FICHE DE RÉVISION — RDS (REMOTE DESKTOP SERVICES)

TSSR — Rôles RDS, collections, licensing, certificats, GPO et RD Gateway

1. Définitions essentielles

Notion	Définition
RDS	**Remote Desktop Services.** Ce n'est en rien de la prise de main à distance : c'est de **l'ouverture de session à distance**. Le rôle Windows Server qui permet à plusieurs utilisateurs de se connecter à distance à un serveur et d'y exécuter des applications ou des bureaux complets, comme s'ils étaient physiquement devant la machine.
NLA	**Network Level Authentication.** Mécanisme d'authentification RDP qui impose à l'utilisateur de **s'authentifier avant** que la session RDP soit établie — contrairement au comportement historique où la connexion s'établissait d'abord, et le bureau de connexion Windows apparaissait ensuite.
MSTSC	Le **client RDP**.
Terminal Server	Ancien nom de RDS : le rôle s'appelait **Terminal Services** jusqu'à Windows Server 2008 R2.
TCO	**Total Cost of Ownership**, coût total de possession : le coût global d'une solution sur **toute sa durée de vie** (achat, déploiement, maintenance, formation, support, remplacement), pas juste le prix d'achat initial.

2. Prérequis techniques

- **Disponibilité** : le Bureau à distance existe sur **toutes les versions Windows Pro**, mais **pas sur Windows Home**.
- **NLA** : authentification préalable à l'établissement de la session.
- **MSTSC** : le client RDP à lancer côté poste utilisateur.

3. Gestion des sessions

3.1 Sur un poste client

En accès à distance, on ne peut être connecté qu'à **un seul utilisateur à la fois** sur la machine (l'utilisateur interactif compte pour 1). Toute la difficulté quand on veut se connecter à distance, c'est **de changer l'utilisateur qui va se logger à distance**.

> *La session se libère directement au bout de 30 secondes. Si on se reconnecte sur le Client 1, un écran spécifique apparaît.*

3.2 Sur un serveur

- Deux sessions **concomitantes** (simultanées) : un utilisateur actif **et** un utilisateur à distance.
- Ou bien deux utilisateurs à distance et **zéro** utilisateur actif.

3.3 Déconnecter vs Se déconnecter

Action	Effet
Déconnecter	coupe le bureau à distance, **mais la session reste ouverte**
Se déconnecter	fermeture du bureau à distance **ET** fermeture de la session

4. Accès RDP selon le rôle du serveur

Type de serveur	Comportement RDP
Serveur membre (non-DC)	accès géré via le groupe **« Utilisateurs du Bureau à distance »** — onglet « Autoriser l'ouverture de sessions »
Contrôleur de domaine (DC)	RDP **réservé aux Administrateurs du domaine** uniquement. Mesure de sécurité **volontaire** de Microsoft : un DC est une ressource critique, on ne laisse pas des utilisateurs lambda s'y connecter à distance

Le groupe « Utilisateurs du Bureau à distance » **n'existe pas en tant que tel sur un DC**, ou en tout cas il n'y a pas l'effet qu'il a sur un serveur membre. Pour autoriser un compte non-admin à se connecter en RDP sur un DC, il faut l'ajouter explicitement dans la GPO **« Autoriser l'ouverture d'une session par les services Bureau à distance »** :

```
Configuration ordinateur > Paramètres Windows > Paramètres de sécurité
> Stratégies locales > Attribution des droits utilisateur
```

En pratique, on ne le fait JAMAIS sur un contrôleur de domaine : c'est une mauvaise pratique de sécurité.

5. TCO — l'argument commercial du RDS

C'est souvent l'argument commercial derrière RDS : un **thin client à 150 €** + un **serveur RDS mutualisé** peut avoir un TCO bien inférieur à 200 postes full équipés à 800 € pièce avec maintenance individuelle.

> *Le RDS fait en sorte que le poste devienne un client léger. Le but du jeu, c'est de pouvoir juste lancer MSTSC pour une ouverture de session à distance : l'ordinateur de l'utilisateur n'est plus le centre de la session, il devient un périphérique d'affichage.*

Axe de rationalisation	Gain
Licences logicielles	on achète une licence serveur au lieu de 200 licences poste
Maintenance applicative	une mise à jour sur le serveur, tout le monde en bénéficie, zéro déplacement
Sécurité	les données ne transitent jamais sur le poste client, elles restent sur le serveur
Durée de vie du parc	un thin client dure 10 ans sans broncher puisqu'il ne calcule rien, pas besoin de renouveler le parc tous les 4 ans

On parle donc d'HÔTE DE SESSIONS, et cette fonctionnalité est PAYANTE.

6. Architecture — les rôles RDS

Rôle	Fonction
Session Host (RDSH)	**Serveur Hôte de Session** — héberge les sessions utilisateurs
Connection Broker (RDCB)	**Serveur Broker de Session** — répartit les connexions entre les serveurs Hôte de Session
Web Access (RDWA)	**Serveur WEB-RDS** — portail web de publication des applications

6.1 RDS vs VDI

	Principe
RDS	plusieurs utilisateurs partagent le **même OS** sur le même serveur (sessions isolées mais OS commun)
VDI	chaque utilisateur a sa **propre VM**, avec son propre OS dédié

Concrètement en VDI : un hyperviseur (Hyper-V, VMware ESXi…) fait tourner X VM, chaque utilisateur se connecte en RDP à **sa** VM — il est seul dessus — et son environnement est **totalement isolé** des autres.

7. Collection d'hôtes de session

On crée une **Collection d'Hôtes de Session** qui réunit plusieurs serveurs Hôte de Session (RDSH) en un **pool logique géré comme une entité unique**.
L'aiguillage se fait par le **Broker de sessions**, qui répartit la charge. Pour l'équilibrage, c'est **au nombre de sessions** : une session vers un serveur, puis l'autre, puis l'autre, etc.

8. RD Connection Broker — rôle et équilibrage

Fonction	Comportement
Équilibrage de charge	distribue les nouvelles connexions vers le serveur RDSH ayant le **moins de sessions actives à l'instant T**. C'est du **round-robin pondéré par le nombre de sessions**, pas une simple alternance mécanique
Reconnexion	si un utilisateur perd sa connexion et se reconnecte, le Broker le redirige vers le serveur RDSH **exact où sa session existe encore**, pas vers un serveur aléatoire de la collection

Il faut VÉRIFIER que le Round Robin est bien activé.

9. Licensing — CAL et virtualisation

9.1 Licensing en volume (Volume Licensing)

Modèle de licensing Microsoft destiné aux entreprises : acquérir des licences **en masse** pour plusieurs postes / serveurs via un **contrat unique**, plutôt que d'acheter une licence individuelle (OEM / Retail) par machine.

9.2 Les deux CAL s'additionnent

CAL	Rôle
CAL Standard (Windows Server)	**obligatoire** pour qu'un client / utilisateur accède à **n'importe quelle** ressource du serveur Windows Server (partage de fichiers, impression, AD…). C'est la licence de base
CAL RDS (Remote Desktop Services)	s'ajoute **par-dessus** la CAL Standard, spécifiquement pour l'utilisation du rôle RDS (session distante)

Ce n'est pas une CAL qui en remplace une autre : ELLES S'ADDITIONNENT.

> *Sans CAL RDS, même avec une CAL Standard valide, impossible de se connecter en session RDS au-delà du mode grâce de 120 jours. Les deux sont vérifiées par le serveur RD Licensing, et doivent être achetées et activées séparément.*

9.3 Licences de virtualisation (depuis Server 2016)

Édition	Licences Hyper-V incluses
Windows Server Standard	**2 licences Hyper-V** fournies — il faut payer pour en avoir plus
Windows Server Datacenter	**pas de limite**

Il faut donc payer : **une licence de virtualisation + une CAL pour l'OS dans la VM**.

10. TP — Sécuriser RDS avec la PKI interne

10.1 Contexte

Objectif : sécuriser l'infrastructure RDS (**SRVPA05** = RDWeb, **SRVPA06** = Broker) en remplaçant les certificats **auto-signés** par des certificats émis par l'autorité de certification interne `dompa-SRVPA02-CA`, puis configurer le **SSO** pour les programmes RemoteApp.

10.2 Certificat pour RDWeb (SRVPA05)

Problème : le portail RDWeb affichait une erreur de certificat, car le certificat en place était **auto-signé** (émis par SRVPA05 lui-même).

- Sur SRVPA05 : **IIS Manager > Certificats de serveur > Créer une demande de certificat**. CN = `srvpa05` (doit correspondre **exactement** à l'URL tapée dans le navigateur), longueur de clé **2048**, enregistrer le fichier `.req`
- Soumettre la CSR sur `http://srvpa02/certsrv` : **Demande avancée > Soumettre une CSR**, coller le contenu du `.req`, modèle **Serveur Web**, télécharger le `.cer` émis
- Sur SRVPA05 : **IIS Manager > Certificats de serveur > Terminer la demande de certificat** > sélectionner le `.cer`
- Lier le certificat dans IIS : **Sites > Default Web Site > Liaisons > HTTPS 443 > Modifier > Certificat SSL**
- Lier le certificat dans le déploiement RDS : **Gestionnaire de serveur > Services Bureau à distance > Tâches > Modifier les propriétés du déploiement > Certificats > RD Web Access > Sélectionner le certificat existant**

Le CN du certificat doit correspondre EXACTEMENT au nom tapé dans la barre d'adresse. Si les clients tapent srvpa05/rdweb, le CN doit être srvpa05, pas srvpa05.dompa.lan.

10.3 Certificat pour le Broker (SRVPA06)

Problème : à l'ouverture d'une RemoteApp (Word via Work Resources), une fenêtre demandait de faire confiance à l'éditeur et de saisir les credentials.
Particularité : SRVPA06 **n'a pas IIS** — la CSR se génère via `certreq`.

- Faire une demande de certificat via la **MMC**
- Soumettre sur `http://srvpa02/certsrv` > modèle **Serveur Web** > télécharger le `.cer`
- Vérifier dans `certlm.msc` > **Personnel > Certificats** > double-clic sur le certificat > onglet **Général** : la mention **« Vous avez une clé privée qui correspond à ce certificat »** doit être présente
- Exporter en `.pfx` (**clé privée incluse**) : clic droit > **Toutes les tâches > Exporter > Oui, exporter la clé privée > format .PFX** > définir un mot de passe
- Lier dans le déploiement RDS : **Tâches > Modifier les propriétés du déploiement > Certificats > RD Connection Broker - Activer l'authentification unique** > chemin `C:\srvpa06.pfx` + mot de passe

> *Modèle Serveur Web pour le Broker : bien que SRVPA06 ne soit pas un serveur web, le modèle Serveur Web est LE bon — il génère les attributs attendus par le rôle RD Connection Broker.*

10.4 PKI Wildcard pour les RDSH

Pour éviter de générer un certificat par serveur, un certificat **wildcard** `*.dompa.lan` couvre tous les serveurs du domaine en un seul certificat. **Règle à retenir :** un wildcard couvre **un seul niveau** de sous-domaine (`srvpa05.dompa.lan` ☑).
Commande à taper dans le `cmd` de SRVPA03 / SRVPA04 (et SRVPA09) :

```
# une seule ligne, en invite de commandes administrateur
wmic /namespace:\\root\cimv2\TerminalServices PATH Win32_TSGeneralSetting
     Set SSLCertificateSHA1Hash="THUMBPRINT"
```

`THUMBPRINT` se remplace par l'**empreinte numérique du certificat** (le hash). Ce qu'on a mis en place :

- Import du `.pfx` (certificat **+ clé privée**) sur **SRVPA03 et SRVPA04**
- Le certificat wildcard `*.dompa.lan` couvre `srvpa03.dompa.lan` et `srvpa04.dompa.lan`
- Le certificat de l'AC `dompa-SRVPA02-CA` déployé sur les postes clients via GPO → racines de confiance → **plus d'alerte à la connexion**

10.5 Séquence complète du handshake

Étape	Ce qui se passe
1	Le client (`mstsc`) se connecte au serveur hôte de session (SRVPA03 ou SRVPA04)
2	Le serveur envoie son **certificat** (qui contient la **clé publique**) au client
3	Le client vérifie que ce certificat est signé par une **AC de confiance** (`dompa-SRVPA02-CA`) → si oui, aucune alerte
4	Le client génère un **secret**, le **chiffre avec la clé publique** du serveur et l'envoie
5	Le serveur **déchiffre ce secret avec sa clé privée**
6	Les deux parties dérivent une **clé de session symétrique** à partir de ce secret
7	Tunnel chiffré établi → tout le trafic RDP est encapsulé dedans

Sans clé privée sur le serveur : impossible de déchiffrer le secret à l'étape 5, donc impossible de dériver la clé de session, donc CONNEXION REFUSÉE.

11. Les GPO du déploiement RDS

11.1 Certificat de l'AC dans les racines de confiance

```
Configuration ordinateur > Paramètres Windows > Paramètres de sécurité
> Stratégies de clé publique
> Autorités de certification racines de confiance
> clic droit > Importer > sélectionner le .cer de dompa-SRVPA02-CA
```

- Récupérer le `.cer` de l'AC sur `http://srvpa02/certsrv` > **Télécharger un certificat d'autorité de certification**
- GPO liée à l'OU `_Ordinateurs-Clients`
- Application au redémarrage ou via `gpupdate /force`

11.2 Approbation automatique de l'éditeur RemoteApp

Pour supprimer le message « Faites-vous confiance à l'éditeur de ce programme RemoteApp ? » :

```
Configuration ordinateur > Modèles d'administration > Composants Windows
> Services Bureau à distance > Client Connexion Bureau à distance
> Spécifier les empreintes numériques SHA1 des certificats représentant
  les éditeurs .rdp approuvés
```

Activer > saisir l'**empreinte SHA1** du certificat de SRVPA06 (visible dans la MMC > onglet **Détails > Empreinte numérique**). GPO liée à l'OU `_Ordinateurs-Clients`.

11.3 SSO (Single Sign-On) pour RemoteApp — 2 paramètres

Paramètre 1 — Authentification serveur :

```
Configuration ordinateur > Modèles d'administration > Composants Windows
```

```
> Services Bureau à distance > Client Connexion Bureau à distance
> Configurer l'authentification du serveur pour le client
```

Activer, puis choisir la valeur : **« Ne pas connecter si l'authentification échoue »** (le modèle logique et normal) ou **« Toujours connecter, même si l'authentification échoue »**.

Paramètre 2 — Délégation des credentials :

```
Configuration ordinateur > Modèles d'administration > Système
> Délégation d'informations d'identification
> Autoriser la délégation d'informations d'identification par défaut
```

Activer > cliquer sur **Afficher** > ajouter :

```
TERMSRV/srvpa06.dompa.lan
```

> *Cocher « Concaténer les valeurs par défaut du système d'exploitation supérieures à » pour ne pas écraser les règles existantes. Les deux GPO sont liées à l'OU _Ordinateurs-Clients (Configuration ordinateur → machines).*

11.4 Publication automatique des RemoteApp dans le menu Démarrer

```
Configuration utilisateur > Modèles d'administration > Composants Windows
> Services Bureau à distance > RemoteApp et Connexions Bureau à distance
> Spécifier l'URL de connexion par défaut
```

```
https://srvpa05/RDWeb/Feed/webfeed.aspx
```

- GPO liée à l'OU des **utilisateurs**
- **Prérequis** : le certificat de SRVPA05 doit être **de confiance** sur les postes clients (voir 11.1)

12. Redirection de dossiers

12.1 Principe

Peu importe la machine sur laquelle l'utilisateur ouvre une session (poste fixe, autre PC du domaine, session RDS), quand il clique sur **Documents**, il voit toujours ses fichiers. Windows pointe **silencieusement** vers `\\SRVPA02\RED-DOC\nomutilisateur\` : l'utilisateur ne voit pas le chemin réseau, il voit juste « Mes Documents ».

> *Différence avec le profil itinérant : la redirection cible uniquement les dossiers choisis, pas tout le profil.*

12.2 Configuration de la GPO

```
Configuration utilisateur > Stratégies > Paramètres Windows
> Redirection de dossiers > Documents > clic droit > Propriétés
> Paramètre : De base - Rediriger les dossiers de tout le monde
              vers le même emplacement
> Emplacement : Créer un dossier pour chaque utilisateur sous le chemin racine
> Chemin racine : \\SRVPA02\RED-DOC\Documents
```

GPO liée à l'OU des **utilisateurs**.

12.3 Options importantes

- **Déplacer le contenu vers le nouvel emplacement** — migre les fichiers existants automatiquement
- **Accorder à l'utilisateur des droits exclusifs** → à **décocher** si on veut que les administrateurs puissent accéder aux dossiers des utilisateurs
- **Suppression de stratégie** → « Rediriger vers le profil local » : si la GPO est supprimée, les documents reviennent en local

12.4 Permissions NTFS sur le dossier racine Documents

Qui	Permission	S'applique à
Administrateurs	Contrôle total	Ce dossier, sous-dossiers et fichiers
SYSTEM	Contrôle total	Ce dossier, sous-dossiers et fichiers
Créateur propriétaire	Contrôle total	Sous-dossiers et fichiers **uniquement**
Utilisateurs authentifiés	Lister + Créer des dossiers	**Ce dossier uniquement**

Cette configuration garantit que **chaque utilisateur est propriétaire de son sous-dossier uniquement**, que **les collègues ne voient pas les dossiers des autres**, que **les admins ont accès à tout**, et que **Windows peut créer le sous-dossier automatiquement** à la première connexion.

12.5 Application

```
gpupdate /force
```

La redirection s'applique À L'OUVERTURE DE SESSION, pas à chaud : gpupdate /force PUIS déconnexion / reconnexion.

> *En environnement RDS : avec le Loopback Processing (Fusionner) actif sur l'OU _RDSH, la GPO s'applique bien en session distante, même si l'OU des utilisateurs est ailleurs.*

13. Association de types de fichiers (RemoteApp)

L'**Association de types de fichiers**, dans les propriétés d'un programme RemoteApp, permet de lier des extensions de fichiers à cette application publiée.
Concrètement : quand un utilisateur double-clique sur un `.docx` sur son poste local, Windows ouvre automatiquement ce fichier dans **Word via RemoteApp**, sans que l'utilisateur ait besoin de lancer manuellement la session RDS. C'est **transparent** : la fenêtre Word s'ouvre comme si Word était installé en local, mais **le process tourne sur le RDSH**.

- `.doc`, `.docx` — à cocher
- `.dotx` (templates) — à cocher
- `.docm` — à cocher si les utilisateurs ont des macros
- Les autres (`.dochtml`, `.docxml`…) relèvent de cas très spécifiques : on peut les laisser décochées en environnement PME standard

14. RD Gateway — accès distant sécurisé

14.1 Pourquoi et comment

Sans RD Gateway, il faudrait ouvrir le port 3389 sur le pare-feu directement vers les RDSH. Mauvaise pratique : port exposé, bruteforce, scan de ports.

La solution : RD Gateway **encapsule le trafic RDP dans du HTTPS (port 443)**. Le protocole de transport s'appelle **RDP over HTTPS** — le client RDP encapsule ses paquets RDP dans un tunnel TLS/HTTPS avant envoi.

```
Internet → Port 443 → NAT/Routeur → SRVPA07 (RD Gateway)
→ Désencapsulation HTTPS → RDP port 3389 → SRVPA03/04 (RDSH)
```

Maillon	Rôle exact
NAT / routeur	redirige simplement le port 443 entrant vers l'IP interne de SRVPA07. C'est la **couche réseau** : il ne comprend rien au contenu

Maillon	Rôle exact
RD Gateway	fait le vrai travail **applicatif** : déchiffre le tunnel HTTPS, récupère le flux RDP nu, et le reroute en interne vers le RDSH sur le port 3389

> *Côté pare-feu : seul le port 443 est ouvert vers le Gateway depuis l'extérieur. Le port 3389 reste fermé de l'extérieur et ne circule qu'en interne, entre le Gateway et les RDSH. Prérequis : un certificat SSL valide sur le Gateway, d'où l'importance de la PKI.*

Sans Gateway : ouverture du 3389, ou VPN. Avec Gateway : publication de la collection via le 443 uniquement. Pas de VPN, pas de 3389 exposé.

14.2 Stratégies du Gateway — tsgateway.msc

Symptôme rencontré en tentant de joindre `GROSCOLIS.DOMPA.LAN` : soit le compte n'est pas autorisé sur la Passerelle, soit le nom n'est pas au format FQDN attendu. Ici le FQDN était correct, donc c'est la **première piste** à privilégier.

Cause : la ressource cible (`GROSCOLIS`) n'est couverte par **aucune stratégie RD RAP** dans `tsgateway.msc`. Même avec un compte valide dans le **RD CAP**, sans **RAP** matchant la machine visée, le Gateway refuse la connexion.

```
Gestionnaire de passerelle des services Bureau à distance
> SRVPA07 (Local) > Stratégies
> Stratégies d'autorisation d'accès aux ressources
```

Vérifier que `GROSCOLIS` est bien inclus dans le groupe de ressources autorisées d'une des stratégies (`RDG_AllDomainComputers` ou une stratégie dédiée), sinon l'ajouter — ou autoriser la connexion à **toutes les ressources du domaine**.

14.3 Chaîne de confiance PKI pour les clients externes

Erreur observée : « Impossible de vérifier l'identité de l'ordinateur distant » — la **vérification de la révocation** n'a pas pu être effectuée pour le certificat, alors que le nom du certificat (`*.dompa.lan`) est correct.

Cause : le domaine `dompa.lan` est **derrière le NAT**. Le certificat pointe vers une adresse **interne à l'AD**, injoignable depuis un client externe sur Internet — le NAT ne route rien vers ce point interne.

- Ajouter le **certificat racine de la PKI** dans les **Autorités de certification racines de confiance** du client externe
- **Publier la liste de révocation (CRL)** sur un site accessible depuis Internet, dans une **DMZ**

> *En production, on achète le certificat à une vraie Autorité de Certification publique. C'est pour ça qu'en prod on ne monte pas de PKI interne pour les services exposés sur Internet : une PKI interne reste réservée aux usages internes (authentification machine, chiffrement interne, etc.).*

15. Pièges et points à retenir pour l'ECF

RDS ≠ prise de main à distance. C'est de l'OUVERTURE DE SESSION à distance.

- RDS = **même OS partagé** (sessions isolées). VDI = **une VM par utilisateur**.
- **Déconnecter** = session toujours ouverte. **Se déconnecter** = session fermée.
- Serveur membre → groupe **« Utilisateurs du Bureau à distance »**. DC → **admins du domaine uniquement**, c'est voulu.
- Il faut **CAL Standard + CAL RDS**, elles s'additionnent. Mode grâce : **120 jours**.
- Server Standard = **2 licences Hyper-V**, Datacenter = illimité.
- Le **CN du certificat RDWeb** doit correspondre **exactement** à l'URL tapée (`srvpa05`, pas `srvpa05.dompa.lan`).
- Le Broker n'a **pas IIS** : CSR via `certreq`, export en `.pfx` **avec la clé privée**, modèle **Serveur Web** quand même.

- SSO : la délégation se trouve sous **Système > Délégation d'informations d'identification**, valeur `TERMSRV/srvpa06.dompa.lan` — **pas** sous les paramètres RDS.
- Redirection de dossiers : s'applique **à l'ouverture de session**, donc `gpupdate /force` puis déconnexion / reconnexion.
- RD Gateway = **RDP over HTTPS**, seul le **443** est ouvert vers l'extérieur, le **3389** reste interne.
- Gateway : un **RD CAP** valide ne suffit pas, il faut aussi un **RD RAP** couvrant la machine cible.
- Client externe + PKI interne = il faut le **certificat racine** dans les racines de confiance **et** la **CRL publiée** sur Internet.