Windows Server 2025 — Services Bureau à Distance (RDS) & RemoteApp

Guide complet pour l'installation et la configuration des Services Bureau à Distance (RDS) sur Windows Server 2025 avec publication d'applications via RemoteApp dans l'infrastructure NOUVY.LAN. Couvre l'architecture (RD Session Host, RD Connection Broker, RD Web Access, RD Licensing, RD Gateway), le déploiement Quick Start, la création des collections, la publication RemoteApp, la gestion des CAL, l'accès web HTTPS et la sécurisation.

50 min de lecture **Niveau Intermédiaire**

Document généré le 11/07/2026 à 20h42 · nouvy.fr/wiki/windows-server-2025-rds-remoteapp

Sommaire

70 section(s) · 50 min de lecture

Environnement du lab

Ce lab étend l'infrastructure **NOUVY.LAN** existante (Active Directory, DHCP, DNS opérationnels sur SRV-NOUVY) avec un nouveau serveur **SRV-RDS** dédié aux Services Bureau à Distance et à la publication RemoteApp.

Rôle	Nom machine	Adresse IP	Système
Contrôleur de domaine / DHCP / DNS	SRV-NOUVY	192.168.1.10	Windows Server 2025
Serveur RDS / RemoteApp	SRV-RDS	192.168.1.30	Windows Server 2025
Domaine	NOUVY.LAN	—	—
Postes clients	PC-XXXX	192.168.1.x (DHCP)	Windows 11 Pro/Education/Enterprise

> ***Prérequis** : SRV-RDS est un serveur **membre du domaine** NOUVY.LAN, à jour Windows Update, avec une adresse IP statique et un enregistrement DNS valide. Compte administrateur du domaine disponible.*

---

1. Introduction aux services Bureau à Distance

Qu'est-ce que RDS ?

Les **Services Bureau à Distance** (*Remote Desktop Services*, abrégé **RDS**) sont une plateforme Windows Server permettant de centraliser l'exécution d'applications et de bureaux sur un ou plusieurs serveurs. Les utilisateurs accèdent à ces ressources depuis un client léger (PC, tablette, smartphone) via le protocole **RDP** (*Remote Desktop Protocol*).

L'utilisateur voit s'afficher sur son poste local soit :

- un **bureau Windows complet** (session Windows hébergée sur le serveur)
- soit une **application unique** (RemoteApp) qui s'exécute sur le serveur mais qui s'affiche comme une fenêtre native sur le poste client

Cas d'usage typiques

Cas d'usage	Bénéfice RDS
Centralisation d'un logiciel métier (ERP, compta, CAO)	Une seule installation à maintenir, données restent sur le serveur
Télétravail / accès distant sécurisé	Aucune donnée ne quitte l'entreprise, accès via HTTPS
Postes peu puissants ou hétérogènes	Le calcul se fait sur le serveur, le client n'a qu'à afficher
Standardisation d'environnement	Tous les utilisateurs ont la même version du logiciel
Continuité d'activité	Si un poste tombe, l'utilisateur se reconnecte ailleurs et retrouve sa session

RDS vs solutions concurrentes

Solution	Type	Hébergement	Public
RDS (Microsoft)	Sessions Windows Server partagées	On-premise / cloud	PME et grandes entreprises Microsoft
Citrix Virtual Apps	Sessions + VDI avancé	On-premise / cloud	Grandes entreprises, fonctionnalités étendues
VMware Horizon	VDI + RDS	On-premise / cloud	Environnements VMware
Azure Virtual Desktop	RDS + W10/W11 multi-sessions	Cloud Azure uniquement	Cloud-first, hybrides
Windows 365	Cloud PC dédié	Cloud Azure	1 utilisateur = 1 PC virtuel persistant

> ***Note** : RDS reste la solution standard et économique pour publier des applications Windows en interne. Pour NOUVY.LAN, RDS sur Windows Server 2025 est largement suffisant.*

---

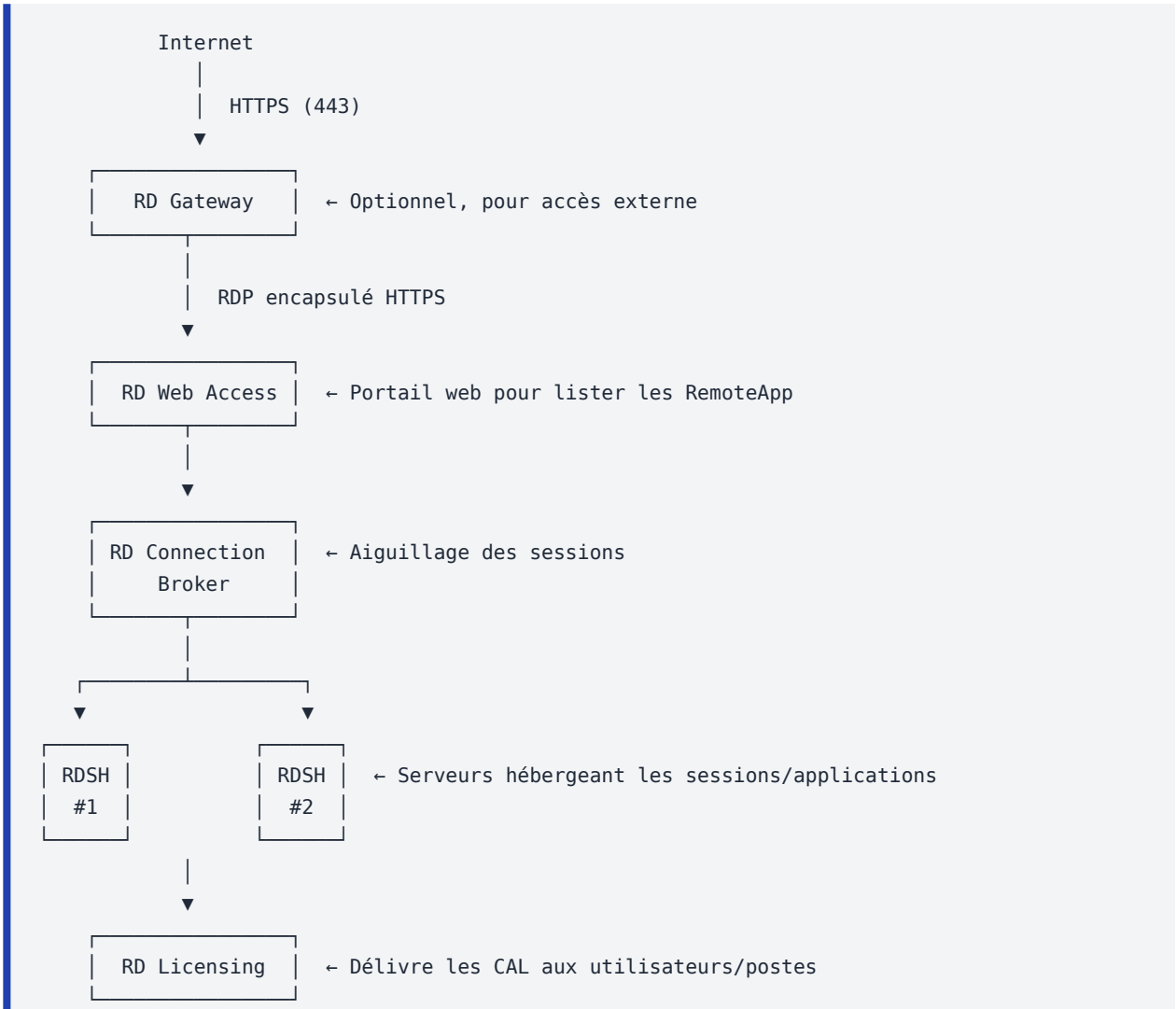
2. Architecture des services RDS

Le rôle **Services Bureau à Distance** se décompose en **6 sous-rôles** distincts. Sur un petit déploiement (lab, PME), tous peuvent cohabiter sur un seul serveur. Sur des déploiements plus larges, ils sont répartis sur plusieurs machines pour la haute disponibilité.

Les 6 rôles RDS

Rôle	Acronyme	Fonction
Hôte de session Bureau à distance	**RDSH** (RD Session Host)	Héberge les sessions utilisateurs et exécute les applications RemoteApp
Service Broker des connexions Bureau à distance	**RDCB** (RD Connection Broker)	Distribue les connexions entrantes vers les RDSH disponibles, gère les reconnexions
Accès Web des services Bureau à distance	**RDWA** (RD Web Access)	Portail web HTTPS où les utilisateurs voient leurs applications publiées
Passerelle des services Bureau à distance	**RDG** (RD Gateway)	Permet l'accès depuis Internet via HTTPS (port 443) sans VPN
Gestionnaire de licences des services Bureau à distance	**RDL** (RD Licensing)	Gère l'attribution des CAL RDS aux utilisateurs ou postes
Hôte de virtualisation des services Bureau à distance	**RDVH** (RD Virtualization Host)	Pour le **VDI** (machines virtuelles individuelles via Hyper-V) — non utilisé dans ce lab

Schéma logique d'un déploiement RDS



Copier

Déploiement Quick Start vs Standard

Type	Description	Quand l'utiliser
Démarrage rapide (Quick Start)	Installe RDSH + RDCB + RDWA sur un seul serveur, avec une collection de démo	Lab, PME, démo, mono-serveur
Déploiement standard	Installe les rôles séparément sur plusieurs serveurs spécifiés	Production, haute disponibilité, architecture multi-serveurs

> ***Choix pour NOUVY.LAN*** *: nous utiliserons le* ***déploiement standard*** *mais en regroupant tous les rôles sur SRV-RDS. C'est la méthode recommandée car elle laisse la flexibilité d'ajouter d'autres serveurs RDSH plus tard.*

---

3. Le concept RemoteApp

Qu'est-ce qu'une RemoteApp ?

RemoteApp est une fonctionnalité de RDS qui permet de publier **une application** (et non un bureau complet). Côté utilisateur, l'application s'affiche dans une fenêtre Windows classique sur son poste local, comme si elle était installée localement.

En réalité, l'application s'exécute sur le serveur RDSH, et seules les images de l'écran (transférées en RDP) sont affichées sur le poste client. Le clavier, la souris, le presse-papiers et les imprimantes sont relayés entre le client et le serveur.

Bureau complet vs RemoteApp

Critère	Bureau complet	RemoteApp
Ce que voit l'utilisateur	Tout un bureau Windows	Une seule fenêtre application
Expérience	Comme un PC distant	Comme une application locale
Cas d'usage	Télétravail générique	Publication d'un logiciel métier ciblé
Lancement	Icône bureau distant	Icône .rdp ou via RD Web Access
Multi-fenêtres	Toutes dans le bureau distant	Chaque appli dans sa fenêtre locale

Avantages de RemoteApp

- **Transparence** : l'application apparait dans la barre des tâches comme une appli locale (ALT+TAB la liste)
- **Simplicité côté utilisateur** : pas de bureau distant à gérer
- **Centralisation** : une seule installation côté serveur, toutes les MAJ se font à un endroit
- **Sécurité** : les données restent sur le serveur, jamais sur le poste client
- **Compatibilité** : permet de faire tourner des applis Windows sur Mac, Linux, iOS, Android via le client RD

Limites

- L'application doit être compatible **multi-utilisateurs** (la plupart des applis Win32 le sont, certaines applis grand public ne le sont pas)
- Performance dépendante du réseau (ping, bande passante)
- **Licences RDS CAL** obligatoires en environnement de production (au-delà de 120 jours d'essai)
- Certaines API graphiques (DirectX 12, jeux) ne sont pas adaptées

---

4. Prérequis pour l'installation

Prérequis infrastructure

Prérequis	Statut	Remarque
Active Directory DS	Operationnel	Domaine NOUVY.LAN sur SRV-NOUVY
DNS	Operationnel	Sur SRV-NOUVY, doit résoudre srv-rds.nouvy.lan
SRV-RDS membre du domaine	A vérifier	Doit être joint à NOUVY.LAN
IP statique sur SRV-RDS	A configurer	192.168.1.30 dans ce lab
Compte admin de domaine	Disponible	Nécessaire pour le déploiement

Vérifications préalables sur SRV-RDS

Ouvrir PowerShell en administrateur sur SRV-RDS :

```
# Vérifier le nom de la machine et l'appartenance au domaine
hostname
(Get-WmiObject Win32_ComputerSystem).Domain

# Vérifier l'adresse IP
Get-NetIPAddress -AddressFamily IPv4 | Where-Object { $_.IPAddress -notlike "127.*" }

# Vérifier la résolution DNS du DC
Resolve-DnsName srv-nouvy.nouvy.lan

# Vérifier l'heure (importante pour Kerberos)
w32tm /query /status
```

Copier

Création des groupes AD

Sur SRV-NOUVY, ouvrir **Utilisateurs et ordinateurs Active Directory** (`dsa.msc`) et créer les groupes suivants dans une OU dédiée (par exemple `OU=Groupes RDS,DC=nouvy,DC=lan`) :

Groupe AD	Membres	Utilité
`GRP_RDS_Users`	Utilisateurs autorisés à se connecter aux RemoteApp	Filtre d'accès aux collections
`GRP_RDS_Admins`	Administrateurs RDS	Gestion du serveur RDS
`GRP_RemoteApp_Compta`	Utilisateurs du logiciel comptable	Publication ciblée
`GRP_RemoteApp_RH`	Utilisateurs RH	Publication ciblée

> ***Convention NOUVY** : préfixe `GRP_` pour tous les groupes AD (cohérent avec `GRP_Direction`, `GRP_Compta`, etc. déjà existants). Ces groupes contiendront les utilisateurs et seront référencés dans les collections RDS.*

---

5. Installation du rôle RDS sur SRV-RDS

Étape 1 — Lancer l'assistant de déploiement

1. Sur SRV-RDS, ouvrir **Server Manager** → **Gérer** → **Ajouter des rôles et fonctionnalités**
2. Page **Type d'installation** : sélectionner **"Installation des services Bureau à distance"** *(et non "Installation basée sur un rôle ou une fonctionnalité")*
3. Page **Type de déploiement** : choisir **"Déploiement standard"** *(plus flexible que le démarrage rapide)*
4. Page **Scénario de déploiement** : choisir **"Déploiement de bureau basé sur une session"** *(et non "Déploiement de bureau basé sur une machine virtuelle" qui correspond au VDI)*

Étape 2 — Sélection des serveurs pour chaque rôle

L'assistant demande de choisir les serveurs cibles pour les 3 rôles principaux :

Rôle	Serveur
Serveur Broker des connexions Bureau à distance	SRV-RDS.nouvy.lan
Serveur d'accès Web des services Bureau à distance	SRV-RDS.nouvy.lan
Serveur hôte de session Bureau à distance	SRV-RDS.nouvy.lan

Pour chaque écran, sélectionner SRV-RDS dans la liste et cliquer sur la flèche pour l'ajouter au panneau de droite.

Étape 3 — Confirmation et installation

1. Cocher **"Redémarrer le serveur de destination automatiquement si nécessaire"**
2. Cliquer **Déployer**
3. L'assistant installe successivement les 3 rôles, redémarre SRV-RDS automatiquement, et reprend le déploiement après le reboot
4. Durée totale : environ 10 à 15 minutes

Étape 4 — Vérification dans Server Manager

Après le redémarrage, ouvrir **Server Manager** → menu de gauche → **Services Bureau à distance**.

La **Vue d'ensemble du déploiement** affiche un schéma des rôles installés :

```
[RD Connection Broker] ——— [RD Web Access] ——— [RD Session Host]
        SRV-RDS                 SRV-RDS               SRV-RDS
```

Copier

Trois rôles supplémentaires apparaissent en grisé (non installés) :

- **RD Gateway** (à installer plus tard pour l'accès externe)
- **RD Licensing** (à installer pour activer les CAL)
- **RD Virtualization Host** (uniquement pour le VDI)

Étape 5 — Premier test rapide

À ce stade, le déploiement est fonctionnel mais sans collection. Tester la connexion RDP classique pour valider que SRV-RDS répond :

```
# Depuis un poste client
mstsc /v:srv-rds.nouvy.lan
```

Copier

Se connecter avec un compte du domaine membre du groupe `Administrateurs du domaine` (les utilisateurs standard ne pourront pas se connecter tant qu'aucune collection n'est créée).

---

6. Création et configuration d'une collection de sessions

Une **collection** regroupe un ou plusieurs serveurs RDSH ayant la même configuration, et publie des ressources (bureaux ou RemoteApp) à un ensemble d'utilisateurs.

Étape 1 — Créer la collection

1. Server Manager → **Services Bureau à distance** → **Collections**
2. Menu **Tâches** → **Créer une collection de sessions**
3. **Nom** : `Collection-Apps-NOUVY` *(nom interne, visible des admins)*
4. **Description** : `Applications publiées NOUVY.LAN`
5. **Hôtes de session** : ajouter SRV-RDS
6. **Groupes d'utilisateurs** : ajouter `NOUVY\GRP_RDS_Users` (au lieu du groupe par défaut `Domain Users`)
7. **Profils d'utilisateurs (UPD)** : décocher pour ce premier test (à activer en production — voir section dédiée)
8. Confirmer → **Créer**

Étape 2 — Examiner les propriétés de la collection

Cliquer sur la collection nouvellement créée → onglet **Propriétés** → **Tâches** → **Modifier les propriétés**.

Onglet Général

- Nom et description (modifiables à tout moment)

Onglet Connexions utilisateur

- **Nombre maximum de connexions actives** par utilisateur (illimité par défaut)
- **Action lors de la déconnexion** : fermer la session après X minutes d'inactivité

Onglet Paramètres de session

- **Durée maximale d'une session active** (illimitée par défaut)
- **Délai d'expiration d'une session inactive** (recommandé : 4h)
- **Délai d'expiration d'une session déconnectée** (recommandé : 1h)
- **Action en fin de délai** : déconnecter ou fermer la session

Onglet Sécurité

- **Couche de sécurité** : **TLS 1.2/1.3** (par défaut sous Windows Server 2025)
- **Niveau de chiffrement** : **Élevé** ou **Compatible FIPS**
- **Authentification au niveau réseau (NLA)** : ☑ activée (recommandé)

Onglet Équilibrage de charge

- Pertinent si plusieurs RDSH dans la collection (poids relatif de chaque serveur)

Onglet Configuration du client

- **Redirection des ressources locales** : imprimantes, presse-papiers, lecteurs, ports
- **Redirection audio** : depuis le serveur vers le client
- **Activer Smart Card** si authentification carte à puce

Onglet Groupes d'utilisateurs

- Liste des groupes AD autorisés (modifiables à tout moment)

Onglet Disques de profil utilisateur (UPD)

- Voir section dédiée ci-dessous

Étape 3 — Configurer les disques de profil utilisateur (UPD)

Les **User Profile Disks** stockent le profil de chaque utilisateur (documents, paramètres, AppData) dans un fichier VHDX dédié sur un partage réseau. Cela évite les profils itinérants classiques (lents et fragiles) et garantit une expérience cohérente entre serveurs RDSH.

Préparer le partage UPD sur SRV-NOUVY

1. Sur SRV-NOUVY, créer un dossier `D:\UPD-NOUVY`
2. Partager ce dossier avec :
    - **Nom du partage** : `UPD-NOUVY$` (le `$` rend le partage caché)
    - **Permissions partage** : `NOUVY\Ordinateurs du domaine` → Contrôle total *(les serveurs RDSH doivent pouvoir écrire)*
    - **Permissions NTFS** : `NOUVY\Ordinateurs du domaine` → Contrôle total + `NOUVY\Administrateurs du domaine` → Contrôle total

Activer UPD dans la collection

1. Properties de la collection → onglet **Disques de profil utilisateur**
2. Cocher **"Activer les disques de profil utilisateur"**
3. **Emplacement** : `\\srv-nouvy.nouvy.lan\UPD-NOUVY$`
4. **Taille maximum** : 20 Go (ajustable selon usage)
5. Choisir entre :
    - **Stocker tous les paramètres et données du profil** (recommandé)

- **Exclure des dossiers spécifiques** (si certains dossiers volumineux ne doivent pas être inclus)

> ***Comportement** : à la première connexion d'un utilisateur, un fichier `UVHD-{SID}.vhdx` est créé dans le partage. Ce VHDX est monté dynamiquement à chaque session de l'utilisateur.*

---

7. Publication d'applications RemoteApp

C'est ici que la magie opère : on publie des applications individuelles plutôt qu'un bureau entier.

Prérequis : installer les applications sur SRV-RDS

Avant de pouvoir les publier, les applications doivent être **installées sur le serveur RDSH** (ici SRV-RDS), en mode RDS.

Mode installation RDS

Deux méthodes pour installer une application en mode RDS :

Méthode 1 — via Panneau de configuration

1. Panneau de configuration → **Programmes** → **Installer une application sur un serveur Bureau à distance**
2. Lancer le programme d'installation
3. Le serveur passe automatiquement en mode installation puis revient en mode exécution

Méthode 2 — via PowerShell (recommandée)

```
# Activer le mode installation
Change user /install

# Installer l'application (ex : msiexec /i ".\monlogiciel.msi" /qb)
msiexec /i "C:\Sources\notepadplusplus.msi" /qb

# Repasser en mode exécution
Change user /execute

# Vérifier l'état actuel
Change user /query
```

Copier

> ***Pourquoi ce mode ?** En mode installation, Windows redirige les écritures de la base de registre vers `HKLM` au lieu de `HKCU`, ce qui rend l'application visible et utilisable par tous les utilisateurs RDS.*

Étape 1 — Publier une RemoteApp

1. Server Manager → **Services Bureau à distance** → **Collections** → cliquer sur

`Collection-Apps-NOUVY`

2. Section **Programmes RemoteApp → Tâches → Publier des programmes RemoteApp**
3. L'assistant scanne `C:\Program Files` et `C:\Program Files (x86)` à la recherche d'applications publiables
4. Cocher les applications souhaitées (ex : `Notepad++`, `Calculatrice`, `WordPad`)
5. Si une application n'apparait pas dans la liste : cliquer **Ajouter** et naviguer manuellement vers son `.exe`
6. Confirmer → **Publier**

Étape 2 — Configurer chaque RemoteApp publiée

Cliquer sur une application publiée → **Tâches** → **Modifier les propriétés**.

Onglet Général

- **Nom du programme RemoteApp** : nom affiché dans RD Web Access (ex : `Notepad++`)
- **Alias** : identifiant unique (utilisé dans le fichier .rdp)
- **Afficher dans le RD Web Access** : ☑ par défaut

Onglet Paramètres

- **Paramètres de ligne de commande** :
  - **Ne pas autoriser** (par défaut, sécurisé)
  - **Autoriser** (l'utilisateur peut passer des arguments)
  - **Toujours utiliser les paramètres suivants** (forcer des paramètres fixes)
- **Icône** : modifiable

Onglet Affectations utilisateur

- **Tous les utilisateurs ayant accès à cette collection** (par défaut)
- **Utilisateurs ou groupes spécifiques** : pour publier l'application à un sous-ensemble (ex : `GRP_RemoteApp_Compta` uniquement pour Sage)

Onglet Associations de types de fichiers

- Permet d'associer une extension (ex: `.txt`) à la RemoteApp côté client : un double-clic sur un fichier `.txt` local lancera Notepad++ sur le serveur

Étape 3 — Vérifier la publication

Les applications publiées apparaissent dans Server Manager → Collections → Programmes RemoteApp.

Sur le serveur, le dossier `C:\Windows\RemoteApps` (et plus précisément la base WMI) stocke les définitions des RemoteApp publiées. La gestion via PowerShell utilise les commandes suivantes :

```
# Lister les RemoteApp publiées dans la collection
Get-RDRemoteApp -CollectionName "Collection-Apps-NOUVY"

# Publier une RemoteApp via PowerShell
New-RDRemoteApp -CollectionName "Collection-Apps-NOUVY" `
                -DisplayName "WordPad" `
                -FilePath "C:\Program Files\Windows NT\Accessories\wordpad.exe"

# Restreindre une RemoteApp à un groupe spécifique
Set-RDRemoteApp -CollectionName "Collection-Apps-NOUVY" `
                -Alias "wordpad" `
                -UserGroups "NOUVY\GRP_RemoteApp_RH"

# Dépublier une RemoteApp
Remove-RDRemoteApp -CollectionName "Collection-Apps-NOUVY" -Alias "wordpad"
```

Copier

Déploiement automatique des RemoteApp aux postes clients via GPO

Plutôt que de demander aux utilisateurs d'ouvrir le portail RD Web Access et de télécharger manuellement les fichiers `.rdp`, on peut **pousser automatiquement les RemoteApp dans le menu Démarrer** des postes clients via une GPO. Le poste se souscrit au **Feed RemoteApp** publié par SRV-RDS et récupère toutes les applications auxquelles l'utilisateur a droit.

Résultat côté client : un dossier **NOUVY** apparaît dans le menu Démarrer, contenant les raccourcis vers chaque RemoteApp publiée. Un clic = lancement de l'application sans aucune interaction supplémentaire.

> ***Prérequis** : la console **Gestion des stratégies de groupe** (`gpmc.msc`) doit être disponible sur le DC. Sur Windows Server 2025, elle est installée par défaut.*

Étape 1 — Créer la GPO

Sur SRV-NOUVY (le DC) :

1. Touche `Windows` → taper **"Gestion des stratégies de groupe"** → ouvrir
2. Arborescence : **Forêt** → **Domaines** → **NOUVY.LAN**
3. Trouver l'**OU contenant les utilisateurs cibles** (ex. `OU=Utilisateurs NOUVY`)
4. Clic droit sur cette OU → **Créer un objet GPO dans ce domaine, et le lier ici...**
5. **Nom** : `RDS - Souscription RemoteApp NOUVY` → **OK**
6. Clic droit sur la GPO créée → **Modifier...**

Étape 2 — Configurer la souscription au Feed (Configuration utilisateur)

Dans l'éditeur GPO, naviguer jusqu'à :

```
Configuration utilisateur
  → Stratégies
    → Modèles d'administration
      → Composants Windows
        → Services Bureau à distance
          → Connexions RemoteApp et Bureau à distance
```

Copier

Double-cliquer sur le paramètre **"Spécifier l'URL des paramètres de connexion par défaut"** :

- Sélectionner **Activé**
- Dans le champ **URL** :

  ```
  https://SRV-RDS.NOUVY.LAN/RDWeb/Feed/webfeed.aspx
  ```

  Copier

- **OK**

Étape 3 — Renommer le workspace côté serveur

Cette étape détermine le **nom du dossier** créé dans le menu Démarrer du client. Par défaut, le dossier s'appellera "RemoteApp et Bureau à distance" — pour qu'il s'appelle **NOUVY**, il faut renommer le workspace côté serveur.

Sur SRV-RDS, ouvrir PowerShell admin :

```
Set-RDWorkspace -Name "NOUVY" -ConnectionBroker "SRV-RDS.NOUVY.LAN"
```

Copier

Vérification :

```
Get-RDWorkspace -ConnectionBroker "SRV-RDS.NOUVY.LAN"
```

Copier

La sortie doit indiquer `Name : NOUVY`.

> ***Sans cette étape**, le dossier dans le menu Démarrer côté client s'appellera "Workspaces" ou "RemoteApp et Bureau à distance", pas NOUVY.*

Étape 4 — Distribuer le certificat auto-signé aux clients

C'est l'étape qu'on oublie systématiquement et qui fait planter la souscription : le poste client doit faire confiance au certificat de SRV-RDS, sinon le feed est rejeté avant même de pouvoir être consulté.

Sur SRV-RDS — exporter le certificat :

1. Touche `Windows` → taper `certlm.msc` → ouvrir
2. Déplier **Personnel** → **Certificats**
3. Trouver le certificat utilisé pour RDWeb (celui lié au binding HTTPS dans IIS)

4. Clic droit → **Toutes les tâches** → **Exporter**
5. Suivant → **"Non, ne pas exporter la clé privée"** → Suivant
6. **Format** : *DER binaire encodé X.509 (.CER)* → Suivant
7. **Nom du fichier** : `C:\Temp\rdweb-srv-rds.cer` → Suivant → Terminer

Copier ce fichier `.cer` sur le DC (partage, clé USB, ou copie réseau).

Dans la GPO (la même que celle créée à l'étape 1) — ajouter la partie ordinateur :

Dans l'éditeur GPO, naviguer jusqu'à :

```
Configuration ordinateur
  → Stratégies
    → Paramètres Windows
      → Paramètres de sécurité
        → Stratégies de clé publique
          → Autorités de certification racines de confiance
```

Copier

Clic droit sur **Autorités de certification racines de confiance** → **Importer...** :

1. Suivant → **Parcourir** → choisir `rdweb-srv-rds.cer` → Suivant
2. **Magasin** : *Autorités de certification racines de confiance* (déjà sélectionné par défaut)
3. Suivant → Terminer

> ***Important** : la GPO contient maintenant des paramètres **Configuration utilisateur** ET **Configuration ordinateur**. Elle doit donc être liée à une OU qui couvre **à la fois** les utilisateurs et les ordinateurs ciblés. Le plus simple : la lier à la **racine du domaine NOUVY.LAN** ou à une OU parente contenant les deux types d'objets. Si le lab a des OU séparées (ex. `OU=Users` et `OU=Computers`), lier la GPO aux deux, ou la lier à la racine `NOUVY.LAN`.*

Étape 5 — Test côté client

Sur un poste Windows membre du domaine NOUVY :

1. Connexion avec un compte AD membre de `GRP_RDS_Users`
2. Ouvrir **cmd** ou **PowerShell** :

   ```
   gpupdate /force
   ```

   Copier

3. **Déconnexion / reconnexion** *(important : la souscription se déclenche à l'ouverture de session, pas avec un simple gpupdate)*

À la prochaine ouverture de session :

- La GPO pousse l'URL du feed
- Le poste client se souscrit automatiquement
- Le certificat est dans le magasin de confiance → pas d'erreur SSL
- Dans le **menu Démarrer** → un dossier **NOUVY** apparaît avec les RemoteApp publiées

Étape 6 — Vérification du résultat

Sur le poste client, après reconnexion :

1. Touche `Windows` → taper **RemoteApp** → ouvrir **"Connexions aux programmes RemoteApp et bureau à distance"**
2. Une connexion active nommée **NOUVY** doit apparaître avec :
    - **Statut** : Connecté
    - **URL** : `https://SRV-RDS.NOUVY.LAN/RDWeb/Feed/webfeed.aspx`
    - **Dernière mise à jour** : récente

Si la connexion n'apparaît pas :

- Vérifier que `gpresult /r` (sur le poste) liste bien la GPO `RDS - Souscription RemoteApp NOUVY`
- Vérifier que le compte utilisateur est membre du groupe AD autorisé sur la collection
- Tester l'URL `https://SRV-RDS.NOUVY.LAN/RDWeb/Feed/webfeed.aspx` dans Edge en tant qu'utilisateur — un fichier XML doit être renvoyé

> ***Bonus** : pour pousser un fichier `.rdp` brut sur le bureau de l'utilisateur (sans passer par le feed), utiliser une **GPO Préférences** → `Configuration utilisateur` → `Préférences` → `Paramètres Windows` → `Fichiers` → copier le `.rdp` exporté depuis Server Manager (cf. section 12) vers `%USERPROFILE%\Desktop`.*

---

8. Accès via RD Web Access

Le portail **RD Web Access** est l'interface web HTTPS où les utilisateurs voient toutes les RemoteApp auxquelles ils ont droit. C'est le point d'entrée principal pour les utilisateurs.

URL d'accès

Par défaut, le portail est accessible à l'URL :

```
https://srv-rds.nouvy.lan/RDWeb
```

Copier

> ***Note** : l'URL `https://srv-rds.nouvy.lan/RDWeb` redirige automatiquement vers `https://srv-rds.nouvy.lan/RDWeb/Pages/fr-FR/login.aspx`.*

Premier accès — avertissement de certificat

Au premier accès, le navigateur affiche un **avertissement de certificat** car SRV-RDS a généré un **certificat auto-signé** lors du déploiement. Ce certificat n'est pas approuvé par les postes clients.

Solutions :

1. **Ignorer l'avertissement** (acceptable en lab uniquement)
2. **Distribuer le certificat auto-signé via GPO** dans le magasin "Autorités de certification racines de confiance" des postes clients
3. **Remplacer par un vrai certificat** (recommandé en production — voir section sécurisation)

Générer un certificat auto-signé avec SAN avant le premier accès web

Pour éviter l'avertissement répété (et surtout pour qu'Edge/Chrome ne refusent pas la connexion à cause d'un SAN manquant), il est recommandé de **générer un certificat auto-signé avec Subject Alternative Names** couvrant à la fois le nom court et le FQDN du serveur RDS, puis de le **lier à HTTPS dans IIS** avant la première connexion.

1. Générer le certificat (PowerShell admin sur le serveur RDS)

```
New-SelfSignedCertificate `
    -DnsName "SRV-RDS02", "SRV-RDS02.NOUVY.LAN" `
    -CertStoreLocation "Cert:\LocalMachine\My" `
    -FriendlyName "RDWeb-SRV-RDS02-SAN" `
    -NotAfter (Get-Date).AddYears(2)
```

Copier

> ***À retenir** : note bien le **Thumbprint** affiché en sortie — il sera utile pour identifier le certificat dans la console IIS et lors du remplacement des certificats RDS dans la console de déploiement.*

2. Lier le certificat au site IIS hébergeant RDWeb

1. Ouvrir **Gestionnaire des services Internet (IIS)** → `inetmgr.exe`
2. Dans l'arborescence : **Sites** → clic droit sur **Default Web Site** → **Modifier les liaisons** *(Edit Bindings)*
3. Sélectionner la ligne **https**, port **443** → **Modifier**
4. Dans le champ **Certificat SSL**, sélectionner `RDWeb-SRV-RDS02-SAN` dans la liste déroulante
5. **OK** → **Fermer**

3. Tester l'accès web

Ouvrir un navigateur et accéder à `https://srv-rds02.nouvy.lan/RDWeb`. L'avertissement initial peut subsister tant que le certificat n'est pas approuvé sur le poste client (point 2 ci-dessus), mais le SAN garantit que les navigateurs modernes acceptent l'alternative `srv-rds02` ↔ `srv-rds02.nouvy.lan` sans erreur de "nom invalide".

> ***Bonne pratique** : ce certificat auto-signé reste réservé aux environnements internes / labs. En production, le remplacer par un certificat émis par l'AD CS interne (cf. section 11) ou par un certificat public (Let's Encrypt, DigiCert) pour les accès externes via RD Gateway.*

Authentification et page d'accueil

1. L'utilisateur saisit son login `nouvy\prenom.nom` et son mot de passe
2. Une fois authentifié, la page **Accès Web RemoteApp et Bureau à distance**

affiche les **icônes des applications** publiées auxquelles il a droit

3. Un clic sur une icône télécharge un fichier `.rdp` qui, à l'ouverture, lance la RemoteApp
4. Lors du premier lancement, le client RDP demande une nouvelle authentification → l'application s'ouvre dans une fenêtre native

Personnalisation du portail

Le portail RD Web Access est entièrement personnalisable (logo, couleurs, message d'accueil). Les fichiers se trouvent dans :

```
C:\Windows\Web\RDWeb\Pages\
```

Copier

Fichiers à modifier :

Fichier	Rôle
`images\logo_02.png`	Logo affiché en haut à gauche
`Site.xsl`	Contenu HTML/XSLT global
`Default.aspx`	Page d'accueil
`fr-FR\RDWAStrings.xml`	Textes affichés en français

> ***Bonne pratique** : sauvegarder les fichiers originaux avant toute modification, et documenter les changements car ils peuvent être écrasés par certaines mises à jour Windows.*

---

9. Gestion des licences (RD Licensing)

Période de grâce

Au démarrage, RDS fournit une **période de grâce de 120 jours** pendant laquelle aucune licence n'est requise. Passé ce délai, **les connexions sont refusées** si aucun serveur de licences n'est configuré.

Vérifier le nombre de jours restants :

```
# Sur SRV-RDS
wmic /namespace:\\root\CIMV2\TerminalServices PATH Win32_TerminalServiceSetting WHERE
(__CLASS !="") CALL GetGracePeriodDays
```

Copier

Types de CAL (Client Access License)

Type	Caractéristique	Quand l'utiliser
Per User (par utilisateur)	Licence attachée à un compte AD, utilisable depuis n'importe quel poste	Utilisateurs nomades, télétravail
Per Device (par périphérique)	Licence attachée à un poste, utilisable par n'importe quel utilisateur	Postes partagés (atelier, kiosque, 3x8)

> ***Choix recommandé pour NOUVY.LAN** : **Per User** dans la majorité des cas, car les utilisateurs peuvent se connecter depuis plusieurs postes (PC fixe, portable, télétravail, mobile).*

Étape 1 — Installer le rôle RD Licensing

1. Server Manager → **Services Bureau à distance** → vue d'ensemble du déploiement
2. Cliquer sur l'icône **RD Licensing** (en grisé)
3. Sélectionner **SRV-RDS** comme serveur de licences
4. Confirmer → l'installation prend ~2 minutes (sans redémarrage)

Étape 2 — Activer le serveur de licences

1. Outils → **Terminal Services** → **Gestionnaire de licences des services Bureau à distance** (`licmgr.exe`)
2. Clic droit sur SRV-RDS → **Activer le serveur**
3. Méthode de connexion :
    - **Connexion automatique** (HTTPS vers Microsoft) — recommandé si SRV-RDS a accès à Internet
    - **Web Browser** (si pas d'accès direct, copier-coller un code sur https://activate.microsoft.com)
    - **Téléphone** (dernier recours)
4. Renseigner le **nom**, **société**, **pays**
5. Coordonnées de l'entreprise (optionnel)
6. À la fin de l'activation, cocher **"Démarrer l'Assistant Installation des licences"**

Étape 3 — Installer les CAL achetées

1. Programme de licences :
    - **Open License** (entreprise)
    - **Select Plus / Open Value** (entreprise)
    - **Enterprise Agreement** (grands comptes)
    - **Détail** (achat unitaire via revendeur Microsoft)
2. Saisir le **numéro d'autorisation** et le **numéro de licence** fournis par Microsoft à l'achat
3. **Type de produit** : Windows Server 2025 — **Per User CAL** (ou Per Device selon achat)
4. **Quantité** : nombre de CAL achetées
5. Confirmer → les CAL sont importées

Étape 4 — Configurer le déploiement RDS pour utiliser le serveur de licences

1. Server Manager → Services Bureau à distance → **Vue d'ensemble du déploiement**
2. Menu **Tâches** → **Modifier les propriétés du déploiement**
3. Onglet **Licences des services Bureau à distance**
4. Sélectionner **Par utilisateur** (ou Par périphérique selon CAL achetées)
5. Spécifier le serveur de licences : **SRV-RDS.nouvy.lan**
6. Cliquer **Ajouter** → **Appliquer**

Étape 5 — Vérifier l'attribution des CAL

Après quelques connexions utilisateurs, ouvrir le **Gestionnaire de licences RDS** → onglet **Rapports** → **Créer un rapport** pour visualiser :

- Nombre de CAL Per User attribuées
- Liste des utilisateurs ayant consommé une CAL
- CAL disponibles vs utilisées

```
# Lister les CAL Per User attribuées
Get-WmiObject -Namespace "Root\CIMV2" -Class "Win32_TSLicenseKeyPack"
```

Copier

> ***Important** : un utilisateur Per User consomme **une CAL pour 60 jours** après sa première connexion. Si l'utilisateur ne se connecte plus, la CAL est libérée automatiquement à l'expiration.*

---

10. RD Gateway — accès externe sécurisé

Pourquoi installer RD Gateway ?

Sans RD Gateway, accéder aux RemoteApp depuis l'extérieur nécessiterait :

- d'**ouvrir le port RDP 3389** sur Internet (très risqué — attaques par force brute, ransomwares)
- ou d'utiliser un **VPN** (complexe à déployer côté client)

RD Gateway offre une troisième voie : l'utilisateur se connecte en HTTPS (port 443) à la passerelle, qui relaie ensuite les paquets RDP en interne. Avantages :

- Un seul port à exposer (443 — déjà ouvert pour la plupart des sites)
- Encapsulation TLS (chiffrement de bout en bout)
- Authentification AD requise avant tout transit RDP
- Politiques d'accès granulaires (CAP/RAP) — qui peut se connecter, à quoi

Étape 1 — Installer le rôle RD Gateway

1. Server Manager → Services Bureau à distance → vue d'ensemble du déploiement
2. Cliquer sur l'icône **RD Gateway** (en grisé)
3. Sélectionner **SRV-RDS** (ou un serveur dédié — recommandé en DMZ pour la production)
4. **Nom du certificat SSL** : `rds.nouvy.fr` (nom DNS public)
5. Confirmer → installation et redémarrage automatique

> ***Production** : RD Gateway devrait idéalement être placé en **DMZ**, séparé de SRV-RDS qui reste sur le LAN. Pour le lab NOUVY.LAN, on accepte la cohabitation sur SRV-RDS.*

Étape 2 — Configurer les CAP et RAP

Deux types de stratégies contrôlent qui peut se connecter et à quoi.

CAP — Connection Authorization Policy

Définit **quels utilisateurs/groupes** peuvent se connecter via la passerelle, et **avec quelles méthodes** (mot de passe, carte à puce).

1. Outils → **Terminal Services** → **Gestionnaire RD Gateway** (`tsgateway.msc`)
2. SRV-RDS → **Stratégies** → **Stratégies d'autorisation des connexions** → clic droit → **Nouvelle stratégie**
3. **Nom** : `CAP-NOUVY-Users`
4. **Méthodes d'authentification** : mot de passe (et/ou carte à puce)
5. **Membres** : `NOUVY\GRP_RDS_Users`
6. **Délai d'inactivité** : 60 minutes (déconnexion auto)
7. **Activation/désactivation des fonctionnalités client** (redirection imprimantes, presse-papiers...)

RAP — Resource Authorization Policy

Définit **à quelles ressources** (serveurs RDSH) chaque utilisateur peut se connecter.

1. Même console → **Stratégies** → **Stratégies d'autorisation des ressources** → clic droit → **Nouvelle stratégie**
2. **Nom** : `RAP-NOUVY-Apps`
3. **Membres** : `NOUVY\GRP_RDS_Users`
4. **Ressources** : sélectionner le groupe `RDS Connection Brokers Servers` (autorise l'accès à tous les RDSH du déploiement)
5. **Ports autorisés** : 3389 (RDP)

Étape 3 — Configurer l'accès externe DNS et pare-feu

Élément	Configuration
Enregistrement DNS public	`rds.nouvy.fr` → IP publique du firewall
NAT/redirection sur le firewall	Port 443 entrant → 192.168.1.30:443 (SRV-RDS)
Certificat SSL public	Certificat valide pour `rds.nouvy.fr` (Let's Encrypt, ou certificat commercial)

Étape 4 — Tester l'accès externe

Depuis un poste hors du réseau (4G mobile, télétravail) :

1. Ouvrir un navigateur → `https://rds.nouvy.fr/RDWeb`
2. S'authentifier
3. Cliquer sur une RemoteApp
4. Le fichier `.rdp` téléchargé contient automatiquement les paramètres pour passer par RD Gateway

Vérifier dans le `.rdp` la présence des lignes :

```
gatewayhostname:s:rds.nouvy.fr
gatewayusagemethod:i:1
gatewaycredentialssource:i:0
gatewayprofileusagemethod:i:1
```

Copier

---

11. Sécurisation du déploiement RDS

Remplacer les certificats auto-signés

Quatre certificats sont utilisés par RDS (visibles dans **Vue d'ensemble du déploiement** → **Tâches** → **Modifier les propriétés du déploiement** → onglet **Certificats**) :

Service	Rôle du certificat	Nom recommandé
RD Connection Broker — Activation unique	Signe les fichiers .rdp	`srv-rds.nouvy.lan`
RD Connection Broker — Publication	Identifie le broker dans les communications	`srv-rds.nouvy.lan`
RD Web Access	HTTPS du portail web	`rds.nouvy.fr` (externe) ou `srv-rds.nouvy.lan` (interne)
RD Gateway	TLS de la passerelle	`rds.nouvy.fr`

Génération d'un certificat depuis l'AD CS interne (lab)

Si un rôle **Active Directory Certificate Services** est en place :

1. Sur SRV-NOUVY (CA), créer un modèle de certificat **Web Server** dupliqué
2. Émettre un certificat avec :
   - **Subject** : `CN=srv-rds.nouvy.lan`
   - **SAN** (Subject Alternative Name) : `DNS=srv-rds.nouvy.lan`, `DNS=rds.nouvy.fr`
3. Exporter le certificat avec sa clé privée au format `.pfx`
4. Importer dans la console RDS → ajouter un mot de passe pour l'import

Certificat public (production)

Pour `rds.nouvy.fr` exposé sur Internet : utiliser **Let's Encrypt** (via win-acme par exemple) ou un certificat commercial DigiCert/Sectigo.

Authentification au niveau réseau (NLA)

NLA force l'authentification **avant** l'ouverture de la session graphique, ce qui empêche les attaques sur l'écran de connexion RDP.

```
# Vérifier que NLA est actif sur SRV-RDS
(Get-WmiObject -Class "Win32_TSGeneralSetting" -Namespace "root\cimv2\terminalservices" -
Filter "TerminalName='RDP-Tcp'").UserAuthenticationRequired
# Doit retourner 1
```

Copier

NLA est **activé par défaut** depuis Windows Server 2012. Ne jamais le désactiver en production.

Restrictions par GPO

Plusieurs paramètres GPO durcissent RDS. Les retrouver dans :

```
Configuration ordinateur → Stratégies → Modèles d'administration → Composants Windows →
Services Bureau à distance → Hôte de session Bureau à distance
```

Copier

GPO recommandée	Valeur
Limiter le nombre de connexions	50 (selon dimensionnement)
Définir un délai d'expiration pour les sessions actives	8 heures
Définir un délai d'expiration pour les sessions inactives	30 minutes
Demander une authentification au niveau réseau pour les connexions distantes	Activé
Exiger l'utilisation d'une couche de sécurité spécifique	TLS 1.2
Définir le niveau de chiffrement	Élevé
Redirection des lecteurs côté client	Désactivée *(évite l'exfiltration de données)*
Redirection du presse-papiers	À évaluer selon besoin

Pare-feu Windows

Les règles suivantes doivent être ouvertes sur SRV-RDS :

Service	Protocole/Port	Source
RDP	TCP 3389	LAN
RD Web Access	TCP 443	LAN + Internet (via NAT)
RD Gateway	TCP 443	Internet (via NAT)
RD Licensing	TCP 135, 49152-65535 (RPC dynamique)	LAN
WMI / management	TCP 135 + RPC	Admins

```
# Vérifier les règles RDP
Get-NetFirewallRule -DisplayGroup "Bureau à distance" | Format-Table DisplayName, Enabled,
Direction, Action
```

Copier

Auditer les connexions

Les événements RDS sont enregistrés dans plusieurs journaux d'observateur d'événements :

Journal	Contenu
`Microsoft-Windows-TerminalServices-LocalSessionManager/Operational`	Ouverture/fermeture de session locale RDS (ID 21, 22, 23, 24, 25)
`Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational`	Tentatives de connexion (ID 1149)
`Microsoft-Windows-TerminalServices-Gateway/Operational`	Connexions RD Gateway (ID 200, 205, 304)
`Sécurité`	Échecs/réussites de connexion AD (ID 4624, 4625)

```
# Lister les connexions RDS récentes
Get-WinEvent -LogName "Microsoft-Windows-TerminalServices-LocalSessionManager/Operational" -
MaxEvents 20 |
    Where-Object { $_.Id -in 21,22,23,24,25 } |
    Select-Object TimeCreated, Id, Message
```

Copier

---

12. Tests et dépannage

Test côté client

Test 1 — Connexion via RD Web Access

1. Ouvrir un navigateur sur un poste client → `https://srv-rds.nouvy.lan/RDWeb`
2. S'authentifier avec un compte de `GRP_RDS_Users`
3. La page doit afficher les RemoteApp publiées
4. Cliquer sur une RemoteApp → un fichier `.rdp` est téléchargé
5. Ouvrir le fichier → l'application s'ouvre dans une fenêtre native sur le poste

Test 2 — Lancement direct via fichier .rdp

Créer un raccourci `.rdp` à distribuer aux utilisateurs (sans passer par le portail web) :

1. Sur SRV-RDS, naviguer dans Server Manager → Collections → RemoteApp publiées
2. Sélectionner une application → **Tâches** → **Exporter les paramètres RemoteApp**
3. Choisir l'emplacement → un fichier `.rdp` est généré
4. Distribuer ce fichier aux utilisateurs (via GPO Drive Mapping, par exemple)

Test 3 — Microsoft Remote Desktop (Mac, iOS, Android)

L'application gratuite **Microsoft Remote Desktop** permet d'utiliser les RemoteApp depuis :

- macOS (App Store)
- iPhone/iPad (App Store)
- Android (Play Store)

Configuration :

1. Ajouter une **Workspace** → URL : `https://srv-rds.nouvy.lan/RDWeb/feed/webfeed.aspx`
2. S'authentifier
3. Toutes les RemoteApp publiées apparaissent dans l'app

Commandes utiles de diagnostic

```
# Lister les utilisateurs connectés à SRV-RDS
qwinsta /server:srv-rds

# Forcer la déconnexion d'une session bloquée (ID de session obtenu via qwinsta)
logoff 3 /server:srv-rds

# Lister les RemoteApp publiées
Get-RDRemoteApp -CollectionName "Collection-Apps-NOUVY"

# Vérifier les rôles RDS installés
Get-WindowsFeature *RDS* | Where-Object { $_.InstallState -eq "Installed" }

# Vérifier l'état du serveur de licences
$LSObject = Get-WmiObject -Class "Win32_TSLicenseServer" -Namespace "Root\CIMV2" -
ComputerName SRV-RDS
$LSObject.GetActivationStatus().ActivationStatus
# 0 = Activated, 1 = Not Activated
```

Copier

Problèmes courants

Symptôme	Cause probable	Résolution
"Le serveur n'est pas disponible. Vérifiez le nom..."	DNS ne résout pas SRV-RDS	Vérifier l'enregistrement DNS et le ping
"Aucune licence Bureau à distance disponible"	Période de grâce expirée, pas de CAL	Installer/activer le serveur de licences, importer des CAL
"Vous n'avez pas l'autorisation de vous connecter..."	Utilisateur pas membre de `GRP_RDS_Users` ou de `Utilisateurs du Bureau à distance`	Ajouter dans le bon groupe
Avertissement de certificat	Certificat auto-signé non approuvé	Déployer le certificat racine via GPO ou utiliser un vrai certificat
L'application ne se lance pas, message "Cette application est associée à plusieurs comptes"	Application installée hors mode RDS	Réinstaller via `Change user /install`
Profil utilisateur lent ou corrompu	Profil itinérant mal configuré	Activer les UPD à la place
Connexion possible mais bureau noir	GPU/Direct3D incompatible	Désactiver l'accélération matérielle dans la collection

---

13. Bonnes pratiques

Dimensionnement

Profil utilisateur	RAM par utilisateur	CPU par utilisateur
Léger (Office, navigateur, mail)	1 à 2 Go	0,25 à 0,5 vCPU
Standard (Office + logiciel métier)	2 à 4 Go	0,5 à 1 vCPU
Lourd (CAO, dev, multimédia)	4 à 8 Go+	1 à 2 vCPU

> ***Règle de base** : pour 50 utilisateurs standard simultanés, prévoir un serveur RDSH avec ~16 cœurs et 128 Go de RAM. Au-delà, ajouter d'autres RDSH dans la collection (équilibrage de charge automatique via le Connection Broker).*

Haute disponibilité

Pour un environnement de production :

- **2 RDSH minimum** dans la collection (équilibrage de charge)
- **2 Connection Brokers** en mode haute disponibilité (avec base SQL externe)

- **2 RD Web Access** derrière un load balancer
- **2 RD Gateway** en cluster (NLB ou load balancer)
- **2 serveurs de licences** RDS

Sauvegardes

Éléments à sauvegarder régulièrement :

Élément	Méthode
Définition des collections et RemoteApp	Export PowerShell `Export-RDDeployment`
Disques de profil utilisateur (UPD)	Sauvegarde du partage `\\srv-nouvy\UPD-NOUVY$`
Base de données du Connection Broker (si HA)	Sauvegarde SQL Server
Configuration RD Gateway (CAP/RAP)	Export depuis la console
Certificats SSL	Export `.pfx` avec clé privée + mot de passe
Serveur de licences (RD Licensing)	Sauvegarde de la base + clés CAL

Maintenance

- **Drain Mode** avant maintenance d'un RDSH : empêche les nouvelles connexions, laisse les sessions existantes se terminer

```
# Mode drain (refuse les nouvelles connexions)
Change logon /drain

# Réactiver les connexions
Change logon /enable

# Vérifier l'état
Change logon /query
```

Copier

- **Patcher en dehors des heures ouvrées** ou utiliser le mode drain en début de soirée
- **Surveiller les logs RDS** quotidiennement (au moins via une supervision Zabbix/PRTG/Nagios)
- **Auditer les CAL** trimestriellement pour ajuster les achats

Documentation à tenir à jour

- Schéma d'architecture RDS (rôles, serveurs, certificats)
- Liste des RemoteApp publiées + responsable métier
- Liste des collections + groupes AD associés
- Procédure de récupération d'urgence (DRP)
- Inventaire des CAL achetées et utilisées