

# Compte Rendu PRA

(Valentin RYCKAERT, Louis BRUNET-LECOMTE, Lucas POURRERON)

## Contexte

Une architecture est mise en place :

- BATIMENT A :
  - client windows 11
  - AD windows server
- BATIMENT B :
  - serveur web Fedora Server hébergeant une stack docker WordPress / MariaDB
  - RODC de l'AD
  - client windows 11

Roles dans l'entreprise :

- 1 développeur (Valentin)
- 2 administrateurs systèmes (Lucas, Louis)

Mise en place d'un état des lieux régulier par le développeur pour vérifier le bon fonctionnement de l'infrastructure.

## Etat des lieux du dimanche 16 février

10h00 : l'état des lieux est effectué, rien d'anormal remarqué

11H50 : nouvel état des lieux avec l'administrateur systèmes (Louis) pour un problème de connection au WordPress

12H15 : le développeur remarque l'impossibilité de se connecter aux deux machines clientes windows 11, les mots de passe ont été modifiés.



**Valentin**

The password is incorrect. Try again.

OK

Déclanchement du PRA pour l'impossibilité de connexion aux sessions windows.

12H20 : L'administrateur systèmes (Louis) se connecte à l'AD avec le compte administrateur, qui n'a pas été modifié.

# Your info

You need to activate Windows before you can personalize your PC.

[Activate Windows now.](#)



**BURGER\ADMINISTRATOR**

BURGER\Administrator  
Administrator



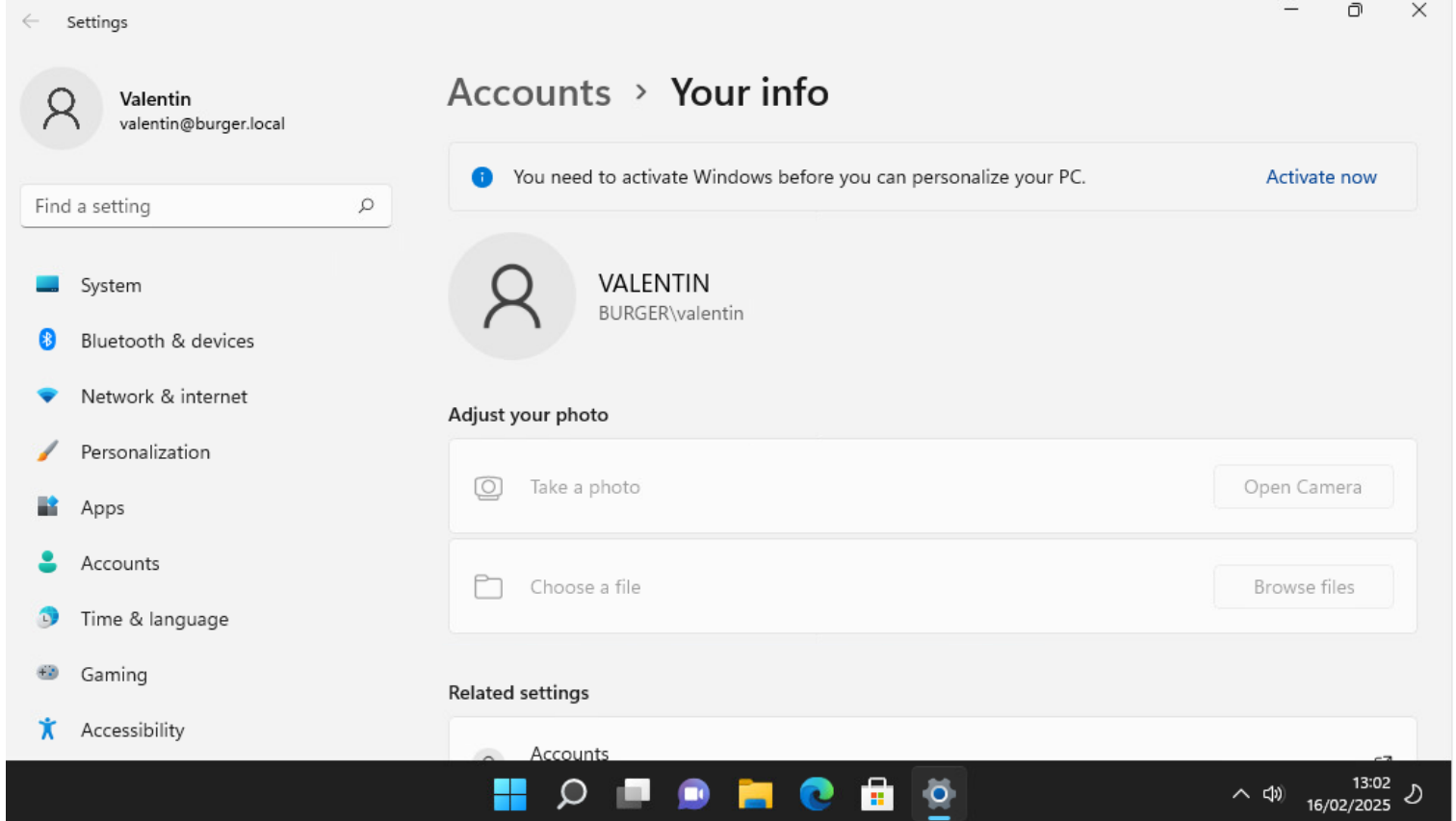
Il restaure un à un les mots de passe des utilisateurs

```
Set-ADAccountPassword -Identity "Louis" -NewPassword (ConvertTo-SecureString  
"123456789+Aze" -AsPlainText -Force) -Reset
```

```
Set-ADAccountPassword -Identity "Lucas" -NewPassword (ConvertTo-SecureString  
"123456789+Aze" -AsPlainText -Force) -Reset
```

```
Set-ADAccountPassword -Identity "Valentin" -NewPassword (ConvertTo-SecureString  
"123456789+Aze" -AsPlainText -Force) -Reset
```

Le deuxième administrateur n'étant pas joignable, c'est le développeur qui se charge de vérifier dans le même temps le bon fonctionnement de chaque compte



12H45 : Tous les utilisateurs sont de nouveau utilisables

13H00 : rédaction de ce compte rendu terminée.

## Analyse

### Le problème n'a pas été remarqué lors des états des lieux du samedi et du dimanche matin

L'administrateur systèmes (Louis) se connectait avec le compte administrateur pour vérifier l'état de l'AD, tandis que le développeur n'avait pas une assez bonne connaissance de l'architecture pour l'analyser correctement.

#### solution

Les états des lieux seront effectués à l'avenir les deux administrateurs systèmes, qui ont une meilleure connaissance de l'infrastructure. Ils vérifieront l'état des machines clientes

### L'un des administrateurs systèmes n'était pas joignable

Le PRA indiquait que le deuxième administrateur devait vérifier le bon fonctionnement des comptes, mais ne prévoyait pas un remplaçant en cas d'absence.

#### solution

Le PRA sera changé pour que le développeur remplace le second administrateur en cas d'absence dans ce genre de situation. Si le développeur est aussi absent, l'administrateur restant se chargera de restaurer

puis tester seul chaque compte utilisateur.

## **Oubli de déconnecter l'AD du réseau**

Le PRA indiquait qu'il fallait déconnecter l'AD du réseau.

### **solution**

Même si cela n'a pas été nécessaire ici, il faudra à l'avenir penser à le faire pour éviter une exposition dangereuse.

## **Restauration des mots de passe et de leur vérification simultanée**

Ceci n'était pas prévu par le PRA, mais cela a permis de gagner une dizaine de minutes.

### **solution**

Ajout dans le PRA de la possibilité de faire ces deux actions en simultané