Organisation du contrôleur de domaine

Table des matières /

Vous pouvez ajouter des titres (Format > Styles de paragraphe) qui apparaîtront dans votre table des matières.

Introduction :
Ce document décrit l'organisation du contrôleur de domaine (DC) nouvellement mis en place dans l'entreprise. Il détaille le choix des logins, les stratégies de sécurité des mots de passe, l'organisation des Unités Organisationnelles (UO), des groupes, et fournit une liste des utilisateurs prévus.

1. Choix de login

Les logins des utilisateurs sont standardisés pour garantir l'unicité et la cohérence. Le format adopté est le suivant :

[Initiale du prénom][Nom de famille]

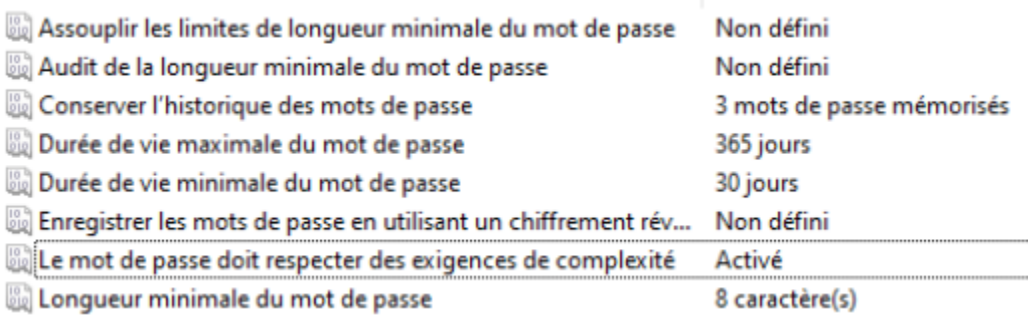
exemple :
Jean Dupont → jdupont
Marie Curie → curie

En cas de doublons, un chiffre est ajouté à la fin : (jdupont1, jdupont2…)

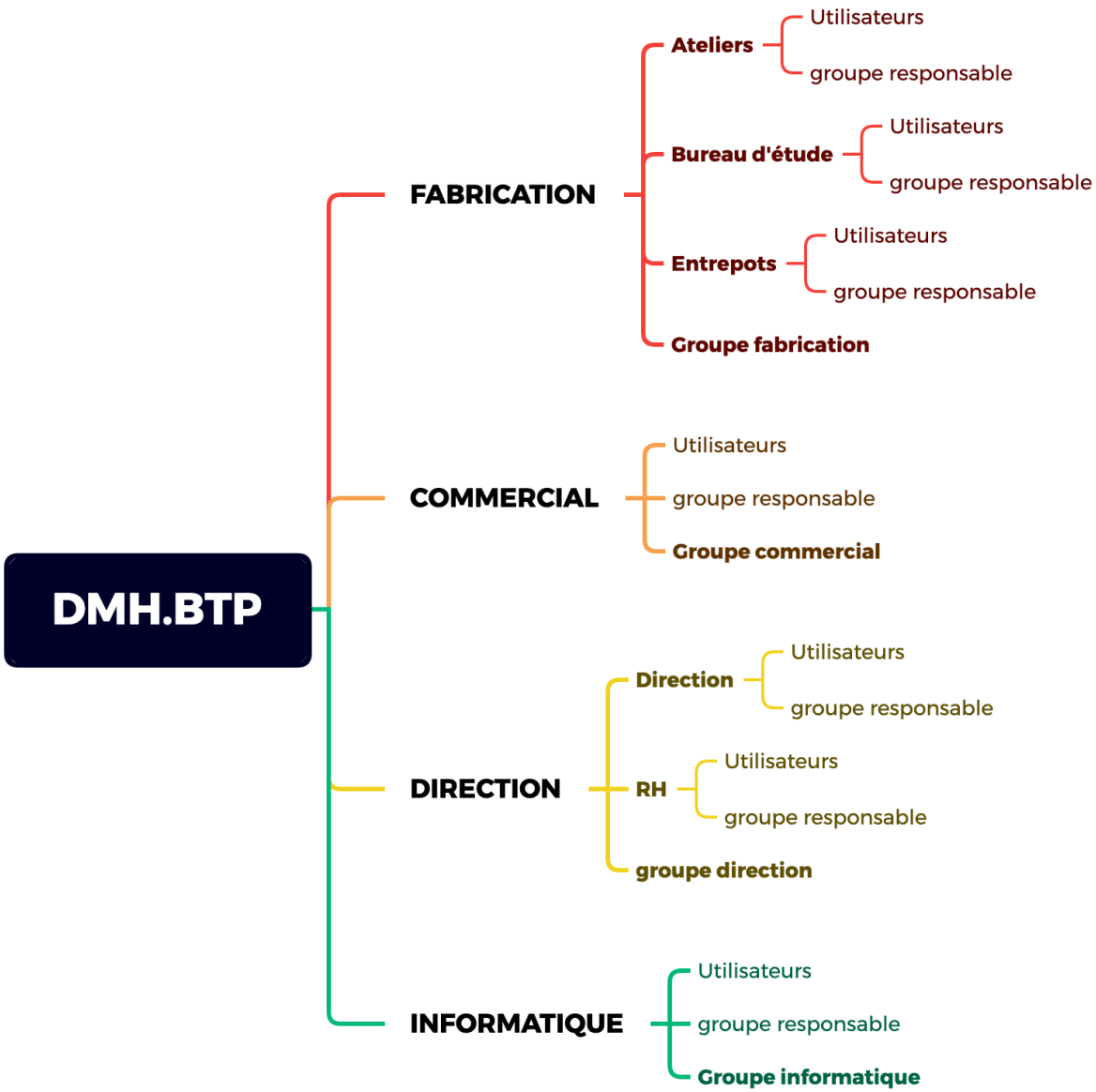
2. choix de stratégie de mots de passe

Pour des besoins de praticité, une politique de mots de passe simplifié a tété mise en place en pré-production

- Longueur minimale : 8 caractères.
- Complexité : le mot de passe doit contenir au moins 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial.
- Expiration : Tous les ans.
- Historique : empêche la réutilisation des 3 derniers mots de passe.



3. organisation Unités d'organisation / Groupes



(outdated)
Chaque UO possède un groupe du responsable du service avec comme membre les responsables.

4. Liste des utilisateurs

Des utilisateurs de test ont été mis en place afin de faire des tests du point de vue des futurs utilisateurs.

- Administrateur : pour toute la configuration des postes et du windows server
- fab fab : utilisateur pour fabrication

- ate ate : utilisateur pour atelier
- bur bur : utilisateur pour bureau d'étude

…

- ldap : utilisateur pour la connexion openVPN / LDAP en tout genre
- test : utilisateur test avec moins de droits

De réelles utilisateurs peuvent être ajoutés via le script d'ajout d'utilisateurs.

5. Arborescence des fichiers de partage