activé la connexion HTTPS, de ce fait lors de la connexion à DSM (page web permettant le contrôle du serveur) cette dernière est chiffrée à l'aide de SSL/TLS, ce qui sécurise la connexion face à des attaques du type Man in the middle.

## Blocage automatique des comptes :

Nous avons activé le blocage automatique pour bloquer une adresse IP après un nombre prédéfini de tentatives de connexion. Cette fonction est applicable aux tentatives de connexion via SSH, Telnet, rsync, Sauvegarde réseau, Synchro du dossier partagé, FTP, WebDAV, applications mobiles Synology, File Station et DSM. Sur notre serveur au bout de 10 connexions infructueuses l’adresse IP est banni pour une durée de 2 semaines.

## Utilisation d’authentification multi facteur :

L'authentification multi facteur offre une sécurité supplémentaire pour les comptes l’ayant activé. S'il cette dernière est activé, il est nécessaire de fournir une seconde vérification d'identité en plus du mot de passe lors de la connexion. Il est obligatoire pour les administrateurs de l’avoir activé afin de renforcer leur sécurité car ils sont des cibles privilégiées.