Configuration avancée de Windows client

SOMMAIRE

1. Paramètres système de base

A. Nom de la machine et workgroup

1. Explications

Chaque ordinateur sous Windows est identifié sur le réseau par un nom unique, appelé **nom de la machine**. Ce nom est utilisé pour identifier le poste lorsqu'il communique avec d'autres appareils dans un réseau. Dans les environnements professionnels ou réseaux locaux, un nom clair et spécifique est essentiel pour retrouver et gérer chaque poste facilement.

Workgroup est un modèle de réseau de groupe de travail utilisé par Windows pour organiser et partager des ressources (fichiers, imprimantes) entre ordinateurs sans nécessiter de serveur centralisé. Contrairement aux **Domaines**, qui nécessitent un serveur central (contrôleur de domaine) et une gestion centralisée des utilisateurs et des permissions, le Workgroup est une configuration simple et peu coûteuse, typiquement utilisée pour des réseaux de petite taille.

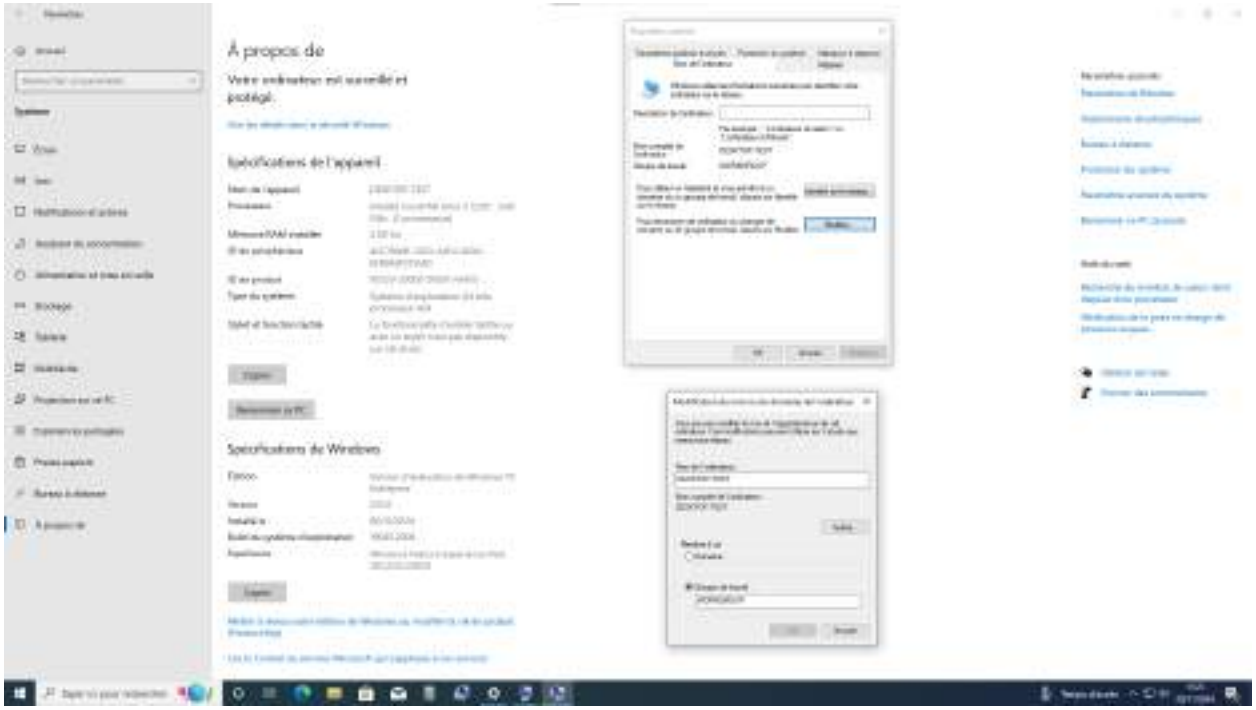
Cette configuration sera utile pour des tâches de partage de fichiers ou d'impression entre postes d'un même réseau.

2. Changer le nom de la machine:

Ouvrez **Paramètres > Système > Informations système.**
Cliquez sur **Renommer ce PC.**
Entrez le "**Nouveau Nom**" pour votre machine.
Redémarrez si nécessaire pour appliquer le changement.

3. Joindre la machine à un Workgroup :

Ouvrez **Paramètres > Système > Informations système.**
Cliquez sur **Modifier les paramètres** sous le nom du PC.
Dans l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier**.
Dans **Membre de**, sélectionnez **Workgroup** et entrez le "**NOM WORKGROUP**".
Redémarrez la VM si demandé.



Questions à rechercher
Qu'est-ce qu'un Workgroup et comment est-il utilisé dans un réseau local ?
Quelles sont les différences entre un Workgroup et un Domaine dans un réseau ?
Dans quel type d'environnement professionnel utiliserait-on un Domaine plutôt qu'un Workgroup ?

B. Gestion des comptes utilisateurs

1. Explications

La gestion des comptes utilisateurs sous Windows est un point central pour la sécurité et le contrôle des accès. Windows distingue généralement deux types de comptes : les **administrateurs** et les **utilisateurs standards**. Les comptes administrateurs disposent de droits étendus pour configurer le système, installer des

logiciels et accéder aux fichiers de tous les utilisateurs. En revanche, les comptes standards disposent de droits limités, ce qui limite les risques de modification non autorisée ou de corruption accidentelle du système.

Dans un environnement de dépannage ou de support informatique, il est essentiel de savoir créer, configurer, et vérifier les permissions des différents comptes. La gestion des utilisateurs peut être effectuée via l'interface graphique de Windows, mais aussi via l'invite de commande (CMD), ce qui est utile pour des tâches rapides ou à distance.

2. Créer des utilisateurs avec différents privilèges :

Accédez à **Paramètres > Comptes > Famille et autres utilisateurs.**
Cliquez sur **Ajouter un autre utilisateur sur ce PC.**

Pour un compte **utilisateur** avec droit standard → Créez simplement un compte (Sélectionner : Je ne dispose pas des informations de connexion de cette personne pour ajouter un compte sans microsoft)
Pour un compte **administrateur** → Créez un compte puis sélectionnez **Changer le type de compte.**

→ Pour sélectionner un compte : au lancement de la machine en bas à gauche

3. Créer un compte utilisateur via l'invite de commande :

Ouvrez l'invite de commande en mode administrateur.
Entrez la commande *net user test /add* pour créer un compte **test**.
Utilisez *net user* pour vérifier la liste des utilisateurs et confirmer la création du compte.
→ *whoami* pour afficher le nom de l'utilisateur actif
→ *hostname* pour afficher le nom de la machine

A noter, les données des utilisateurs sont enregistrer sous le Chemin :
C:\Users\[NomUtilisateur]

2. Configuration réseau et Internet

A. Configuration IP fixe et tests de connectivité

1. Explications

Dans un réseau, chaque appareil doit disposer d'une **adresse IP unique** pour communiquer avec les autres. Une adresse IP peut être **dynamique** (fournie automatiquement par un serveur DHCP) ou **statique** (configurée manuellement). L'assignation d'une IP fixe est utile pour les serveurs et appareils nécessitant une adresse stable et constante, facilitant ainsi leur identification et l'accès à distance.

Les outils de diagnostic réseau comme **ping** et **tracert** sont essentiels pour vérifier la connectivité et diagnostiquer des problèmes de réseau. La commande *ping* envoie une série de paquets à une adresse IP spécifiée et enregistre les réponses, permettant de tester la connexion entre deux appareils. La commande *tracert* (ou *traceroute*) suit le chemin des paquets à travers le réseau jusqu'à leur destination. Cette commande identifie les "sauts" entre les routeurs et peut aider à localiser les interruptions ou les ralentissements sur le réseau.

Dans cet exercice, vous allez configurer une adresse IP fixe sur la VM, vérifier la connexion avec votre poste physique, et analyser le chemin des paquets réseau vers une adresse publique (Google DNS à 8.8.8.8).

2. Configurer une IP statique sur la carte réseau de la VM :

Allez dans **Paramètres > Réseau et Internet > Centre Réseau et partage.**
Cliquez sur **Modifier les paramètres de la carte.**
Clic droit sur votre carte réseau, puis sélectionnez **Propriétés.**
Double-cliquez sur **Protocole Internet version 4 (TCP/IPv4).**
Cochez **Utiliser l'adresse IP suivante** et entrez les informations suivantes :

- **Adresse IP** : 192.168.0.x (où "x" est un chiffre unique, par exemple, 10)
- **Masque de sous-réseau** : 255.255.255.0
- **Passerelle par défaut** : 192.168.0.254
- **Serveur DNS préféré** : 8.8.8.8 (serveur DNS public de Google)

Cliquez sur **OK** pour valider la configuration et fermez toutes les fenêtres.

3. Reconfigurer la carte réseau pour la connexion avec votre poste physique :

Modifiez la configuration IP de la carte réseau pour qu'elle puisse communiquer directement avec votre poste hôte (par exemple, en assignant une IP dans le même sous-réseau que votre poste).

4. Vérifier la connectivité avec ping :

- Ouvrez l'invite de commande (CMD) sur la VM.
- Tapez la commande *ping [adresse IP de votre poste physique].*
- Observez les résultats pour confirmer que la connexion entre la VM et votre poste est fonctionnelle.

5. Analyser le chemin réseau avec tracert :

Exemple avec Google :

- Dans l'invite de commande de la VM, tapez *tracert 8.8.8.8* pour voir le chemin que les paquets prennent vers Google DNS.
- Notez les différents "sauts" et commentez les résultats.

Que signifient les "sauts" dans la commande tracert et comment cette commande aide-t-elle à diagnostiquer des problèmes réseau ?
Quels sont les avantages et les inconvénients de l'utilisation d'une adresse IP fixe par rapport à une adresse IP dynamique ?

B. Configuration DNS

1. Explications

Le **DNS (Domain Name System)** est un service essentiel qui traduit les noms de domaine (comme www.google.com) en adresses IP, ce qui permet aux ordinateurs de communiquer sur Internet. Windows utilise un fichier spécial, appelé **hosts**, qui permet de contrôler localement certaines résolutions DNS. En ajoutant des entrées dans ce fichier, on peut associer des noms de domaine à des adresses IP spécifiques de manière locale, sans que les requêtes ne soient envoyées aux serveurs DNS habituels.

Bien que ce ne soit pas sa fonction principale, le fichier hosts peut agir comme un **proxy détourné** en bloquant ou en redirigeant certains domaines vers une adresse locale (comme 127.0.0.1). Par exemple, si on configure le fichier hosts pour que le domaine korben.info soit associé à 127.0.0.1 (l'adresse IP de l'ordinateur local), les tentatives d'accès au site seront redirigées vers l'ordinateur lui-même et n'aboutiront pas, bloquant ainsi l'accès au site sans l'aide d'un logiciel supplémentaire.

Cette technique de blocage local par le fichier hosts est une méthode simple et rapide pour contrôler l'accès à certains sites ou pour tester des environnements de développement.

Remarque : Pour que les modifications soient immédiatement effectives, il est nécessaire de vider le **cache DNS** de Windows à l'aide de la commande ipconfig /flushdns. Cela force Windows à recharger les informations du fichier hosts sans délai.

2. Localiser et ouvrir le fichier hosts :

Naviguez vers le dossier C:\Windows\System32\drivers\etc\.
Faites un clic droit sur le fichier **hosts** et sélectionnez **Ouvrir avec > Bloc-notes**.
Assurez-vous d'ouvrir le Bloc-notes en tant qu'administrateur pour pouvoir modifier le fichier.

3. Ajouter une entrée pour bloquer korben.info :

Au bas du fichier hosts, ajoutez la ligne suivante pour rediriger korben.info vers l'adresse locale, 127.0.0.1:
127.0.0.1 korben.info
Cette configuration empêche toute tentative de connexion à korben.info en redirigeant les requêtes vers l'ordinateur local.
Enregistrez et fermez le fichier hosts.

4. Vider le cache DNS :

Ouvrez l'invite de commande en tant qu'administrateur.
Tapez ipconfig /flushdns et appuyez sur Entrée pour vider le cache DNS.
Cette commande garantit que Windows rechargera les nouvelles informations du fichier hosts.

5. Tester la configuration :

Ouvrez votre navigateur et essayez d'accéder à korben.info.
Vous devriez voir une erreur de connexion ou une page vierge, confirmant que l'accès est bloqué.

Documentez chaque étape :

Notez le chemin d'accès au fichier hosts, la commande ipconfig /flushdns, et la ligne ajoutée dans le fichier hosts.
Prenez des captures d'écran du fichier modifié et du résultat de la commande ipconfig /flushdns dans l'invite de commande.

Questions à rechercher
Quel est le rôle principal du fichier hosts dans la configuration réseau de Windows ?
Comment le fichier hosts peut-il être utilisé pour bloquer ou rediriger un site de manière locale ?
Pourquoi est-il nécessaire de vider le cache DNS après modification du fichier hosts ?
Quels sont les cas d'usage courants du fichier hosts dans des environnements de développement ou de test ?

3. Gestion des mises à jour Windows (MAJ)

1. Explications

Windows Update est le service de Microsoft permettant de maintenir le système d'exploitation à jour en téléchargeant et installant automatiquement les correctifs de sécurité, les mises à jour de pilotes, et les nouvelles fonctionnalités. Ces mises à jour sont essentielles pour garantir la sécurité et la stabilité de l'ordinateur, en particulier dans un environnement professionnel où des données sensibles peuvent être exposées aux menaces extérieures.

Bien que les mises à jour automatiques soient recommandées, elles peuvent parfois poser des problèmes de compatibilité, notamment avec des logiciels métiers ou des configurations matérielles spécifiques. C'est pourquoi il est important de savoir comment gérer ces mises à jour, contrôler leur installation et, si nécessaire, les désactiver temporairement ou les supprimer.

Dans cet exercice, vous allez configurer les options de mise à jour, désactiver le service Windows Update pour comprendre son impact, et apprendre à désinstaller une mise à jour problématique. Cela vous permettra de maîtriser la gestion des mises à jour et de garantir que celles-ci n'interfèrent pas avec le fonctionnement optimal de votre système.

2. Configurer les options de Windows Update :

Allez dans **Paramètres > Mise à jour et sécurité > Windows Update.**
Configurer un rappel avant redémarrage : Activez les options de notification pour que Windows vous avertisse avant un redémarrage lié aux mises à jour.
Activer le téléchargement à partir d'autres PC : Cette option, que l'on trouve dans **Options avancées > Optimisation de la distribution**, permet de télécharger des mises à jour depuis d'autres ordinateurs du réseau local, réduisant ainsi la bande passante utilisée par Windows Update.

3. Désactiver le service Windows Update :

Ouvrez **Gestion de l'ordinateur** en cliquant droit sur le menu **Démarrer** et en sélectionnant **Gérer**.
Allez dans **Services et applications > Services**.
Recherchez le service **Windows Update**, cliquez droit et sélectionnez **Propriétés**.
Changez le type de démarrage en **Désactivé** pour stopper temporairement le service et empêcher les mises à jour automatiques.
Confirmez et fermez les fenêtres.

4. Désinstaller une mise à jour problématique :

Supposons qu'une mise à jour récente ait causé des problèmes de compatibilité, par exemple la **KB4477137**.
Allez dans **Paramètres > Mise à jour et sécurité > Historique des mises à jour > Désinstaller des mises à jour.**
Recherchez la mise à jour **KB4477137** (ou une mise à jour disponible sur votre version de Windows), sélectionnez-la et cliquez sur **Désinstaller**.
Redémarrez la VM pour appliquer les changements.

Documentez chaque étape :

Notez les chemins d'accès aux options de Windows Update et aux services.
Capturez les configurations modifiées dans Windows Update et la liste des mises à jour installées.

Questions à rechercher
Quels types de mises à jour Windows Update fournit-il, et pourquoi sont-elles importantes pour la sécurité du système ?
En quoi consiste l'option "Téléchargement à partir d'autres PC", et quels sont ses avantages et ses inconvénients ?
Pourquoi certaines mises à jour ne sont-elles pas disponibles pour toutes les versions de Windows ?
Quels sont les risques de désactiver complètement Windows Update et dans quelles situations pourrait-on envisager de le faire temporairement ?
Comment identifier le numéro KB d'une mise à jour problématique, et quels outils peut-on utiliser pour rechercher des informations détaillées sur cette mise à jour ?

4. Optimisation de la confidentialité

1. Explications

La **confidentialité** des données et le respect de la vie privée des utilisateurs sont des sujets particulièrement sensibles sous Windows 10. Par défaut, Windows collecte des informations via la **télémétrie** pour envoyer des données de diagnostic et d'utilisation à Microsoft. Cette collecte de données est censée permettre à Microsoft d'améliorer la sécurité et les performances de Windows en analysant les comportements des utilisateurs, mais elle peut aussi soulever des inquiétudes en termes de protection des données personnelles.

Pour gérer la confidentialité, Windows permet de contrôler les niveaux de télémétrie, de définir les autorisations pour les applications, et de désactiver certains services ou paramètres qui accèdent aux informations personnelles (comme la localisation, le microphone ou la caméra). Dans cet exercice, vous allez explorer les paramètres de télémétrie, configurer les autorisations des applications, et apprendre à désactiver certains services pour optimiser la confidentialité de votre système.

2. Configurer le niveau de télémétrie :

Accédez à **Paramètres > Confidentialité > Commentaires et diagnostics.**
Sous **Données de diagnostic**, sélectionnez le niveau de collecte souhaité. Pour une meilleure confidentialité, choisissez **Essentiel** pour limiter la collecte aux données minimales nécessaires.

Notez que certains niveaux de télémétrie avancés peuvent ne pas être disponibles dans certaines éditions de Windows (comme Windows 10 Famille).

3. Désactiver la télémétrie via le registre :

Ouvrez **Regedit** en tapant *regedit* dans la barre de recherche et en lançant l'application avec les droits d'administrateur.
Naviguez jusqu'à la clé suivante : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection.
Si la clé **DataCollection** n'existe pas, créez-la en faisant un **clic droit > Nouveau > Clé.**
Dans cette clé, créez une nouvelle **Valeur DWORD (32 bits)** appelée **AllowTelemetry** et assignez-lui la valeur **0** pour désactiver la télémétrie.
Fermez Regedit et redémarrez la VM pour appliquer les modifications.

4. Configurer les autorisations des applications :

Accédez à **Paramètres > Confidentialité.**
Dans les sections comme **Caméra, Microphone**, et **Informations de compte**, désactivez les autorisations pour les applications qui n'ont pas besoin d'accéder à ces informations.
Par exemple, désactivez l'accès au microphone et à la caméra pour toutes les applications, sauf celles dont vous avez réellement besoin pour des raisons de sécurité.

5. Désactiver certains services liés à la confidentialité :

Ouvrez **Services** en tapant services.msc dans la barre de recherche.
Localisez le service **Diagnostics Tracking Service** (ou **Connected User Experiences and Telemetry** dans certaines versions).
Cliquez droit sur le service, sélectionnez **Propriétés**, et changez le type de démarrage en **Désactivé** pour empêcher la collecte de données de télémétrie par ce service.
Appliquez les modifications et fermez la fenêtre des services.

Documentez chaque étape :

Notez les chemins d'accès et les modifications apportées pour chaque configuration.

Prenez des captures d’écran des paramètres de confidentialité ajustés dans Windows et dans le registre.

Questions à rechercher
Quelles sont les différences entre les niveaux de télémétrie (Essentiel, Complet) et quelles données sont collectées à chaque niveau ?
Quels sont les avantages et les inconvénients de la désactivation de la télémétrie pour les utilisateurs et pour Microsoft ?
Pourquoi certaines applications demandent-elles un accès aux fonctionnalités comme la caméra ou le microphone, et comment ces autorisations peuvent-elles affecter la confidentialité ?
Quels autres services de Windows collectent ou partagent des données, et comment peut-on les configurer pour renforcer la confidentialité ?

5. Personnalisation de l’environnement utilisateur

1. Explications

La **personnalisation de l’environnement utilisateur** sous Windows permet d’adapter l’interface et les fonctionnalités de l’OS aux préférences et besoins de chaque utilisateur. Windows offre des options pour configurer l'apparence de l’Explorateur de fichiers, ajuster les paramètres d'affichage et de veille, et gérer les applications qui s'exécutent au démarrage. Ces paramètres sont utiles pour optimiser l’ergonomie, le confort visuel et la gestion des performances, en particulier dans un contexte professionnel où les interruptions dues à des applications non essentielles doivent être minimisées.

Dans cet exercice, vous allez configurer des paramètres de base de l’interface utilisateur, personnaliser l'Explorateur de fichiers, et ajuster les paramètres d’économie d’énergie. Vous allez également ajouter un raccourci personnalisé et paramétrer une page intranet pour qu’elle s’ouvre automatiquement au démarrage de la session.

2. Personnalisation de l’Explorateur de fichiers :

Ouvrez **Explorateur de fichiers.**
Allez dans **Affichage** et cochez les options suivantes :

Afficher les dossiers cachés : Affiche les dossiers cachés pour accéder à tous les fichiers système.
Afficher les extensions de fichiers : Active les extensions pour tous les types de fichiers, utile pour identifier facilement les formats.
Par défaut, configurez l'Explorateur pour qu'il affiche **Ce PC** au lieu de **Accès rapide**:
Allez dans **Fichier > Options**.
Dans l'onglet **Général**, sélectionnez **Ce PC** dans le menu déroulant **Ouvrir l'Explorateur de fichiers dans.**

3. Ajuster les paramètres de gestion de l'alimentation :

Accédez à **Paramètres > Système > Alimentation et mise en veille.**
Modifiez les paramètres suivants :
Éteindre l'écran après **30 minutes** d'inactivité.
Mise en veille de l'ordinateur après **1 heure** d'inactivité.
Dans **Options d'alimentation avancées**, configurez l'ordinateur pour **ne pas effectuer d'action à la fermeture du capot** (utile pour les ordinateurs portables).
Configurez également l'arrêt du disque dur après **15 minutes** d'inactivité, sur batterie comme sur secteur.

4. Désactiver les applications au démarrage :

Appuyez sur **Ctrl + Shift + Échap** pour ouvrir le **Gestionnaire des tâches**.
Allez dans l'onglet **Démarrage**.
Désactivez les applications inutiles au démarrage (par exemple, **OneDrive** et **Microsoft Teams** si ces services ne sont pas requis).
Documentez les applications désactivées pour référence.

5. Ajouter un raccourci vers Microsoft Edge sur le bureau :

Ouvrez **Démarrer > Microsoft Edge**.
Faites un clic droit sur l'icône et sélectionnez **Plus > Ouvrir l'emplacement du fichier.**
Cliquez droit sur l'icône dans l'Explorateur et choisissez **Envoyer vers > Bureau (créer un raccourci).**

6. Configurer l’ouverture automatique d’une page intranet au démarrage :

Ouvrez **Internet Explorer** (ou **Microsoft Edge** en mode Internet Explorer si IE n’est pas disponible).
Dans **Options Internet > Général**, définissez la page d’accueil comme http://www.intranet.local.
Créez un raccourci vers **Internet Explorer** avec cette URL.
Allez dans **Démarrer > Exécuter**, tapez shell:startup et appuyez sur Entrée pour ouvrir le dossier de démarrage.
Déplacez le raccourci de la page intranet dans ce dossier pour qu’il se lance automatiquement à l’ouverture de session.

7. Activer la confirmation de suppression des fichiers dans la Corbeille :

Cliquez droit sur la **Corbeille > Propriétés.**
Cochez **Afficher la confirmation de suppression** pour éviter de supprimer des fichiers par erreur.

Documentez chaque étape :

Notez le chemin d'accès pour chaque configuration.
Capturez les paramètres appliqués et enregistrez des captures d’écran des étapes clés.

Questions à rechercher
Quelles sont les extensions de fichiers les plus courantes et à quoi servent-elles ?
Pourquoi est-il recommandé de désactiver les applications inutiles au démarrage ?
Quels avantages cela apporte-t-il en termes de performances ?
Dans quelles situations la confirmation de suppression des fichiers peut-elle être utile, et comment ce paramètre améliore-t-il la sécurité ?
Quelles sont les différences entre la veille, l’arrêt du disque dur, et l’extinction de l’écran en termes de gestion d’énergie ?

6. Bureau à distance

1. Explications

La fonctionnalité de **Bureau à distance** permet à un utilisateur de se connecter à un autre ordinateur via le réseau, offrant ainsi un accès complet à l'interface et aux ressources de cette machine. Elle est particulièrement utile pour les administrateurs système ou les techniciens en informatique qui doivent effectuer des interventions à distance. Cette connexion est sécurisée et nécessite des autorisations spécifiques pour chaque utilisateur.

Dans cette section, vous allez activer le Bureau à distance, ajouter un utilisateur autorisé, et tester la connexion à la VM à partir d'une autre machine. Vous apprendrez également à créer un fichier de configuration RDP pour simplifier les connexions futures.

2. Activer le Bureau à distance :

Accédez à **Paramètres > Système > Bureau à distance**.
Activez l'option **Activer Bureau à distance** pour permettre l'accès à distance.
Confirmez l'activation si Windows vous demande une confirmation de sécurité.

3. Ajouter un utilisateur autorisé :

Toujours dans les paramètres de **Bureau à distance**, cliquez sur **Sélectionner les utilisateurs autorisés**.
Ajoutez l'utilisateur **user1** pour lui permettre de se connecter via Bureau à distance.

4. Tester la connexion Bureau à distance depuis le poste physique :

Depuis votre poste physique, ouvrez **Connexion Bureau à distance** (appuyez sur *Windows + R*, tapez *mstsc* et appuyez sur Entrée).
Dans le champ **Ordinateur**, entrez l'adresse IP de la VM.
Cliquez sur **Se connecter**, puis entrez les identifiants de **user1** pour établir la connexion.

5. Créer un fichier RDP pour une connexion rapide :

Ouvrez **Connexion Bureau à distance** et configurez l'adresse IP de la VM.

Cliquez sur **Afficher les options** et enregistrez les informations de connexion en créant un fichier *.rdp* sur votre bureau.
Double-cliquez sur ce fichier *.rdp* pour tester la connexion.

Questions à rechercher
Quelle est la différence entre Bureau à distance et Assistance à distance dans Windows ?
Comment sécuriser davantage les connexions Bureau à distance ?
Quels sont les risques de sécurité liés à l'activation de Bureau à distance sur une machine ?

7. Dossiers partagés

1. Explications

Le partage de dossiers sous Windows permet à plusieurs utilisateurs d'accéder à un ensemble de fichiers centralisés, facilitant ainsi la collaboration et le partage de ressources au sein d'un réseau. Un dossier partagé peut être configuré avec des **permissions spécifiques** (lecture, écriture, ou contrôle total), permettant de contrôler précisément les droits d'accès des utilisateurs. En ajoutant le symbole $ à la fin du nom d'un dossier partagé, on peut également le rendre caché, ce qui signifie qu'il ne sera pas visible dans l'Explorateur réseau sans connaître son nom exact.

Dans cette section, vous allez créer un dossier partagé sur votre VM, le configurer pour qu'il soit accessible par un utilisateur spécifique avec des droits de lecture/écriture, et tester l'accès depuis un autre poste.

2. Créer un dossier partagé :

Sur la VM, créez un nouveau dossier sur le volume **E:** et nommez-le **Dossier_partagé**.
Faites un clic droit sur le dossier **> Propriétés > Partage > Partage avancé.**
Cochez **Partager ce dossier**, et dans **Nom du partage**, entrez *Dossier_partagé$* pour le rendre caché sur le réseau.
Cliquez sur **Permissions** et ajoutez l'utilisateur **user1** avec des droits **Lecture/Écriture**.
Appliquez et fermez la fenêtre.

3. Vérifier l’accès au dossier partagé depuis le poste physique :

Depuis le poste physique, ouvrez l’Explorateur de fichiers et tapez *\\[IP de la VM]\Dossier_partagé$* dans la barre d’adresse.
Connectez-vous en utilisant les identifiants de **user1** si nécessaire.
Testez les droits d'accès en créant un fichier texte dans le dossier partagé pour vérifier que l’utilisateur **user1** a bien les droits d’écriture.

Questions à rechercher
Quelles sont les différences entre les permissions Lecture, Écriture et Contrôle total pour un dossier partagé ?
Que signifie le symbole $ ajouté à la fin d’un nom de partage ? Dans quels cas est-il utilisé ?
Quels sont les risques de sécurité associés au partage de dossiers, et comment les atténuer ?

8. Gestion des volumes et partitions

1. Explications

La gestion des volumes et partitions permet d’organiser, d’allouer et de sécuriser le stockage des données sur un système. Les **partitions** sont des divisions logiques d’un disque physique, et un disque peut contenir plusieurs partitions pour séparer les données, le système d'exploitation, et les sauvegardes. Les **volumes** désignent ces partitions une fois qu'elles sont formatées et prêtes à être utilisées.

Windows inclut des fonctionnalités avancées pour gérer les disques, créer des partitions, et configurer le **RAID (Redundant Array of Independent Disks).** Le RAID permet d'utiliser plusieurs disques physiques pour améliorer la redondance ou les performances. Par exemple, le **RAID 1** offre une duplication des données sur deux disques (miroir), assurant que les informations sont toujours accessibles même en cas de défaillance d’un disque.

Dans cet exercice, vous allez ajouter des disques virtuels à la VM, créer une nouvelle partition et configurer le RAID 1 pour mieux comprendre la gestion de stockage sous Windows.

2. Ajouter des disques virtuels à la VM :

Ouvrez les paramètres de la machine virtuelle dans votre hyperviseur (par exemple, VMware ou VirtualBox).
Ajoutez deux nouveaux disques virtuels de **1 Go** chacun. Notez les noms de ces disques pour les retrouver facilement.

3. Accéder à la gestion des disques :

Sur la VM, faites un clic droit sur le menu **Démarrer** et sélectionnez **Gestion des disques**.
Vous verrez les deux nouveaux disques que vous venez d'ajouter, marqués comme non initialisés.

4. Initialiser les disques :

Dans la fenêtre **Gestion des disques**, faites un clic droit sur chaque nouveau disque et choisissez **Initialiser le disque**.
Sélectionnez le style de partition **MBR** (Master Boot Record) pour ces disques.

5. Créer un volume en RAID 1 (miroir) :

Dans **Gestion des disques**, faites un clic droit sur l'un des disques non alloués et sélectionnez **Nouveau volume en miroir**.
Suivez les instructions pour ajouter le deuxième disque au volume miroir, créant ainsi un **RAID 1**.
Attribuez la lettre de lecteur **E:** à ce volume et nommez-le **Data**.
Formatez le volume en **NTFS** et terminez la création du volume.

6. Vérifier le volume RAID 1 :

Dans l'Explorateur de fichiers, accédez au volume **E:** (Data).
Créez un fichier texte pour vérifier que le volume est opérationnel.
Ce volume **miroir** assure que toutes les données sont identiques sur les deux disques. Vous pouvez tester la redondance en éteignant un des disques virtuels (optionnel).

Questions à rechercher
Qu'est-ce que le RAID et quels types de RAID sont les plus courants ? (RAID 0, RAID 1, RAID 5, etc.)
Quels sont les avantages et les inconvénients d'un volume RAID 1 par rapport à un volume RAID 0 ?
Quelle est la différence entre un disque MBR et un disque GPT, et dans quels cas utiliser chacun de ces styles de partitionnement ?
Comment peut-on vérifier l'intégrité d'un volume RAID sous Windows en cas de défaillance d'un des disques ?

9. Maintenance et restauration du système

1. Explications

La **maintenance** et la **restauration du système** sont des pratiques essentielles pour garantir la stabilité et la performance de Windows. La maintenance comprend des tâches régulières comme le nettoyage des fichiers temporaires, la mise à jour des pilotes, et la gestion des points de restauration pour prévenir des pertes de données lors d'incidents. La **restauration du système** permet de revenir à un état antérieur de Windows en cas de problèmes dus à des logiciels installés ou des configurations incorrectes, sans affecter les fichiers personnels.

Dans cette section, vous apprendrez à utiliser les outils de Windows pour maintenir un système propre et stable : la création de points de restauration, la restauration du système à un point antérieur, l'utilisation du rollback des pilotes pour corriger les erreurs de compatibilité, et le nettoyage du disque pour optimiser l’espace de stockage.

2. Activer et configurer la protection du système :

Allez dans **Panneau de configuration > Système et sécurité > Système**.
Cliquez sur **Paramètres système avancés** dans le volet de gauche.
Dans l’onglet **Protection du système**, sélectionnez le disque **C:** et cliquez sur **Configurer**.
Activez **Activer la protection du système** et définissez une quantité d’espace disque à utiliser pour la restauration (par exemple, 5 %).
Cliquez sur **Appliquer** et **OK**.

3. Créer un point de restauration :

Toujours dans l'onglet **Protection du système**, cliquez sur **Créer...** pour définir un nouveau point de restauration.
Nommez-le (par exemple, "Point de restauration avant maintenance") et confirmez la création.
Ce point de restauration servira de sauvegarde pour le système dans l'état actuel, permettant un retour à cet état si nécessaire.

4. Effectuer une restauration du système :

En cas de besoin, retournez dans **Protection du système** et cliquez sur **Restauration du système...**.
Suivez les étapes pour restaurer le système à un point de restauration précédemment créé.
Choisissez le point de restauration créé dans l'étape précédente, puis redémarrez la VM pour appliquer la restauration.

5. Rollback des pilotes :

Si un périphérique présente des problèmes après une mise à jour de pilote, allez dans **Gestionnaire de périphériques**.
Cliquez droit sur le périphérique concerné, sélectionnez **Propriétés**, puis l'onglet **Pilote**.
Cliquez sur **Revenir à la version précédente** pour annuler la dernière mise à jour du pilote.
Redémarrez la VM et vérifiez si le périphérique fonctionne correctement.

6. Utiliser l'outil de nettoyage de disque :

Ouvrez **Explorateur de fichiers**, faites un clic droit sur le lecteur **C:** et sélectionnez **Propriétés**.
Cliquez sur **Nettoyage de disque** pour lancer l'outil.
Sélectionnez les fichiers à supprimer (comme les fichiers temporaires, les fichiers de la corbeille, etc.) et cliquez sur **OK** pour libérer de l'espace.
Vous pouvez également cliquer sur **Nettoyer les fichiers système** pour supprimer les anciens fichiers de mise à jour Windows.

Questions à rechercher
Quelles différences existent entre la restauration du système et la réinitialisation de Windows ?
Quels types de fichiers sont supprimés par l'outil de nettoyage de disque, et dans quels cas cet outil est-il le plus utile ?
En quoi consiste la fonctionnalité rollback des pilotes, et dans quels cas l'utiliser pour résoudre des problèmes ?
Quels sont les avantages de la création régulière de points de restauration pour un utilisateur professionnel ?

10. Imprimante

1. Explications

Dans un environnement de travail, l'accès à une imprimante est essentiel pour de nombreuses tâches, mais il n'est pas toujours possible d'installer une imprimante physique sur chaque machine, surtout dans le cadre d'un TP. Windows permet l'installation d'imprimantes virtuelles, telles que **PDFCreator**, qui "impriment" des documents au format PDF au lieu de les envoyer à une imprimante physique. Cela est particulièrement utile pour sauvegarder des documents en PDF, les partager numériquement, ou créer des archives sans consommer de papier.

PDFCreator est un logiciel qui installe une imprimante virtuelle sur votre ordinateur. Lorsque vous choisissez d'imprimer un document via PDFCreator, celui-ci est converti en PDF et enregistré sur votre disque. Dans cet exercice, vous allez installer PDFCreator, le configurer comme imprimante par défaut, et tester son fonctionnement en créant un fichier PDF à partir d'un document texte.

2. Télécharger et installer PDFCreator :

Allez sur le site officiel de PDFCreator (https://www.pdfforge.org/pdfcreator) et téléchargez le programme d'installation.
Exécutez l'installateur et suivez les instructions pour installer PDFCreator.
Lorsque vous y êtes invité, définissez PDFCreator comme imprimante par défaut.

3. Vérifier l'installation de PDFCreator :

Accédez à **Paramètres > Périphériques > Imprimantes et scanners.**
Vérifiez que **PDFCreator** est bien listé comme une imprimante installée et définie par défaut.

4. Tester PDFCreator en créant un fichier PDF :

Ouvrez **Bloc-notes** et écrivez du texte simple (par exemple, "Test PDF").
Cliquez sur **Fichier > Imprimer**.
Sélectionnez **PDFCreator** comme imprimante et cliquez sur **Imprimer**.
PDFCreator vous demandera où enregistrer le fichier PDF. Choisissez un emplacement, nommez le fichier, et enregistrez-le.
Accédez au fichier PDF dans l'Explorateur pour vérifier qu'il a bien été créé.

5. Configurer les options de PDFCreator :

Ouvrez **PDFCreator** et accédez aux **Paramètres**.
Explorez les options pour personnaliser les paramètres, comme :
Qualité du PDF : Choisissez une qualité plus élevée ou plus basse selon vos besoins.
Dossier de destination par défaut : Modifiez l'emplacement de sauvegarde des fichiers PDF si vous souhaitez qu'ils soient enregistrés automatiquement dans un dossier spécifique.
Sécurité PDF : Activez des options de sécurité pour protéger les documents avec un mot de passe ou pour restreindre les autorisations d'impression et de modification.
Enregistrez les modifications.

Questions à rechercher
Quels sont les avantages d'utiliser une imprimante virtuelle comme PDFCreator par rapport à une imprimante physique ?
Comment PDFCreator peut-il être utilisé pour sécuriser des documents ?
Quelles autres imprimantes virtuelles existe-t-il pour Windows, et quelles sont leurs particularités ?

11. Mode Kiosque / borne

1. Explications

Le mode kiosque est une fonctionnalité de Windows permettant de configurer un appareil pour un usage spécifique et restreint. Il est couramment utilisé dans des environnements où les utilisateurs ne doivent accéder qu'à une ou plusieurs applications déterminées, comme des bornes interactives, des systèmes en libre-service ou des environnements éducatifs. Cette configuration garantit la sécurité et empêche les utilisateurs de naviguer en dehors des applications autorisées.

Microsoft a introduit cette fonctionnalité sous différents noms au fil des versions de Windows, selon les évolutions et les contextes d'utilisation. Le mode kiosque permet notamment de :

Lancer une application en mode plein écran sans possibilité de sortie.
Limiter les actions de l'utilisateur, comme accéder au bureau ou à d'autres paramètres.
Renforcer la sécurité dans les environnements publics ou d'entreprise.
Attention, le mode kiosque a porte un nom différent en fonction de votre version de windows client :

- accès affecté
- mode kiosque
- borne

Dans cet exercice, vous allez configurer un compte en mode Kiosque sur la VM pour qu'il n'ait accès qu'à l'application Calculatrice. Cela vous permettra de comprendre comment limiter l'accès aux ressources de l'ordinateur pour certains utilisateurs.

2. Créer un compte en mode Kiosque :

Accédez à **Paramètres > Comptes > Famille et autres utilisateurs**.
Cliquez sur **Configurer le mode Kiosque (accès attribué).**
Sélectionnez **Configurer un compte en mode Kiosque.**
Créez un nouveau compte nommé **user2** pour l'assigner au mode Kiosque.

3. Configurer l'application de kiosque :

Sélectionnez **user2** comme compte Kiosque.
Choisissez l'application **Calculatrice** comme seule application autorisée.

Enregistrez et appliquez les paramètres.

4. Tester le mode Kiosque :

Déconnectez-vous et connectez-vous avec **user2** pour vérifier que seule l'application Calculatrice est disponible.
Documentez l'expérience.

5. Sortir du mode Kiosque :

Redémarrez la VM ou déconnectez le compte en utilisant les touches **Ctrl + Alt + Suppr.**

Questions à rechercher
Quelles sont les autres applications ou scénarios d'utilisation courants pour le mode Kiosque ?
Comment réinitialiser un compte en mode Kiosque pour lui redonner un accès normal ?
Quels sont les avantages et les inconvénients de l'utilisation du mode Kiosque pour la sécurité ?

12. Sécurité et gestion des politiques de groupe

1. Explications

Les stratégies locales permettent aux administrateurs de configurer et de contrôler les paramètres de sécurité et de configuration directement sur un ordinateur spécifique, sans dépendre d'un serveur ou d'un environnement Active Directory. Ces stratégies sont particulièrement utiles pour gérer la sécurité, restreindre certaines actions des utilisateurs, et uniformiser les configurations sur des machines autonomes ou non connectées à un domaine. Contrairement aux stratégies de groupe (GPO) centralisées, elles s'appliquent uniquement à l'ordinateur sur lequel elles sont configurées.

Dans cet exercice, vous allez explorer certaines politiques de sécurité de base et apprendre à configurer une politique locale pour restreindre des actions spécifiques sur la VM.

2. Ouvrir l’éditeur de stratégie de groupe :

Appuyez sur *Windows + R*, tapez *gpedit.msc*, et appuyez sur Entrée pour ouvrir l’éditeur de stratégies de groupe.

3. Configurer des politiques de sécurité locales :

Dans **Configuration de l'utilisateur > Modèles d'administration > Système.**
Activez la politique **Désactiver l'accès à l'invite de commandes** pour empêcher l’utilisateur d'accéder à CMD.
Dans **Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégies de verrouillage des comptes**
activez **Seuil de verrouillage des comptes** pour sécuriser l’accès en mettant la valeur à 3

4. Tester les restrictions :

Essayez d'accéder à l'invite de commandes pour vérifier que l’accès est bloqué.
Testez la politique de verrouillage après plusieurs tentatives de connexion échouées.

Questions à rechercher
Quelle est la différence entre les politiques locales et les politiques de groupe appliquées par un contrôleur de domaine ?
Dans quels cas pourrait-on vouloir restreindre l’accès à l’invite de commandes ?
Comment les politiques de sécurité influencent-elles la sécurité globale d’un réseau d’entreprise ?

13. Gestion des applications et autorisations

1. Explications

La gestion des applications et des autorisations est cruciale pour garantir la sécurité et la performance d'un système. Windows permet de restreindre l’exécution de certaines applications, de configurer le **contrôle de compte utilisateur (UAC)** pour limiter les actions des utilisateurs, et de surveiller l’exécution des scripts. Ces paramètres aident à prévenir l’installation de logiciels malveillants, à éviter les actions accidentelles nuisibles et à mieux sécuriser le système.

Dans cet exercice, vous allez explorer le contrôle des applications autorisées, configurer l'UAC, et définir les autorisations d'exécution des scripts PowerShell.

2. Configurer le contrôle des applications :

Accédez à **Paramètres > Applications > Applications et fonctionnalités**.
Dans **Choisir où obtenir les applications**, sélectionnez **Microsoft Store uniquement** pour limiter l'installation aux applications de confiance.

3. Configurer l'UAC (Contrôle de compte utilisateur) :

Ouvrez le **Panneau de configuration > Comptes d'utilisateurs > Modifier les paramètres de contrôle de compte utilisateur.**
Réglez l'UAC sur le niveau **Toujours m'avertir** pour plus de sécurité.
Testez le réglage en tentant d'installer un logiciel.

4. Configurer les autorisations pour les scripts PowerShell :

Ouvrez PowerShell en tant qu'administrateur.
Tapez *Set-ExecutionPolicy RemoteSigned* pour autoriser uniquement les scripts signés provenant d'une source distante.
Vérifiez le paramètre d'exécution avec la commande *Get-ExecutionPolicy*.

Questions à rechercher
Quelles sont les différentes options d'UAC, et quels niveaux de sécurité offrent-elles ?
Pourquoi est-il recommandé de restreindre l'exécution des scripts PowerShell ?
Dans quels cas est-il pertinent de limiter les installations aux applications provenant du Microsoft Store ?

14. Base de registre Windows

1. Explications

La **Base de Registre** de Windows est une base de données hiérarchique où sont stockés tous les paramètres et configurations du système, des applications, des périphériques, et des utilisateurs. La modification du registre permet de réaliser des ajustements fins sur le système, mais une mauvaise manipulation peut rendre le

système instable. Il est donc recommandé de sauvegarder les clés de registre avant de les modifier.

Dans cet exercice, vous allez explorer la base de registre, modifier un paramètre pour activer le pavé numérique au démarrage, et apprendre à sauvegarder des clés pour restaurer le registre en cas de problème.

2. Ouvrir et explorer la Base de Registre :

Appuyez sur *Windows + R*, tapez *regedit*, et appuyez sur Entrée pour ouvrir l'éditeur de registre.
Familiarisez-vous avec les sections principales (comme **HKEY_LOCAL_MACHINE et HKEY_CURRENT_USER)**.

3. Activer le pavé numérique au démarrage :

Accédez à la clé suivante : *HKEY_USERS\.DEFAULT\Control Panel\Keyboard*.
Double-cliquez sur la valeur **InitialKeyboardIndicators** et modifiez-la à **2** pour activer le pavé numérique par défaut.
Redémarrez la VM pour vérifier que le pavé numérique est activé à l'écran de connexion.

4. Sauvegarder et restaurer une clé de registre :

Cliquez droit sur la clé **Keyboard** et sélectionnez **Exporter**.
Enregistrez le fichier *.reg* sur le bureau.
Pour tester la restauration, supprimez la clé **Keyboard**, puis double-cliquez sur le fichier *.reg* pour restaurer les paramètres.

Questions à rechercher
Quelles sont les principales ruches de la base de registre, et que stocke chacune d'elles ?
Pourquoi est-il essentiel de sauvegarder une clé de registre avant de la modifier ?
Quels types de modifications peuvent être apportés à la base de registre pour personnaliser l'expérience utilisateur ?