Réalisé par Pareja Tristan et Laurie Trintignac

Projet Gestion Horizons

Documentation utilisateur

Introduction

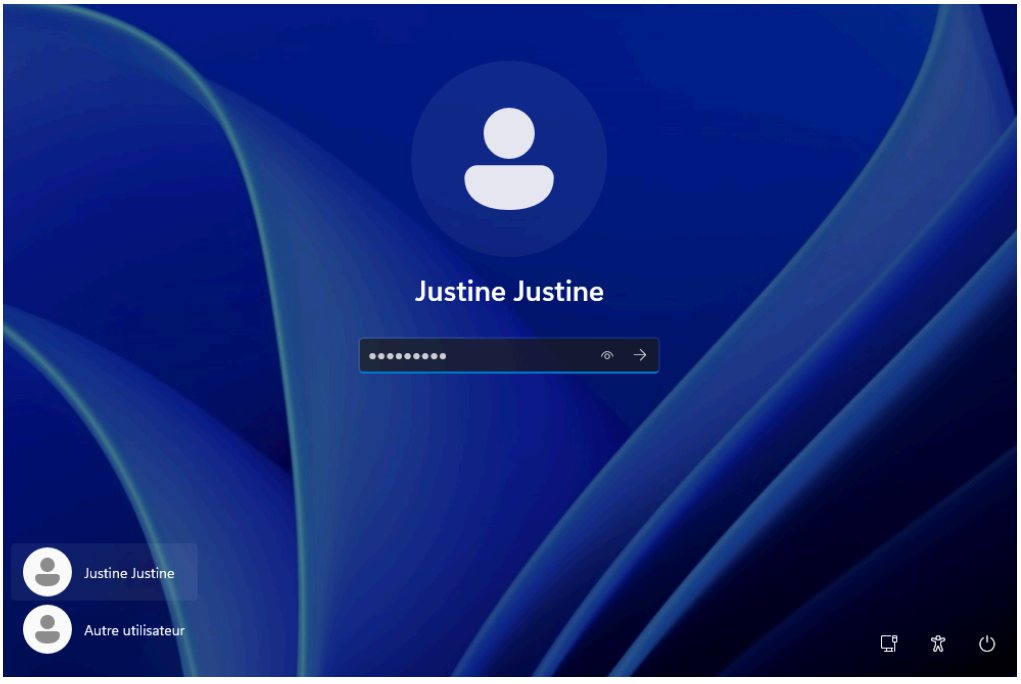
Dans un souci d'amélioration continue de ses outils informatiques, le cabinet Gestion Horizons modernise son infrastructure. Ce projet vise à vous offrir un environnement de travail plus sécurisé, plus fiable et accessible à distance depuis vos ordinateurs ou téléphones professionnels.

Ce guide vous accompagnera dans la prise en main des outils déployés dans le cadre de ce projet. Pas besoin d'être un expert en informatique : suivez simplement les étapes décrites.

I. Accéder à votre poste de travail

1. Connexion à votre PC Windows

- Allumez votre ordinateur, sur l'écran de connexion, entrez votre identifiant et mot de passe fournis par l'administrateur
- **2. Connexion au domaine "gestionhorizons.local"**
- Votre session est liée à un compte centralisé
- Cela vous permet d'accéder aux fichiers partagés et imprimantes.

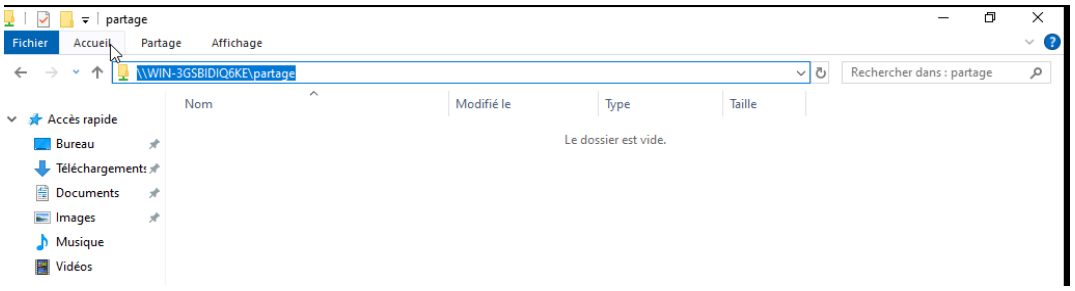


**En cas d'oubli de mot de passe, contactez l'administrateur informatique*

II. Sauvegarde et stockage de vos fichiers

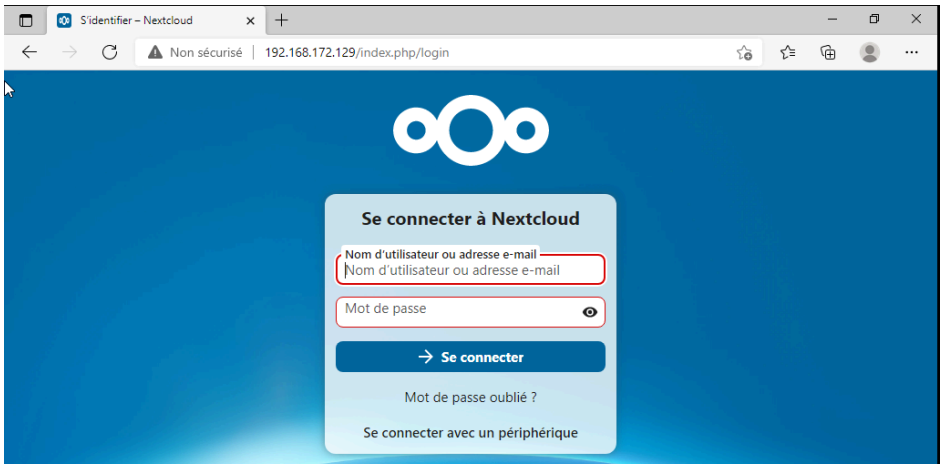
1. Où stocker vos fichiers ?

- Vous pouvez stocker vos fichiers en local sur votre pc.
- Pour partager vos dossiers avec vos collègues vous avez accès à un dossier "Partage", pour y accéder il suffit de taper dans la barre de votre explorateur de fichier le lien \\WIN-3GSBIDIQ6KE\partage.

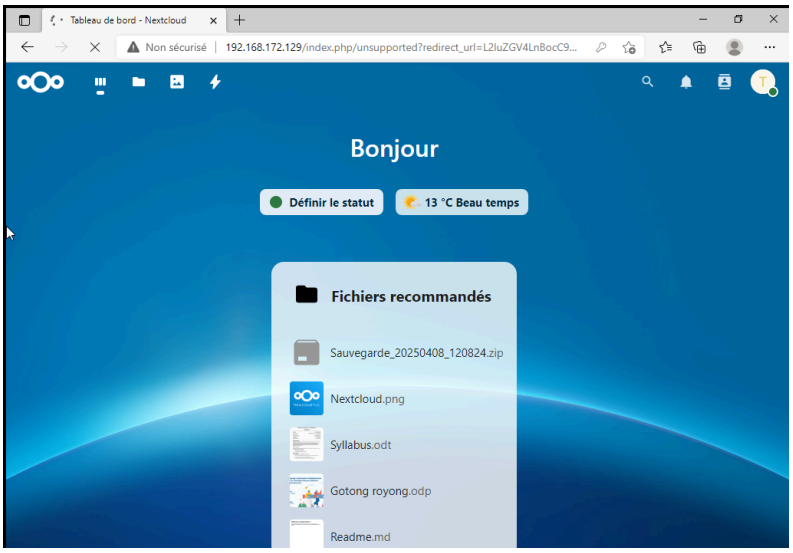


2. Accès à la sauvegarde

- En cas de perte de fichier, contactez l'administrateur.
- Les sauvegardes sont conservées sur un serveur sécurisé et dans le cloud via Nextcloud.
- Il est possible d'accéder sur le Nextcloud via l'adresse ip 192.168.172.129 et ensuite il faut renseigner votre identifiant et mot de passe fournis par l'administrateur informatique.



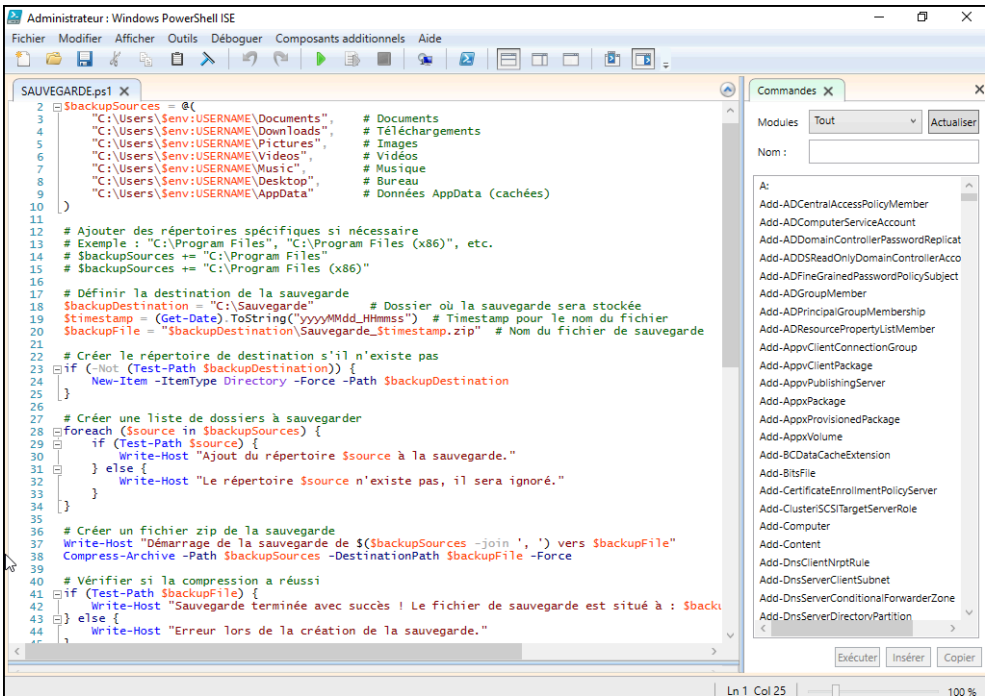
Ici vous pouvez voir l'interface d'accueil du Nextcloud :



L'accès au Nextcloud sera autorisé uniquement pour les directeurs d'entreprise, pour une question de données et de sauvegarde sensible.

3. Lancer le script de sauvegarde

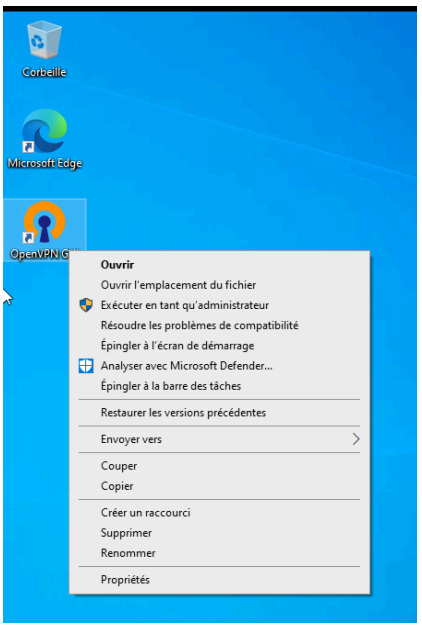
Pour exécuter ce script il suffit d'aller dans le dossier "partage" ou il se trouve et double cliquer pour l'exécuter.



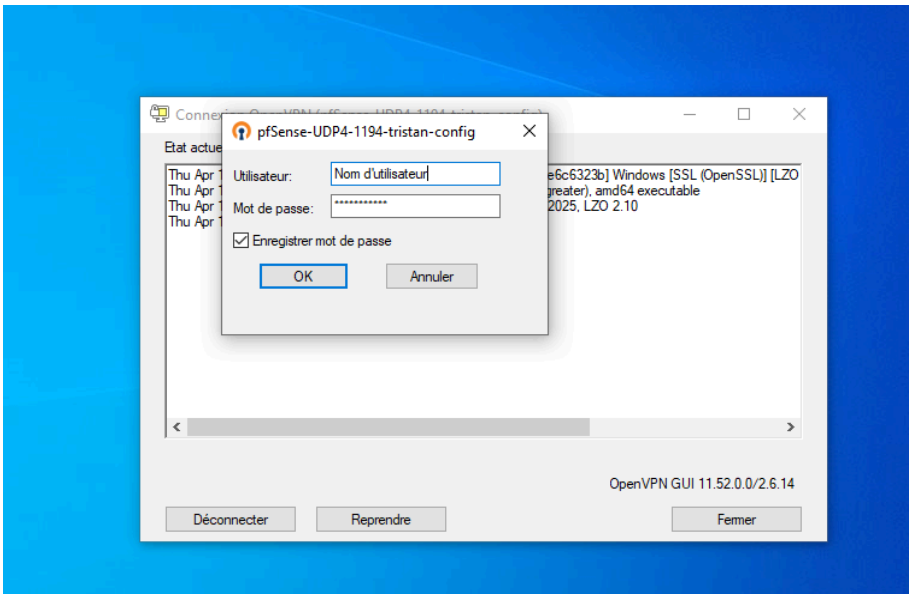
III. Accès à distance (télétravail)

1. Connexion VPN avec OpenVPN

- Pour ce connecter au VPN il suffit tout d'abord de double cliquer sur l'application "OpenVPN"

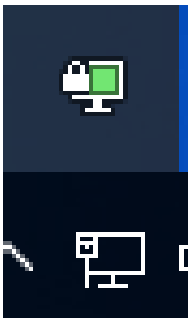


- Ensuite il vous demandera de vous identifier, donc avec l'identifiant et mot de passe fournis par l'administrateur lancer la connexion.



2. Une fois connecté

- Vous pouvez maintenant accéder aux fichiers partagés et aux services comme si vous étiez au bureau



IV. Utilisation du Wi-Fi invité (visiteurs)

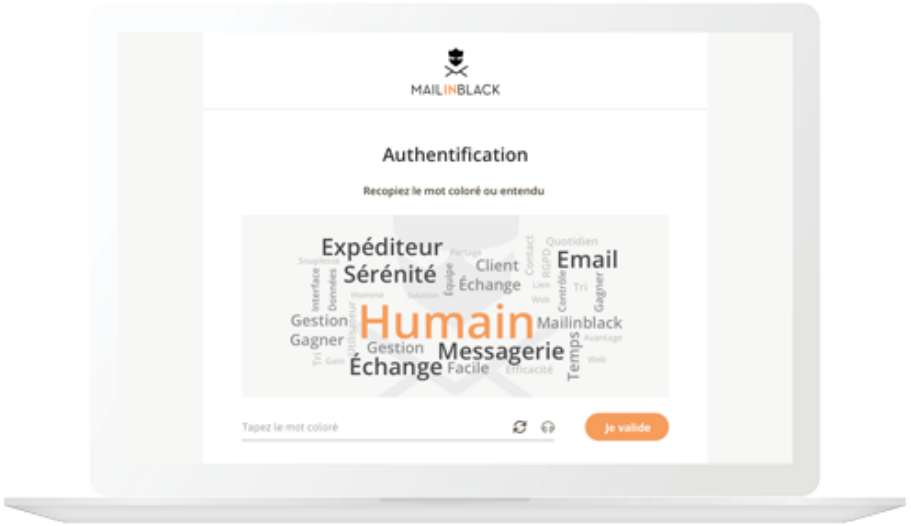
1. Connexion Wi-Fi Guest

- SSID (nom du réseau) : **GestionHorizons_Guest**
- Mot de passe : fourni par l'administrateur ou affiché à l'accueil
- Ce réseau donne uniquement accès à Internet, pas aux données internes

V. Accès à votre boîte mail (Mailinblack)

1. Accès à vos e-mails professionnels

- Vous disposez d'un filtre de sécurité via **Mailinblack** https://www.mailinblack.com/
- Lorsqu'un expéditeur inconnu vous écrit, il doit valider son identité
- Cela réduit considérablement le spam et les menaces

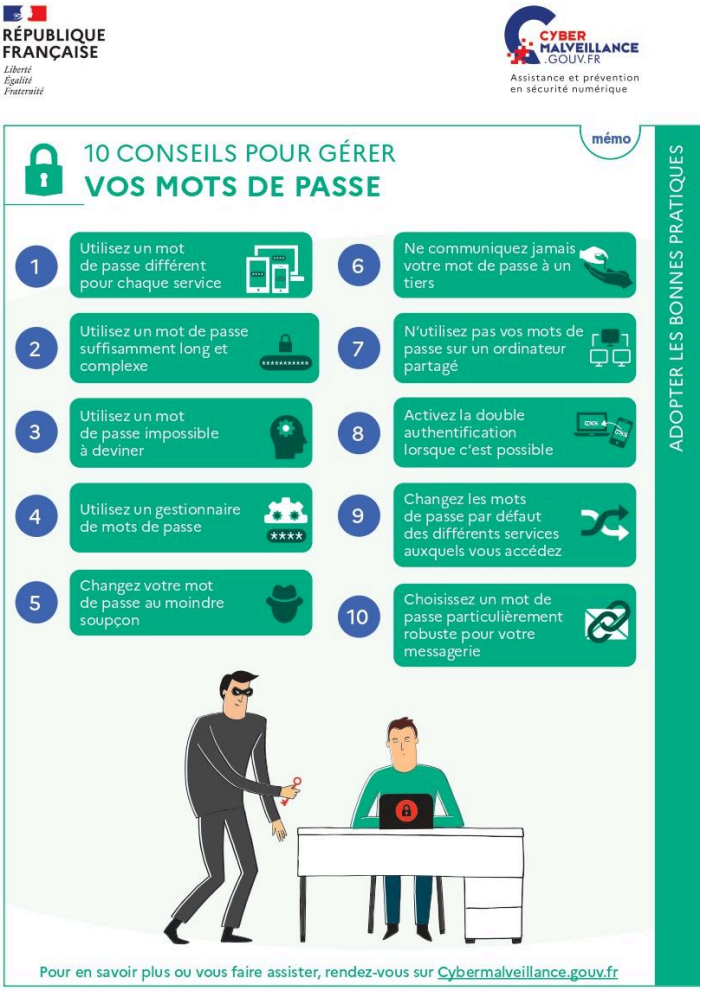


VI. Bonnes pratiques et sécurité

1. Conseils simples à suivre

Tiré des bonnes pratique de l'ANSI : https://cyber.gouv.fr/bonnes-pratiques-protegez-vous

- Gérez vos mots de passe avec soin



Il est important de verrouiller votre session à chaque fois que vous quittez votre bureau, vous pouvez pour cela faire un “Windows+L” qui verrouille votre pc automatiquement.

Soyez attentif aux mails extérieurs de l’entreprise que vous pouvez recevoir, si vous avez un doute sur la provenance du mail ne l’ouvrez pas, ne cliquez pas sur les liens qui y sont présents et n’ouvrez pas les pièces jointes.

Cela est de même pour un mail qui au premier abord a été envoyé par votre collègue depuis sa messagerie mais son discours semble incohérent ou douteux.

Dans ces deux cas, avertissez automatiquement votre administrateur informatique !

2. Formations internes

- Des sessions de **sensibilisation à la cybersécurité** sont prévues : votre présence est importante

Assistance technique

En cas de problème, contactez l’administrateur informatique.