**TS services informatiques aux organisations**

*SI 1*

**Étape 07**

**Module :**

**Système d'exploitation**

**Séquence 01 :**

**Windows Server**

Gilles BOHL

Lycée Pasteur Mont Roland, Enseignement supérieur l 40, rue du Gouvernement l 39100 DOLE

SOMMAIRE

1. ) Présentation de Windows 2

1.1. ) Le noyau NT 2

1.2. ) La sécurité 2

1.3. ) Notion de session 2

1.4. ) Sécurité du poste de travail 2

1.5. ) Appel Gestionnaire des tâches 3

2. ) Gestion des utilisateurs 3

2.1. ) Notion d'utilisateur 3

2.2. ) Gérer les utilisateurs 3

2.3. ) Convention de nommage 4

2.4. ) Types de comptes 4

2.5. ) Sécurité 4

2.6. ) Emplacement des comptes 5

2.6.1. ) Les comptes d’utilisateur de domaine 5

2.6.2. ) Les comptes d’utilisateur local : 5

2.7. ) Dossiers personnels 5

2.8. ) Proﬁl 5

3. ) Gestion des groupes 6

3.1. ) Notion de groupe 6

3.2. ) Groupes prédéﬁnis 6

3.3. ) Gérer les groupes 6

4. ) Les stratégies de sécurité 6

4.1. ) Notion de stratégie 6

4.2. ) Gérer les stratégies 6

5. ) Partages et permissions 7

5.1. ) Notion de partage 7

5.2. ) Notion de permissions 7

5.3. ) Les permissions de dossier partagé 7

5.4. ) Les permissions aux utilisateurs et aux groupes 8

6. ) Commandes Windows 8

6.1. ) ipconfig 8

6.1. ) ping 8

6.2. ) Tracert 9

6.1. ) netstat 9

6.1. ) SFC /scannow 10

6.1. ) wbAdmin start backup 10

Objectifs :

1. Connaitre le fonctionnement d'un système d'exploitation serveur.

|  |
| --- |
| 1. Comprendre la notion de sécurité |
| 1. Comprendre l'intérêt de créer des utilisateurs |
| 1. Comprendre l'intérêt de créer des groupes |
| 1. Comprendre la notion de partages et de permissions |

02 Windows server.docx

Le Système d'exploitation Windows Server

# ) Présentation de Windows

## ) Le noyau NT

NT pour «New Technology.

Depuis Windows 2000 Microsoft se base sur le noyau de Windows NT et possèdent les caractéristiques suivantes :

è

è

è

è

## ) La sécurité

Elle se met en place grâce à 2 éléments :

è L'administrateur

è

è Le système de fichiers NTFS

è Pour la sécurité des fichiers

## ) Notion de session

Pour accéder à un système fonctionnant sous Windows, *il faut ouvrir une session*.

La session peut être ouverte pour

è Gère les droits de chaque utilisateur

è Et le système de fichier NTFS permet de définir les droit d’accès aux fichiers

Besoin pour cet accès :

è

è

**è**

è

è.

è

è

Appel d'ouverture de session

è

## ) Sécurité du poste de travail

Lorsqu’un utilisateur a ouvert une session, la séquence de touche CTRL+ALT+SUPPR ouvre une autre boîte de dialogue appelée Sécurité de Windows.

Voici les différentes options proposées :

**Verrouiller la station de travail è** Assure la sécurité de l’ordinateur sans fermeture de la session.

**Changer de mot de passe è** Permet à l’utilisateur de changer de mot de passe.

**Fermer la session è** Ferme la session actuelle mais les services continuent d’être actifs.

**Gestionnaire des tâches è** Indique quelles applications sont en cours d’exécution.

**Arrêter le système è** Ferme tous les fichiers, sauvegarde toutes les données système et prépare l’ordinateur à être éteint en toute sécurité.

**Annuler è** Referme la boîte de dialogue.

## ) Appel Gestionnaire des tâches

**è**

è

è

# ) Gestion des utilisateurs

## ) Notion d'utilisateur

Par défaut, lors de l'installation de Windows Server, 2 comptes utilisateur, sont créés :

è

**è**

Il est possible et même conseillé, de modifier è

Il est possible d'en ajouter avec è

Un compte d’utilisateur è

Cela lui permet d'ouvrir une session sur :

è

è

***Chaque utilisateur utilisant l’ordinateur de façon régulière doit ainsi avoir son propre compte.***

## ) Gérer les utilisateurs

è Le **gestionnaire** **d'utilisateur** (utilitaire fourni en standard avec Windows).

è Dans les Outils d’administration via la console Gestion de l’ordinateur.

è Panneau de configuration puis Comptes d'utilisateurs sur un SE non-réseau.

Pour créer un nouveau compte, il suffit de saisir des informations sur le nouvel utilisateur :

**è**

**è**

**è**

**è**

## ) Convention de nommage

La convention de nommage des utilisateurs è

Il faut tenir compte des éléments suivants pour les utilisateurs :

è

è Les noms peuvent contenir tout caractère **majuscule** ou **minuscule** à l’exception des caractères suivants :

**/ \ [ ] : . | = , + \* ? < >.**

è

## ) Types de comptes

Il existe deux types de comptes sous Windows.

è Les comptes prédéfinis ou par défaut

è

è

è Les comptes que vous créez.

è

## ) Sécurité

Pour des raisons de sécurité, après installation de Windows, il est essentiel :

è

è

Il est possible de paramétrer les postes à partir desquels un utilisateur peut se connecter au réseau.

On peut l'autoriser soit à ouvrir une session à partir :

è

è

è

Il est également possible de fixer une date d’expiration du compte d’un utilisateur.

è

è

## ) Emplacement des comptes

### ) Les comptes d’utilisateur de domaine

Enregistrés sur è

Utilité è

Dès la création, l’utilisateur peut ouvrir une session sur le domaine à partir de n’importe quel poste du réseau en fonction de ses autorisations.

### ) Les comptes d’utilisateur local :

Enregistrés sur è

Le compte n’est créé que sur l’ordinateur local.

L’utilisateur ne peut donc ouvrir de session que sur l’ordinateur en question.

## ) Dossiers personnels

Le dossier de base est le dossier è

Il est utilisé comme dossier par défaut lors de l’exécution de commandes telles qu’Enregistrer***.***

Il peut être stocké sur :

è

è

Pour savoir où les créer, il faut prendre en compte les points suivants :

Sauvegarde et restauration è

Espace sur les contrôleurs de domaine è

Ordinateur sans disque dur è

Avantage du stockage en local è

## ) Proﬁl

Ouverture d'une session pour la première fois

è un profil d’utilisateur par d’défaut et crée

**Script d’ouverture de session** è configure les protection réseaux

èconfigure les imprimente

è défini l’environnement de travail

***Il s’agit en fait d’un fichier de commande (.bat) ou d’un fichier exécutable (.exe)***

***qui s’exécute automatiquement lorsque l’utilisateur ouvre une session.***

**Utilisation de profils errants ou itinérants**

**è** offert le même environnement de travail quel que soit la station ou l’on se connecte

è Ils ont enregistré sur le serveur

# ) Gestion des groupes

## ) Notion de groupe

Définition è prenait de définir les ensembles d’utilisateur avec les mêmes permissions

Représentation è c’est un ensemble de compte utilisateur

Intérêt è un utilisateur a toutes les permissions du groupe

Utilité è cela simplifie l’administration

## ) Groupes prédéﬁnis

Lors de l’installation de Windows, des groupes par défaut sont créés sans qu'on puisse les supprimer.

Liste des groupes :

* Administrateurs.
* Opérateurs de sauvegarde.
* Opérateurs de configuration réseau.
* Duplicateurs.
* Utilisateurs du bureau à distance.
* Utilisateurs avec pouvoir.
* Utilisateurs.
* Invités.

Le groupe **Tout le monde** est également créé, mais n’apparaît pas dans la liste des groupes du gestionnaire de groupe.

Il contient systématiquement tous les comptes utilisateurs présents sur le système, ***y-compris celui de l’administrateur*.**

## ) Gérer les groupes

Il est possible d'ajouter des groupes d'utilisateurs personnalisés, avec des permissions particulières selon les opérations qu'ils sont amenés à faire sur le système.

Utilitaire permettant de gérer les groupes è c’est le gestionnaire de groupe

**Où è** Les Outils d’administration via la console Gestion de l’ordinateur.

Pour créer un nouveau groupe è Cliquer sur **Nouveau groupe** dans le menu Action.

Le bouton Ajouter è permet d’ajouter des différant utilisateur aux groupe

# ) Les stratégies de sécurité

## ) Notion de stratégie

***La stratégie de sécurité (security policy) correspond à l'ensemble des règles de sécurité***

***que l'on désire mettre en place dans une organisation,***

***ainsi que le niveau de celles-ci.***

## ) Gérer les stratégies

Utilitaire è le gestionnaire de stratégie local

Ou è outil d’administration

Celui-ci contient un menu contenant plusieurs éléments, parmi lesquels :

1. ***Stratégies de compte : options relatives à la connexion des utilisateurs (mots de passe et verrouillage des comptes).***

* Conserver l’historique des mots de passe

Intérêt è pas 2 fois le même mdp

* Durée de vie maximale du mot de passe

Intérêt è obliger de modifier le mot de passe

* Durée de vie minimale du mot de passe

Intérêt è obligation de conserve sont mdp

* Exigences de complexité

Intérêt è oblige à alterner entre les majuscules les chiffre et les caractères spéciaux

* Longueur minimale du mot de passe

Intérêt è éviter le piratage trop rapide

* Seuil de verrouillage du compte

Intérêt è bloque le compte après trop de tentative

* Durée de verrouillage des comptes

Intérêt è

1. ***Stratégies des droits utilisateurs*** définissant les permissions accordées à chaque d'utilisateur.
2. ***Stratégie d'audits*** permettant de définir les événements à enregistrer dans un fichier journal visualisable par l'observateur d'événements.
3. ***Options de sécurité*** permettant de définir plusieurs paramètres relatifs à la sécurité du système.

# ) Partages et permissions

## ) Notion de partage

Le partage permet de désigner les ***ressources*** auxquelles les utilisateurs doivent pouvoir accéder par le biais du réseau.

Lorsqu’un dossier est partagé, les utilisateurs peuvent se connecter au dossier à travers le réseau et avoir accès aux fichiers qu’il contient comme si celui-ci se trouvait en local

## ) Notion de permissions

Afin d’accroître la sécurité du réseau, il est possible d’attribuer des permissions à ces ressources pour contrôler les actions des utilisateurs sur ces ressources.

Une fois qu’un dossier est partagé, les utilisateurs qui en ont la permission, ont accès à tous les fichiers et dossiers contenus dans le dossier partagé.

## ) Les permissions de dossier partagé

Elles permettent de contrôler l’utilisation des ressources par un utilisateur ou un groupe donné.

Il existe quatre permissions différentes sur les dossiers ou les fichiers:

* **Contrôle total** è Permission par défaut

è Lire crée modifier supprimer

è Modifier les permission

* **Modifier è**  lire crée modifier supprimer

è pas de modification de permission

* **Lire è**  lire les fichiers et parcourir les dossiers

è pas de création ni modification ni suppressions

* **Aucun accès** è Interdis l’accès aux dossiers

Les permissions affectées à un utilisateur ***ne prennent effet qu’à sa prochaine connexion***.

***Il faut faire très attention au fait que par défaut,***

***la permission "Contrôle total" soit affectée au groupe "Tout le monde".***

Il faut donc modifier, dès le début, ce groupe et cette permission associée.

De même, il faut éviter de mettre une permission "Aucun accès" au groupe "Tout le monde" car l’Administrateur fait partie de ce groupe.

## ) Les permissions aux utilisateurs et aux groupes

Un utilisateur peut se voir attribuer des permissions soit *directement*, soit en tant que *membre d’un groupe*.

Cas où un utilisateur fait partie de plusieurs groupes ayant des permissions différentes sur un même dossier partagé.

Voici comment sont gérées ces permissions :

* **Les permissions effectives** sont une combinaison des différentes permissions attribuées aux différents groupes.  
  Un utilisateur d’un groupe, ayant la permission "Lire" sur un dossier et faisant également partie d’un groupe ayant la permission "Contrôle total" à ce même dossier se verra attribuer la permission

è aucun accès

* **La seule exception à cette règle** est la permission "***Aucun accès***" qui est totalement restrictive.  
  Si un utilisateur fait partie d’un groupe ayant une permission "Contrôle total" sur un dossier et qu’il fait également partie d’un groupe ayant une permission "Aucun accès" sur ce même dossier, la permission attribuée sera

è

*Cours sous licence Creative Commons issu de commentcamarche.net*

# ) Commandes Windows

Ces commandes sont à exécuter dans la console cmd (invite de commande dos) ou en powershell.

## ) ipconfig

Donne è ip machine

è passerelle

Paramètres complémentaires

**ipconfig /all**

Donne encore plus d’informations è

NetBIOS èpermet dassocier un nom d'utilisateur a une addresse ip

**ipconfig /release et ipconfig /renew**

è relancer une requet DHCP

**ipconfig / flushdns**

è reboot le client du cache dns

## ) ping

è

**Ping google.com**

C:\Users\Gilles>**ping google.com**

Envoi d'une requête 'ping' sur google.com [173.194.40.164] avec 32 octets de données :

Réponse de 173.194.40.164 : octets=32 temps=34 ms TTL=52

Réponse de 173.194.40.164 : octets=32 temps=34 ms TTL=52

Réponse de 173.194.40.164 : octets=32 temps=34 ms TTL=52

Réponse de 173.194.40.164 : octets=32 temps=35 ms TTL=52

Statistiques Ping pour 173.194.40.164:

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

Durée approximative des boucles en millisecondes :

Minimum = 34ms, Maximum = 35ms, Moyenne = 34ms

TTL è nombre maximal de routeur de transite

è fixe par le système d’exploitation qui récit le ping

è 128 win

è 64 linux

è 54 – 62 12 routeurs

**Ping google.com**

Problème è procède de nombre serveur

è

**Ping 192.168.1.1**

C:\Users\Gilles>**ping 192.168.1.1**

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :

Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64

Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64

Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64

Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.1:

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

Durée approximative des boucles en millisecondes :

Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

è

**Ping google.fr**

C:\Users\Gilles>ping google.fr

Envoi d'une requête 'ping' sur google.fr [173.194.34.23] avec 32 octets de données :

Réponse de 173.194.34.23 : octets=32 temps=35 ms TTL=52

Réponse de 173.194.34.23 : octets=32 temps=33 ms TTL=52

Réponse de 173.194.34.23 : octets=32 temps=34 ms TTL=52

Réponse de 173.194.34.23 : octets=32 temps=34 ms TTL=52

Statistiques Ping pour 173.194.34.23:

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

Durée approximative des boucles en millisecondes :

Minimum = 33ms, Maximum = 35ms, Moyenne = 34ms

**Ping 192.168.0.254**

C:\Users\Gilles>ping **192.168.0.254**

Envoi d'une requête 'Ping' 192.168.0.254 avec 32 octets de données :

Réponse de 192.168.0.254 : octets=32 temps<1ms TTL=63

Réponse de 192.168.0.254 : octets=32 temps<1ms TTL=63

Réponse de 192.168.0.254 : octets=32 temps<1ms TTL=63

Réponse de 192.168.0.254 : octets=32 temps<1ms TTL=63

Statistiques Ping pour 192.168.0.254:

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

Durée approximative des boucles en millisecondes :

Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

è

## ) Tracert

è résoudre les problèmes de connexion réseau

è retrace l’itinéraires d’un packts avant d’arriver à destination

è permet de comprend ou bloque la connexion réseaux

**tracert google.com**

C:\Users\Gilles>tracert google.com

Détermination de l'itinéraire vers google.com [173.194.67.101]

avec un maximum de 30 sauts :

1 <1 ms <1 ms <1 ms READYSHARE [192.168.1.1]

2 <1 ms <1 ms <1 ms FREEBOX [192.168.0.254]

3 23 ms 23 ms 22 ms 88.186.224.254

4 23 ms 23 ms 23 ms dijon-6k-1-a5.routers.proxad.net [213.228.13.190]

5 32 ms 30 ms 31 ms strasbourg-6k-1-v802.intf.routers.proxad.net [212.27.50.133]

6 29 ms 30 ms \* strasbourg-crs8-1-be1001.intf.routers.proxad.net [78.254.250.217]

7 36 ms 37 ms 35 ms th2-crs16-1-be1101.intf.routers.proxad.net [212.27.50.9]

8 35 ms 35 ms 34 ms p11-crs16-1-be1001.intf.routers.proxad.net [78.254.249.5]

9 35 ms 34 ms 34 ms p11-9k-1-be1000.intf.routers.proxad.net [78.254.249.130]

10 34 ms 34 ms 40 ms cbv-9k-1-be1009.intf.routers.proxad.net [78.254.249.157]

11 35 ms 34 ms 34 ms 74.125.50.116

12 34 ms 46 ms 35 ms 72.14.238.234

13 36 ms 34 ms 35 ms 209.85.245.83

14 40 ms 39 ms 46 ms 209.85.246.167

15 48 ms 47 ms 47 ms 209.85.250.161

16 \* \* \* Délai d'attente de la demande dépassé.

17 41 ms 41 ms 40 ms wi-in-f101.1e100.net [173.194.67.101]

Itinéraire déterminé.

## ) netstat

è affiche les statistiques de connexion réseau TCP/IP

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]

-a è Affiche toutes les connexions et tous les ports d'écoute.

-b è Affiche l'exécutable impliqué dans la création de chaque connexion ou port d'écoute. Dans certains cas, des exécutables reconnus hébergent plusieurs composants indépendants, et la séquence des composants impliqués dans la création de la connexion ou du port d'écoute s'affiche alors. Dans ce cas, le nom de l'exécutable se trouve dans [] en bas, au-dessus du composant qu'il a appelé, et ainsi de suite jusqu'à ce que TCP/IP soit atteint. Notez que cette option peut être très longue et échouera si vous n'avez pas d'autorisations suffisantes.

-e è Affiche des statistiques Ethernet. Cette option peut être combinée avec l'option -s.

-f è Affiche les noms de domaine complets (FQDN) pour des adresses étrangères.

-n è Affiche des adresses et numéros de ports en format numérique.

-o è Affiche l'identificateur du processus propriétaire associé à chaque connexion.

-p proto è Affiche les connexions pour le protocole spécifié par proto ;

proto peut être une des valeurs suivantes : TCP, UDP, TCPv6 ou UDPv6. S'il est utilisé avec l'option -s pour afficher les statistiques par protocole, le protocole peut être une des valeurs suivantes : IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ou UDPv6.

-r è Affiche la table de routage.

-s è Affiche les statistiques par protocole. Par défaut, les statistiques sont affichées pour IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP et UDPv6 ; l'option -p peut être utilisée pour spécifier un sous-jeu de la valeur par défaut.

-t è Affiche l'état de déchargement de connexion actuel.

Interval è Affiche régulièrement les statistiques sélectionnées, en faisant une pause pendant le nombre de secondes spécifié par l'intervalle entre chaque affichage. Appuyez sur CTRL+C pour arrêter l'affichage des statistiques. Si l'intervalle est omis, netstat n'affichera les informations de configuration actuelle qu'une seule fois.

**netstat-an** è connextion ouvert sur le pc

è port utiliser

-addres IP extrenne sur le quel le pc et connecter

Intérêt è

## ) SFC /scannow

utilisation è scan les fichier pour vérifier leurs intégrité

SFC è system fils chek

Obligation èadm

Microsoft Windows [version 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>sfc /scannow

Début de l'analyse du système. Cette opération peut nécessiter un certain temps.

Démarrage de la phase de vérification de l'analyse du système.

La vérification 100% est terminée.

La protection des ressources Windows a trouvé des fichiers endommagés, mais n'a pas réussi à tous les réparer.

Des détails sont inclus dans le journal CBS.Log windir\Logs\CBS\CBS.log.

Par exemple C:\Windows\Logs\CBS\CBS.log

Pour ouvrir un fichier .log, il faut NotePad++ et le démarrer en mode administrateur (c'est un fichier de plusieurs milliers de lignes!).

## ) wbAdmin start backup

Définition è

Obligation è

Sauvegarder le système de C: sur le disque D:

La sauvegarde a été faite dans le dossier WindowsImageBackup sur D:\

Pourquoi la remarque ?:

L'emplacement de stockage des sauvegardes sélectionné est sur le même disque dur physique que votre système d'exploitation. En cas de défaillance du disque dur, vous pouvez perdre vos données système et vos données de sauvegarde.

è