Les outils de prise en main à distance

Remote management

Leur utilité ?

Des exemples d’outils ?

Sommaire

De quoi s'agit-il ?

Introduction

Pourquoi c’est essentiel ?

Mais pourquoi ?

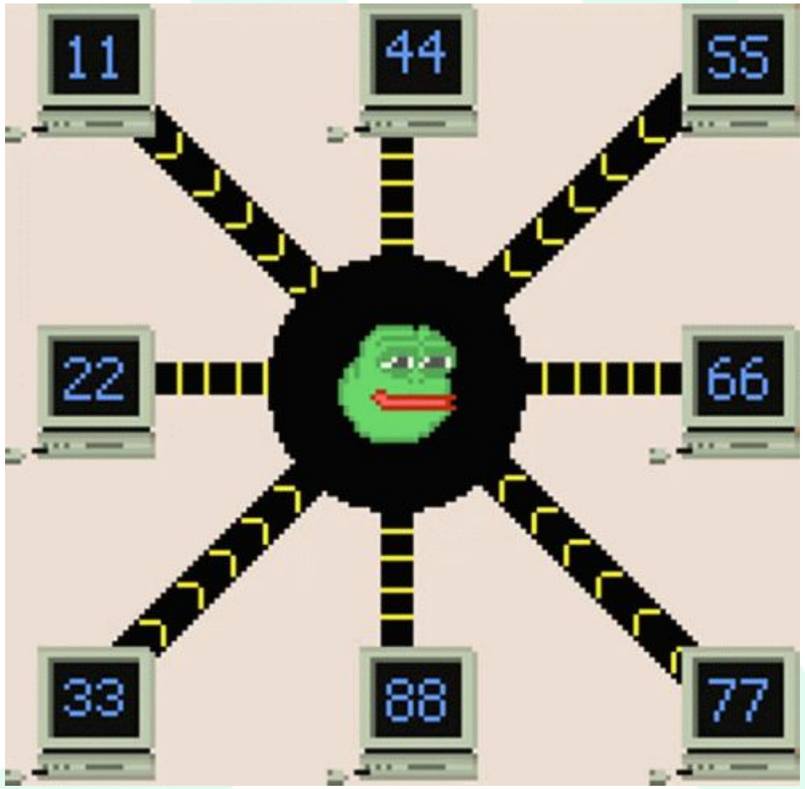
- Maintenance rapide (intra et hors site)
- Réduction des coûts de déplacement
- Réduction des temps d’intervention (transport, recherche des locaux, etc.)

Cas concret

Pourquoi faire ?

- Support utilisateur (accès aux ordinateurs clients)
- Administration de serveurs
- Télétravail

Les protocoles



Protocole de Bureau à Distance (RDP)

Microsoft

Protocole propriétaire développé par Microsoft.
Port par défaut :TCP/UDP 3389 .

Objectifs: Fournir une interface graphique pour contrôler un ordinateur distant et faciliter l'administration à distance.

Cas d’usage : support IT, gestion des « ordinateurs sans tête »..

Protocole de Bureau à Distance (RDP) suite

Microsoft

Scénario d’échange :

Étape 1 : Poignée de main (négociation des paramètres de connexion).

Étape 2 : Connexion de canal (établissement du canal de communication).

Étape 3 : Initiation de sécurité (création de clés de chiffrement pour sécuriser la communication).

Étape 4 : Échange des paramètres sécurisés (notamment l'envoi du mot de passe de manière chiffrée).

Étape 5 : Octroi de licence (vérification de la licence d'utilisation, si applicable)

Protocole Remote Frame Buffer (RFB)

Multi plateforme

Protocole utilisé par le système Virtual Network Computing (VNC). modèle client/serveur sur port TCP 5900.

Solution très polyvalente : logiciels clients et serveurs disponibles pour Windows, macOS et Linux

Cas d’usage : support technique, accéder à des systèmes embarqués, partage d'écran et la collaboration.

Secure Shell (SSH)

Linux

Protocole réseau cryptographique (alternative sécurisée de Telnet).
Port TCP 22

Objectif : fournir une méthode sécurisée pour la connexion à distance d'un ordinateur à un autre.
Protocole largement utilisé pour la gestion à distance des serveurs de type unix, routeurs, pare-feu et commutateurs.

Installé par défaut sur les OS de type Unix .
Depuis Windows 10, client OpenSSH inclus par défaut.

Système de Fenêtrage X (X11)

Linux

Protocole utilisé pour les interfaces graphiques, notamment dans les systèmes Unix/Linux, réseau-transparent.
Modèle client-serveur sur le port par défaut TCP 6000.

Son objectif principal : permettre aux applications graphiques (appelées clients X) de s'afficher sur un serveur X, qui est responsable de la gestion de l'affichage et des périphériques d'entrée tels que le clavier et la souris.

Simple Protocol for Independent Computing Environments (SPICE)

Multi plateforme

Protocole d'affichage à distance open source.
Port par défaut TCP 3001
Objectif : fournir un accès à distance aux machines virtuelles, en particulier dans les environnements virtualisés par QEMU/KVM.

Peut être utilisé avec différents systèmes d'exploitation invités (Windows, Linux..).

Cas d'utilisation courants : plateformes de gestion de cloud privé comme oVirt et Proxmox VE

Pour configurer SPICE sur PROXMOX

En résumé

Protocole	Objectif principal	Port par défaut	Cryptage par défaut	Authentification courante
RDP	Accès au bureau à distance (principalement Windows)	TCP/UDP 3389	RC4 (options TLS)	Nom d'utilisateur/mot de passe
VNC	Partage de bureau multiplateforme	TCP 5900+N	Aucun (souvent via TLS)	Mot de passe VNC
SSH	Accès sécurisé en ligne de commande	TCP 22	Chiffrement symétrique	Nom d'utilisateur/mot de passe, Clé publique
X11	Affichage d'applications graphiques à distance	TCP 6000+N	Aucun (souvent via SSH)	xauth (via SSH)
SPICE	Accès à distance pour machines virtuelles	TCP 3001 (varie)	TLS en option	Ticket, SASL (Kerberos)

Les outils

Outils commerciaux

Gratuit mais pas que

TeamViewer :
Très utilisé, simple, usage personnel gratuit.

AnyDesk :
Rapide, léger, licence abordable.

Avantages : performance, sécurité, multi-plateforme.
Inconvénients : nécessite une licence pour des fonctionnalités avancées.

Outils intégrés

Sans installation

RDP (Windows) : intégré aux éditions Pro/Entreprise
Sécurisation possible via VPN ou tunnel SSH.

Outils open source

Licence open source

VNC : protocole léger, multiplateforme

Guacamole : accès via navigateur, supporte VNC/RDP/SSH

Remmina : client Linux polyvalent pour RDP, VNC, SSH

Avantages : gratuits, flexibles, personnalisables.

Les terminaux légers

Définition

Quoi ?

Un terminal léger est un poste client sans disque dur local.
Le système et les données sont sur un serveur distant.
=> Aucune données n’est conservées en local.

Par rapport à un poste classique :

- Plus simple (à mettre en place, à maintenir)
- Plus économique (uniquement un écran et une connexion réseau)

Fonctionnement général

Comment ça marche ?

Architecture client/serveur.

Démarrage via la carte réseau (boot PXE).

L’écran local affiche le contenu distant.

Un exemple : Citrix

Un exemple professionnel

- Entreprise multinationale Américaine
- Propose de la virtualisation et des outils collaboratifs
- Acteur incontournable dans le monde des clients légers

Citrix - Fonctionnement général

Citrix ICA

Un terminal Citrix n'exécute quasiment rien en local : il sert uniquement d'interface pour afficher le bureau distant.
Il lance une connexion vers un serveur Citrix via le protocole **ICA** (*Independent Computing Architecture*) ou **HDX** (*High Definition eXperience*).
Le traitement des applications et du bureau est effectué sur les serveurs Citrix, pas sur le client

Type d’affichage distant

La publication

Il y a 2 possibilités :

- **Publication de bureau** : l’utilisateur accède à un bureau complet hébergé sur un serveur, Windows Server ou VDI (V*irtual Desktop Infrastructure*)
- **Publication d’application** : les applications seule sont publiées sur le bureau locale et intégrées dans l’environnement local

Dans les 2 cas, c’est l’**Agent Citrix**, ou **VDA** (*Virtual Delivery Agent*) installé sur le client citrix qui gère ces publications.

Ferme Citrix

Tous les serveurs

Ensemble de serveurs Citrix configurés pour fournir les ressources aux clients Citrix.
Les serveurs sont en général redondant et réparti.

Citrix - Connexion et authentification

Au début...

- Le client léger démarre, lance Citrix Workspace
- Il contacte un portail Citrix, un StoreFront (interface utilisateur pour accéder aux ressources)
- Le StoreFront transmet l’authentification au Delivery Controller, qui la valide via un Active Directory
- L'utilisateur s’authentifie (AD / LDAP / SAML)
- StoreFront renvoie la liste des applications ou bureaux disponibles

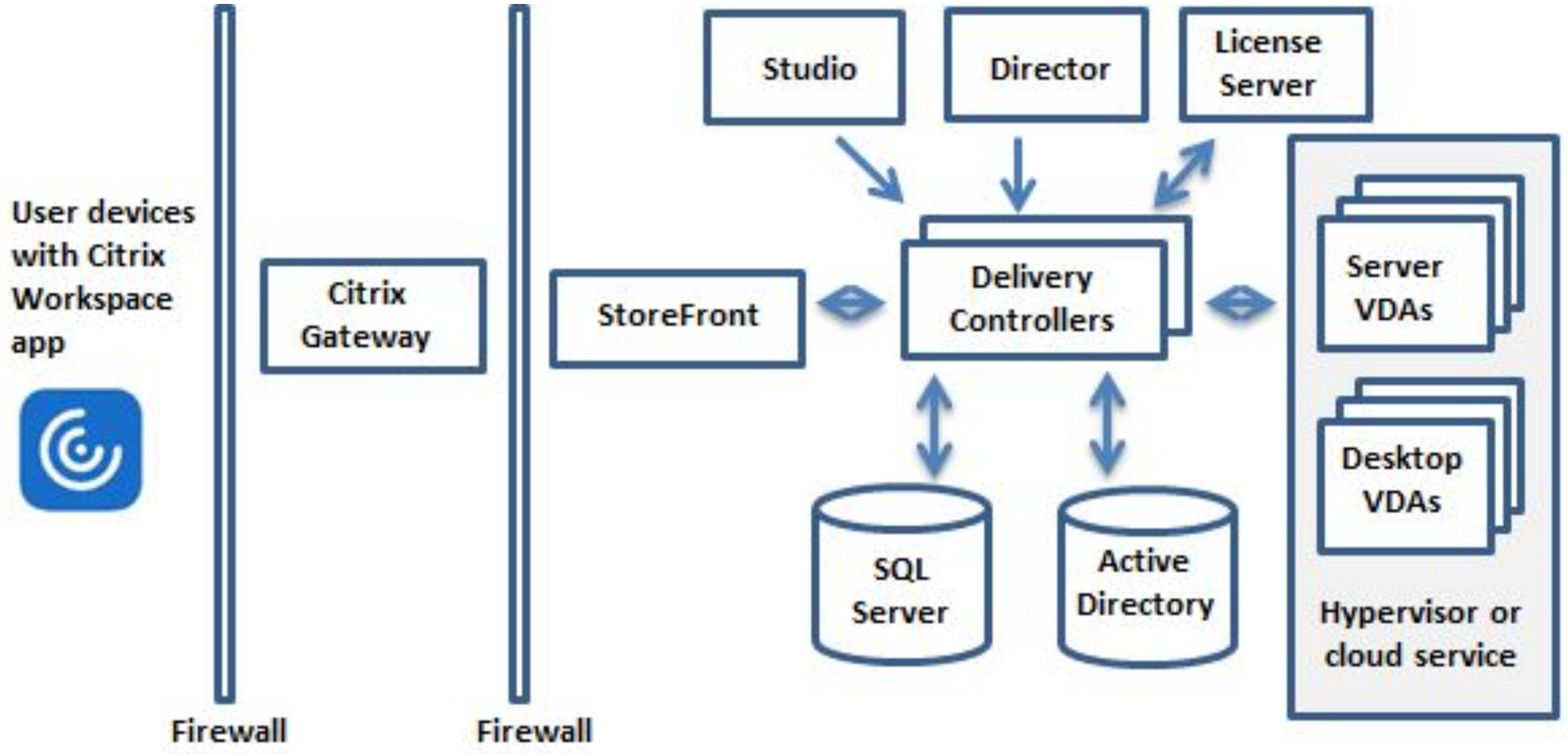
Citrix - Connexion et authentification (suite)

... et ça s'affiche !

- L'utilisateur sélectionne une ressource
- Génération d'un fichier **.ica** qui contient les infos de connexion au VDA (pas au Delivery Controller), qui héberge la session utilisateur
- Le client établit ensuite une connexion directe (par ICA/HDX) vers le VDA (pas le Delivery Controller) qui héberge la ressource (bureau ou application)

Schéma d’une architecture réseaux classique Citrix

aa



[lien de l'image]

Cloud Citrix

Tout dans la nuage

- Tout ou une partie de l’infrastructure réseau Citrix peut être mise en Cloud.
- Dans ce cas, on parle de **DaaS** (*Desktop as a Service*) pour les terminaux

Alternatives

D’autres solutions

Systancia

LTSP

Bonnes pratiques

Infrastructure réseau

Et les câbles ?

- Connexion réseau : privilégier une connexion Ethernet au lieu du sans fils pour les postes clients
- Redondance matérielle : pour avoir de la HA (Haute Disponibilité) avoir plusieurs serveurs d'infrastructure (ex. pour Citrix, avoir plusieurs Delivery Controllers, VDA, et StoreFront)
- VLAN : avoir des vlans dédiés pour le trafic client léger/serveur

Sécurité

Cadenas ?

- Authentification centralisée : Active Directory (+ MFA si possible)
- Communication sécurisées en SSL/TLS
- Pour les terminaux : Pas d’écriture disque en local, pas de stockage persistant
- Utilisation de profils utilisateurs itinérants et de GPO

En résumé

A retenir

- Prise en main à distance GUI ou CLI
- Outils libres ou propriétaires

MERCI

pour votre participation.

C’est à vous maintenant.
Des questions ?
Des remarques ?