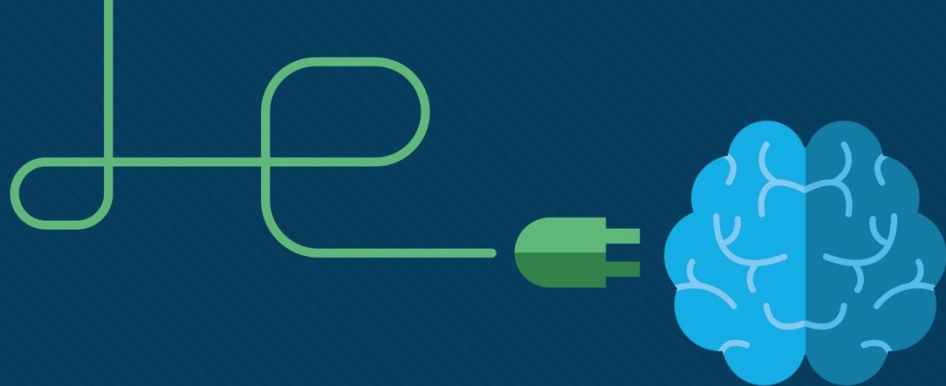




Module 3: Le système d'exploitation Windows

CyberOps Associate v1.0



Objectifs du module

Titre de Module: Le système d'exploitation Windows

Objectif du Module: Présenter les fonctionnalités de sécurité du système d'exploitation Windows.

Titre du Rubrique	Objectif du Rubrique
Histoire de Windows	Décrire l'histoire du système d'exploitation Windows.
Architecture et fonctionnement de Windows	Expliquer l'architecture de Windows et son fonctionnement.
Configuration et contrôle de Windows	Expliquer comment configurer et surveiller Windows.
Sécurité Windows	Expliquer comment Windows peut être sécurisé.

3.1 L'histoire de Windows

Disque du système d'exploitation

- Le système d'exploitation de disque (DOS) est un système que l'ordinateur utilise pour permettre à ces dispositifs de stockage de données de lire et d'écrire des fichiers.
- Le DOS fournit un système de fichiers qui organise les fichiers de manière spécifique sur le disque.
- MS-DOS, créé par Microsoft, disposait d'une interface de ligne de commande dont se servaient les utilisateurs pour créer des programmes et manipuler des fichiers de données. Les commandes DOS sont affichées en caractères gras dans la sortie de commande donnée.
- Avec MS-DOS, l'ordinateur disposait d'une connaissance pratique de base sur la façon d'accéder au lecteur de disque et de charger les fichiers du système d'exploitation directement depuis le disque dans le cadre du processus de démarrage.

```
Starting MS-DOS...
HIMEM is testing extended memory... done.
C:\> C:\DOS\SMARTDRV.EXE /X
C:\> dir
Volume in drive C is MS-DOS_6
Volume Serial Number is 4006-6939
Directory of C:\
DOS          <DIR>          05-06-17  1:09p
COMMAND.COM  54,645 05-31-94  6:22a
WINA20      386      9,349 05-31-94  6:22a
CONFIG.SYS  71 05-06-17  1:10p
AUTOEXEC.BAT 78 05-06-17  1:10p
             5 file(s)      64,143 bytes
             517,021,696 bytes free
C:\>
```

Disque du système d'exploitation (Suite)

- La première version de Windows, Windows 1.0 en 1985, se composait d'une interface utilisateur graphique (GUI) exécutée sur MS-DOS.
- Dans les versions plus récentes de Windows, basées sur NT, le système d'exploitation lui-même contrôle directement l'ordinateur et ses composants matériels.
- Une grande partie de ce que vous faisiez par l'intermédiaire de l'interface de ligne de commande MS-DOS peut être réalisée aujourd'hui dans l'interface utilisateur graphique Windows.
- Pour savoir à quoi ressemblait MS-DOS, ouvrez une fenêtre de commande, tapez **cmd** dans Recherche Windows et appuyez sur **Entrée**.

Disque du système d'exploitation (Suite)

Le tableau suivant répertorie certaines des commandes de MS-DOS :

Commande MS-DOS	Description
dir	Affiche une liste de tous les fichiers dans le répertoire (dossier) actuel
cd <i>directory</i>	Change le répertoire dans le répertoire indiqué
cd ..	Change le répertoire au répertoire situé au-dessus du répertoire actuel
cd \	Change le répertoire au répertoire racine (en règle générale, C:)
copy <i>source destination</i>	Copie les fichiers d'un emplacement à un autre.
del <i>filename</i>	Supprime un ou plusieurs fichiers.
find	Rechercher du texte dans des fichiers
<i>Répertoire</i> mkdir	Crée un nouveau répertoire.
Renom_anciennewname	Permet de renommer un fichier
Aide	Affiche toutes les commandes pouvant être utilisées, avec une brève description
<i>Commande</i> help	Affiche l'aide détaillée de la commande indiquée

Versions de Windows

- Depuis 1993, plus de 20 versions de Windows basées sur le système d'exploitation NT ont vu le jour.
- car de nombreuses éditions ont été spécifiquement créées pour les postes de travail, les serveurs professionnels, les serveurs avancés et les serveurs de datacenters, pour n'en citer que quelques-uns.
- Le système d'exploitation 64 bits propose une architecture totalement nouvelle, avec un espace d'adressage de 64 bits au lieu de 32 bits.
- En général, les ordinateurs et les systèmes d'exploitation 64 bits sont rétrocompatibles avec les anciens programmes 32 bits ; en revanche, il est impossible d'exécuter des programmes 64 bits sur un ordinateur 32 bits.
- Au fil des versions, Microsoft a perfectionné le système d'exploitation Windows en y intégrant davantage de fonctionnalités.
- Microsoft a annoncé que Windows 10 est la dernière version de Windows. Selon la société, plutôt que d'acheter de nouveaux systèmes d'exploitation, les utilisateurs devront simplement mettre à jour Windows 10.

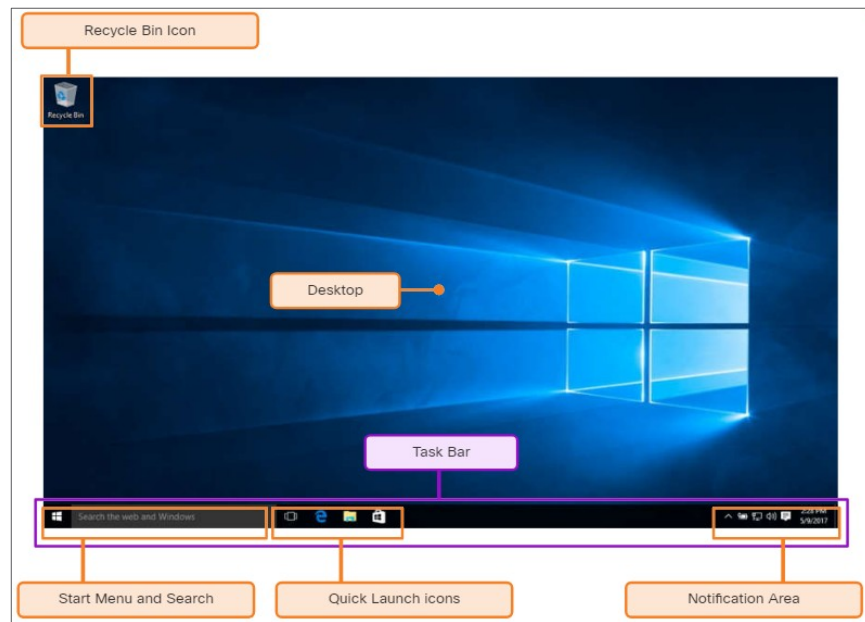
Versions de Windows (Suite)

Le tableau suivant répertorie les versions courantes de

SE	versions
Windows 7	Starter, Familiale Basique, Familiale Premium, Professionnel, Entreprise, Intégrale
Windows Server 2008 R2	Foundation, Standard, Entreprise, Datacenter, Serveur web, Serveur HPC, Systèmes Itanium
Windows Home Server 2011	Néant
Windows 8	Windows 8, Windows 8 Pro, Windows 8 Entreprise, Windows RT
Windows Server 2012	Fondation, Essentials, Standard, Datacenter
Windows 8.1	Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise, Windows RT 8.1
Windows Server 2012 R2	Fondation, Essentials, Standard, Datacenter
Windows 10	Familiale, Pro, Professionnel Éducation, Entreprise, Éducation, IoT Standard, Mobile, Mobile Entreprise
Windows Server 2016	Essentials, Standard, Datacenter, Premium Multipoint Server, Storage Server, Hyper-V Server

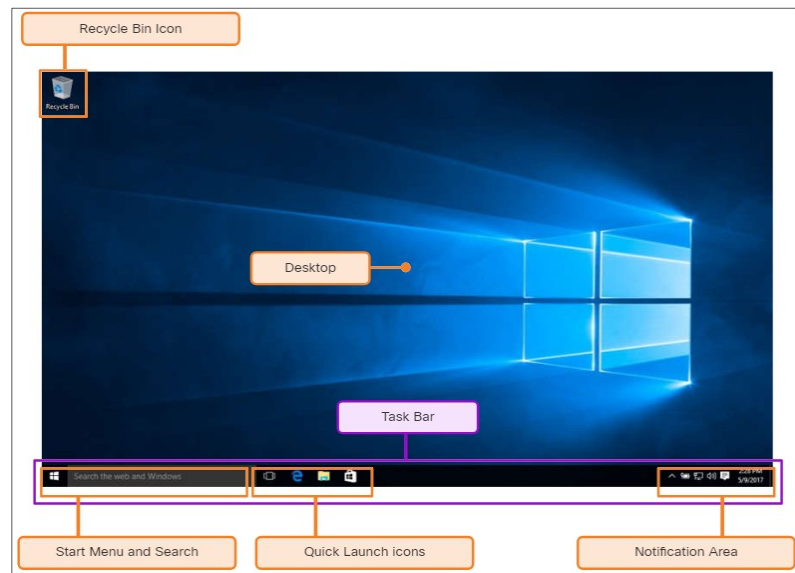
Interface utilisateur de Windows

- Windows propose une interface utilisateur graphique pour permettre aux utilisateurs d'exploiter le logiciel et les fichiers de données.
- L'interface utilisateur graphique dispose d'une zone principale appelée Bureau. Il est possible de personnaliser le Bureau avec diverses couleurs et images d'arrière-plan.
- Dans la mesure où Windows prend en charge plusieurs utilisateurs, chaque utilisateur peut personnaliser le Bureau à sa convenance.
- Le Bureau peut stocker des fichiers, des dossiers, des raccourcis vers des emplacements et des programmes ainsi que des applications.
- Le Bureau dispose également d'une icône représentant une corbeille, qui contient les fichiers que supprime l'utilisateur. Vous pouvez récupérer les fichiers de la corbeille ou vider la corbeille pour les supprimer définitivement.



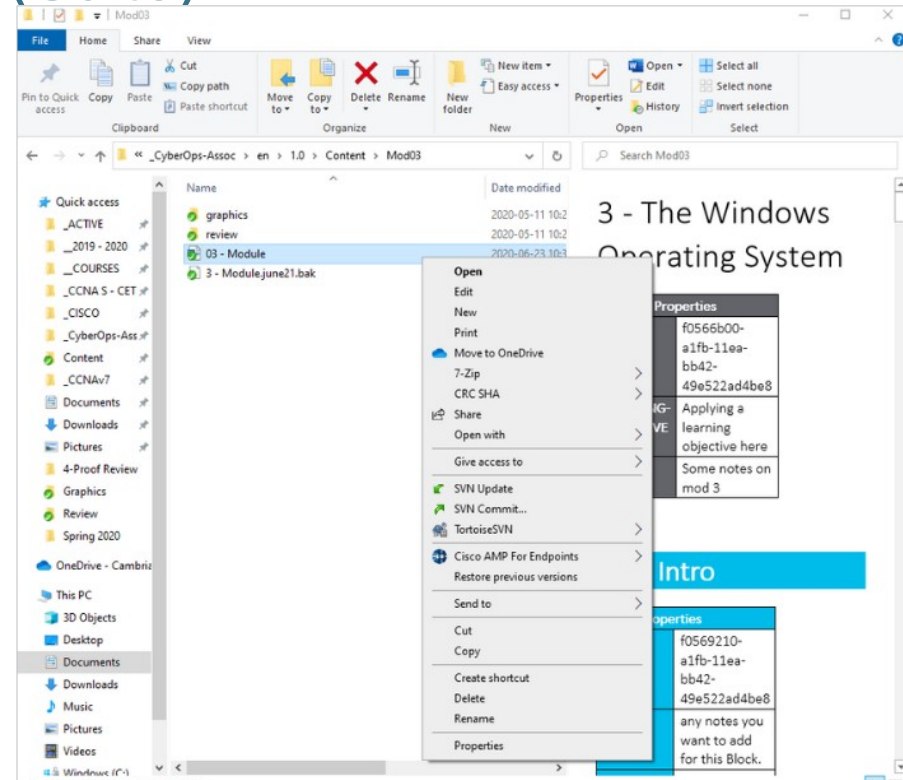
Interface utilisateur de Windows (Suite)

- En bas du Bureau se trouve la barre des tâches.
- À gauche se trouve le menu Démarrer qui permet d'accéder à tous les programmes installés, aux options de configuration et à la fonction de recherche.
- Au centre, les utilisateurs placent des icônes de lancement rapide en vue d'exécuter des programmes ou d'ouvrir des dossiers spécifiques.
- À droite de la barre des tâches se situe la zone de notification. La zone de notification permet de consulter rapidement l'état d'un programme ou d'une fonction.



Interface utilisateur de Windows (Suite)

- Il suffit souvent de cliquer avec le bouton droit de la souris sur une icône pour afficher des fonctions supplémentaires. Cette liste est connue sous le nom de Menu contextuel.
- Des menus contextuels sont disponibles pour les icônes de la zone de notification, pour les icônes de lancement rapide, les icônes de configuration système ainsi que les fichiers et les dossiers.
- D'un simple clic, le menu contextuel permet d'accéder à de nombreuses fonctions couramment utilisées.



Vulnérabilités du système d'exploitation

- Les systèmes d'exploitation sont constitués de millions de lignes de code. Tout ce code augmente la vulnérabilité des systèmes.
- Une vulnérabilité est une faille ou une faiblesse dont peut profiter un hacker pour réduire la viabilité des informations d'un ordinateur.
- Le hacker doit utiliser une technique ou un outil pour exploiter une vulnérabilité du système d'exploitation.
- Le hacker peut ensuite utiliser cette vulnérabilité pour détourner l'usage initialement prévu de l'ordinateur.
- En règle générale, son objectif est de contrôler l'ordinateur, de modifier les autorisations ou de manipuler des données.

Vulnérabilités du système d'exploitation (Suite)

Voici quelques recommandations de sécurité relatives au système d'exploitation Windows:

Recommandation	Description
Protection contre les virus antivirus ou les logiciels malveillants.	<ul style="list-style-type: none">• Par défaut, Windows utilise Windows Defender pour la protection contre les logiciels malveillants• Windows Defender offre une suite d'outils de protection intégrés au système.• Si Windows Defender est désactivé, le système devient plus vulnérable aux attaques et aux logiciels malveillants.
Les services inconnus ou non gérés.	<ul style="list-style-type: none">• De nombreux services s'exécutent en arrière-plan.• Il est important de s'assurer que chaque service est identifiable et sécurisé.• Lorsqu'un service inconnu s'exécute en arrière-plan, l'ordinateur peut être vulnérable aux attaques.
Chiffrement	<ul style="list-style-type: none">• Lorsque les données ne sont pas chiffrées, elles sont facilement accessibles et exploitables.• Il est donc important de les chiffrer sur les ordinateurs de bureau, mais surtout sur les terminaux mobiles.
Stratégie de sécurité	<ul style="list-style-type: none">• Une politique de sécurité adéquate doit être configurée et suivie.• De nombreux paramètres dans le contrôle de la Stratégie de la sécurité Windows empêchent les attaques.

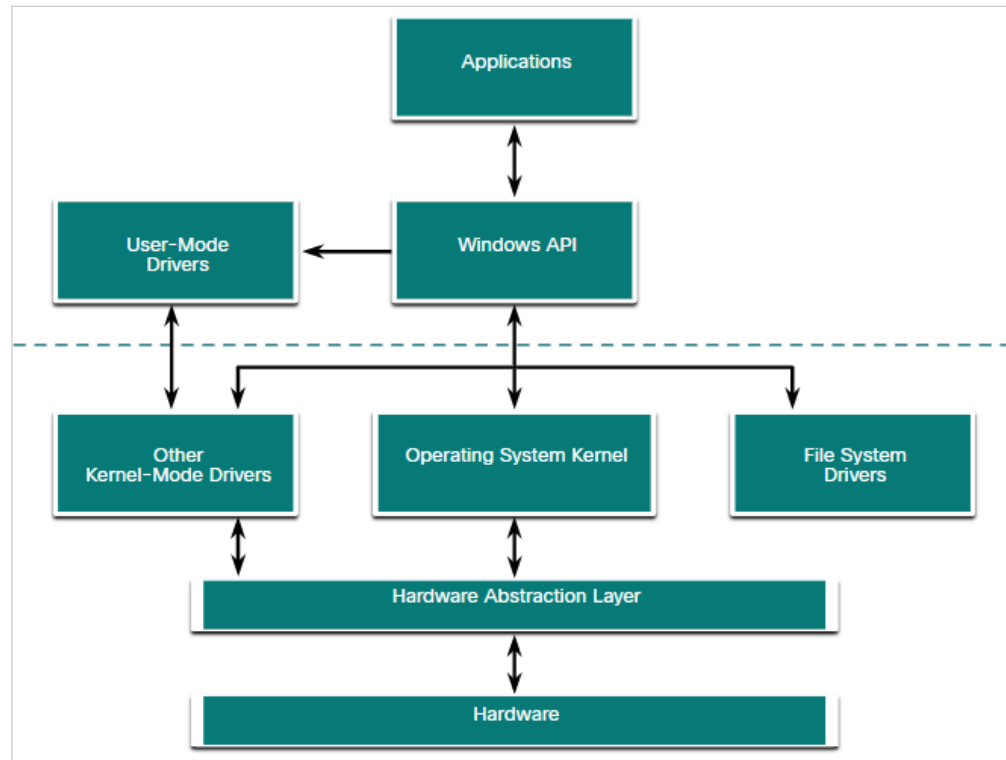
Vulnérabilités du système d'exploitation (Suite)

Recommandation	Description
Pare-feu	<ul style="list-style-type: none">• Par défaut, Windows utilise le pare-feu Windows pour limiter la communication avec les appareils sur le réseau. Au fil du temps, il est possible que certaines règles deviennent obsolètes.• Il est important de revoir périodiquement les paramètres du pare-feu pour s'assurer que les règles s'appliquent toujours et supprimer celles devenues obsolètes.
Autorisations de fichier et de partage	<ul style="list-style-type: none">• ces autorisations doivent être correctement définies. Il est facile d'attribuer un contrôle total au groupe « Tout le monde », mais cette autorisation permet à tous les utilisateurs de manipuler l'ensemble des fichiers.• Il est donc préférable de fournir à chaque utilisateur ou groupe les autorisations minimales nécessaires pour l'ensemble des fichiers et dossiers.
Mot de passe faible ou aucun mot de passe	<ul style="list-style-type: none">• De nombreux utilisateurs choisissent des mots de passe faibles ou n'en utilisent pas du tout.• Il est particulièrement important de s'assurer que tous les comptes, en particulier le compte d'administrateur, disposent d'un mot de passe fort.
Connectez-vous en tant qu'administrateur	<ul style="list-style-type: none">• Lorsqu'un utilisateur se connecte en tant qu'administrateur, tous les programmes qu'il exécute disposent des privilèges de ce compte.• Il est donc préférable de se connecter en tant qu'utilisateur standard et d'utiliser uniquement le mot de passe d'administrateur pour accomplir certaines tâches.

3.2 Architecture et fonctionnement de Windows

Couche HAL (Hardware Abstraction Layer)

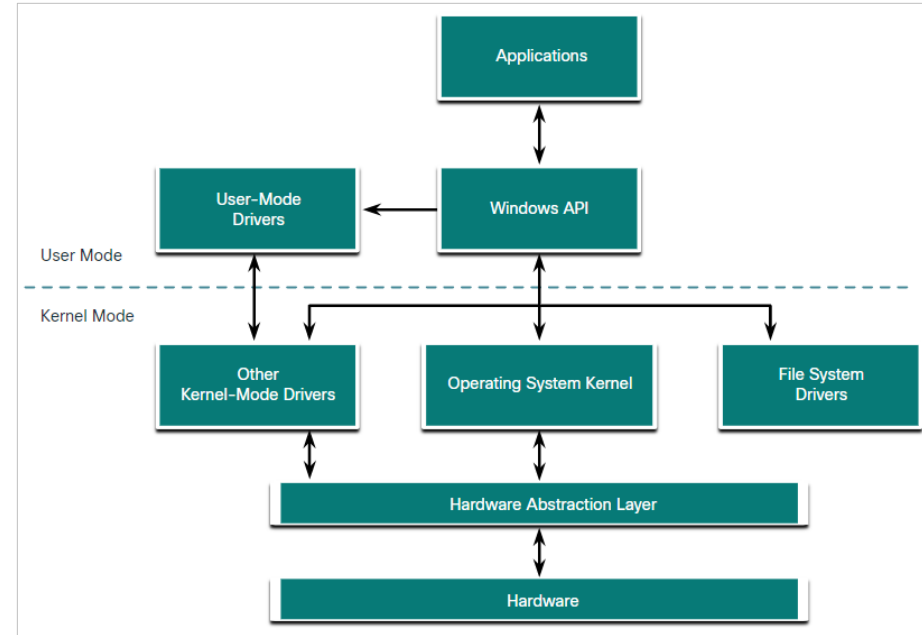
- Une couche d'abstraction du matériel est un logiciel qui gère l'ensemble des communications entre le matériel et le noyau.
- Le noyau est le cœur du système d'exploitation qui contrôle tout l'ordinateur.
- Il gère toutes les demandes d'entrée et de sortie, la mémoire ainsi que tous les appareils connectés à l'ordinateur.
- La figure illustre l'architecture Windows de base.



Architecture et fonctionnement de Windows

Mode utilisateur et mode noyau

- Le CPU peut fonctionner dans deux modes différents si Windows est installé, le mode utilisateur et le mode noyau.
- Les applications installées sont exécutées en mode utilisateur et le code du système d'exploitation est exécuté en mode noyau.
- Le code qui s'exécute en mode noyau utilise le même espace d'adressage.
- Lorsque le code est exécuté en mode utilisateur, il bénéficie de son propre espace d'adressage limité par le noyau ainsi que d'un processus créé spécifiquement pour l'application.



Systèmes de fichiers Windows

Un système de fichiers détermine la méthode d'organisation des informations sur les supports de stockage. Les systèmes de fichiers suivants sont pris en charge par Windows:

Systèmes de fichiers Windows	Description
exFAT	<ul style="list-style-type: none">• Ce système de fichiers simple est pris en charge par de nombreux systèmes d'exploitation.• La table d'allocation des fichiers impose des limites quant au nombre de partitions, à la taille des partitions et à la taille des fichiers qu'elle peut adresser ; elle n'est donc plus utilisée pour les disques durs (HD) ou les disques SSD (Solid State Drive).• Les tables FAT16 et FAT32 sont disponibles, FAT32 étant la plus commune, car elle présente moins de restrictions que la table FAT16.
Hierarchical File System Plus (HFS+)	<ul style="list-style-type: none">• Ce système de fichiers est utilisé sur les ordinateurs MAC OS X permet de gérer des noms de fichiers, des tailles de fichier et des tailles de partition.• Bien qu'il ne soit pas pris en charge par Windows sans logiciel spécial, Windows est capable de lire les données des partitions HFS+.

Systèmes de fichiers Windows (Suite)

Systèmes de fichiers Windows	Description
Extended File System (EXT)	<ul style="list-style-type: none">• Ce système de fichiers est utilisé avec les ordinateurs Linux.• Bien qu'il ne soit pas pris en charge par Windows, Windows est capable de lire les partitions EXT avec un logiciel spécial.
NTFS (New Technology File System)	<ul style="list-style-type: none">• Ce système de fichiers est le plus fréquemment utilisé lors de l'installation de Windows. Toutes les versions de Windows et Linux prennent en charge NTFS.• Les ordinateurs Mac-OS X ne peuvent lire qu'une partition NTFS. Ces ordinateurs écrivent sur une partition NTFS après l'installation de pilotes spéciaux.

Systèmes de fichiers Windows (Suite)

Le formatage NTFS crée d'importantes structures sur le disque pour le stockage des fichiers ainsi que des tables pour l'enregistrement des emplacements de fichiers :

- **Secteur de démarrage de la partition:** Il s'agit des 16 premiers secteurs du disque. Ce secteur contient l'emplacement de la table de fichier maître (MFT). Les 16 derniers secteurs contiennent une copie du secteur de démarrage.
- **Master File Table (MFT):** ce tableau contient les emplacements de tous les fichiers et répertoires sur la partition, notamment les attributs de fichiers tels que les informations de sécurité et les horodatages.
- **Fichiers système:** Ces fichiers cachés stockent des informations sur d'autres volumes et attributs de fichier.
- **Zone de fichiers** - Il s'agit de la zone principale de la partition où sont stockés les fichiers et les répertoires.

Remarque: Lors du formatage d'une partition, vous pouvez récupérer les données précédentes, car les données ne sont pas toutes définitivement supprimées. Il est recommandé d'effectuer une analyse sécurisée sur un lecteur réutilisé. L'analyse sécurisée écrit plusieurs fois les données sur la totalité du disque pour s'assurer qu'il ne reste aucune donnée.

Flux de données alternatifs

- NTFS stocke les fichiers sous la forme d'une série d'attributs, tels que le nom du fichier, ou d'un horodatage.
- Les données du fichier sont stockées dans l'attribut \$DATA et sont connues comme étant un flux de données.
- L'utilisation de NTFS vous permet de connecter des flux de données alternatifs au fichier.
- Un hacker peut stocker un programme malveillant dans un flux de données alternatif pour ensuite l'appeler depuis un autre fichier.
- Dans le système de fichiers NTFS, un fichier avec un flux de données alternatif est identifié après le nom de fichier et un signe deux-points, par exemple, **Testfile.txt:ADSdata**. Ce nom de fichier indique qu'un flux de données alternatif appelé ADS est associé au fichier **Testfile.txt**.

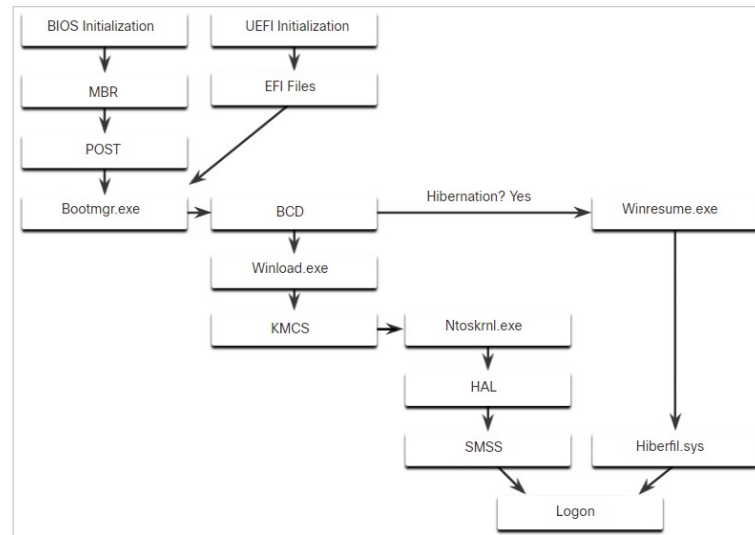
```
C:\ADS> echo "Alternate Data Here" > Testfile.txt:ADS
C:\ADS> dir
Volume in drive C is Windows
Volume Serial Number is A606-CB1B
Directory of C:\ADS
2020-04-28  04:01 PM    <DIR>          .
2020-04-28  04:01 PM    <DIR>          ..
2020-04-28  04:01 PM                0 Testfile.txt
                1 File(s)                0 bytes
                2 Dir(s)  43,509,571,584 bytes free

C:\ADS> more < Testfile.txt:ADS
"Alternate Data Here"
C:\ADS> dir /r
Volume in drive C is Windows
Volume Serial Number is A606-CB1B
Directory of C:\ADS
2020-04-28  04:01 PM    <DIR>          .
2020-04-28  04:01 PM    <DIR>          ..
2020-04-28  04:01 PM                0 Testfile.txt
                24 Testfile.txt:ADS:$DATA
                1 File(s)                0 bytes
                2 Dir(s)  43,509,624,832 bytes free

C:\ADS>
```

Processus de démarrage de Windows

- De nombreuses actions se produisent entre le moment où vous appuyez sur le bouton d'alimentation de l'ordinateur et le chargement total de Windows. Ceci est connu sous le nom de processus de démarrage Windows. Il existe deux types de microprogrammes informatiques:
- Système d'entrée-sortie de base (BIOS):** Le processus commence par la phase d'initialisation du BIOS dans laquelle les périphériques matériels sont initialisés et un POST est effectué. Lorsque le disque système est découvert, le POST se termine et recherche l'enregistrement de démarrage principal (MBR). Le BIOS exécute le code MBR et le système d'exploitation commence à se charger.
- L'interface UEFI démarre en chargeant les fichiers de programme EFI**, stockés au format .efi dans une partition de disque spéciale appelée « partition système EFI » (ESP).



Processus de démarrage de Windows (Suite)

- Que vous utilisiez le BIOS ou UEFI, le fichier **Bootmgr.exe** est exécuté une fois qu'une installation Windows valide est localisée.
- **Le fichier Bootmgr.exe** lit la base de données de configuration de démarrage (BCD).
- Si l'ordinateur quitte le mode de veille prolongée, le processus de démarrage se poursuit avec **Winresume.exe**.
- Si l'ordinateur effectue un démarrage à froid, le fichier **Winload.exe** est chargé.
- **Le fichier Winload.exe** utilise également la signature de code du mode noyau (KMCS) pour s'assurer que tous les pilotes sont signés numériquement.
- Une fois les pilotes examinés, le fichier **Winload.exe** exécute **Ntoskrnl.exe**, qui démarre le noyau Windows et configure la couche d'abstraction matérielle.

Remarque: *Un ordinateur qui utilise l'interface UEFI stocke le code de démarrage dans le micrologiciel. Cela permet d'augmenter la sécurité de l'ordinateur au démarrage, car l'ordinateur passe directement en mode protégé.*

Démarrage de Windows

- Deux éléments de registre importants permettent de démarrer automatiquement les applications et les services :
 - **HKEY_LOCAL_MACHINE : plusieurs aspects de la configuration Windows sont stockés dans cette clé, notamment les informations sur les services lancés à chaque démarrage.**
 - **HKEY_CURRENT_USER : plusieurs aspects liés à l'utilisateur connecté sont stockés dans cette clé, notamment les informations sur les services qui démarrent uniquement lorsque l'utilisateur se connecte à l'ordinateur.**
- Différentes entrées dans ces emplacements du Registre définissent les services et les applications qui démarreront en fonction de leur type.
- Parmi ces types, on compte Run, RunOnce, RunServices, RunServicesOnce et Userinit. Vous pouvez saisir ces entrées manuellement dans le registre, mais il est beaucoup plus sûr d'utiliser l'outil **Msconfig.exe**.
- Cet outil permet d'afficher et de modifier toutes les options de démarrage de l'ordinateur. Il ouvre la fenêtre Configuration du système.

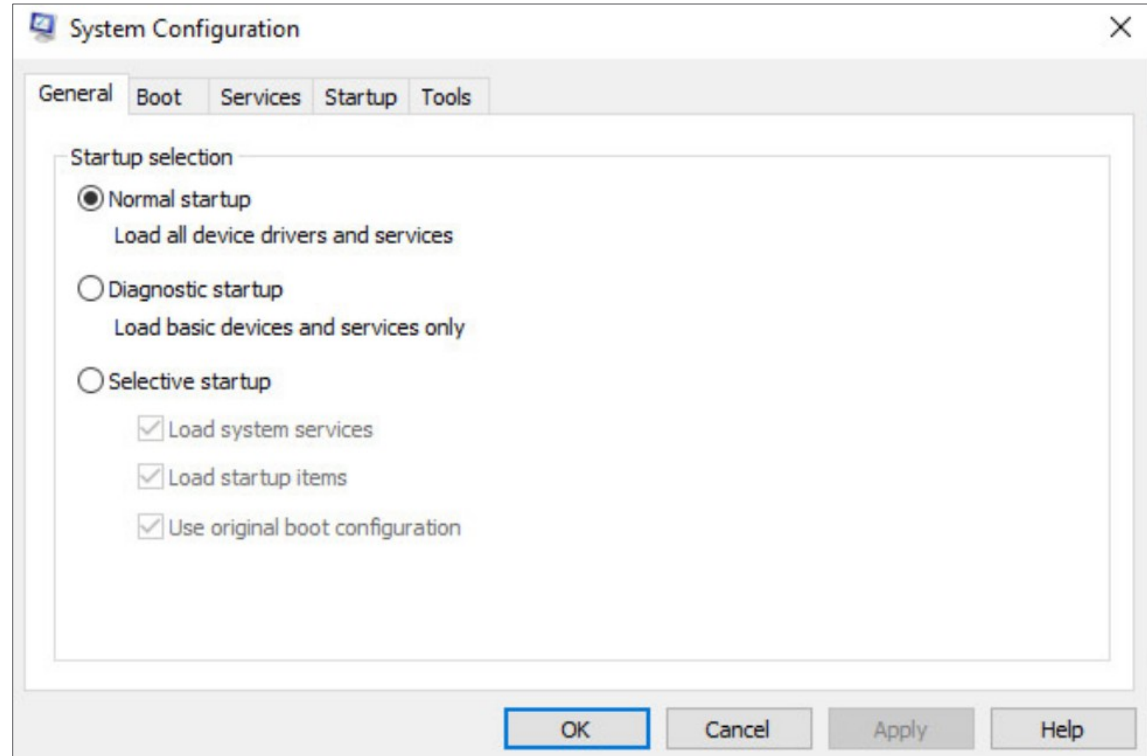
Démarrage de Windows (Suite)

There are five tabs that contain the configuration options.

Généralités

Three different startup types can be chosen here:

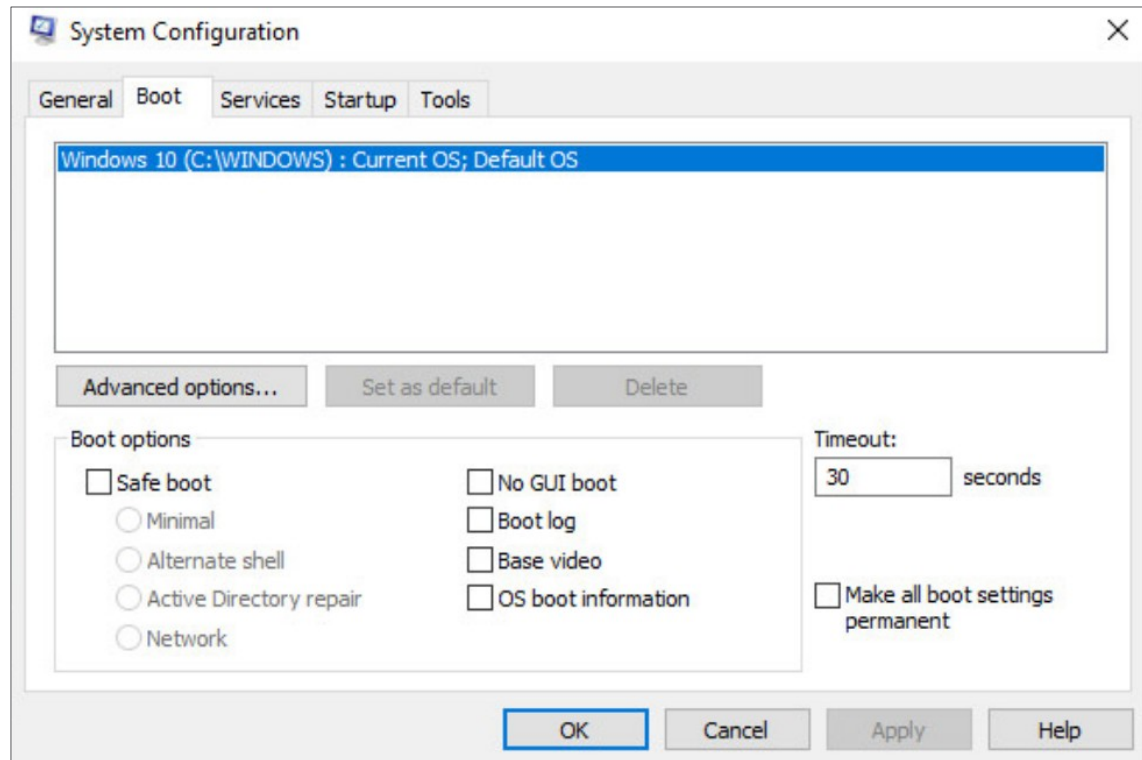
- Le démarrage normal charge tous les pilotes et les services.
- Le démarrage en mode diagnostic charge uniquement les pilotes et les services de base.
- Le démarrage sélectif permet à l'utilisateur de choisir les éléments à charger au démarrage.



Démarrage de Windows (Suite)

Démarrer

- Vous pouvez sélectionner n'importe quel système d'exploitation installé en vue de le démarrer.
- Vous disposez également d'options de démarrage sécurisé pour résoudre les problèmes de démarrage.

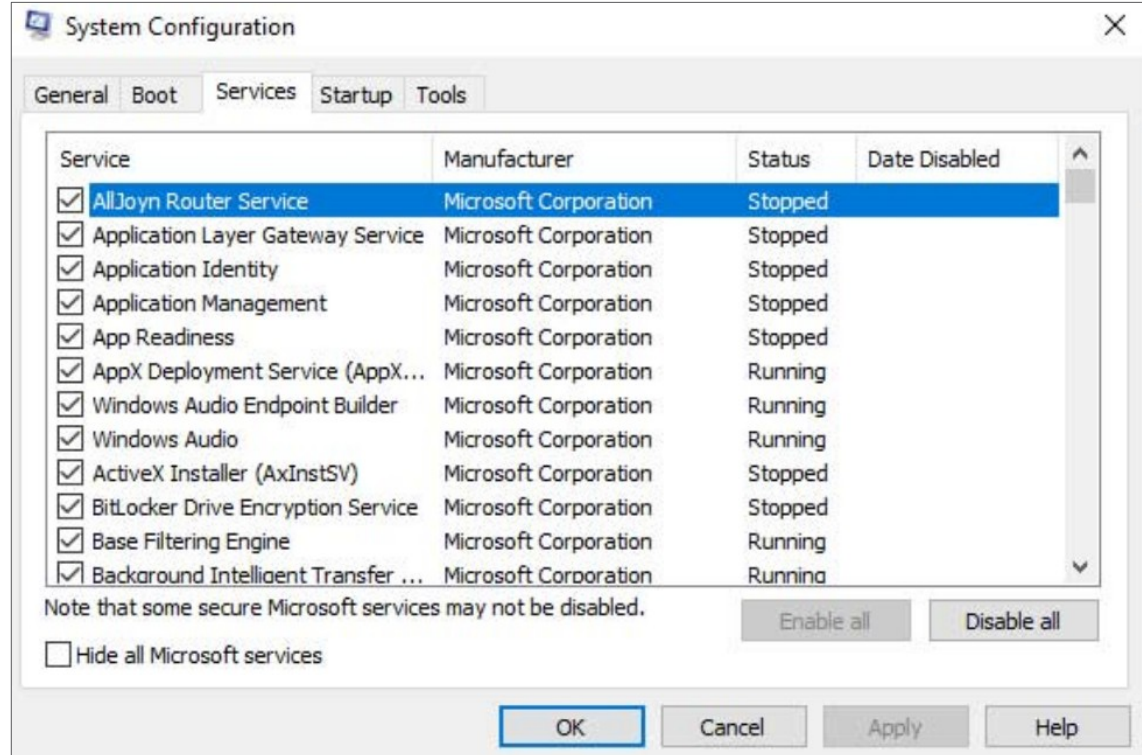


Architecture et fonctionnement de Windows

Démarrage de Windows (Suite)

Services

- Cette liste vous permet de sélectionner les services installés que vous souhaitez lancer au démarrage.

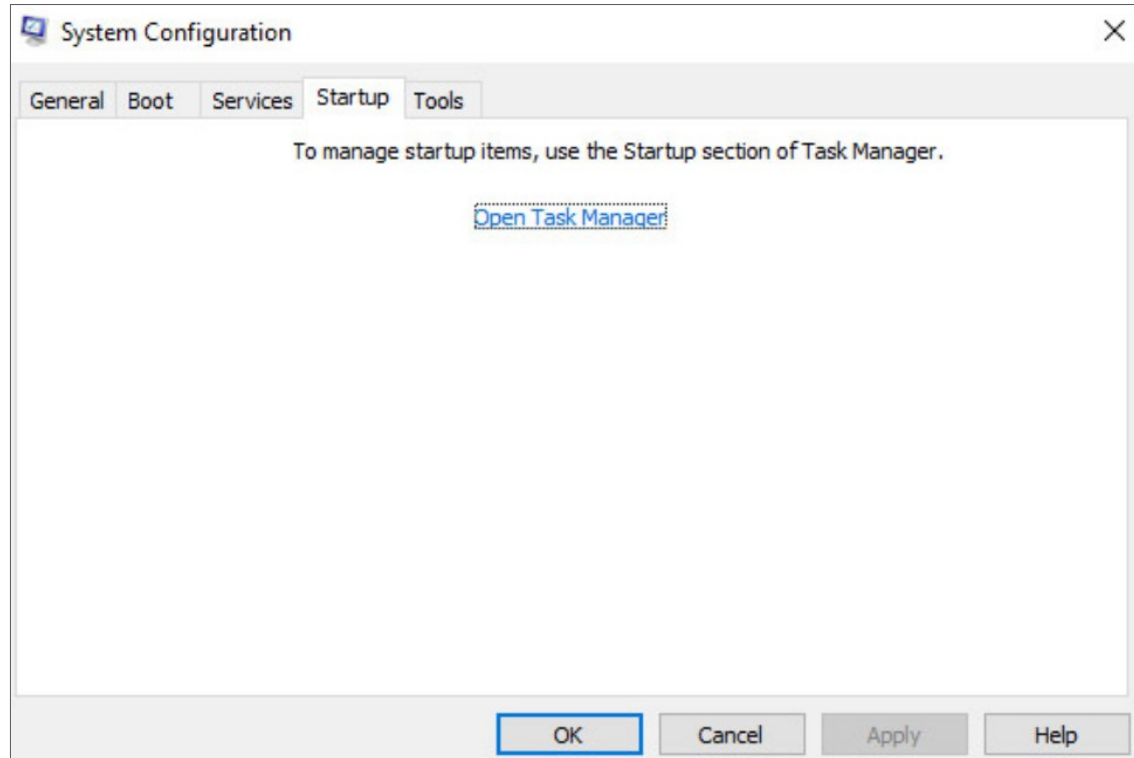


Architecture et fonctionnement de Windows

Démarrage de Windows (Suite)

Démarrage

- Vous pouvez sélectionner ou désélectionner les applications et les services à lancer automatiquement au démarrage pour cela, ouvrez le gestionnaire des tâches à partir de cet onglet.

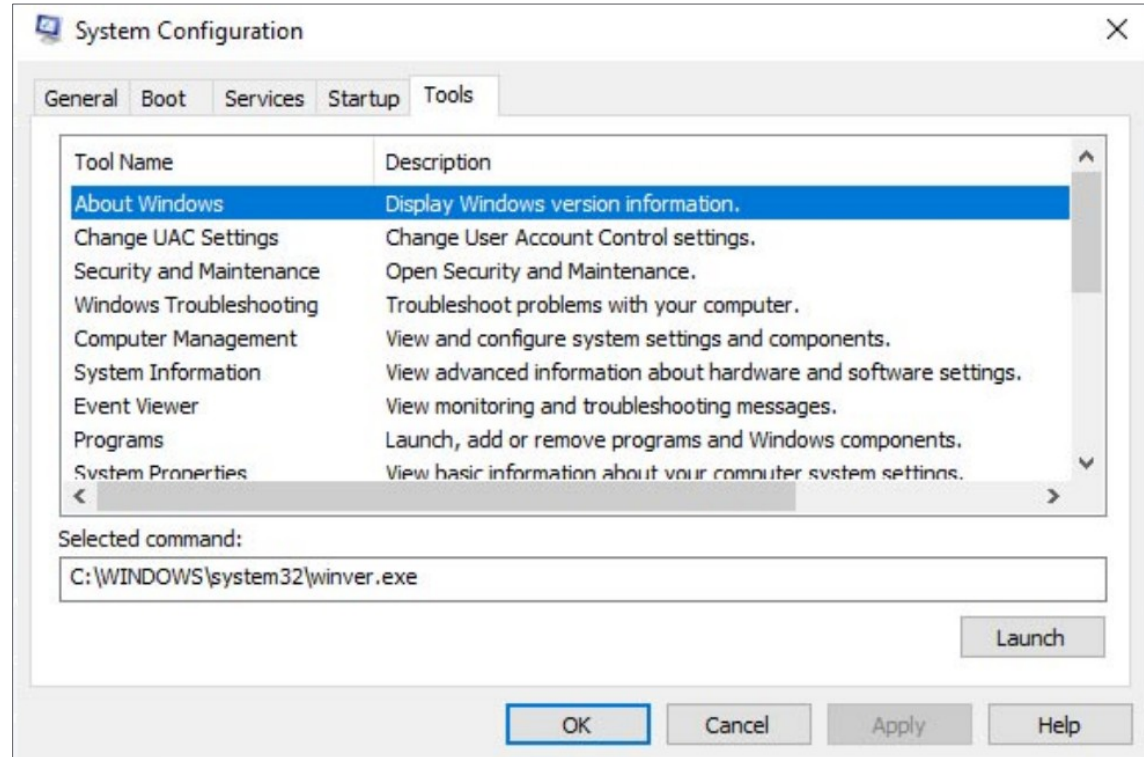


Architecture et fonctionnement de Windows

Démarrage de Windows (Suite)

Outils

- vous pouvez lancer de nombreux outils courants du système d'exploitation directement à partir de cet onglet.



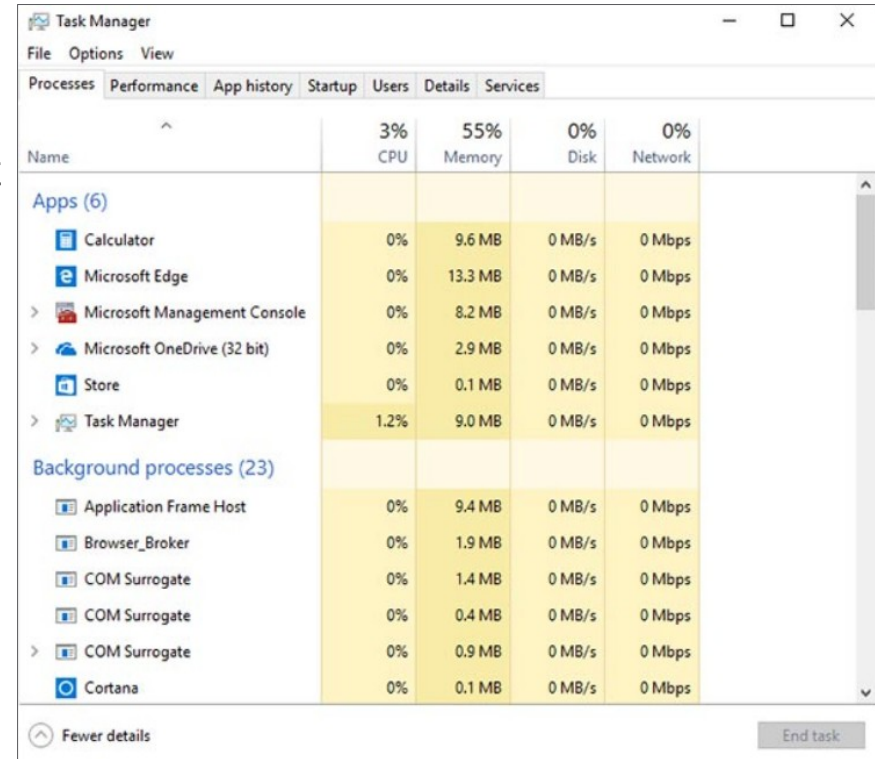
Démarrage et arrêt de Windows

- Il est toujours préférable d'arrêter les tâches en cours avant d'éteindre l'ordinateur. L'ordinateur a besoin de temps pour fermer les applications, arrêter chaque service et enregistrer les modifications de configuration avant la mise hors tension.
- Pendant l'arrêt, l'ordinateur ferme tout d'abord les applications en mode utilisateur, puis les processus en mode noyau.
- Il existe plusieurs façons d'arrêter un ordinateur Windows : à l'aide des options d'alimentation du menu Démarrer, à l'aide de la commande **shutdown** de la ligne de commande ou en appuyant sur les touches **Ctrl + Alt + Suppr** tout en cliquant sur l'icône d'alimentation.
- Il y a trois options différentes à choisir lors de l'arrêt de l'ordinateur:
 - **Arrêt** : éteint l'ordinateur (hors tension).
 - **Redémarrer** : redémarre l'ordinateur (hors tension et mise sous tension).
 - **Hibernater** : enregistre l'état actuel de l'ordinateur et de l'environnement utilisateur et le stocke dans un fichier. La mise en veille prolongée permet à l'utilisateur de reprendre rapidement la session au point où il l'a laissée, avec les fichiers et programmes encore ouverts.

Architecture et fonctionnement de Windows

Processus, threads et services

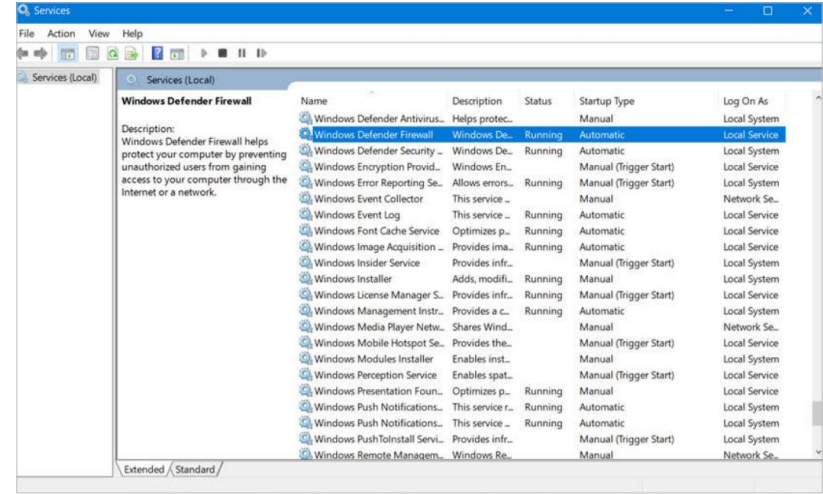
- Une application Windows est composée de divers processus. Un processus est un programme en cours d'exécution.
- Chaque processus en cours d'exécution contient au moins un thread. Un thread est une partie du processus qui peut être exécutée.
- Pour configurer les processus Windows, ouvrez le Gestionnaire des tâches. La figure illustre l'onglet Processus du Gestionnaire des tâches.
- Tous les threads dédiés à un processus sont contenus dans le même espace d'adressage, ce qui signifie que ces threads peuvent ne pas accéder à l'espace d'adressage d'un autre processus. afin d'éviter de l'endommager.



Name	3% CPU	55% Memory	0% Disk	0% Network
Apps (6)				
Calculator	0%	9.6 MB	0 MB/s	0 Mbps
Microsoft Edge	0%	13.3 MB	0 MB/s	0 Mbps
Microsoft Management Console	0%	8.2 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)	0%	2.9 MB	0 MB/s	0 Mbps
Store	0%	0.1 MB	0 MB/s	0 Mbps
Task Manager	1.2%	9.0 MB	0 MB/s	0 Mbps
Background processes (23)				
Application Frame Host	0%	9.4 MB	0 MB/s	0 Mbps
Browser_Broker	0%	1.9 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.9 MB	0 MB/s	0 Mbps
Cortana	0%	0.1 MB	0 MB/s	0 Mbps

Processus, threads et services (Suite)

- Certains processus exécutés sous Windows sont des services. Ce sont des programmes qui s'exécutent en arrière-plan pour prendre en charge le système d'exploitation et les applications.
- Les services fournissent des fonctionnalités de longue durée, tels que l'accès sans fil ou l'accès à un serveur FTP.
- Pour configurer les services Windows, recherchez les services. La figure illustre l'applet du panneau de configuration des services Windows.
- Configurez ces services avec une extrême précaution. L'arrêt d'un service peut avoir une incidence négative sur les applications ou d'autres services.

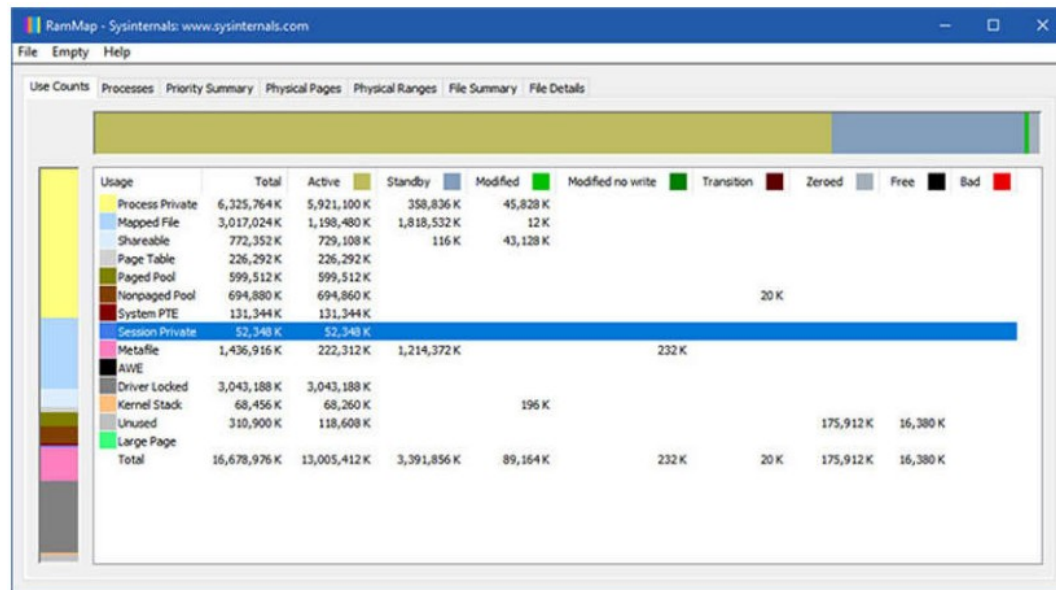


Allocation de mémoire et handles

- L'espace d'adressage virtuel d'un processus est un ensemble d'adresses virtuelles utilisables par le processus.
- L'adresse virtuelle ne correspond pas à l'emplacement physique réel dans la mémoire, mais à une entrée dans une table de pagination utilisée pour traduire l'adresse virtuelle en adresse physique.
- Chaque processus d'un ordinateur Windows 32 bits prend en charge un espace d'adressage virtuel de 4 gigaoctets maximum.
- Chaque processus d'un ordinateur Windows 64 bits prend en charge un espace d'adressage virtuel de 8 téraoctets.
- Chaque processus de l'espace utilisateur s'exécute dans un espace d'adressage privé, séparé des autres processus de l'espace utilisateur.
- Lorsque le processus de l'espace utilisateur doit accéder aux ressources du noyau, il doit utiliser un handle de processus.
- Comme le processus d'espace utilisateur n'est pas autorisé à accéder directement à ces ressources du noyau, le gestionnaire de processus fournit l'accès nécessaire au processus d'espace utilisateur sans connexion directe à celui-ci.

Allocation de mémoire et handles (Suite)

- Un outil puissant pour afficher l'allocation de mémoire est RamMap, qui est illustré dans la figure.
- RamMap fait partie de la suite d'outils Sysinternals de Windows. Il peut être téléchargé à partir de Microsoft.
- RamMap fournit des informations sur la façon dont Windows a alloué de la mémoire système au noyau, aux processus, aux pilotes et aux applications.



Registre Windows

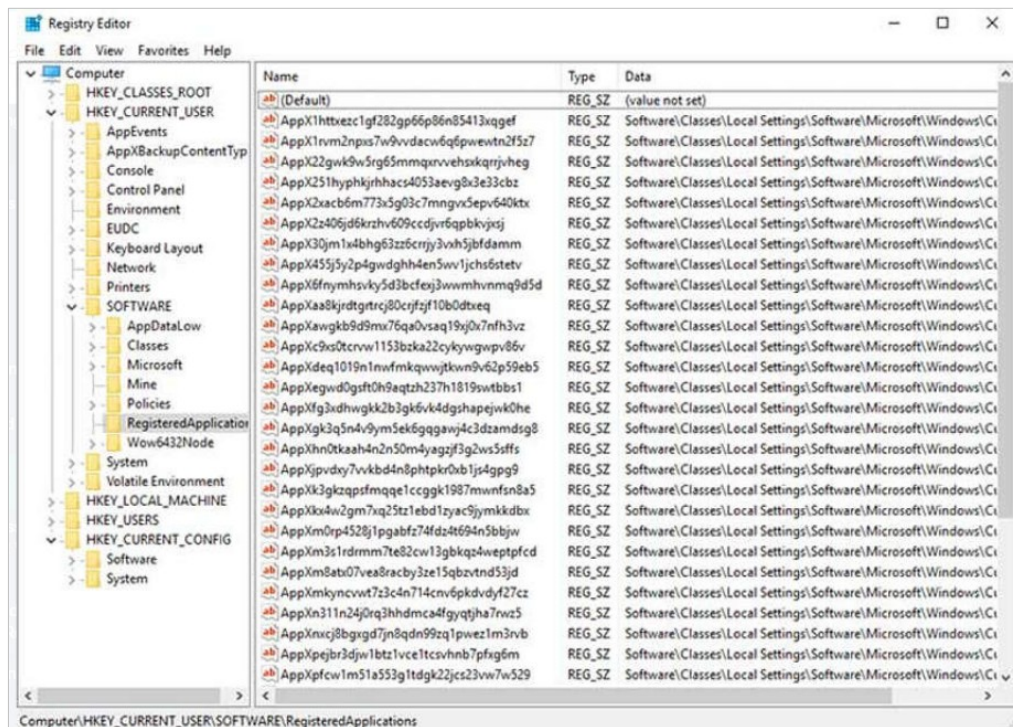
- Windows stocke toutes les informations relatives aux paramètres du matériel, des applications, des utilisateurs et du système dans une grande base de données appelée le Registre.
- Le registre est une base de données hiérarchique dont le niveau le plus élevé est appelé « ruche », et dont les niveaux inférieurs sont appelés clés ou sous-clés, respectivement.
- Les valeurs stockent les données et les enregistrent dans les clés et les sous-clés. La clé de registre peut comporter jusqu'à 512 niveaux.
- Le tableau répertorie les cinq ruches du registre Windows.

Ruche du registre	Description
HKEY_CURRENT_USER (HKCU)	Contient des informations sur l'utilisateur actuellement connecté.
HKEY_USERS (HKU)	Contient des informations sur les comptes d'utilisateur sur l'hôte.
HKEY_CLASSES_ROOT (HKCR)	Contient des informations sur la liaison d'objets et l'incorporation d'enregistrements (OLE). Il permet aux utilisateurs d'incorporer des objets d'autres applications dans un seul document.
HKEY_LOCAL_MACHINE (HKLM)	Contient des informations relatives au système.
HKEY_CURRENT_CONFIG (HKCC)	Contient des informations sur le profil matériel actuel.

Architecture et fonctionnement de Windows

Registre Windows (Suite)

- Il est impossible de créer de nouvelles ruches. En revanche, il est possible de créer, modifier ou supprimer des clés et des valeurs de registre dans les ruches via un compte disposant de privilèges d'administrateur.
- Comme le montre la figure, l'outil **regedit.exe** permet de modifier le registre.
- Utilisez cet outil avec une extrême précaution. Toute modification, aussi insignifiante soit-elle, peut avoir des conséquences graves, voire dramatiques, sur le registre.



Registre Windows (Suite)

- La navigation dans le registre est similaire à l'Explorateur de fichiers Windows.
- Utilisez le panneau de gauche pour parcourir les ruches et la structure inférieure, et le panneau de droite pour afficher le contenu de l'élément en surbrillance dans le panneau de gauche.
- Ce chemin s'affiche au bas de la fenêtre.
- Les clés de registre contiennent une sous-clé ou une valeur. Les différentes valeurs que peuvent contenir les clés sont les suivants:
 - **REG_BINARY:** Nombres ou valeurs booléennes
 - **REG_DWORD:** Nombres supérieurs à 32 bits ou données brutes
 - **REG_SZ:** Valeurs de chaîne
- Le registre contient également des données concernant l'activité d'un utilisateur pendant l'utilisation quotidienne de l'ordinateur,
- notamment l'historique des appareils et des appareils ayant été connectés à l'ordinateur (nom, fabricant et numéro de série).

Travaux pratiques – Découvrir les processus, les threads, les handles et le Registre Windows

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Vous allez découvrir les processus, les threads et les handles à l'aide de Process Explorer de Sysinternals Suite.
- Utiliser le Registre Windows pour modifier un paramètre.

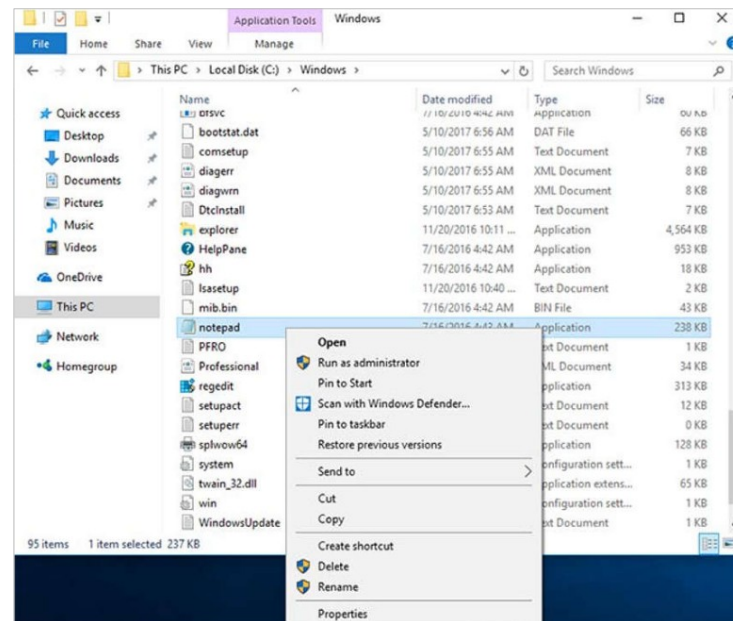
3.3 Configuration et surveillance de Windows

Exécution en tant qu'administrateur

- Pour des raisons de sécurité, il est déconseillé de se connecter à Windows avec le compte d'administrateur ou un compte disposant de privilèges d'administrateur.
- Vous devrez parfois exécuter ou installer un logiciel qui exige des privilèges d'administrateur.

Administrateur

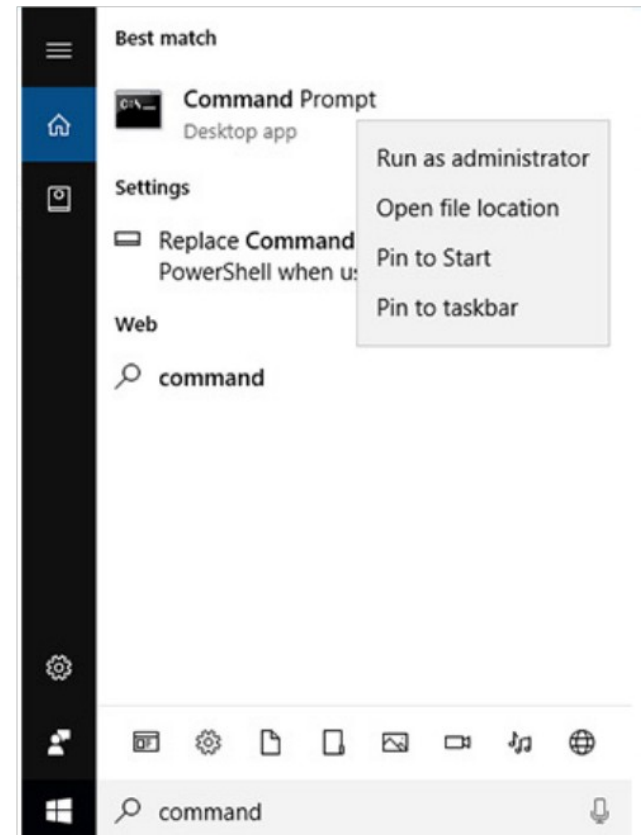
- Cliquez avec le bouton droit de la souris sur la commande dans l'Explorateur de fichiers et choisissez Exécuter en tant qu'administrateur dans le menu contextuel..



Exécution en tant qu'administrateur (Suite)

L'invite de commande d'administrateur

- Recherchez la **commande**, cliquez avec le bouton droit de la souris sur le fichier exécutable, puis choisissez Exécuter en tant qu'administrateur dans le menu contextuel.
- Toutes les commandes exécutées à partir de cette ligne de commande disposent de privilèges d'administrateur, y compris l'installation du logiciel.



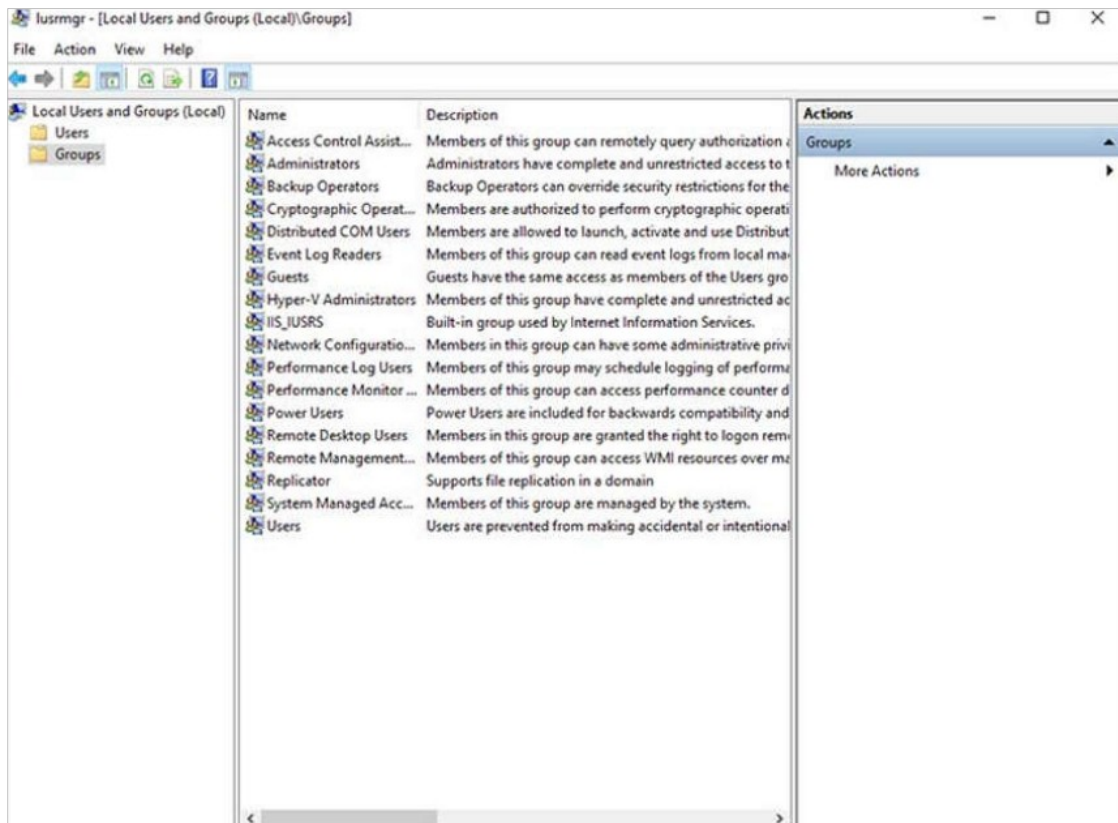
Utilisateurs locaux et domaines

- Lorsque vous démarrez un nouvel ordinateur pour la première fois ou que vous installez Windows, vous devrez créer un compte utilisateur appelé « utilisateur local ».
- Ce compte contient les paramètres de personnalisation, les autorisations d'accès, les emplacements de fichiers ainsi que de nombreuses autres données propres à l'utilisateur.
- Pour faciliter l'administration des utilisateurs, Windows utilise des groupes. Un groupe possède un nom et dispose d'un ensemble d'autorisations spécifiques.
- Lorsqu'un utilisateur est placé dans un groupe, les autorisations de ce groupe sont accordées à cet utilisateur.
- Un utilisateur peut appartenir à plusieurs groupes afin de disposer de diverses autorisations. Lorsque les autorisations se répètent, certaines d'entre elles, telles que « refuser explicitement », remplacent l'autorisation accordée par un groupe différent.
- Il existe de nombreux groupes d'utilisateurs différents intégrés à Windows, chacun étant destiné à des tâches spécifiques.

Configuration et surveillance de Windows

Utilisateurs locaux et domaines

- Les utilisateurs et les groupes locaux sont gérés à l'aide de l'applet **lusrmgr.msc** du panneau de configuration, comme le montre la figure.
- Windows permet également d'utiliser des domaines pour définir des autorisations. Un domaine est un type de service de réseau où tous les utilisateurs, les groupes, les ordinateurs, les périphériques et les paramètres de sécurité sont stockés dans une base de données et sont contrôlés par celle-ci.



Interface de ligne de commande et PowerShell

- L'interface de ligne de commande Windows permet d'exécuter des programmes, de parcourir le système de fichiers et de gérer les fichiers et les dossiers.
- Pour ouvrir l'interface de ligne de commande Windows, recherchez **cmd.exe** et cliquez sur le programme. Voici quelques points à retenir lors de l'utilisation de l'interface de ligne de commande :
 - Par défaut, les noms de fichiers et les chemins d'accès ne sont pas sensibles à la casse.
 - Les appareils de stockage se voient attribuer une lettre de référence. Ceci est suivi d'un deux-points et d'une barre oblique inverse (\).
 - Les commandes qui ont des commutateurs optionnels utilisent la barre oblique avant (/) pour délimiter la commande et l'option de commutateur.
 - Vous pouvez utiliser la touche **Tab** pour renseigner automatiquement les commandes lors du référencement des répertoires ou des fichiers.
 - Windows conserve un historique des commandes saisies lors d'une session d'interface de ligne de commande. Vous pouvez accéder aux commandes historiques à l'aide des flèches vers le haut et vers le bas.
 - Pour passer d'un appareil de stockage à un autre, saisissez la lettre de l'appareil suivie de deux-points, puis appuyez sur **Enter**.

Interface de ligne de commande et PowerShell (Suite)

- Un autre environnement, appelé Windows PowerShell, permet de créer des scripts d'automatisation des tâches que l'interface de ligne de commande standard ne peut pas créer.
- PowerShell fournit également une interface de ligne de commande pour exécuter des commandes.
- PowerShell est un programme intégré dans Windows.
- À l'instar de l'interface de ligne de commande, le programme PowerShell peut être exécuté avec des privilèges d'administrateur.
- PowerShell peut exécuter les types de commandes suivants :
 - **Applets de commande** : ces commandes exécutent une action et renvoient un résultat ou un objet à la commande à exécuter suivante.
 - **Scripts PowerShell** - ces fichiers portant l'extension **.ps1** contiennent les commandes PowerShell qui sont exécutées.
 - **Fonctions PowerShell** - il s'agit d'extraits de code pouvant être référencés dans un script.

Interface de ligne de commande et PowerShell (Suite)

- Pour en savoir plus sur le PowerShell Windows et commencer à l'utiliser, tapez **help** dans PowerShell, comme le montre la sortie de commande.
- Il existe quatre niveaux d'aide dans le PowerShell Windows :
 - **get-help PS command** - Affiche les rubriques d'aide de base d'une commande
 - **get-help PS command [-examples]** - Affiche les rubriques d'aide de base d'une commande avec des exemples
 - **get-help PS command [-detailed]** - Affiche les rubriques d'aide détaillées d'une commande avec des exemples
 - **get-help PS command [-full]** - Affiche les rubriques d'aide complètes d'une commande avec des exemples

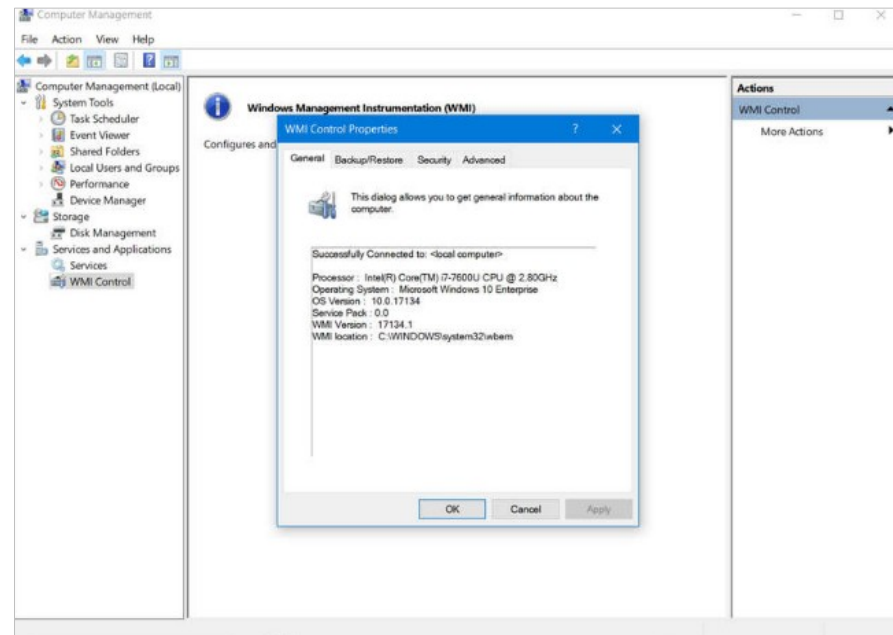
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32> help
TOPIC
    Windows PowerShell Help System
SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.
LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.
    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.
    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.
    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.
ONLINE HELP
    You can find help for Windows PowerShell online in the TechNet Library
    beginning at http://go.microsoft.com/fwlink/?LinkID=198518.
    To open online help for any cmdlet or function, type:
        Get-Help <cmdlet-name> -Online
UPDATE-HELP
    To download and install help files on your computer:
        1. Start Windows PowerShell with the "Run as administrator" option.
        2. Type:
            Update-Help
    After the help files are installed, you can use the Get-Help cmdlet to
    display the help topics. You can also use the Update-Help cmdlet to
    download updated help files so that your local help files are always
    up-to-date.
    For more information about the Update-Help cmdlet, type:
        Get-Help Update-Help -Online
-- More --
```

WMI

- Windows Management Instrumentation (WMI) est utilisé pour gérer les ordinateurs distants.
- Cette fonction peut collecter des informations statistiques sur les composants, le matériel et les logiciels, et gérer l'intégrité des ordinateurs distants.
- Pour ouvrir le contrôle WMI à partir du Panneau de configuration, double-cliquez sur **Outils d'administration > Gestion de l'ordinateur** pour ouvrir la fenêtre Gestion de l'ordinateur, développez l'arborescence **Services et applications** et cliquez avec le bouton droit sur l'**icône Contrôle WMI Propriétés**.

Configuration et surveillance de Windows WMI (Suite)

- La figure de gauche représente la fenêtre Propriétés de : Contrôle WMI. La fenêtre Propriétés de : Contrôle WMI comporte quatre onglets :
- **Général** : cet onglet contient des informations récapitulatives sur l'ordinateur local et WMI
- **Sauvegarder/Restaurer**- Sauvegarder manuellement les statistiques recueillies par WMI
- **Sécurité** : cet onglet contient des paramètres pour définir les utilisateurs ayant accès aux différentes statistiques WMI
- **Options avancées** : cet onglet contient des paramètres pour configurer l'espace de noms par défaut pour WMI



La commande net

- La commande **net**, qui permet de gérer et d'assurer la maintenance du système d'exploitation.
- La commande **net** prend en charge plusieurs autres commandes qui suivent la commande et peut être combinée avec des options pour obtenir un résultat spécifique.
- Pour afficher la liste des nombreuses commandes **net**, tapez **net help** à l'invite de commande.
- La sortie de commande présente les commandes prises en charge par la commande **net**.
- Pour afficher les rubriques d'aide d'une commande **net**, tapez **C:\>net help**.

```
C:\> net help
The syntax of this command is:
NET HELP
command
-or-
NET command /HELP
Commands available are:
NET ACCOUNTS      NET HELPMSG      NET STATISTICS
NET COMPUTER      NET LOCALGROUP   NET STOP
NET CONFIG         NET PAUSE        NET TIME
NET CONTINUE      NET SESSION      NET USE
NET FILE           NET SHARE        NET USER
NET GROUP          NET START        NET VIEW
NET HELP
NET HELP NAMES explains different types of names in NET HELP syntax lines.
NET HELP SERVICES lists some of the services you can start.
NET HELP SYNTAX explains how to read NET HELP syntax lines.
NET HELP command | MORE displays Help one screen at a time.
C:\>
```

La commande net (Suite)

Le tableau suivant répertorie certaines commandes **réseau** courantes :

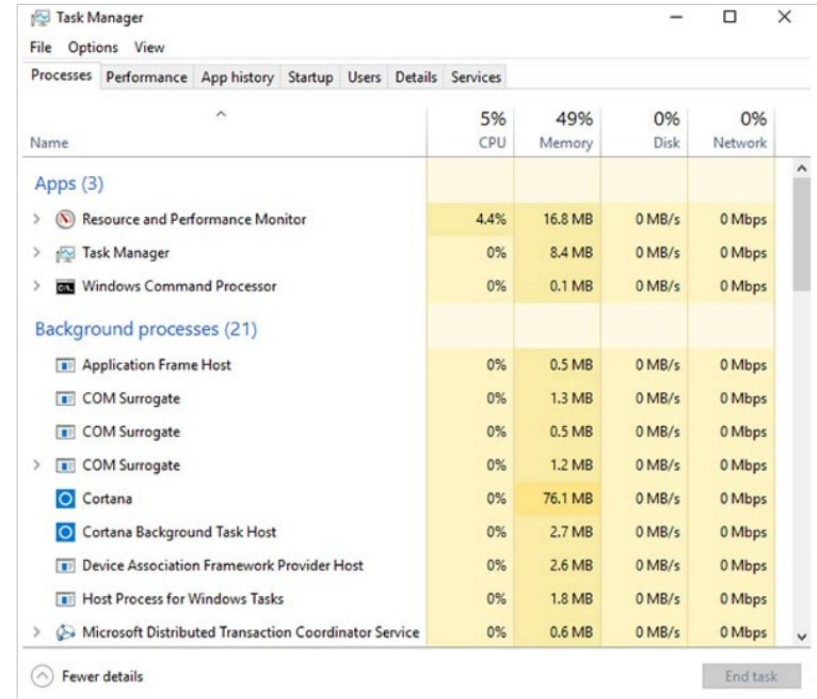
Commande	Description
net accounts	Définit les exigences de mot de passe et de connexion pour les utilisateurs
net session	Répertorie ou déconnecte les sessions entre un ordinateur et d'autres ordinateurs sur le réseau
net share	Crée, supprime ou gère des ressources partagées
net start	Démarre un service réseau ou répertorie les services réseau en cours d'exécution
net stop	Arrête un service réseau
net use	Se connecte, se déconnecte et affiche des informations sur les ressources réseau partagées
net view	Affiche une liste des ordinateurs et des appareils sur le réseau

Le gestionnaire des tâches et le moniteur de ressources

L'administrateur dispose de deux outils très utiles qui l'aident à comprendre les divers services, applications et processus qui s'exécutent sur un ordinateur Windows.

Gestionnaire des tâches

- Le gestionnaire des tâches présenté à la figure fournit de nombreuses informations sur tout ce qui est en cours d'exécution et sur les performances générales de l'ordinateur.
- Le Gestionnaire des tâches de Windows 10 comporte sept onglets.



The screenshot shows the Windows Task Manager window with the 'Performance' tab selected. The window title is 'Task Manager' and it has a menu bar with 'File', 'Options', and 'View'. Below the menu bar are tabs for 'Processes', 'Performance', 'App history', 'Startup', 'Users', 'Details', and 'Services'. The 'Performance' tab displays a table of system resource usage. The table has five columns: 'Name', 'CPU', 'Memory', 'Disk', and 'Network'. The 'CPU' column shows 5%, 'Memory' shows 49%, 'Disk' shows 0%, and 'Network' shows 0%. The table is divided into two sections: 'Apps (3)' and 'Background processes (21)'. The 'Apps (3)' section lists 'Resource and Performance Monitor' (4.4% CPU, 16.8 MB Memory), 'Task Manager' (0% CPU, 8.4 MB Memory), and 'Windows Command Processor' (0% CPU, 0.1 MB Memory). The 'Background processes (21)' section lists various system processes, including 'Application Frame Host', 'COM Surrogate', 'Cortana', 'Cortana Background Task Host', 'Device Association Framework Provider Host', 'Host Process for Windows Tasks', and 'Microsoft Distributed Transaction Coordinator Service'. The 'Cortana' process is highlighted with a blue icon and shows 76.1 MB of memory usage. At the bottom of the window, there is a 'Fewer details' button on the left and an 'End task' button on the right.

Name	5% CPU	49% Memory	0% Disk	0% Network
Apps (3)				
Resource and Performance Monitor	4.4%	16.8 MB	0 MB/s	0 Mbps
Task Manager	0%	8.4 MB	0 MB/s	0 Mbps
Windows Command Processor	0%	0.1 MB	0 MB/s	0 Mbps
Background processes (21)				
Application Frame Host	0%	0.5 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.3 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.5 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.2 MB	0 MB/s	0 Mbps
Cortana	0%	76.1 MB	0 MB/s	0 Mbps
Cortana Background Task Host	0%	2.7 MB	0 MB/s	0 Mbps
Device Association Framework Provider Host	0%	2.6 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	1.8 MB	0 MB/s	0 Mbps
Microsoft Distributed Transaction Coordinator Service	0%	0.6 MB	0 MB/s	0 Mbps

Le gestionnaire des tâches et le moniteur de ressources (Suite)

Le tableau suivant décrit les sept onglets du Gestionnaire des tâches :

Onglets Gestionnaire des tâches	Description
Processus	<ul style="list-style-type: none">• Répertorie tous les programmes et processus en cours d'exécution.• Affiche le processeur, la mémoire, le disque et l'utilisation du réseau de chaque processus.• Les propriétés peuvent être examinées ou terminées si elles ne se comportent pas correctement ou si elles sont bloquées.
Performances	<ul style="list-style-type: none">• Afficher toutes les statistiques de performance concernant le processeur, la mémoire, le disque et le réseau.• Cliquez sur chaque élément dans le volet de gauche pour afficher les statistiques détaillées correspondantes dans le volet de droite.
Historique de l'application	<ul style="list-style-type: none">• L'utilisation des ressources de chaque application identifie les applications qui consomment plus de ressources que prévu.• cliquez sur Options et sur Afficher l'historique pour tous les processus pour afficher l'historique des processus exécutés depuis le démarrage de l'ordinateur.
Démarrage	<ul style="list-style-type: none">• Toutes les applications et tous les services exécutés au démarrage de l'ordinateur sont affichés dans cet onglet.• Pour éviter l'exécution d'un programme au démarrage, cliquez avec le bouton droit de la souris sur un élément et choisissez Désactiver.

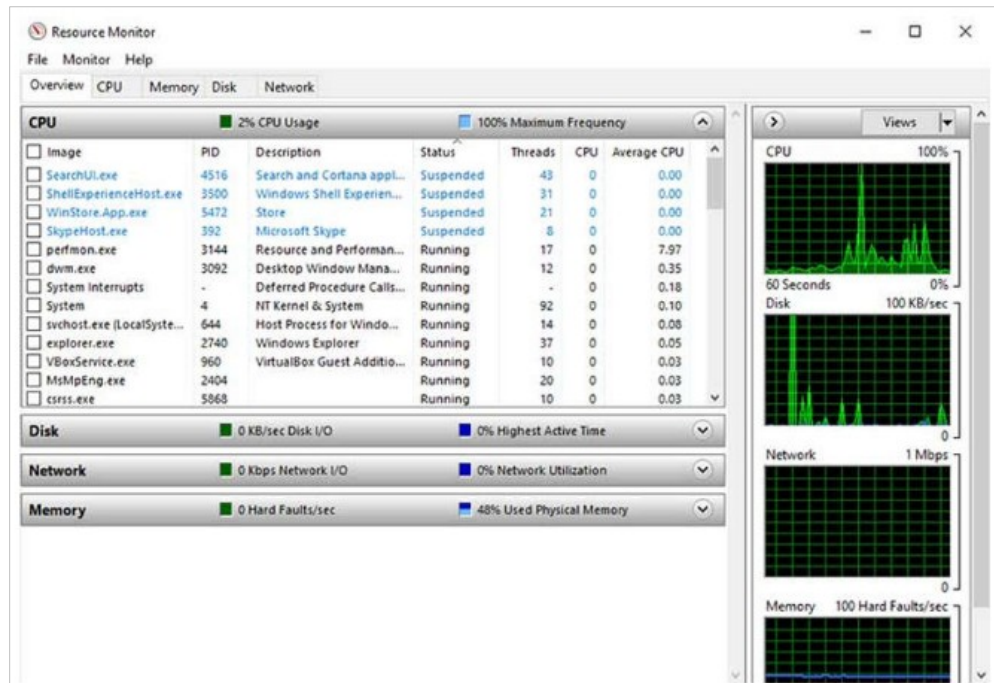
Le gestionnaire des tâches et le moniteur de ressources (Suite)

Onglets Gestionnaire des tâches	Description
Utilisateurs	<ul style="list-style-type: none">• Tous les utilisateurs connectés à l'ordinateur et toutes les ressources utilisées par les applications et processus de chaque utilisateur sont affichés dans cet onglet.• Dans cet onglet, un administrateur peut déconnecter un utilisateur de l'ordinateur.
En savoir plus	<ul style="list-style-type: none">• Cet onglet fournit des options de gestion supplémentaires pour les processus, notamment la définition d'une priorité de façon à ce que le processeur consacre plus ou moins de temps à un processus.• Il est également possible de définir l'affinité UC, qui détermine le noyau ou le processeur que doit utiliser un programme.• Une fonction utile appelée Analyser la chaîne d'attente indique les processus pour lesquels un autre processus est en attente. Cette fonction permet de déterminer si un processus est en attente ou est bloqué.
Services	<ul style="list-style-type: none">• Tous les services qui sont chargés sont affichés dans cet onglet.• L'ID du processus (PID), une brève description et le statut « En cours » ou « Arrêté » sont également indiqués.• Un bouton situé dans la partie inférieure permet d'ouvrir la console Services, qui fournit d'autres options de gestion des services.

Le gestionnaire des tâches et le moniteur de ressources (Suite)

Contrôle des ressources

- Si vous avez besoin d'informations plus détaillées sur l'utilisation des ressources, vous pouvez consulter le moniteur de ressources.
- Lorsque vous cherchez à comprendre les raisons d'un dysfonctionnement de l'ordinateur, le Moniteur de ressources peut vous aider à déterminer l'origine du problème.
- Le Moniteur de ressources comporte cinq onglets :



Le gestionnaire des tâches et le moniteur de ressources (Suite)

Le tableau suivant décrit les cinq onglets du Moniteur de ressources :

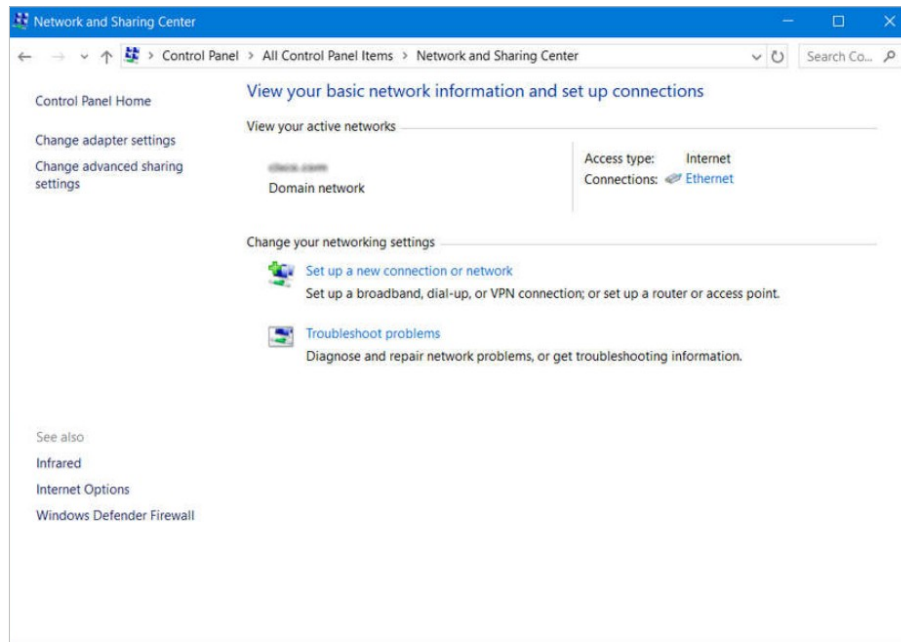
Onglets du moniteur de ressources	Description
Présentation	L'onglet affiche l'utilisation générale de chaque ressource.
Processeur	<ul style="list-style-type: none">• Il indique le PID, le nombre de threads, les processeurs utilisés par le processus et l'utilisation moyenne de chaque processus par le processeur.• Pour obtenir des informations supplémentaires sur les services sur lesquels le processus repose et sur les handles et les modules associés, développez les lignes inférieures.
Mémoire	Toutes les informations statistiques sur la façon dont chaque processus utilise la mémoire sont affichées dans cet onglet et une vue d'ensemble de l'utilisation de toute la RAM est affichée sous la ligne Processus.
Disque	Il répertorie les processus qui utilisent un disque; il indique par ailleurs les statistiques de lecture/écriture, et fournit un aperçu de chaque appareil de stockage.
Réseau	<ul style="list-style-type: none">• Il répertorie les processus qui utilisent le réseau; il indique par ailleurs les statistiques de lecture/écriture.• Cet onglet est très utile lorsque vous tentez d'identifier les applications et les processus qui communiquent sur le réseau. Indiquez également si un processus non autorisé accède au réseau.

Mise en réseau

- L'une des fonctionnalités les plus importantes d'un système d'exploitation est la capacité de l'ordinateur à se connecter à un réseau.
- Le centre Réseau et partage permet de configurer et de tester les propriétés du réseau Windows.

Centre Réseau et partage

- Il est utilisé pour vérifier ou créer des connexions réseau, configurer le partage réseau et modifier les paramètres de la carte réseau.
- L'affichage initial présente un aperçu du réseau actif.
- Dans cette fenêtre, vous pouvez afficher le groupe résidentiel auquel l'ordinateur appartient ou en créer un. Notez que HomeGroup a été supprimé de Windows 10 dans la version 1803.



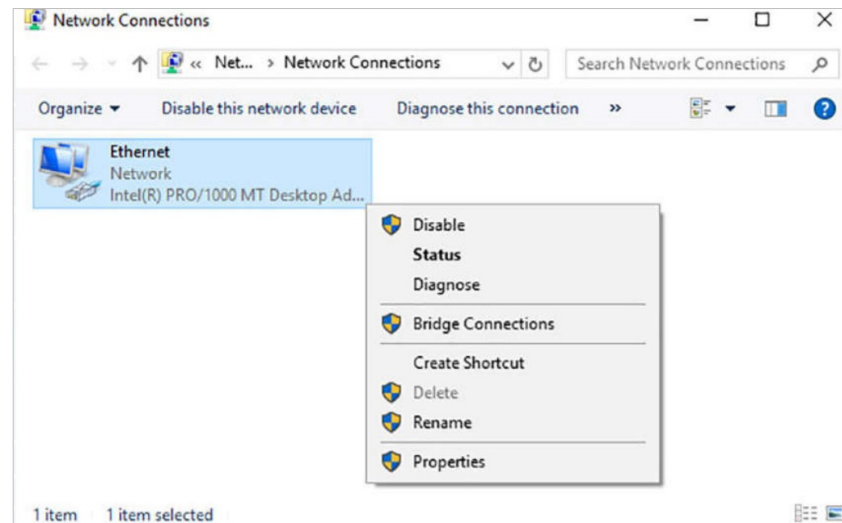
Mise en réseau (Suite)

Modifier les paramètres de la carte.

- Pour configurer une carte réseau, choisissez **Modifier les paramètres de la carte** dans le le Centre réseau et partage pour afficher toutes les connexions réseau disponibles Sélectionnez la carte à configurer.
- Voici les étapes pour modifier une carte Ethernet pour acquérir automatiquement son adresse IPv4 à partir du réseau :

Étape 1 : Propriétés de l'adaptateur d'accès

Cliquez avec le bouton droit de la souris sur la carte que vous souhaitez configurer, puis choisissez **Propriétés**, comme le montre la Figure 2.

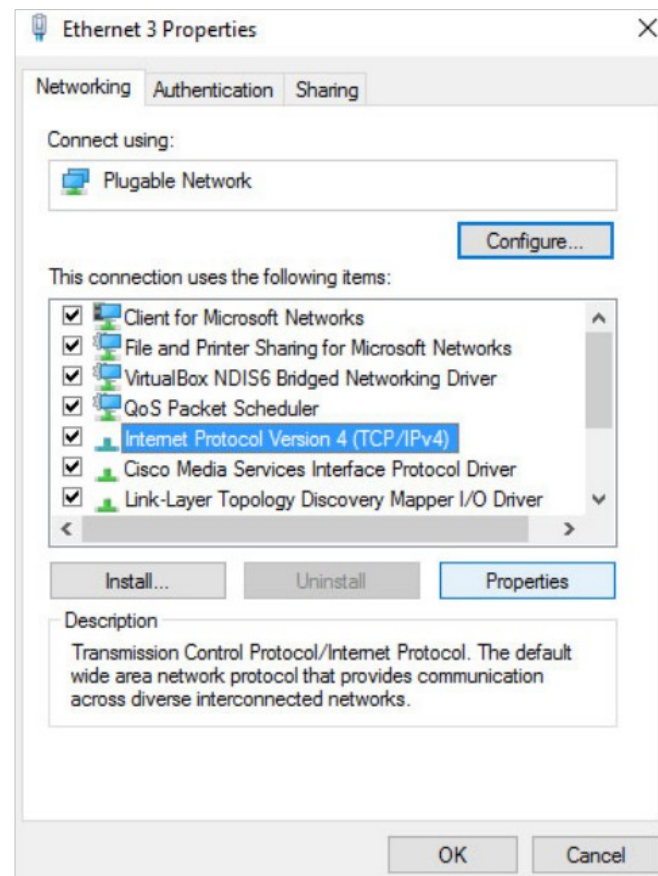


Configuration et surveillance de Windows

Mise en réseau (Suite)

Étape 2 : Accès aux propriétés TCP/IPv4

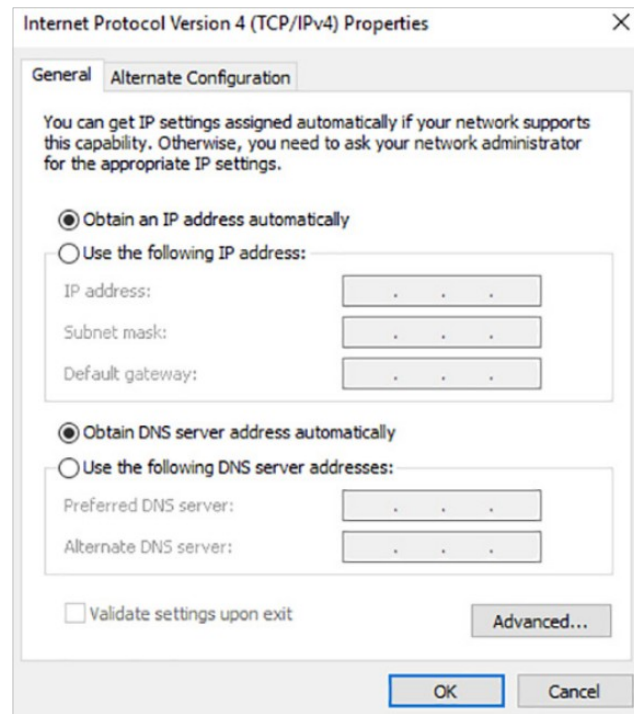
- Cette connexion utilise les éléments suivants: **Internet Protocol Version 4 (TCP/IPv4)** ou **Internet Protocol Version 6 (TCP/IPv6)** selon la version que vous souhaitez utiliser
- Dans la figure, IPv4 est en cours de sélection.



Mise en réseau (Suite)

Étape 3 : Modifier les paramètres

- Cliquez sur **Propriétés** pour configurer la carte.
- Dans la boîte de dialogue **Propriétés**, choisissez **d'obtenir une adresse automatiquement** si un serveur DHCP est disponible sur le réseau ou si l'utilisateur souhaite configurer l'adressage manuellement, renseignez l'adresse, le sous-réseau, la passerelle par défaut et les serveurs DNS.
- Cliquez sur **OK** pour valider les modifications.
- Vous pouvez également utiliser l'outil **netsh.exe** pour configurer les paramètres du réseau depuis une invite de commande.
- Ce programme peut afficher et modifier la configuration du réseau.
- Tapez **netsh /?** à l'invite de commande pour afficher une liste de toutes les options disponibles avec cette commande.



Mise en réseau (Suite)

nslookup et netstat

- Il est également conseillé de tester le système de noms de domaine (DNS), car il est très souvent utilisé pour rechercher l'adresse des hôtes en la traduisant d'un nom, comme un URL.
- Utilisez la commande **nslookup** pour tester le DNS.
- Tapez **nslookup cisco.com** à l'invite de commande pour trouver l'adresse du serveur web Cisco. Si l'adresse est renvoyée, le DNS fonctionne correctement.
- Tapez **netstat** à l'invite de commande pour afficher les détails des connexions réseau actives.

```
C:\Users\USER>netstat

Active Connections


```

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:3030	USER-VGFFA:58652	ESTABLISHED
TCP	127.0.0.1:3030	USER-VGFFA:62114	ESTABLISHED
TCP	127.0.0.1:3030	USER-VGFFA:62480	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62481	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62484	TIME_WAIT

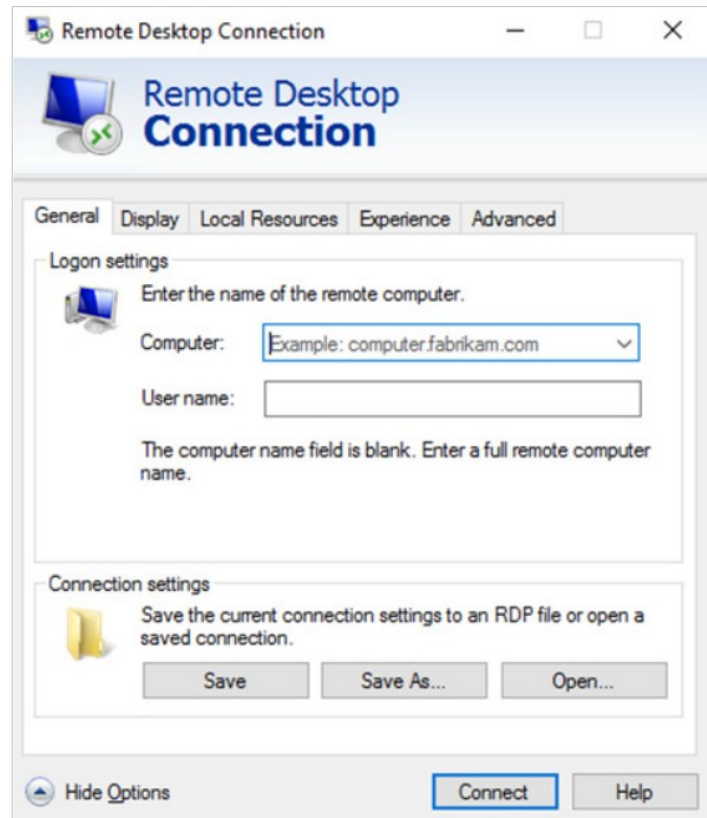
Configuration et surveillance de Windows

Accès aux ressources réseau

- Comme d'autres systèmes d'exploitation, Windows utilise la technologie de réseau pour de nombreuses applications, telles que le web, la messagerie électronique et les services de fichiers.
- Le protocole SMB (Server Message Block) est utilisé pour partager des ressources réseau. SMB est surtout utilisé pour accéder à des fichiers sur des hôtes distants.
- Le format UNC (Universal Naming Convention) vous permet de vous connecter aux ressources par exemple **\\servername\sharename\file**.
- Dans UNC, servername correspond au serveur qui héberge la ressource. sharename correspond à la racine du dossier dans le système de fichiers sur l'hôte distant, tandis que file correspond à la ressource que recherche l'hôte local.
- Lors du partage de ressources sur le réseau, la zone du système de fichiers partagée doit être identifiée. Le contrôle d'accès peut être appliqué aux dossiers et aux fichiers pour limiter les utilisateurs et les groupes à des fonctions spécifiques telles que la lecture, l'écriture ou le refus.
- Certains partages spéciaux sont automatiquement créés par Windows. Un partage administratif est identifié par le signe dollar (\$), situé après le nom du partage.

Accès aux ressources réseau (Suite)

- Outre l'accès aux partages sur des hôtes distants, vous pouvez vous connecter à un hôte distant et gérer cet ordinateur comme s'il s'agissait d'une machine locale en vue de modifier la configuration, d'installer un logiciel ou de résoudre un problème.
- Sous Windows, cette fonction est appelée protocole RDP (Remote Desktop Protocol). La figure de gauche illustre la fenêtre Connexion Bureau à distance.
- Étant donné que le protocole RDP (Remote Desktop Protocol) est conçu pour permettre aux utilisateurs distants de contrôler des hôtes individuels, il constitue une cible naturelle pour les acteurs de menace.



Windows Server

- La plupart des installations Windows sont effectuées sur des ordinateurs de bureau et des ordinateurs portables.
- Windows Server, une autre édition de Windows, est principalement utilisé dans les data centers. Cette famille de produits Microsoft commence à partir de Windows Server 2003.
- Windows Server, qui héberge de nombreux services, est utilisé à différentes fins dans une entreprise.
- Voici quelques-uns des services que Windows Server fournit:
 - **Services réseau:** DNS, DHCP, Terminal Services, contrôleur de réseau et virtualisation de réseau Hyper-V
 - **Services de fichiers:** SMB, NFS, et DFS
 - **Services web:** FTP, HTTP, et HTTPS
 - **Gestion:** Politique de groupe et contrôle des services de domaine Active Directory

***Remarque:** Bien qu'il existe Windows Server 2000, elle est considérée comme une version cliente de Windows NT 5.0. Basé sur NT 5.2, Windows Server 2003 est la première édition d'une nouvelle famille de versions de Windows Server.*

travaux pratiques – Création de comptes d'utilisateur

Au cours de ces travaux pratiques, vous allez créer et modifier des comptes d'utilisateur dans Windows.

Travaux pratiques – Utiliser Windows PowerShell

Dans ce laboratoire, vous allez explorer certaines des fonctions de PowerShell.

Travaux pratiques– Gestionnaire des tâches Windows

Dans ces travaux pratiques, vous allez explorer le Gestionnaire des tâches et y gérer les processus.

Travaux pratiques– Contrôler et gérer les ressources système sous Windows

Au cours de ces travaux pratiques, vous allez utiliser des outils d'administration pour contrôler et gérer les ressources système.

3.4 La sécurité Windows

La commande netstat

- La commande **netstat** permet de rechercher les connexions entrantes ou sortantes qui ne sont pas autorisées.
- La commande **netstat** affiche toutes les connexions TCP actives disponibles.
- L'examen de ces connexions permet de déterminer les programmes qui écoutent les connexions non autorisées.
- Vous pouvez dès lors arrêter le processus correspondant à l'aide du Gestionnaire des tâches, puis utiliser un logiciel de suppression de malwares pour nettoyer l'ordinateur.
- Pour faciliter cette tâche, vous pouvez lier les connexions aux processus en cours d'exécution dans le Gestionnaire des tâches.

La commande netstat (Suite)

- Pour ce faire, ouvrez une invite de commande avec des privilèges d'administrateur, puis utilisez la commande **netstat -abno**, comme le montre la figure.
- L'examen des connexions TCP actives doit permettre à un analyste de déterminer la présence de programmes suspects qui écoutent les connexions entrantes sur l'hôte.
- Plusieurs processus peuvent porter le même nom. Dans ce cas, utilisez le PID pour identifier le processus correct. Pour afficher le PID des processus dans le Gestionnaire des tâches, ouvrez le **Gestionnaire des tâches**, cliquez avec le bouton droit de la souris sur l'en-tête du tableau et sélectionnez **PID**.

```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32> netstat -abno

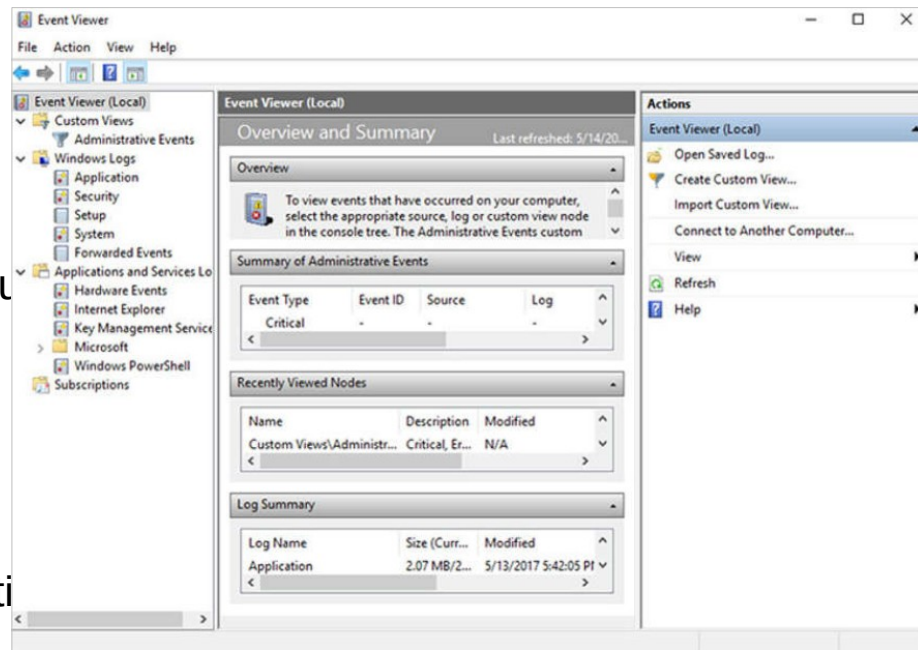
Active Connections

```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	952
RpcSs				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:623	0.0.0.0:0	LISTENING	14660
[LMS.exe]				
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1396
TermService				
[svchost.exe]				
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	9792
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:5593	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:8099	0.0.0.0:0	LISTENING	5248
[SolarWinds TFTP Server.exe]				
TCP	0.0.0.0:16992	0.0.0.0:0	LISTENING	14660

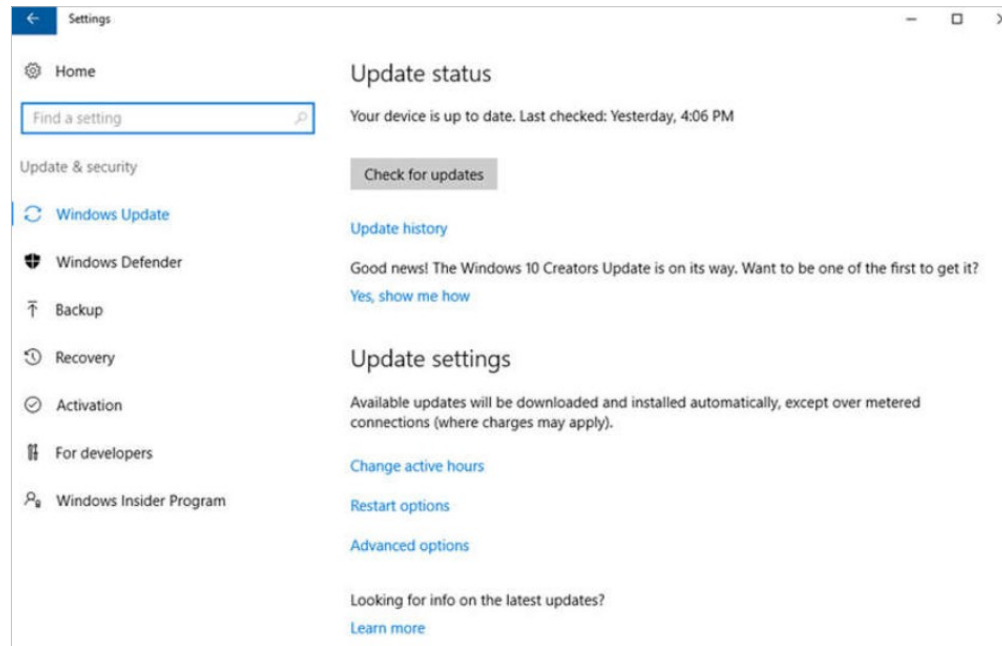
Observateur d'événements

- L'Observateur d'événements Windows contient un historique des événements concernant les applications, la sécurité et le système.
- Ces fichiers journaux constituent un outil de dépannage précieux, car ils fournissent les informations nécessaires à l'identification des problèmes.
- Windows comprend deux catégories de journaux d'événements : journaux de Windows, et journaux des applications et des services.
- Une vue personnalisée intégrée appelée Événements d'administration répertorie les événements des niveaux Critique, Erreur et Avertissement de tous les journaux administratifs.
- Les journaux des événements de sécurité se trouvent sous Journaux Windows. Ils utilisent des ID d'événement pour identifier le type d'événement.



Gestion de Windows Update

- Pour renforcer la protection contre ces attaques, assurez-vous d'avoir installé les derniers Service Packs et correctifs de sécurité Windows.
- La fenêtre État de mise à jour illustrée dans la figure vous permet de rechercher manuellement les mises à jour et de consulter l'historique des mises à jour de l'ordinateur.
- Les correctifs sont des mises à jour du code que les éditeurs fournissent afin d'empêcher un nouveau virus ou ver de contaminer un ordinateur.

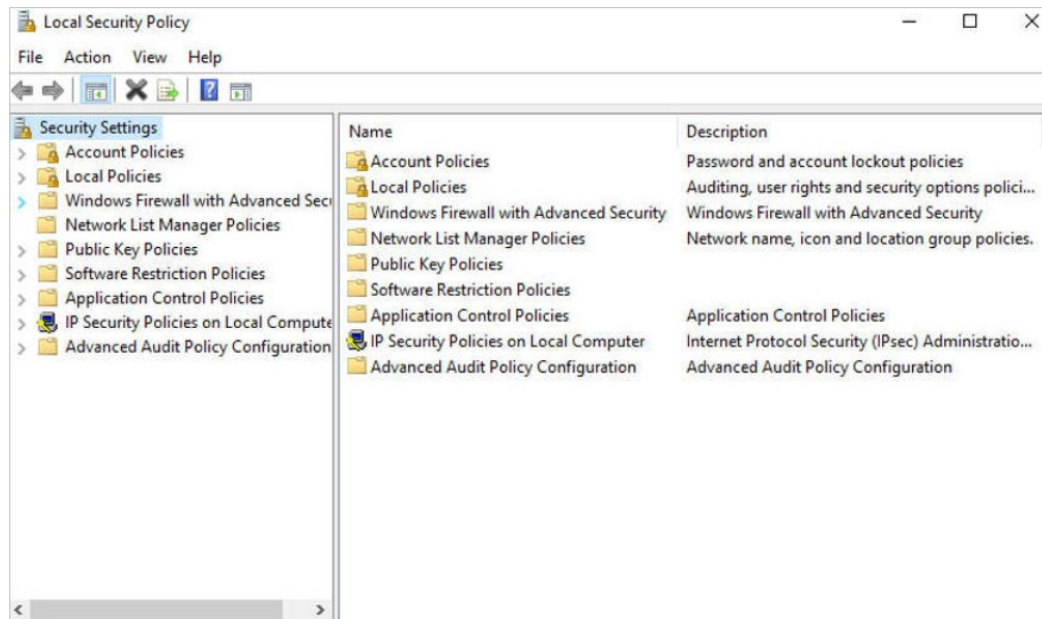


Gestion de Windows Update (Suite)

- De temps à autre, les correctifs et les mises à jour sont combinés dans une application de mise à jour complète appelée Service Pack.
- De nombreuses attaques de virus particulièrement dévastatrices auraient pu être beaucoup moins graves si davantage d'utilisateurs avaient téléchargé et installé le Service Pack le plus récent.
- Il est hautement souhaitable que les entreprises utilisent des systèmes qui distribuent, installent et suivent automatiquement les mises à jour de sécurité.
- Windows vérifie régulièrement si le site web de Windows Update contient des mises à jour cruciales qui peuvent contribuer à la protection d'un ordinateur contre les menaces les plus récentes.
- Vous pouvez également indiquer les heures auxquelles l'ordinateur ne doit pas redémarrer automatiquement, par exemple durant les heures de bureau.
- Des options sont aussi disponibles pour sélectionner le mode d'installation des mises à jour et obtenir des mises à jour pour d'autres produits Microsoft.

Politique de sécurité locale

- Une politique de sécurité est un ensemble d'objectifs qui assurent la sécurité d'un réseau, des données et des systèmes informatiques d'une entreprise.
- Sur la plupart des réseaux qui utilisent des ordinateurs Windows, un serveur Windows avec un domaine et Active Directory sont configurés. Les ordinateurs Windows se joignent au domaine.
- La stratégie de sécurité locale de Windows peut être appliquée aux ordinateurs autonomes qui ne font pas partie d'un domaine Active Directory.



Politique de sécurité locale (Suite)

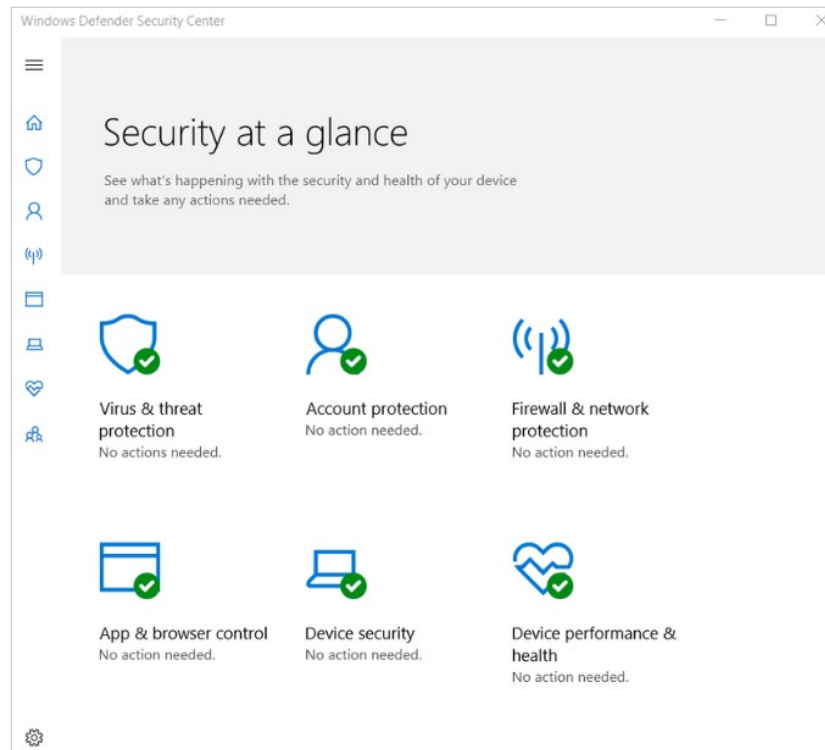
- Les directives relatives aux mots de passe sont une composante importante d'une stratégie de sécurité.
- Dans la politique de sécurité locale, l'option politique de mot de passe, située sous Stratégies de comptes, définit les critères des mots de passe pour tous les utilisateurs sur l'ordinateur local.
- Utilisez l'option Politique de verrouillage du compte du paramètre Stratégies de comptes pour éviter toute tentative de connexion forcée.
- Il est également important de s'assurer que les ordinateurs sont sécurisés même lorsque les utilisateurs ont quitté leur poste. Une stratégie de sécurité doit contenir une règle sur le verrouillage des ordinateurs en mode veille.
- Si la politique de sécurité locale est la même sur chaque ordinateur autonome, utilisez la fonction Exporter la stratégie. Cela peut être particulièrement utile si l'administrateur doit configurer des stratégies locales complexes pour les profils d'utilisateur et les options de sécurité.

Windows Defender

- Les programmes malveillants peuvent être des virus, des vers, des chevaux de Troie, des enregistreurs de frappe, des logiciels espions ou des logiciels publicitaires. Tous visent à porter atteinte à la vie privée, voler des informations, endommager l'ordinateur ou endommager les données.
- Il est important de protéger les ordinateurs et les terminaux mobiles à l'aide d'un logiciel antimalware renommé. Voici les types de logiciels existants :
 - **Protection antivirus** - Ce programme recherche continuellement la présence de virus.. Lorsqu'un virus est détecté, l'utilisateur reçoit une notification et le programme tente de mettre le virus en quarantaine ou de le supprimer.
 - **Protection contre les logiciels de publicité** - ce programme recherche continuellement les programmes qui affichent des publicités sur votre ordinateur.
 - **Protection contre l'hameçonnage**: Ce programme bloque les adresses IP des sites Web d'hameçonnage connus et signale les sites suspects à l'utilisateur.
 - **Protection contre les logiciels espions**: Ce programme recherche les enregistreurs de frappe et autres logiciels espions.
 - **Sources approuvées/non approuvées**: cet utilitaire identifie les programmes non sécurisés avant leur installation ou les sites Internet non sécurisés avant toute consultation.

Windows Defender (suite)

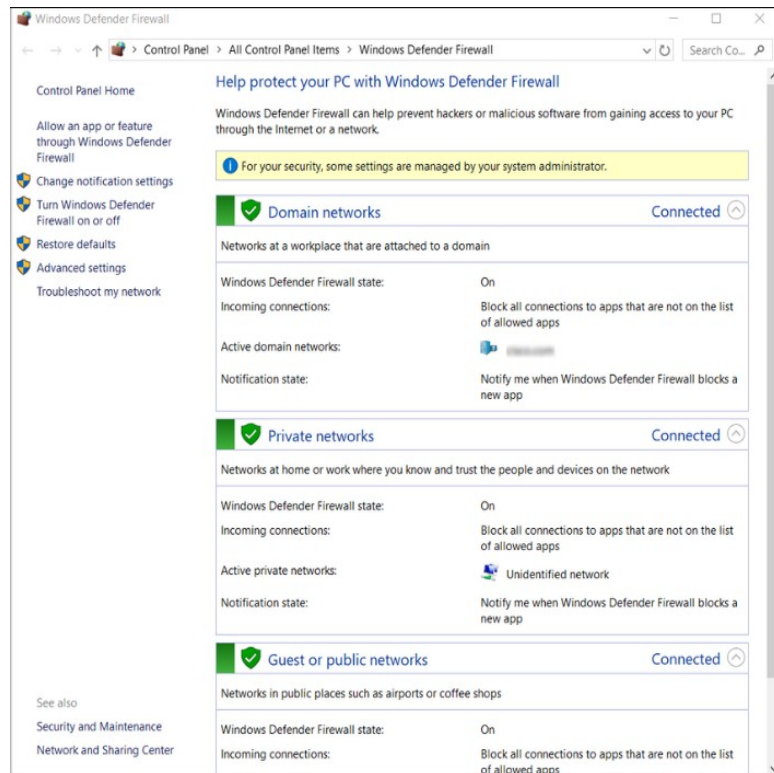
- Plusieurs programmes et analyses différents peuvent être nécessaires pour les supprimer complètement. Toutefois, n'exécutez qu'un seul utilitaire de protection à la fois.
- Diverses sociétés de sécurité réputées telles que McAfee, Symantec et Kaspersky offrent des solutions de protection contre les malwares pour les ordinateurs et les terminaux mobiles.
- Windows intègre un système de protection contre les virus et les logiciels espions appelé Windows Defender.
- Windows Defender est activé par défaut pour fournir une protection en temps réel contre toute infection.
- Bien que Windows Defender fonctionne en arrière-plan, vous pouvez effectuer des analyses manuelles de l'ordinateur et des appareils de stockage.



Sécurité de Windows

Pare-feu Windows

- Un pare-feu interdit le trafic vers un ordinateur ou un segment de réseau.
- Pour autoriser l'accès au programme via le pare-feu Windows Defender, recherchez **Panneaux de configuration**. Sous **Systèmes et sécurité**, recherchez le **pare-feu Windows Defender**. Cliquez sur **Autoriser une application ou une fonctionnalité via le Pare-feu Windows**.
- Pour désactiver le Pare-feu Windows, cliquez sur **Activer ou désactiver le Pare-feu Windows**.
- De nombreux autres paramètres sont disponibles sous **Paramètres avancés**. Ici, des règles de trafic entrant ou sortant peuvent être créées et différents aspects du pare-feu peuvent être surveillés.



3.5 Récapitulation : le système d'exploitation Windows

Qu'est-ce que j'ai appris dans ce module?

- Les premiers ordinateurs nécessitaient un système d'exploitation de disque (DOS) pour créer et gérer des fichiers.
- Microsoft a développé MS-DOS comme interface de ligne de commande (CLI) pour accéder au lecteur de disque et charger les fichiers du système d'exploitation. Les premières versions de Windows se composaient d'une interface utilisateur graphique (GUI) exécutée sur MS-DOS.
- Windows comporte une couche d'abstraction du matériel est un code qui gère l'ensemble des communications entre le matériel et le noyau.
- Windows fonctionne en deux modes différents, le mode utilisateur et le mode noyau. La plupart des programmes dans Windows s'exécutent en mode utilisateur. Le mode noyau permet au code du système d'exploitation d'accéder directement au matériel informatique.
- Pour fonctionner, un ordinateur stocke des instructions dans la mémoire RAM en vue de leur traitement par le processeur.
- Chaque processus d'un ordinateur Windows 32 bits prend en charge un espace d'adressage virtuel jusqu'à quatre gigaoctets. Chaque processus d'un ordinateur Windows 64 bits prend en charge un espace d'adressage virtuel jusqu'à huit téraoctets.

Qu'est ce que j'ai appris dans ce Module? (suite)

- Windows stocke toutes les informations relatives aux paramètres du matériel, des applications, des utilisateurs et du système dans une grande base de données appelée le Registre.
- Le registre est une base de données hiérarchique dont le niveau le plus élevé est appelé « ruche », et dont les niveaux inférieurs sont appelés clés ou sous-clés, respectivement.
- Il existe cinq ruches de Registre qui contiennent des données concernant la configuration et le fonctionnement de Windows. Il y a des centaines de clés et de sous-clés.
- Pour des raisons de sécurité, il est déconseillé de se connecter à Windows avec le compte d'administrateur ou un compte disposant de privilèges d'administrateur.
- Pour faciliter l'administration des utilisateurs, Windows utilise des groupes. Les utilisateurs et les groupes locaux sont gérés à l'aide de l'applet `lusrmgr.msc` du panneau de configuration.
- Vous pouvez utiliser l'interface de ligne de commande ou Windows PowerShell pour exécuter des commandes. PowerShell, permet de créer des scripts d'automatisation des tâches que l'interface de ligne de commande standard ne peut pas créer.
- Windows Management Instrumentation (WMI) est utilisé pour gérer les ordinateurs distants.

Qu'est ce que j'ai appris dans ce Module? (suite)

- La commande **net** prend en charge plusieurs autres commandes qui suivent la commande et peut être combinée avec des options pour obtenir un résultat spécifique.
- Le gestionnaire des tâches fournit de nombreuses informations sur tout ce qui est en cours d'exécution et sur les performances générales de l'ordinateur. Le moniteur de ressources fournit des informations plus détaillées sur l'utilisation des ressources.
- Le protocole SMB (Server Message Block) est utilisé pour partager des ressources réseau.
- La commande **Netstat** de Windows affiche tous les ports de communication ouverts sur un ordinateur et peut également afficher les processus logiciels associés aux ports.
- L'observateur d'événements Windows permet d'accéder à de nombreux événements consignés concernant le fonctionnement d'un ordinateur.
- Il est très important de garder Windows à jour pour se prémunir contre les nouvelles menaces de sécurité.
- Windows doit être configuré pour télécharger et installer automatiquement les mises à jour à mesure qu'elles deviennent disponibles.

