# WINDOWS SERVER

## Refaire une machine en comprenant chaque étape

AD DS • DNS • DHCP • RDS • AD CS • Certificats

- Partage de mes notes au fil du cours -

## Objectif : savoir refaire le TP sans cliquer “au hasard”.

Chaque action est accompagnée de son “pourquoi”, des vérifications à faire et des corrections de tes notes.

### CONTEXTE DU TP

Le document suit ton labo Windows Server avec un serveur multicarte et plusieurs rôles regroupés sur la même machine. C’est acceptable pour apprendre. En production, on sépare généralement les rôles sensibles (contrôleur de domaine, RDS, autorité de certification, etc.) pour réduire les risques de sécurité et de panne.

| Ordre | Bloc | Résultat attendu |
|---|---|---|
| 1 | Préparer Windows Server | Nom du serveur + interfaces LAN/WAN + IP fixes |
| 2 | AD DS + DNS + DHCP | Domaine tssr.info, résolution de noms et attribution IP |
| 3 | DNS propre | A / NS / SOA / PTR cohérents + redirecteur |
| 4 | RDS | Session-based deployment + collection + RemoteApp + licences |
| 5 | AD CS | Autorité de certification + certificat RDS approuvé |
| 6 | Validation | nslookup, DHCP, RDWeb et chaîne de certificats |

**Nom vu dans tes captures : SRVRDS • FQDN : srvrds.tssr.info • IP LAN du TP : 192.168.100.10**

# 0. Les corrections indispensables avant de réviser

### .info n’est PAS un suffixe privé

“.info” est un domaine de premier niveau public. Le domaine tssr.info peut être utilisé dans un labo isolé, mais pas parce que .info serait privé. En production, Microsoft recommande d’utiliser un espace de noms DNS basé sur un domaine enregistré par l’organisation, souvent un sous-domaine comme ad.exemple.fr.

### Une APIPA ne veut pas dire « LAN »

169.254.0.0/16 est l’adressage automatique qu’un poste Windows peut s’attribuer lorsqu’il est configuré en DHCP mais ne reçoit aucune réponse DHCP. Dans TON TP, cette carte correspondait au réseau LAN isolé. C’est le contexte du montage qui permet de l’identifier.

### Le certificat RDS est un .PFX, pas un .PKX

Un fichier .pfx (PKCS #12) peut contenir le certificat ET sa clé privée. C’est ce format que RDS attend quand on applique un certificat aux rôles. Un .cer DER classique contient le certificat public, sans la clé privée.

### Pas de règle « attendre 24 h » pour sécuriser RDWeb

Un avertissement “site non sécurisé” vient typiquement d’un certificat non approuvé, expiré ou dont le nom ne correspond pas à l’URL. Une fois le bon certificat appliqué et sa chaîne approuvée, il n’existe pas de délai fixe de 24 heures.

### Racine ≠ Entreprise

“Entreprise / autonome” décrit l’intégration de l’AC à Active Directory. “Racine / secondaire” décrit sa place dans la hiérarchie PKI. Pour une première AC intégrée au domaine et sans AC parente : Entreprise + Racine.

### SHA-256 n’est pas un chiffrement

SHA-256 est une fonction de hachage utilisée notamment lors des signatures. RSA est un algorithme asymétrique. Lors de l’export PFX, Windows peut proposer AES256-SHA256 pour protéger le fichier et sa clé privée.

# 1. Avant l'installation : édition Windows Server et mot de passe

## 1.1 Standard ou Datacenter ?

| Édition | Virtualisation | À retenir pour le TSSR |
|---|---|---|
| Windows Server Standard | Droits de virtualisation pour 2 VM Windows Server par licence lorsque l'hôte est correctement licencié ; Hyper-V est disponible. | Convient à beaucoup de petits/moyens environnements et aux besoins de virtualisation limités. |
| Windows Server Datacenter | Droits pour un nombre illimité de VM Windows Server sur l'hôte correctement licencié. | Destinée aux environnements très virtualisés et inclut davantage de fonctions avancées de datacenter. |

**MÉMO**

Datacenter n'est pas "Hyper-V" et Standard "sans Hyper-V". Les deux peuvent faire tourner Hyper-V. La différence importante pour ton cours est surtout le droit de virtualiser beaucoup plus de Windows Server avec Datacenter.

**Source vérifiée :** Microsoft Learn — Locks and limits in Windows Server

## 1.2 Mot de passe : ce que Windows exige réellement

Si la stratégie "Le mot de passe doit respecter des exigences de complexité" est activée, Windows n'exige pas obligatoirement les 4 catégories à la fois. Il faut des caractères provenant d'au moins 3 catégories parmi majuscules, minuscules, chiffres, caractères non alphanumériques (et, selon la version, une catégorie Unicode supplémentaire). Le mot de passe ne doit pas contenir le nom du compte ou des parties significatives du nom complet.

**POUR LE TP**

Si ton formateur impose « 1 majuscule + 1 minuscule + 1 chiffre + 1 caractère spécial + au moins 8 caractères », respecte cette règle de TP : elle est plus stricte que le minimum de la stratégie de complexité Windows. Exemple de forme : Tssr@2026! (ne pas réutiliser cet exemple en vrai).

**Source vérifiée :** Microsoft Learn — Password must meet complexity requirements

# 2. Préparer la machine : nom, LAN, WAN et IP statiques

## 2.1 Pourquoi commencer par le nom et le réseau ?

AD DS, DNS, DHCP, RDS et les certificats dépendent fortement du nom DNS du serveur et de son adressage. On fixe donc ces éléments AVANT d'installer les rôles.

| Action | Pourquoi |
|---|---|
| Renommer le serveur (ex. SRVRDS) | Le nom deviendra une partie du FQDN, des enregistrements DNS et des certificats. |
| Identifier les cartes réseau | Éviter de publier l'adresse WAN dans le DNS interne ou d'utiliser la mauvaise carte. |
| Mettre des IP stables | Un serveur AD/DNS/DHCP ne doit pas changer d'adresse au hasard. |

## 2.2 Distinguer LAN et WAN dans TON labo

```
ipconfig /all
```

Affiche les cartes, leurs IP, masque, passerelle, DNS et l'état DHCP.

Dans ton montage, la carte qui affichait une adresse 169.254.x.x était la carte du réseau LAN isolé. Windows lui avait donné une APIPA car aucun DHCP ne lui répondait encore.

> **IMPORTANT**
>
> Une adresse 169.254.x.x est un indice "pas de DHCP disponible", pas une définition du LAN. Renomme les cartes d'après le schéma du TP : LAN pour le réseau interne ; WAN pour le réseau qui donne accès à l'extérieur/NAT.

## 2.3 Configurer le LAN

| Paramètre LAN | Valeur du TP | Pourquoi |
|---|---|---|
| IPv4 | 192.168.100.10 | Adresse fixe du serveur sur le réseau interne. |
| Masque / préfixe | Celui prévu par le plan d'adressage du TP | Définit le sous-réseau. |

| Paramètre LAN | Valeur du TP | Pourquoi |
|---|---|---|
| Passerelle | Aucune à ce stade sur le LAN isolé | La passerelle sert à joindre d'autres réseaux. On évite aussi plusieurs passerelles par défaut sur un serveur multicarte. |
| DNS | Aucun au tout début ; après installation DNS, le serveur et les clients du domaine doivent utiliser le DNS interne | AD DS dépend du DNS interne. Le DNS public sera utilisé comme redirecteur, pas comme DNS direct des clients AD. |

## 2.4 Configurer le WAN

Dans ton TP, tu reprends les paramètres vus avec ipconfig sur la carte WAN : adresse IPv4, masque, passerelle par défaut et DNS amont. Si l'adresse avait été donnée dynamiquement, la figer n'est correct que dans le cadre prévu par le labo ou si l'adresse est réservée.

> **APRÈS LA PROMOTION AD DS**
>
> Sur un contrôleur de domaine multicarte, on évite que la carte WAN s'enregistre dans le DNS du domaine. On limitera l'écoute DNS à 192.168.100.10 et on désactivera l'inscription DNS sur la carte WAN.

**Source vérifiée :** Microsoft Learn — APIPA / adressage TCP-IP automatique

**Source vérifiée :** Microsoft Learn — DNS client settings / multi-homed servers

# 3. Installer AD DS, DNS et DHCP puis créer le domaine

## 3.1 Les trois rôles en une phrase

| Rôle | Définition simple | Exemple concret |
|---|---|---|
| AD DS | Annuaire central qui stocke les utilisateurs, groupes, ordinateurs et règles d'accès du domaine. | Créer TSSR\Alice, joindre un PC au domaine, appliquer une GPO. |
| DNS | Fait la correspondance entre les noms DNS et les adresses IP, et permet à AD de localiser ses services. | srvrds.tssr.info → 192.168.100.10. |
| DHCP | Fournit automatiquement une configuration IP aux clients à partir d'une étendue. | IP + masque + éventuellement passerelle + DNS + durée de bail. |

## 3.2 Installation des rôles

1. Gestionnaire de serveur → Gérer → Ajouter des rôles et fonctionnalités.
2. Installation basée sur un rôle ou une fonctionnalité.
3. Sélectionner le serveur local.
4. Cocher : Services AD DS, Serveur DNS, Serveur DHCP. Ajouter les fonctionnalités demandées.
5. Installer.

## 3.3 Promouvoir le serveur en contrôleur de domaine

Après l'installation AD DS, le drapeau de notification propose "Promouvoir ce serveur en contrôleur de domaine". Comme il n'existe encore aucun domaine dans le TP, on crée une nouvelle forêt.

| Écran | Choix du TP | Ce que cela signifie |
|---|---|---|
| Configuration de déploiement | Ajouter une nouvelle forêt : tssr.info | Le premier domaine de la première forêt est créé. |
| Options du contrôleur de domaine | Serveur DNS : coché | Le contrôleur de domaine hébergera aussi le DNS nécessaire à AD. |
| Catalogue global (GC) | Coché | Le GC fournit une vue recherchable des objets de toute la forêt ; utile aux recherches et aux ouvertures de session. |

| Écran | Choix du TP | Ce que cela signifie |
|---|---|---|
| Nom NetBIOS | TSSR | Ancien nom court du domaine, visible par exemple dans TSSR\Utilisateur. |

**SUR tssr.info**

Le TP peut fonctionner ainsi. Mais .info n'est pas "privé". Dans un vrai SI, on préfère un nom basé sur un domaine réellement enregistré par l'organisation pour éviter les collisions de noms.

**DÉLÉGATION DNS**

Lors de la création d'une nouvelle forêt, l'assistant peut avertir qu'il ne peut pas créer une délégation DNS dans la zone parente. Si aucune zone parente DNS n'existe dans ton labo, CET avertissement précis est attendu. Cela ne veut pas dire qu'on ignore n'importe quelle erreur DNS.

**Source vérifiée :** Microsoft Learn — AD DS overview

**Source vérifiée :** Microsoft Learn — Selecting the forest root domain

# 4. Nettoyer et configurer le DNS correctement

## 4.1 Pourquoi le serveur multicarte demande de l'attention ?

Un contrôleur de domaine qui possède un LAN et un WAN peut enregistrer plusieurs adresses dans DNS. Dans ton TP, on veut que les clients du domaine trouvent SRVRDS sur l'adresse interne 192.168.100.10, pas sur l'adresse WAN.

1. Ouvrir Gestionnaire DNS → clic droit sur le serveur → Propriétés → Interfaces.
2. Choisir "Écouter uniquement sur les adresses IP suivantes".
3. Garder l'adresse LAN 192.168.100.10.
4. Sur la carte WAN : Propriétés IPv4 → Avancé → DNS → décocher "Enregistrer les adresses de cette connexion dans le système DNS".

**BUT**

Empêcher AD/DNS d'annoncer l'IP WAN comme adresse du contrôleur de domaine et éviter que des clients internes tentent de joindre le mauvais réseau.

**Source vérifiée :** Microsoft Learn — Restrict DNS to selected interfaces

**Source vérifiée :** Microsoft Learn — Unwanted NIC registration on a multihomed DC

## 4.2 Ajouter un redirecteur DNS

Un redirecteur est un serveur DNS auquel ton DNS interne envoie les requêtes qu'il ne peut pas résoudre localement. Dans le TP, 8.8.8.8 est utilisé comme DNS amont.

1. Gestionnaire DNS → clic droit sur SRVRDS → Propriétés → Redirecteurs → Modifier.
2. Ajouter 8.8.8.8 → Appliquer / OK.

**NE PAS CONFONDRE**

Les postes du domaine doivent demander les noms au DNS interne. C'est le serveur DNS interne qui peut ensuite transmettre les requêtes Internet au redirecteur 8.8.8.8.

**Source vérifiée :** Microsoft Learn — DNS Forwarding

## 4.3 Les enregistrements à connaître

| Type | Sens | Rôle |
|---|---|---|
| A | Nom → IPv4 | Associe un nom d'hôte à une adresse IPv4. |

| Type | Sens | Rôle |
|---|---|---|
| NS | Zone → serveur DNS | Indique quel(s) serveur(s) DNS font autorité pour la zone. |
| SOA | Métadonnées de zone | Indique notamment le serveur principal de référence, le numéro de série et les temporisations de la zone. |
| PTR | IPv4 → nom | Permet la résolution inversée. |

## 4.4 Zone directe : vérifier NS et SOA

Dans Zone de recherche directe → tssr.info, vérifie que l'enregistrement A de SRVRDS pointe vers 192.168.100.10. Si des adresses WAN indésirables sont présentes, supprime-les après avoir corrigé l'inscription de la carte WAN.

Dans l'enregistrement NS, le serveur de noms doit être srvrds.tssr.info et son adresse associée doit résoudre vers 192.168.100.10.

> **SOA**
>
> Le SOA contient un NOM de serveur principal, pas une IP directement. Si tu utilises "Parcourir", tu sélectionnes le serveur/FQDN correct ; son enregistrement A doit ensuite mener à 192.168.100.10.

## 4.5 Créer la zone de recherche inversée

1. Gestionnaire DNS → Zones de recherche inversée → clic droit → Nouvelle zone.
2. Type : Zone principale. Dans un domaine, on peut la stocker dans Active Directory pour bénéficier de la réplication AD et des mises à jour sécurisées.
3. Choisir le périmètre de réplication demandé dans le TP (par exemple tous les serveurs DNS du domaine).
4. Zone IPv4.
5. Saisir l'ID réseau correspondant au sous-réseau du TP.
6. Terminer puis créer/vérifier le PTR de 192.168.100.10 vers srvrds.tssr.info.

| Type de zone | Définition ultra simple |
|---|---|
| Principale | Copie modifiable de la zone. Si elle est intégrée à AD, plusieurs DC/DNS peuvent accepter les mises à jour. |
| Secondaire | Copie en lecture seule obtenue par transfert depuis une autre zone DNS. |

| Type de zone | Définition ultra simple |
|---|---|
| Stub | Petite copie qui ne garde que les informations nécessaires pour trouver les serveurs DNS faisant autorité pour l'autre zone. |

**À QUOI SERT LA ZONE INVERSÉE ?**

Elle répond à la question inverse : "Je connais 192.168.100.10, quel est son nom ?" grâce à un enregistrement PTR. Pour IPv4, Windows utilise l'espace in-addr.arpa.

**Source vérifiée :** Microsoft Learn — DNS zones

**Source vérifiée :** Microsoft Learn — Reverse lookup

**Source vérifiée :** Microsoft Learn — DNS resource records

## 4.6 Vérifier avec nslookup

```
nslookup srvrds.tssr.info
```

Attendu : le nom se résout vers 192.168.100.10.

```
nslookup 192.168.100.10
```

Attendu : la réponse inverse renvoie srvrds.tssr.info grâce au PTR.

**SI ÇA NE MARCHE PAS**

Vérifier d'abord : enregistrement A → NS/SOA → PTR → paramètres DNS du client → carte WAN qui ne doit pas s'enregistrer → cache DNS. Ne pas modifier au hasard plusieurs éléments à la fois.

# 5. Configurer DHCP : l'étendue dans le bon ordre

## 5.1 Finaliser le rôle DHCP

Après l'installation, le drapeau du Gestionnaire de serveur propose "Terminer la configuration DHCP". Dans un domaine AD, cette étape sert notamment à autoriser le serveur DHCP dans Active Directory avec les informations d'identification adéquates.

1. Cliquer sur "Terminer la configuration DHCP".
2. Utiliser les informations d'identification du domaine si l'assistant le demande.
3. Valider → Fermer.

## 5.2 Créer une nouvelle étendue IPv4

1. Outils → DHCP → développer le serveur → IPv4 → clic droit → Nouvelle étendue.
2. Nommer l'étendue.
3. Saisir la plage d'adresses et le masque.
4. Configurer les exclusions seulement si certaines adresses comprises DANS la plage ne doivent jamais être louées.
5. Laisser le délai à 0 ms si tu n'as qu'un seul serveur DHCP dans ce scénario.
6. Choisir la durée du bail.
7. Configurer les options DHCP nécessaires.

| Élément | À quoi il sert | Dans ton TP |
|---|---|---|
| Plage | Ensemble des IP que le serveur peut louer. | Prévoir 51 adresses clientes si c'est l'objectif du TP. |
| Masque | Définit le sous-réseau des clients. | Même logique que le plan d'adressage du LAN. |
| Exclusion | IP située dans la plage mais interdite à DHCP. | Aucune si la plage choisie ne chevauche pas les IP statiques. |
| Délai | Retarde la réponse DHCP ; utile dans certains montages avec plusieurs serveurs. | 0 ms avec un seul serveur. |
| Bail | Temps pendant lequel une adresse est attribuée avant renouvellement. | Valeur choisie dans le TP. |
| Passerelle (option 003) | Route vers les autres réseaux. | Omettre si le LAN est volontairement isolé et ne doit joindre aucun autre réseau. |
| DNS (option 006) | Serveur(s) DNS remis aux clients. | 192.168.100.10, le DNS interne du domaine. |
| Nom de domaine (option 015) | Suffixe DNS remis aux clients. | tssr.info. |
| WINS | Ancien service de résolution de noms NetBIOS. | Pas de serveur WINS dans ce TP. |

### 51 MACHINES : L'ERREUR "OFF-BY-ONE"

Si tu comptes une plage de valeurs sur le même dernier octet : nombre = fin − début + 1. On ajoute +1 car l'adresse de début compte aussi. Attention : l'adresse réseau et l'adresse de broadcast d'un sous-réseau ne sont pas des adresses clientes.

### PASSERELLE

"Pas de passerelle" ne signifie pas "pas d'accès distant" au sens RDS. Cela signifie surtout : les clients n'ont pas besoin de router vers un autre réseau. S'ils doivent sortir du sous-réseau, une passerelle est nécessaire.

**Source vérifiée :** Microsoft Learn — DHCP scopes

**Source vérifiée :** Microsoft Learn — Install and configure DHCP Server

# 6. Installer RDS : comprendre ce qu’on construit

## 6.1 Le vrai but de RDS

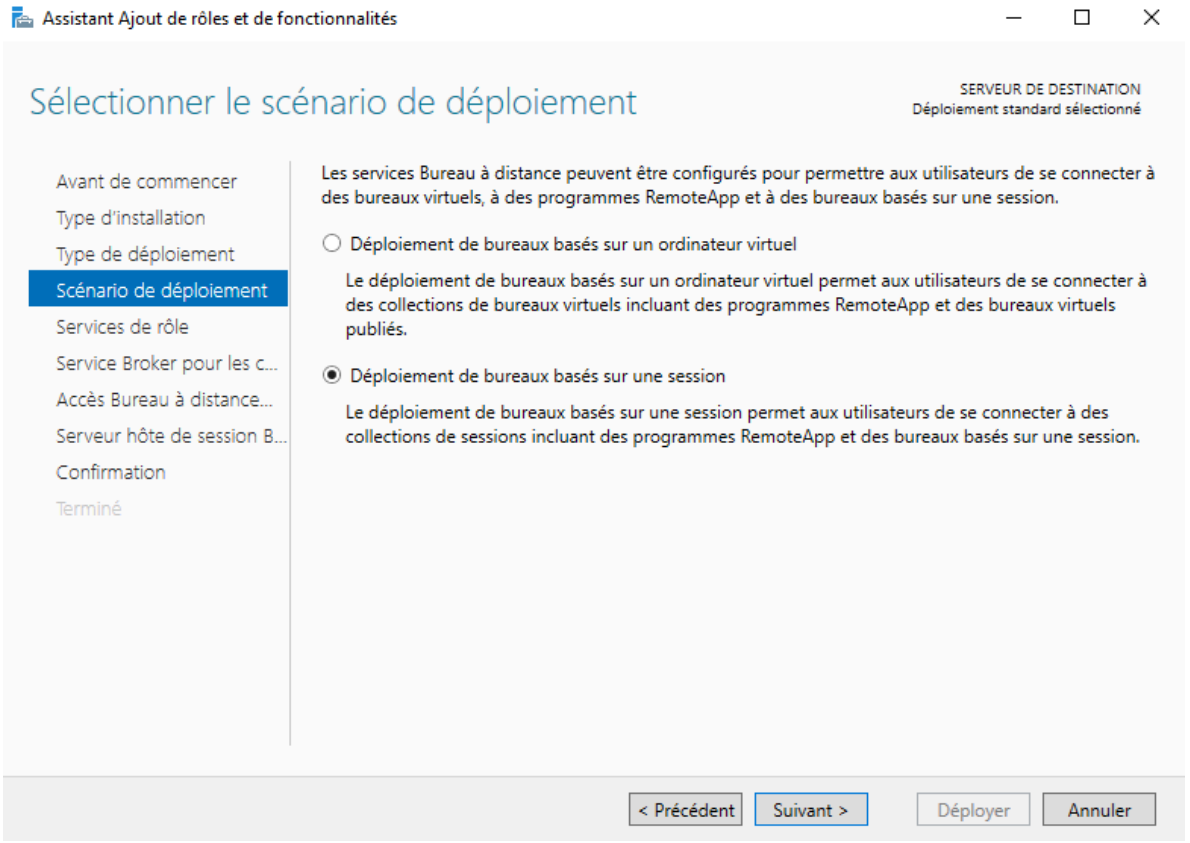
Remote Desktop Services permet à des utilisateurs autorisés d’accéder à un bureau complet ou à des applications publiées alors que l’exécution réelle se fait sur un serveur. Le poste client affiche l’interface et envoie clavier/souris via RDP. Cela centralise l’installation, les mises à jour, les calculs et les données.

> **TON IMAGE MENTALE**
>
> Le petit PC ne “fait pas tourner Paint à distance” lui-même : Paint s’exécute sur le serveur RDS. Le client reçoit principalement l’affichage et renvoie les entrées utilisateur.

**Source vérifiée :** Microsoft Learn — Remote Desktop Services overview

## 6.2 Session-based ou VDI ?

| Scénario | Principe | Choix du TP |
|---|---|---|
| Déploiement basé sur une session | Plusieurs utilisateurs ouvrent des sessions sur un ou plusieurs Windows Server RD Session Host. | OUI — c’est celui de tes captures. |
| Déploiement basé sur des ordinateurs virtuels (VDI) | Les utilisateurs reçoivent des bureaux exécutés dans des VM dédiées/pooled. | NON dans cette séquence. |

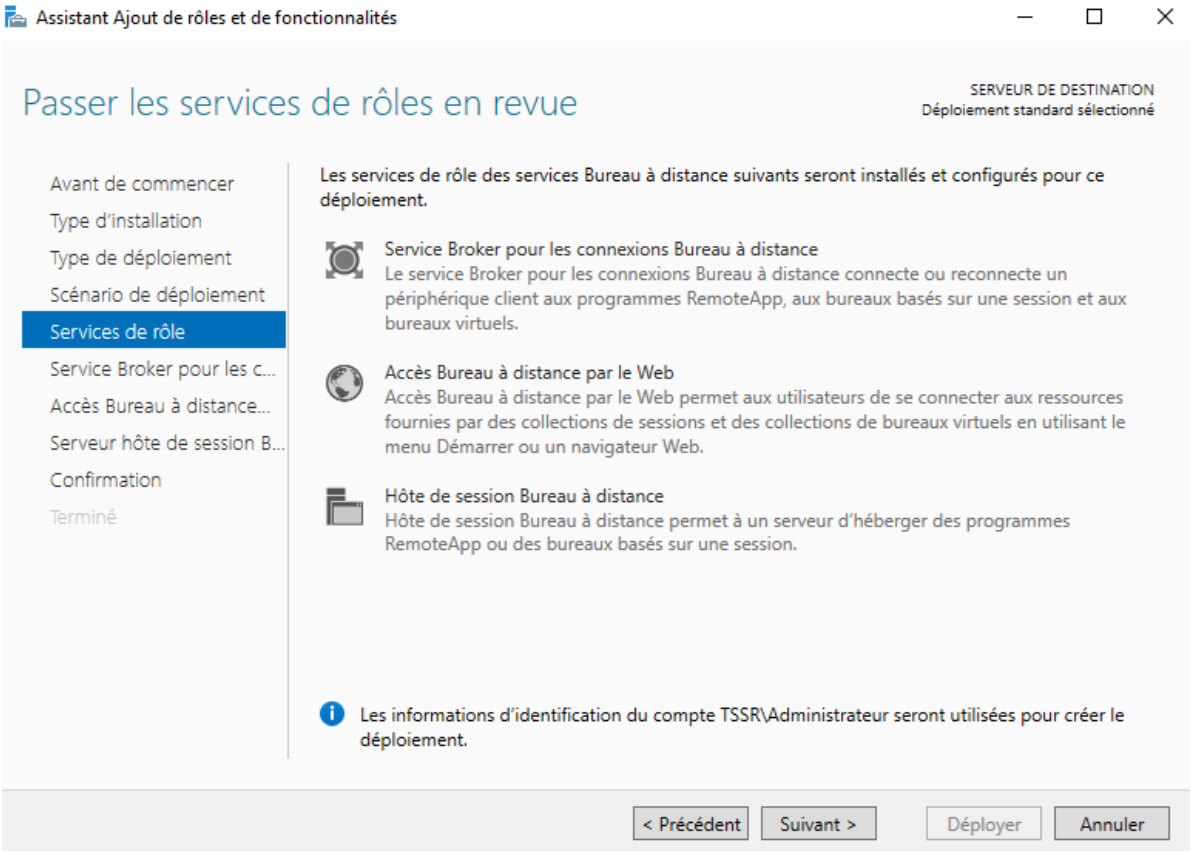



**Capture 1 — Choisir “Déploiement de bureaux basés sur une session”.**

*La première option correspond au VDI. La seconde correspond au RDS Session Host classique utilisé dans le TP.*

## 6.3 Les trois services de rôle installés

| Service de rôle | Rôle |
|---|---|
| RD Connection Broker | Orchestre les connexions, reconnecte un utilisateur à sa session existante et répartit les nouvelles connexions entre hôtes si plusieurs existent. |
| RD Web Access | Expose les bureaux et RemoteApps via un portail Web. |
| RD Session Host | Héberge réellement les sessions utilisateurs et exécute les applications. |

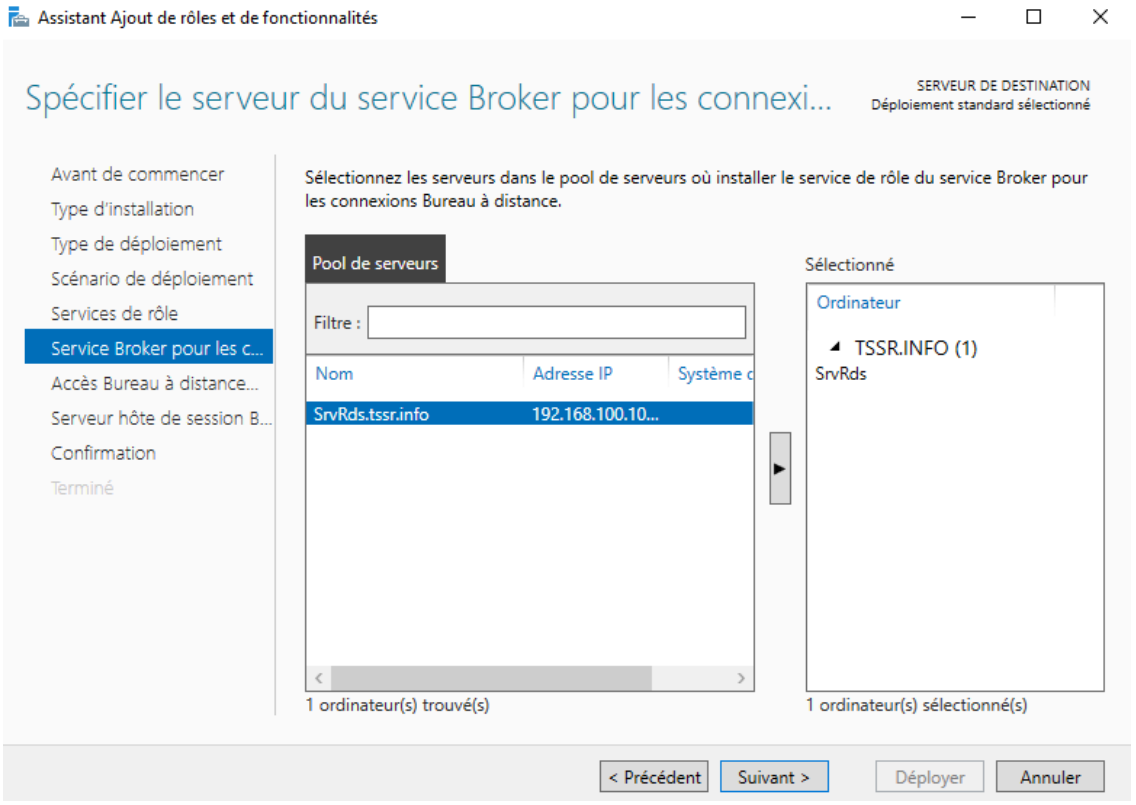



**Capture 2 — Services de rôle du déploiement basé sur une session.**

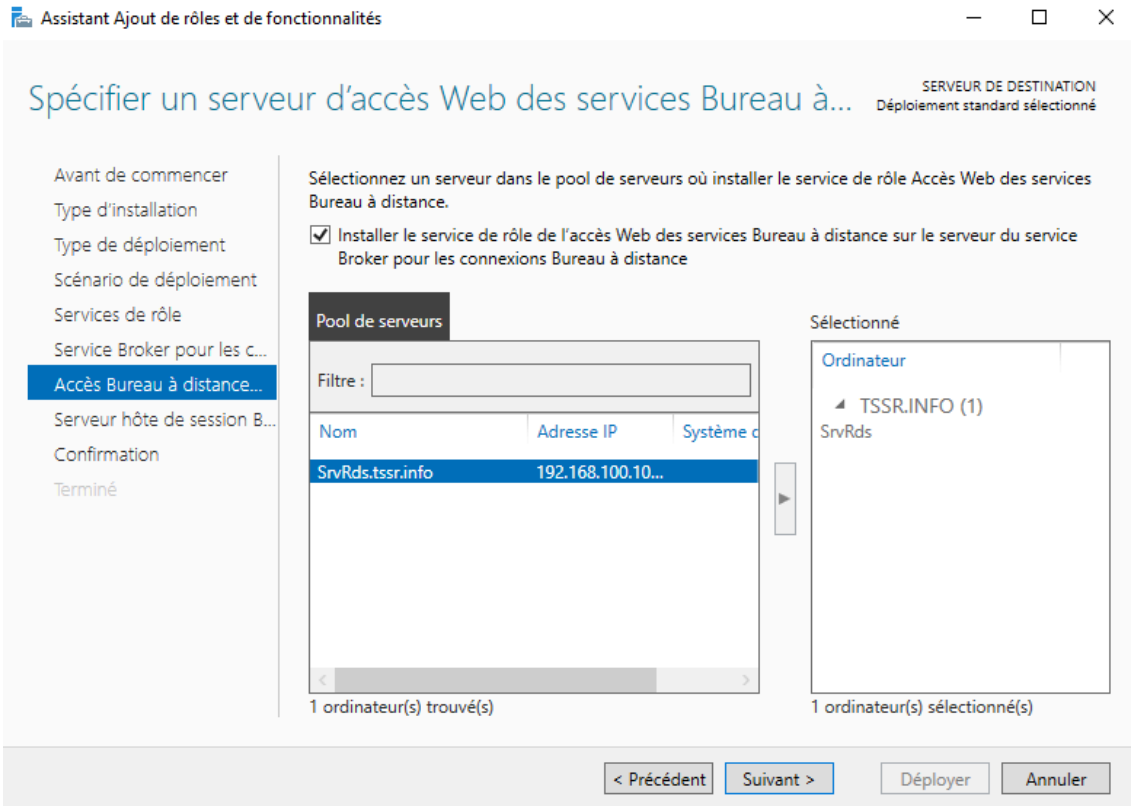
**Source vérifiée :** Microsoft Learn — RDS deployment infrastructure

## 6.4 Dans le TP : les trois rôles sur SRVRDS

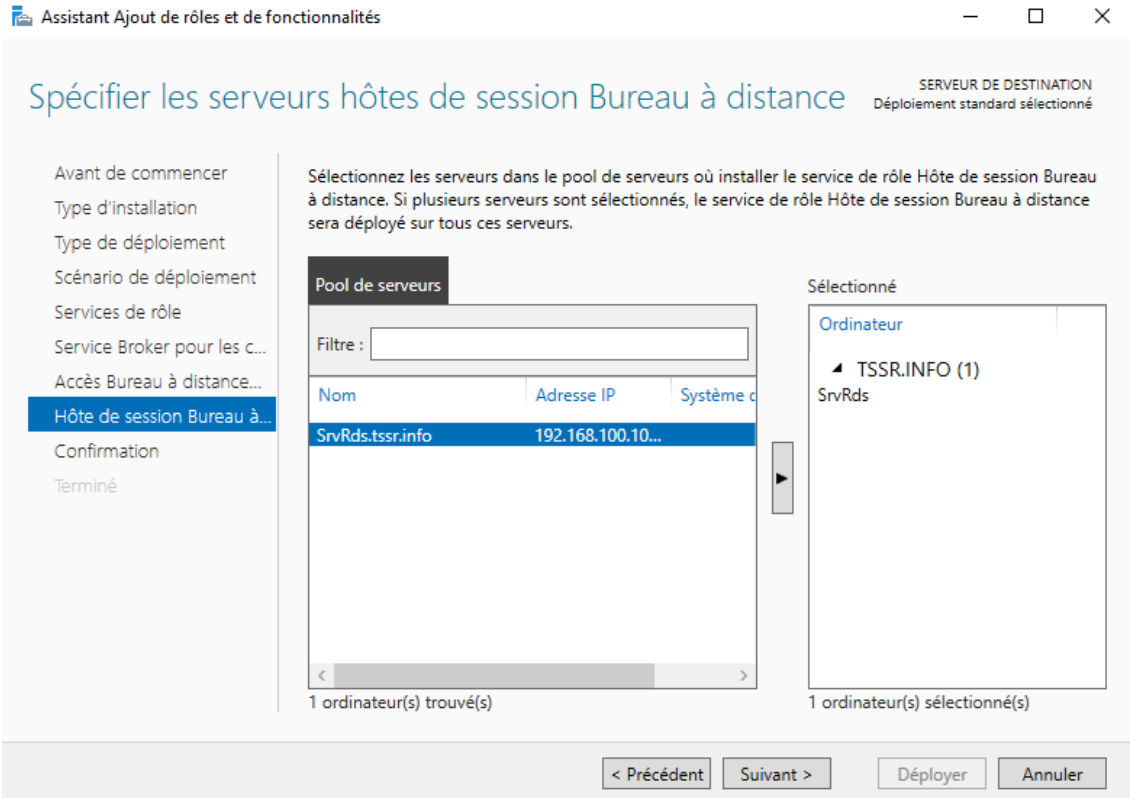
L'assistant demande successivement quel serveur doit recevoir le Broker, RD Web Access et l'Hôte de session. Dans ton labo, SRVRDS.TSSR.INFO est sélectionné pour les trois.




**Capture 3 — SRVRDS sélectionné comme RD Connection Broker.**




**Capture 4 — RD Web Access installé sur le même serveur que le Broker.**



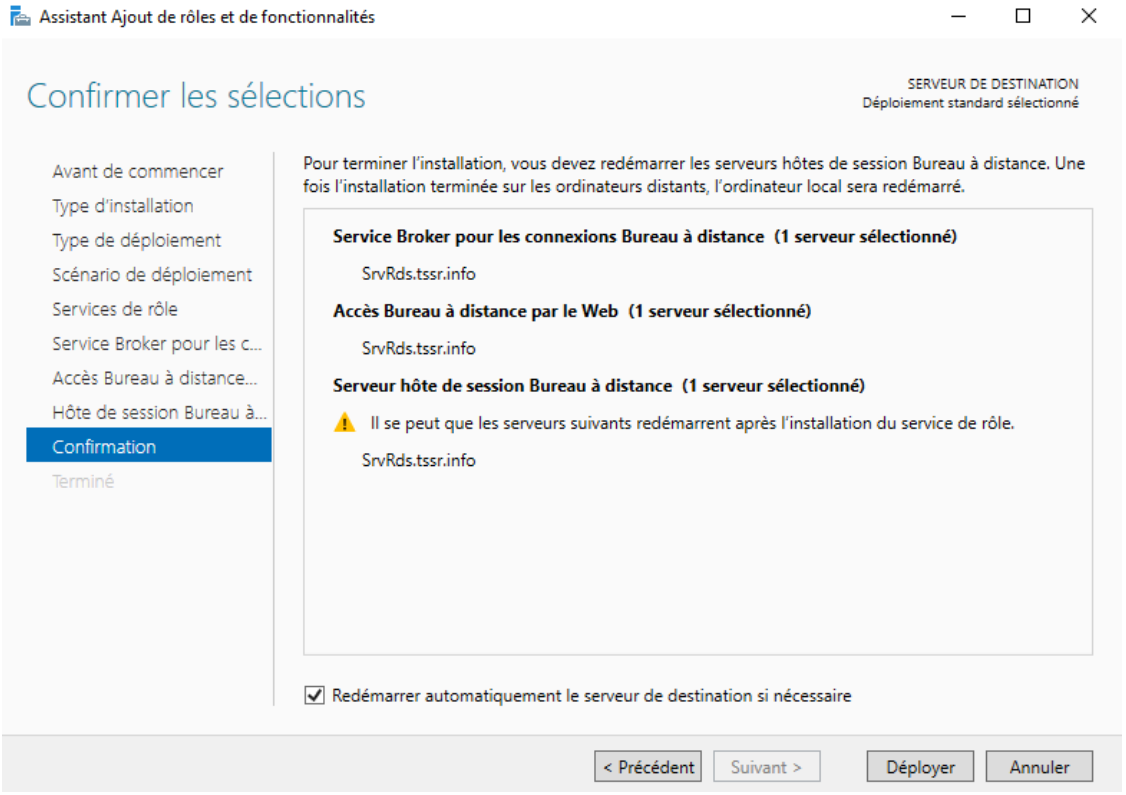

**Capture 5 — SRVRDS sélectionné comme RD Session Host.**

**PRODUCTION**

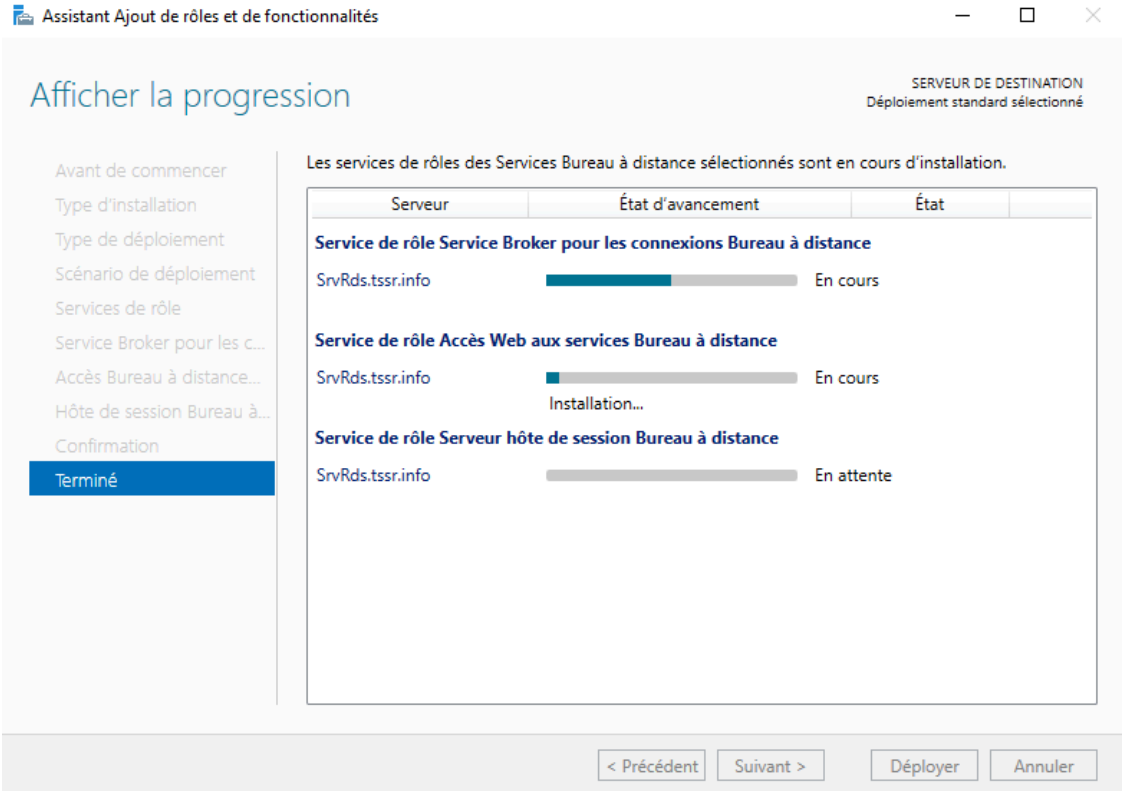
Mettre Broker, Web Access, Session Host, contrôleur de domaine et CA sur la même machine simplifie un labo, mais augmente fortement l'impact d'une panne ou d'une compromission. On sépare normalement les responsabilités.

## 6.5 Confirmation et redémarrage

Cocher "Redémarrer automatiquement le serveur de destination si nécessaire", puis Déployer. L'hôte de session peut nécessiter un redémarrage pour terminer l'installation.




**Capture 6 — Confirmation des trois services de rôle.**

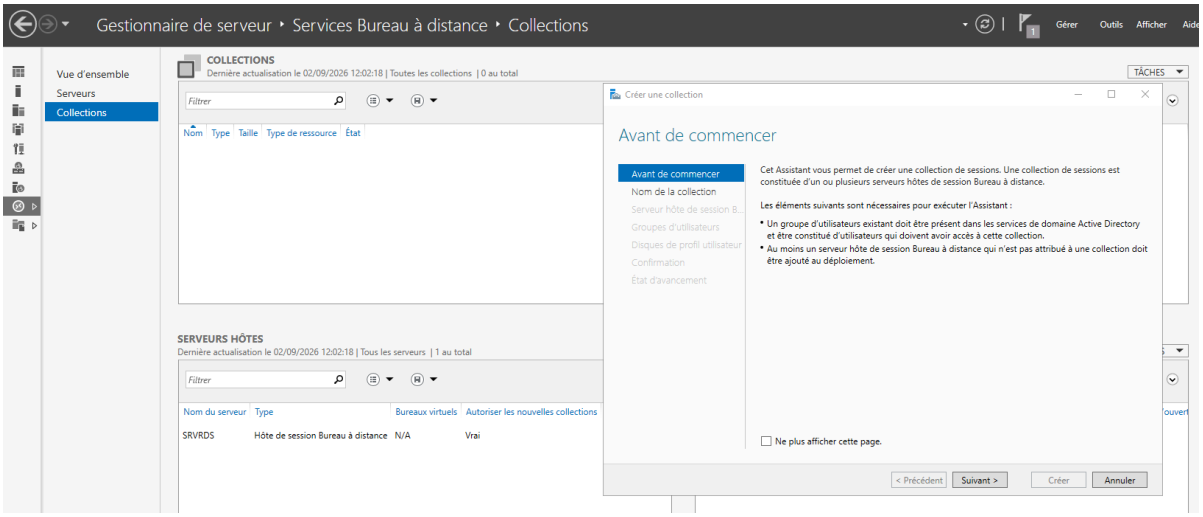



**Capture 7 — Installation RDS en cours.**

# 7. Collections et RemoteApp : qui accède à quoi ?

## 7.1 Une collection RDS, ce n’est pas juste un partage

Une collection de sessions regroupe les hôtes de session, les utilisateurs/groupes autorisés et les ressources publiées (bureaux/RemoteApps) qui vont ensemble. Le Broker s’appuie sur cette collection pour diriger les connexions.




**Capture 8 — Assistant “Créer une collection”.**

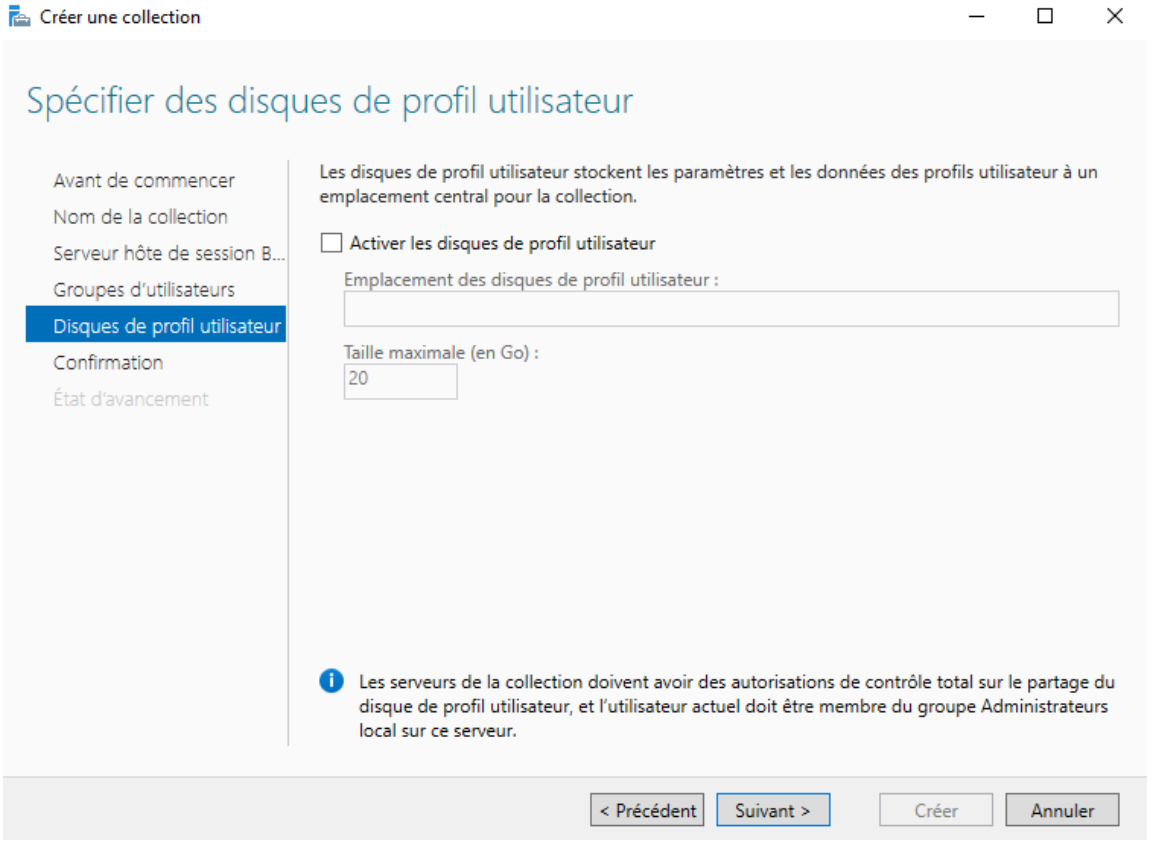
### DANS TON TP

“Collection TSSR” représente l’ensemble de ressources RDS auxquelles le groupe choisi pourra accéder. La capture montre “Utilisateurs du domaine”, ce qui est large ; en entreprise on préfère souvent un groupe AD dédié.

## 7.2 Disques de profil utilisateur (UPD)

Un User Profile Disk est un fichier VHD/VHDX par utilisateur stocké sur un partage central. Il est monté à l’ouverture de session pour conserver le profil et les paramètres d’un utilisateur au sein de la collection.

Dans ton TP, la case est laissée décochée : aucun emplacement central ni taille de disque de profil n’est donc à définir.

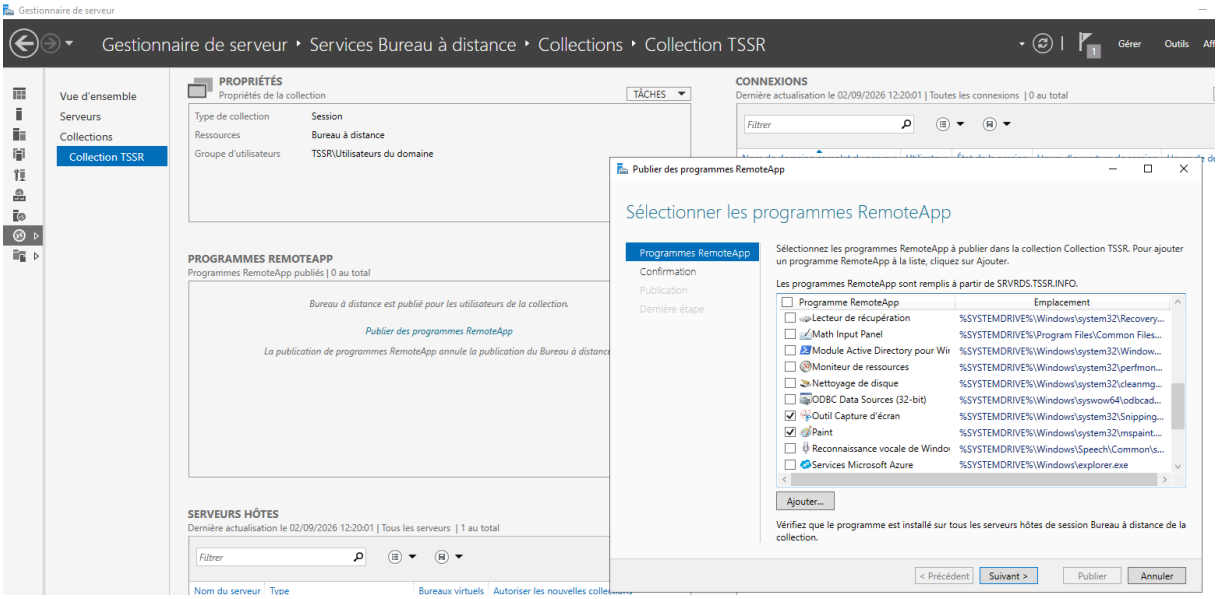



**Capture 9 — Disques de profil utilisateur laissés désactivés.**

**Source vérifiée :** [Microsoft Learn — User Profile Disks / secure data storage]

## 7.3 Publier les RemoteApps

1. Gestionnaire de serveur → Services Bureau à distance → Collections → Collection TSSR.
2. Programmes RemoteApp → Tâches / Publier des programmes RemoteApp.
3. Sélectionner les applications installées sur le RD Session Host (ex. Paint, Outil Capture d'écran).
4. Publier.



**Capture 10 — Sélection de programmes RemoteApp à publier.**

## POURQUOI ?

L’application reste installée et exécutée sur le serveur RDS. L’utilisateur autorisé la lance depuis RD Web / le client RDS et l’utilise comme une application distante.

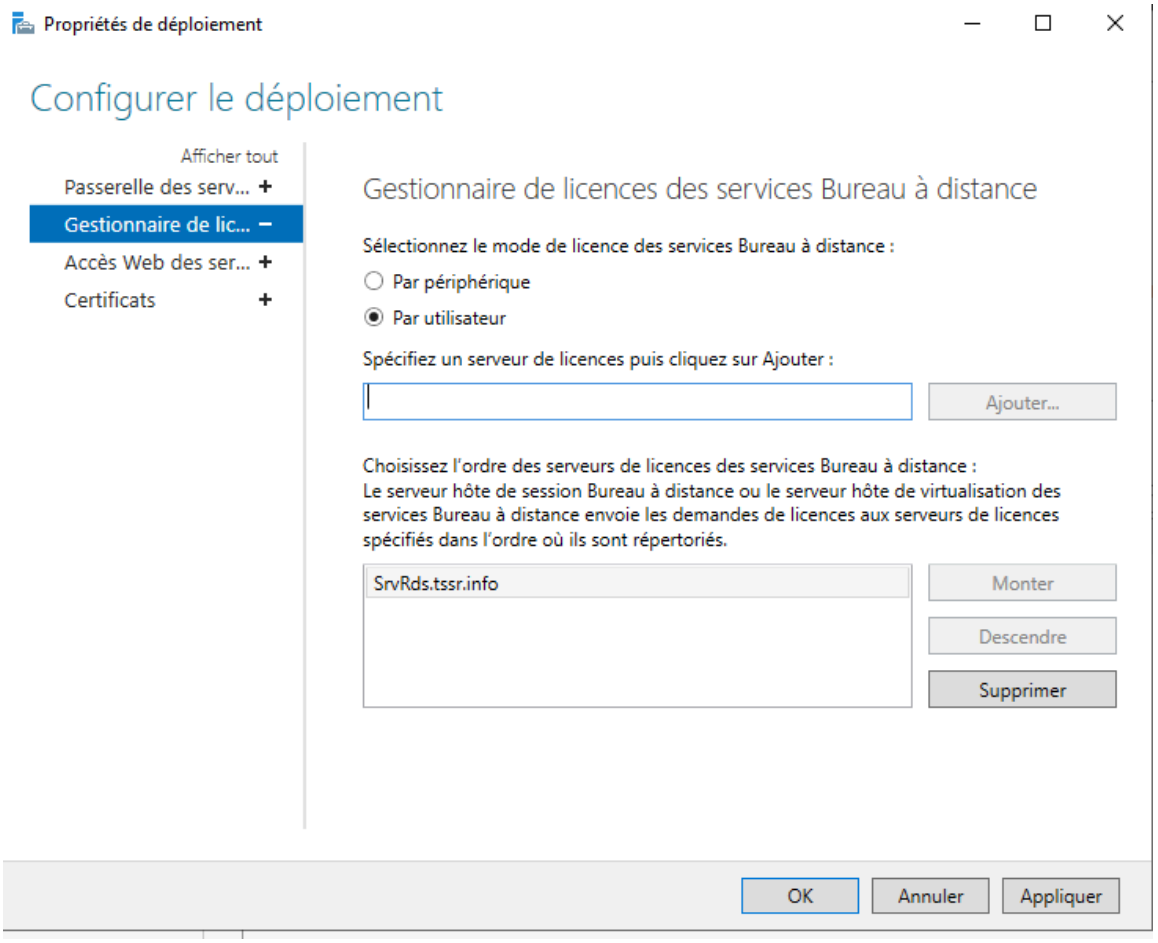
**Source vérifiée :** Microsoft Learn — Create an RDS collection and publish RemoteApps

# 8. Licences RDS et premier certificat

## 8.1 Ajouter et configurer le serveur de licences

Un environnement RDS de production a besoin d'un serveur de licences RDS activé et de CAL RDS adaptées. Il existe deux modes : Par utilisateur et Par périphérique.

1. Ajouter le service de rôle RD Licensing au serveur prévu.
2. Activer le serveur de licences dans le Gestionnaire de licences RDS.
3. Installer les CAL RDS acquises.
4. Dans Services Bureau à distance → Vue d'ensemble → Tâches → Modifier les propriétés du déploiement → Gestionnaire de licences : choisir le mode (dans ton TP : Par utilisateur) et ajouter SRVRDS.




**Capture 11 — Mode de licence "Par utilisateur" et serveur SRVRDS.**

**IMPORTANT**

Ajouter simplement le nom du serveur dans cette fenêtre ne crée pas des licences. En production, le serveur RD Licensing doit être activé et recevoir des CAL RDS. Microsoft prévoit une période de grâce de 120 jours pour un nouvel hôte de session.

**Source vérifiée :** Microsoft Learn — RDS CAL model

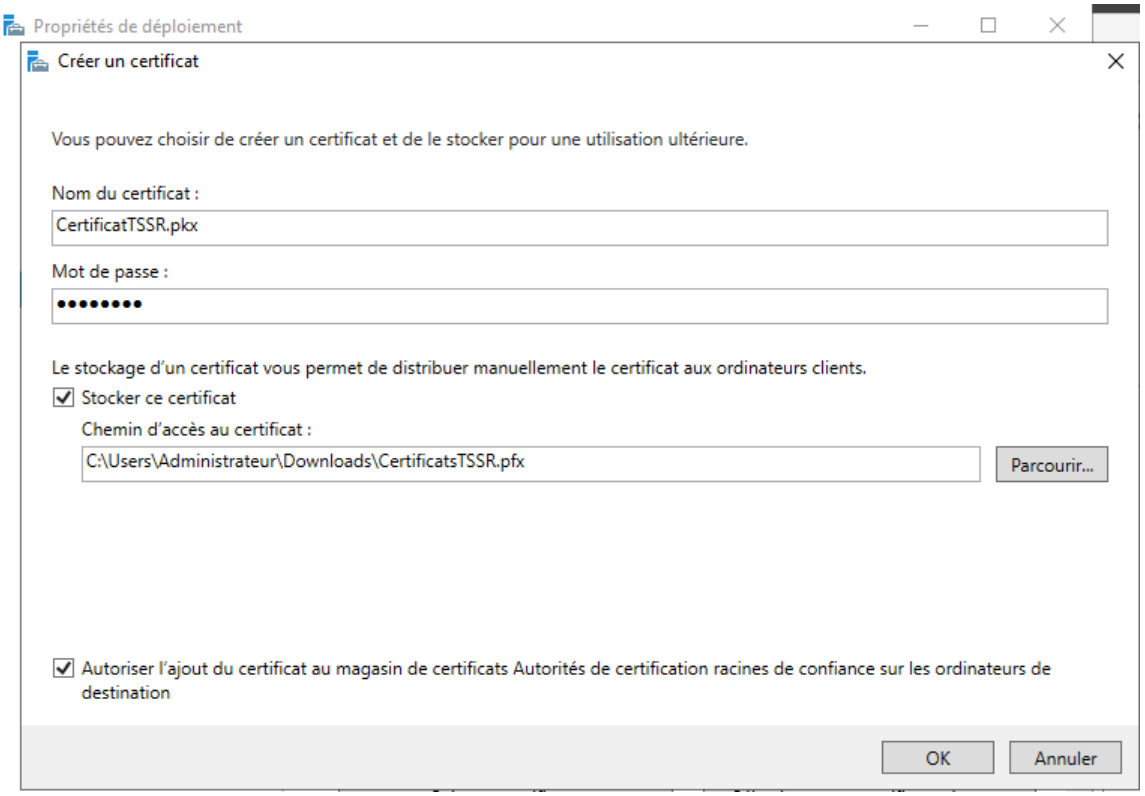
Source vérifiée : Microsoft Learn — License RDS session hosts

## 8.2 Le certificat RDS temporaire / auto-signé

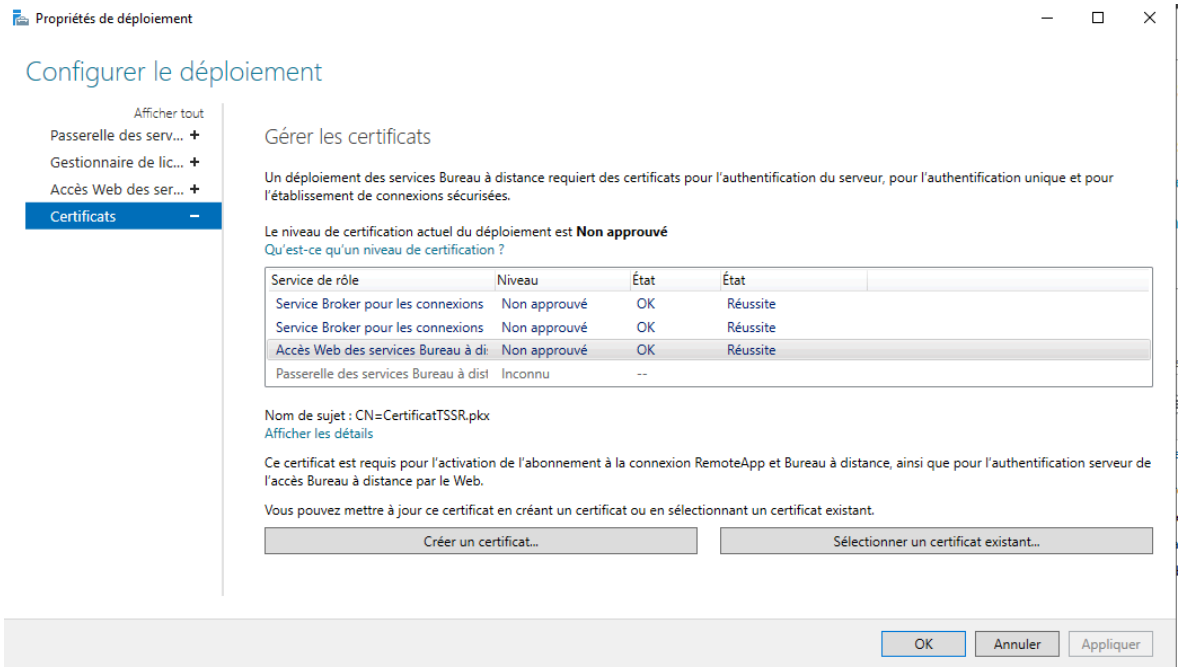
RDS peut utiliser un certificat créé depuis les propriétés du déploiement. Ce type de certificat permet de mettre le service en place, mais un certificat auto-signé est généralement marqué “Non approuvé” par les clients qui ne lui font pas confiance.

**EXTENSION CORRECTE**

Le chemin de ta capture se termine bien par CertificatTSSR.pfx. Si le champ “Nom du certificat” contient “.pkx”, c’est une faute de frappe : le format attendu est .PFX.




**Capture 12 — Création d’un certificat RDS et stockage en .pfx.**

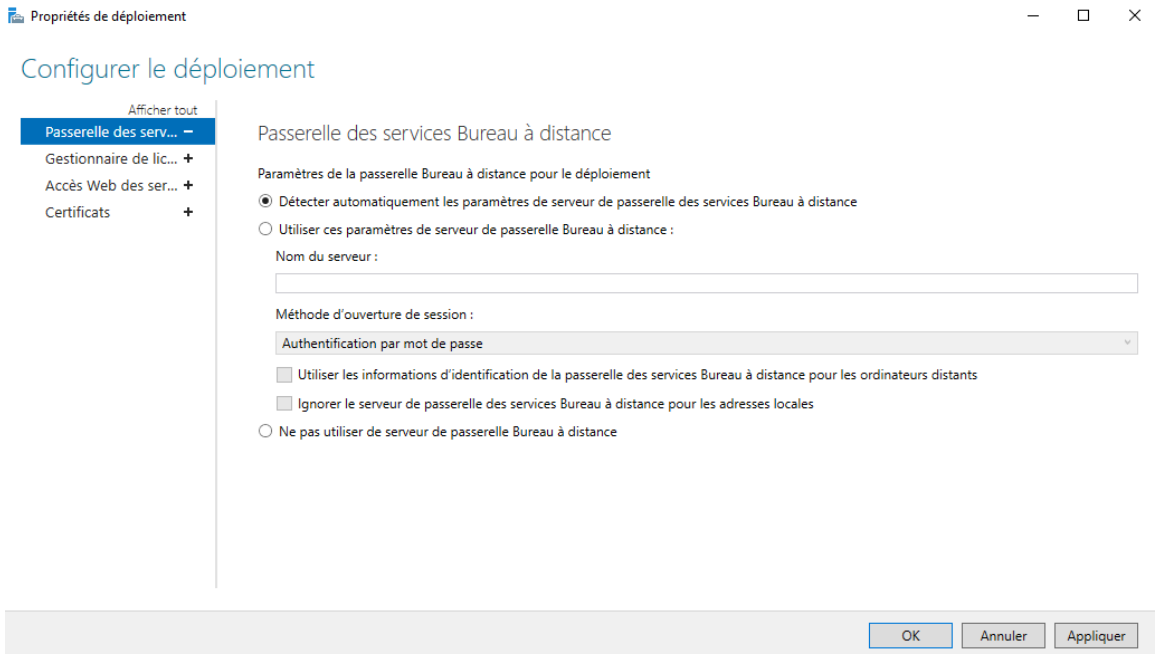



**Capture 13 — Les rôles RDS indiquent encore un niveau “Non approuvé”.**

**Source vérifiée :** Microsoft Learn — Use certificates in Remote Desktop Services

## 8.3 Passerelle RDS et RD Web Access

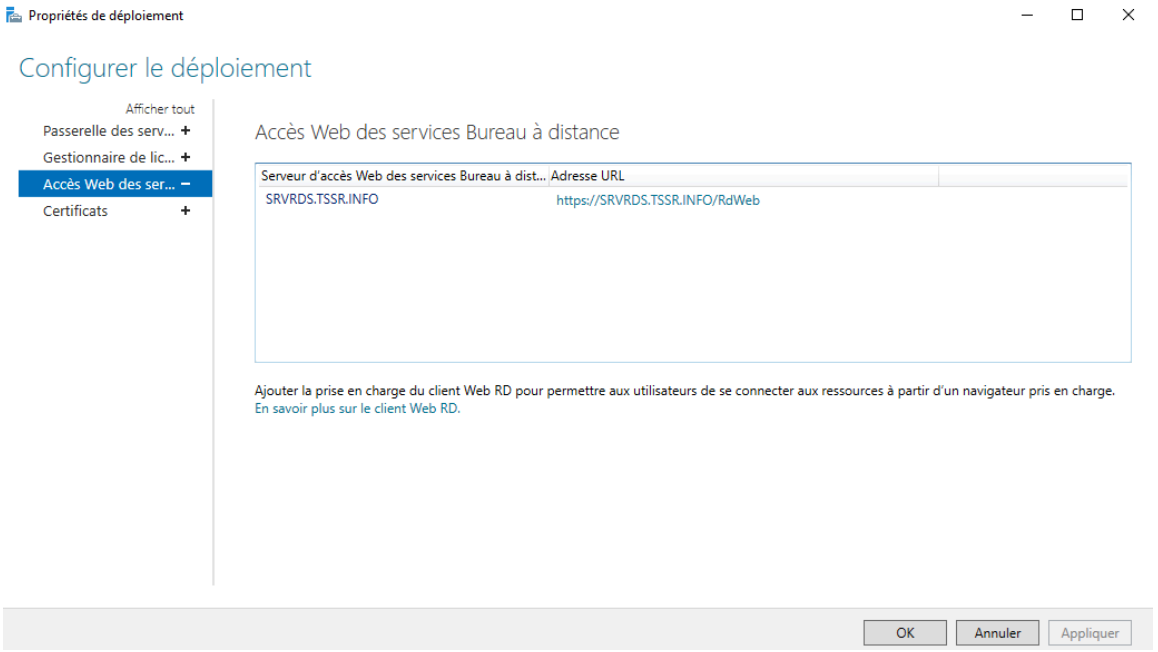
RD Gateway sert surtout à fournir un accès RDP sécurisé à travers HTTPS depuis l’extérieur. Dans un labo interne qui n’utilise pas le rôle Gateway, ce réglage n’est pas indispensable. Ta capture montre l’option de détection automatique.



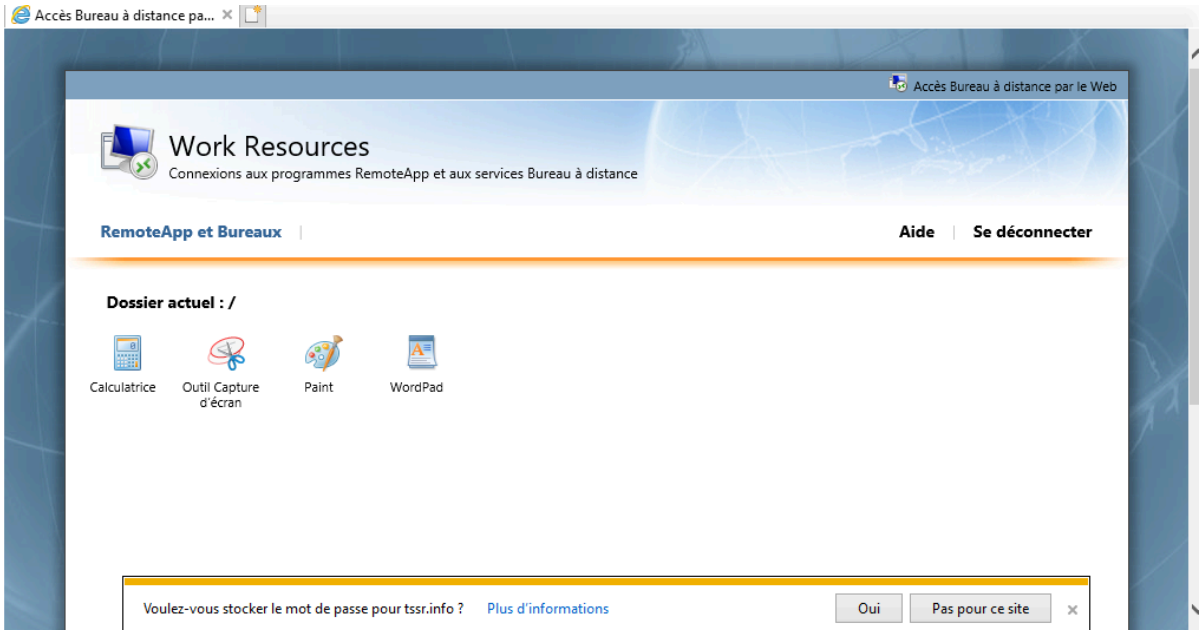

**Capture 14 — Paramètres de passerelle RDS en détection automatique.**

RD Web Access expose ensuite les ressources via une URL HTTPS. Dans tes captures :

```
https://SRVRDS.TSSR.INFO/RdWeb
```




**Capture 15 — URL RD Web Access du déploiement.**




**Capture 16 — RD Web affiche les RemoteApps publiées.**

**SI LE NAVIGATEUR DIT “SITE NON SÉCURISÉ”**

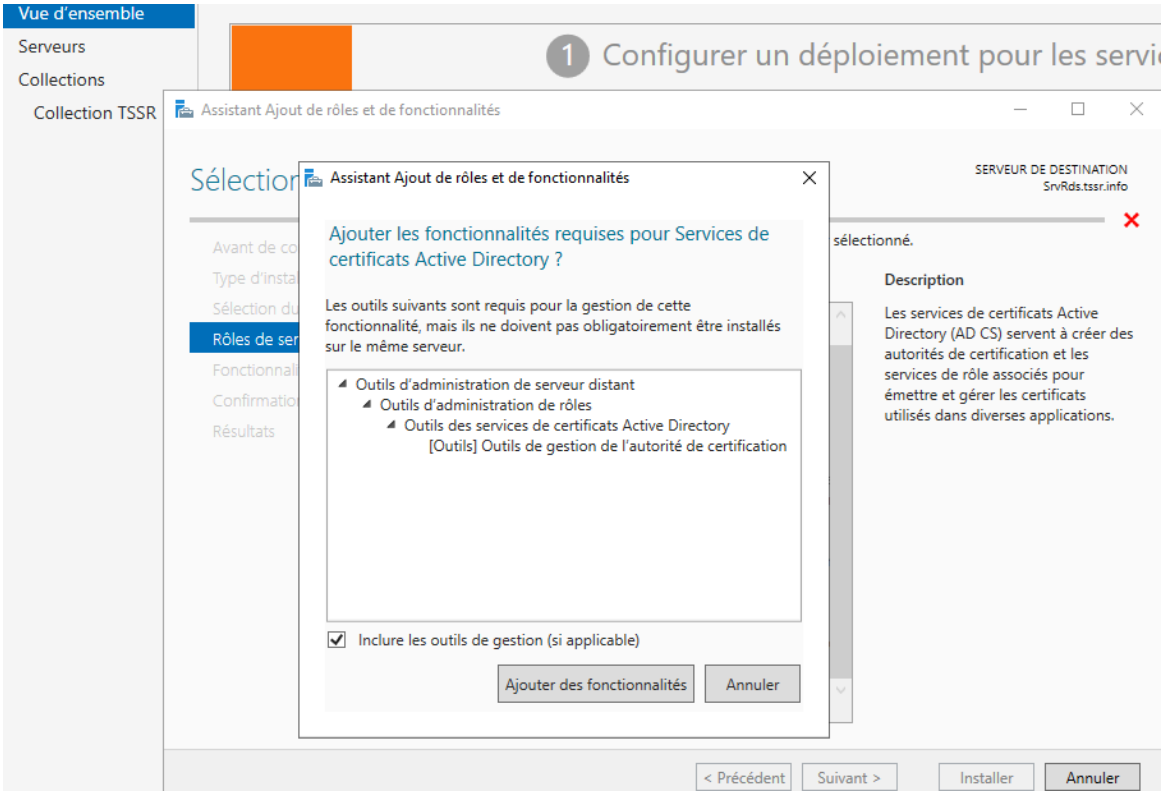
Vérifie la chaîne de confiance du certificat et le nom du certificat. Le certificat présenté doit être approuvé par le client et correspondre au FQDN utilisé dans l’URL. Il n’existe pas de délai fixe de 24 h.

# 9. Installer AD CS : créer une vraie autorité de certification interne

## 9.1 À quoi sert AD CS ?

Active Directory Certificate Services fournit une infrastructure PKI : il permet d'émettre et de gérer des certificats pour l'authentification, le chiffrement, les signatures et les connexions TLS. Ici, le but est d'émettre un certificat RDS approuvé par les machines du domaine.

1. Gestionnaire de serveur → Ajouter des rôles et fonctionnalités.
2. Cocher "Services de certificats Active Directory (AD CS)" → Ajouter les fonctionnalités.
3. Installer le rôle.

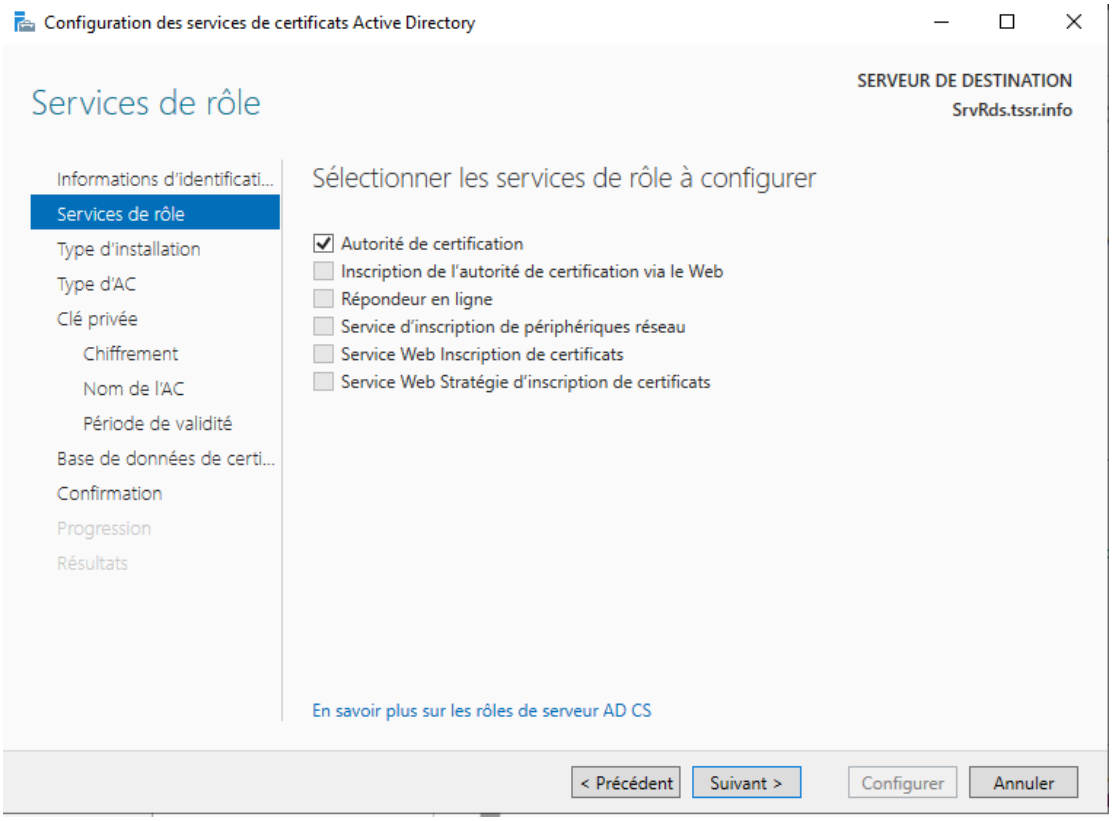



**Capture 17 — Ajout du rôle AD CS et de ses outils de gestion.**

**Source vérifiée :** Microsoft Learn — Active Directory Certificate Services overview

## 9.2 Service de rôle : Autorité de certification

Dans ton TP, le service de rôle indispensable est "Autorité de certification". Il permet à ce serveur de devenir une AC et d'émettre des certificats.



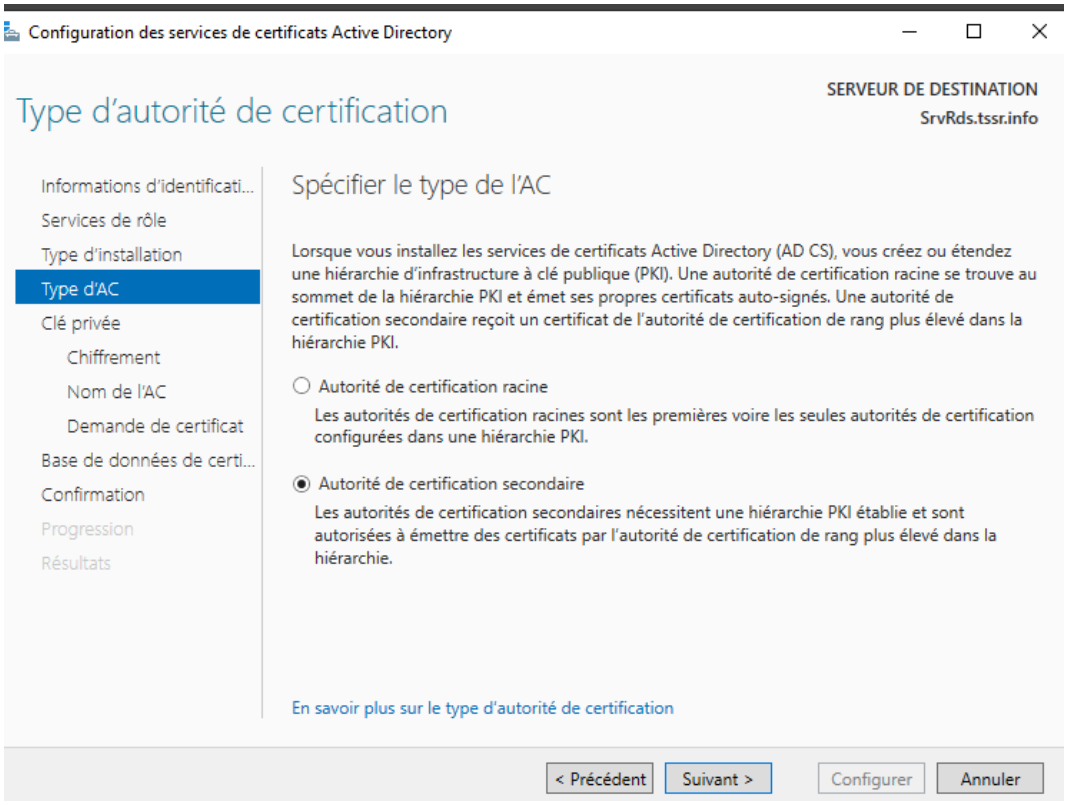

**Capture 18 — Service de rôle “Autorité de certification” sélectionné.**

## 9.3 Entreprise ou autonome ? Racine ou secondaire ?

| Question | Choix correct dans ce labo | Pourquoi |
|---|---|---|
| Type d’installation de l’AC | AC d’entreprise (Enterprise CA) | Le serveur est membre du domaine et on veut utiliser AD DS, les modèles de certificats et l’inscription. |
| Position dans la hiérarchie | AC racine (Root CA) SI c’est la première AC et qu’aucune AC parente n’existe | Une AC racine est au sommet de la chaîne. Une AC secondaire doit recevoir son certificat d’une AC parente. |

**TA CAPTURE**

La capture “Type d’AC” montre “Autorité de certification secondaire” sélectionnée. Si ce serveur est réellement la toute première AC de ton labo, ce choix n’est pas cohérent : il faut Racine. “Racine” n’est pas choisi “parce qu’on est entreprise”, mais parce qu’il n’y a pas d’AC parente.

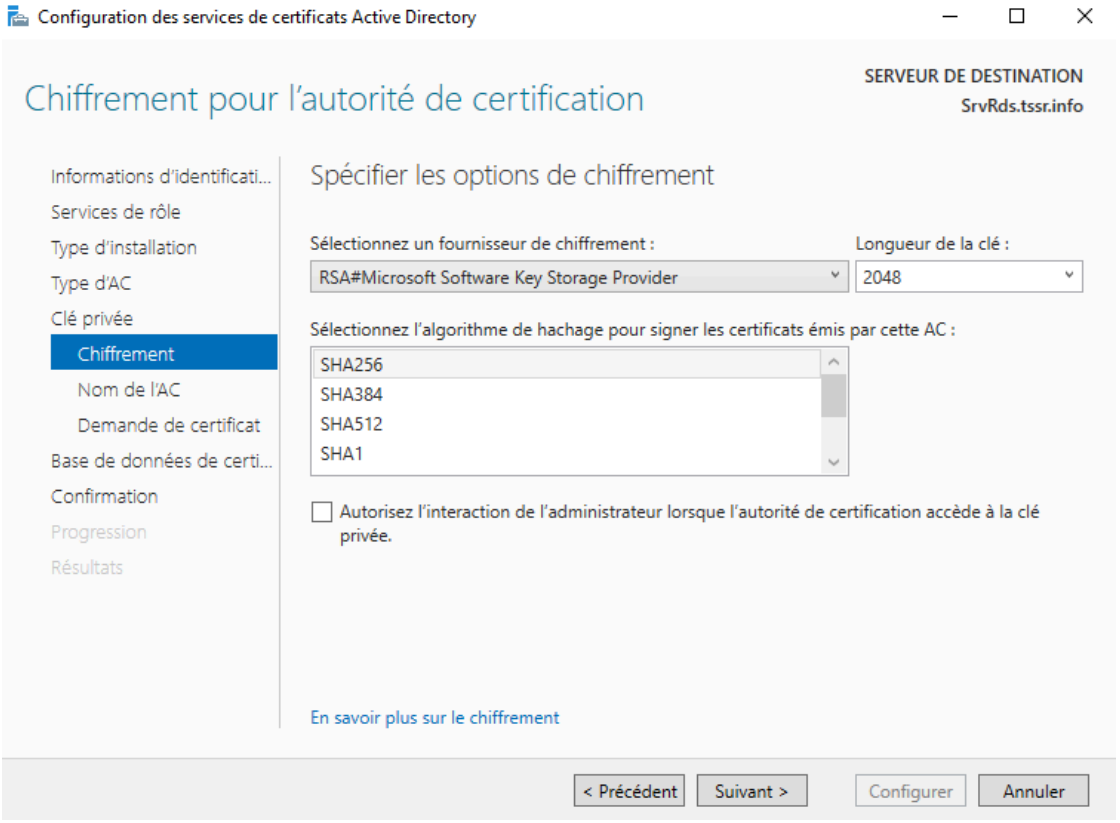



**Capture 19 — Écran Racine / Secondaire. Vérifier le choix selon la hiérarchie réelle.**

**Source vérifiée :** Microsoft Learn — Certification Authority role / CA types

## 9.4 Clé privée et algorithmes

1. Choisir “Créer une nouvelle clé privée” pour une nouvelle AC.
2. Fournisseur : un fournisseur RSA Microsoft adapté au système.
3. Longueur : 2048 bits dans ton TP.
4. Algorithme de hachage de signature : SHA256.




**Capture 20 — RSA 2048 bits + SHA256 dans l'assistant AD CS.**

## VOCABULAIRE

RSA = algorithme asymétrique basé sur une paire clé privée / clé publique.
SHA-256 = fonction de hachage utilisée dans la signature. Ce ne sont pas deux "chiffrements" équivalents.

Ensuite : définir le nom de l'AC, sa période de validité et les emplacements de la base de données / journaux. Dans un labo, on peut garder les emplacements par défaut sauf consigne contraire.

# 10. Créer un modèle de certificat RDS avec MMC

## 10.1 Ouvrir le magasin de certificats de l’ordinateur

```
Win + R  →  mmc
```

1. Fichier → Ajouter/Supprimer un composant logiciel enfichable.
2. Certificats → Ajouter.
3. Compte d’ordinateur → Suivant.
4. Ordinateur local → Terminer → OK.

**POURQUOI “COMPTE D’ORDINATEUR” ?**

Le certificat RDS représente le serveur, pas un utilisateur connecté. Il doit donc se trouver dans le magasin de certificats de l’ordinateur local avec sa clé privée.

## 10.2 Dupliquer le modèle “Serveur Web”

1. Ouvrir l’Autorité de certification → Modèles de certificats → Gérer.
2. Clic droit sur “Serveur Web” → Dupliquer le modèle.
3. Onglet Général → nom d’affichage : CertificatRDS.
4. Onglet Traitement de la demande → autoriser l’exportation de la clé privée si le certificat doit être exporté en PFX puis appliqué aux rôles RDS.
5. Onglet Sécurité → accorder Lecture + Inscrire (Enroll) au serveur ou au groupe de serveurs qui doivent recevoir le certificat.
6. Auto-inscription : ne cocher Autoenroll que si tu as réellement configuré la GPO d’auto-inscription. Pour une demande manuelle, Enroll suffit.
7. Onglet Nom du sujet → pour un certificat d’ordinateur/serveur, inclure le nom DNS/FQDN du serveur. Le FQDN utilisé par les clients doit correspondre au certificat.

**UPN**

Le “Nom principal de l’utilisateur (UPN)” sert aux identités utilisateur. Pour un certificat de serveur RDS basé sur un compte ordinateur, le nom DNS/FQDN est l’information essentielle ; cocher UPN n’est pas nécessaire.

**Source vérifiée :** Microsoft Learn — Certificate template concepts

**Source vérifiée :** Microsoft Learn — RDS certificate requirements

## 10.3 Les onglets du modèle : ce qu'ils veulent dire

| Onglet | Définition simple |
|---|---|
| Conditions d'émission | Règles supplémentaires avant qu'une demande soit délivrée : approbation du gestionnaire, signatures autorisées, etc. Dans un labo simple, on n'ajoute généralement pas d'approbation manuelle sauf consigne. |
| Modèles obsolètes / Superseded Templates | Indique quels anciens modèles ce nouveau modèle remplace. Utile lors d'une migration/évolution de modèles. |
| Extensions | Définit les usages et propriétés X.509 : Key Usage, Enhanced Key Usage (EKU), contraintes, stratégies, etc. Pour RDS, "Server Authentication" doit être présent. |
| Chiffrement / Cryptography | Définit la famille d'algorithmes, le fournisseur de clé et la taille minimale de clé pour les certificats issus du modèle. |
| Traitement de la demande | Définit l'usage de la clé et des options comme l'export de la clé privée. |
| Sécurité | Définit QUI peut lire le modèle, demander un certificat et éventuellement s'inscrire automatiquement. |
| Nom du sujet | Détermine comment le Subject et le Subject Alternative Name sont construits. Pour un serveur, le nom DNS est central. |

**SÉCURITÉ**

Donner Enroll/Autoenroll à "Utilisateurs authentifiés" est beaucoup trop large pour une infrastructure réelle. Pour un TP, suis la consigne du formateur ; en production, cible un groupe de serveurs RDS ou le compte ordinateur concerné.

## 10.4 Publier le nouveau modèle sur l'AC

1. Console Autorité de certification → clic droit "Modèles de certificats".
2. Nouveau → Modèle de certificat à délivrer.
3. Sélectionner CertificatRDS → OK.

**POURQUOI ?**

Dupliquer un modèle dans la console "Modèles de certificats" ne suffit pas. Il faut aussi l'autoriser sur l'autorité de certification pour que celle-ci puisse réellement l'émettre.

**Source vérifiée :** Microsoft Learn — Manage certificate templates

# 11. Demander, exporter et appliquer le certificat RDS

## 11.1 Demander le certificat

1. MMC → Certificats (ordinateur local) → Personnel → Certificats.
2. Clic droit → Toutes les tâches → Demander un nouveau certificat.
3. Sélectionner le modèle CertificatRDS → Inscrire / Enroll → Terminer.

Avant d'exporter, ouvre le certificat et vérifie :

- Usage prévu : Server Authentication.
- Nom/SAN DNS : srvrds.tssr.info (ou le FQDN réellement utilisé par les clients).
- Une clé privée est associée au certificat.
- La chaîne remonte vers ton AC d'entreprise.

## 11.2 .CER DER ou .PFX ?

| Format | Contenu | Quand l'utiliser |
|---|---|---|
| .CER en DER | Certificat public uniquement. Pas de clé privée. | Diffuser la partie publique / la racine de confiance. |
| .PFX / PKCS #12 | Certificat + clé privée + éventuellement chaîne de certification. | Appliquer un certificat serveur à RDS ou migrer le certificat avec sa clé privée. |

## 11.3 Exporter en PFX avec la clé privée

1. Clic droit sur le certificat → Toutes les tâches → Exporter.
2. Oui, exporter la clé privée.
3. Format : Échange d'informations personnelles — PKCS #12 (.PFX).
4. Inclure la chaîne de certification si possible.
5. Protéger la clé privée avec un mot de passe.
6. Méthode de chiffrement proposée par Microsoft : AES256-SHA256.
7. Enregistrer par exemple : CertificatRDS.pfx.

**Source vérifiée :** Microsoft Learn — Export a certificate with its private key

## 11.4 Appliquer le PFX aux rôles RDS

1. Gestionnaire de serveur → Services Bureau à distance → Vue d'ensemble → Tâches → Modifier les propriétés du déploiement.
2. Certificats → sélectionner le rôle → "Sélectionner un certificat existant".
3. Choisir CertificatRDS.pfx et saisir son mot de passe.
4. Appliquer au minimum aux rôles présents : RD Web Access, RD Connection Broker — Publication, RD Connection Broker — Activer l'authentification

unique. Appliquer aussi à RD Gateway si ce rôle existe réellement dans le déploiement.

5. Vérifier que le niveau devient approuvé/trusted et que le navigateur ne signale plus un problème de confiance ou de nom.

> **CONFIANCE DANS LE DOMAINE**
>
> Les membres d'un domaine reçoivent automatiquement le certificat d'une AC racine d'entreprise dans leur magasin "Autorités de certification racines de confiance". Un client non joint au domaine devra recevoir cette racine par un autre moyen.

**Source vérifiée :** Microsoft Learn — Enterprise Root CA trust for domain members

# 12. Checklist finale : savoir si la machine est réellement correcte

| Bloc | Contrôle | Résultat attendu |
|---|---|---|
| Nom / réseau | Nom SRVRDS + LAN 192.168.100.10 + WAN identifié | Aucune ambiguïté de carte réseau. |
| AD DS | Domaine tssr.info / NetBIOS TSSR | Le serveur est contrôleur de domaine et GC. |
| DNS direct | nslookup srvrds.tssr.info | Retourne 192.168.100.10. |
| DNS inverse | nslookup 192.168.100.10 | Retourne srvrds.tssr.info. |
| DNS interfaces | Serveur DNS écoute sur le LAN ; WAN non inscrit | Pas d'adresse WAN publiée par erreur. |
| Redirecteur | 8.8.8.8 configuré comme forwarder du DNS interne | Les noms Internet peuvent être résolus via le DNS interne. |
| DHCP | Étendue active + 51 IP clientes prévues + DNS interne | Un client DHCP reçoit IP/masque/DNS cohérents. |
| RDS | Session deployment + collection + RemoteApps | Les utilisateurs autorisés voient les applis publiées. |
| RDS Licensing | Serveur de licences activé + CALs en production + mode correct | Pas de panne après la période de grâce. |
| AD CS | AC Entreprise Racine si première AC | Chaîne de confiance interne opérationnelle. |
| Certificat RDS | PFX avec clé privée, Server Authentication, bon FQDN | RD Web / Broker présentent un certificat approuvé. |

## 12.1 Les 10 phrases à savoir réciter

- AD DS centralise les identités, ordinateurs, groupes et politiques du domaine.
- DNS résout les noms ; Active Directory dépend de DNS pour localiser ses services.
- Un enregistrement A fait nom → IPv4 ; un PTR fait IPv4 → nom.
- Un redirecteur DNS traite les requêtes que le serveur DNS interne ne résout pas localement.
- DHCP loue une configuration IP à partir d'une étendue et peut fournir passerelle, DNS et suffixe de domaine.
- APIPA 169.254.x.x signifie qu'un client DHCP n'a pas obtenu de bail ; ce n'est pas synonyme de LAN.
- RDS exécute bureaux et RemoteApps sur le serveur et transmet l'interface à l'utilisateur via RDP.
- Une collection RDS regroupe les hôtes, les utilisateurs autorisés et les ressources publiées.

- AD CS émet et gère des certificats ; Enterprise/Standalone et Root/Subordinate sont deux choix différents.
- Pour RDS, le certificat doit être approuvé, correspondre au FQDN, contenir Server Authentication et posséder une clé privée exportable en PFX.

## 12.2 Chemin mental de dépannage

| Symptôme | Commencer par vérifier |
|---|---|
| Le PC ne rejoint pas le domaine | DNS du client → doit pointer vers le DNS interne ; résolution du domaine ; connectivité LAN. |
| nslookup renvoie la mauvaise IP | A/NS/SOA + inscription de la carte WAN + interface d'écoute DNS. |
| La résolution inverse échoue | Zone inversée + PTR de 192.168.100.10. |
| Le client DHCP n'a pas d'IP | Étendue active, autorisation DHCP AD, plage disponible, connectivité de couche 2. |
| RemoteApp absente | Application installée sur RDSH + publiée dans la bonne collection + groupe utilisateur autorisé. |
| RDWeb affiche "non sécurisé" | Nom du certificat, date, chaîne de confiance, rôle RDS auquel le certificat est appliqué. |
| Le modèle CertificatRDS n'apparaît pas | Template publié sur l'AC + droits Read/Enroll + compatibilité du modèle + actualisation de stratégie. |

# Sources officielles vérifiées

Sources principales utilisées pour corriger et valider cette fiche. Elles proviennent de Microsoft Learn et couvrent Windows Server 2019/2022/2025 selon les pages.


1. Microsoft Learn — Locks and limits in Windows Server
2. Microsoft Learn — AD DS overview
3. Microsoft Learn — Forest root domain naming
4. Microsoft Learn — DNS quickstart / interfaces / forwarders
5. Microsoft Learn — DNS forwarding
6. Microsoft Learn — DNS zones
7. Microsoft Learn — Reverse lookup
8. Microsoft Learn — DNS resource records
9. Microsoft Learn — DHCP scopes
10. Microsoft Learn — DHCP quickstart
11. Microsoft Learn — RDS overview
12. Microsoft Learn — Deploy RDS infrastructure
13. Microsoft Learn — RDS collections
14. Microsoft Learn — RDS CALs
15. Microsoft Learn — RDS certificates
16. Microsoft Learn — AD CS overview
17. Microsoft Learn — CA role and CA types
18. Microsoft Learn — Certificate templates
19. Microsoft Learn — Manage certificate templates
20. Microsoft Learn — Export certificate with private key


**RÈGLE DE RÉVISION**

Quand tu refais le TP : ne cherche pas seulement “où cliquer”. À chaque écran, pose-toi 3 questions : 1) quel rôle je configure ? 2) quelle dépendance il utilise (nom, IP, DNS, certificat, groupe) ? 3) comment je vérifie que le résultat est bon ?