Leçon 10 : Service de bureau à distance[34]

10.1 Introduction

Le service de bureau à distance est un moyen simple de permettre à des utilisateurs de se connecter *en mode graphique* sur le serveur. En effet, ce service permet aux utilisateurs désignés d'ouvrir une session distante sur le serveur : les programmes sont lancés à distance mais l'affichage est local.

Microsoft propose, depuis Windows XP, l'accès bureau à distance sur toutes les versions professionnelles de son système d'exploitation. Sur ces versions *non-serveurs*, seul un utilisateur peut être connecté à la machine (soit localement, soit à distance).

Sur un serveur Windows Server *sans le service de bureau à distance*, Microsoft autorise 2 connexions au total : soit 2 sessions distantes, soit une session locale et une session distante. Si le service de bureau à distance est activé, le nombre de connexion est limité en fonction des licences acquises.

10.2 Activation du bureau à distance

Sans installation du service bureau à distance (service RD), il est possible d'activer le bureau à distance sur des postes clients (Windows XP, Windows Vista, …) ou sur des serveurs. Pour ce faire, il faut aller dans **Control Panel > System and security > System** et choisir l'option **Remote Settings**.

Dans le panneau du bas, on trouve l'espace *remote desktop*. Il suffit de choisir l'option *autorisant la connexion* [Allow remote connection] pour que le bureau à distance limité soit activé. Par défaut, seuls les administrateurs peuvent ouvrir une session à distance. Si vous souhaitez autoriser des utilisateurs, il faut cliquer sur **select Users** et ajouter les utilisateurs souhaités.

Une fois le bureau à distance activé, il est possible de se connecter à l'ordinateur en question en démarrant, depuis une autre machine, le programme de **Remote Desktop connection**[35] et en entrant **le nom ou l'adresse IP de la machine** sur laquelle vous souhaitez vous connecter.

Pour information, le port réseau utilisé pour la connexion bureau à distance est le port TCP 3389. **Attention !** La connexion bureau à distance n'est pas jugée comme *suffisamment* sûre que pour pouvoir l'autoriser à travers l'internet. Il est possible de sécuriser cette installation en déployant une passerelle TS utilisant SSL. Il est également possible d'activer des options de verrouillage dans le cas de plusieurs tentatives de connexion ratées.

10.3 Le service bureau à distance

Le service bureau à distance est moins limité que le bureau à distance. En effet, utiliser le service permet :

- D'avoir plusieurs utilisateurs connectés en même temps (en fonction du modèle de licences choisi).
- De lancer des applications distantes, s'exécutant sur le serveur mais visible sur le poste client (sans avoir besoin d'ouvrir une session au préalable)
- D'avoir une interface web d'accès au service de bureau à distance

[34] Ce service se nommait *Terminal Server* dans les versions Windows Server 2008 et antérieures
[35] Vous pouvez également chercher après le programme mstsc.exe (MicroSoft Terminal Server Client)

- D'installer une passerelle bureau à distance permettant l'accès à d'autres serveurs même s'ils sont localisés derrière un routeur (qui cache leur adresse IP en faisant du NAT). De plus, la communication est sécurisée au moyen de SSL.

10.3.1 Modèle de licences

Le service bureau à distance admet 2 modèles de licences : les licences *par utilisateur* et *par périphérique*[36]. Un modèle de licence *par utilisateur* permet une connexion simultanée d'un nombre défini d'utilisateurs (les licences n'étant pas attitrées mais consommées et libérées au fur et à mesure). Ainsi, si une entreprise achète 10 licences utilisateurs pour ses 30 employés, 10 utilisateurs maximum peuvent se connecter au serveur à un instant donné.

A l'inverse, les licences *par périphérique* sont attachées au périphérique. Elles sont donc permanentes et réservées. Ce modèle de licence est rarement utilisé pour la gestion des connexions au service bureau à distance.

Pour gérer ces licences, il faut installer le service des licences bureau utilisateur sur un serveur. Cependant, nous n'étudierons pas cet aspect. De plus, Microsoft propose une période *de grâce* (sans limitation) de 120 jours.

10.3.2 Installation

L'installation du service bureau à distance passe par l'ajout d'un rôle sur les serveurs concernés. Pour ce faire, **il faut être connecté avec un compte du domaine** (comme l'administrateur du domaine `DOMAINE\Administrator`) et aller dans **Server Manager > Manage > Add Roles and Features**. Dans le *type d'installation*, choisir **Remote Desktop Services installation**.

Attention ! Le service ne doit être installé que sur les machines qui doivent accueillir des connexions d'utilisateurs en mode graphique. S'il s'agit simplement de permettre à l'administrateur d'accéder à distance à ses serveurs le mécanisme *bureau à distance* intégré à toutes les versions de Windows est suffisant.

L'installation se passe en plusieurs étapes :

1. L'écran suivant propose le *type de déploiement*, il convient de choisir l'option **Standard deployment**.
2. Ensuite, le *Scénario de déploiement* propose deux choix, il convient de choisir l'option **Session-based desktop deployment**. Ainsi les services de rôle suivants seront installés : Service Broker pour les connexions Bureau à distance, Accès Bureau à distance par le web et Hôte de session Bureau à distance.
3. Dans l'étape suivante (*Specify RD Connection Broker Server)* il faut ajouter le serveur courant dans les ordinateurs sélectionnés.
4. Sur l'écran *Specify RD Web Access server,* il faut cocher l'option *Install the RD Web Access role service on the RD connection Broker server* qui se trouve en haut de la fenêtre, puis choisir **Next**.
5. Sur l'écran *Specify RD Session Host Servers*, il faut ajouter le serveur courant aux serveurs sélectionnés, puis choisir **Next**.

[36] On parle de *licence CAL par utilisateur* ou de *licence CAL par périphérique*

6. Dans l'écran de confirmation, il faut simplement cocher la case *Restart the destination server automatically if required* et choisir l'option **Deploy**.

Pour des raisons de sécurité, il n'est pas recommandé d'installer les services bureau à distance sur le contrôleur de domaine.

10.3.3 Configuration

La configuration du service de bureau à distance passe par le **server manager** via l'option *Remote Desktop Services* dans le menu de gauche (cf. figure 10.1).

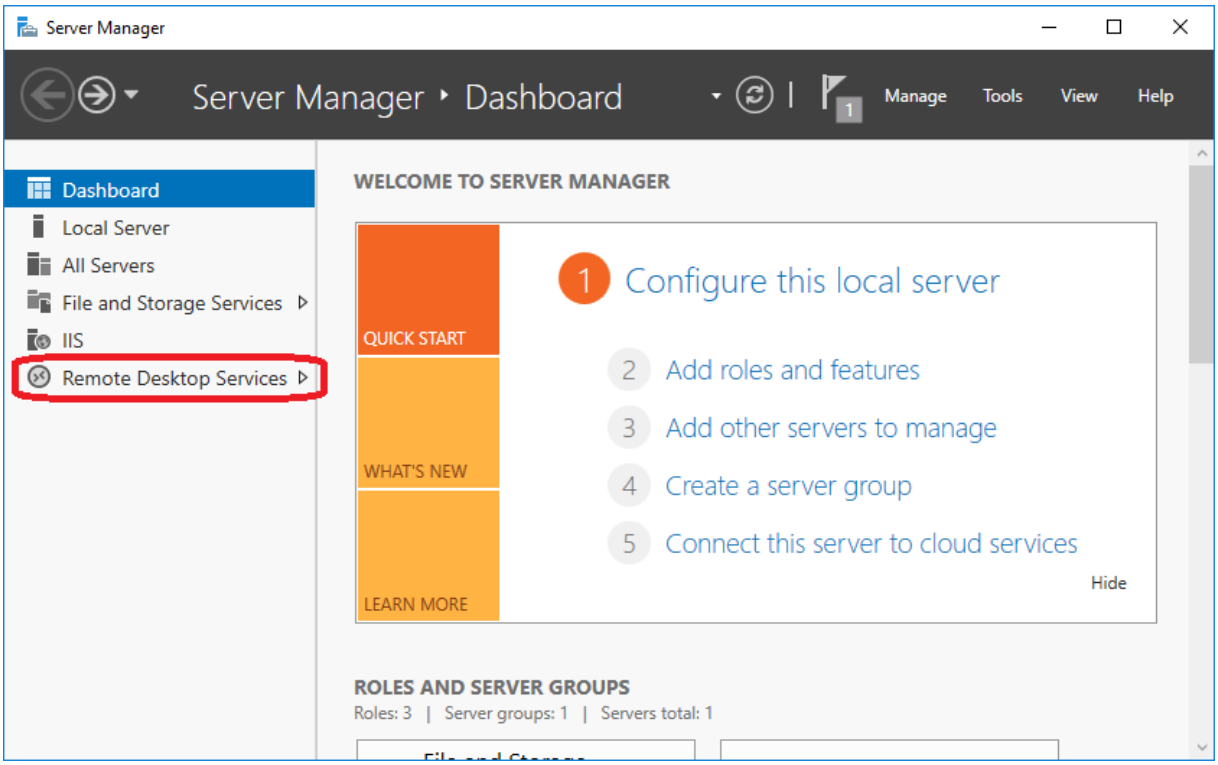

Figure 10.1 : Gestionnaire de serveur et l'option de configuration du service bureau à distance

Dans la configuration, on trouve :

- *Overview* : qui reprend le mode de déploiement des différents services liées au bureau à distance.
- Servers : qui reprennent la liste des serveurs sur lesquels les services bureau à distance sont déployés
- Collections : elles permettent de gérer les connexions actives et de définir une collection de sessions. La collection de sessions permet d'autoriser la connexion sur un ou plusieurs serveurs.

Il faut donc créer une **nouvelle collection** (en cliquant sur **Tasks > Create Session Collection**) pour débuter. Sur l'écran *Name the collection*, il faut choisir un nom. Sur l'écran *Specify RD Session Host servers*, Il faut ensuite sélectionner le ou les serveurs inclus dans cette collection. Le système propose alors de sélectionner les utilisateurs (*Specify user groups*) qui seront autorisés à se connecter au service de bureau à distance. Il est possible d'inclure un groupe d'utilisateurs ici. L'option *User Profile Disks* est une option que nous n'utiliserons pas ici, il convient donc de **désactiver** ce paramètre. Apparaît alors l'écran de *Confirmation*. En cliquant sur **Create** la collection de sessions est créée.

Une fois la session créée, elle apparait dans le **Server Manager**. Les paramètres de la collection de sessions peuvent être modifiés via l'option **Tasks > Edit Properties** (voir figure 10.2).

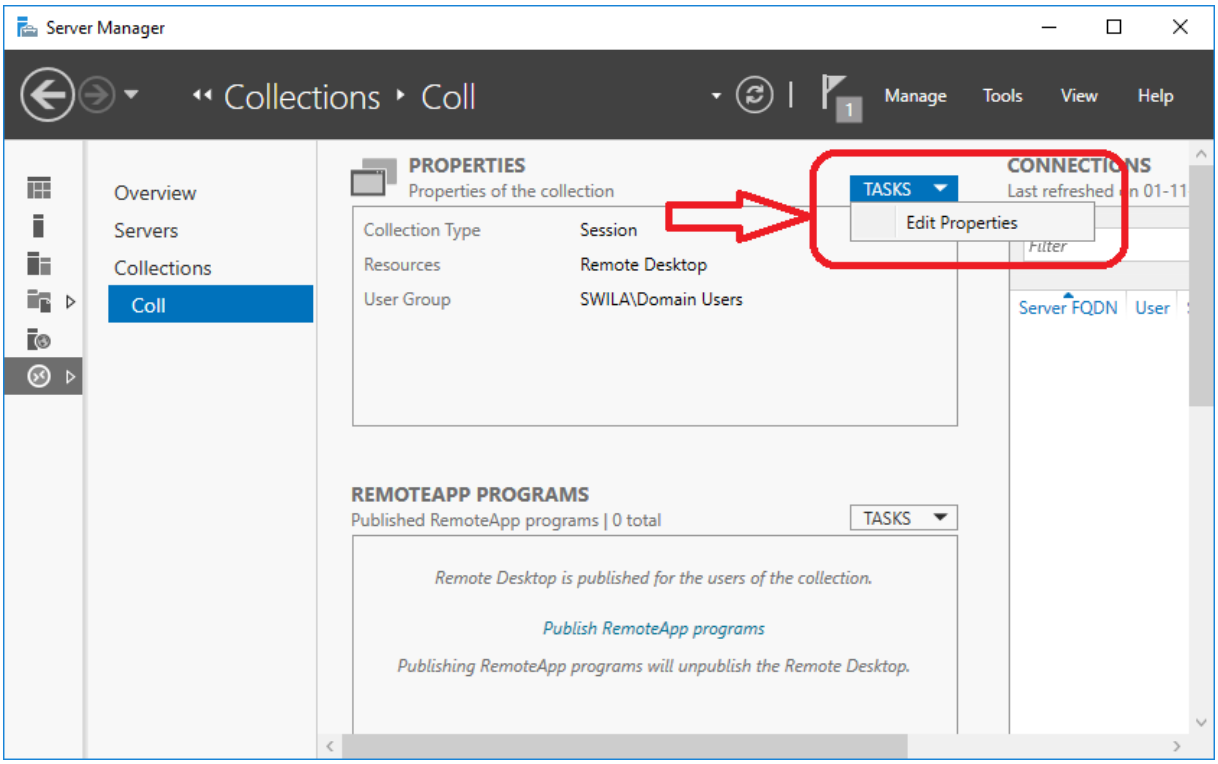

Figure 10.2 : Propriétés d'une collection de sessions (ici nommée Coll)

Par cette option, il est possible de modifier/préciser les propriétés suivantes :

- *General* : qui précise le nom de la collection
- *User Groups* : précise les groupes d'utilisateurs qui sont autorisés à accéder au service de bureau à distance et aux éventuelles RemoteApp configurées.
- *Session* : qui permet de définir les paramètres propres à la session de l'utilisateur qui se connecte. On y trouve ainsi tous les paramètres permettant de *limiter* dans le temps la session bureau à distance. En effet, tant que l'utilisateur ne clique pas expressément sur *Sign out*, celle-ci reste présente au niveau du serveur. Il est donc impératif de configurer les paramètres de fin de session sinon celles-ci peuvent durer plusieurs jours et consommer une licence. Cependant, on gère rarement ces paramètres depuis le serveur lui-même. En effet, on préfère habituellement définir une *policy* particulière qui s'appliquera au(x) serveur(s) concerné(s). Le comportement lorsque la limite de la session est atteinte peut également être précisé ici.
- *Security* : permet de mentionner les paramètres de sécurité applicables à la collection de sessions. Précisément, cette option détermine comment les informations sont chiffrées, avec quel niveau de chiffrement. Il faut noter que l'option **allow connections only from computers running Remote Desktop with Network Level Authentication** exige que les postes clients exécute au moins Windows XP SP2 ou supérieur.
- *Load Balancing* : détermine quels serveurs doivent être préféré en fonction des ressources disponibles. Nous utiliserons un seul serveur, ce paramètre n'est pas important pour nous.

- *Client Settings* : permet d'autoriser ou non les redirections des ressources (disques, presse-papier, imprimantes) du client.
- *User Profile Disks* : permet d'activer ou non le stockage des paramètres utilisateurs (dans des profils particuliers) vers un emplacement réseau. Cette option est intéressante si les utilisateurs qui se connectent sur le serveur n'ont pas de profil itinérant stocké sur un serveur particulier ou si l'administrateur souhaite que l'utilisateur dispose d'un profil particulier lorsqu'il ouvre une session bureau à distance.

Les différents états d'une session sont : **active** lorsque l'utilisateur est connecté à la session et est en occupé à travailler, **inactive** lorsque l'utilisateur est connecté à la session mais n'y travaille plus depuis un certain temps et **disconnected** lorsque l'utilisateur a *fermé la connexion au serveur sans fermer la session (sans passer par l'option Sign Out)*. Ainsi il est recommandé de limiter le temps des différents états d'une session et, dans certains cas, de fermer automatiquement les sessions déconnectées après un temps donné.

En ce qui concerne **les utilisateurs autorisés** : une bonne pratique serait de créer un groupe dans le domaine reprenant tous les utilisateurs autorisés à se connecter en bureau à distance. Il est également possible de spécifier les utilisateurs autorisés à se connecter au moyen d'une GPO applicable à cet ordinateur : **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services**. On peut, là aussi, y mentionner les groupes qui peuvent se connecter. La **GPO est prioritaire** (écrase les paramètres) dans le choix des groupes qui peuvent se connecter au serveur.

10.3.4 Déploiement de logiciels sur le serveur RD

Très souvent, on utilise le service de bureau à distance pour mettre à disposition des utilisateurs une application commune. Cette application peut, dès lors, être utilisée en même temps par plusieurs utilisateurs connectés à des sessions bureau à distance.

Afin de pouvoir réaliser l'installation de l'application pour l'ensemble des utilisateurs, Microsoft propose de réaliser l'installation en *basculant* le serveur en mode d'installation bureau à distance. Pour ce faire, il faut aller dans le **Control Panel** du serveur exécutant le service RD et choisir **Install Application on Remote Desktop Server.** Une autre possibilité existe en utilisant la *ligne de commande*. En effet, il suffit d'entrer :

```
C:\> change user /install
```
Cette commande permet de basculer le serveur en mode installation.

```
C:\> change user /query
```
Cette commande permet de connaître le mode dans lequel le serveur se trouve.

```
C:\> change user /execute
```
Cette commande permet de basculer le serveur en mode exécution (mode par défaut).

Cette étape, nécessaire sous Windows Server 2008 R2 et précédent ne *semble plus nécessaire dans tous les cas*[37] avec la version Windows Server 2016.

[37] Notamment lors de l'installation de packages .msi. Cependant, en cas de problème, cette option reste toujours disponible.

10.4 Les sessions Bureau à distance

10.4.1 Démarrer une session depuis un poste client

Le poste client peut démarrer une connexion bureau à distance en démarrant l'outil *remote desktop connection* ou en exécutant le programme `mstsc.exe`. L'intérêt de l'outil est de pouvoir configurer quelques éléments en cliquant sur le bouton **Show Options**.

Comme nous pouvons le voir sur la figure 10.3, que de nombreuses options sont présentes :

- *L'onglet General* : présente les options principales comme l'ordinateur distant vers lesquels il faut établir la connexion dans le champ *Computer* (son nom ou son adresse IP), le nom d'utilisateur à utiliser dans le champ *User name* (il est toujours préférable de mentionner **DOMAINE\Login** dans le cas d'une connexion avec un compte d'utilisateur définit dans le domaine ou **MACHINE\Login** dans le cas d'une connexion avec un compte d'utilisateur local au serveur. Mentionnons également la possibilité de **créer un fichier RDP de connexion**. Ce fichier contient alors tous les paramètres et peut être facilement distribué aux utilisateurs.
- *L'onglet Display* : qui mentionne les paramètres d'affichage comme la résolution ou le nombre de couleurs.
- *L'onglet Local Ressources* : qui mentionne les ressources locales qui seront automatiquement connectées à la session de l'utilisateur lors de la connexion.

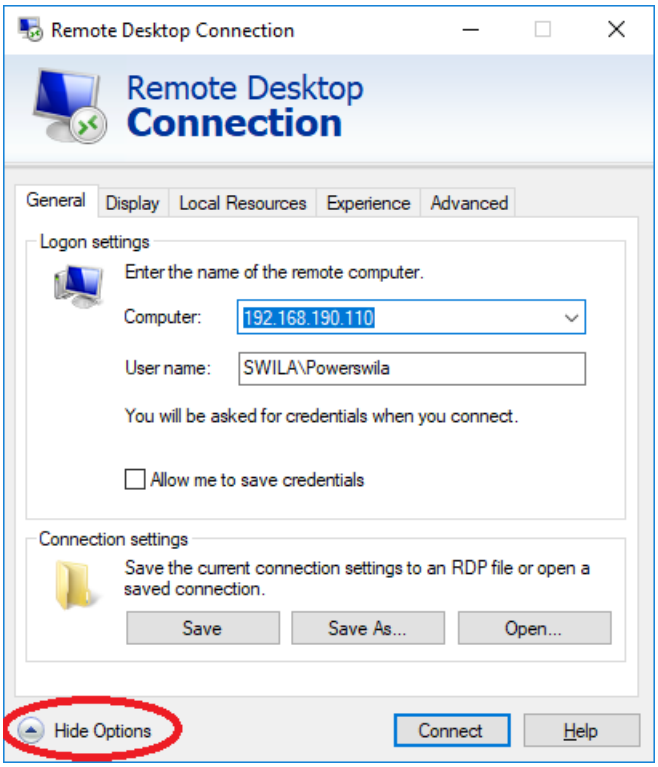

Figure 10.3 : Options pour la connexion Bureau à distance

- *L'onglet Experience* : gère les options d'optimisation et de reconnexion en cas de perte de celle-ci.
- *L'onglet Advanced* : permet de déterminer comment la connexion doit être réalisée vers le serveur. Il est ainsi possible de mentionner les options d'authentification mais également les options de passerelles. La passerelle est un mécanisme utilisant le serveur Web IIS pour

réaliser une connexion sécurisée vers un serveur RD au travers d'internet. Pour configurer cette particularité, il faut sélection l'option *RD Gateway* dans le tableau *Overview* (cf. Figure 10.1).

Une fois l'ensemble des paramètres définit, il est possible d'enregistrer ceux-ci dans un fichier RDP (onglet *General* option *Save* en bas de la fenêtre). La connexion se fait en cliquant sur le bouton **Connect** (ou en cliquant deux fois sur le fichier RDP sauvegardé).

10.4.2 Gestion des sessions utilisateurs

Lorsque des utilisateurs sont connectés via le service RD, il est possible de gérer les différentes sessions depuis le serveur lui-même. En effet, via la *collection des sessions* dans *le service Bureau à distance*, il est possible de visualiser les sessions en cours.

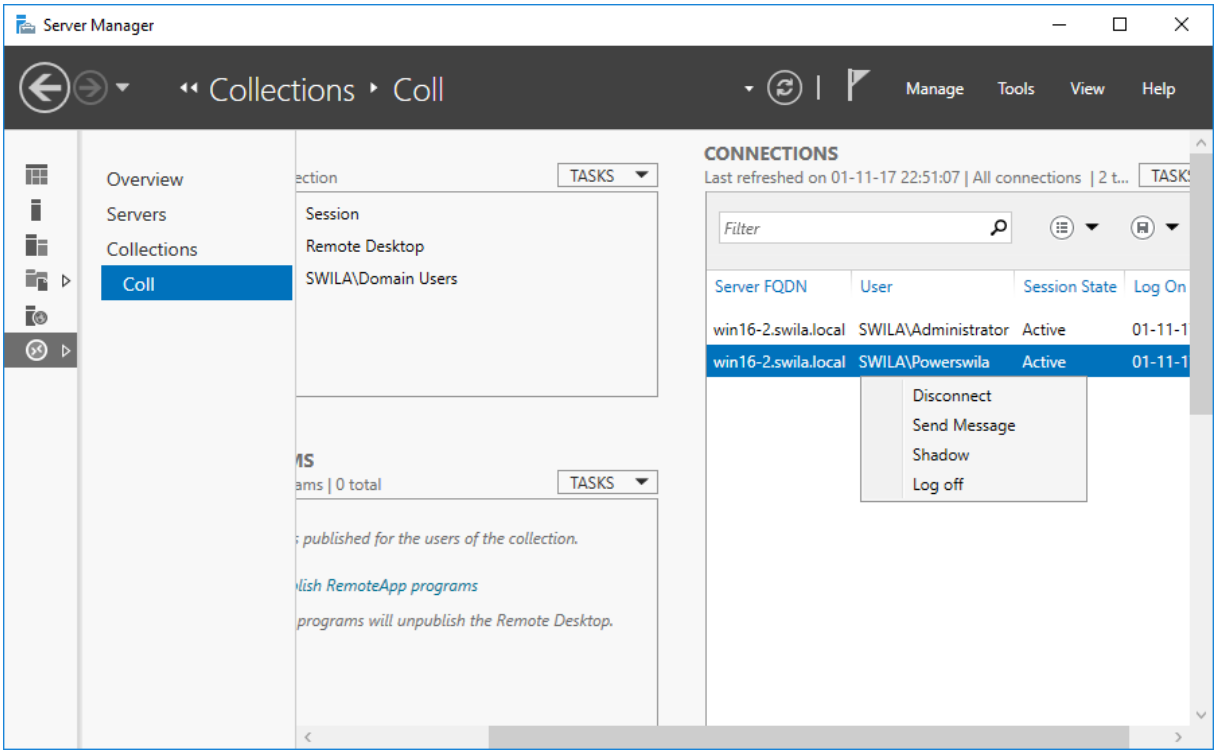

Figure 10.4 : Les sessions en cours sur le serveur RD

La figure 10.4 montre les sessions en cours sur le serveur : l'*administrator* est connecté en console et l'utilisateur *powerswila* est connecté par une connexion bureau à distance. Il faut remarquer l'état *active* mentionné.

En effectuant un **clic-droit** sur une session, on voit les quatre actions possibles :

1. Disconnect – qui permet de déconnecter l'utilisateur (la session devient Disconnected, les programmes démarrés restent actifs)
2. Send message – qui permet de faire apparaitre un message (pop-up) dans la session de l'utilisateur
3. Shadow – qui permet de voir la session utilisateur. Le consentement de l'utilisateur peut être nécessaire.
4. Log off – qui permet de clôturer la session (déconnexion et fermeture de tous les programmes démarrés).

Il faut remarquer que des options complémentaires sont possibles **par le Task Manager** *(ou gestionnaire des tâches)*. En effet, il est possible (par l'onglet *Users),* en choisissant l'option *Connect* (après un clic-droit) de récupérer la session de l'utilisateur (en fournissant son mot de passe). Il est possible aussi de **tuer un processus (par l'option *end task)*** lancé par l'utilisateur.

10.5 Configurer une RemoteApp

10.5.1 Les RemoteApp

Une *RemoteApp* ou application distante est une fonctionnalité du service bureau à distance permettant de lancer une application sur le serveur mais d'afficher l'application lancée sur le poste client. En fait, une session sera ouverte sur le serveur afin de lancer l'application mais cette session ne sera pas visible par l'utilisateur qui verrait uniquement l'application s'exécuter.

C'est une fonctionnalité intéressante pour lancer des applications s'exécutant à distance. Il faut cependant ne pas perdre de vue que l'application, s'exécutant sur un ordinateur distant, n'a pas nécessairement accès aux ressources locales (il convient de configurer ces ressources locales convenablement pour que l'utilisateur ne soit pas perdu).

En effet, un des grands dangers de l'utilisation des *RemoteApp* est que l'utilisateur ne perçoive pas nécessairement qu'il travaille depuis un serveur distant et que, par conséquent, l'accès à son environnement (dossiers, fichiers, imprimantes, mail, …) ne soit pas possible.

10.5.2 Configuration de l'application RemoteApp

La première étape est de procéder à l'installation de l'application sur le serveur exécutant le service RD. Pour installer l'application, comme nous l'avons vu précédemment (cf. 10.3.4), il faut basculer le serveur en mode *installation* afin de réaliser une installation propre.

Une fois l'installation de l'application achevée, il faut procéder à la configuration *RemoteApp* en allant dans **Server Manager > Remote Desktop Services > Collection > collection créée** et puis **RemoteApp Programs** (voir figure 10.5).

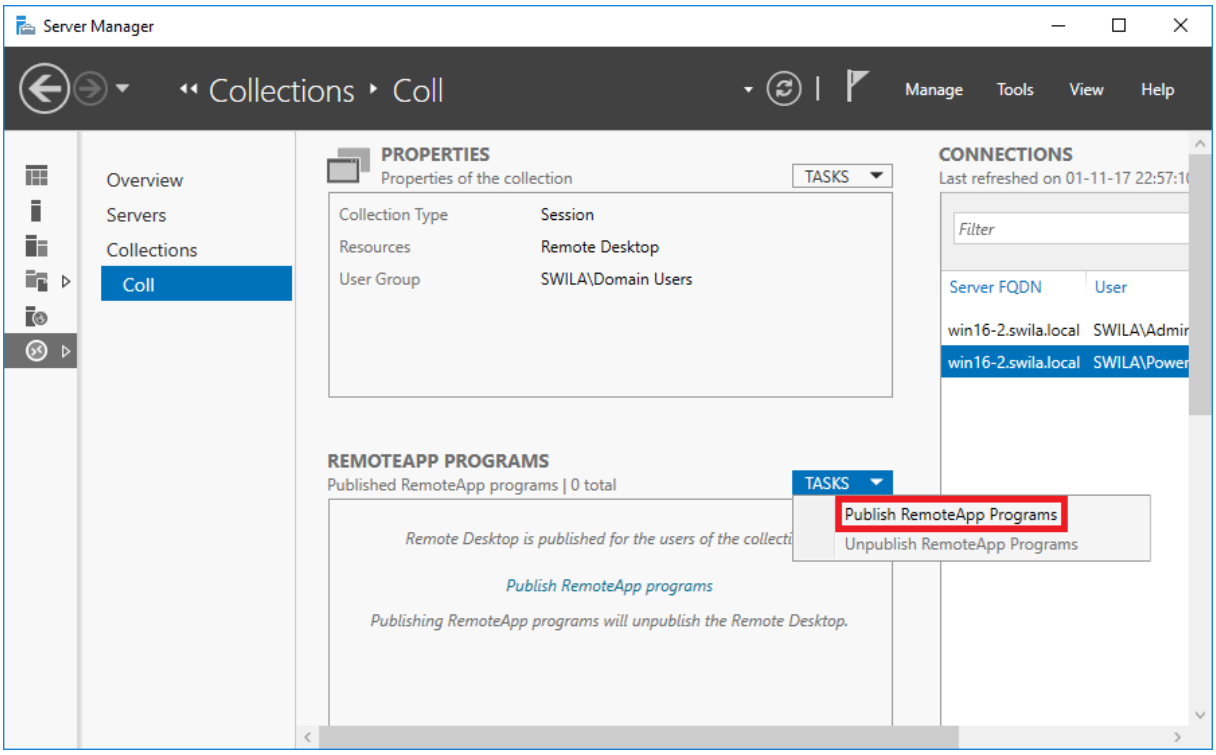

Figure 10.5 : Publication d'une RemoteApp

Pour ce faire, il faut choisir l'option *Publish RemoteApp programs* et sélectionner le programme souhaité dans la liste ou, s'il n'apparaît pas, via l'option *Add*. Une fois le programme ajouté, il est possible, en faisant un **clic-droit** sur celui-ci puis **Edit Properties**, d'interdire ou autoriser les paramètres en ligne de commande (option *Do not allow/Allow any command-line parameters)*, de modifier les utilisateurs qui peuvent exécuter l'application distante (*specify users and groups who should see this Remote App program*) ou encore d'associer des types de fichier avec l'application RemoteApp (*Select the file types to associate with this Remote App)*. Par défaut, tout utilisateur ayant le droit d'ouvrir une session sur le serveur peut exécuter l'application en mode *RemoteApp*.

Nous verrons dans la suite comment il est possible **d'obtenir le fichier .rdp permettant le lancement de l'application**.

10.5.3 Apparition des RemoteApp du côté client

Les *RemoteApp* apparaissent dans le *Menu Démarrer* dès que le client *s'y est abonné*. Cela peut se faire au moyen d'une GPO (uniquement pour les clients Windows 8 et supérieur) ou bien en configurant le flux dans l'outil adéquat.

Voici les étapes à suivre, **à partir du poste client** :

1. En *Administrator*, accepter le certificat créé pour la distribution des RemoteApp. Pour ce faire, il faut démarrer *Internet Explorer*[38] et entrer l'adresse suivante : `https://nomDNS.domaine` (exemple : `https://win16-2.swila.local`). Internet Explorer vous informe qu'il y a un problème de certificat. Il faut choisir l'option **Go to the webpage (not recommended)**.

[38] Pour démarrer Internet Explorer sous Windows 10, il faut rechercher `iexplore`

a. La barre d'adresse apparaît en rouge, avec la mention **Certificate Error**. Il faut cliquer sur cette erreur et **view certificates**[39].
b. Une fois que la fenêtre donnant les informations sur le certificat apparait, il faut choisir l'option **Install Certificate**.
c. L'assistant d'importation apparaît, il faut alors choisir **Local Machine** et puis **Place all certificates in the following store : Trusted Root Certification Authorities** et confirmer l'importation.
d. Quitter Internet Explorer et retourner sur la page, l'erreur de certificat doit avoir disparu.

2. Avec l'utilisateur souhaité, démarrer l'outil **RemoteApp and Desktop Connections**, qui est accessible dans **le control panel** (voir figure 10.6) :

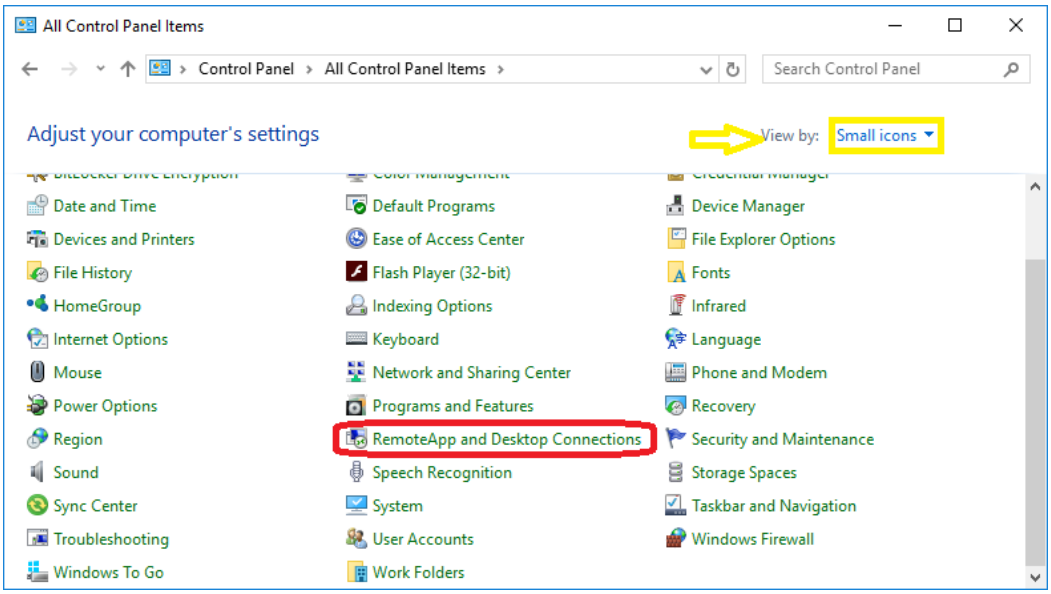

Figure 10.6 : RemoteApp and Desktop Connections

a. Dans le menu de droite, choisir **Access RemoteApp and Desktops**
b. Le système attend une URL de connexion. L'URL à fournir est de la forme : `https://nomDNS.domaine/RDWeb/Feed/webfeed.aspx` (le nom de votre serveur exécutant le service Bureau à Distance).
c. Si le système vous informe d'un problème de certificat, il convient de se reporter à l'étape 1 ci-dessus.
d. Une fois l'ajout terminé, un nouveau groupe *Work Ressources* apparaît dans le *Start Menu* du poste en question renseignant les applications RemoteApp publiées.
e. Pour **obtenir le RDP de l'application**, il faut retourner dans la fenêtre *RemoteApp and Desktop Connections* depuis le panneau de configuration et choisir **View ressources.** Faire ensuite un **clic-droit** sur l'application souhaitée (celle dont on veut obtenir le fichier **.rdp**) et choisir **Properties**. Le champ *Target* mentionne le chemin vers le fichier **.rdp** qui peut être ainsi récupéré pour être copié sur une autre machine.

10.6 Les GPO intéressantes pour les sessions RD

La première GPO intéressante est celle permettant de *Mentionner les utilisateurs qui peuvent se connecter en bureau à distance :* comme nous l'avons déjà mentionné, il est possible, par une stratégie,

[39] Cette possibilité n'est pas offerte dans Edge

de mentionner les groupes d'utilisateurs qui peuvent se connecter en mode bureau à distance. Il faut bien se rappeler que si une GPO définit cette propriété, cela écrase toute autre configuration. La GPO à configurer se trouve ici : **Computer Configuration\Policies\Windows Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services**.

Il y a un certain nombre de d'autres GPO utiles lorsqu'on active le service RD aussi bien en *Computer Configuration* (et donc applicable à la machine) qu'en *User Configuration* (applicable aux utilisateurs se connectant par le service RD).

On trouve parfois les mêmes éléments dans la *Computer Configuration* et dans la *User Configuration*. L'objectif est alors différent : faut-il autoriser la configuration pour l'utilisateur, quelque soit le serveur RD sur lequel il se connecte (=> user configuration) ou faut-il autoriser la configuration sur le ou les serveurs donnés, peu importe les utilisateurs qui se connecte (=> computer configuration).

Les stratégies applicables à la configuration ordinateur se trouvent dans **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services**.

Les stratégies applicables à la configuration utilisateur se trouvent dans **User Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services.**

Quelques stratégies intéressantes :

- *Restrict Remote Desktop Services users to a single Remote Desktop Sercvices Session :* Cette stratégie permet d'éviter qu'un utilisateur (avec son login) ne puisse ouvrir plus d'une session sur le serveur (et donc économie des licences) à la fois (*computer configuration*).
- *Session Time Limits* : il y a quelques stratégies importantes permettant de définir les délais d'expiration des sessions. Ces paramètres permettent d'éviter que des sessions ne restent ouvertes indéfiniment. Ces paramètres sont présents dans la computer configuration et user configuration. S'ils sont définis des deux côtés, la *computer* configuration est prioritaire.
- *Printer Redirection* : Ces stratégies mentionnent le comportement à adopter face aux imprimantes. En effet, les imprimantes de l'utilisateur qui se connecte sont par défaut émulées dans la session RD. Or, si de nombreux utilisateurs se connectent avec, pour chacun, toutes leurs imprimantes, le système peut vite saturer. Il est dès lors conseillé d'activer *Redirect only the default client printer* (uniquement l'imprimante par défaut de l'utilisateur). Ces paramètres sont présents dans la computer configuration et user configuration. S'ils sont définis des deux cotés, la computer configuration est prioritaire.
- *Device and Resource Redirection :* ces stratégies permettent de limiter les ressources et redirections réalisées entre le client et le serveur RD. Ces paramètres sont présents dans la computer configuration et user configuration. S'ils sont définis des deux cotés, la computer configuration est prioritaire.

10.7 Exercices

1. Installer le service Remote Desktop sur la machine *SRV2016-2* (cf. leçon 8, exercice 2).
    a. Autoriser les membres `elearning` et `travaux` à se connecter au serveur (via la collection de session)
    b. Tester la connexion depuis la machine VM Windows 10 (par exemple `eg0050`[40])
2. Modifier la stratégie `boucleRappel` (exercice 5d, leçon 8) :
    a. Empêcher toute redirection du presse-papier et n'autoriser que la redirection de l'imprimante par défaut
    b. N'autoriser qu'une session par utilisateur
    c. Définir les délais pour une session inoccupée à `5` minutes. Mentionner qu'une session déconnectée depuis `10` minutes doit être fermée.
    d. Autoriser le groupe `travaux` à ouvrir une session via le service Desktop Services
    e. Tester la connexion depuis la machine VM Windows 10 (pour `tx0050`[40] et `eg0050`).
3. Configurer une *RemoteApp*
    a. Installer, au préalable, le programme WinSCP sur le serveur *SRV2016-2* (cf. leçon 8, exercice 2)
    b. Configurer une *RemoteApp* pour permettre l'exécution de ce programme
    c. Tester la *RemoteApp* depuis votre machine VM Windows 10 avec un membre du groupe travaux (par exemple `tx0050`). Connectez-vous à *Dartagnan*[41] et copier le contenu de votre dossier `public_html` depuis votre espace vers le disque `C:`. Quitter la RemoteApp. Trouver les fichiers transférés.
    d. Obtenir le fichier `.rdp` permettant de démarrer la RemoteApp. Copier ce dernier sur le bureau de l'utilisateur.

[40] Pour rappel, tous les utilisateurs portant le numéro 50 ont comme mot de passe `P@ssw0rd`
[41] L'adresse IP de Dartagnan est `192.168.128.13`