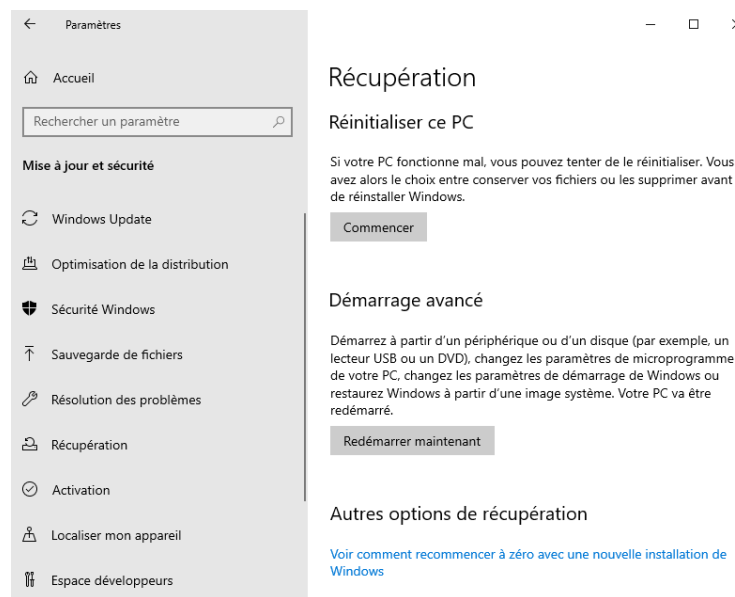


TP 1 : Réinitialiser un PC virtuel :

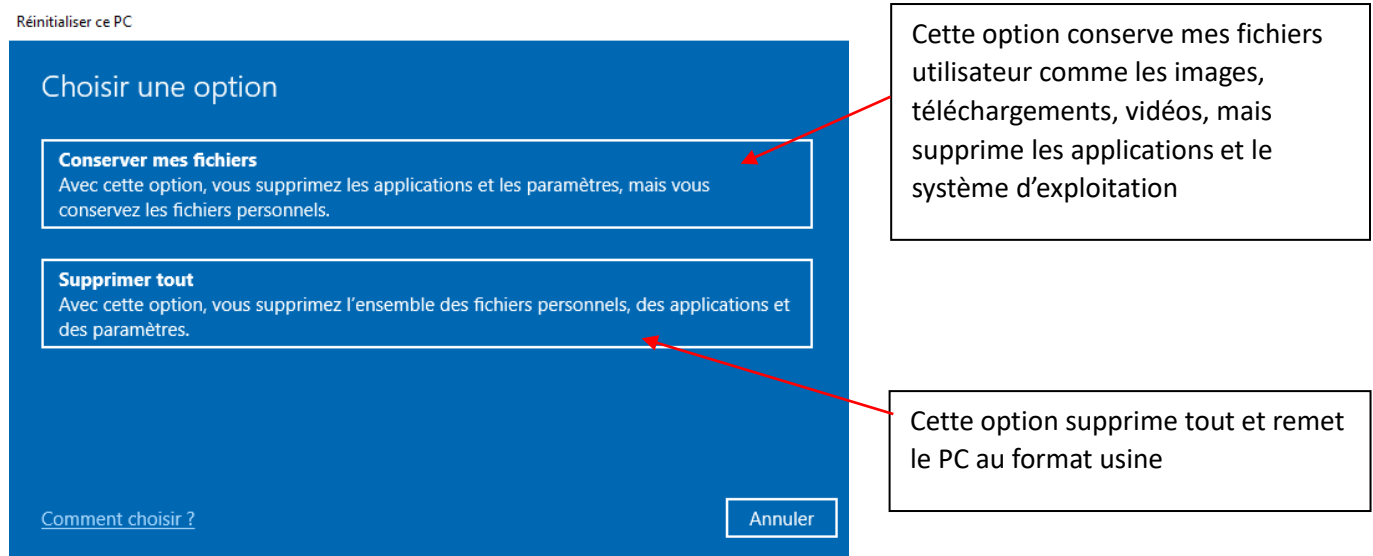
Contexte : Un employé a installé des logiciels malveillants, rendant le système instable.

Objectif : Tester les deux options de réinitialisation sur une machine virtuelle.

On se rend dans les paramètres « Mise à jour et sécurité » du pc que l'on veut réinitialiser.



Après cela nous avons 2 options :

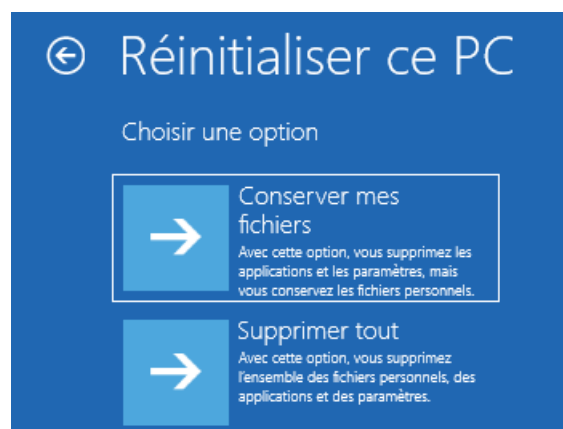
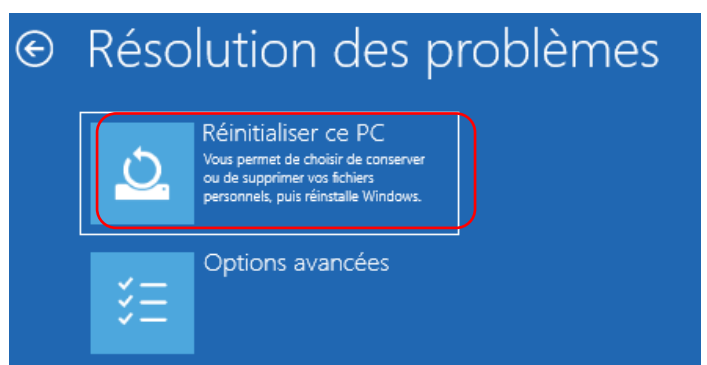
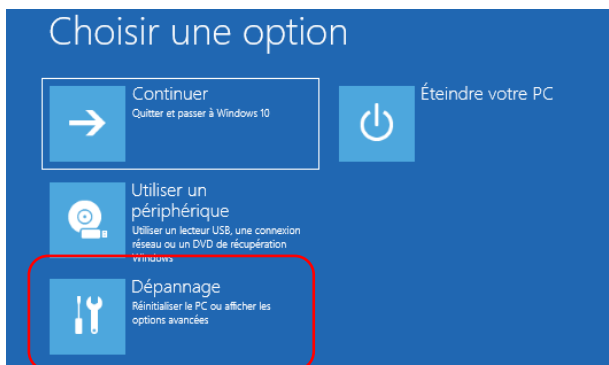
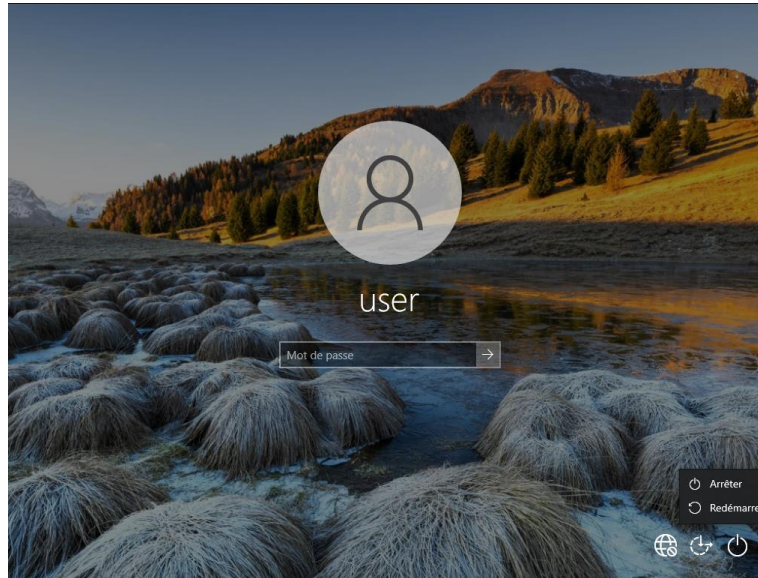


Cette option conserve mes fichiers utilisateur comme les images, téléchargements, vidéos, mais supprime les applications et le système d'exploitation

Cette option supprime tout et remet le PC au format usine

Si on n'est pas connecté à la session, on peut ouvrir ce menu de réinitialisation sur la page de connexion Windows.

On reste appuyé sur la touche shift tout en cliquant sur « Redémarrer ».

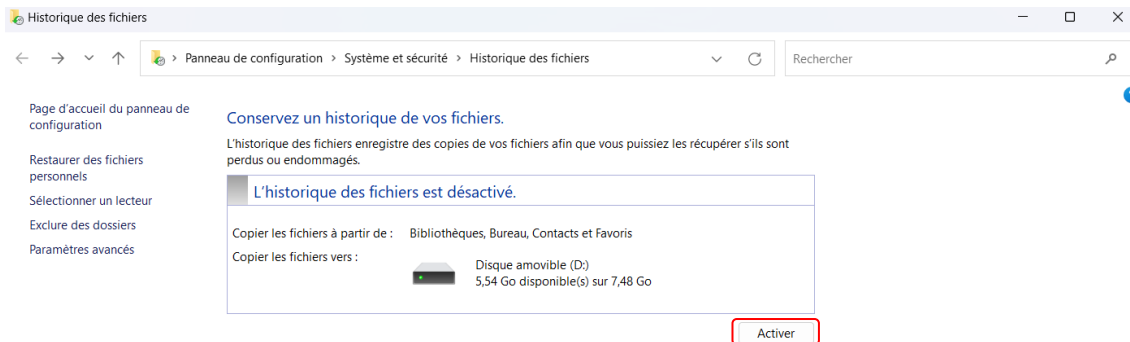


TP 2 : Configurer l'historique des fichiers

Contexte : l'entreprise XYZ veut protéger les fichiers critiques de son service RH.

Objectif : Configurer une sauvegarde avec historique des fichiers sur un disque externe.

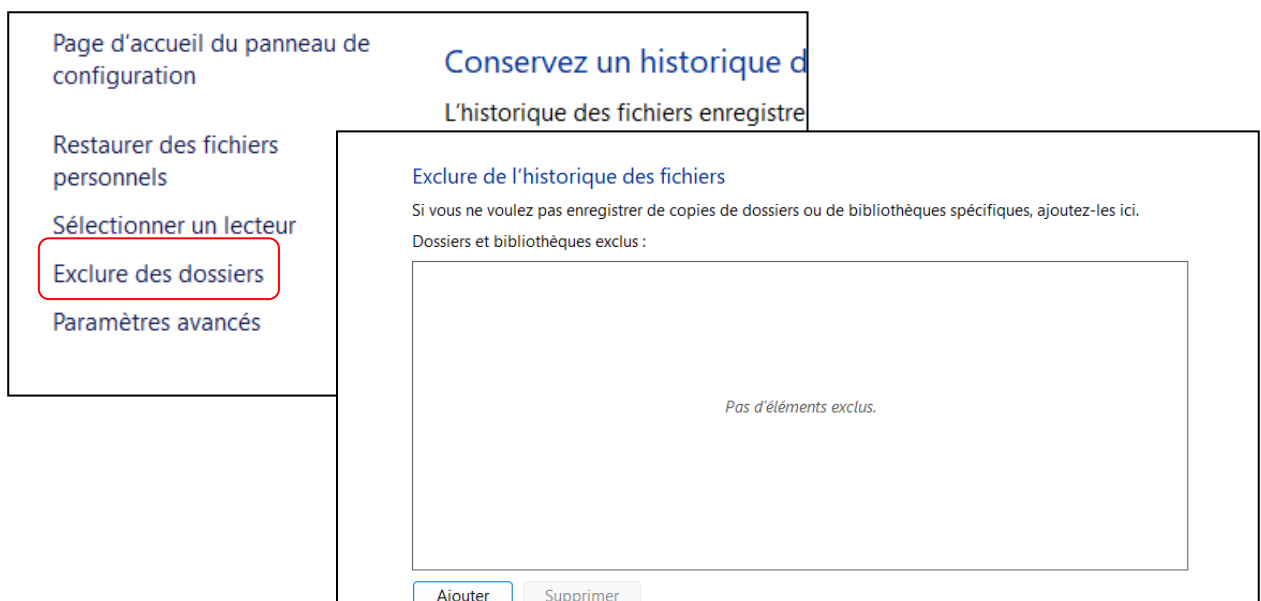
Pour effectuer un historique de fichier on se rend dans la barre de recherche du menu démarrer et on saisit « Historique des fichiers ».



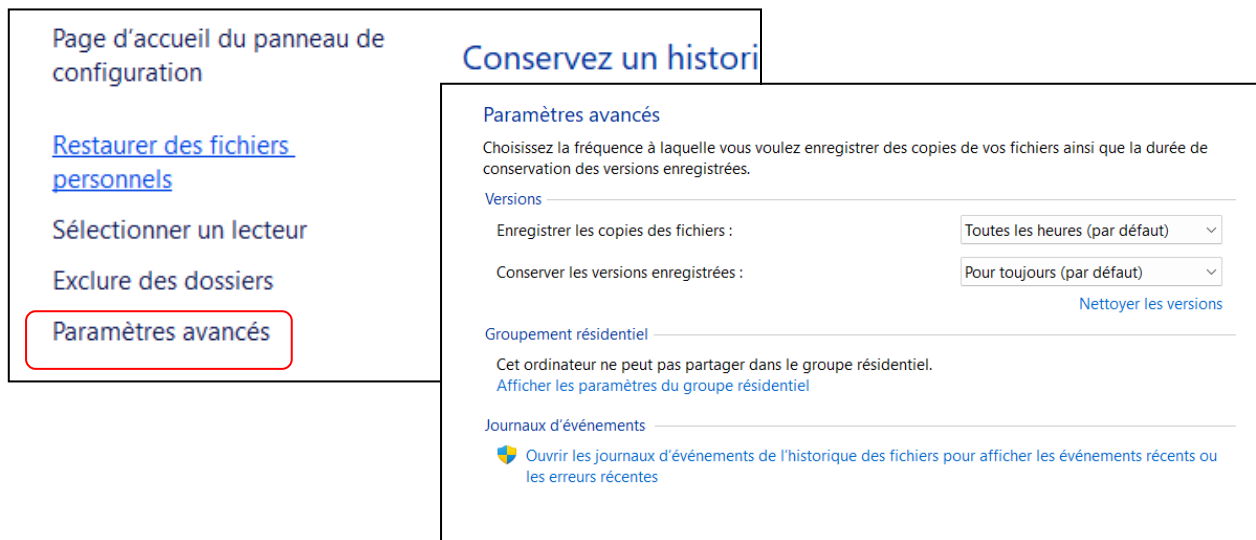
J'ai le choix de sélection entre un dossier partagé réseau et un disque externe dans mon cas je souhaite utiliser une clé USB ou un disque dur.

Je commence par activer et la clé USB va stocker tous les fichiers de mon espace utilisateur.

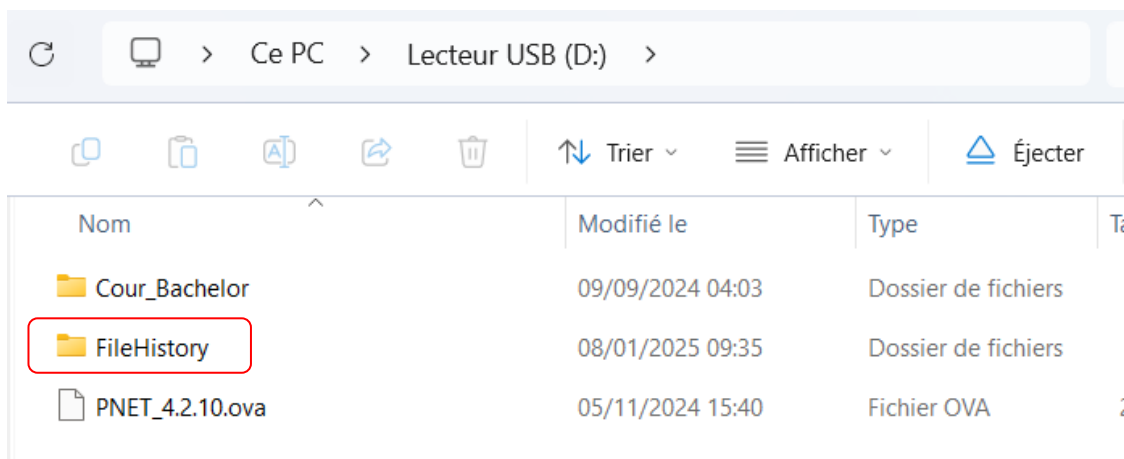
On peut définir manuellement les dossiers que l'on veut exclure de la sauvegarde



Ici on peut définir la fréquence de sauvegarde des fichiers, c'est-à-dire que l'on définit à quelle fréquence les fichiers sont sauvegardés.



Je peux voir ensuite que ma clé USB a bien stocké une sauvegarde de mes fichiers utilisateurs



TP3 : Sauvegarde avec Veeam Agent

Contexte : Une entreprise veut protéger ses fichiers critiques sur un poste Windows.

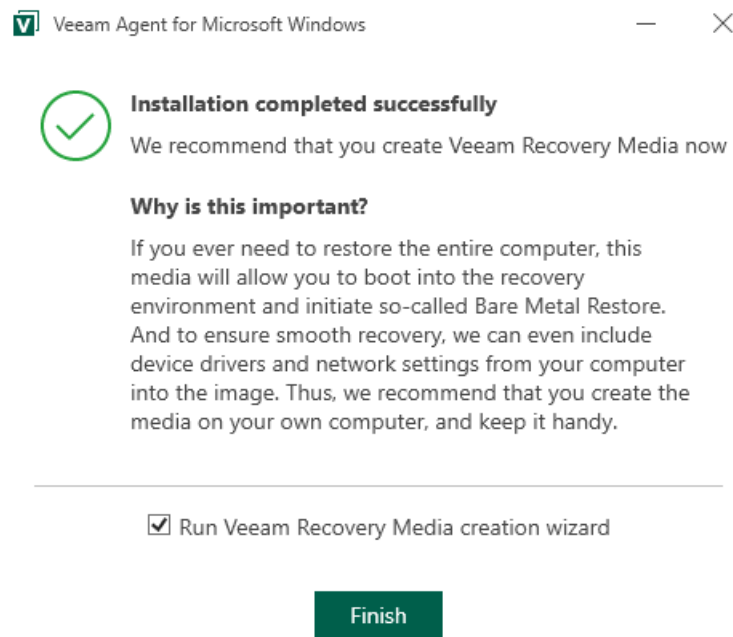
Objectif : Configurer une sauvegarde automatique avec le logiciel Veeam Agent.

1/ On se rend sur le site de Veeam Agent afin d'obtenir le fichier d'installation de Veeam

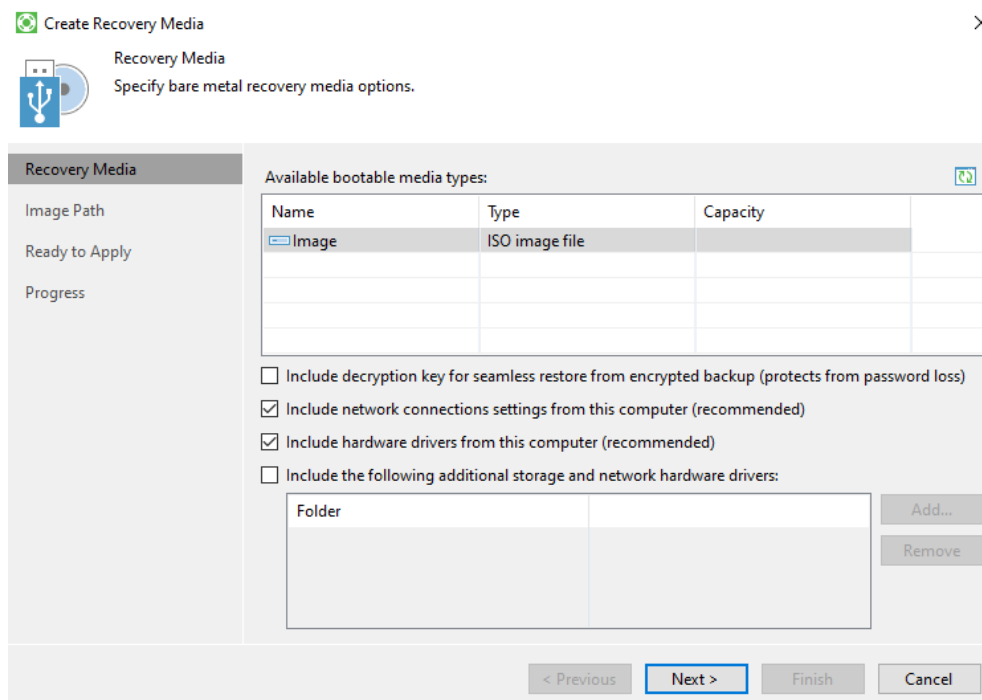
<https://www.veeam.com/fr>

Il faut créer un compte afin d'obtenir ce fichier.

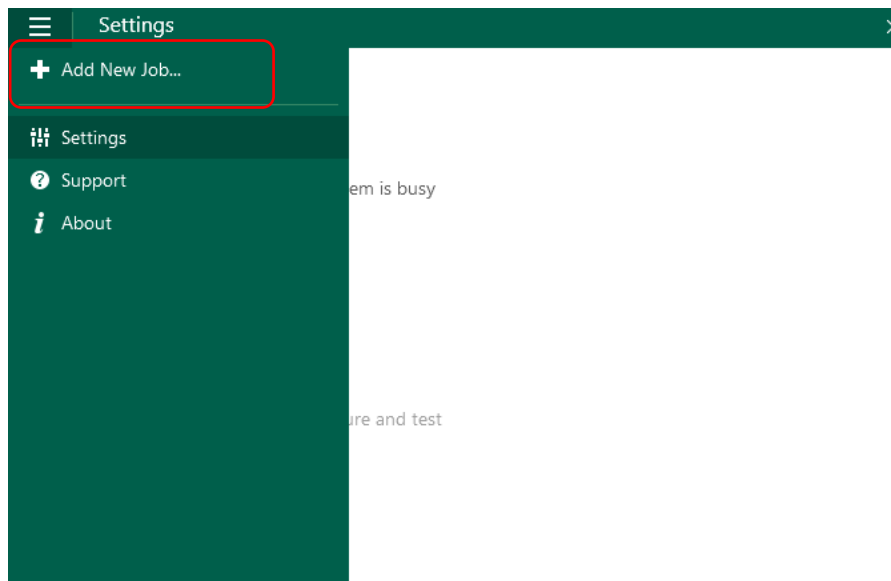
Une fois ce fichier téléchargé on lance l'application et on arrive sur cette page.



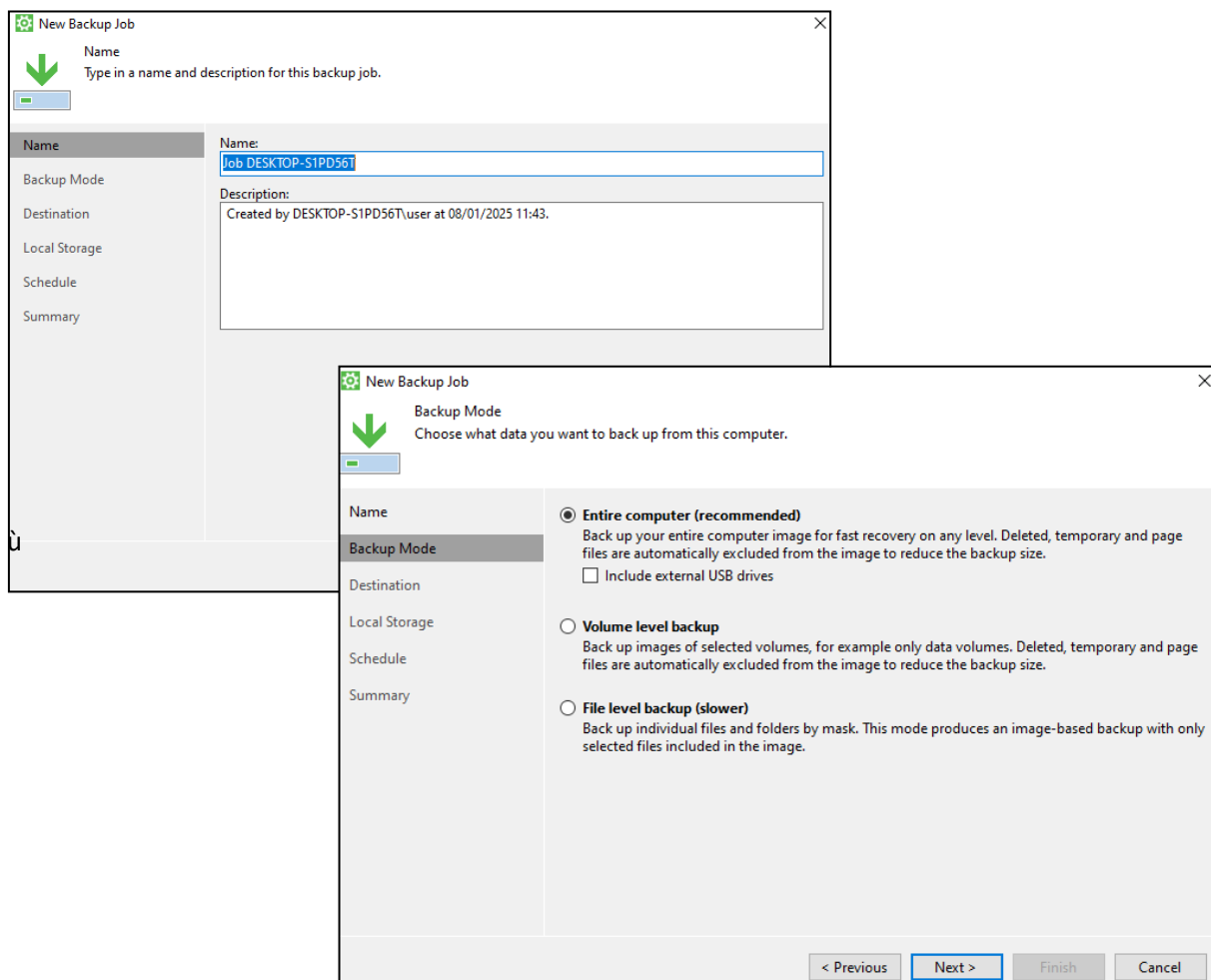
On passera l'Etape du recovery média pour cette procédure car elle sert de capture d'image sur le PC. L'option « include the following additional ... » permettra de capture l'iso des disques externes connectés sur les ports du PC.



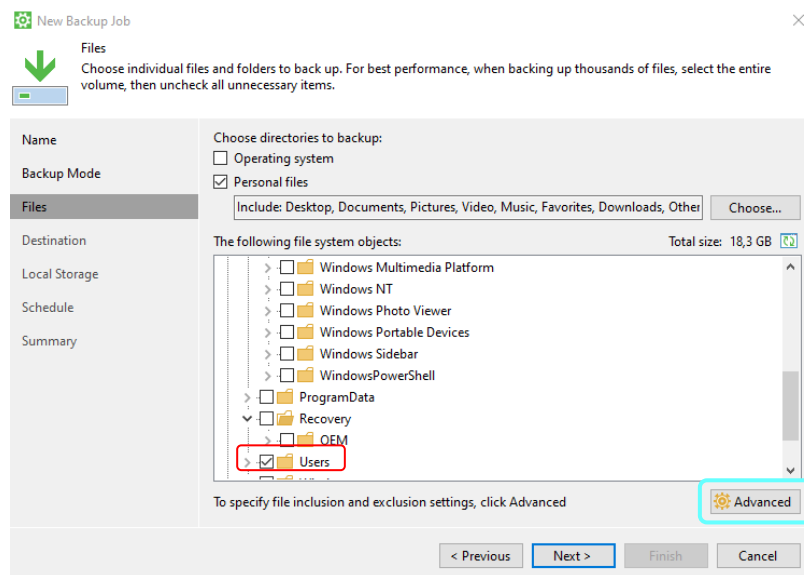
On ouvre dans la barre de recherche « Veeam agent for microsoft ». Une fois l'application lancée on sélectionne « Add New job »



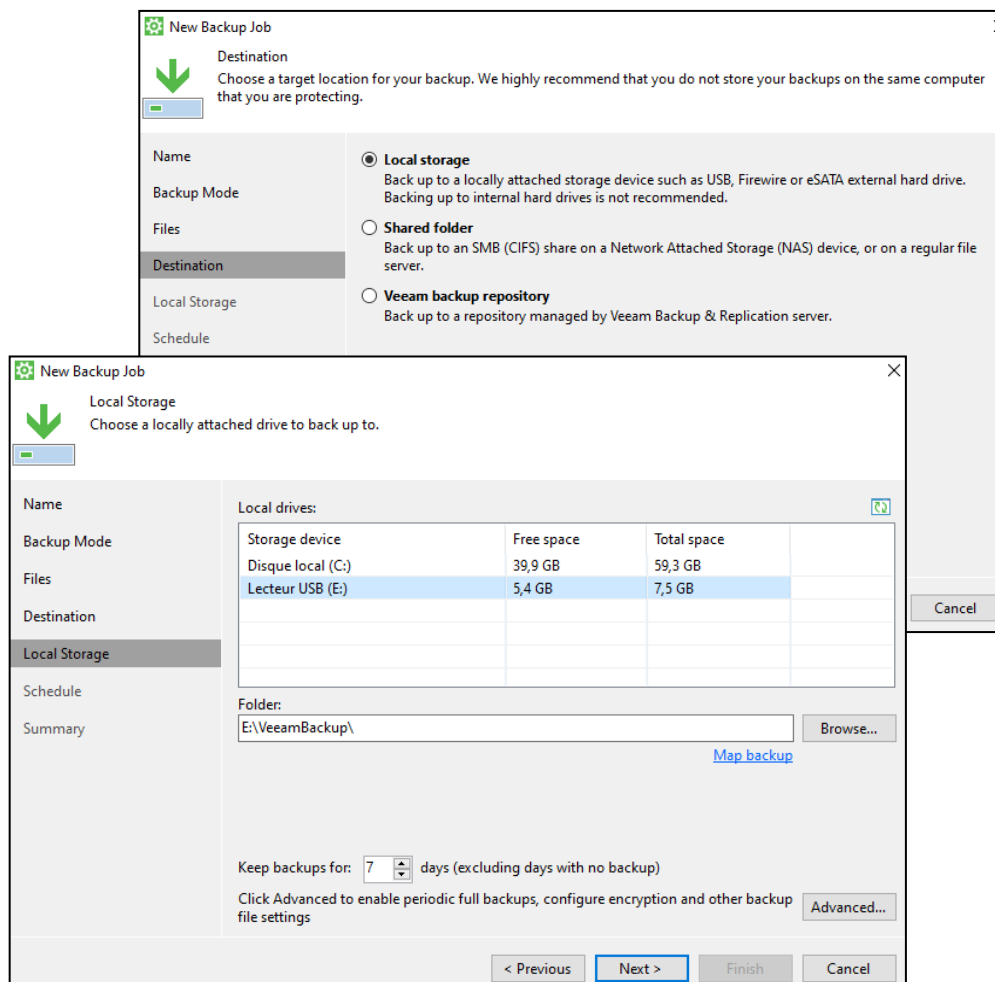
Ici on peut choisir le nom que l'on veut donner au backup, et sur la deuxième image, le mode de sauvegarde que l'on veut. Tout dépend du besoin.



Ensuite on sélectionne les dossiers que l'on veut inclure dans la sauvegarde. Dans mon cas je choisis uniquement mon dossier utilisateur pour l'exemple.



Ensuite j'appuie sur « **Local storage** » où je sélectionnerai ma clé USB pour stocker la sauvegarde. D'autres moyens sont proposés mais dans mon cas je sélectionne ma clé USB mais j'aurai pu utiliser un dossier partagé. Dans « **Advanced** » nous avons la possibilité de programmer une sauvegarde périodiquement.



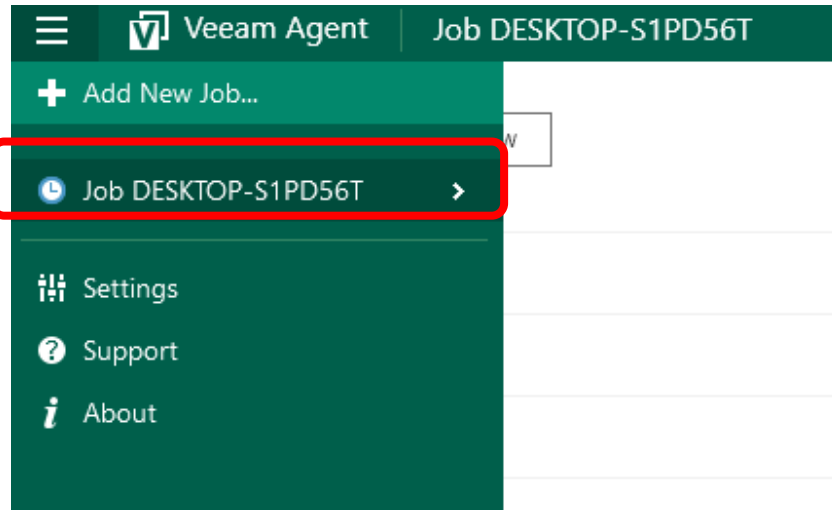
Ensuite on peut ajouter des options spécifiques concernant la sauvegarde. Si on sauvegarde au démarrage, tous les jours etc.

The screenshot shows the 'New Backup Job' window with the 'Schedule' tab selected. The left sidebar lists 'Name', 'Backup Mode', 'Files', 'Destination', 'Local Storage', 'Schedule', and 'Summary'. The 'Schedule' tab is active, showing options for periodic backups. The 'Periodically' section is expanded, showing a checkbox for 'Daily at' (checked), a time of '00:30', and a frequency of 'Everyday'. Below this, there are dropdown menus for 'If computer is powered off at this time' (set to 'Backup once powered c') and 'Once backup is taken, computer should' (set to 'Keep running'). The 'At the following events' section has checkboxes for 'Lock', 'Log off', and 'When backup target is connected' (all unchecked). There is also an option for 'Eject removable storage once backup is completed (ransomware protection)' which is unchecked. A 'Back up no more often than every' section shows '2' hours. At the bottom, there are buttons for '< Previous', 'Apply', 'Finish', and 'Cancel'.

Arrivé au résumé on peut sélectionner « **Finish** » et décider d'activer le « **job** » en cochant la case.

The screenshot shows the 'New Backup Job' window with the 'Summary' tab selected. The left sidebar lists 'Name', 'Backup Mode', 'Files', 'Destination', 'Local Storage', 'Schedule', and 'Summary'. The 'Summary' tab is active, showing a summary of the backup job. The 'Summary' section contains the text: 'Backup job was created successfully.' Below this, there are sections for 'General' (Backup job name: Job DESKTOP-S1PD56T, Backup job description: Created by DESKTOP-S1PD56T\user at 08/01/2025 14:19), 'Source' (Backup mode: file level backup, Included items: Desktop, Documents, Pictures, Video, Music, Favorites, Downloads, Other files and folders, Disque local (C:)), and 'Excluded items'. At the bottom, there is a checkbox labeled 'Run the job when I click Finish' which is unchecked. Below the checkbox, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a red box.

Et enfin on retrouve le job que l'on vient de créer.



TP N°4 : Sauvegarde avec Veeam Agent

Contexte : Une entreprise veut protéger ses fichiers critiques sur un poste Windows.

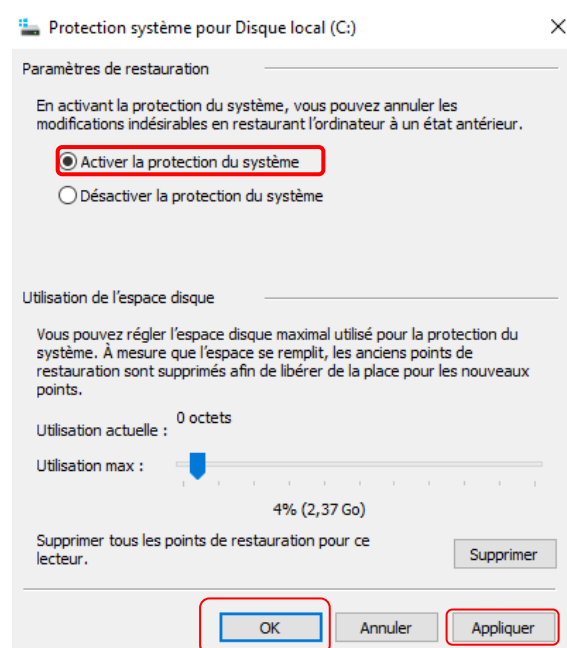
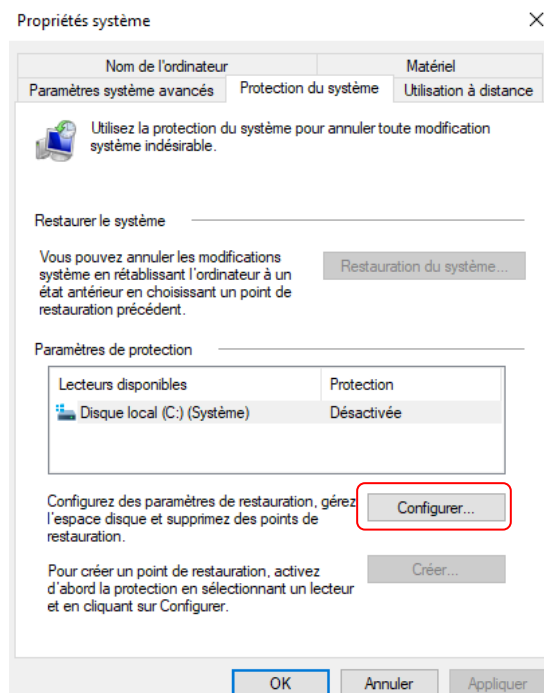
Objectif : Configurer une sauvegarde automatique avec le logiciel Veeam Agent.

On saisit dans la barre de recherche « **Point de restauration** ». On appuie sur configurer

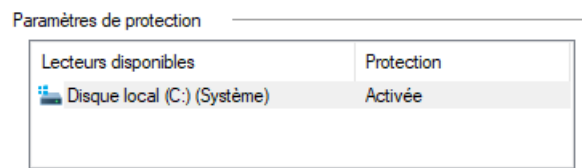
Il suffit d'activer la protection du système et de choisir un pourcentage (%) d'utilisation du

Disque qui correspond au nombre de mo/go qui sera pris par ce point de restauration. On choisit un

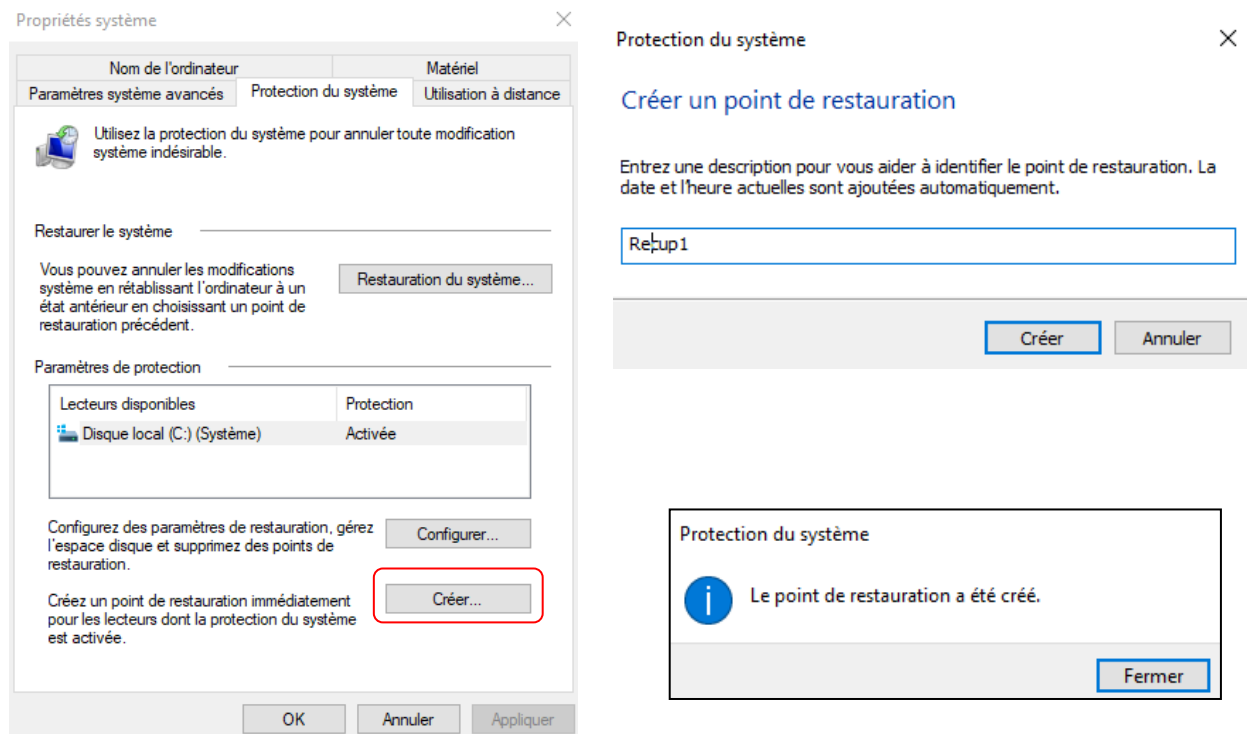
Pourcentage et on appuie sur appliquer.



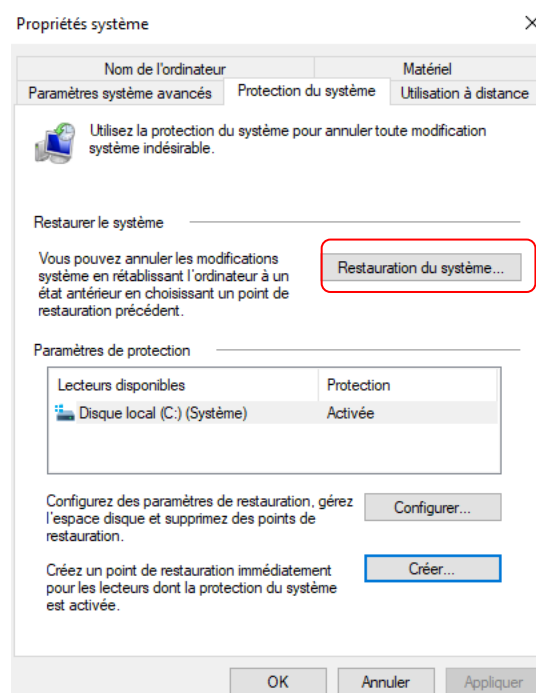
La protection est ensuite activée

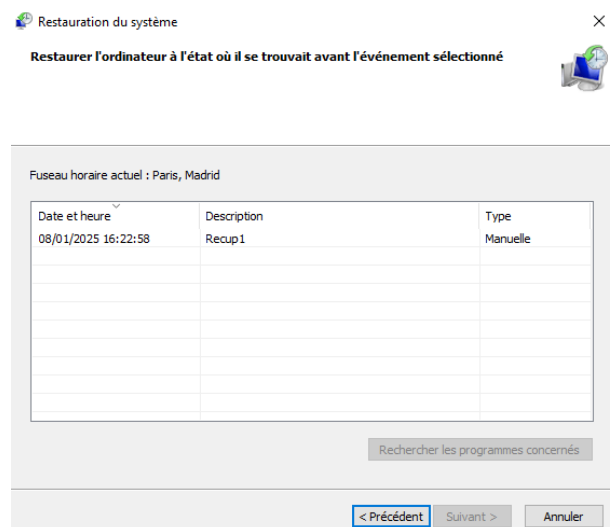
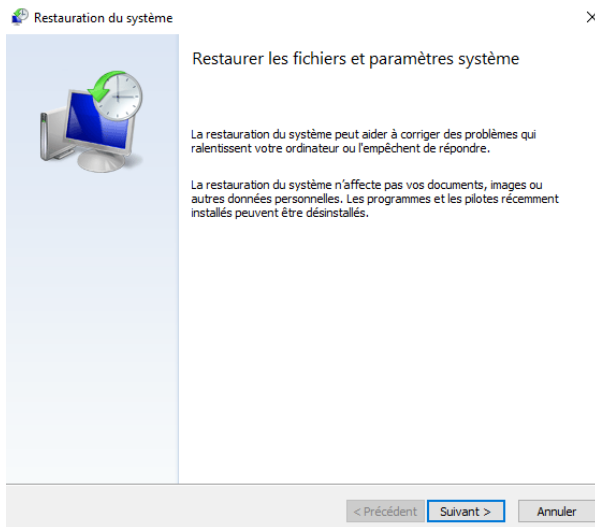


Ensuite on crée un point de restauration

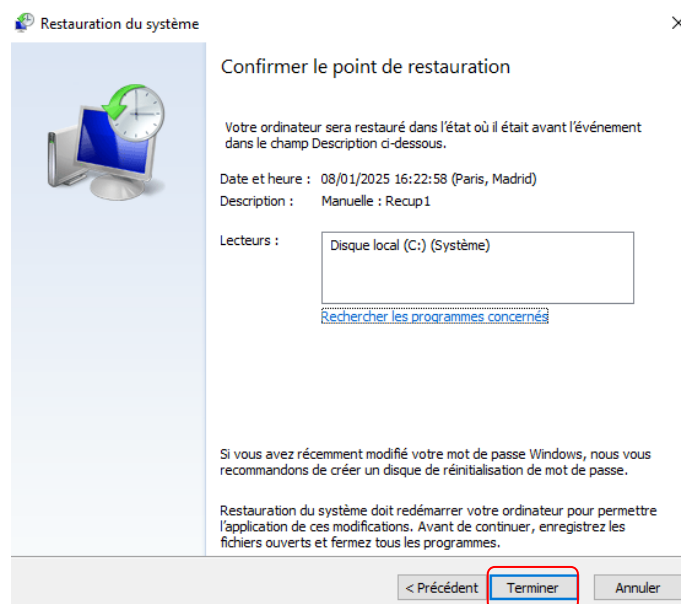


On peut ensuite utiliser la restauration du système





On clôture avec le bouton « terminer ».



TP N°5 : Utilisation de BCD

Contexte : Une machine dual-boot affiche des problèmes lors du démarrage. Le

Technicien doit inspecter et corriger les entrées BCD.

Objectif : Découvrir et manipuler les entrées BCD avec des commandes simples.

Gestion du BCD avec bcdedit :

→ **bcdedit /enum**

Affiche les entrées actuelles du BCD.

→ **bcdedit /set {ID} description « Nouveau nom »**

Change la description d'une entrée.

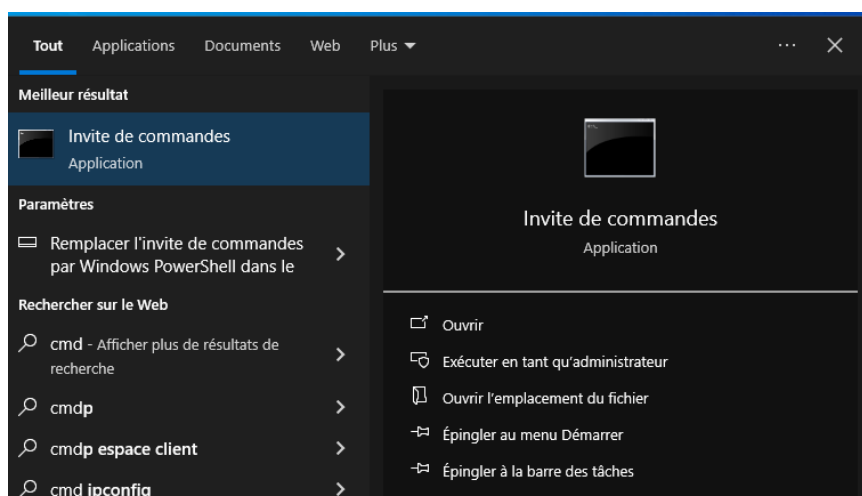
→ **bcdedit /delete {ID}**

Supprime une entrée du BCD.

→ **bcdedit /default {ID}**

Définit l'entrée par défaut pour le démarrage.

On commence par exécuter l'invite de commande en mode administrateur.



Après avoir saisi la commande « `bcdedit /enum` », je peux voir 2 entrées telles que `bootmgr` et `current`.

```
C:\Windows\system32>bcdedit /enum

Gestionnaire de démarrage Windows
-----
identificateur    {bootmgr}
device            partition=\Device\HarddiskVolume1
path              \EFI\Microsoft\Boot\bootmgfw.efi
description       Windows Boot Manager
locale            fr-FR
inherit           {globalsettings}
default           {current}
resumeobject      {1e0d7fce-b7c7-11ef-889f-ff393af5bd09}
displayorder      {current}
toolsdisplayorder {memdiag}
timeout           30

Chargeur de démarrage Windows
-----
identificateur    {current}
device            partition=C:
path              \Windows\system32\winload.efi
description       Windows 10
locale            fr-FR
inherit           {bootloadersettings}
recoverysequence  {1e0d7fd0-b7c7-11ef-889f-ff393af5bd09}
displaymessageoverride CommandPrompt
recoveryenabled   Yes
isolatedcontext   Yes
allowedinmemorysettings 0x15000075
```

Avec les différentes commandes vu précédemment je peux interagir avec le gestionnaire de démarrage en supprimant une entrée, en définissant une entrée par défaut.

Pour l'exemple je vais me contenter de changer la description d'une entrée.

```
C:\Windows\system32>bcdedit /set {current} description essai1
L'opération a réussi.
```

Cette commande à bien changé la description de **{current}**

```

identificateur {current}
device         partition=C:
path           \Windows\system32\winload.efi
description    essai1
locale        fr-FR
inherit        {bootloadersettings}
recoverysequence {1e0d7fd0-b7c7-11ef-889f-ff393af5bd09}
displaymessageoverride CommandPrompt
recoveryenabled Yes
isolatedcontext Yes
allowedinmemorysettings 0x15000075
osdevice       partition=C:
systemroot     \Windows
resumeobject   {1e0d7fce-b7c7-11ef-889f-ff393af5bd09}
nx             OptIn
bootmenupolicy Standard

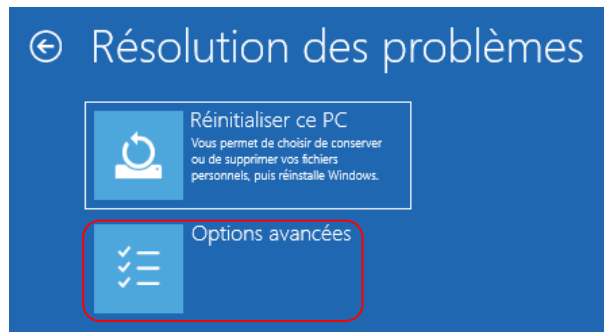
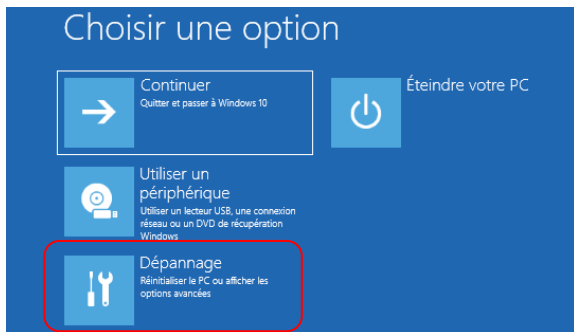
```

TP N°6 : Exploration de Windows RE

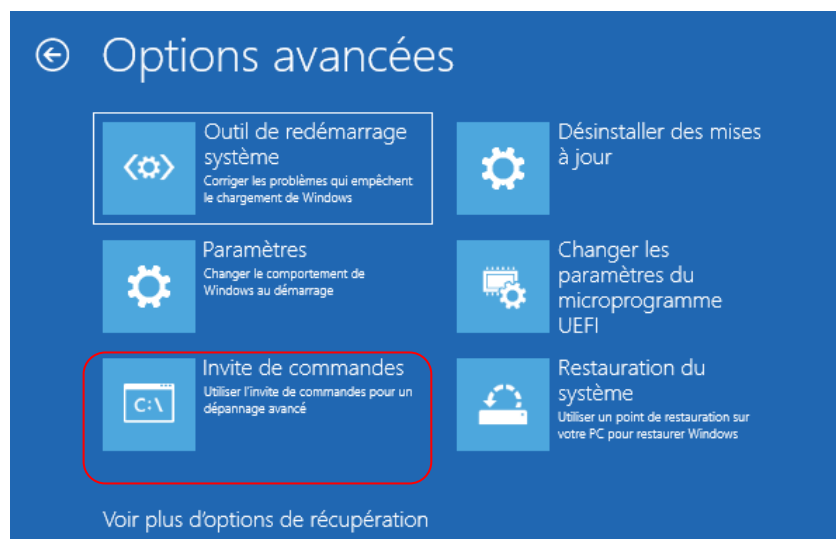
Contexte : Une entreprise constate que certains ordinateurs ne démarrent plus après une mise à jour importante.

Objectif : Diagnostiquer et résoudre un problème de démarrage via WindowsRE.

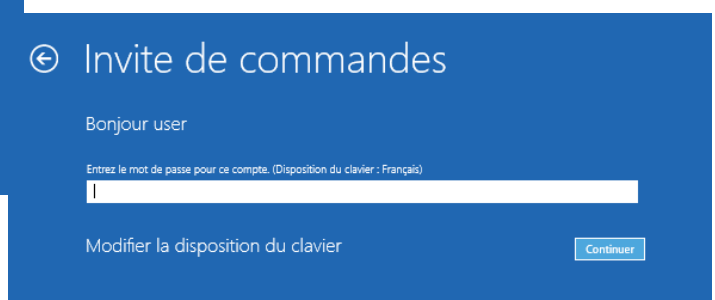
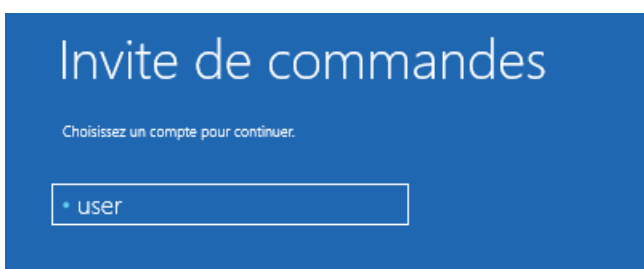
On rend dans menu de WindowsRE. On peut s'y rendre en restant appuyé sur shift + redémarrage.



On navigue jusqu'à options avancées et on sélectionne « Invite de commandes »



Le PC redémarre et nous devons nous connecter en sélectionnant l'utilisateur et le mot de passe associé



L'invite de commande est lancée et on saisira la commande « **chkdsk c : /f** » et cette commande nous affichera ce résultat.

```
Administrateur: X:\windows\system32\cmd.exe
Microsoft Windows [version 10.0.19041.1]
(c) 2019 Microsoft Corporation. Tous droits réservés.

X:\windows\system32>chkdsk c: /f
Le type du système de fichiers est NTFS.

Étape 1 : Examen de la structure du système de fichiers de base...
135424 enregistrements de fichier traités.                               reste : 0:00:04
La vérification des fichiers est terminée.
Durée de la phase (Vérification des enregistrements de fichiers) : 1.74 secondes.
2216 enregistrements de grand fichier traités.                          n reste : 0:00:04 .
Durée de la phase (Récupération des enregistrements de fichiers orphelins) : 0.00 millisecondes.
0 enregistrements de fichier incorrect traités.                        : 0:00:04 ..
Durée de la phase (Vérification des enregistrements de fichiers incorrects) : 1.45 millisecondes.

Étape 2 : Examen de la liaison des noms de fichiers...
5390 enregistrements d'analyse traités.                                n reste : 0:00:03 .
202826 entrées d'index traitées.                                       e : 0:00:03 .
La vérification des index est terminée.
Durée de la phase (Vérification de l'index) : 6.43 secondes.
0 fichiers non indexés analysés.                                       : 0:00:03 ..
Durée de la phase (Reconnexion orpheline) : 59.72 millisecondes.
0 fichiers non indexés récupérés dans le répertoire des fichiers perdus et trouvés.

Durée de la phase (Récupération orpheline vers éléments perdus et trouvés) : 13.85 millisecondes.
5390 enregistrements d'analyse traités.                                n reste : 0:00:03
Durée de la phase (Vérification de l'ID d'objet et du point de réanalyse) : 13.68 millisecondes.

Étape 3 : Examen des descripteurs de sécurité...
La vérification des descripteurs de sécurité est terminée.
```

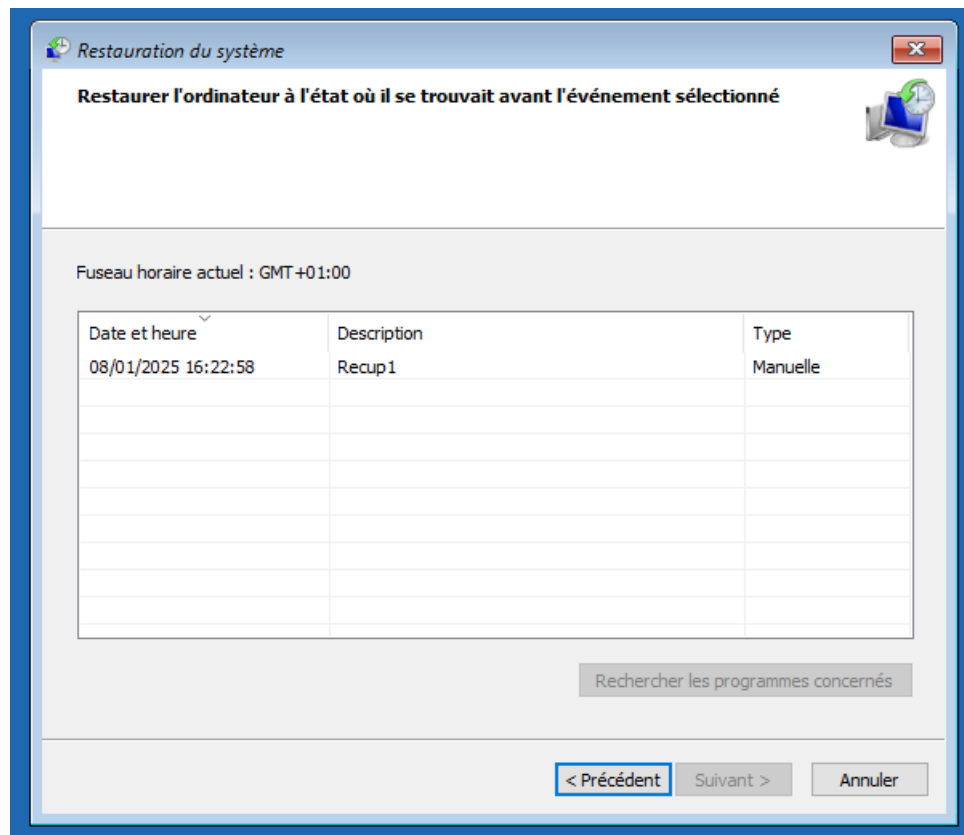
On ferme ensuite l'invite de commande pour retourner sur **WindowsRE**.

Toujours dans « **Dépannage -> Options avancées** » nous testerons la réparation du démarrage avec « **Réparation automatique** » le système redémarre.

Et ensuite nous utiliseront la restauration du système



Nous y retrouverons la page de restauration que l'on a vu précédemment dans le **TP N°4** avec le point de restauration que nous avons fait.



Fin de procédure – NIGRO Antony

