Les différents moyens d'accès à distance

RDP - Chrome Remote Desktop - AnyDesk

Yanis Dahman

Sommaire

RDP

Qu'est-ce que le protocole Remote Desktop ?

Le protocole Remote Desktop (RDP) est un protocole propriétaire développé par Microsoft qui permet aux utilisateurs de se connecter à un autre ordinateur via une connexion réseau. Il fournit une interface graphique pour se connecter à un autre ordinateur fonctionnant sous Windows, permettant aux utilisateurs d'interagir avec le système distant comme s'ils étaient assis devant.

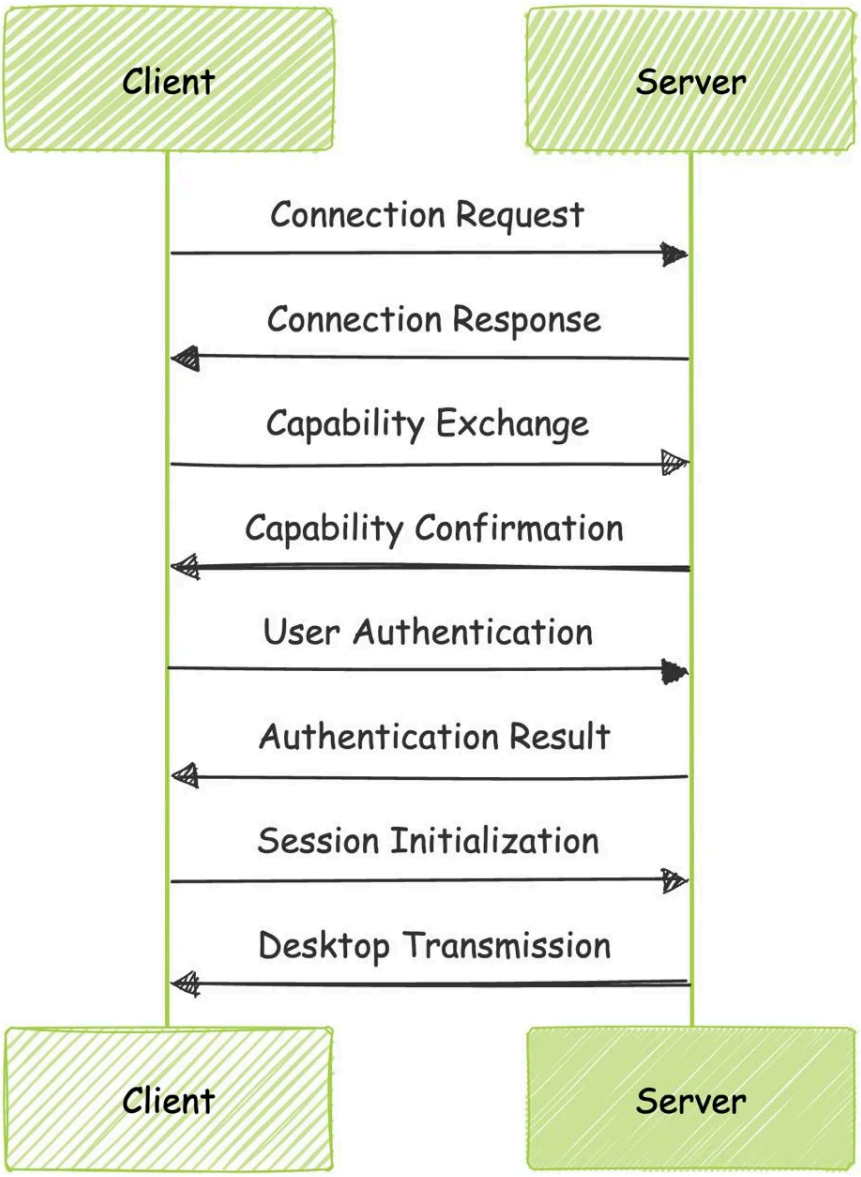
Principales caractéristiques du RDP de Windows

1. Interface utilisateur graphique : Le RDP transmet l'interface utilisateur graphique de l'ordinateur distant vers l'appareil client.
2. Communication multi-canaux : Prend en charge des canaux virtuels séparés pour transporter les données de présentation, la communication des périphériques série, les informations de licence et les données cryptées.
3. Chiffrement : Utiliser le chiffrement RC4 avec une clé de 128 bits pour crypter la transmission des données.
4. Redirection audio : Permet aux utilisateurs d'entendre l'audio de l'ordinateur distant sur leur appareil local.
5. Redirection du système de fichiers : Permet d'accéder aux fichiers et dossiers locaux depuis la session distante.
6. Redirection d'imprimante : Permet d'imprimer sur des imprimantes locales depuis la session distante.
7. Prise en charge multi-écrans : Prend en charge l'utilisation de plusieurs moniteurs dans les sessions distantes.

Comment fonctionne le RDP :

Le RDP fonctionne sur un modèle client-serveur :

1. Le serveur RDP écoute par défaut sur le port TCP 3389.
2. Lorsqu'un client initie une connexion, il envoie une demande de connexion au serveur.
3. Le serveur répond et un canal sécurisé est établi en utilisant TLS (Transport Layer Security).
4. Le client et le serveur échangent leurs capacités et négocient les termes de la connexion.
5. Une fois authentifié, le serveur envoie la sortie graphique au client, et le client renvoie les entrées de l'utilisateur au serveur.



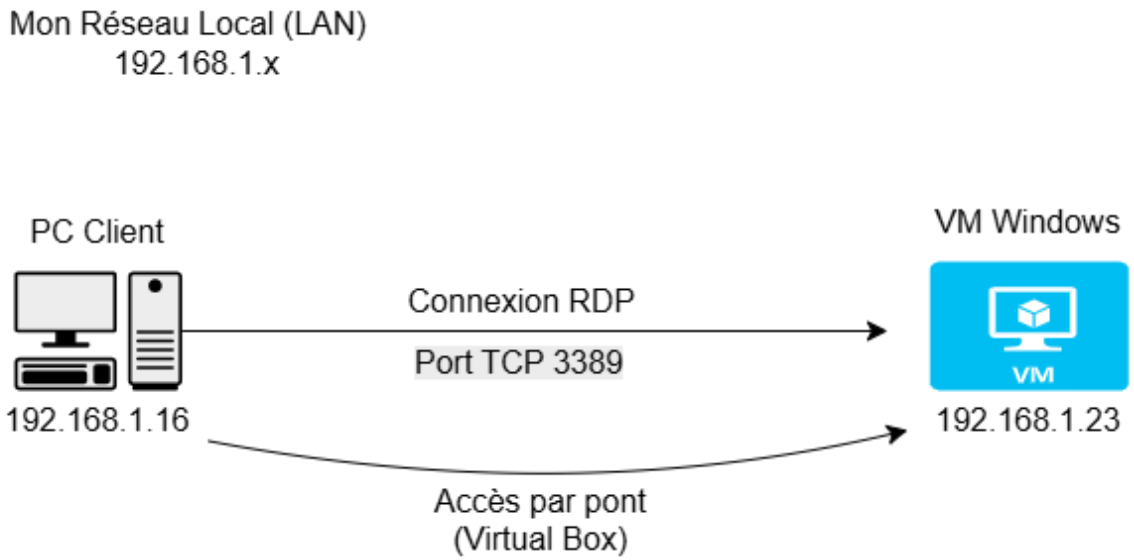
Avantages de l'utilisation du RDP

1. Accès à distance : Travailler de n'importe où avec une connexion Internet.
2. Rentabilité : Réduire le besoin de support informatique sur site et de déplacements.
3. Gestion centralisée : Gérer facilement plusieurs systèmes depuis un seul endroit.
4. Productivité améliorée : Accéder aux ressources de travail depuis divers appareils et lieux.
5. Évolutivité : Augmenter facilement les ressources informatiques sans investissements matériels importants.

RDP face aux autres solutions d'accès à distance

Fonctionnalité	RDP	VNC	TeamViewer	SSH
Interface graphique de support	**Oui**	Oui	Oui	Limité
Port par défaut	**3389**	5900	5938	22
Chiffrement	**Oui**	Optionnel	Oui	Oui
Multiplateforme	**Limité**	Oui	Oui	Oui
Transfert de fichiers	**Oui**	Limité	Oui	Oui
Performance	**Élevée**	Modérée	Élevée	Élevée (CLI)

Schéma de l'infrastructure



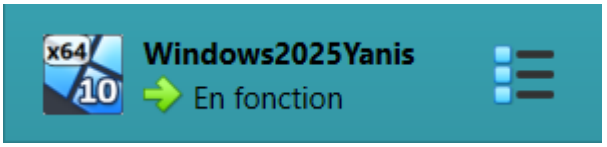
Utilisation du RDP

Installation de la VM

Pour ce test, la machine "Hôte" (celle qui sera contrôlée) est une machine virtuelle Windows 10.

Le choix de l'édition **"Pro"** est obligatoire. En effet, les versions "Famille" (Home) de Windows possèdent bien le *client* RDP (pour se connecter aux autres), mais n'incluent pas la fonction **"Serveur Bureau à distance"**.

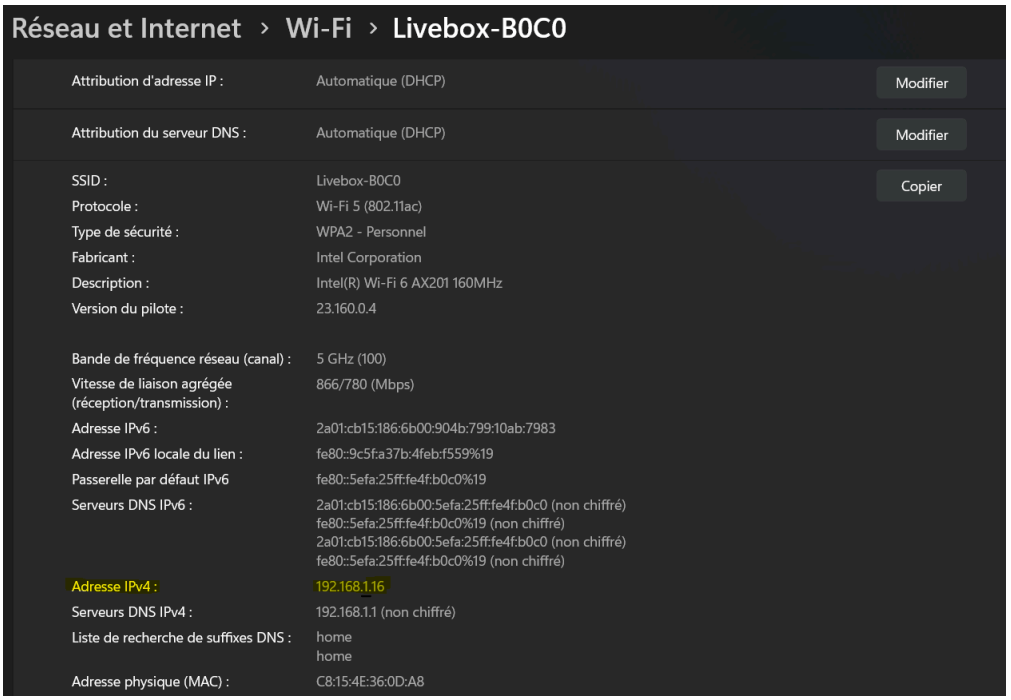
Il est donc impossible de prendre le contrôle d'un poste "Famille" avec cet outil.



Configuration Réseau (Client)

Avant de configurer la VM, nous vérifions l'adresse IP de votre machine **Client** (le PC physique) pour identifier le réseau sur lequel nous travaillons.

La capture d'écran montre que notre PC a l'adresse IP `192.168.1.16`. Cela signifie que pour communiquer en RDP, notre machine virtuelle (l'Hôte) devra impérativement se trouver sur le même sous-réseau, c'est-à-dire avoir une adresse commençant par `192.168.1.x`.

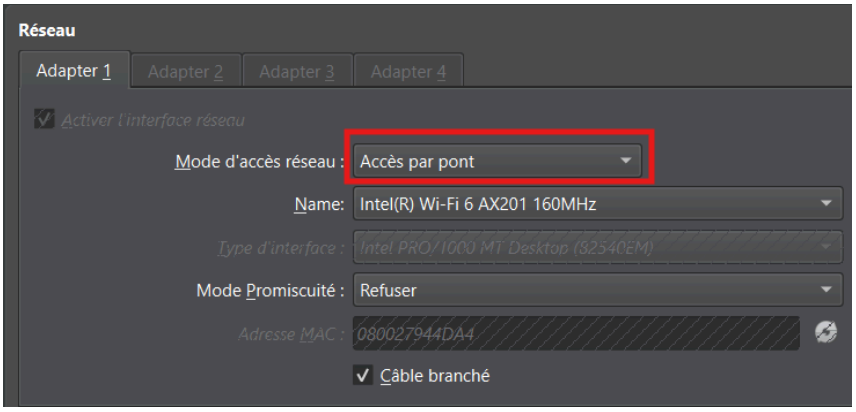


Configuration Réseau (Hôte - VM)

Pour que notre VM (Hôte) rejoint ce réseau `192.168.1.x`, nous modifions sa configuration dans VirtualBox.

Nous réglons le "Mode d'accès réseau" sur **"Accès par pont" (Bridged Adapter)**. Ce mode permet à la machine virtuelle de "traverser" le PC et de se connecter **directement à la box Internet** (le routeur).

Elle agit comme un appareil physique distinct et demandera sa propre adresse IP au routeur, garantissant ainsi qu'elle sera sur le **même réseau local** que notre PC Client.



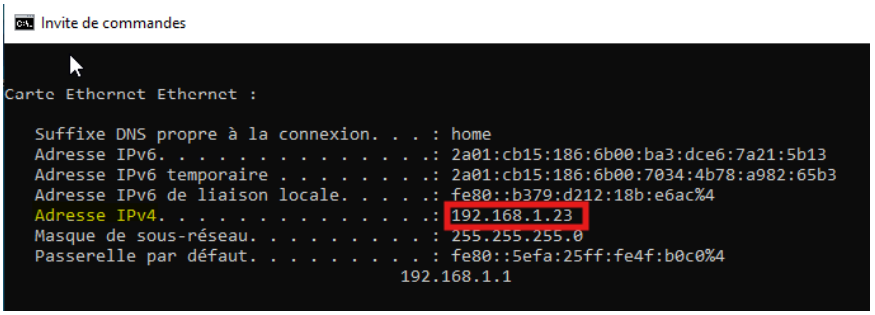
Vérification de l'IP Hôte (VM)

Une fois la VM démarrée avec sa carte réseau en accès par pont, nous devons vérifier l'adresse IP qu'elle a reçue de la box Internet.

À l'intérieur de la VM, nous ouvrons une **Invite de commandes (`cmd`)** et nous tapons la commande `ipconfig`. La capture confirme que notre configuration a fonctionné :

- L'adresse IPv4 de la VM est **`192.168.1.23`**.
- Cette adresse est bien sur le **même sous-réseau** que notre PC Client (qui était en `192.168.1.16`).

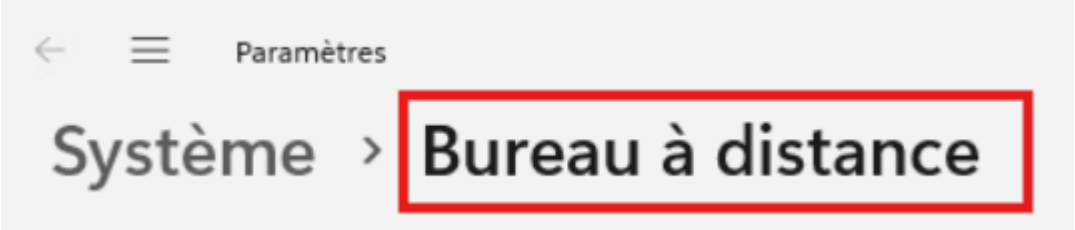
Les deux machines peuvent désormais communiquer.



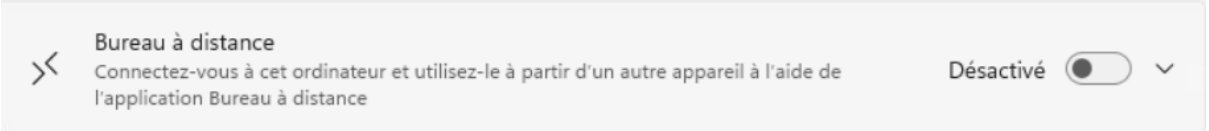
Activation du Bureau à distance (Hôte - VM)

Maintenant que notre VM Hôte est correctement configurée sur le réseau, nous devons y activer la fonction "serveur" RDP.

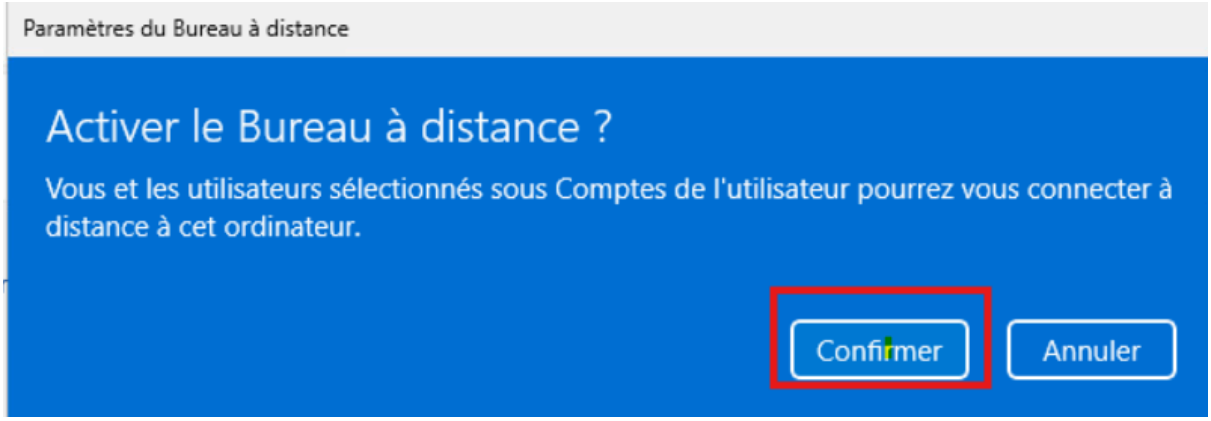
Sur la VM (Windows 10 Pro), nous allons dans les `Paramètres` > `Système` > **`Bureau à distance`**.



Par défaut, cette fonctionnalité est **"Désactivé"**.
Nous cliquons sur l'interrupteur pour l'activer.



Windows affiche un avertissement de sécurité.
Nous cliquons sur **"Confirmer"** pour autoriser les connexions à distance sur cet ordinateur.

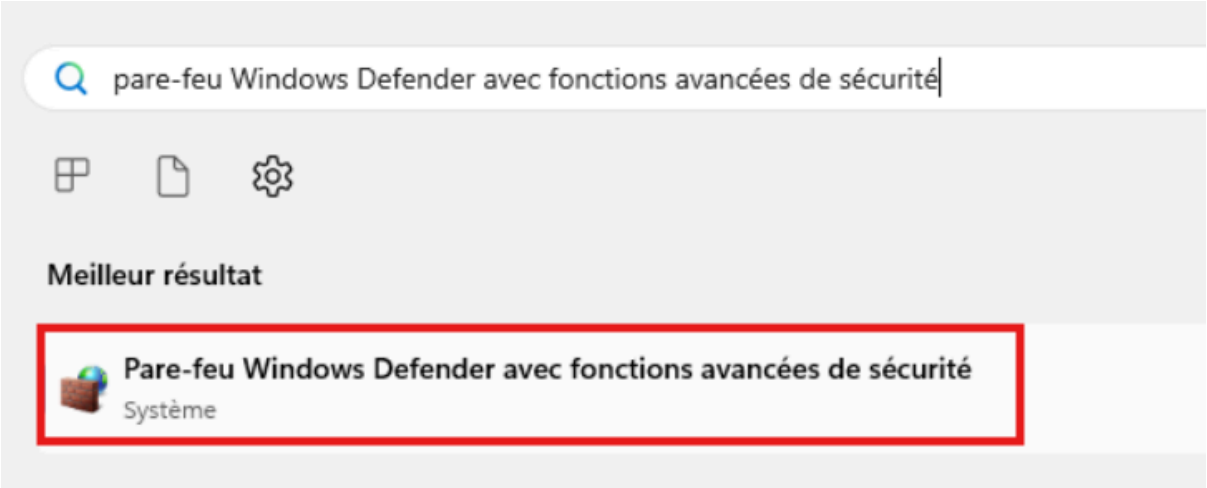


Le service RDP est maintenant en écoute sur la machine hôte.

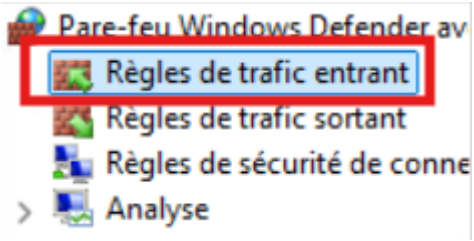
Vérification du Pare-feu (Hôte - VM)

Une fois le service RDP activé, il faut s'assurer que le **Pare-feu Windows** ne bloque pas la connexion entrante.

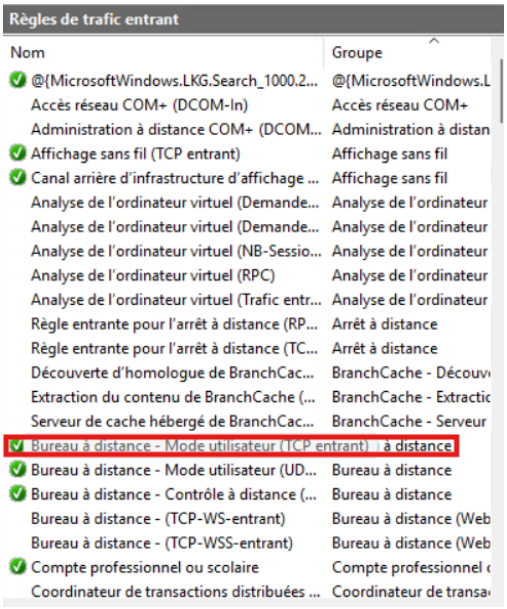
1. Sur la VM (Hôte), nous ouvrons le **"Pare-feu Windows Defender avec fonctions avancées de sécurité"**.



Nous cliquons sur **"Règles de trafic entrant"** pour inspecter les ports ouverts.

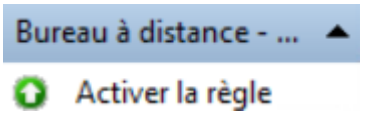


Nous cherchons les règles nommées "Bureau à distance". Le plus souvent, l'étape 5 (activer RDP) active déjà ces règles.



Nous vérifions que la règle **"Bureau à distance - Mode utilisateur (TCP entrant)"** (qui concerne le port TCP 3389) est bien active (coche verte).

Si elle était désactivée (coche grise), nous devrions faire un clic droit et **"Activer la règle"** pour autoriser la connexion.

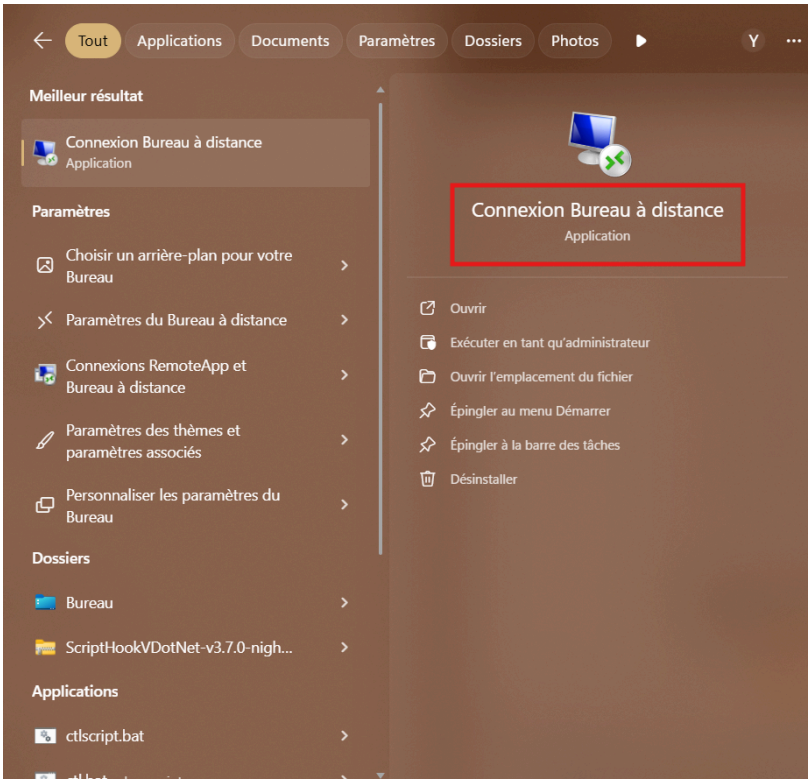


Établissement de la Connexion (Client - PC)

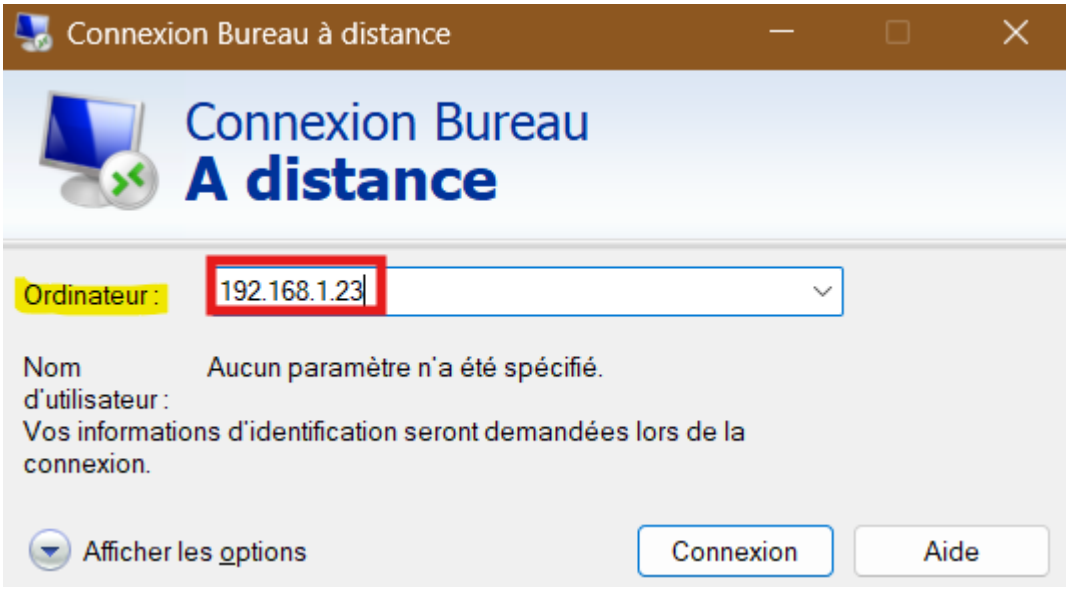
La configuration est terminée.

Nous retournons sur notre **PC Client (Windows 11)** pour initier la connexion.

1. Nous lançons l'application "Connexion Bureau à distance"

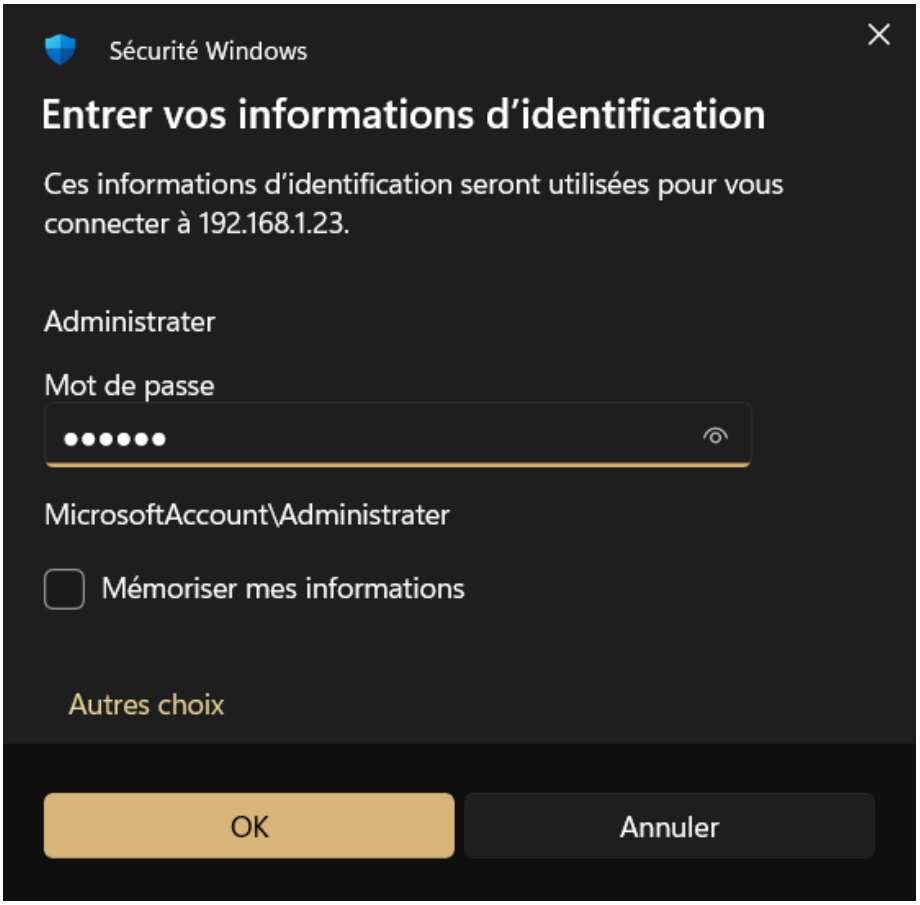


Dans le champ "Ordinateur", nous entrons l'adresse IP de notre VM Hôte, que nous avons identifiée dans le cmd : **`192.168.1.23`**

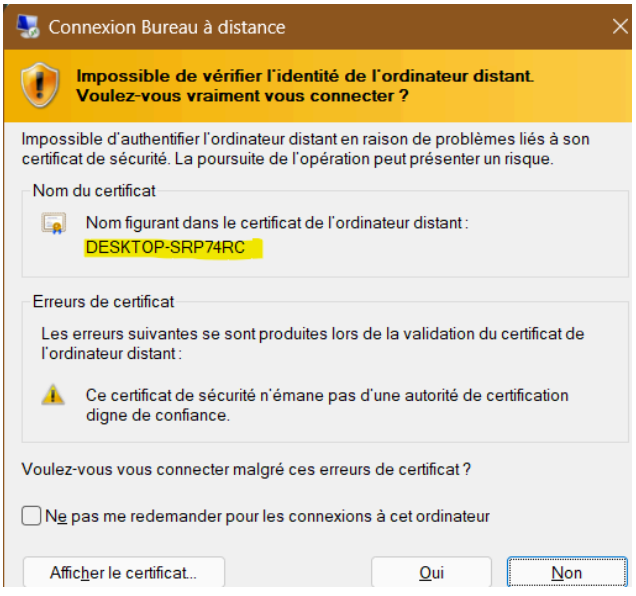


Une fenêtre de sécurité s'ouvre, nous demandant les informations d'identification **de la VM**.

Nous saisissons le nom d'utilisateur et le mot de passe du compte administrateur de notre Windows 10



Un avertissement de certificat apparaît. C'est un comportement **normal** en réseau local, car la VM utilise un certificat "auto-signé" que notre PC ne connaît pas. Nous cliquons sur **"Oui"** pour valider la connexion.



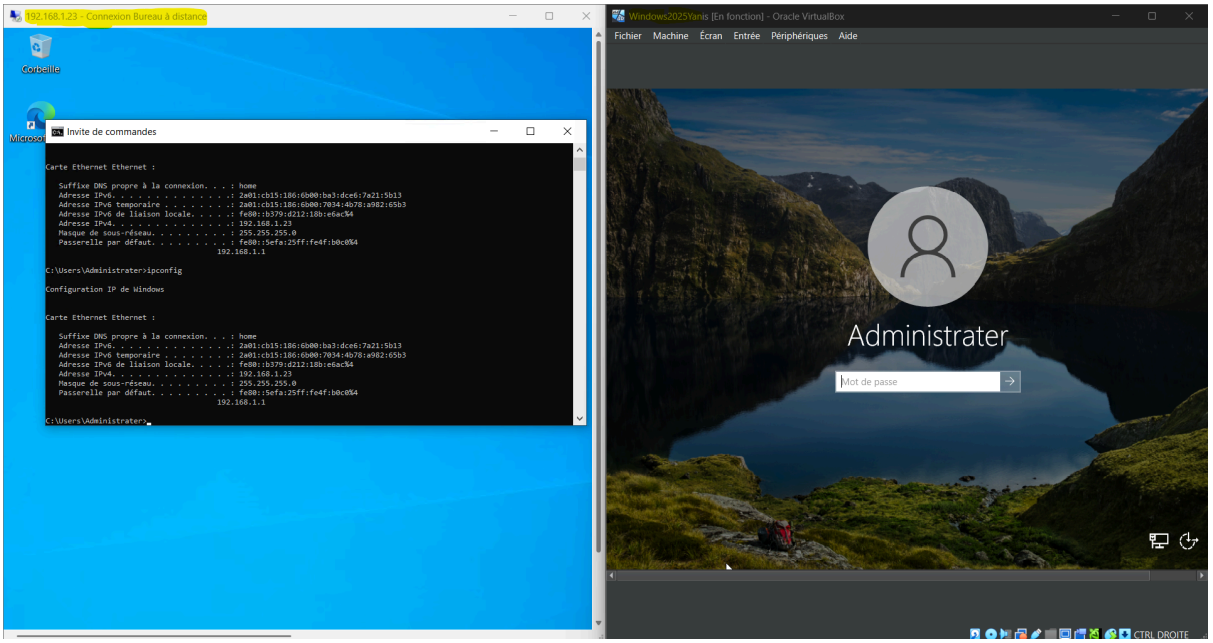
La connexion est établie et le bureau de la machine virtuelle s'affiche sur notre PC.

Connexion Réussie et Observation Clé

La connexion est établie avec succès, comme le montre la capture d'écran.

On observe deux choses distinctes et fondamentales :

1. **Sur la gauche (PC Client)** : C'est la fenêtre "Connexion Bureau à distance" de notre PC Windows 11. Nous avons un contrôle total sur le bureau de la VM distante (on y voit l'invite de commandes avec l'IP `192.168.1.23`).
2. **Sur la droite (Hôte VM)** : C'est la fenêtre de la console VirtualBox. Au moment exact où la connexion RDP s'est établie, la session sur la machine hôte a été **automatiquement verrouillée**, affichant l'écran de connexion "Administrater".



C'est une **différence majeure** avec AnyDesk : RDP ne fait pas de *partage d'écran*.
Il ouvre une **session utilisateur privée et exclusive**.
Si quelqu'un était physiquement devant la machine hôte, il ne pourrait pas voir ce que nous faisons, il verrait juste cet écran de verrouillage.

Introspection (Mon analyse)

Mon analyse pour RDP est très différente de celle d'AnyDesk. Avec AnyDesk, j'avais été surpris par la simplicité. Ici, j'ai d'abord été surpris par la **difficulté**.

Ma toute première tentative a échoué (quand j'ai essayé de me connecter à la VM via vSphere). J'ai tout de suite compris que RDP n'est **pas "magique" comme AnyDesk**.

Il ne peut pas traverser Internet tout seul, juste avec un ID. Il est fait pour fonctionner *à l'intérieur* d'un **réseau local**.

Ça m'a forcé à comprendre ce que "être sur le même réseau" veut dire. J'ai dû créer une VM sur mon propre PC, mais même là, ça n'a pas marché du premier coup (j'avais une IP en `192.168.56.x`). J'ai dû chercher dans les réglages de VirtualBox et trouver le mode **"Accès par pont"**.

C'est là que j'ai eu le déclic : ce mode a permis à ma VM d'aller chercher une IP sur ma box, et de se retrouver sur le même réseau (`192.168.1.x`) que mon PC.

RDP m'a forcé à réfléchir au réseau, là où AnyDesk faisait tout pour moi.

L'autre grande découverte, c'est ce qui s'est passé à la fin. Quand je me suis connecté, l'écran de ma VM s'est **verrouillé**. AnyDesk *partage* l'écran (on voit la même chose, c'est fait pour aider). RDP, lui, **ouvre une session privée**. C'est fait pour l'administration, pour que je puisse travailler sur un serveur sans que personne ne voie ce que je fais (ou ne me dérange).

En résumé, RDP est un vrai outil d'administration, plus puissant, mais **beaucoup moins simple** à mettre en place pour un dépannage rapide.

Bureau à distance Chrome (Chrome Remote Desktop)

Qu'est-ce que le Bureau à distance Chrome ?

Le Bureau à distance Chrome (Chrome Remote Desktop) est un service gratuit développé par Google qui permet à un utilisateur de contrôler à distance un autre ordinateur.

Contrairement à RDP qui est un protocole intégré à Windows, Chrome Remote Desktop fonctionne comme une application web et une extension **à l'intérieur du navigateur Google Chrome**. L'authentification et la connexion ne se basent pas sur une adresse IP, mais sur le **compte Google** de l'utilisateur et un code PIN personnel.

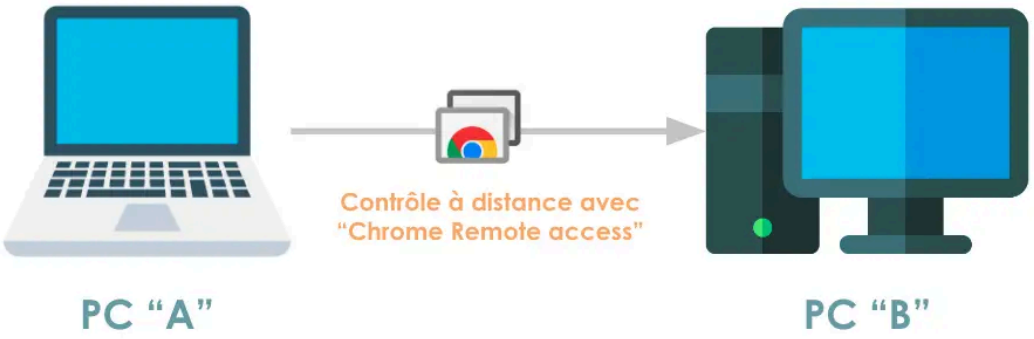
Principales caractéristiques de Chrome Remote Desktop

1. **Basé sur le compte Google :** L'authentification principale repose sur la connexion au même compte Google sur les deux machines. C'est ce qui remplace le besoin de connaître une IP ou un ID.
2. **Multi-plateforme :** Fonctionne sur n'importe quel ordinateur (Windows, Mac, Linux) où Google Chrome peut être installé, ainsi que sur les appareils mobiles (Android, iOS).
3. **Partage d'écran :** Tout comme AnyDesk (et contrairement à RDP), il effectue du **partage de session**. L'utilisateur sur la machine hôte peut voir tout ce que l'utilisateur distant fait en temps réel.
4. **Traverse les réseaux (NAT) :** Tout comme AnyDesk, il utilise les serveurs de Google pour la mise en relation. Il n'y a **aucune configuration de pare-feu** ou de routeur (box Internet) à effectuer.
5. **Sécurité :** La connexion est entièrement chiffrée (via les protocoles web sécurisés de Google) et nécessite un **code PIN** personnel défini par l'utilisateur pour l'accès non surveillé.

Comment fonctionne Chrome Remote Desktop :

Le service fonctionne en deux modes :

- **Assistance à distance :** Un utilisateur génère un code à usage unique pour une aide ponctuelle.
- **Accès à distance (celui que nous allons tester) :**
    1. L'utilisateur installe l'application "Hôte" sur la machine à contrôler (la VM).
    2. Cette application s'enregistre auprès des serveurs de Google et s'associe au compte Google de l'utilisateur. Un code PIN est créé.
    3. Sur la machine Client, l'utilisateur se connecte au même compte Google via le site `remotedesktop.google.com`.
    4. Google affiche la liste des machines "Hôtes" associées à ce compte.
    5. En cliquant sur la machine, Google demande le code PIN.
    6. Après vérification, une connexion chiffrée (WebRTC) est établie entre les deux navigateurs.



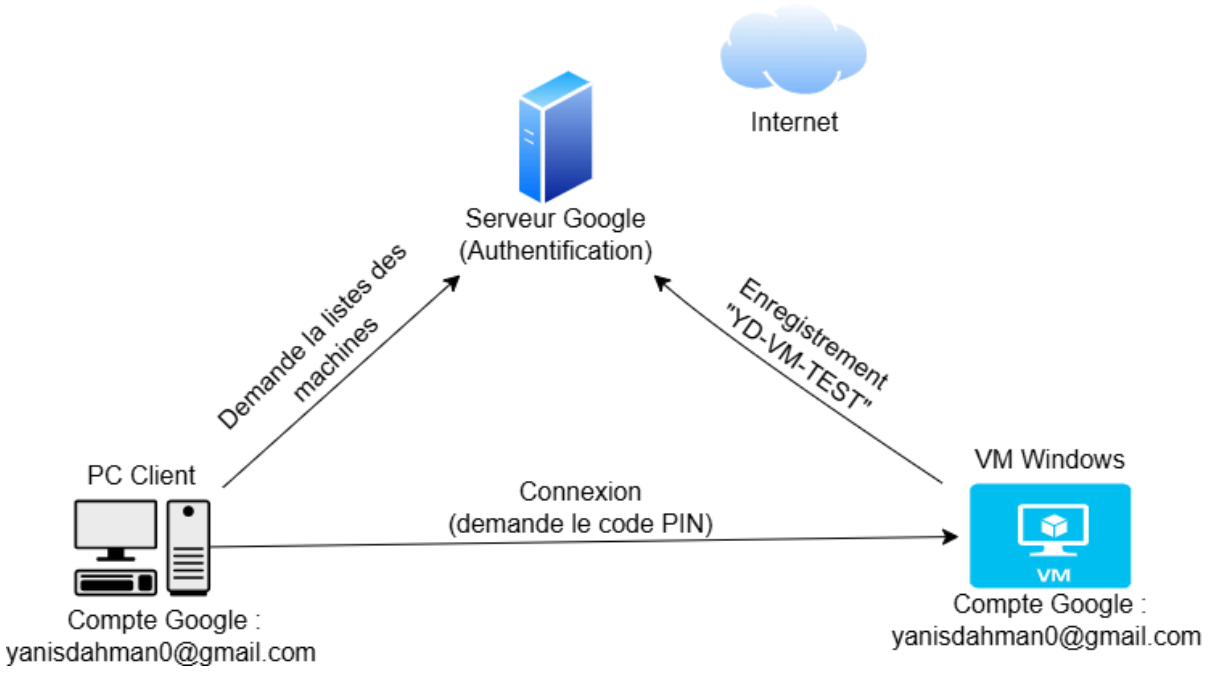
Avantages de l'utilisation de Chrome Remote Desktop

- **Zéro configuration réseau :** Fonctionne instantanément sur Internet sans avoir à régler d'adresse IP, de ports ou de pare-feu.
- **Totalement gratuit :** Solution 100% gratuite, sans version "Pro" payante ni détection d'usage commercial.
- **Excellente multi-compatibilité :** Fonctionne sur tous les systèmes (Windows, Mac, Linux) via le navigateur Chrome.
- **Installation simplifiée :** L'installation se fait en quelques clics via une simple extension de navigateur et un petit service.
- **Authentification unifiée :** Utilise la sécurité de votre compte Google et un code PIN personnel, ce qui est souvent plus simple à gérer qu'un ID ou un compte Windows.

Chrome Remote Desktop face aux autres solutions d'accès à distance

Fonctionnalité	RDP	VNC	TeamViewer	SSH	Chrome Remote Desktop
Interface graphique de support	Oui	Oui	Oui	Limité (Texte)	**Oui (via Navigateur)**
Port par défaut	3389	5900	5938 (ou 443)	22	**443 (Web)**
Chiffrement	Oui	Optionnel	Oui	Oui	**Oui**
Multiplateforme	Limité (Serveur Windows)	Oui	Oui	Oui	**Oui**
Transfert de fichiers	Oui	Limité	Oui	Oui (via SCP)	**Oui**
Performance	Élevée (en local)	Modérée	Élevée	Élevée (CLI)	**Modérée à Élevée**

Schéma de l'infrastructure



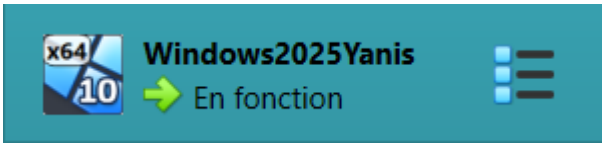
Utilisation de Chrome Remote Desktop

Préparation de la Machine Hôte

Pour ce test, la machine "Hôte" (celle qui sera contrôlée) est la même machine virtuelle Windows 10 que celle utilisée pour RDP, configurée en mode "Accès par pont" pour avoir un accès à Internet.

Une différence majeure avec RDP est que Chrome Remote Desktop **n'exige pas une version "Pro" de Windows**.

Il peut être installé sur n'importe quelle édition (y compris "Famille"), car il ne dépend pas des services Windows mais uniquement du navigateur Google Chrome.

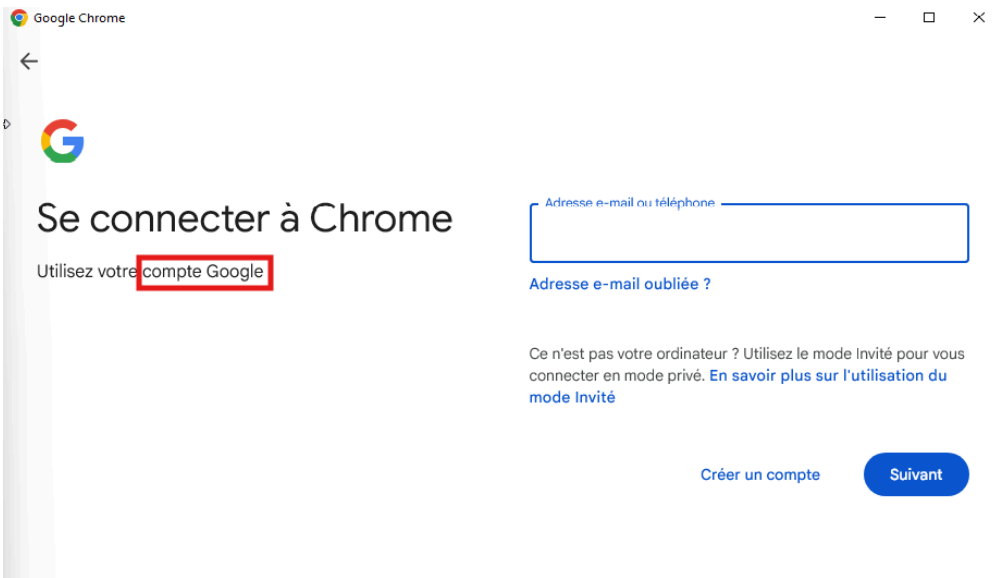


Connexion au compte Google (Hôte - VM)

La première étape se déroule sur la **VM Hôte (Windows 10)**.

Contrairement à RDP qui utilise un compte Windows ou AnyDesk qui utilise un ID, Chrome Remote Desktop lie l'ordinateur à un **compte Google**.

Nous nous connectons donc au navigateur Google Chrome avec le compte qui servira à l'authentification. Ce même compte devra être utilisé sur la machine Client pour retrouver cet ordinateur.

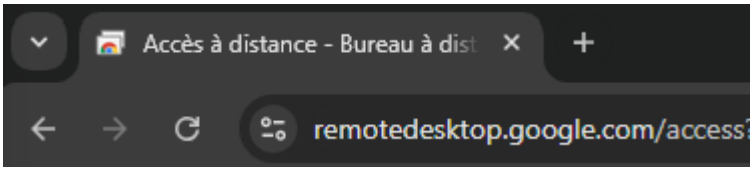


Accès au service (Hôte - VM)

Une fois connecté au compte Google, nous accédons au portail de service de Chrome Remote Desktop.

Sur la **VM Hôte**, nous saisissons l'URL `remotedesktop.google.com/access` dans la barre d'adresse.

C'est depuis cette page que nous allons configurer l'ordinateur pour qu'il puisse être contrôlé à distance, sans avoir besoin de connaître son adresse IP.



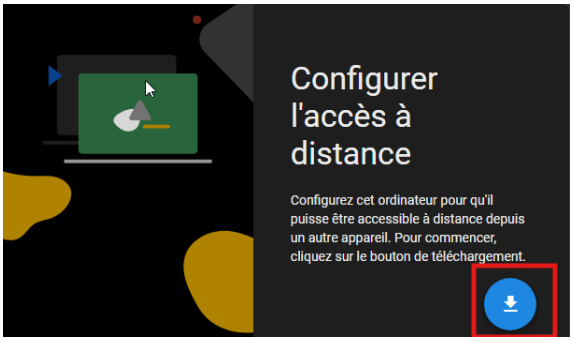
Installation du service Hôte (sur la VM)

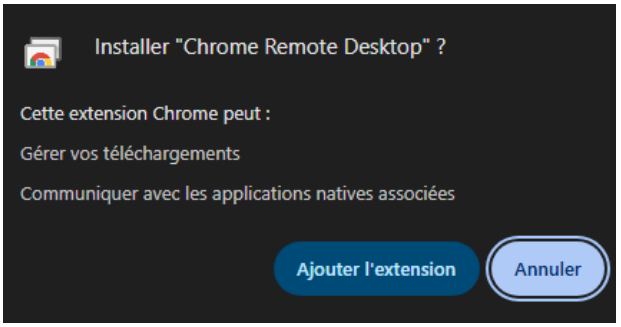
Une fois sur le portail, nous cliquons sur le bouton de téléchargement pour "Configurer l'accès à distance".

Le processus d'installation se fait en deux parties :

1. **Une extension Chrome** (`Chrome Remote Desktop`) qui s'intègre au navigateur.
2. **Un service Hôte** (`.msi`) qui s'installe sur Windows et permet à la machine d'être contrôlée même si Chrome est fermé.

Nous installons les deux composants pour transformer cette VM en Hôte accessible.



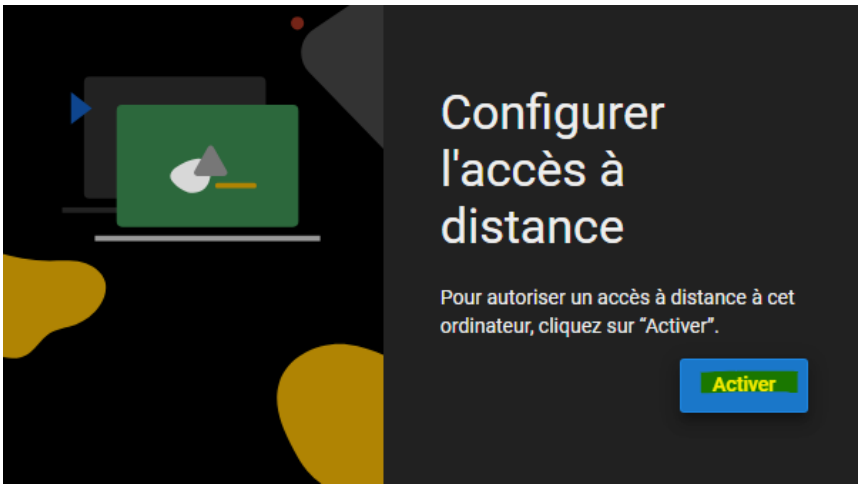


Activation du service Hôte (sur la VM)

Une fois l'extension et le service hôte installés, la page web `remotedesktop.google.com` se met à jour.

Le bouton de téléchargement a été remplacé par un bouton **"Activer"**.

Nous cliquons dessus pour démarrer le processus d'enregistrement de cette machine sur notre compte Google et la rendre accessible à distance.

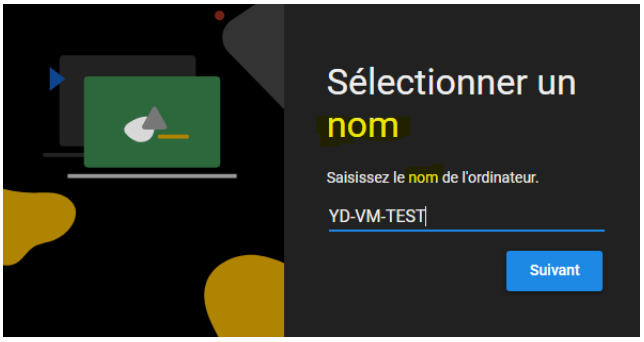


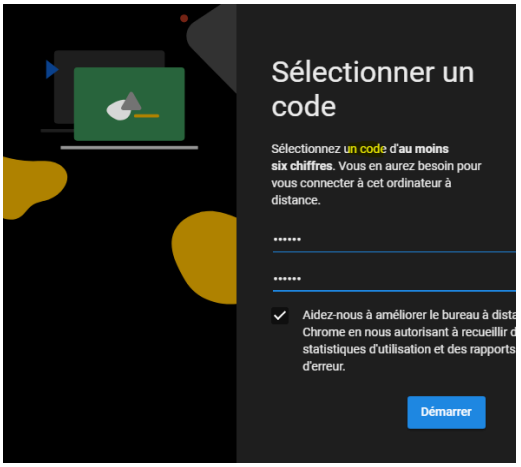
Nommage et création du Code PIN (Hôte - VM)

Une fois le service activé, le processus de configuration continue :

1. **Nommage :** Nous devons d'abord donner un nom à notre machine hôte . C'est ce nom qui apparaîtra dans notre liste d'appareils, au lieu d'une adresse IP ou d'un ID.
2. **Sécurité :** Ensuite, nous devons définir un **code PIN** d'au moins 6 chiffres. Ce code est la deuxième couche de sécurité après le compte Google ; il sera demandé à chaque tentative de connexion.

Une fois le code PIN créé, le service démarre et la machine est enregistrée comme "En ligne".



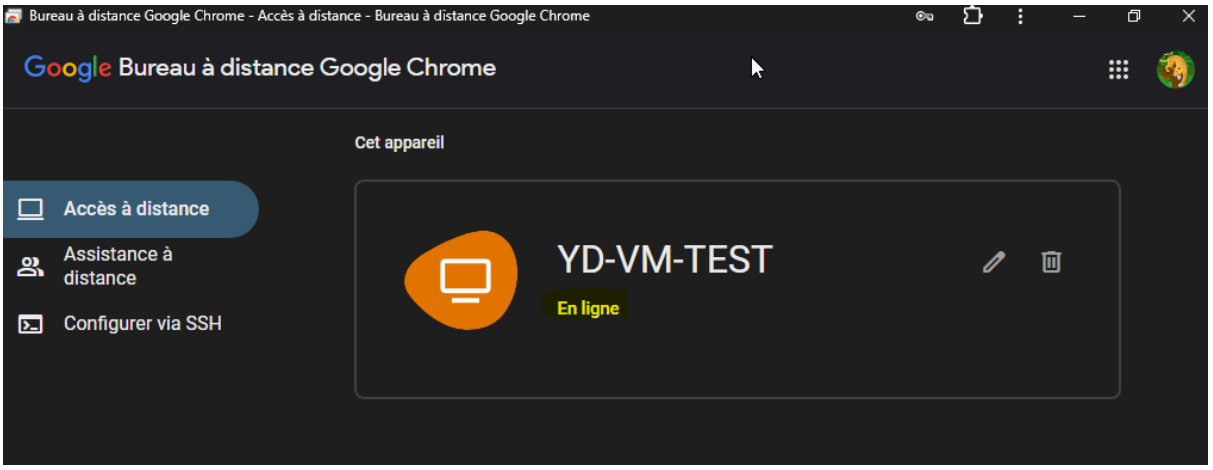


Hôte "En Ligne" (sur la VM)

Après avoir autorisé le service à s'exécuter et défini notre code PIN, l'installation sur la VM Hôte est terminée.

La page `remotedesktop.google.com` confirme que notre machine, "YD-VM-TEST", est maintenant **"En ligne"**. Elle est enregistrée sur mon compte Google et est prête à recevoir une connexion.

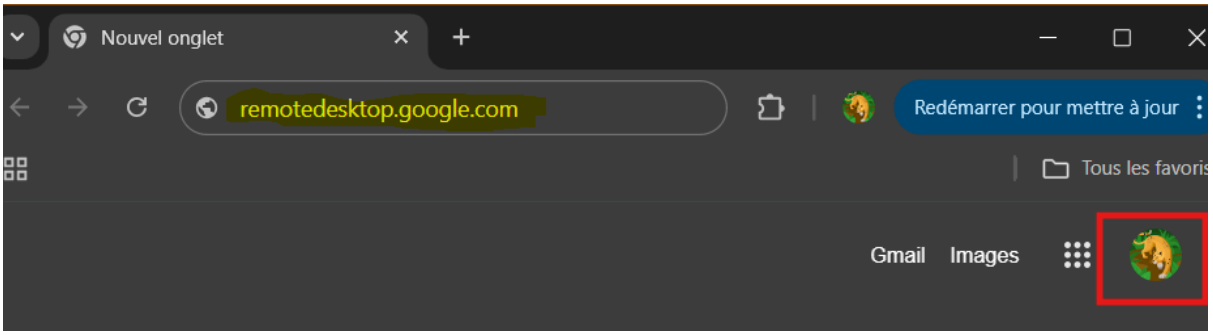
Toute la configuration de l'Hôte est finie. Nous allons maintenant passer sur le **PC Client**.



Lancement de la Connexion (sur le PC Client)

Nous passons maintenant sur le **PC Client (Windows 11)**.

Nous nous connectons au **même compte Google** que sur la VM et nous allons sur `remotedesktop.google.com/access`.

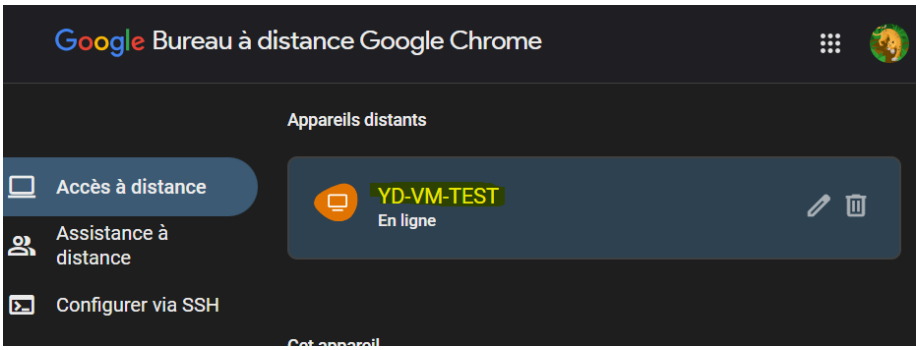


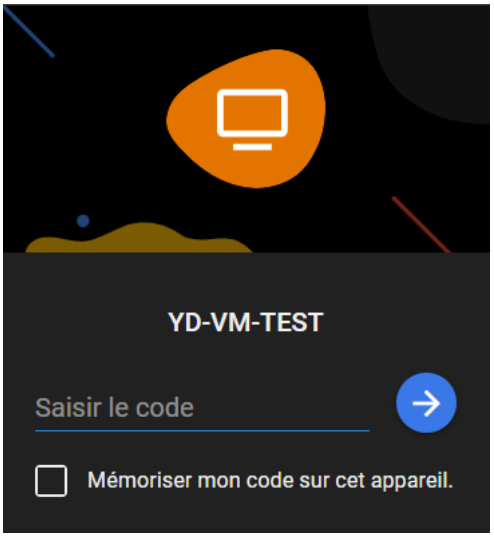
Authentification Finale (sur le PC Client)

Après avoir cliqué sur la machine hôte, le service tente d'établir la connexion et demande la deuxième couche de sécurité.

Une fenêtre s'ouvre pour nous demander le **code PIN**. C'est le code à 6 chiffres que nous avons créé sur la VM Hôte. C'est cette étape qui garantit que seule une personne connaissant le compte Google **et** le code PIN peut prendre le contrôle.

Nous saisissons le code PIN pour valider.





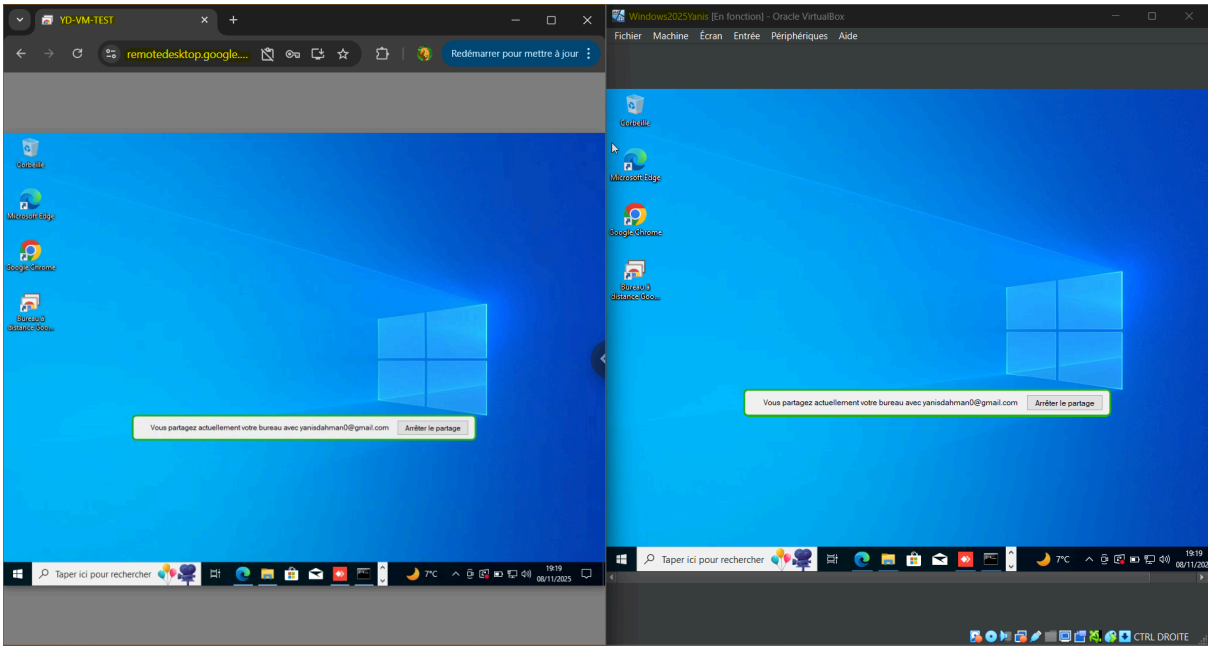
Connexion Réussie et Observation Clé

Après avoir saisi le bon code PIN, la connexion s'établit immédiatement.

La capture d'écran finale montre le bureau de notre PC Client (Windows 11) contrôlant la VM Hôte **à l'intérieur d'un onglet du navigateur Google Chrome**.

On observe une différence fondamentale par rapport à RDP :

- **Avec RDP**, la session de l'hôte est **verrouillée**.
- **Avec Chrome Remote Desktop**, la session sur la VM reste ouverte. C'est du **partage d'écran**, similaire à AnyDesk. Si quelqu'un était devant la VM, il verrait la souris bouger toute seule.



Introspection (Mon analyse)

Mon analyse pour Chrome Remote Desktop est que c'est un **hybride** très intéressant entre la simplicité d'AnyDesk et un système de sécurité plus personnel.

L'installation m'a surpris. Je n'ai pas eu à gérer d'adresse IP (comme pour RDP) ni à échanger un ID (comme pour AnyDesk).

Tout était lié à mon **compte Google**. C'est ce qui a servi de clé. J'ai dû être connecté au même compte des deux côtés, et le service a immédiatement su quelle machine était "En ligne".

Le schéma que j'ai dessiné ressemblait beaucoup à celui d'AnyDesk, et j'ai compris pourquoi : ils utilisent tous les deux un serveur central sur Internet pour "l'annuaire". Mais l'identifiant est totalement différent. Je trouve que l'identifiant (le compte Google) est plus sécurisé et plus facile à mémoriser qu'un ID aléatoire.

La deuxième sécurité était le **code PIN**. C'est une bonne idée : même si quelqu'un a mon mot de passe Google, il ne peut pas se connecter sans ce code que j'ai défini.

Enfin, comme AnyDesk, c'est du **partage d'écran**. Quand je me suis connecté, l'écran de la VM n'a pas été verrouillé (contrairement à RDP).

En résumé, Chrome Remote Desktop est la solution parfaite pour un usage personnel, pour accéder à *ses propres* machines. Sa seule contrainte est qu'il oblige à être dans l'écosystème Google. C'est moins "universel" qu'AnyDesk pour dépanner un inconnu, et moins "professionnel" que RDP pour un parc d'entreprise.

AnyDesk

Qu'est-ce que AnyDesk ?

AnyDesk est un logiciel de bureau à distance qui permet aux utilisateurs d'accéder et de contrôler des ordinateurs à distance.
Facilitant ainsi le support, la collaboration et la gestion des tâches informatiques depuis n'importe quel endroit.
Lancé en 2014, AnyDesk est rapidement devenu un choix populaire pour les particuliers et les entreprises, reconnu pour sa rapidité, sa sécurité et sa facilité d'utilisation.

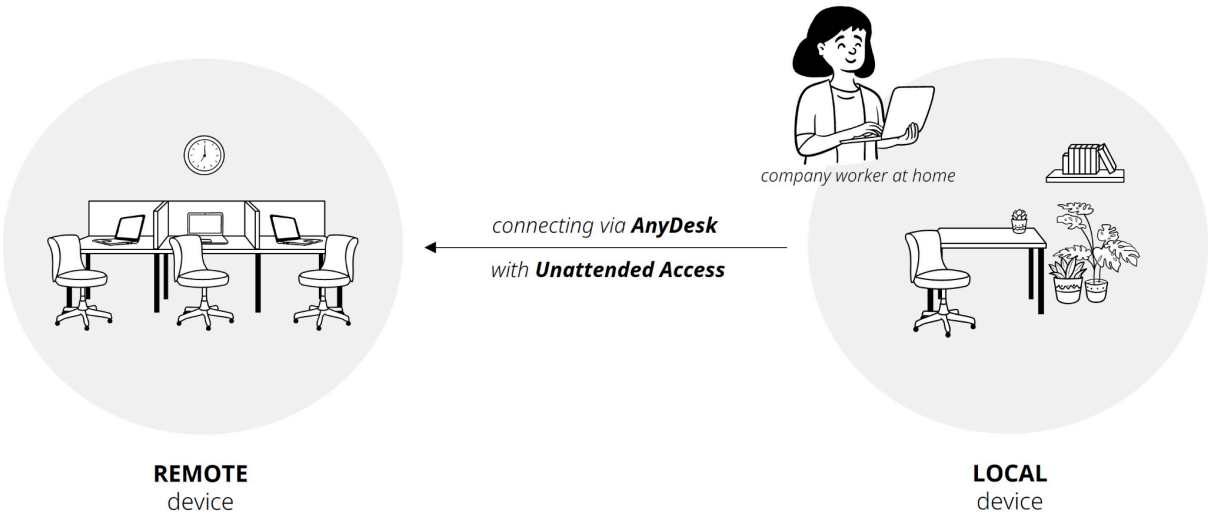
Principales caractéristiques d'AnyDesk

1. **Connexion par ID :** N'utilise pas d'adresse IP mais un **ID unique** (ex: 123 456 789) pour identifier chaque machine. C'est ce qui le rend si simple à utiliser sur Internet.
2. **Traverse les pare-feu (NAT) :** Utilise un serveur d'annuaire central pour mettre en relation les machines. Il n'y a **aucune configuration de pare-feu** ou de routeur (box) à faire.
3. **Haute Performance (Codec DeskRT) :** Utilise un codec vidéo propriétaire (DeskRT) conçu pour être extrêmement rapide et fluide, même avec de faibles connexions Internet.
4. **Multiplateforme :** Fonctionne sur quasiment tous les systèmes d'exploitation (Windows, macOS, Linux, Android, iOS), permettant de contrôler un PC depuis un téléphone, par exemple.
5. **Mode "Partage d'écran" :** C'est un outil de **partage** et de collaboration. L'hôte et le client voient le même écran et peuvent interagir, ce qui est l'opposé du mode "session privée" de RDP.
6. **Sécurité :** Utilise un chiffrement de niveau militaire (TLS 1.2) et une vérification de connexion (l'hôte doit cliquer sur "Accepter").

Comment fonctionne AnyDesk

AnyDesk fonctionne sur un modèle client-serveur. Il est conçu pour être simple et traverser les réseaux sans aucune configuration.

1. **Enregistrement (Annuaire) :** Au démarrage, le logiciel AnyDesk sur l'ordinateur **Hôte** se connecte aux serveurs d'annuaire d'AnyDesk (sur Internet). Il s'enregistre et reçoit un **numéro d'identification unique** (ex: `1 023 068 792`). Cet ID est l'adresse publique de la machine.
2. **Demande de Connexion (Client) :** L'utilisateur sur l'ordinateur **Client** ouvre AnyDesk et saisit l'ID de l'Hôte qu'il souhaite contrôler. Cette demande est envoyée aux serveurs d'annuaire d'AnyDesk.
3. **Mise en Relation (Broker) :** Le serveur d'annuaire (aussi appelé "broker") reçoit la demande, vérifie que l'ID de l'Hôte est "En ligne", et transmet la demande de connexion à l'Hôte.
4. **Connexion Directe (Peer-to-Peer) :** Une fois que l'Hôte accepte la connexion (en cliquant sur "Accepter"), AnyDesk tente d'établir une **connexion directe chiffrée (Peer-to-Peer)** entre le Client et l'Hôte. C'est ce qui permet une grande rapidité.
5. **Partage d'Écran :** Contrairement à RDP qui ouvre une session privée, AnyDesk **partage l'écran existant**. Le Client voit exactement ce que l'Hôte voit, et les deux peuvent interagir en même temps.



Avantages de l'utilisation d'AnyDesk

- **Zéro configuration :** Fonctionne immédiatement sans aucun réglage réseau (pas besoin de connaître d'IP, de ports ou de pare-feu).
- **Connexion par ID :** Utilise un numéro d'identification simple pour trouver un ordinateur n'importe où sur Internet.
- **Haute performance :** Très rapide et fluide, même sur des connexions Internet lentes, grâce à son codec vidéo (DeskRT).
- **Multiplateforme :** Fonctionne sur quasiment tous les systèmes (Windows, macOS, Linux, Android, iOS).
- **Simplicité d'utilisation :** Idéal pour l'assistance rapide, car l'utilisateur n'a qu'à télécharger, lancer et communiquer son ID.
- **Mode "Partage d'écran" :** Permet à l'hôte et au client de voir la même chose et de collaborer, ce qui est parfait pour le dépannage.

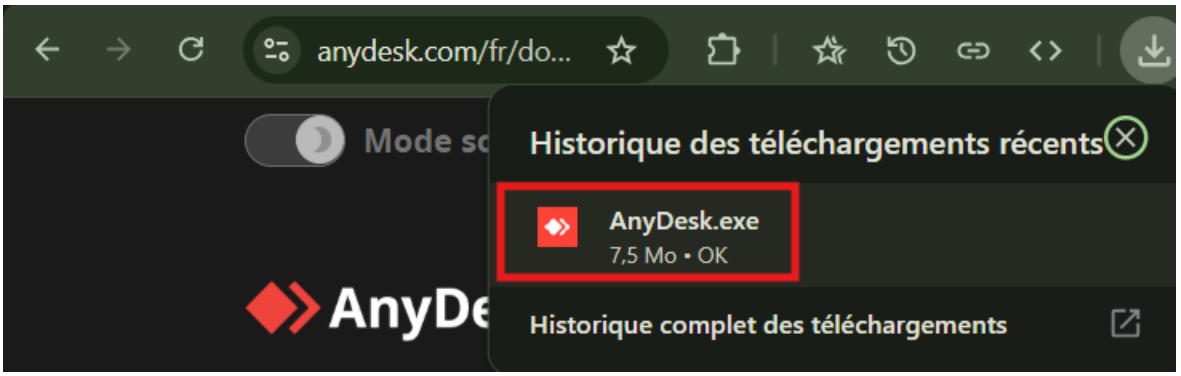
AnyDesk face aux autres solutions d'accès à distance

Fonctionnalité	**RDP**	**VNC**	**TeamViewer**	**SSH**	**AnyDesk**
Interface graphique de support	Oui	Oui	Oui	Limité (Texte)	**Oui**
Port par défaut	3389	5900	5938 (ou 443)	22	**TCP 80 et 443 (Web)**
Chiffrement	Oui	Optionnel	Oui	Oui	**Oui**
Multiplateforme	Limité (Serveur Windows)	Oui	Oui	Oui	**Oui**
Transfert de fichiers	Oui	Limité	Oui	Oui (via SCP)	**Oui**
Performance	Élevée (en local)	Modérée	Élevée	Élevée (CLI)	**Élevée**

Utilisation d’AnyDesk

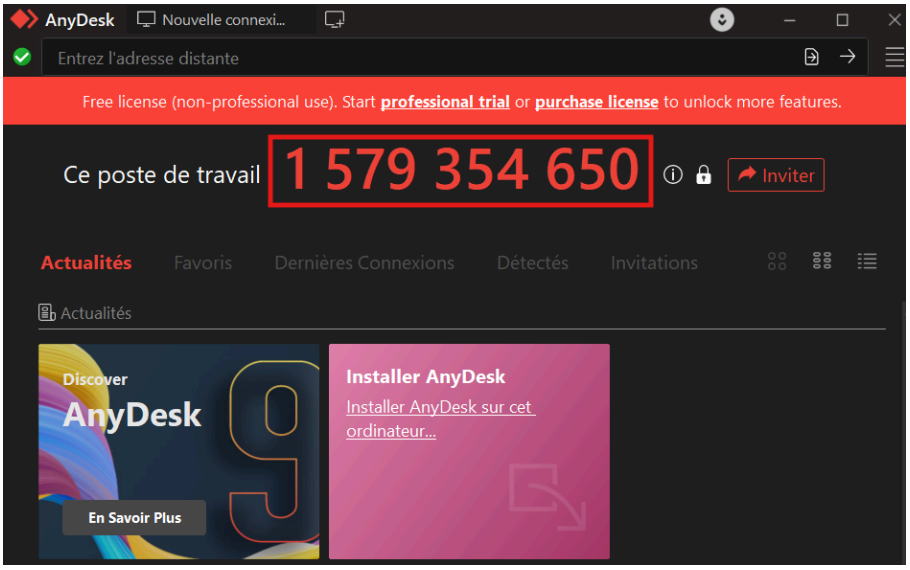
Installation sur le PC Client (Windows 11)

La première étape consiste à télécharger le logiciel depuis une source fiable. Nous nous rendons sur le site officiel anydesk.com.
Sur la page d'accueil, nous cliquons sur le bouton "Télécharger" (entouré en rouge) pour obtenir la dernière version du client compatible avec notre système d'exploitation (Windows dans ce cas).



Exécution sur le PC Client (Windows 11)

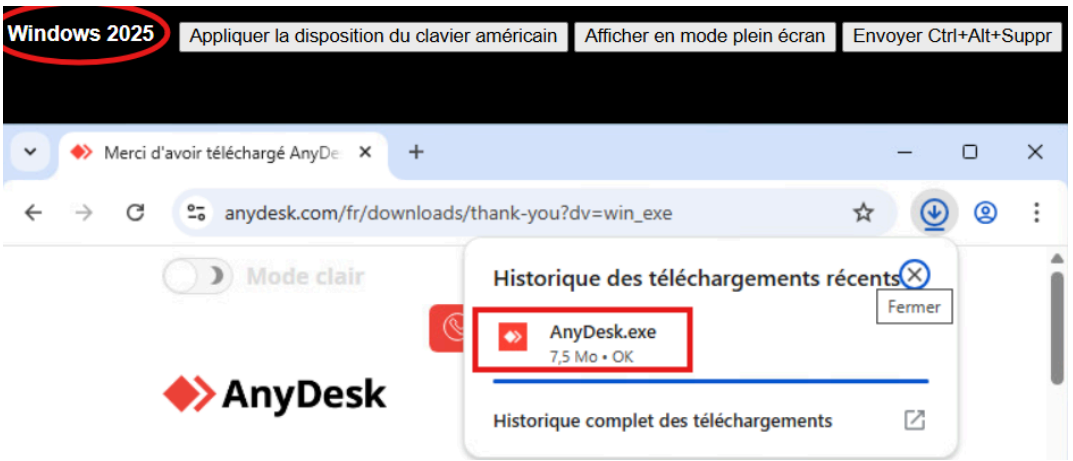
Une fois le fichier `.exe` téléchargé, nous exécutons. AnyDesk se lance alors en mode "portable" (sans installation complète). La fenêtre principale affiche deux informations capitales :



"Votre adresse (encadré en rouge) : Il s'agit de l'identifiant (ID) unique de 9 chiffres de ce poste de travail. C'est cette adresse que nous devrons communiquer à une personne distante pour qu'elle puisse prendre le contrôle de notre machine.
"Entrer l'adresse du poste distant" (encadré en vert) : C'est dans ce champ que nous devons saisir l'ID de l'ordinateur auquel nous souhaitons nous connecter.

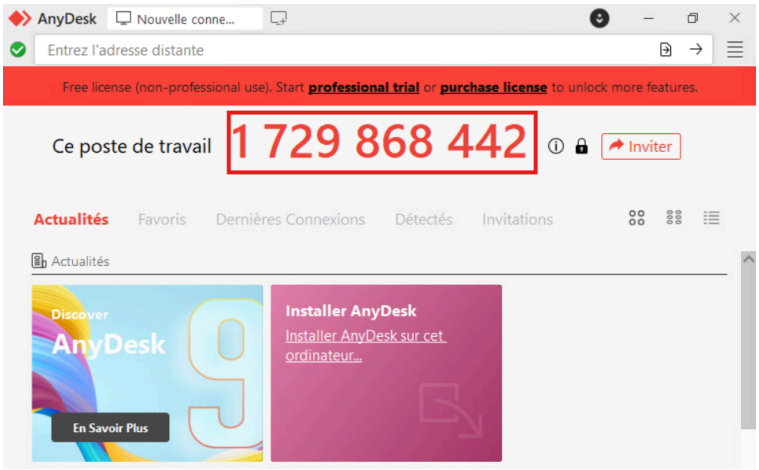
Installation sur le Serveur Hôte (VM Windows 2025)

La première étape consiste à télécharger le logiciel depuis une source fiable. Nous nous rendons sur le site officiel anydesk.com.
Sur la page d'accueil, nous cliquons sur le bouton "Télécharger" (entouré en rouge) pour obtenir la dernière version du client compatible avec notre système d'exploitation (Windows dans ce cas).



Exécution sur le Serveur Hôte (VM Windows 2025)

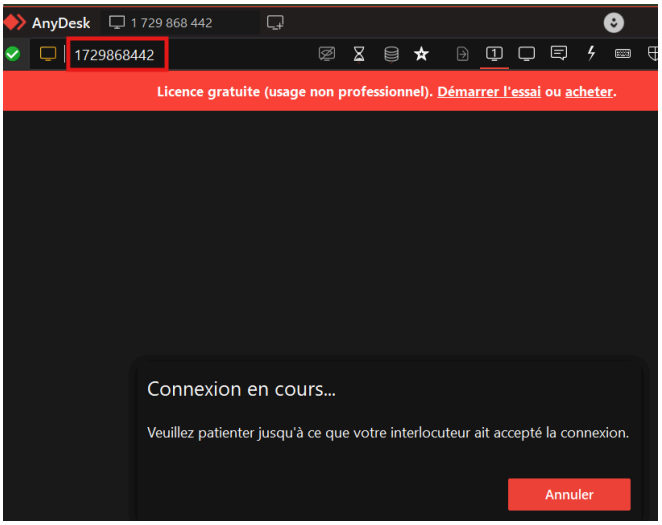
Une fois le fichier `.exe` téléchargé, nous exécutons. AnyDesk se lance alors en mode "portable" (sans installation complète). La fenêtre principale affiche deux informations capitales :



"Votre adresse (encadré en rouge) : Il s'agit de l'identifiant (ID) unique de 9 chiffres de ce poste de travail. C'est cette adresse que nous devrons communiquer à une personne distante pour qu'elle puisse prendre le contrôle de notre machine.
"Entrer l'adresse du poste distant" (encadré en vert) : C'est dans ce champ que nous devons saisir l'ID de l'ordinateur auquel nous souhaitons nous connecter.

Lancement de la Connexion (Poste Client)

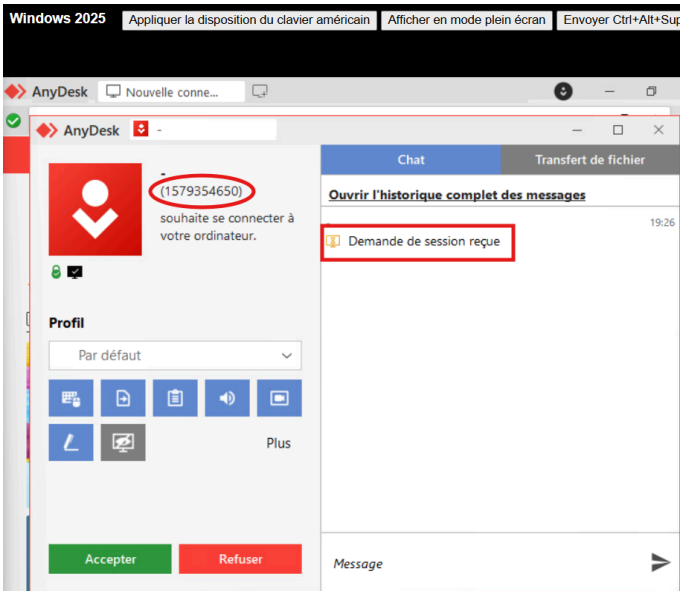
De retour sur notre machine "Client" (celle qui va prendre le contrôle), nous saisissons l'ID de notre machine distante (la VM) dans le champ de connexion.
Nous cliquons ensuite sur le bouton "Connecter" pour initier la demande de session à distance.



Acceptation de la Connexion (Poste Hôte)

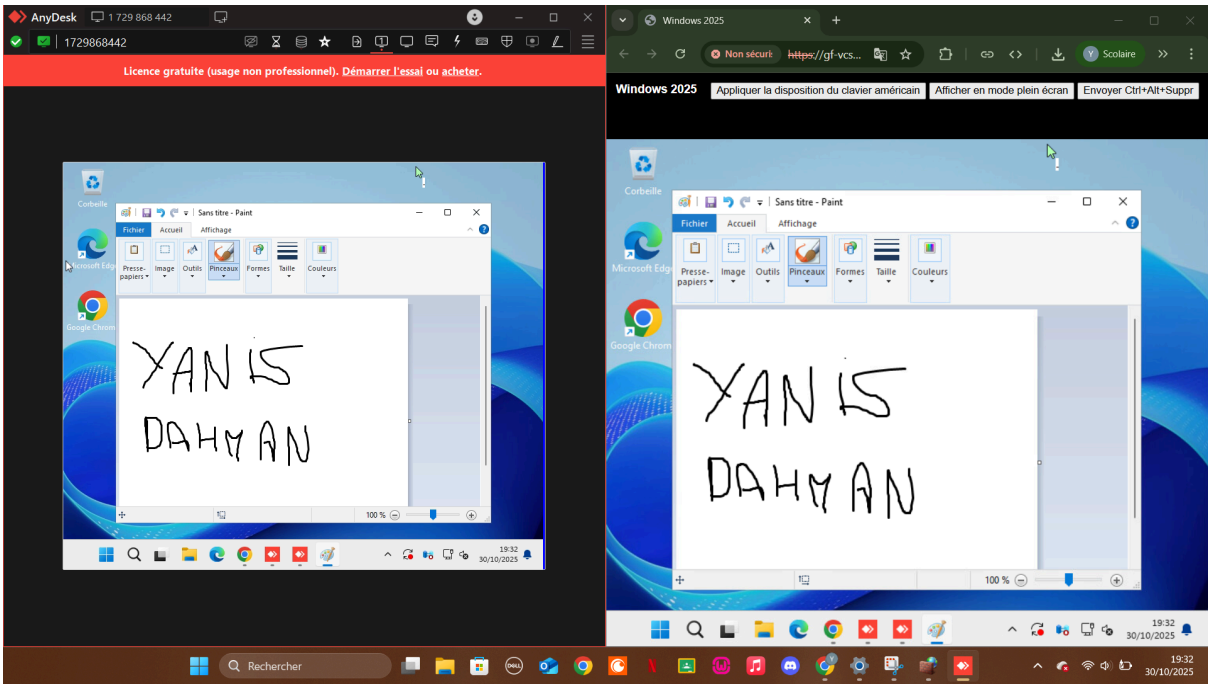
Sur la machine "Hôte" (celle qui va être contrôlée), une fenêtre de sécurité apparaît instantanément. C'est le mode de connexion "surveillé" :

- Les profils de permissions : Ils permettent à l'utilisateur hôte de limiter ce que le client peut faire ("Partage d'écran" pour juste montrer, "Standard" pour un contrôle normal, "Accès complet" avec transfert de fichiers, etc.).
- Le bouton "Accepter" (en bas) : En cliquant sur ce bouton, l'utilisateur hôte autorise la session à démarrer. Sans cette action manuelle, la connexion est impossible dans ce mode.



Connexion Établie (Vue Global)

Une fois la connexion acceptée par l'hôte (ou le mot de passe non surveillé validé), la session est active.
Sur notre poste client, le bureau de l'ordinateur distant apparaît dans une fenêtre. Nous pouvons désormais contrôler la souris et le clavier de la machine distante comme si nous étions physiquement devant, nous permettant ainsi d'effectuer des tâches de maintenance, du dépannage ou du travail à distance.



Nous pouvons ainsi observer à gauche notre poste client (PC Windows 11) qui à l’accès sur le serveur hôte (Windows 2025)

J’ai ouvert une page et écrit du texte depuis le post client afin de montrer que je possède bien l’accès à distance

Introspection (Mon Analyse)

Ce qui m'a le plus marqué avec AnyDesk, c'est à quel point c'est simple.
Je pensais qu'il faudrait régler des adresses IP ou ouvrir des ports sur ma box Internet, comme on le voit parfois en cours.
Mais là, pas du tout. Il suffit d'un simple numéro (l'ID) pour se connecter.
J'ai compris pourquoi tout le monde l'utilise pour dépanner la famille ou les amis : ça marche directement.

Le deuxième point, c'est la sécurité. Justement parce que c'est si simple, le plus gros risque, c'est l'utilisateur.
Si on donne son ID à un inconnu au téléphone (comme dans les arnaques), on lui donne les clés de son PC.
La sécurité ne dépend pas de réglages compliqués, mais juste de ne pas faire confiance à n'importe qui.

Enfin, j'ai remarqué qu'on partage son écran. La personne qui se connecte voit exactement ce que je vois, et on peut utiliser la souris en même temps.
C'est vraiment fait pour "aider" quelqu'un ou "montrer" un problème.
C'est différent d'autres outils (comme RDP) où on se connecte à un serveur de manière invisible, sans que personne ne voie ce qu'on fait