



ADMINISTRATION DES SYSTÈMES ET RÉSEAUX

LES LOGICIELS DE CONTRÔLE A DISTANCE

Version	Date	Description
1.0	03/09/2018	Version initiale

Table des matières

I. DÉFINITION:.....	3
II. UTILISATION :.....	3
II.1. PRINCIPAUX CAS D'UTILISATION :.....	3
II.2. CONDITIONS D'UTILISATION:.....	3
III. PRINCIPAUX LOGICIELS:.....	5
III.1. BUREAU A DISTANCE DE WINDOWS :.....	5
III.1.1. AUTORISER LA CONNEXION SUR LE POSTE A CONTRÔLER :.....	5
III.1.2. PRENDRE LE CONTRÔLE A DISTANCE D'UN POSTE WINDOWS:.....	6
III.2. TEAMVIEWER.....	8
III.2.1. PRÉSENTATION GÉNÉRALE :.....	8
III.2.2. PRINCIPE DE FONCTIONNEMENT:.....	8
III.2.3. SÉCURITÉ ;.....	9
III.2.4. UTILISATION POUR LE CONTRÔLE A DISTANCE:.....	9
III.3. LE LOGICIEL VCN :.....	11
III.3.1. PRÉSENTATION :.....	11
III.3.2. FONCTIONNEMENT :.....	11
III.3.3. UTILISATION EN MODE LISTENING VIEWER (ULTRA VNC):.....	12
III.3.3.1. INTRODUCTION :.....	12
III.3.3.2. LANCEMENT DU SERVEUR SUR LA MACHINE A CONTRÔLER :.....	12
III.3.3.3. LANCEMENT DU CLIENT SUR LA MACHINE DU CONTRÔLEUR :.....	14

I.DÉFINITION:

En informatique, la PRISE DE CONTRÔLE A DISTANCE d'un ordinateur est une méthode qui consiste à prendre, depuis un ordinateur distant, le contrôle de l'IHM de l'ordinateur local, de telle manière que l'on puisse effectuer les mêmes opérations que si l'on travaillait directement avec l'IHM local (clavier, souris, écran).

Ceci implique que :

- L'écran d'affichage de l'ordinateur contrôlé s'affiche dans une fenêtre de l'ordinateur distant ;
- Le curseur graphique sur l'écran de l'ordinateur contrôlé puisse être manipulé avec l'organe de pointage de l'ordinateur distant (déplacements, boutons de clics, boutons de défilement, etc.) ;
- Les saisies sur le clavier de l'ordinateur distant soient transmises à l'ordinateur contrôlé et traitées par celui-ci comme si elles provenaient de son clavier local.

REMARQUE : en général, les logiciels de contrôle à distance supportent d'autres fonctionnalités comme le transfert de fichiers entre les deux postes ou le support de téléconférences .

II.UTILISATION :

II.1.PRINCIPAUX CAS D'UTILISATION :

- Le CONTRÔLE A DISTANCE est utilisé essentiellement pour le DÉPANNAGE et l'ADMINISTRATION des postes de travail ou des serveurs. Dans ce cadre, Il a l'avantage de permettre de limiter les déplacements des personnels aux seuls cas où leur présence physique est indispensable. Il permet également de raccourcir les délais d'intervention. Grâce au contrôle à distance, l'administrateur ou le technicien de maintenance peuvent, pour investiguer ou intervenir sur le paramétrage du système d'exploitation, utiliser les outils et menus graphiques du système d'exploitation de l'ordinateur contrôlé, ce qui très souvent permet d'améliorer la rapidité d'intervention.
- Le contrôle à distance peut également permettre à un agent en déplacement de prendre la main à distance sur son ordinateur personnel (à condition que celui-ci reste accessible sur le web) ;
- Le contrôle à distance est également utilisé dans un BUT PÉDAGOGIQUE (enseignement à distance): l'apprenant peut, par ce moyen, "vivre en direct" sur son propre écran la manipulation que lui montre son tuteur comme si celui-ci était à côté de lui.

II.2.CONDITIONS D'UTILISATION:

- Le débit entre les deux postes doit être suffisant pour assurer un bon rafraîchissement de

DOC-Administration des systèmes et réseaux : les logiciels de contrôle à distance

la fenêtre ouverte sur le poste de travail distant;

- Les deux postes de travail doivent être équipés des logiciels adéquats;
- La prise de contrôle à distance suppose toujours une phase d'authentification réciproque des deux machines:
 - Le poste de travail distant fait une demande de connexion au poste à contrôler (en lui envoyant des informations d'authentification);
 - Le poste à contrôler examine ces informations et autorise ou non la connexion.

III.PRINCIPAUX LOGICIELS:

III.1.BUREAU A DISTANCE DE WINDOWS :

Ce logiciel propriétaire de Microsoft permet à un poste de travail muni du système d'exploitation WINDOWS de prendre le contrôle à distance d'un autre ordinateur muni d'une version PROFESSIONNELLE d'un système d'exploitation WINDOWS.

En effet, ce mécanisme suppose que le système à contrôler abrite un SERVEUR de contrôle à distance, tandis que le système contrôleur doit abriter un CLIENT de cette application. Or, si tous les systèmes windows sont équipé du CLIENT, les SERVEURS ne sont présents que sur les versions professionnelle.

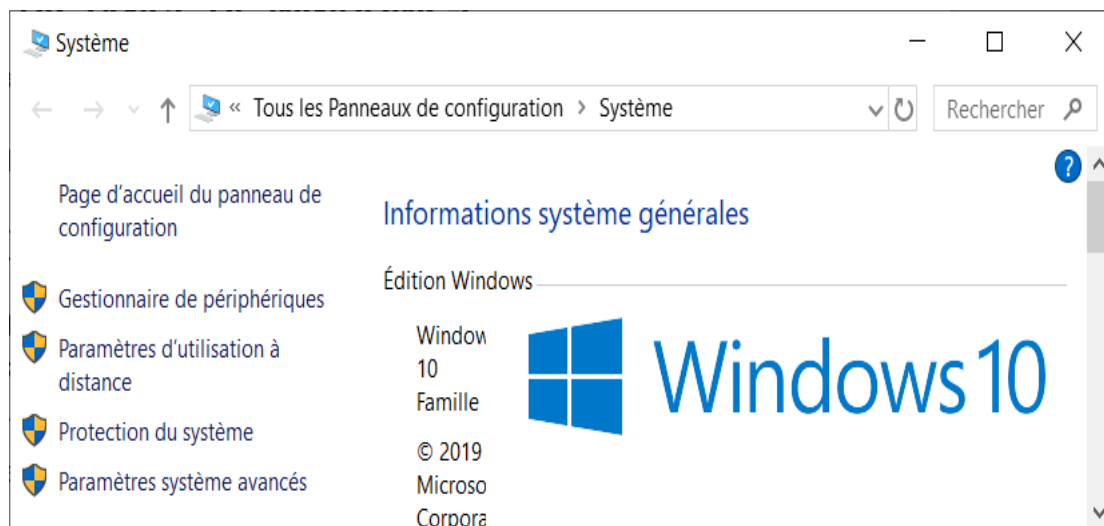
EXEMPLE : depuis un système windows en version "famille", il est possible de prendre le contrôle d'un système windows en version professionnelle. L'inverse n'est pas vrai.

Les deux paragraphes suivants décrivent les manipulations nécessaires.

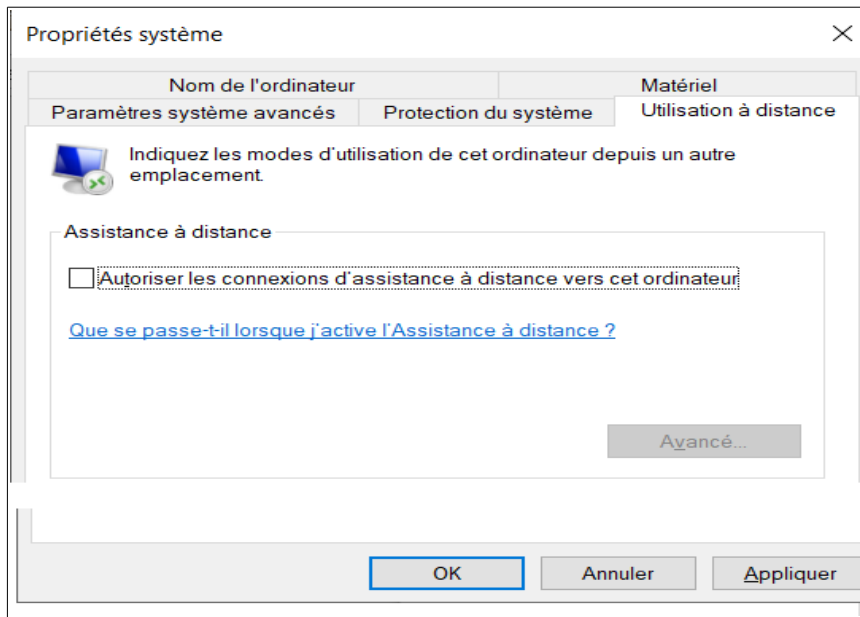
III.1.1.AUTORISER LA CONNEXION SUR LE POSTE A CONTRÔLER :

RAPPEL : Cette opération ne peut être effectuée que sur un ordinateur muni d'une version professionnelle de windows.

Sur le poste à contrôler, activer les touches clavier [windows]+[Pause]. La fenêtre suivante s'affiche :



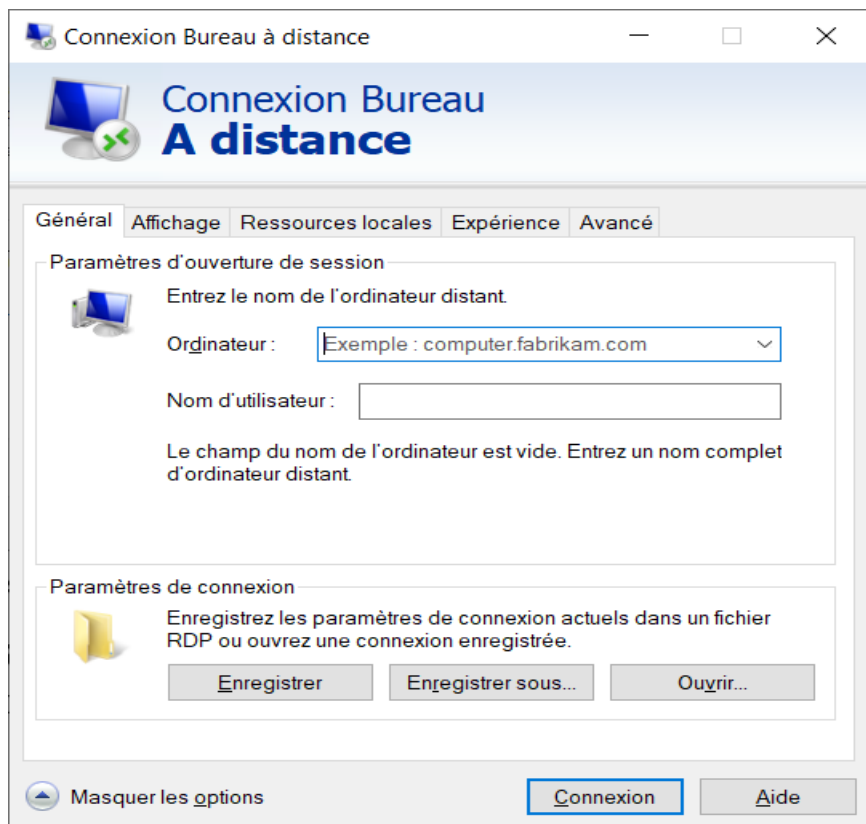
Activer alors "Paramètres d'utilisation à distance". La fenêtre suivante s'ouvre :



Cette fenêtre permet d'autoriser les postes distant à se connecter au poste local en cliquant sur le bouton "Autoriser les connexions à distance ...".

III.1.2.PRENDRE LE CONTRÔLE A DISTANCE D'UN POSTE WINDOWS:

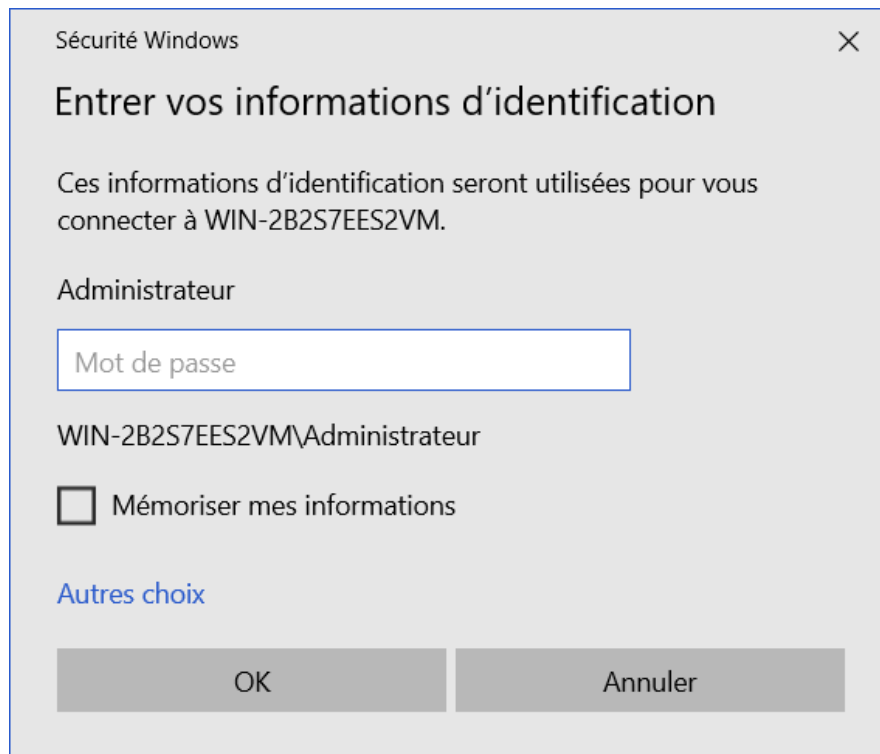
Sous Windows 10 : Rechercher "Connexion Bureau à distance". Le menu suivant s'affiche :



DOC-Administration des systèmes et réseaux : les logiciels de contrôle à distance

NOTA : pour utiliser ce menu, il faut décocher "Masquer les options", si nécessaire.

Saisir alors le nom de l'ordinateur (par exemple, WIN-2B2S7EES2VM) et le nom d'utilisateur (par exemple : "Administrateur"), puis activer "Connexion". Le menu de connexion suivant s'affiche :



The image shows a Windows Security dialog box titled "Sécurité Windows" with a close button (X) in the top right corner. The main heading is "Entrer vos informations d'identification". Below this, a message states: "Ces informations d'identification seront utilisées pour vous connecter à WIN-2B2S7EES2VM." The username field is pre-filled with "Administrateur". Below the username field is a password field with the placeholder text "Mot de passe". Underneath the password field, the system path "WIN-2B2S7EES2VM\Administrateur" is displayed. There is a checkbox labeled "Mémoriser mes informations" which is currently unchecked. At the bottom left, there is a link "Autres choix" in blue. At the bottom, there are two buttons: "OK" and "Annuler".

Saisir alors le mot de passe de l'utilisateur du système distant et valider (ok). La fenêtre de contrôle s'affiche alors sur l'écran : elle visualise le bureau de l'ordinateur contrôlé. Lorsque le curseur de la souris se trouve dans cette fenêtre, les informations en provenance du clavier et de la souris de l'ordinateur local sont envoyées à l'ordinateur contrôlé et traitées comme si elle provenaient de son clavier ou de sa souris.

III.2.TEAMVIEWER

III.2.1.PRÉSENTATION GÉNÉRALE :

TeamViewer permet de contrôler un PC à distance via internet. C'est un logiciel propriétaire payant (environ 500 euros), mais qui est distribué gratuitement si l'acquéreur s'engage à l'utiliser dans un but non commercial.

Attention, cette condition est effectivement contrôlée par la société éditrice car l'utilisation de TeamViewer nécessite la connexion à un de ses serveurs : en cas d'utilisation "illicite", l'éditeur peut vous interdire l'utilisation, à moins d'acheter la licence.

Le principal avantage de TeamViewer est qu'il ne nécessite pas d'installer un serveur sur les postes : de ce fait, il peut fonctionner derrière un NAT sans redirection de port.

TeamViewer offre aux utilisateurs trois fonctionnalités principales :

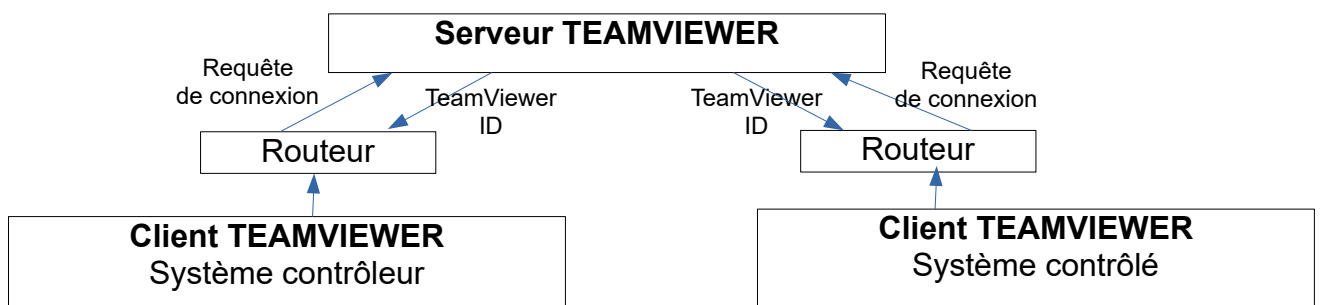
- Prise de contrôle à distance d'un ordinateur connecté au web ("bureau" à distance);
- Transfert de fichiers entre deux ordinateurs connectés au web ;
- Support pour des conférences.

III.2.2.PRINCIPE DE FONCTIONNEMENT:

La transaction entre les postes participants s'effectue par l'intermédiaire un SERVEUR de la société éditrice. Ce serveur assure :

- L'identification des postes connectés par un identificateur UNIQUE sur le web, associé à un mot de passe (TeamViewer ID).;
- Le transfert des données entre les postes connectés.

Au lancement de TeamViewer sur un ordinateur client, le logiciel se connecte au serveur TeamViewer, qui attribut à l'ordinateur concerné sa "TeamViewer ID" unique. Les connexions sont de type TCP :



De ce fait, Teamviewer n'a pas besoin de faire une redirection de port pour atteindre des adresses au-delà du routeur, car on n'utilise que des connexions TCP sortantes. Cette technique s'appelle:

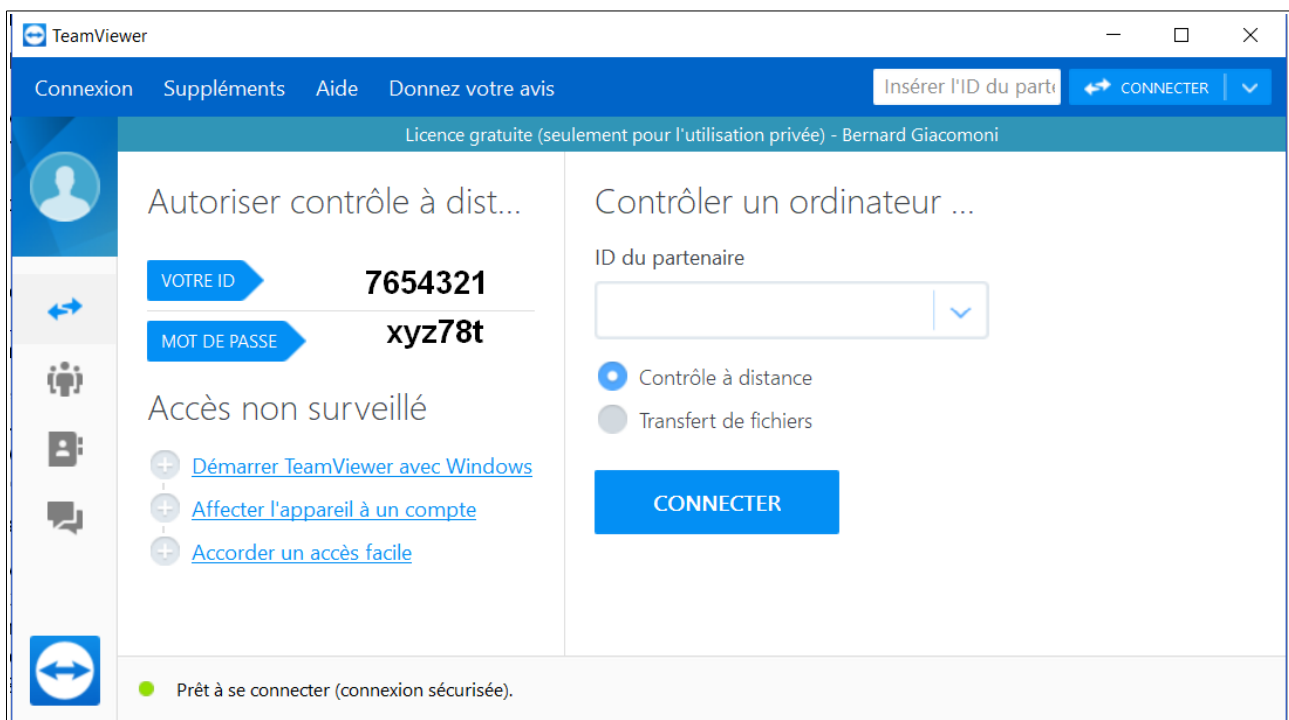
reverse connection. En général, la connexion TCP se fait sur le port 80 (utilisé par les serveurs web) car ce port, utilisé par le web, n'est jamais bloqué par les pare-feux.

III.2.3.SÉCURITÉ ;

TeamViewer utilise pour les transmissions de données un cryptage par clé symétrique de 256 bits ; L'échange de cette clé est crypté par une paire de clés asymétrique RSA de 2048 bits. La sécurité est donc comparable à celle d'une transmission SSH.

III.2.4.UTILISATION POUR LE CONTRÔLE A DISTANCE:

Au lancement de TeamViewer, quelle que soit l'utilisation que l'on veut en faire (contrôleur ou contrôlé), la fenêtre suivante s'affiche sur l'écran :



COMMENTAIRES :

- Le champ qui apparaît à droite du label « VOTRE ID » est la « TeamViewer ID » attribuée à la machine par le serveur TeamViewer.
- A droite du label « MOT DE PASSE » apparaît le mot de passe correspondant à cette ID.
- Le champ situé en dessous du label « ID du partenaire vous permet de saisir l'ID de la machine que vous voulez contrôler.

Pour prendre le contrôle d'un ordinateur à distance, il suffit donc :

- De lancer teamViewer sur votre machine en sélectionnant « Contrôle à distance » dans l'IHM ;
- De demander au responsable de l'ordinateur à contrôler de lancer TeamViewer sur cet

DOC-Administration des systèmes et réseaux : les logiciels de contrôle à distance

ordinateur (si ce n'est pas déjà fait), puis de vous communiquer l'ID de cet ordinateur (par téléphone, par mail, oralement, etc.) ;

- De saisir cette ID dans le champ labellisé « ID du partenaire » et d'activer le bouton de connexion.

Le TeamViewer du PC contrôleur demande alors au serveur Teamviewer de l'autoriser à prendre le contrôle de la machine correspondant à l'ID saisie dans le champ « ID du partenaire ». Comme le logiciel TeamViewer est aussi lancé sur la machine à contrôler, celle-ci est également connectée au serveur Teamviewer. Le serveur peut alors faire transiter les données et commandes entre les deux machines par son intermédiaire. Ces deux machines ne communiquant physiquement qu'avec le serveur, il n'est nul besoin de faire une redirection de port.

III.3.LE LOGICIEL VCN :

III.3.1.PRÉSENTATION :

Comme TeamViewer, VCN est un logiciel dont la principale fonction est la prise de contrôle à distance d'un poste informatique. En revanche, VCN est un logiciel GRATUIT et OPEN SOURCE.

Tout comme Teamviewer, VCN est principalement utilisé pour la télémaintenance et la téléadministration des systèmes informatiques ainsi que pour la téléformation. il fonctionne sur les plateformes Windows, Mac et Linux.

III.3.2.FONCTIONNEMENT :

Le VNC "de base" est composé de 2 applications communicant entre elles :

- Le SERVEUR VNC, exécuté sur la machine contrôlée à distance (le port VNC par défaut est 5900) ;
- Le CLIENT VNC (ou VIEWER), qui tourne sur la machine contrôleur à distance. Le viewer affiche la fenêtre de contrôle sur l'ordinateur distant et gère le clavier, la souris et le presse-papier.

Il supporte deux modes de fonctionnement :

Dans le premier mode ("mode normal"), le CLIENT se connecte au SERVEUR. De ce fait, le port utilisé par VNC doit être redirigé vers la machine commandée, pour qu'on puisse s'y connecter depuis internet. Ceci implique d'avoir accès à la configuration du routeur.

Dans le second mode de fonctionnement (mode "listening viewer"), la connexion s'établit en sens inverse : c'est le SERVEUR qui sollicite le client. Le CLIENT attend donc les sollicitations du serveur ("Listening Viewer"). De ce fait, ce mode permet de contrôler un ordinateur derrière un NAT ou un firewall même si on ne peut pas créer de redirection de port (par exemple, si on n'a pas accès à la configuration du routeur).

Le second mode correspond au logiciel Ultra VNC dont nous allons aborder l'utilisation.

III.3.3.UTILISATION EN MODE LISTENING VIEWER (ULTRA VNC):

III.3.3.1.INTRODUCTION :

UltraVNC est une évolution du logiciel libre VNC suivant les principes de l'OPEN SOURCE. Il en exploite l'option LISTENNING VIEWER. De ce fait, aucune redirection de port n'est nécessaire.

Le logiciel UltraVNC se compose d'un SERVEUR, installé sur le système à contrôler et d'un CLIENT qui permet de se connecter au serveur et d'afficher l'écran (bureau) du système contrôlé dans une fenêtre.

III.3.3.2.LANCEMENT DU SERVEUR SUR LA MACHINE A CONTRÔLER :

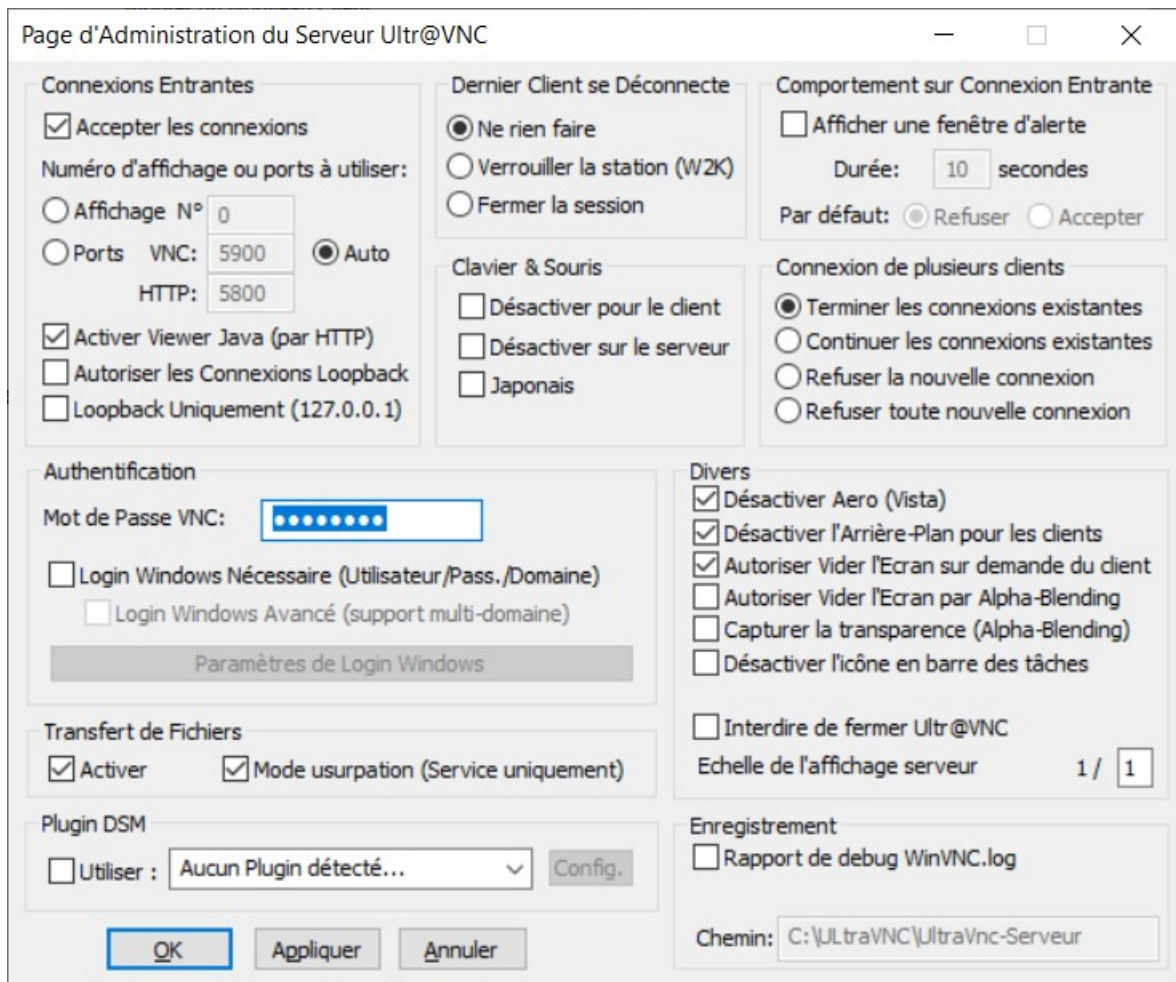
Sous WINDOWS : L'activation du lien d'exécution du logiciel VNC Server déclenche l'apparition dans la barre des tâches de l'icône :



Un clic droit sur cette icône permet d'afficher le menu contextuel suivant :



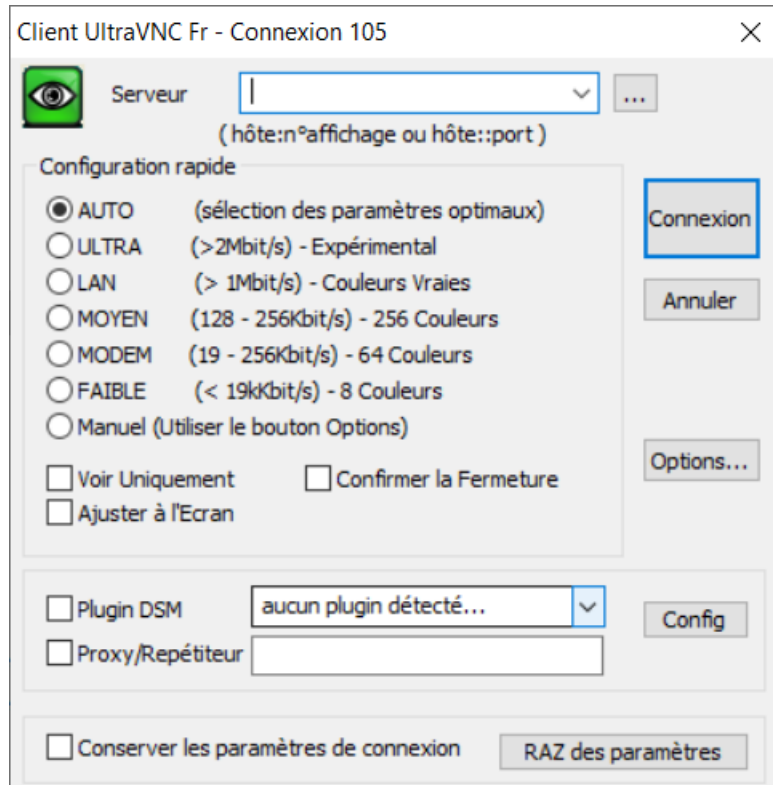
L'activation de "Paramètres d'administration ouvre un menu de configuration du serveur :



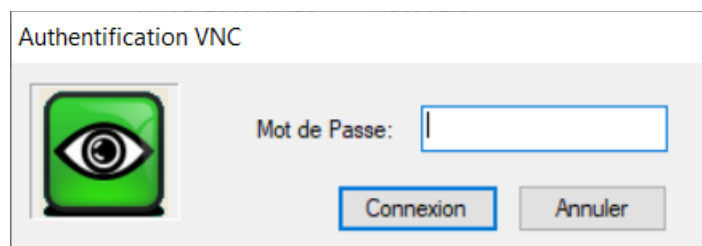
Ce menu d'administration permet en particulier de définir un "Mot de passe VCN" qui permettra aux clients (systèmes désirant contrôler l'ordinateur local) de se connecter.

III.3.3.3.LANCEMENT DU CLIENT SUR LA MACHINE DU CONTRÔLEUR :

Sous WINDOWS : L'activation du lien d'exécution du logiciel VNC Client déclenche l'ouverture du menu suivant :



Saisir alors le nom d'hôte ou l'adresse IP de la machine à contrôler (éventuellement accompagné du numéro de port, si le port par défaut n'est pas utilisé). L'activation de "Connexion" entraînera l'affichage d'un menu de connexion au serveur :



La saisie du mot de passe SERVEUR et l'activation de "Connexion" entraîne la connexion au serveur et l'affichage du bureau de la machine distante dans une fenêtre de l'écran local.