Windows et Active Directory

Installation du système

Démarrage du système

Configuration du système

Comptes locaux

SR v2019

Windows et Active Directory

Installation

SR v2019

INSTALLATION DE WINDOWS

Prérequis

- Configuration système minimum requise pour l'installation
  - Processeur : 1.4 GHz 64Bits
  - Mémoire vive : 512 Mo
  - Espace disque requis : 32 Go

- Quelques règles de base
  - Mot de passe pour accéder au Setup du BIOS
  - Pas de démarrage autre que sur le disque hébergeant l'OS
  - Serveur physiquement protégé

INSTALLATION DE WINDOWS

Installation et paramétrage de base

- Installation très simple où les seuls choix sont
  - Langue du système, format horaire et clavier
  - Édition Standard ou Datacenter complète ou Core
  - Upgrade ou nouvelle installation
  - Disque et partition d'installation
  - Mot de passe du compte Builtin\Administrateur

- Le paramétrage de base consiste à
  - Fournir un nom de machine spécifique
  - Intégrer la machine à un domaine ou un groupe de travail
  - Autoriser l'accès via le bureau à distance (ou pas)
  - Désactiver IPv6 si non utilisé
  - Paramétrer IPv4
  - Paramétrer les mises à jour
  - Activer le produit

Windows et Active Directory

Démarrage du système

SR v2019

DÉMARRAGE DE WINDOWS

Processus

- Mise sous tension
- Chargement du BIOS
- Séquence POST
- Chargement du MBR
- Chargement du secteur de boot de la partition active
- Chargement du fichier de démarrage BOOTMGR
  - Situé à la racine de la partition active
- Chargement du BCD
  - Si plusieurs entrées, affichage du menu de démarrage

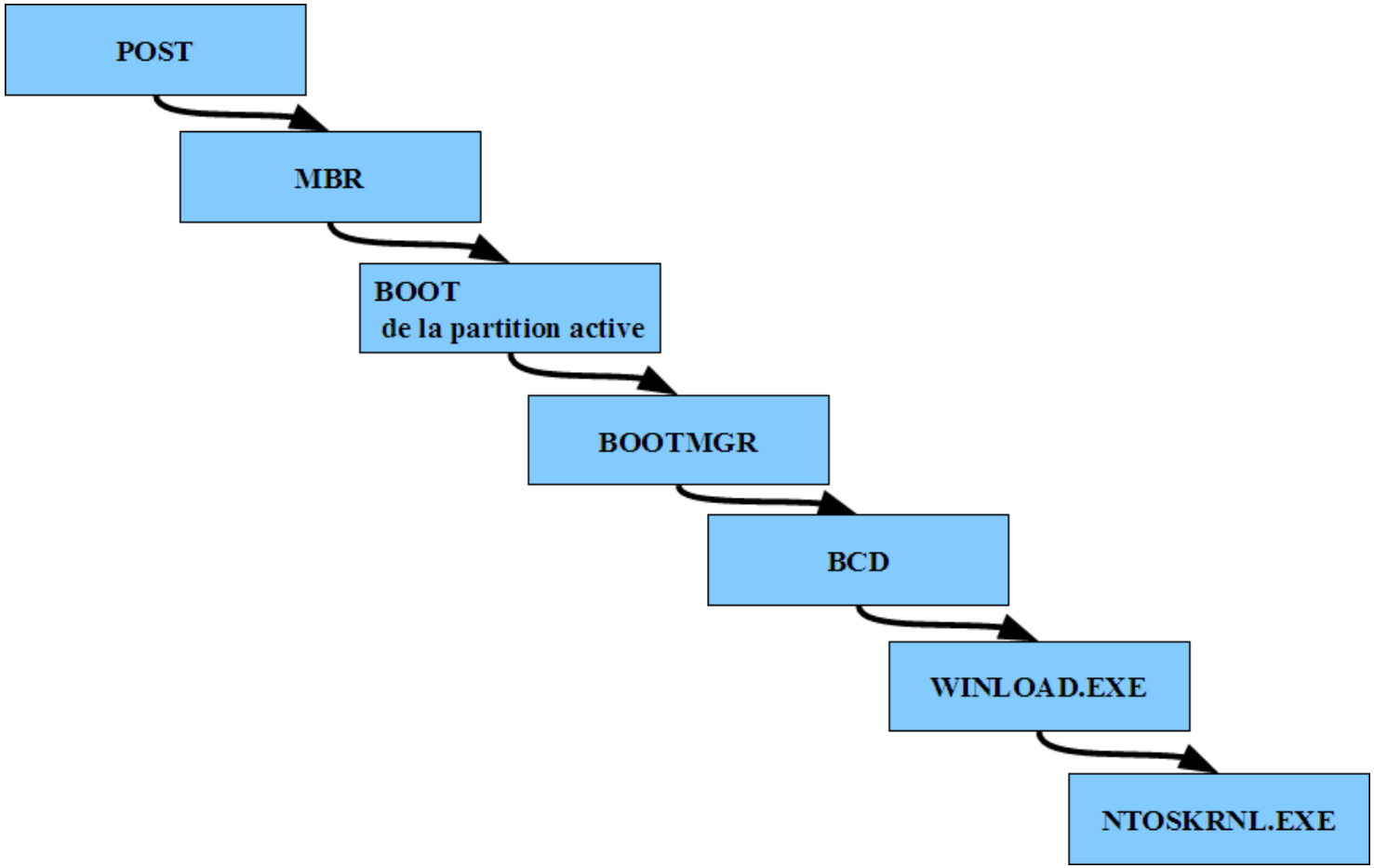
DÉMARRAGE DE WINDOWS

Processus

- Lancement du chargeur WINLOAD.EXE
  - WINLOAD remplacé par WINRESUME si sortie de mise en veille
  - Charge en mémoire le noyau (NTOSKRNL.EXE) puis la HAL (HAL.DLL)
  - Charge en mémoire la ruche du registre (SYSTEM32\CONFIG\SYSTEM) puis les services et pilotes
  - Activation du fichier d'échange puis transmission du contrôle au noyau
- Lancement du noyau NTOSKRNL.EXE
  - Le noyau et la HAL initialise HKLM\SYSTEM\CURRENTCONTROLSET
- Ouverture de session
  - Winlogon.exe démarre
  - Démarrage du processus LSA (Local Security Authority, Lsass.exe)
  - Validation de l'authentification de l'utilisateur (Kerberos v5 ou NTLM)

DÉMARRAGE DE WINDOWS

Processus



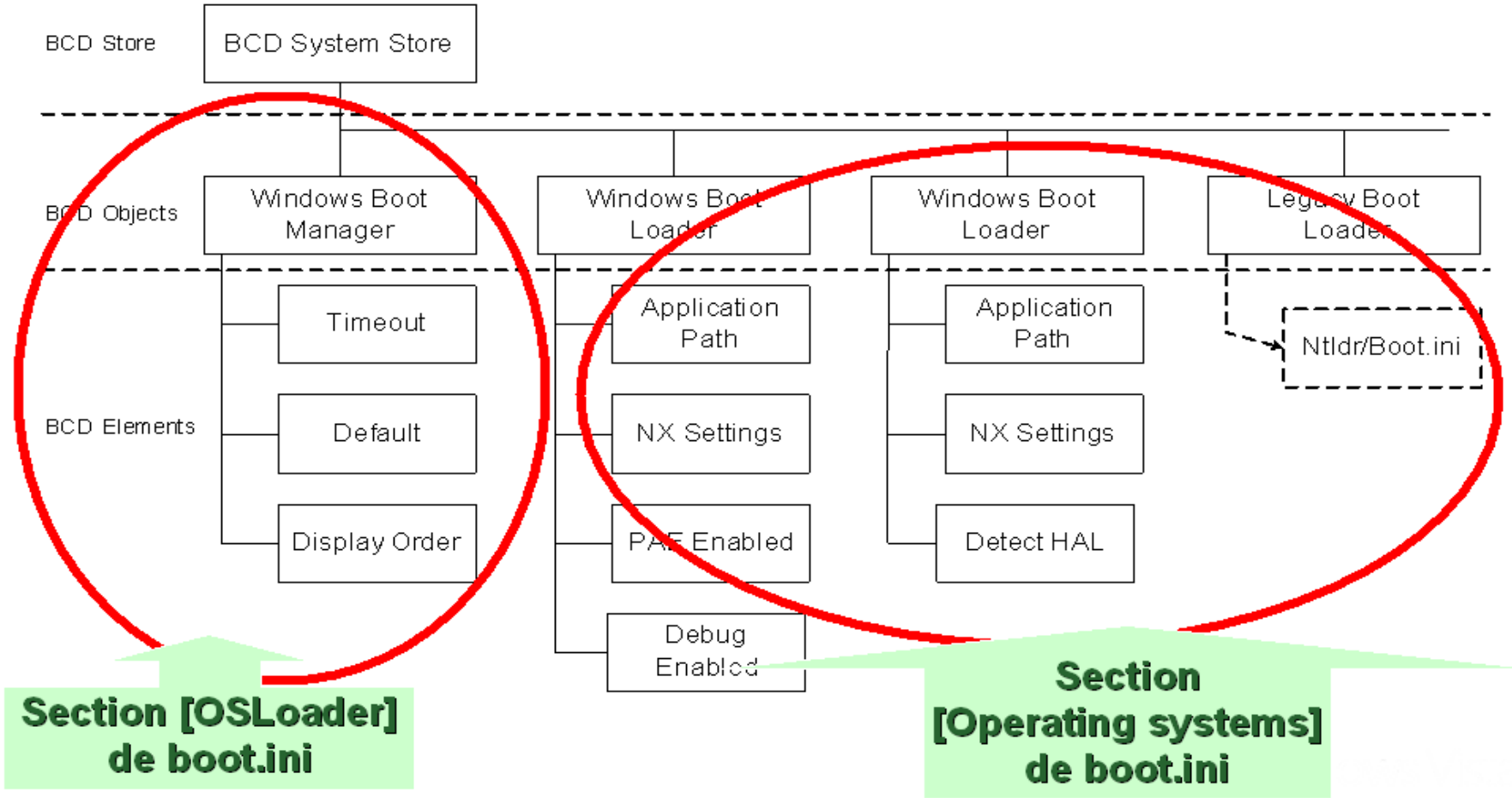
DÉMARRAGE DE WINDOWS

BCD

- Boot Configuration Data
- Depuis Windows Vista et Windows 2008
- Remplaçant du fichier BOOT.INI de Windows XP
- Modifiable avec la commande BCDEDIT.EXE
- Informations stockées dans le registre
  - HKLM/BCD00000000
- Fichier BCD dans la partition de démarrage
  - C:\Boot\
- 3 composants
  - Le magasin (BCD Stores)
  - Les objets (BCD Objects)
  - Les éléments de mises au point (BCD Elements)

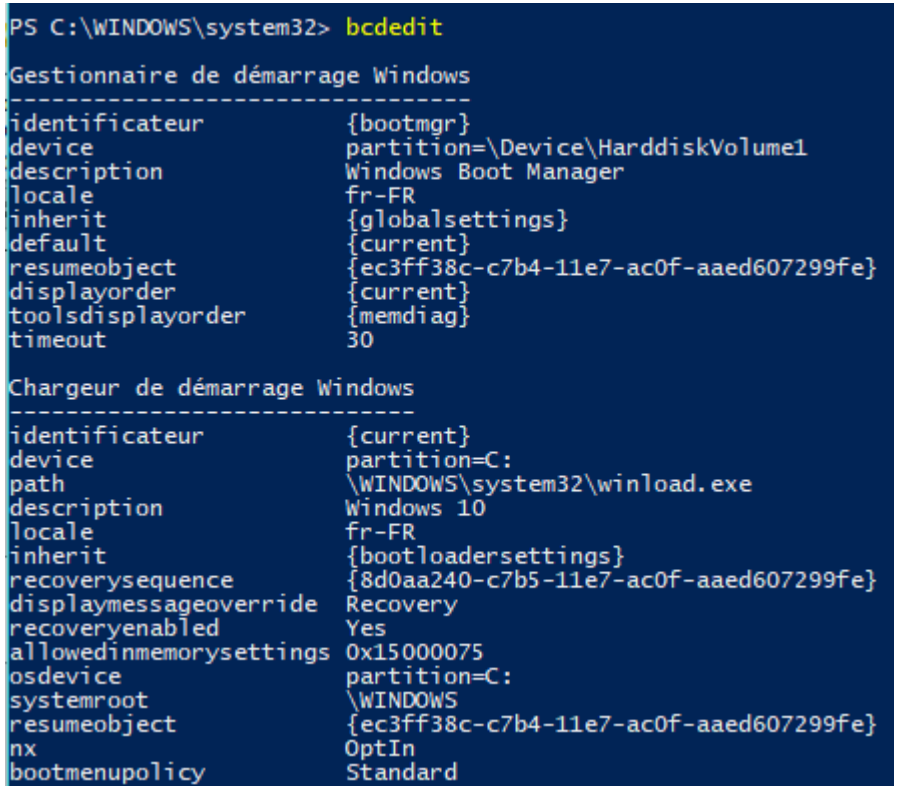
DÉMARRAGE DE WINDOWS

BCD



DÉMARRAGE DE WINDOWS
BCD

- Les données du BCD ne sont pas accessibles directement car stockées de manière binaire.
- Un outil pour modifier le BCD
  - BCDEdit.exe
    - Ligne de commande
    - Nombreuses commandes et options
- D'autres outils
  - MsConfig.exe
  - EasyBCD (outil tiers)
  - Etc…



Windows et Active Directory

Configuration

SR v2019

CONFIGURATION

Outils de base

- Gestionnaire de serveur
  - Ajouter ou supprimer des rôles et des fonctionnalités
  - Gérer les disques
  - Gérer le pare-feu
  - Diagnostiquer le système
  - Gérer les comptes utilisateurs locaux
  - Gérer les périphériques
  - Planifier des tâches
  - Etc…
- Consoles MMC

CONFIGURATION

Outils de base

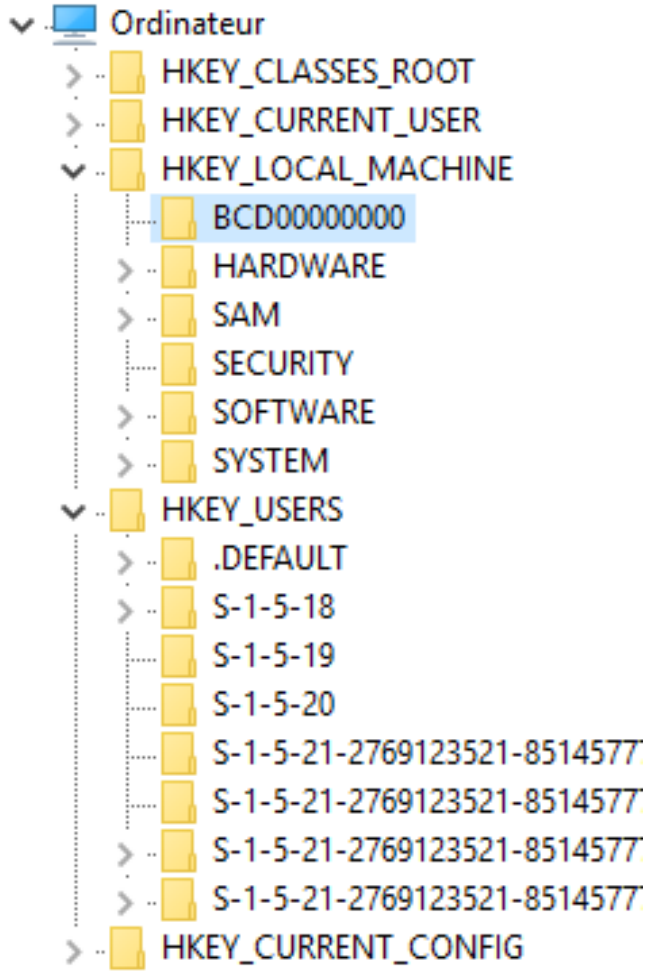
- Remote Server Administration Tools (RSAT)
  - Fonctionnalité de serveur
  - Outils d'administration de serveur distant
  - Remplaçant de l'ADMINPAK depuis Windows 7
- Administration à distance
  - Activer la fonctionnalité sur le serveur
  - Utilisation du protocole RDP 6.1 (Remote Desktop Protocol)
- Invite de commandes CMD.EXE
- Invite de commandes POWERSHELL.EXE

CONFIGURATION

Base de registres

- Base de données contenant la majeure partie des paramètres de configuration d'un système Windows

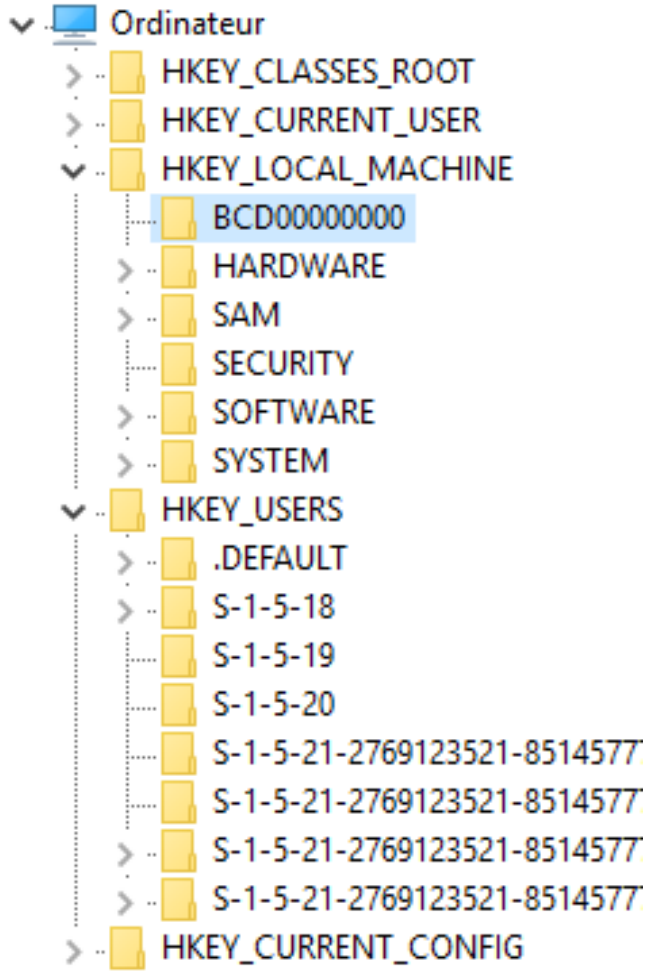
- Editable via REGEDIT.EXE ou REG.EXE
  - Branches
  - Clés et sous-clés
  - Valeurs typées
  - Données



CONFIGURATION

Base de registres

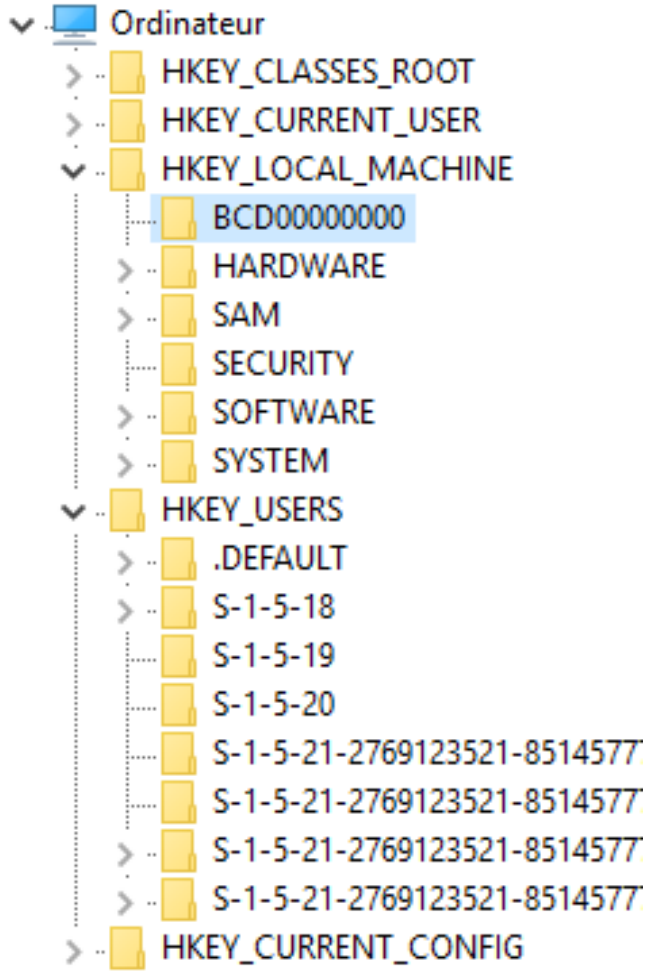
- HKEY_LOCAL_MACHINE (HKLM)
  - Configuration de la machine, du système et des applications. Uniquement modifiable par le système et les Administrateurs.
  - 6 clés : HARDWARE, SAM, SECURITY, SOFTWARE, SYSTEM, BCD
- HKEY_USERS (HKU)
  - Chaque utilisateur y dispose d'une entrée où sont stockés ses paramètres personnels



CONFIGURATION

Base de registres

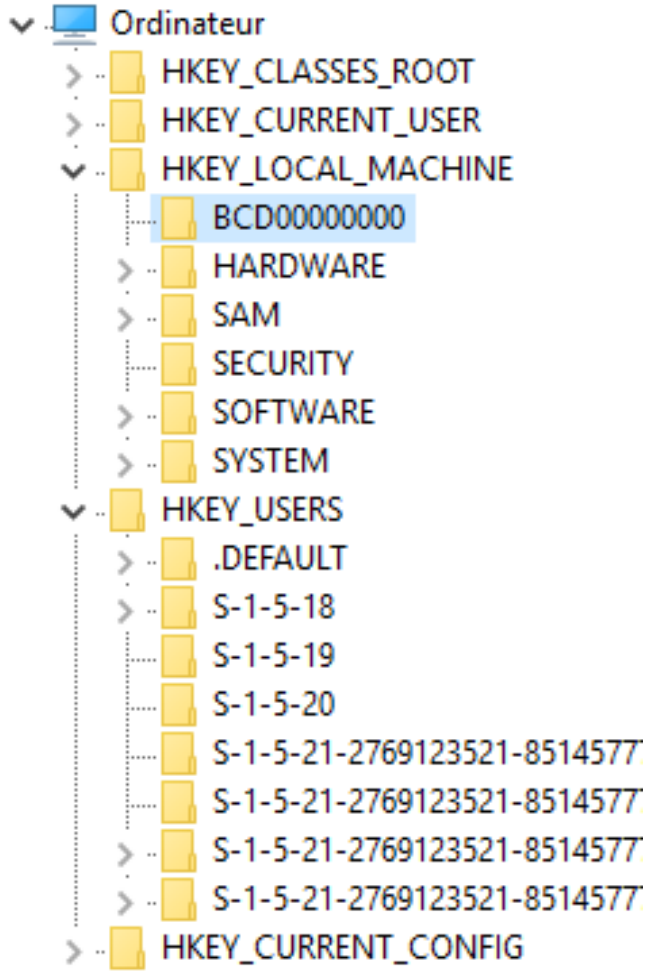
- HKEY_CURRENT_USER (HKCU)
  - Lien vers la sous-clé de l'utilisateur courant
    - HKEY_USER\<SID utilisateur courant>
- HKEY_CLASSES_ROOT (HKCR)
  - Configuration des objets COM (ProgIDs, CLSIDset IIDs) et des associations de fichiers
  - Fusion de deux parties :
    - HKEY_CURRENT_USER\SOFTWARE\Classes
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes



CONFIGURATION

Base de registres

- HKEY_PERFORMANCE_DATA (HKPD)
  - Journaux et compteurs de performances
  - Non visible via REGEDIT
- HKEY_CURRENT_CONFIG (HKCC)
  - Informations sur le profil matériel (uniquement pour compatibilité)
  - Lien vers
    - HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current



CONFIGURATION

Base de registres

- HARDWARE
  - détection PnP de la configuration matérielle
- SAM
  - base des comptes utilisateurs locaux
- SECURITY
  - paramètres de la politique de sécurité locale, domaines approuvés, secret d'identification des comptes de service
- SOFTWARE
  - paramètres de configuration du système et des logiciels
- SYSTEM
  - paramètres de configuration du système
- BCD00000000
  - Boot Configuration Data

CONFIGURATION

Base de registres

- Types de valeurs

REG_BINARY	Valeur binaire. Données binaires brutes
REG_DWORD	Valeur DWORD. Données représentées par un entier 32 bits
REG_EXPAND_SZ	Valeur de chaîne extensible. Chaîne de données à longueur variable pouvant contenir des variables.
REG_MULTI_SZ	Valeur de chaîne multiple. Liste de valeurs chaines.
REG_SZ	Valeur de chaîne.
REG_QWORD	Valeur QWORD. Données représentées par un entier 64 bits.

CONFIGURATION

Base de registres

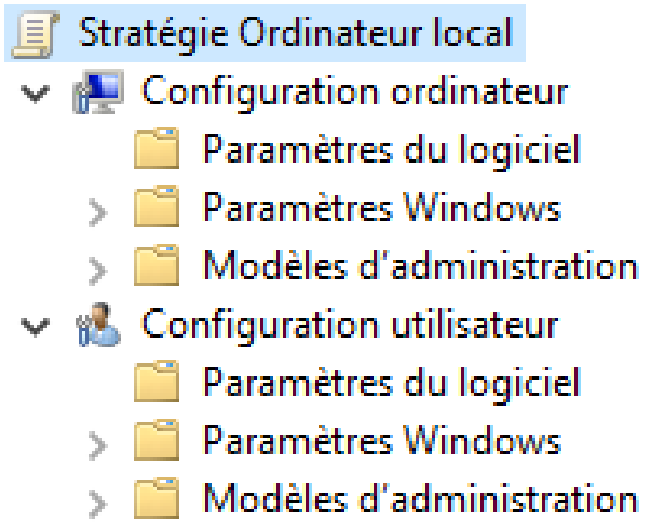
- Localisation des fichiers contenant la BDR (ruches)
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Hivelist

(par défaut)	REG_SZ	(valeur non définie)
\REGISTRY\MACHINE\BCD00000000	REG_SZ	\Device\HarddiskVolume1\Boot\BCD
\REGISTRY\MACHINE\HARDWARE	REG_SZ	
\REGISTRY\MACHINE\SAM	REG_SZ	\Device\HarddiskVolume2\WINDOWS\System32\config\SAM
\REGISTRY\MACHINE\SECURITY	REG_SZ	\Device\HarddiskVolume2\WINDOWS\System32\config\SECURITY
\REGISTRY\MACHINE\SOFTWARE	REG_SZ	\Device\HarddiskVolume2\WINDOWS\System32\config\SOFTWARE
\REGISTRY\MACHINE\SYSTEM	REG_SZ	\Device\HarddiskVolume2\WINDOWS\System32\config\SYSTEM
\REGISTRY\USER\.DEFAULT	REG_SZ	\Device\HarddiskVolume2\WINDOWS\System32\config\DEFAULT
\REGISTRY\USER\S-1-5-19	REG_SZ	\Device\HarddiskVolume2\WINDOWS\ServiceProfiles\LocalService\NTUSER.DAT
\REGISTRY\USER\S-1-5-20	REG_SZ	\Device\HarddiskVolume2\WINDOWS\ServiceProfiles\NetworkService\NTUSER.DAT
\REGISTRY\USER\S-1-5-21-2769123521...	REG_SZ	\Device\HarddiskVolume2\Users\adminlocal\NTUSER.DAT
\REGISTRY\USER\S-1-5-21-2769123521...	REG_SZ	\Device\HarddiskVolume2\Users\adminlocal\AppData\Local\Microsoft\Windows\UsrClass.dat
\REGISTRY\USER\S-1-5-21-2769123521...	REG_SZ	\Device\HarddiskVolume2\Users\Steeve\NTUSER.DAT
\REGISTRY\USER\S-1-5-21-2769123521...	REG_SZ	\Device\HarddiskVolume2\Users\Steeve\AppData\Local\Microsoft\Windows\UsrClass.dat

CONFIGURATION

Stratégies de groupe locales

- Fonctionnalité apparue avec Windows 2000
  - Héritée des stratégies de comptes, des stratégies de droits, des stratégies d'audit et des stratégies systèmes de NT4
- Accessible via GPEDIT.MSC
- Permet de gérer simplement
  - La configuration ordinateur
  - La configuration utilisateur
- Paramètres fusionnés au registre
  - Au démarrage du système
  - À l'ouverture de session



CONFIGURATION
Stratégies de groupe locales

- Configuration ordinateur
  - DNSSec
  - Script de démarrage ou d'arrêt
  - Paramètres de sécurité
    - stratégies de comptes : mots de passe, verrouillage de comptes
    - Stratégies locales : audit, droits, options de sécurité
    - Parefeu
    - Stratégies de clé publique
    - AppLocker
    - IPSec
  - QoS
  - Modèles d'administration (composants Windows, imprimantes, serveur, système…)
- Configuration utilisateur
  - Script d'ouverture ou de fermeture de session
  - Stratégies de clé publique
  - QoS
  - Modèles d'administration (bureau, dossiers partagés, menu démarrer…)

CONFIGURATION

Stratégies de groupe locales

- Les paramètres définis sont stockés dans
  - %SystemRoot%\System32\ GroupPolicy\Machine\registry.pol
  - %SystemRoot%\System32\ GroupPolicy\User\registry.pol

- Les modèles d'administration sont définis
  - Par fichiers .ADMX et .ADML
  - Dans C:\WINDOWS\PolicyDefinitions

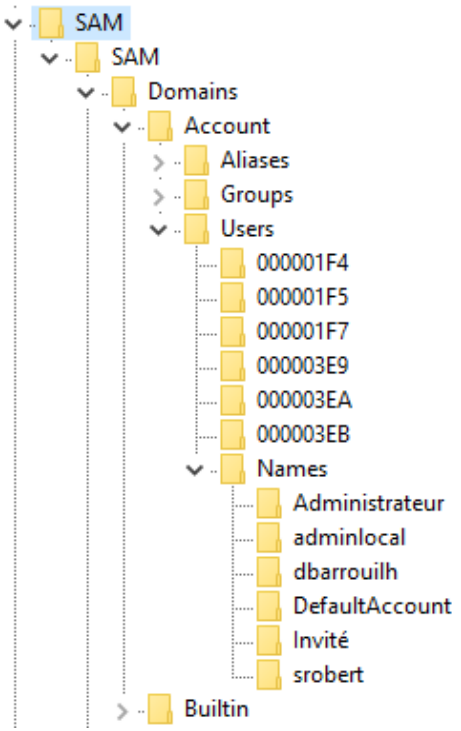
Windows et Active Directory

Comptes locaux

SR v2019

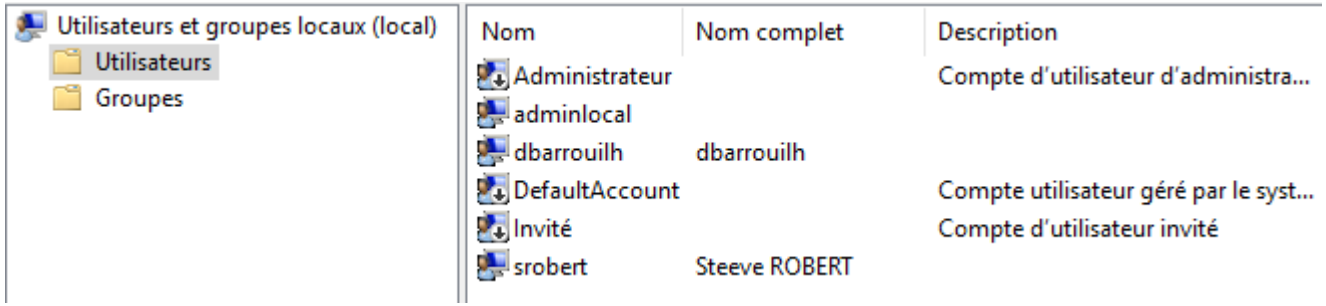
COMPTES LOCAUX

Base SAM



- Comptes d'utilisateurs et de groupes stockés localement sur un serveur
  - %SYSTEMROOT%\SYSTEM32\CONFIG\SAM

- Gérés par LUSRMGR.MSC



- Droits et autorisations accordés sur ce serveur uniquement

COMPTES LOCAUX
Base SAM

- Utilisateurs locaux par défaut
  - Administrateur
  - Invité

- Groupes locaux par défaut
  - Administrateurs
  - Opérateurs de sauvegarde
  - Invités
  - HelpServicesGroup
  - Opérateurs de configuration réseau
  - Utilisateurs de l'Analyseur de performances
  - Utilisateurs du journal des performances

COMPTES LOCAUX
Base SAM

- Utilisateurs avec pouvoir
  - peuvent créer des comptes d'utilisateurs, les modifier et les supprimer, peuvent créer des groupes locaux, puis y ajouter ou supprimer des utilisateurs.
- Opérateurs d'impression
- Utilisateurs du Bureau à distance
- Réplicateur
- Utilisateurs Terminal Server
  - contient tous les utilisateurs actuellement connectés au système à l'aide de Terminal Server.
- Utilisateurs