Services Windows
et pilotes

AB – v1.30 (29/09/2022)

Services

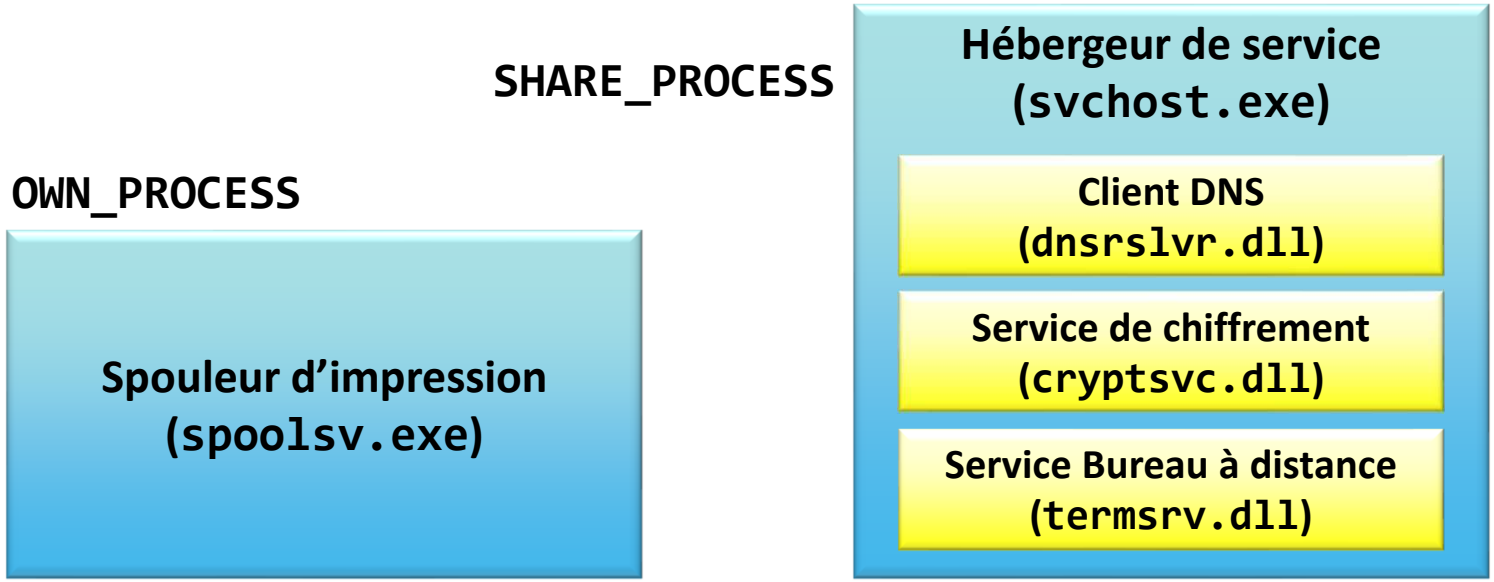
- Le terme « service » fait référence à deux concepts :
  - **Service applicatif (*service application*)** : programme destiné à s'exécuter en arrière plan, généralement démarré à l'initialisation du système et avant les connexions des utilisateurs
  - **Pilote (*driver service*)** : fichier de type pilote de périphériques et chargé par le noyau

SCM (Service Control Manager)

- C'est le **SCM (Service Control Manager)** qui est chargé de la gestion des **services** et d'une partie des **pilotes** :
  - gestion de la base des **services**/**pilotes** installés :
    - ajout/suppression/configuration
    - verrouillage de la base
  - démarrage (automatique/manuel) et arrêt des **services** et de certains **pilotes**
  - gestion de l'exécution des **services** (liste des services actifs, surveillance des processus, etc.)

Types de services

- Un **service** peut prendre la forme :
  - D'un processus autonome (**OWN_PROCESS**)
  - D'un module chargé dans l'hébergeur de service svchost.exe (**SHARE_PROCESS**)



Paramètres des services

Configuration des services

- La base de configuration des services et des pilotes (*Services Active database* ou *SCM database*) est stockée dans le registre :

  `HKLM\SYSTEM\CurrentControlSet\Services`

- Il n'est pas recommandé de manipuler directement cette base mais plutôt de passer par l'API du SCM : `QueryServiceConfig2()`, `ChangeServiceConfig()`, etc.

Outils de gestion des services

- **Ligne de commande :**
  - net start / net stop
  - sc (très complet)
- **Graphique :**
  - services.msc
- **Powershell :**
  - Get-Service, Set-Service, Start-Service, etc.
- **Autres :**
  - ProcessHacker

Paramètres de base

- Nom du service (nom de la clé)
- Nom d'affichage (**`DisplayName`**)
- Description (**`Description`**)
- Chemin de l'exécutable (**`BinaryPathName`** → **`ImagePath`**) :
  - exe ou dll pour les services
  - sys pour les pilotes
- Dépendances (**`Dependencies`** → **`DependOnGroup/DependOnService`**)
- Groupe de chargement (**`LoadOrderGroup`** → **`Group`**)
- Identifiant (**`TagId`** → **`Tag`**)
- Compte sous lequel le service s'exécute ou nom explicite de l'objet pilote associé (**`ServiceStartName`** → **`ObjectName`**)
- Mot de passe (**`Password`**)
- Comportement en cas d'impossibilité de démarrer le service (**`ErrorControl`**)

Paramètres de base

- Type de service (*dwServiceType***Type**) :
  - SERVICE_WIN32_OWN_PROCESS
  - SERVICE_WIN32_SHARE_PROCESS
  - + SERVICE_INTERACTIVE_PROCESS
  - SERVICE_KERNEL_DRIVER
  - SERVICE_FILE_SYSTEM_DRIVER
- Méthode de démarrage (*dwStartType***Start**) :
  - SERVICE_AUTO_START
  - SERVICE_DEMAND_START
  - SERVICE_DISABLED
  - SERVICE_BOOT_START
  - SERVICE_SYSTEM_START

Paramètres avancée

- Actions d'échec (**FAILURE_ACTIONS**)
- Démarrage différé (**DELAYED_AUTO_START**) Vista
- Délai de pré-arrêt (**PRESHUTDOWN**) Vista
- Déclencheurs (**TRIGGER**) 7
- Nœud processeur (**PREFERRED_NODE**) 7
- Sécurité (cf. cours mécanismes avancés) :
  - Privilèges requis (**REQUIRED_PRIVILEGES**) Vista
  - Niveau SID de service (**SID**) Vista
  - Niveau de PPL (**LAUNCH_PROTECTED**) 8.1

Compte associé
et
comptes de service

Comptes exécutant les services

- Chaque service applicatif s'exécute dans le contexte de sécurité d'un compte. Il est possible d'utiliser :
  - Un compte utilisateur local ou d'un domaine (non recommandé)
  - Un des trois **comptes de services** intégrés (préférable) :
    - **`LocalSystem`**
    - **`LocalService`** (XP)
    - **`NetworkService`** (XP)
  - Un compte de service virtuel (7/2008 R2)
  - Un compte de service géré (MSA) :
    - local : sMSA (7/2008 R2)
    - de groupe : gMSA (8/2012)
  - Le compte d'un utilisateur authentifié interactivement (10)

LocalSystem
(NT AUTHORITY\SYSTEM)

- Entité de sécurité qui possède le plus haut niveau de droits et privilèges. Ce contexte de sécurité contient :
  - NT AUTHORITY\SYSTEM
  - BUILTIN\Administrateurs
- Utilise le profil `HKEY_USERS\.DEFAULT` (alias `S-1-5-18`)
- Authentification à distance :
  - Kerberos : s'authentifie avec le compte de l'ordinateur
  - NTLM : ne peut pas s'authentifier (session NULL / utilisateur anonyme). Modifiable depuis Windows 7
- Possibilité d'interagir avec le bureau (obsolète depuis Vista)

LocalService (NT AUTHORITY\LOCALSERVICE)

- Compte à droits restreints disponible à partir de XP
- Utilise le profil HKEY_USERS\S-1-5-19
- Peu de privilèges :
  - AUDIT, CHANGE_NOTIFY, UNDOCK, IMPERSONATE
  - Ceux de Utilisateurs et Utilisateurs authentifiés
- Ne peut pas s'authentifier à distance (session NULL / utilisateur anonyme)

NetworkService
(NT AUTHORITY\NETWORK SERVICE)

- Compte à droits restreints disponible à partir de XP
- Utilise le profil HKEY_USERS\S-1-5-20
- Peu de privilèges :
  - AUDIT, CHANGE_NOTIFY, UNDOCK, IMPERSONATE
  - Ceux de Utilisateurs et Utilisateurs authentifiés
- S'authentifie avec le compte de l'ordinateur lors des authentifications distantes (Kerberos et NTLM)

Service Host Process (svchost.exe)

- C'est l'hébergeur de services pour les services de type `SERVICE_WIN32_SHARE_PROCESS`, implémentés sous forme de bibliothèque (DLL)
- Plusieurs `svchost.exe` s'exécutent simultanément (un par groupe de service)

- Liste des groupes de services :

  HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Svchost

- DLL d'exécution :

HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters (ServiceDll)

Regroupement des services Microsoft (Windows 8)

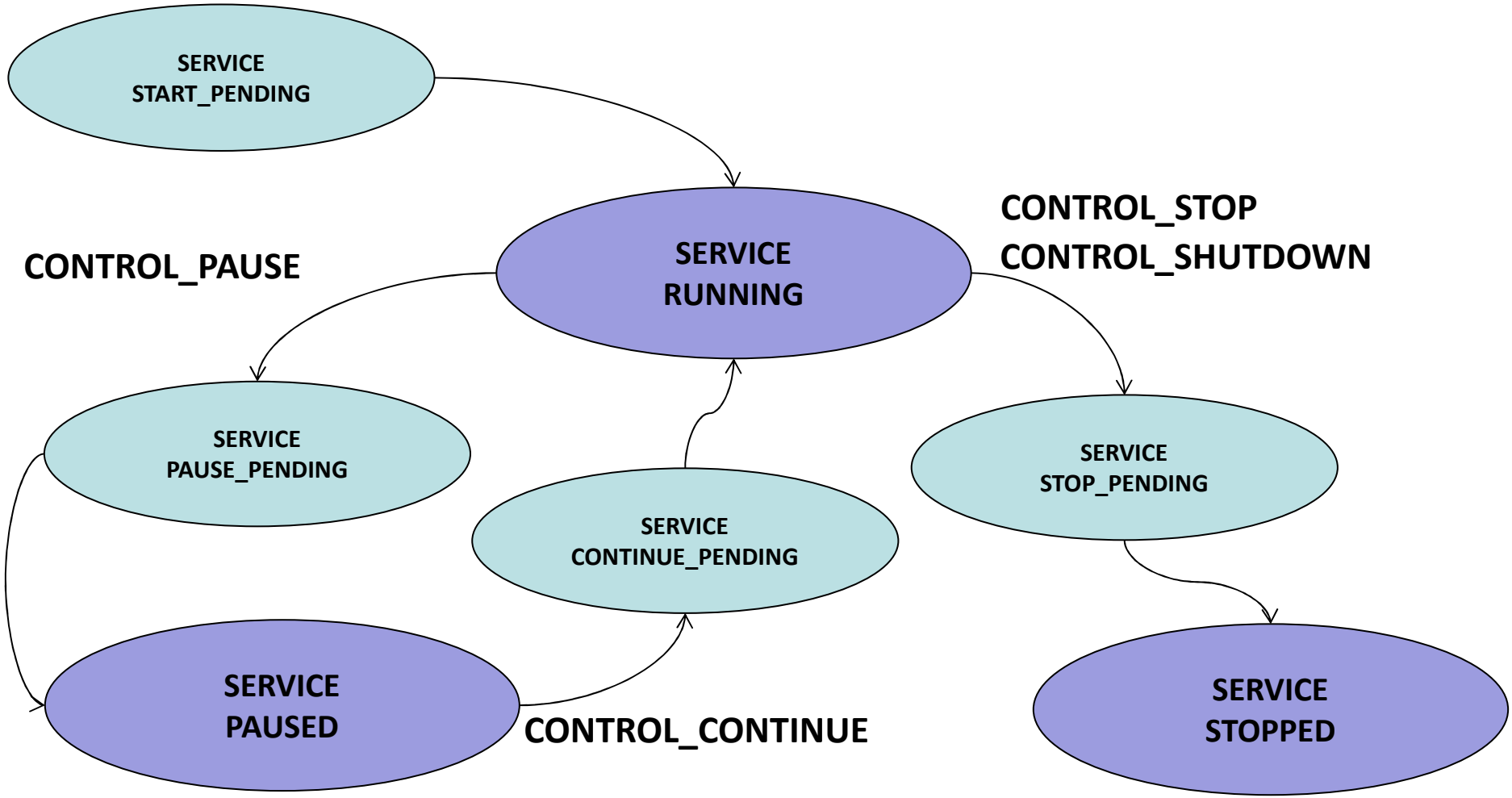
Nom	Compte de service	Note
LocalSystemNetworkRestricted	SYSTEM	
LocalService	LocalService	
LocalServiceAndNoImpersonation	LocalService	Perte de privilège Impersonation
LocalServiceNetworkRestricted	LocalService	
LocalServiceNoNetwork	LocalService	Pas d'accès réseau
LocalServicePeerNet	LocalService	
NetworkService	NetworkService	
NetworkServiceAndNoImpersonation	NetworkService	Perte de privilège Impersonation
NetworkServiceNetworkRestricted	NetworkService	
Autres : RPCSS, DcomLaunch, netsvcs, imgsvc	Divers	Divers

Nouveautés de Windows 10

- Services de type **`SERVICE_USER_SERVICE`**
  - À chaque ouverture d'une session d'un utilisateur, un service de type **`SERVICE_USERSERVICE_INSTANCE`** est automatiquement créé
  - Si le service est démarré, il s'exécute dans le même contexte de sécurité que celui de l'utilisateur qui a ouvert la session
  - Ces services sont automatiquement arrêtés et supprimés lorsque l'utilisateur ferme sa session
- Windows 10 RS2 :
  - Pour les systèmes avec plus de 3,5Go de mémoire, les services partagés sont exécutés dans un hébergeur de service différents (`svchost.exe -k <svchost name> -s <service name>`)

États et notifications des services

États et notifications d'un service



Programmation d’un service

Forme du programme

- Pour les services de type **SERVICE_WIN32_OWN_PROCESS**, choisir une application de type console ou graphique afin de générer un programme autonome

- Pour les services de type **SERVICE_WIN32_SHARE_PROCESS**, choisir une application de type bibliothèque (DLL) qui sera chargée via l'hébergeur de service (svchost.exe)

Étape 1

- Au lancement du programme :
  - enregistrement des services (structure `SERVICE_TABLE_ENTRY`)
  - définition de la fonction d'initialisation de chaque service

```
SERVICE_TABLE_ENTRY DispatchTable[] =
{
   { ... SvcServiceMain },
   ...
};

StartServiceCtrlDispatcher(DispatchTable);
```

Étape 2

- Définition de la fonction d'initialisation du service (**`ServiceMain`**) :
  1. Appel à **`RegisterServiceCtrlHandle`** :
     - Enregistrement d'un *control Handler*
     - *R*écupération du *handle* d'état du service (*service status handle*)
  2. Notification d'état de démarrage (**`SERVICE_START_PENDING`**)
  3. Code d'initialisation du service
  4. Lorsque le service est en état opérationnel, notification d'état de fin de démarrage (**`SERVICE_RUNNING`**)

Notification émise par le service au SCM

- Réalisé via la fonction **`SetServiceStatus`**, qui prend en paramètres :
  - le *handle* d'état du service
  - une structure de type **`SERVICE_STATUS`** définissant :
    - Le type de service
    - L'état du service :
      - CONTINUE_PENDING, PAUSE_PENDING, PAUSED, RUNNING, START_PENDING, STOP_PENDING, STOPPED
    - Les notifications acceptées :
      - STOP, SHUTDOWN, PRESHUTDOWN, PAUSE_CONTINUE, PARAMCHANGE, NETBINDCHANGE

Control Handler
Handler / HanlerEx

- Permet au SCM de notifier un changement d'état pour le service (fonction de type *callback*) :
- Changements d'états possibles :
  - INTERROGATE
  - STOP
  - SHUTDOWN
  - PAUSE
  - PARAMCHANGE
  - CONTINUE
  - NETBINDXXX