



RDS



Qu'est-ce que RDS ?

RDS signifie **Remote Desktop Services**, et c'est une fonctionnalité du système d'exploitation **Windows Server** qui permet aux utilisateurs d'accéder à une session ou une application de bureau sur un ordinateur distant via une connexion réseau.

En termes plus simples, **RDS permet aux utilisateurs de se connecter à distance à un autre ordinateur Windows Server**, qu'il se trouve dans le même bâtiment ou à travers le monde, et de l'utiliser comme s'ils étaient assis devant. Cela peut être utile pour une variété de scénarios, comme permettre aux employés de travailler à domicile ou donner au personnel informatique un accès à distance pour gérer les serveurs.

Lorsqu'un utilisateur se connecte à un ordinateur distant à l'aide de RDS, il exécute essentiellement une session à distance sur cet ordinateur. Cela signifie que toutes les applications qu'ils exécutent ou les modifications qu'ils apportent seront stockées sur cet ordinateur distant plutôt que sur leur ordinateur local. Les utilisateurs peuvent également se connecter à une application spécifique sur l'ordinateur distant plutôt qu'à la session de bureau complète.



RDS se compose de plusieurs composants, notamment le courtier de connexion Bureau à distance, la passerelle Bureau à distance, l'accès Web Bureau à distance, l'hôte de session Bureau à distance et l'hôte de virtualisation Bureau à distance. Ces composants fonctionnent ensemble pour offrir aux utilisateurs une expérience de bureau à distance transparente et sécurisée.

L'agent de connexion Bureau à distance est chargé de gérer les connexions des utilisateurs et de les acheminer vers le serveur hôte de session Bureau à distance approprié. La passerelle de bureau à distance fournit un accès sécurisé aux sessions de bureau à distance sur Internet en canalisant le trafic **RDP** via **HTTPS**. L'accès Web au bureau à distance permet aux utilisateurs de se connecter à des bureaux et applications distants via un navigateur Web. L'hôte de session de bureau à distance est responsable de l'hébergement des sessions de bureau à distance, tandis que l'hôte de virtualisation de bureau à distance permet aux utilisateurs de se connecter à des bureaux virtuels exécutés sur un serveur.

En résumé, RDS est une fonctionnalité de Windows Server qui permet aux utilisateurs de se connecter à distance et d'utiliser un ordinateur ou une application sur un autre ordinateur via une connexion réseau. Il se compose de plusieurs composants qui fonctionnent ensemble pour offrir aux utilisateurs une expérience de bureau à distance sécurisée et transparente.

Pourquoi avons-nous besoin de tout cela ?

Accès à distance : RDS permet l'accès à distance à un ordinateur ou à une application, permettant aux utilisateurs de travailler de n'importe où et d'accéder à des ressources auxquelles ils ne pourraient pas accéder autrement. Ceci est particulièrement utile pour les employés qui doivent travailler à domicile, sur la route ou ailleurs.



SOMMAIRE

1. [Vision generale su RDS](#)
2. [Installation RDS sur Win Server 2022](#)
3. [TIPS: Comme Securiser RDS](#)
 - a. [EvlWatcher](#)
 - b. [MFA](#)
 - c. [RDP sur un port personnalisé](#)
4. [TIPS: Installation de RDS sans AD DS](#)
5. [Conclusion et comparaison des deux mode de licenses. users vs devices](#)

Dans les pages suivantes, la procédure étape par étape pour configurer les fonctions décrites ci dessus sera expliquée avec une explication d'accompagnement

Dans ce tutoriel, nous utiliserons un systeme de test basée sur Hyper-V:

- Une machine agirà come hyperviseur (Hyper-V) (Always thanks to M. K.ROTH)
- Une autre machine agira en tant que «SERVER» → Windows Server 2022
- Trois autres machines agiront en tant que «VM client» → Windows 10



Toutes les captures d'écran de ce didacticiel seront disponibles sur ce lien sur [Google Drive](#) pour permettre la visualisation en HD de toutes les captures d'écran.

Raccourci	Explication
VPN	virtual private network
FTP	file transfer protocol
SFTP	secure (ssl) file transfer protocol
RDP	remote desktop protocol
RDS	remote desktop service
IP	interne protocol
Win srv	windows server

Vision generale su RDS

Bureau virtuel Azure

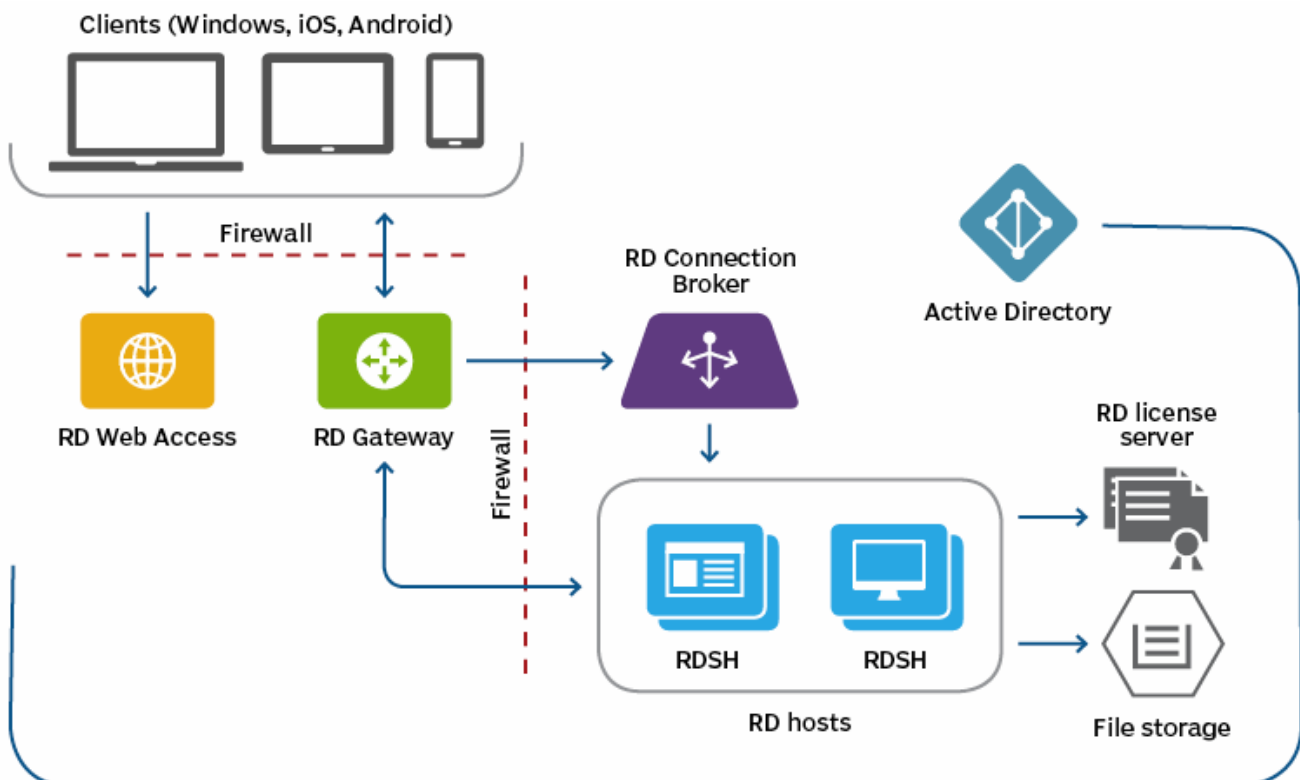
En 2017, Microsoft a annoncé un aperçu de nouvelles options d'infrastructure basées sur Azure pour les services de bureau à distance sous l'infrastructure moderne de bureau à distance (RDmi). La société a fourni des rôles d'infrastructure pour RD Connection Broker, RD Web et RD Gateway en tant que services Azure Web App, au lieu de serveurs individuels. RDmi utilisait Azure Active Directory pour l'authentification, et les charges de travail, telles que les serveurs RDSH, devaient s'exécuter dans Azure. RDmi était un moyen plus simple d'activer les déploiements RDS mutualisés.

Par la suite, en 2018, Microsoft a annoncé qu'il utiliserait RDmi pour une nouvelle offre de bureau et d'application basée sur le cloud appelée Windows Virtual Desktop, qui a ensuite été renommée Azure Virtual Desktop (**AVD**). AVD est un produit de bureau en tant que service (DaaS) qui offre un accès aux bureaux virtuels et aux applications via l'infrastructure cloud de Microsoft Azure.

Services de bureau à distance sur Windows Server 2022

Les services Bureau à distance sont disponibles dans Windows Server 2019 et 2022. Cependant, depuis l'introduction de Windows Server 2019, certaines fonctionnalités sont limitées. Windows Server Desktop Experience et RDSH n'incluent pas les nouvelles fonctionnalités telles que Microsoft Cortana, le Microsoft Store et l'application et les services Xbox.


Les produits concurrents tels que Citrix Virtual Apps and Desktops et VMware Horizon utilisent le rôle de serveur RDSH.





Installation RDS sur Win Server 2022

Attention

Avant de poursuivre, il est bon de rappeler qu'un service RPD (best practice) ne doit jamais être exposé sur le web, il serait toujours préférable de passer par un VPN ou au moins d'installer un pare-feu intelligent qui bloque déjà toutes les IP indésirables (voir le bloc fonction geo-ip) Il peut être intéressant d'installer un VPN  Wireguard sur le serveur lui-même (sauf s'il y a un pare-feu en amont capable de faire office de vpn)

Les services Bureau à distance peuvent être configurés pour permettre aux utilisateurs de se connecter à des bureaux virtuels, à des programmes RemoteApp et à des bureaux basés sur une session.

Déploiement de bureaux basés sur un ordinateur virtuel

Le déploiement de bureaux basés sur un ordinateur virtuel permet aux utilisateurs de se connecter à des collections de bureaux virtuels incluant des programmes RemoteApp et des bureaux virtuels publiés.

Déploiement de bureaux basés sur une session

Le déploiement de bureaux basés sur une session permet aux utilisateurs de se connecter à des collections de sessions incluant des programmes RemoteApp et des bureaux basés sur une session.

Il est bon de savoir qu'il est possible de se déployer de deux manières différentes. Via un bureau distant basé sur un ordinateur séparé ou via une session séparée. En général, cette dernière option est la plus utilisée car elle est la moins chère et la plus simple à mettre en œuvre.

Passer les services de rôles en revue

SERVEUR DE DESTINATION
Déploiement standard sélectionné

Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Services de rôle

Service Broker pour les connexions Bureau à distance
Le service Broker pour les connexions Bureau à distance connecte ou reconnecte un périphérique client aux programmes RemoteApp, aux bureaux basés sur une session et aux bureaux virtuels.

Accès Bureau à distance par le Web
Accès Bureau à distance par le Web permet aux utilisateurs de se connecter aux ressources fournies par des collections de sessions et des collections de bureaux virtuels en utilisant le menu Démarrer ou un navigateur Web.

Hôte de session Bureau à distance
Hôte de session Bureau à distance permet à un serveur d'héberger des programmes RemoteApp ou des bureaux basés sur une session.

Les informations d'identification du compte LPASR\Administrateur seront utilisées pour créer le déploiement.

Nous aurions alors plus de services à installer. Le service broker est le service qui gère les sessions utilisateur ouvertes. L'accès web simplifie l'utilisation à distance qui peut se faire via un navigateur. L'hôte de session est le serveur lui-même qui gère les sessions.

Dans les captures d'écran suivantes, nous devons simplement confirmer les rôles que nous avons vus dans la capture d'écran précédente.

Assistant Ajout de rôles et de fonctionnalités

Spécifier le serveur du service Broker pour les connexions Bureau à distance

SERVEUR DE DESTINATION
Déploiement standard sélectionné

Sélectionnez les serveurs dans le pool de serveurs où installer le service de rôle du service Broker pour les connexions Bureau à distance.

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
winsrv1.lpasr.local	192.168.1.1	

Sélectionné

Ordinateur

- LPASR.LOCAL (1)
winsrv1



Assistant Ajout de rôles et de fonctionnalités

Spécifier un serveur d'accès Web des services Bureau à...

SERVEUR DE DESTINATION
Déploiement standard sélectionné

Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Services de rôle
Service Broker pour les c...
Accès Bureau à distance...
Serveur hôte de session B...
Confirmation
Terminé

Sélectionnez un serveur dans le pool de serveurs où installer le service de rôle Accès Web des services Bureau à distance.

Installer le service de rôle de l'accès Web des services Bureau à distance sur le serveur du service Broker pour les connexions Bureau à distance

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
winsrv1.lpasr.local	192.168.1.1	

1 ordinateur(s) trouvé(s)

Sélectionné

Ordinateur

- LPASR.LOCAL (1)
winsrv1

1 ordinateur(s) sélectionné(s)

Assistant Ajout de rôles et de fonctionnalités

Spécifier les serveurs hôtes de session Bureau à distance

SERVEUR DE DESTINATION
Déploiement standard sélectionné

Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Services de rôle
Service Broker pour les c...
Accès Bureau à distance...
Hôte de session Bureau à...
Confirmation
Terminé

Sélectionnez les serveurs dans le pool de serveurs où installer le service de rôle Hôte de session Bureau à distance. Si plusieurs serveurs sont sélectionnés, le service de rôle Hôte de session Bureau à distance sera déployé sur tous ces serveurs.

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
winsrv1.lpasr.local	192.168.1.1	

1 ordinateur(s) trouvé(s)

Sélectionné

Ordinateur

- LPASR.LOCAL (1)
winsrv1

1 ordinateur(s) sélectionné(s)

< Précédent Suivant > Déployer Annuler



Assistant Ajout de rôles et de fonctionnalités

Afficher la progression

SERVEUR DE DESTINATION
Déploiement standard sélectionné

Terminé

Les services de rôles des Services Bureau à distance sélectionnés sont en cours d'installation.

Serveur	État d'avancement	État
Service de rôle Service Broker pour les connexions Bureau à distance		
winsrv1.lpasr.local	<div style="width: 100%;"></div>	Réussi
Service de rôle Accès Web aux services Bureau à distance		
winsrv1.lpasr.local	<div style="width: 100%;"></div>	Réussi
Service de rôle Serveur hôte de session Bureau à distance		
winsrv1.lpasr.local	<div style="width: 100%;"></div>	Réussi

< Précédent Suivant > Fermer Annuler

Lors de l'installation des différents rôles le serveur devra redémarrer, ceci est tout à fait normal lors de l'installation. Une fois que tout est terminé, nous pouvons cliquer sur "Fermer" et revenir à l'interface de notre gestionnaire de serveur.

On peut donc voir que le gestionnaire de licence n'est pas installé.
Cliquez simplement dessus pour l'installer.

Gestionnaire de serveur

Gestionnaire de serveur > Services Bureau à distance > Vue d'ensemble

Vue d'ensemble

PRISE EN MAIN DES SERVICES BUREAU À DISTANCE

1 Configurer un déploiement pour les services Bureau à distance

DÉMARRAGE RAPIDE

Déploiement de bureaux basés sur un ordinateur virtuel

Déploiement de bureaux basés sur une session

2 Ajouter des serveurs hôtes de virtualisation des services Burea

3 Créer des collections de bureaux virtuels

2 Ajouter des serveurs hôtes de session Bureau à distance

3 Créer des connexions de sessions

EN SAVOIR PLUS

VUE D'ENSEMBLE DU DÉPLOIEMENT

Serveur du service Broker pour les connexions Bureau à distance : winsrv1.lpasr.local

Géré comme : LPASR/administrateur

Accès Bureau à dista... Passerelle des service... Gestionnaire de licen...

Service Broker pour l...

Serveur hôte de virtu... Serveur hôte de sessi...

REPERES DE DÉPLOIEMENT

Dernière actualisation le 19/03/2023 22:32:26 | Tous les services de rôle des services Bureau à distance | 3... TÂCHES

Nom de domaine Complet du serveur	Service de rôle installé
WINSRV1.LPASR.LOCAL	Service Broker pour les connexions Bureau à distance
WINSRV1.LPASR.LOCAL	Hôte de session Bureau à distance
WINSRV1.LPASR.LOCAL	Accès Web des services Bureau à distance



Ainsi, dès que nous avons cliqué, nous avons pu spécifier le serveur qui s'occupera de la gestion des licences. Le rôle sera donc installé à la fin de la procédure.

Ajouter Gestionnaire de licences des services Bureau à distance serveurs

Sélectionner un serveur

Cet Assistant vous permet d'ajouter Gestionnaire de licences des services Bureau à distance serveurs au déploiement. Sélectionnez les serveurs sur lesquels installer le rôle de service Gestionnaire de licences des services Bureau à distance.

Pool de serveurs

Filtre :

Nom	Adresse IP	Système
winsrv1.lpasr.local	192.168.1.1	

1 ordinateur(s) trouvé(s)

Sélectionné

Ordinateur

0 ordinateur(s) sélectionné(s)

Ajouter Gestionnaire de licences des services Bureau à distance serveurs

Afficher la progression

Le service de rôle est en cours d'installation sur les serveurs suivants.

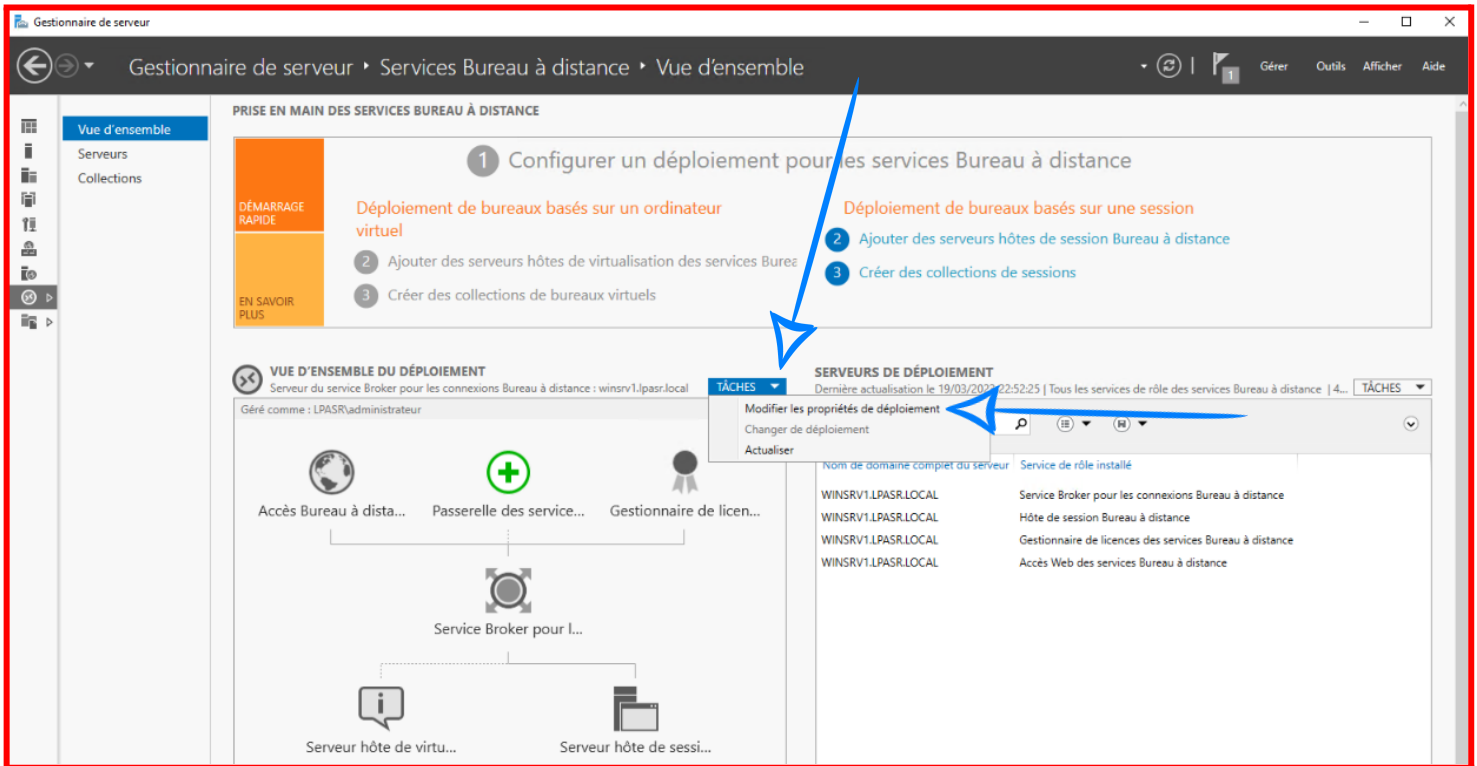
Serveur	État d'avancement	État
Service de rôle Gestionnaire de licences des services Bureau à distance		
winsrv1.lpasr.local	<div style="width: 100%;"></div>	Réussi

Vérifier les propriétés du Gestionnaire de licences des services Bureau à distance pour le déploiement

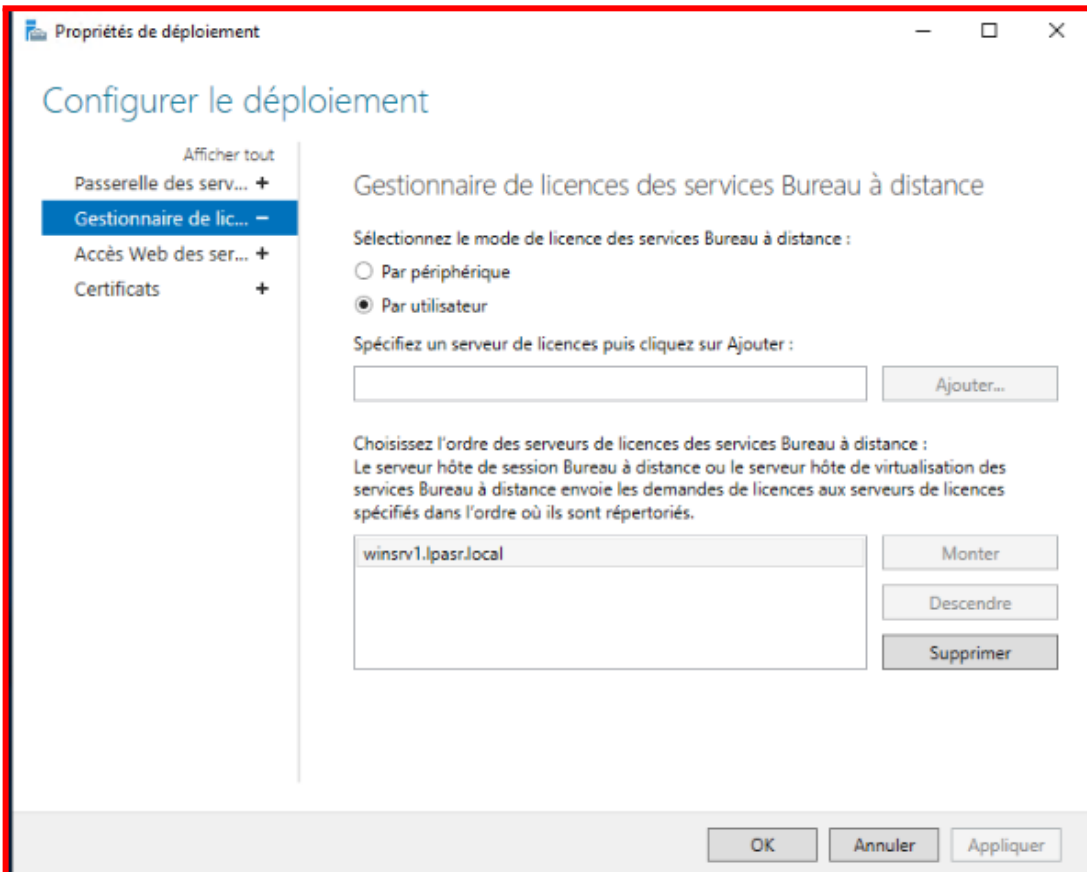
< Précédent Suivant > Fermer Annuler



Nous devons maintenant configurer le mode de licence. Par défaut, aucun mode de licence n'est configuré. Des licences utilisateur ou des licences de périphérique (**User-Cal** et **Device-Cal**) peuvent être créées.

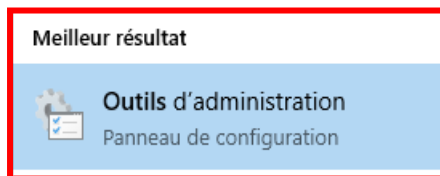


L'écran précédent peut être laissé avec les paramètres par défaut. mais c'est ici que nous choisirons s'il s'agit de licences par utilisateur ou par appareil. Le plus utilisé est le mode de licence par utilisateur

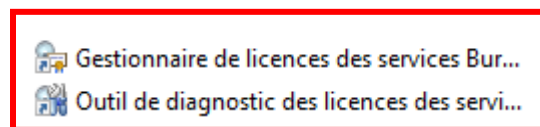




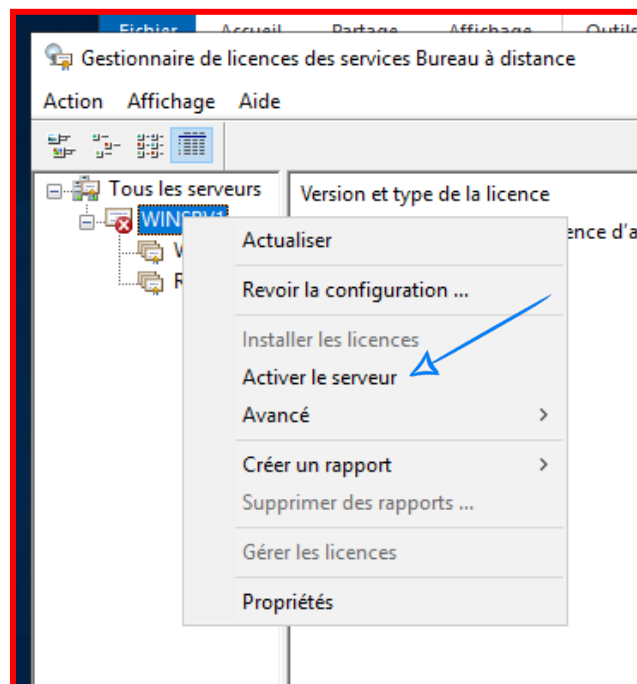
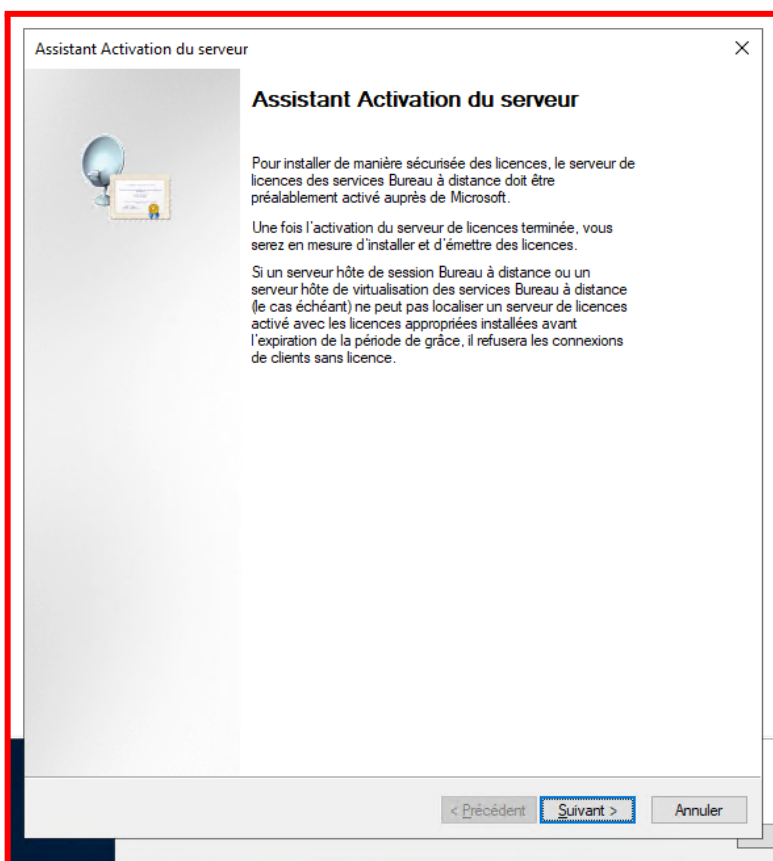
Recherchez ensuite le panneau des utilitaires d'administration puis allez dans : Gestionnaire de licences des services bureau à distance.



Une fois la fenêtre ouverte, nous verrons qu'aucune licence n'est active pour le moment.



Il faudra donc cliquer avec le bouton droit de la souris sur "**Activer le serveur**" pour activer les licences cibles.



Par défaut tout le monde peut se connecter via RDP à un serveur, il vaudra donc mieux créer un groupe dédié aux personnes pouvant entrer sur le serveur via RDP et configurer manuellement les personnes pouvant entrer sur le serveur.

Il sera également intéressant de masquer tous les lecteurs de notre serveur. Pour que notre utilisateur ne puisse pas voir le disque c et tous les autres disques connectés.

Tout cela sera possible via les GPO.

TIPS: Comme securiser RDS

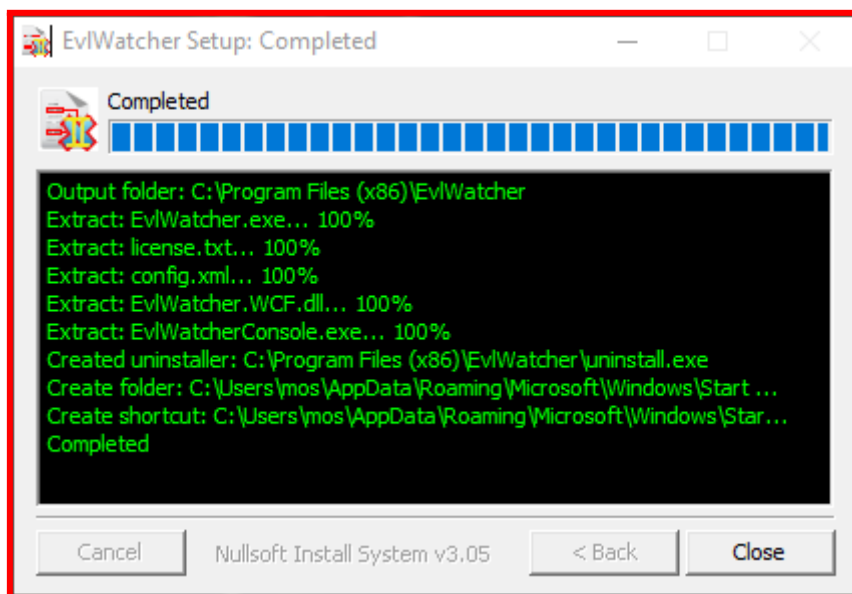
EvWatcher → <https://github.com/devnulli/EvWatcher/releases>

Bannir les adresses IP effectuent des attaques par Brute Force : c'est ce que nous allons voir avec la mise en place du logiciel EvWatcher

Pourquoi EvWatcher et pas un autre outil ?".

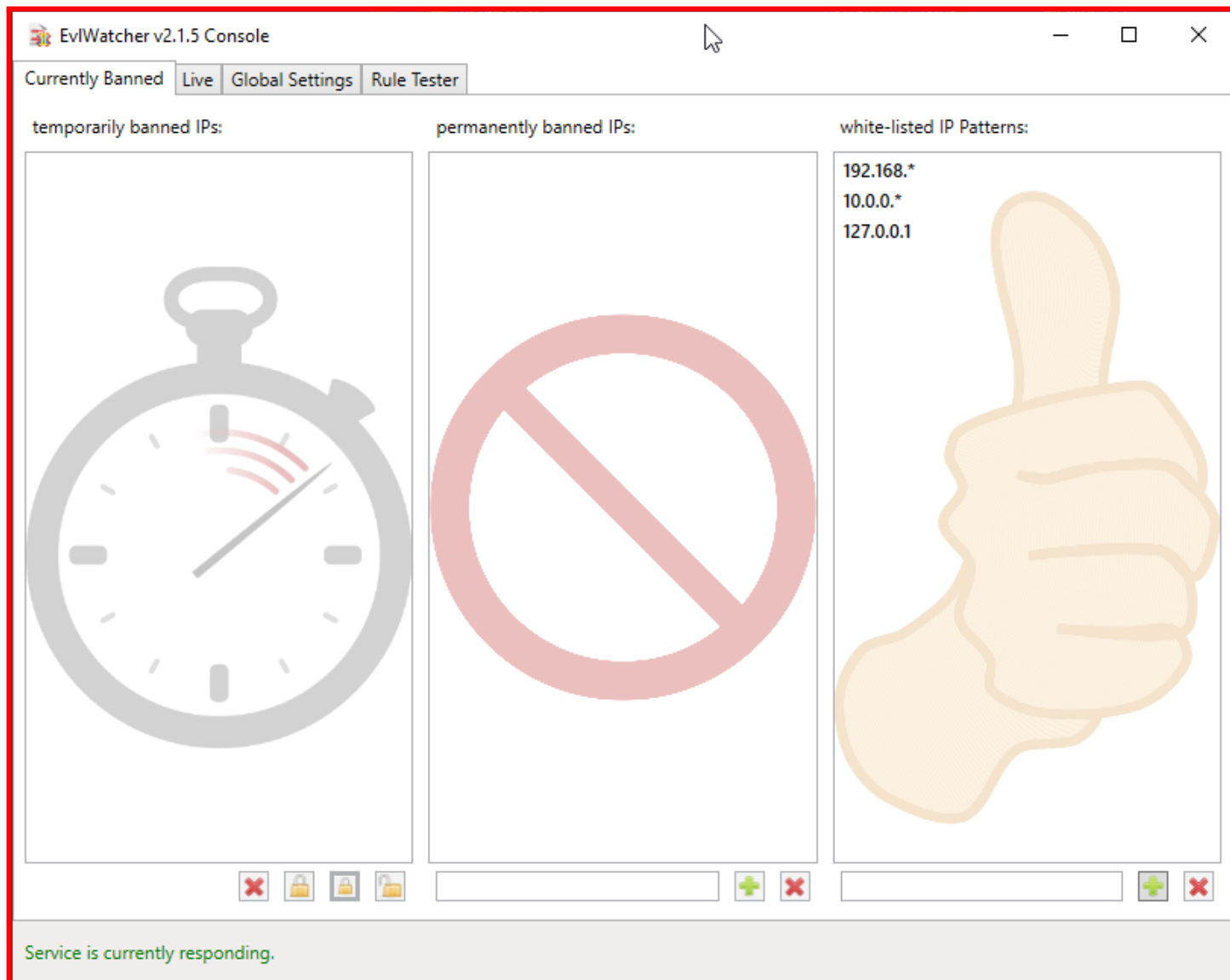
Il est gratuit, son code source est disponible sur GitHub, il s'installe très rapidement et il fonctionne bien!

EvWatcher va permettre de détecter les attaques par Brute Force sur la machine Windows cible en analysant les journaux d'événements de Windows et en bloquant les adresses IP malveillantes à l'aide du pare-feu de Windows. C'est en quelque sorte un fail2ban pour Windows qui surveille le service RDP.



Vous obtiendrez un exécutable très léger : procédez à l'installation, deux trois clics suffisent. Il faut savoir que par défaut l'outil s'installe dans "C:\Program Files (x86)\EvWatcher" et qu'il crée un service nommé "EvWatcher service" sur la machine.

Dans le menu Démarrer, vous allez trouver un raccourci nommé "EvWatcherConsole" qui donne accès à l'interface de gestion du logiciel. Voici



L'onglet "Currently Banned" se découpe en trois parties :

- IP temporairement bannies : les adresses IP bannies temporaires, pour une durée limitée
- IP bannies définitivement : les adresses IP bannies définitivement (après plusieurs bannissements temporaires)
- White-Listed IP Patterns : les adresses IP ou les sous-réseaux en liste blanche

Il est possible d'ajouter ou de supprimer des adresses IP manuellement dans chaque section. C'est simple, mais efficace pour visualiser rapidement l'état des bannissements sur son serveur.

Au sein des règles de trafic entrant du pare-feu Windows, vous allez retrouver une règle nommée "*EvilWatcher*" qui est utilisée par le logiciel pour bloquer l'accès (sur tous les ports) aux adresses IP bannies. L'onglet "*Live*" permet de suivre en live l'activité du logiciel.



Onglet "Rule Tester"

EvWatcher v2.1.5 Console

Currently Banned Live Global Settings Rule Tester

On this tab you can test out the rules of EvlWatcher, to find out if it would work for a given event-log entry

1) Select task:

Regex:

Event Path:

Booster Words:

2) Insert XML from event-log

3) Hit the test button. If it doesn't work, fiddle with the Regex and hit the test button again.. You can also try regex101.com, it's great for testing regex

Test with Regex:

Test Reset

4) React

You found something that should be blocked but isn't? (RDP or any other protocol?). Feel free to repair or create new tasks in your config.xml file. But hey.. please don't just correct it in your config file.. instead, please make a github issue (and paste above XML and Regex), so other users can benefit of that.

Service is currently responding.

Lorsque vous trouvez quelque chose que vous voulez interdire automatiquement, vous pouvez utiliser cet onglet pour vous aider à composer une règle pour cela. Vous copiez votre XML Event-Log Windows ici et essayez de trouver un Regex pour cela. Lorsque vous appuyez sur le "bouton de test" et qu'une adresse IP peut être extraite, vous avez trouvé une nouvelle règle.

Une fois que vous avez fait cela, vous pouvez soit créer une nouvelle tâche d'interdiction dans votre configuration, soit publier un problème ici, afin que nous l'ajoutions globalement à la configuration.

Remarque : Lorsque vous copiez une expression régulière passée dans un XML, vous devez échapper les crochets avec **<** et **>**;



TIPS: Comme sécuriser RDS

MFA - 2FA

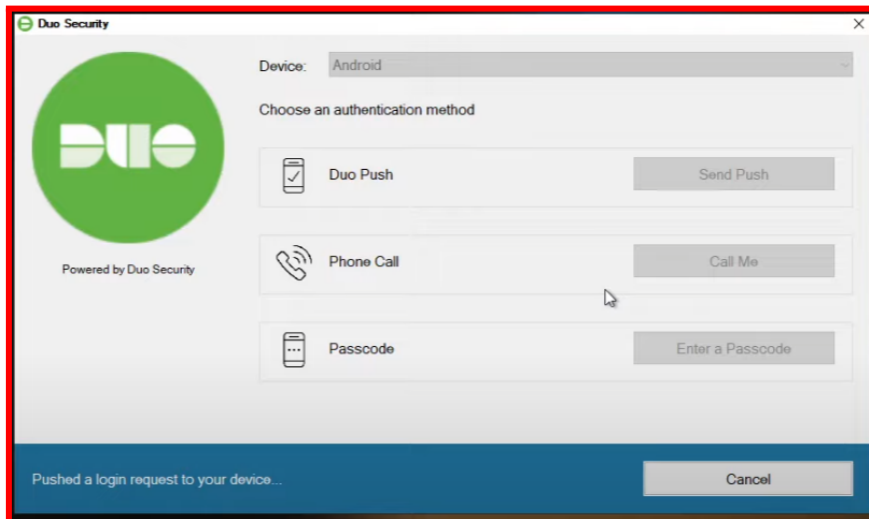
Bien que RDP soit un outil extrêmement pratique, il peut également poser un risque de sécurité important s'il n'est pas correctement sécurisé.

L'un des moyens de sécuriser les connexions RDP consiste à mettre en œuvre une authentification à deux facteurs (2FA). 2FA est un processus de sécurité qui oblige les utilisateurs à fournir deux formes d'authentification avant d'accorder l'accès à un système. Cela implique généralement quelque chose que l'utilisateur connaît, comme un mot de passe, et quelque chose que l'utilisateur possède, comme un jeton de sécurité ou une application pour smartphone.

La mise en œuvre de 2FA pour les connexions RDP est importante car elle augmente considérablement la sécurité du protocole RDP. Il fournit une couche supplémentaire de protection contre les accès non autorisés, même si un mot de passe est compromis. Sans 2FA, un attaquant qui a obtenu le mot de passe d'un utilisateur peut facilement accéder au système distant.

En plus de fournir une sécurité renforcée, la mise en œuvre de 2FA pour les connexions RDP peut également aider les organisations à se conformer aux réglementations industrielles et gouvernementales. De nombreuses réglementations obligent les organisations à mettre en œuvre des mécanismes d'authentification solides pour protéger les données sensibles, et 2FA est souvent considérée comme une meilleure pratique pour y parvenir.

Dans l'ensemble, la sécurisation des connexions RDP via 2FA est une étape critique pour maintenir la sécurité et l'intégrité de l'accès à distance aux systèmes informatiques et aux serveurs. Il aide les organisations à se protéger contre les cybermenaces et garantit que les données sensibles restent sécurisées.



Il existe une multitude de logiciels qui permettent de sécuriser notre AD (mais sans forcément modifier le système de fichiers et/ou la structure de l'AD). Nous en avons testé deux : **Userlock** et **Duo**

- Userlock** → <https://www.isdecisions.com/products/userlock/>
- Duo** → <https://duo.com/>



Autoriser RDP sur un port personnalisé

Par défaut, la connexion Bureau à distance s'appuie sur le port 3389. Il est préférable d'utiliser un port spécifique pour la connexion Bureau à distance, cela permet de masquer le service en quelque sorte. Pour cela, il faut modifier le Registre de Windows.

Chemin d'accès de la clé :

SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

Modifier la valeur DWORD 32 bits

Nom de la valeur :
PortNumber

Données de la valeur :
54321

Base
 Hexadécimale
 Décimale

OK Annuler

Du coup, pour le moment, le Bureau à distance est activé et accessible sur le port 54321 sur le poste Windows 10/11. Par contre, depuis une machine distante, cela ne fonctionne pas ! Pourquoi ? C'est simple! Parce que le pare-feu Windows bloque la connexion.

Nous devrions ensuite ouvrir le port nouvellement choisi via le pare-feu, donc une série de captures d'écran suivra ici pour ouvrir le port cible dans le protocole TCP.

Assistant Nouvelle règle de trafic entrant

Type de règle

Sélectionnez le type de règle de pare-feu à créer.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Quel type de règle voulez-vous créer ?

Programme
Règle qui contrôle les connexions d'un programme.

Port
Règle qui contrôle les connexions d'un port TCP ou UDP.

Prédéfinie :
@FirewallAPI.dll,-80200
Règle qui contrôle les connexions liées à l'utilisation de Windows.

Personnalisée
Règle personnalisée.

RDP fonctionne via le port TCP, nous devons donc choisir le protocole TCP



Assistant Nouvelle règle de trafic entrant

Protocole et ports

Spécifiez les protocoles et les ports auxquels s'applique cette règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Cette règle s'applique-t-elle à TCP ou UDP ?

TCP
 UDP

Cette règle s'applique-t-elle à tous les ports locaux ou à des ports locaux spécifiques ?

Tous les ports locaux
 Ports locaux spécifiques :
Exemple : 80, 443, 5000-5010

A ce stade il faut donc autoriser le port choisi précédemment

Assistant Nouvelle règle de trafic entrant

Action

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

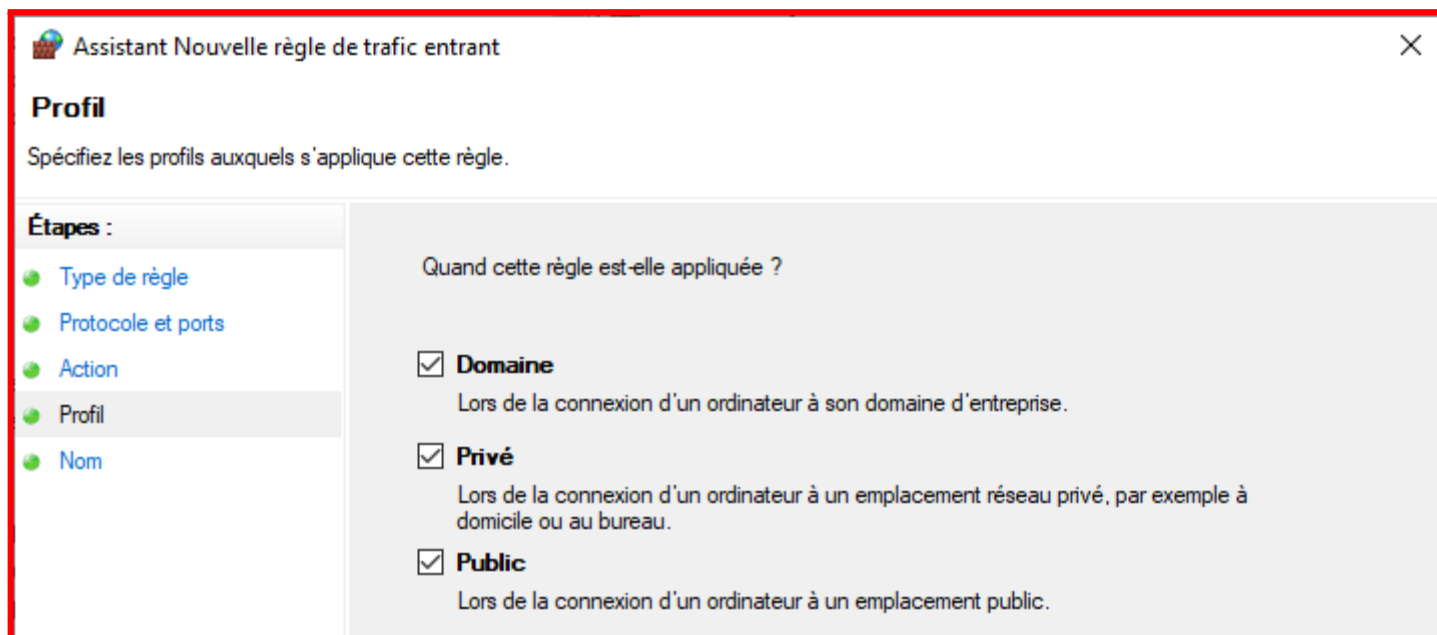
Autoriser la connexion
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

Autoriser la connexion si elle est sécurisée
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

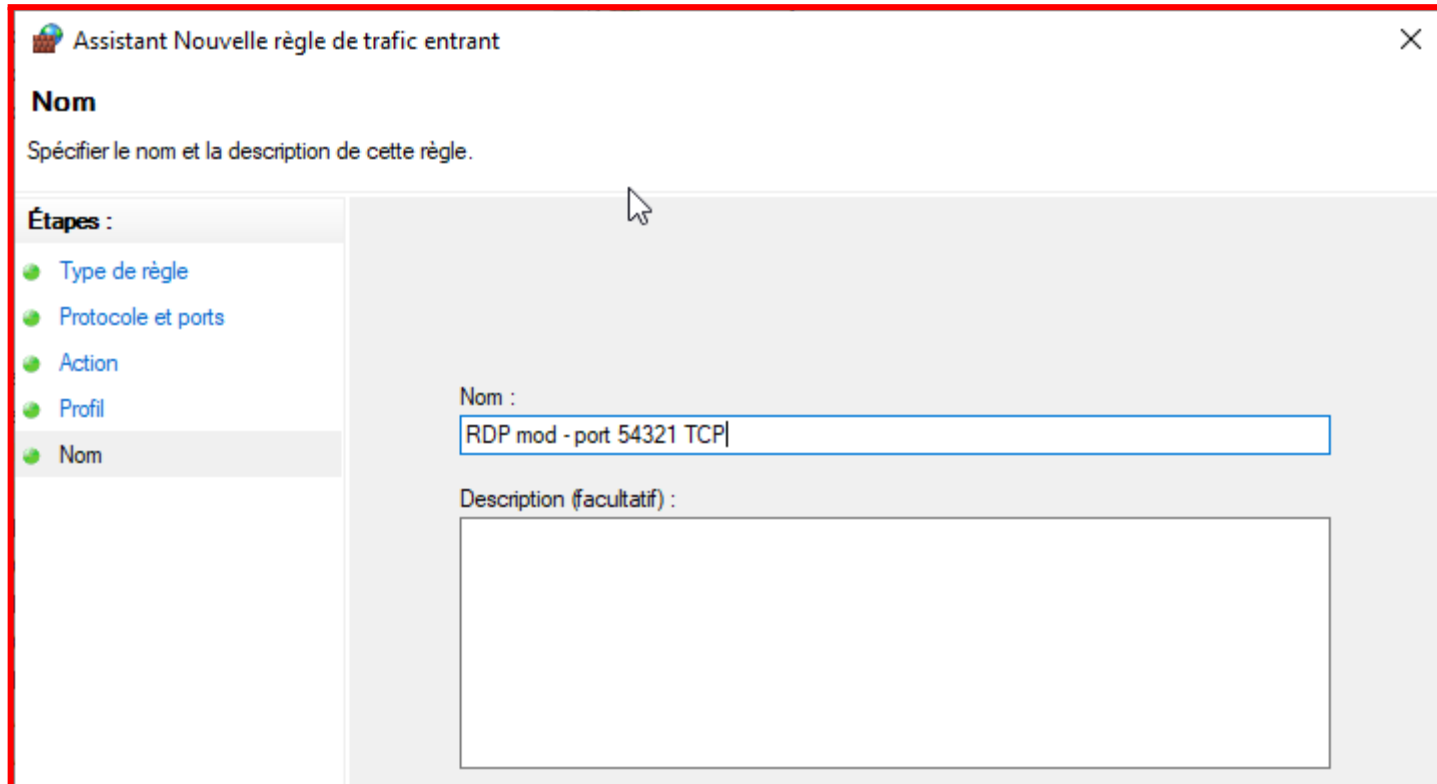
Bloquer la connexion



À ce stade, nous laissons généralement les trois options sélectionnées pour éviter tout problème dérivant du pare-feu Windows.

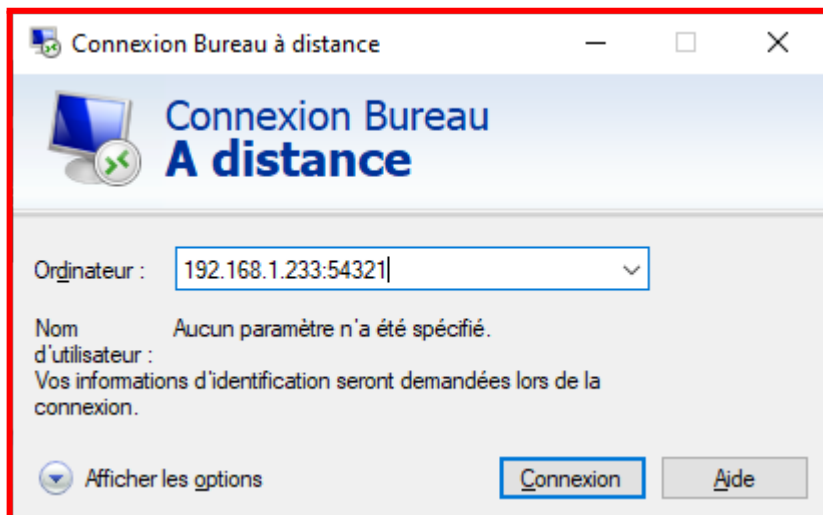


Ici, nous pouvons entrer le nom à donner à la règle nouvellement créée et, si nécessaire, également une description.





En consequence, vous devriez pouvoir vous connecter en RDP sur le port customisée !



PS : pour se connecter en Bureau à distance sur un port personnalisé, il faut spécifier à la suite de l'adresse IP (ou au nom d'hôte) la port cible.



TIPS: Installation de RDS sans AD DS

Cet section de ce TP décrit comment installer et configurer un rôle de *terminal server role Remote Desktop Session Host* dans un groupe de travail WORKGROUP (sans domaine Active Directory) et sans aucun autre rôle supplémentaire. Puis il s'agira d'un déploiement RDS à serveur unique sur Windows Server 2022 (mais également possible sur Windows Server 2019).

Il arrive que RDS doive être installé sur des versions de serveur Windows dans certains contextes où vous êtes obligé d'installer (ou avez déjà prêt) un système d'exploitation basé sur Windows Server et vous n'avez pas besoin d'AD DS.

Il est supposé que vous avez déjà installé Windows Server et configuré les paramètres de base (adresse IP, nom du serveur, heure/date, mises à jour installées, etc.). Ensuite, vous pouvez installer



le rôle RDS. Pour ce faire, vous pouvez utiliser le Gestionnaire de serveur ou PowerShell. Nous utiliserons PowerShell:

```
Install-WindowsFeature -Name RDS-Licensing, RDS-RD-Server -IncludeManagementTools
```

Vérifiez quels rôles RDS sont installés sur votre serveur :

```
Get-WindowsFeature -Name RDS* | Where installed
```

Puis redemarrez votre ordinateur

```
Restart-Computer
```

Maintenant, quand le pc à redémarré, allez dans:

Panneau de configuration -> Système et sécurité -> Outils d'administration -> Services Bureau à distance -> Diagnostic de licence Bureau à distance.

Veillez noter que votre serveur n'est pas encore configuré pour recevoir les CAL RDS du serveur de licences. Les messages suivants le prouvent :

The screenshot shows the 'Diagnostic des licences des services Bureau à distance' window. The main content area displays the following information:

Diagnostic des licences des services Bureau à distance (SRVX1)

L'outil de diagnostic des licences des services Bureau à distance fournit des informations pour aider à identifier les problèmes de licence possibles pour le serveur hôte de session des services Bureau à distance.

Les licences ne sont pas disponibles pour ce serveur hôte de session des services Bureau à distance a identifié des problèmes de licence pour le serveur hôte de session d

Détails de la configuration du serveur hôte de session Bureau à distance

SRVX1	
Nombre de licences disponibles pour les clients :	0
Version du serveur hôte de session Bureau à distance :	Windows Server 2019
Domaine Active Directory :	Non applicable
Mode de licence :	Par périphérique



Il faut maintenant configurer les paramètres de licence RDS avec l'éditeur de stratégie de groupe local (**gpedit.msc**) :

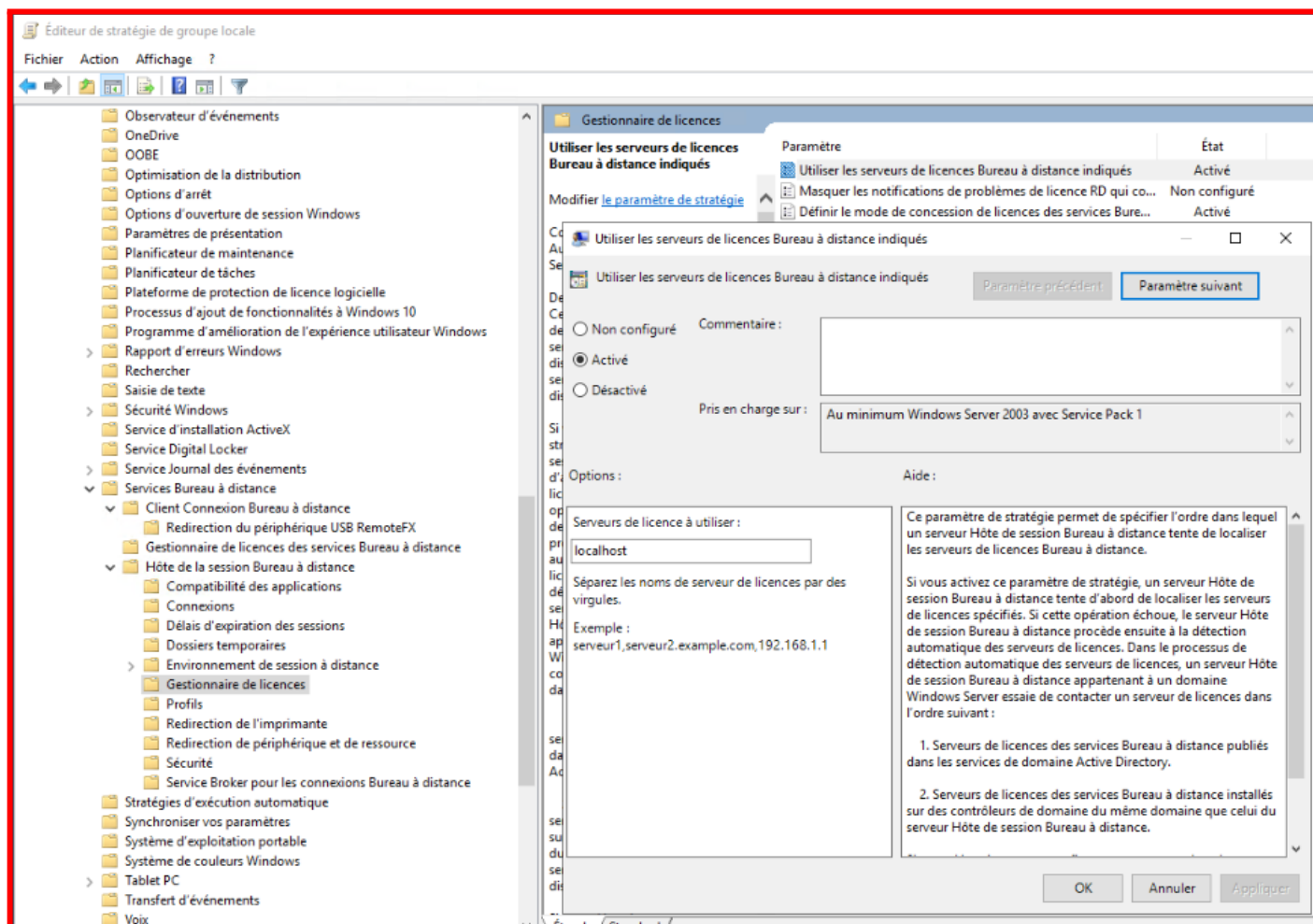
Accédez à Configuration ordinateur

-> Modèles d'administration -> Composants Windows -> Services Bureau à distance -> -->Hôte de session Bureau à distance -> Licences ;

Modifier Définissez le mode de licence du Bureau à distance sur **Par appareil**

Dans l'option Utiliser les serveurs de licences Bureau à distance spécifiés, spécifiez l'adresse IP du serveur sur lequel le serveur RDLicensing est installé.

Si le serveur de licences est installé localement, entrez localhost ou 127.0.0.1 ;



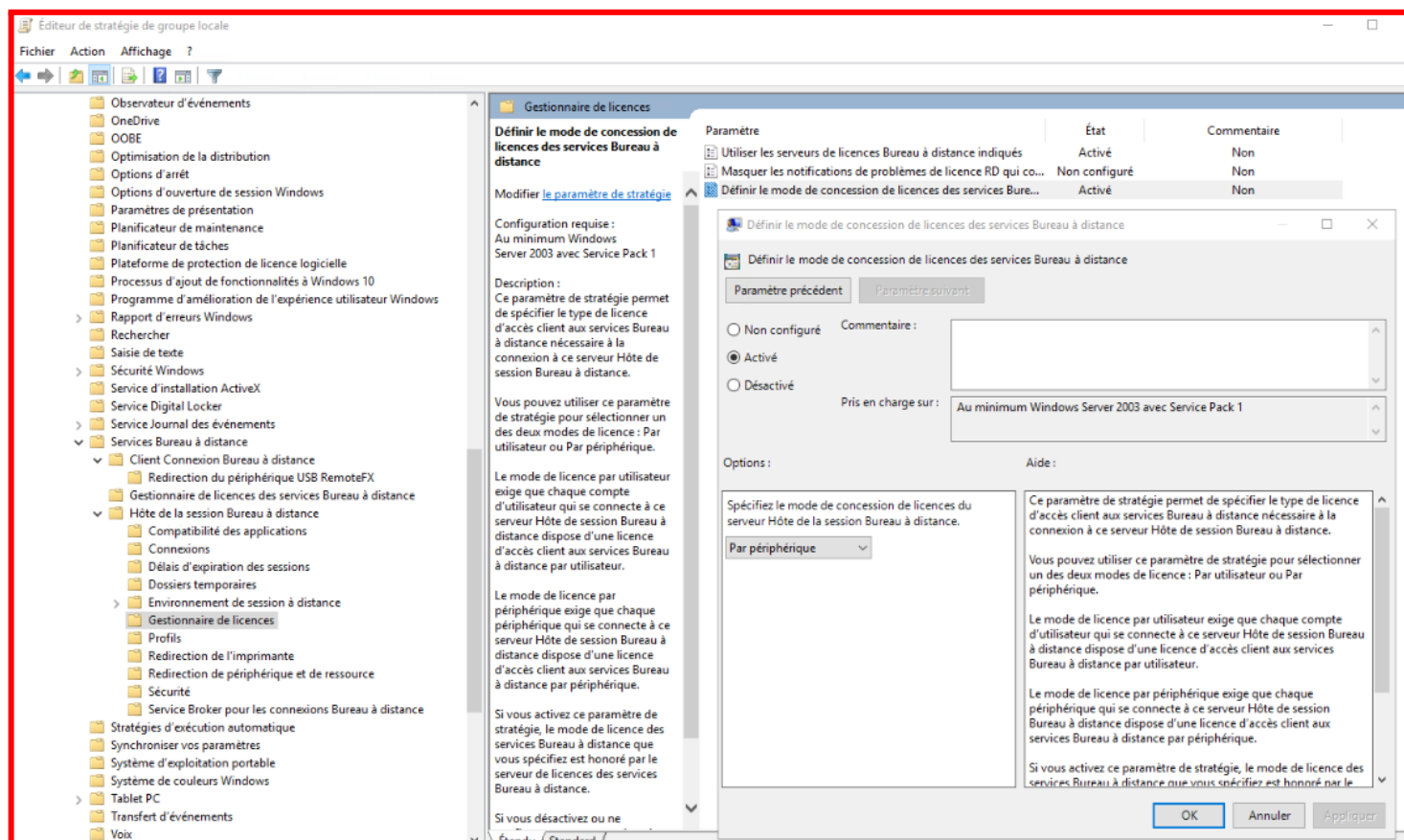
Si vous ne ciblez pas votre serveur RDSH sur le serveur de licences RDS capable d'émettre des CAL à vos utilisateurs, votre serveur restera en mode d'évaluation.

Dans ce mode, les services RDS ne fonctionnent que pendant 120 jours (à chaque connexion, vous verrez ce message dans la barre d'état :

« Le service Bureau à distance cessera de fonctionner dans xxx jours »).

(Le message de notification de licence peut en fait être supprimé avec quelques ajustements.)

Une fois la période de grâce terminée, les utilisateurs ne pourront plus se connecter à RDS.



Après, ca sera possible créer ensuite des comptes d'utilisateurs locaux sur le serveur RDS.

Vous pouvez créer des utilisateurs dans **lusrmgr.msc** ou avec **PowerShell** :

```
$UserPassword = ConvertTo-SecureString "PASSWORD" -AsPlainText -Force  
Net-LocalUser m.rossi -Password $UserPassword -FullName "Mario Rossi"
```

Pour permettre à un utilisateur de se connecter à un serveur via les services Bureau à distance, ajoutez le compte d'utilisateur au groupe local Utilisateurs du Bureau à distance. Ajoutez des utilisateurs manuellement à l'aide de la console de gestion de l'ordinateur ou avec PowerShell :

```
Add-LocalGroupMember -Group "Utilisateurs du Bureau à distance" -Membre m.rossi
```

Désormais, les utilisateurs peuvent essayer de se connecter à votre hôte RDS à l'aide de mstsc.exe (ou de tout autre client RDS) à partir de leurs ordinateurs.



Conclusion

Comme expliqué déjà dans l'introduction, Il existe plusieurs raisons pour lesquelles les services Bureau à distance (**RDS**) sont utiles et nécessaires pour certains scénarios :

- **Accès à distance** : RDS permet l'accès à distance à un ordinateur ou à une application, permettant aux utilisateurs de travailler de n'importe où et d'accéder à des ressources auxquelles ils ne pourraient pas accéder autrement. Ceci est particulièrement utile pour les employés qui doivent travailler à domicile, sur la route ou ailleurs.
- **Optimisation des ressources** : RDS permet à plusieurs utilisateurs d'accéder aux mêmes ressources sur un serveur, telles que des applications ou des bureaux virtuels, ce qui peut réduire le coût et la complexité de la gestion des ordinateurs de bureau ou portables individuels pour chaque utilisateur.
- **Gestion centralisée** : RDS permet au personnel informatique de gérer de manière centralisée les applications et les environnements de bureau sur les serveurs, réduisant ainsi le besoin de gérer des ordinateurs de bureau ou des ordinateurs portables individuels pour chaque utilisateur. Cela peut faciliter le déploiement des mises à jour et des correctifs, la gestion de la sécurité et la surveillance de l'utilisation.
- **Sécurité** : RDS peut fournir un environnement plus sécurisé pour l'accès à distance que d'autres méthodes, telles que VPN ou FTP, car il utilise le cryptage pour sécuriser les données transmises sur le réseau. Cela peut aider à protéger les données sensibles et empêcher tout accès non autorisé.
- Dans l'ensemble, les services de bureau à distance sont utiles pour les **organisations** qui doivent fournir un accès à distance aux applications et aux environnements de bureau pour leurs employés ou clients, ou qui doivent gérer les ressources de manière centralisée. RDS peut augmenter la productivité, réduire les coûts et améliorer la sécurité pour les scénarios d'accès à distant

Quelle est la différence entre un **USER-CAL** et **DEVICE-CAL** ?

Un **Device-CAL** est une licence pour accéder à un appareil connecté à un serveur, quel que soit le nombre d'utilisateurs de l'appareil. Les **Device-CAL** sont idéales pour les clients ayant plusieurs utilisateurs pour un seul appareil, tels que les travailleurs postés.

Un **User-CAL** est une licence permettant à chaque utilisateur nommé d'accéder à un serveur (depuis n'importe quel appareil) quel que soit le nombre d'appareils qu'il utilise. Les **User-CAL** sont idéales pour les entreprises dont les employés ont besoin d'un accès itinérant au réseau de l'entreprise à l'aide de plusieurs appareils, ainsi qu'à partir d'appareils inconnus.