Rapport de stage pour l'obtention du Titre de Technicien Supérieur Exploitant de Ressources Informatiques

Campus de Formation AFPA St Jérôme Marseille

Promotion 2012 / 2013

BERNIER François
francois@bernier-family.fr – francois.bernier.fr@free.fr
http://superghost.fr – http://astronomie-astrophotographie.fr

Mise en place d'un Serveur Applicatif

Mise en place d'un Connexion BROKER

Effectué à : **Tourisme et Services,**
4 Rue Henri et Antoine Maurras
Avenue André Roussin Imm. le N
13016 Marseille

Sous la responsabilité de : Mr. Marc LESBROS
Tuteur pédagogique : Mr. Nicolas PAUGAM

CAMPUS AFPA St JEROME
54 boulevard Laveran
13013 MARSEILLE
Tél. : 04 91 05 57 57
Fax : 04 91 70 93 95

Remerciements

Avant tout, je tiens à remercier personnellement Mr Marc LESBROS, Directeur du SI de la société Tourisme et Services, qui a bien voulu m'accueillir dans son équipe, me confier un projet particulièrement intéressant et m'accorder d'excellentes conditions de travail.

Je remercie également Nicolas PAUGAM, Administrateur Cloud, qui a travaillé avec moi durant mon séjour chez Tourisme et Services sur les projets de Connexion Broker et de Serveur Applicatif. J'ai souvent eu recours à ses connaissances approfondies en réseaux. Grâce à lui mon expérience chez Tourisme et Services a été très enrichissante.

Je souhaite faire part de ma reconnaissance à l'ensemble du personnel des pôles Réseaux et Système et des différentes agences de voyage où j'ai effectué mon stage. Ils m'ont réservé un accueil chaleureux ainsi qu'un climat de travail convivial.

Merci à la société Tourisme et Services de m'avoir reçu en tant que stagiaire durant ces huit semaines, pour cette expérience très instructive et très enrichissante. Cette collaboration m'a permis de découvrir réellement le fonctionnement d'un SI. Elle m'a surtout donné l'occasion d'appliquer concrètement – et donc de mieux comprendre – mes connaissances théoriques.

Je remercie également mon employeur actuel ayant accepté mon projet de formation auprès du Fongecif et mon absence durant une année qui aura certainement amenée quelques modifications organisationnelles auprès de mon équipe.

Je remercie également les stagiaires de la formation TSGERI avec lesquels j'ai échangé et travaillé durant ces 8 mois de formation théorique .En particulier , Oliver OZIER , Vincent REMY et Jean Jérôme TONNEL.

Enfin je remercie mon formateur Oscar LOOGER, pour sa contribution à ma formation.

Sommaire

1 INTRODUCTION 5

1.1 PRESENTATION DU STAGE 5
1.2 MON PARCOURS PROFESSIONNEL 6
1.3 PRESENTATION DE LA SOCIETE 7
1.3.1 Geophyle et Tourisme & Services 7
1.3.2 Tourisme & Services et Tourism-it 8
1.3.3 Tourism-it : Les activités 9
1.3.3.1 Gestion du parc client physique et virtuel 9
1.3.3.2 Gestion du parc serveur physique et virtuel 11
1.3.3.3 La gestion du Système d'information 11
1.3.3.4 Gestion du Support Utilisateur 12
1.3.3.5 Recherche, développement et intégration des solutions métiers 13
1.3.3.6 Architecture et principe 13
1.3.3.7 Téléphonie et Télécommunications 14

2 LES PROJETS 15

3 INFRASTRUCTURE LOGICIELLE ACTUELLE 16

4 INSTALLATION ET CONFIGURATION DES PROJETS 20

4.1 LE SERVEUR D'APPLICATIONS 20
4.1.1 SOLUTION 1 : Ulteo OVD 3.0.4 (release 7/2013 → disponibilité OVD 4 Beta 10/2013) 20
4.1.1.1 Installation du Serveur Session Manager 22
4.1.1.2 Installation du Serveur d'applications Windows 32
4.1.1.3 Conclusions de la solution Ulteo OVD 3.0.4 41
4.1.2 SOLUTION 2 : REMOTE-APP TERMINAL SERVER WINDOWS 2008 R2 43
4.1.2.1 INSTALLATION ET CONFIGURATION TERMINAL SERVEUR – APPREMOTE SUR WINDOWS Server 2008 R2 45
4.1.2.1.1 Installation des services TSE 45
4.1.2.1.2 Configuration de TSE 54
4.1.2.1.3 Configuration Remote App 55
4.1.2.1.4 Les modes de connexions aux logiciels 58
4.1.2.1.5 A propos des serveurs de licences Windows 60
4.1.2.1.6 Installation et configuration du serveur de licences des services Bureau à distance 61
4.1.2.1.7 Conclusions sur la solution RemoteApp de Windows Server 2008 R2 65
4.1.3 SOLUTION 3 : 2X APPLICATION SERVEUR 66
4.2.1.1 Installation 2xApplicationServer XG sur Windows Server 2008 R2 67
4.2.1.2 Installation 2X client sur un poste Utilisateur 71
4.2.1.3 Installation de l'interface WebPortal 2X client (Windows Server 2008 R2) 73
4.2.1.4 Conclusion sur la Solution 2X ApplicationServer XG 76

5 INSTALLATION ET CONFIGURATION D'UN CONNEXION BROKER 77

5.1 SOLUTION 1 : 2XAPPLICATION SERVER 78
5.1.1 Conclusions de la Solution BROKER 2XApplicationsServer 82
5.2 SOLUTION ERICOM POWERTERM WEBCONNECT REMOTEVIEW 83
5.2.1 Préconfiguration du serveur Windows 2008 R2 84
5.2.2 Installation d'Ericom Secure Gateway 86
5.2.3 Installation du Server Powerterm Webconnect 91
5.2.4 Conclusion sur la Solution ERICOM Powerterm Webconnect 98
5.3 COMPTE RENDU DE REUNION DE PRESENTATION DES SOLUTIONS A L'ADMINISTRATEUR LE 11 SEPTEMBRE 2013 98

6 MISE EN PRE-PRODUCTION DE LA SOLUTION ULTEO 99

6.1 MISE EN PRODUCTION - PROCEDURE DE SAUVAGARDE 100

7 ANNEXES....102
7.1 PROPOSITIONS DES SOLUTIONS DE PROJET AU SI DE TOURISM-IT....102
7.2 MISSIONS EN COURS DE STAGE....108
7.2.1 Datacenter....109
7.2.2 Pré configuration et installation d'un SWICTH CISCO Catalyst 2960....114
7.2.2.1 Configuration....**114**
7.2.2.2 Mise en production....**116**
7.2.3 Configuration et Installation d'un Téléphone IP THOMSON ST2030....118
7.2.4 Installation et Configuration d'un poste Client DELL OPTIPLEX 3010....121
7.2.4.1 Installation du système d'exploitation....**121**
7.3 SCHEMA INFRASTRUCTURE TOURISM-IT FORMAT A3....125
8 BIBLIOGRAPHIE ET WEBOGRAPHIE....126

1 Introduction

1.1 Présentation du stage

Ce mémoire est rédigé suite à un stage de fin de formation du Titre de Technicien Supérieur Gestionnaire Exploitant de Ressources Informatiques. Le stage effectué a duré 8 semaines : du 22 Juillet au 2 Aout 20013 et du 19 Aout au 27 Septembre 2013 à Marseille 13016 au sein de la société Tourisme et Services, qui est le SI du Groupe Géophyle.

Pour faire ce stage, j'ai rejoint l'équipe de Compétences Systèmes et Réseaux dirigée par Mr Marc LESBROS. Il m'a été confié deux projets principaux dont la mise en place d'un Broker de connexion pour les accès aux bureaux virtuels des utilisateurs et d'un Serveur d'Applications en ligne pour deux logiciels métier utilisés par les différentes agences du groupe Géophyle. A l'issu de ce projet je devrais effectuer différents tests afin de valider la possible mise en production de ces services au sein du SI.

Dans la première partie de ce projet j'exposerais le choix des solutions utilisées et leurs installations suivant le cahier des charges qui m'aura été donné. En deuxième partie j'effectuerais les tests sur le fonctionnement des solutions installées, et exposerais les conclusions que la direction du SI m'aura fourni après avoir évaluer mon travail.

Ce rapport se compose de trois parties précédées par une présentation générale de la société Tourisme et Services. La première partie présente l'architecture réseau et les solutions existantes sur lesquels je devrais travailler. En second lieu je détaillerais la mise en place et l'installation des deux solutions de projets que j'aurais retenues en accord avec mon tuteur. Et en dernière partie de ce mémoire je réaliserais une description des différentes missions qui m'auront été confiées durant mon stage en parallèle des deux projets principaux.

1.2 Mon parcours professionnel

Mon parcours professionnel débute à l'âge de 18 ans, à la fin de mon BEP d'électrotechnicien, j'ai décidé de m'engager comme militaire pour une durée de 20 mois dans les services de transmissions de l'Armée de Terre Française. Durant cette expérience très enrichissante, j'ai pu apprendre le métier de Crypto régulateur télégraphiste, de valider le PEG (Peloton d'élèves gradé) ainsi que le PESO (Peloton d'élèves sous-officier) me permettant de prouver mes aptitudes à diriger une équipe. J'ai également continué mes études durant cette période effectuant un BAC F2 (Electronicien) auprès de l'organisme de formation Educatel.

A la fin de ma période d'engagement en Juillet 1990, j'ai intégré un bureau d'étude de L'Entreprise Industrielle pour un CDD en tant que contremaître de Chantier pour la réalisation d'une section du réseau câblé de Marseille.

J'ai ensuite intégré en Janvier 1991 la SARL Michel en CDI en tant qu'Electrotechnicien sur machine à bois, me permettant d'assurer la maintenance de nombreuses sociétés sur toute la région PACA.

En Février 1992, j'ai intégré la Société AGEI en CDD en tant que vendeur préparateur en matériel Electrique et Informatique.

J'ai ensuite connu une longue période de chômage durant laquelle je me suis formé à l'informatique en autodidacte qui était à ses tout premiers balbutiements et réalisé un stage en Infographie durant 6 mois à la société BORA-BORA.

En janvier 1995 j'ai intégré le Centre de Formation du CFBT à Marseille en tant qu'apprenti pour l'obtention d'un BAC PRO MAVELEC (maintenance audiovisuelle et électronique).Apprentissage que j'ai réalisé au sein du Service après-vente de la marque CANON qui m'a ainsi intégré à son équipe après l'obtention de mon diplôme en Juillet 1997.

Durant les 2 années suivantes j'ai réalisé auprès du CNAM à l'Université Aix-Marseille St Charles en cours du soir et week-end, en parallèle de mon activité professionnelle, un DPCT Prévention- Sécurité Ecosystème-Niveau III.
Un cursus qui m'a permis d'acquérir les connaissances de nombreuses matières scientifiques (Chimie, Chimie Organique, Microbiologie….) qui m'attiraient depuis de nombreuses années.

A ce jour, je suis toujours employé au SAV de la marque CANON (1995-2013). Malheureusement les restructurations et ventes successives de la société, les changements de technologies de l'électronique, ont mené à une diminution des cycles de formation et à des changements profonds dans le poste de technicien que j'occupe depuis maintenant 17 ans.

Ma soif de savoir, l'envie de faire évoluer ma seconde partie de carrière professionnelle m'ont donné l'envie et le courage de me lancer dans la formation de Technicien Supérieur Gestionnaire Exploitant de Ressources Informatiques.

Formation qui me permettra d'acquérir les compétences et connaissances dans le secteur d'activité de l'informatique qui m'a toujours attiré et de valider le savoir déjà acquis avec les outils avec lesquels je travaille quotidiennement depuis le début de ma carrière professionnelle ainsi que dans mon parcours personnel.

BERNIER François

1.3 Présentation de la société

1.3.1 Geophyle et Tourisme & Services

La société **Tourisme et Services** est une dépendance de **Geophyle**[1] qui a été créée le 1 Juillet 2012. C'est une Société par Actions Simplifiée (SAS), son siège social se situe au 4 Rue Henri et Antoine Maurras, 13016 Marseille.

Geophyle est né de l'idée de créer une véritable communauté autour des pratiques actives et bénéfiques. Les pratiques actives et bénéfiques sont des activités sportives, culturelles, de découverte et de bien-être qui permettent d'être :

Mieux dans son corps, mieux dans sa tête, mieux avec les autres, mieux sur terre.

Grâce à leurs partenaires spécialisés dans les domaines du tourisme, des loisirs, de l'alimentation ou des medias ils ont construit le réseau qui permet à leurs utilisateurs de découvrir et d'accéder à de multiples pratiques telles que la randonnée, la plongée, la glisse aquatique, le bien-être, le voyage découverte, la croisière, les voyages nordiques.

Michel Leclerc Directeur général et **Steve Hans** Directeur Administratif et Financier en sont les dirigeants. Geophyle regroupe plusieurs marques de voyage qui dépendent du système d'information de tourisme et services.

[1] Geophyle : http://www.geophyle.com

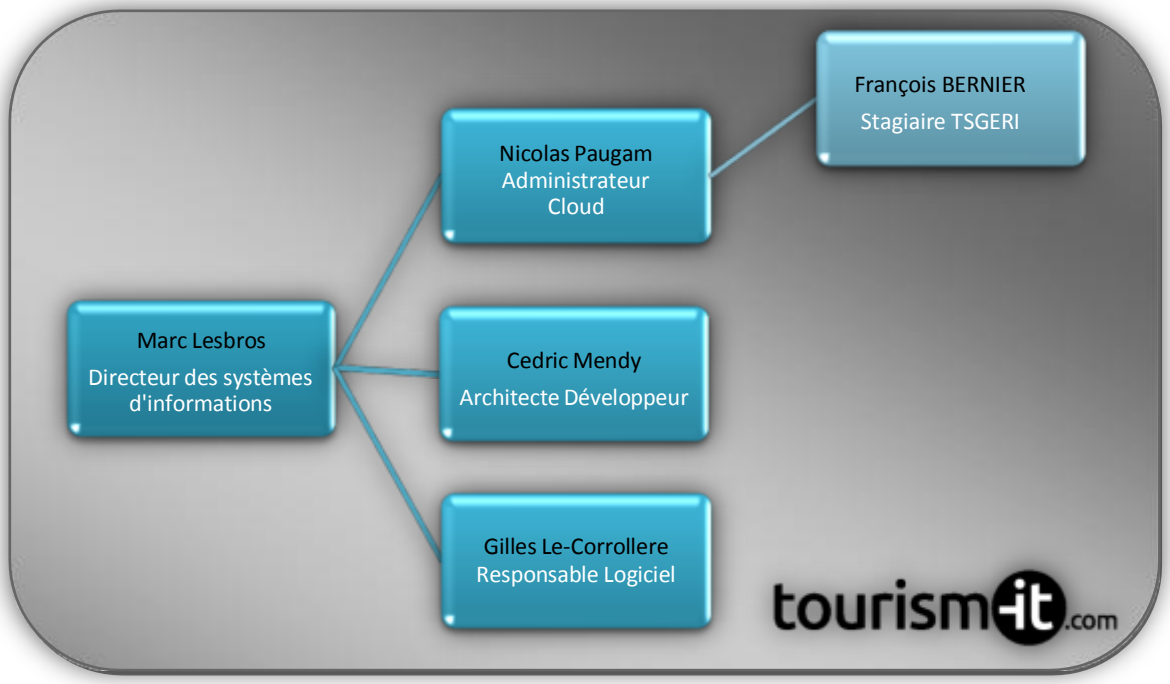
1.3.2 Tourisme & Services et Tourism-it

Tourisme et Services se divise en 3 départements. **Xavier Deschamps** directeur et **Jean-Charles Dezutter** Directeur administratif et financier en sont les dirigeants.

Le service Ressources Humaines : Ce département recouvre la comptabilité et les ressources humaines.

Le service **Transport Irwigoo** : Ce département s'occupe de la gestion de tous les transports pour les marques de tourismes qui sont regroupées sous **Géophyle**.

Le service **Informatique Tourism-it** : Ce département, dont je dépends pendant la durée de mon stage, s'occupe de tous les systèmes d'informations et téléphonie, de **Geophyle** et de toutes les entreprises qui lui sont associées ou apparentées.



1.3.3 Tourism-it : Les activités

Le réseau dont s'occupe Tourism-it est assez étendu. La première mission qui m'a été donnée à mon entrée en stage a été de réaliser la cartographie du réseau (voir page 9) que gère actuellement le SI.

Les principaux sites dont s'occupe Tourism-it sont :

- Marseille, où se trouve le cœur du réseau et le siège social.
- Montpellier, où se situe le Datacenter.
- Lyon, qui est un relais technique important du réseau.
- Toulouse - Paris – Bouc-Bel-Air - Monaco – Lille (sites en France).
- Islande - Finlande - Belgique - Norvège – (sites internationaux).

Malgré le fait que Tourism-it appartient à Geophyle, il n'en est pas moins soumis à la concurrence de n'importe quelle SSII. En effet, les marques et les entreprises regroupées par Geophyle sont libres de choisir le prestataire qui s'occupera de son système d'informations. Que ce soit pour les outils logiciels, le réseau, l'hébergement de leurs sites Web ou bien la téléphonie.

Chaque site possède une connexion ADSL pour la navigation Internet et une connexion SDSL ou fibre optique pour les flux internes. L'échange interne de flux de site à site se fait via des connexions VPN SSL établies par des routeurs Astaro. Le Datacenter de Montpellier est équipé d'un routeur Astaro redondé et chaque agence est équipée d'un routeur Astaro d'une gamme adaptée au nombre d'utilisateurs.

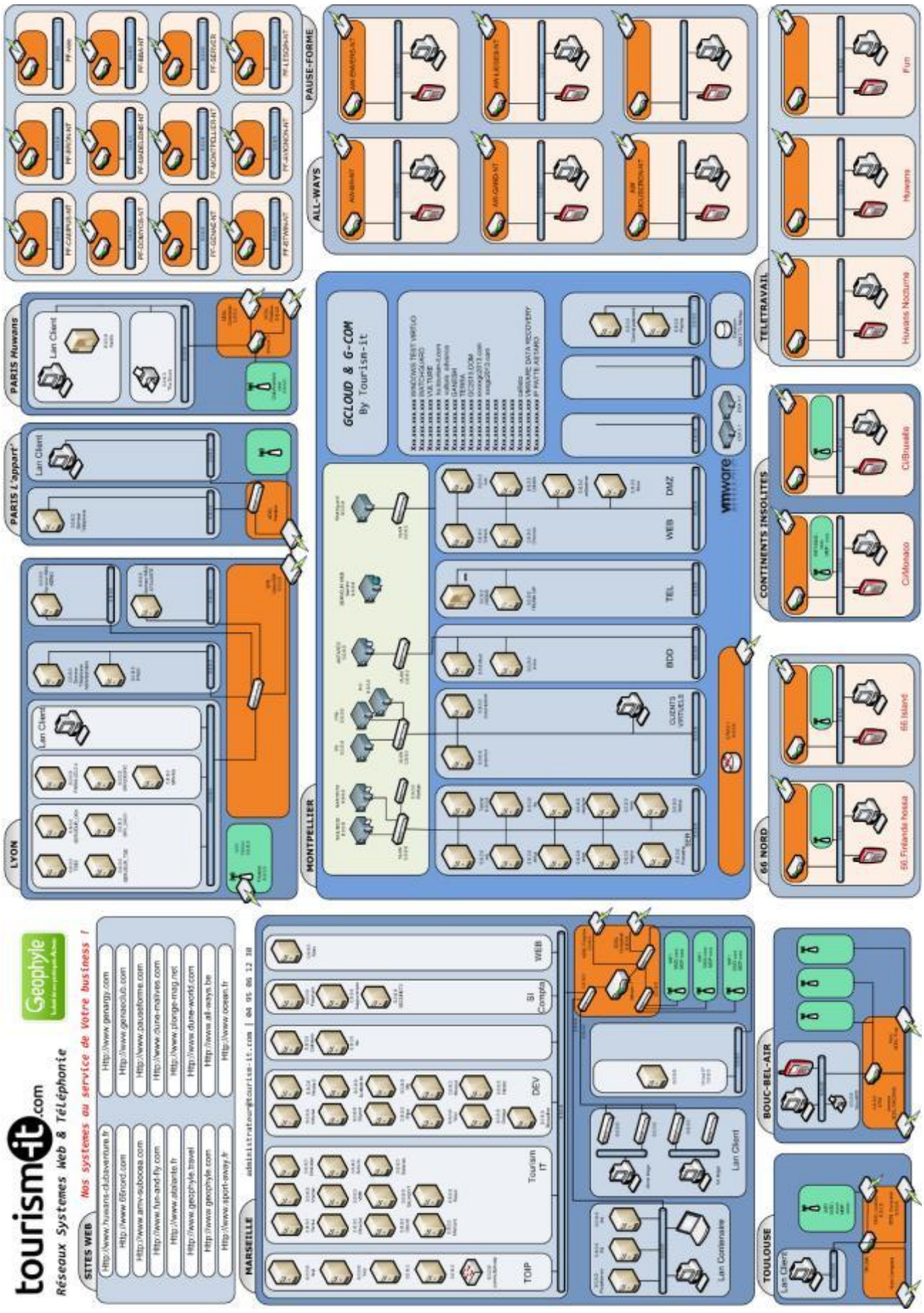
1.3.3.1 Gestion du parc client physique et virtuel

Tourism-it gère actuellement plus de 250 utilisateurs sédentaires ou nomades.
A l'origine, tous les clients utilisaient leur poste de travail pour accéder à leurs outils logiciel, sauf pour les agents nomades.
On peut dire que Tourism-it fut un pionner dans la mise en place d'environnement client virtualisé appelé **contenaire**. Les contenaires sont des machines virtuelles créées avec la technologie Parallels Virtuozzo. Elle permet aux utilisateurs nomades d'accéder à leurs outils logiciels, peu importe le lieu. Je reviendrais plus en détail sur cette technologie dans la mise en place de mes projets.

L'agrandissement de Geophyle avec l'acquisition de nouvelles marques, le non renouvellement du parc client et l'ajout de nouveaux postes d'utilisateurs ont créé une hétérogénéité devenue quasi- impossible à gérer. La compatibilité des outils et des logiciels est vite devenue un problème.

Tourism-it a fait le choix de mettre le système de contenaire à disposition de tous ses utilisateurs afin de compenser le problème d'homogénéité. La duplication des contenaires à l'identique, permet d'avoir cet environnement homogène à moindre coût. Afin de personnaliser le contenaire de chaque utilisateur au niveau des outils utilisés, un système de **template** existe. Les templates facilitent le déploiement de mise à jour ou de nouveau logiciel.

Aujourd'hui, le parc client est devenu obsolète pour une utilisation standard. Certains postes ont presque 10 ans. Ces machines permettent tout de même, en tant que client léger, une utilisation correcte du système de **contenaire** mis à disposition.


tourism-it.com
Réseaux Systèmes Web & Téléphonie
Geophyle
Nos systèmes au service de Votre business !
SITES WEB
MARSEILLE
LYON
PARIS L'appart'
PARIS Huwans
MONTPELLIER
GCLOUD & G-COM
By Tourism-it
ALL-WAYS
PAUSE-FORME
TELETRAVAIL
CONTINENTS INSOLITES
66 NORD
BOUC-BEL-AIR
TOULOUSE
Lan Client
Lan Commerce
Tourism IT
TOIP
DEV
SI Compta
WEB
DMZ
TEL
BDD
CLIENTS VIRTUELS
vmware

1.3.3.2 Gestion du parc serveur physique et virtuel

Le parc serveur du réseau Geophyle se compose de machines physiques et virtuelles. Les serveurs sont répartis en majorité sur les sites de Marseille et de Lyon. Le cœur du système d'information est hébergé au Datacenter de Montpellier. Un système de virtualisation VMware ESXi 4.1 est en place sur Marseille et une Version ESXi 5.0 sur Montpellier.

L'ensemble des serveurs physiques de production sont de marque HP gamme G6 et G7 et sont en contrat de support avec HP : Une carte mère défectueuse doit être remplacée sous 24h par HP.

La maintenance préventive et curative des machines physiques se fait par Tourism-IT. Il subsiste quelques vieilles machines qui sont en passe d'être virtualisées.

Tous les serveurs physiques HP disposent d'un système de supervision SMART en communication permanente avec le serveur Nagios. La perte d'un organe d'un serveur, d'un disque dur ou d'un processeur ..., génère immédiatement une alerte mail aux administrateurs du système d'information.

La gestion des mises à jour Windows se fait au cas par cas sauf pour les systèmes **parallels** qui sont beta testé. La mise en place d'un serveur Windows Server Update Service est en étude et devrait débuter courant 2013.

Globalement les systèmes d'exploitation Windows sont Windows Server 2008 R2 Standard et Debian 5 et 6 pour Unix. Seuls les serveurs ESX sont sous Cent-OS.

La société Tourism-it héberge elle-même toutes ses applications et sites Web. Ils sont répartis entre les sites de Marseille et de Montpellier.
Les services les plus critiques sont hébergés à Montpellier et leur disponibilité est contractualisée.

1.3.3.3 La gestion du Système d'information

Les équipes de Tourism-it étant assez réduites, elles se sont dotées d'outils afin d'optimiser la gestion du Système d'information :

- 5 contrôleurs de domaine pour gérer les utilisateurs et les ressources.
- Un serveur d'ordonnancement Talend.
- Un serveur de supervision Nagios.
- Un robot et un serveur de sauvegarde.
- Un système de détection d'intrusion Snort.
- Un système de reverse proxy redondé Vulture.
- Un outil de centralisation de demande OTRS.
- Un système centralisé d'antivirus Kapersky.

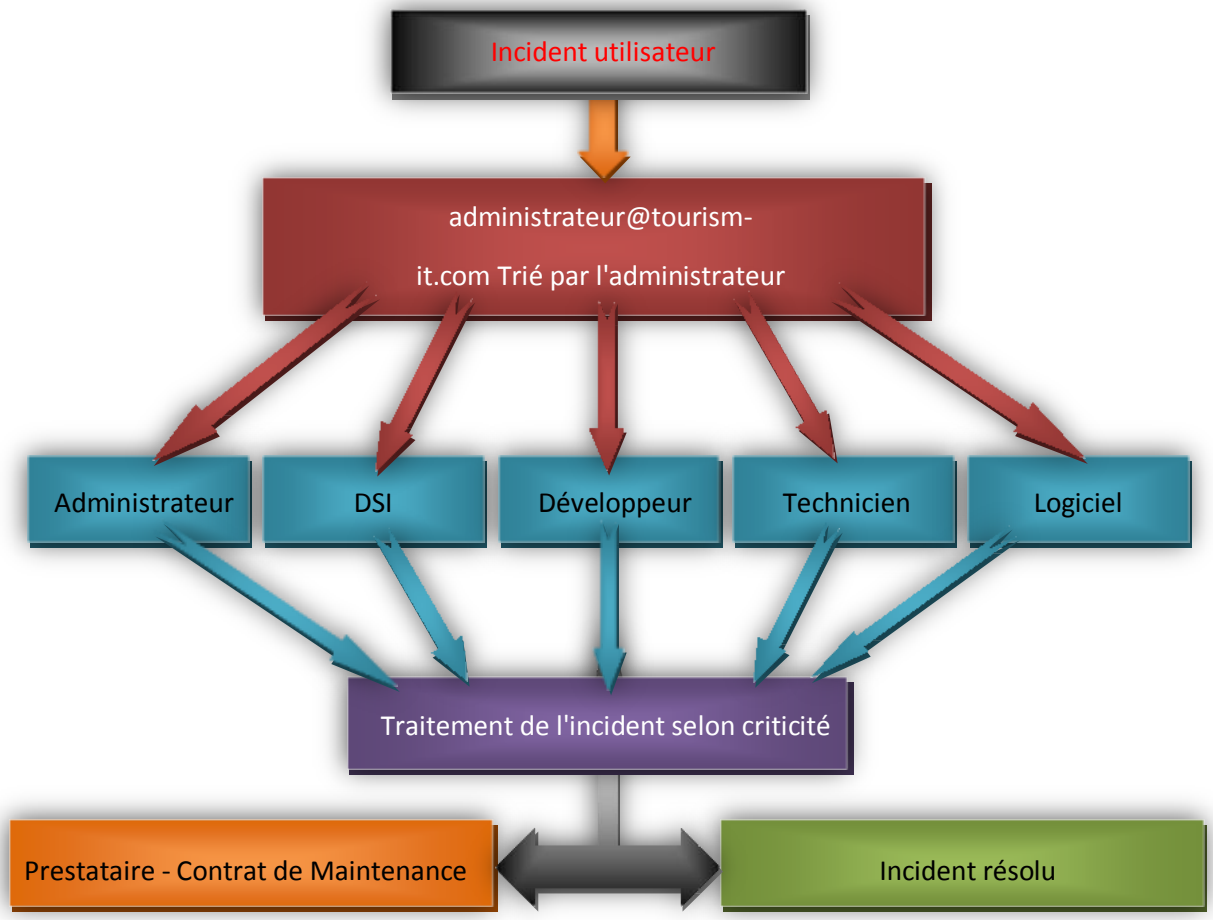
L'utilisation de GPO permet de simplifier le déploiement de nouvelles ressources (imprimantes, logiciels...) et d'administrer certaines demandes personnalisées et particulières.

1.3.3.4 Gestion du Support Utilisateur

Tourism-it se rend disponible pour ses utilisateurs de 9h30 à 18h30 les jours ouvrables et 24h/24, 7jours/7 en astreinte téléphonique et par mail.

La gestion des incidents est centralisée par OTRS (Open-source Ticket Request System). Il s'agit d'un outil qui aide à répondre aux demandes et réclamations des utilisateurs grâce à un principe de files classées par domaines et priorités. La gestion de support demande de la rigueur et de l'organisation.

Les utilisateurs doivent envoyer un mail à administrateur@tourism-it.com en détaillant le plus, précisément l'incident qui s'est produit.
Le ticket est classé selon les domaines de compétences et il est traité selon l'urgence de l'incident.
Ce dernier peut être résolu directement par le responsable du domaine ou bien par un prestataire responsable d'un contrat de maintenance lié à l'incident.



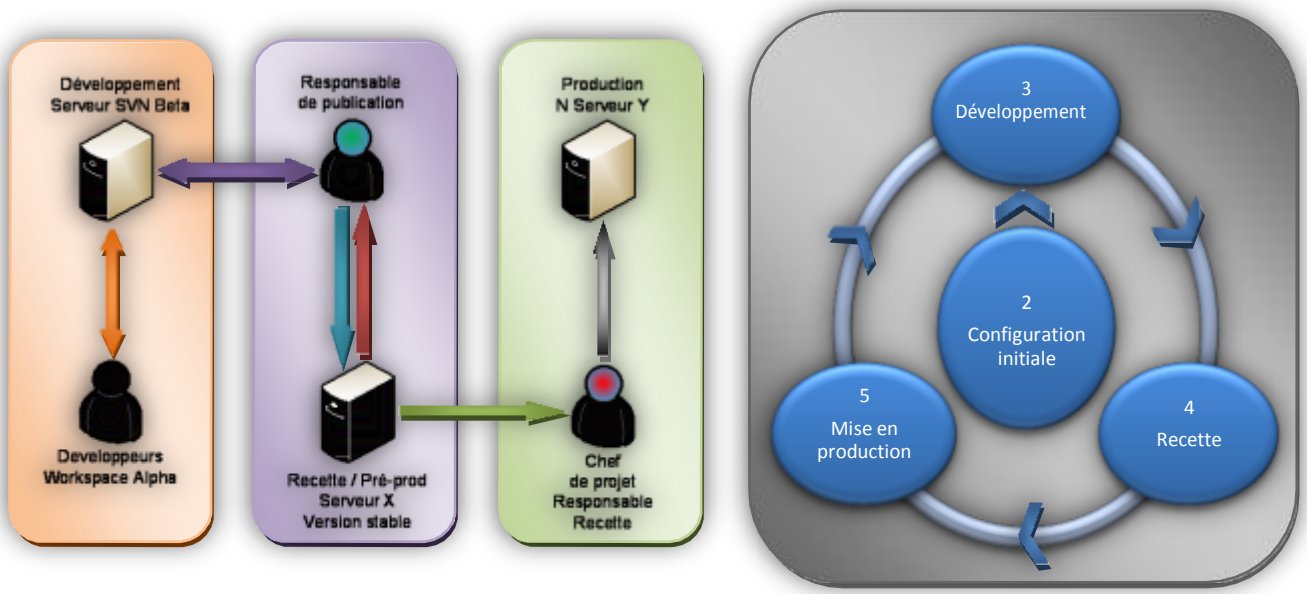
Il reste néanmoins un problème récurrent. Certaines marques ou entreprises résident dans le même bâtiment que Tourism-it, les utilisateurs viennent donc directement exposer leurs incidents dans le service, que ce soit urgent ou bien pas du tout. A noter que l'utilisateur considère par défaut que son problème est toujours le plus urgent et qu'il n'est donc pas évident de leur faire comprendre, sans qu'ils ne se sentent pas pris au sérieux.

1.3.3.5 Recherche, développement et intégration des solutions métiers

Tourism-it possède une branche Développement qui travaille avec les développeurs de chaque entité présente de Geophyle. Certains projets sont aussi développés en partie par des prestataires.
Afin de coordonner ces travaux, Cédric Mendy a mis en place un système de gestion de version, Subversion SVN. Cela permet de centraliser les sources pour tous les développeurs et de conserver une trace de toutes les modifications apportées sur chaque projet.
Le contrôle de versions décrit l'art de gérer les changements apportés à de l'information. Il s'agit depuis longtemps d'un outil vital pour les programmeurs, qui passent généralement leur temps à réaliser de petites modifications qu'ils annulent le lendemain. Partout où vous trouvez des gens utilisant des ordinateurs pour gérer des informations changeant fréquemment, il y a de la place pour le contrôle de version.

1.3.3.6 Architecture et principe

Serveur SVN : Hébergé en interne, il gère les développements et la gestion des dépôts de versions beta.
Serveur Recette : Hébergé en interne, il gère le dépôt des versions stables.
Serveur Production: Hébergé chez un prestataire. Il sert à la mise en production des versions stable



Mode opératoire : Le processus se décompose en 5 étapes

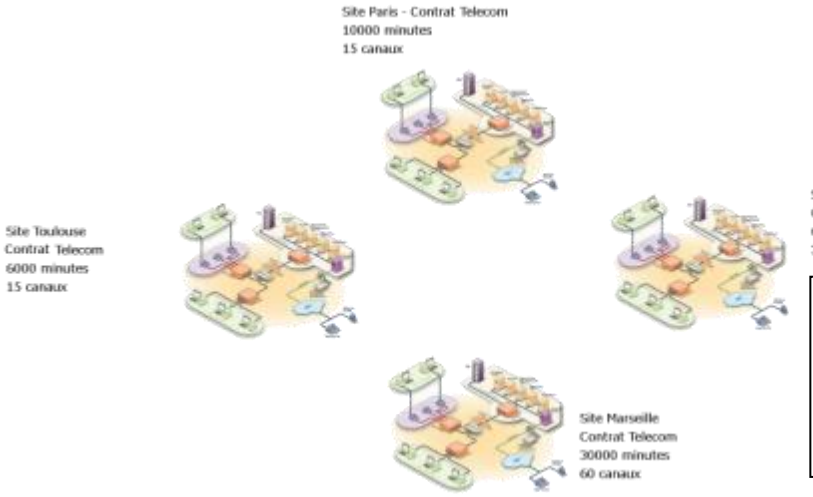
1- Création d'un projet "dépôt initial".
2 - Configuration initiale : Ajout d'un dépôt en local "synchronisation d'un projet avec SVN".
3 - Développement : Mises à jour des développements.
4 - Recette : Synchronisation des développements sur le serveur de recette et validation.
5 - Mise en production : Synchronisation des mises à jour sur le serveur de production.

1.3.3.7 Téléphonie et Télécommunications

La téléphonie au sein de Geophyle est relativement critique. Les ventes de voyage par téléphone représentent 80% du chiffre d'affaire global contre 20% des ventes en agences physiques. L'indisponibilité du téléphone pourrait priver de vente les marques de voyage de Geophyle.

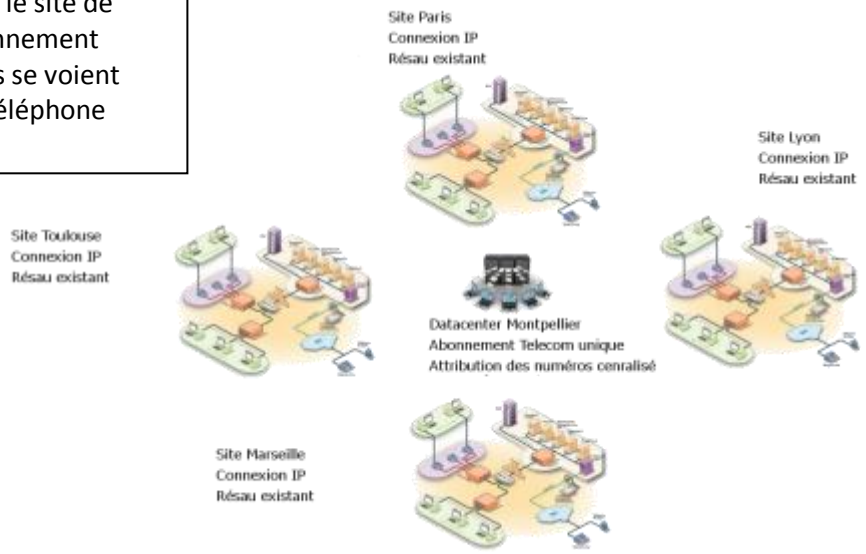
Tourism-it toujours en quête de nomadisme et de flexibilité pour ses agences de vente a mis en place progressivement un système de téléphonie IP déporté.
Ce qui a l'avantage de centraliser en un point unique l'ensemble des lignes internes et externes dans son ensemble. Cela concerne plus de 300 lignes téléphoniques répartis sur 10 sites.
La voix arrive désormais dans les agences non pas par un abonnement France télécom classique mais par un tuyau IP.

L'amortissement du système s'est fait grâce aux économies effectuées en coupant petit à petit les abonnements télécom des agences locales.



Avant l'implémentation de la technologie de téléphonie déportée, chaque site possédait plusieurs contrats d'abonnement Telecom analogique classique

Avec l'implémentation de la technologie de téléphonie déportée, seul le site de Montpellier possède un abonnement télécom. Tous les autres sites se voient attribués leurs numéros de téléphone depuis Montpellier.



2 Les Projets

Dans le cadre de mon stage, Nicolas PAUGAM , administrateur Cloud au sein de Tourisme et Services , m'a donné comme mission de mettre en place un Broker de connexion pour les contenaires Parallels Virtuozo des utilisateurs et de mettre également en place un serveur d'applications pour deux logiciels métier utilisés par la plupart des agences du groupe Geophyle.

Le cahier des charges devra respecter les conditions suivantes :

- Coût de revient le moins élevé possible (solutions OpenSource ou intégrées au logiciels déjà acquis par Tourisme et Services)
- Compatibilité avec le matériel et les logiciels déjà présents dans l'infrastructure existante.
- Flux de connexion sécurisé à l'extérieur

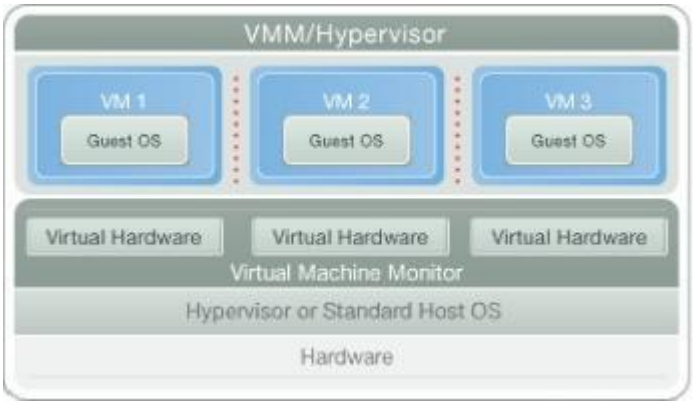
Voici le déroulement de la mise en place de mes 2 projets :

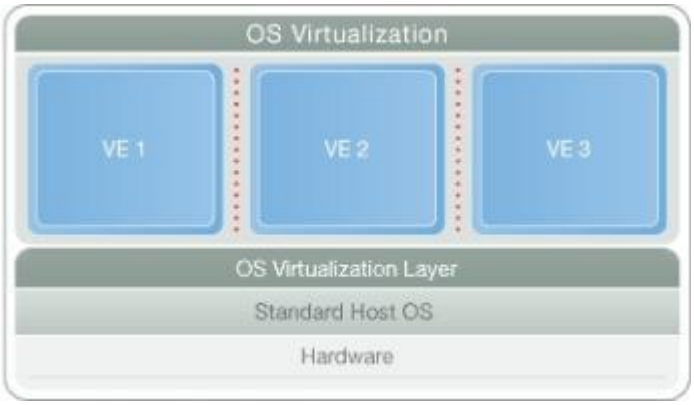
- Evaluer l'infrastructure logicielle actuelle
- Etudier les différentes offres du marché
- Evaluer les besoins en matériel et logiciels ainsi que les licences à acquérir pour mettre en place ces deux solutions.
- Présenter mes propositions aux responsables du SI
- Effectuer l'installation et la configuration des deux solutions
- Effectuer les tests en conditions d'utilisation avant mise en production.

3 Infrastructure logicielle actuelle

Virtualisation d'OS

Parfois appelée virtualisation au niveau OS ou virtualisation d'OS mutualisés, la virtualisation d'OS consiste à créer des serveurs dématérialisés au niveau de la couche du système d'exploitation (noyau).
Avec cette méthode de virtualisation, des partitions isolées, également appelées environnements virtuels (VE) sont créées sur un seul serveur physique et sur une même instance d'OS pour une rationalisation des ressources matérielles, logicielles, des centres de données utilisés et des tâches de gestion.
Les deux schémas ci-dessous représentent l'hyperviseur - ou technologie de virtualisation du matériel - et la technologie de virtualisation d'OS, en comparaison.





Le modèle Hyperviseur est constitué d'une couche de base (en général, il s'agit d'un très petit noyau Linux représenté ici par un hyperviseur ou un OS standard) qui se charge directement dans le serveur vide. Pour pouvoir affecter du matériel ou des ressources à des machines virtuelles, il faut virtualiser l'ensemble du matériel du serveur. La deuxième couche montre toutes les puces ou cartes qui doivent être virtualisées pour pouvoir être affectées à des machines virtuelles. Dans la machine virtuelle elle-même, se trouve une copie complète d'un système d'exploitation et enfin l'application ou la charge.

Le modèle de virtualisation de l'OS est conçu pour favoriser la performance, la gestion et l'efficacité. Ce modèle repose sur un système d'exploitation standard de l'hôte qui, dans le cas de Parallels Virtuozzo Containers, comprend à la fois Windows et Linux. Vient ensuite la couche de virtualisation avec un système de gestion de fichiers propriétaire et une couche d'abstraction pour les services du noyau qui garantit l'isolation et la sécurité des ressources entre les différents environnements virtuels. La couche de virtualisation permet à chaque environnement virtuel d'apparaître comme étant un serveur autonome. Enfin, l'environnement virtuel lui-même héberge l'application ou la charge.

Qu'est-ce qu'un VPS ?

Le VPS est un serveur virtuel qui possède tous les avantages d'un serveur dédié physique : sécurité, stabilité, disponibilité, autonomie et une totale maîtrise.

Avec ses propres DNS et adresses IP fixes, l'administrateur d'un VPS dispose d'un accès **root** (pour Linux) ou administrateur (pour Windows), et d'un VZPP (Virtuozzo Power Panels) pour administrer son VPS.

Il peut également installer les applications de son choix, et redémarrer ou même formater son serveur en cas de besoin.
Tout professionnel, développeur web, hébergeur…. est amené, dans son travail de tous les jours, à profiter des différents avantages d'un VPS, par exemple :

- Sauvegarde et accessibilité : Vous pouvez utiliser votre VPS pour la sauvegarde de vos applications importante (ex : comptabilité) et que vous pouvez consulter et mettre à jour à partir de n'importe quel ordinateur connecté à Internet en totale sécurité.
- Développement : En étant en parfaite maîtrise de votre VPS, vous pouvez y tester et lancer des applications et scripts que vous développez dans un environnement que vous pouvez personnaliser et adapter à vos besoins.
- Hébergement web professionnel : En bénéficiant de la totalité des ressources du serveur, vous pouvez héberger vos clients sur votre VPS en toute fiabilité et disponibilité. Vous pourrez même leur allouer certains droits et accès pour la gestion de leurs espaces.

Sans oublier que le VPS est parfaitement flexible : pour plus de ressources et de capacité vous pouvez transférer vos fichiers et applications de votre VPS vers un autre plus puissant sans aucun temps d'arrêt !

Qu'est-ce que la technologie Parallels Virtuozzo Containers ?

Parallels Virtuozzo Containers est une solution de virtualisation et d'automatisation qui permet de partitionner un serveur physique en plusieurs serveurs privés isolés les uns des autres.

Il est ainsi possible d'obtenir plusieurs entités complètement indépendantes de la couche matérielle sur une seule machine, chaque entité est en isolation totale, elle a ses propres répertoires, utilisateurs, adresses IP, mémoire, processus, fichiers, systèmes de librairies, fichiers de configuration, etc... Les dites entités sont appelées : VPS (Virtual Private Server).

Grâce à cette répartition parfaite, chaque VPS est en autonomie totale :

- Accès **root** pour Linux ou administrateur pour Windows
- Possibilité d'installer de nouvelles applications
- Possibilité de redémarrer le VPS ou même le formater sans affecter le reste de la machine.

En cas de besoin de plus de ressources et de capacités, Parallels® Virtuozzo Containers facilite le transfert d'un VPS à un autre sans aucune difficulté ni temps d'arrêt (d'où vient l'appellation DDS « Dynamique Dedicated Server »)

Pour l'administration, Virtuozzo Power Panels (VZPP) est un outil Web très performant pour gérer les différents VPS. Avec VZPP, n'importe quel utilisateur ayant les droits nécessaires peut facilement effectuer les taches d'administration courantes :

- Démarrage/Arrêt/Redémarrage du VPS
- Monitorage et Gestion des services du VPS
- Sauvegarde/Restauration
- Réinstallation ou réparation du VPS

Les ressources **Parallels Virtuozzo Containers** sont gérées par un système de **QoS** (quality of service). Ce dernier permet d'assurer à chaque VPS un quota de ressources propres, auquel aucun autre VPS ne peut accéder ni l'utiliser. La QoS permet ainsi de disposer d'un ensemble de ressources suffisantes pour être indépendant et en totale maîtrise de la machine.

Avec plus de 200 000 VPS en production, **Parallels Virtuozzo** Containers est actuellement la solution la plus stable et la plus éprouvée dans le domaine de la virtualisation des serveurs.

Les serveurs

Tous les principaux serveurs fonctionnent sous Microsoft serveur 2008 Standard R2

Accès aux contenaires des utilisateurs

L'accès aux containers **Parallels** se fait principalement à l'aide du **Remote Desktop Protocol (RDP).**

Propositions au SI

Après diverses recherches, j'ai rédigé un document regroupant les principales solutions possibles et l'ai présenté en réunion à la direction du SI.

Vous retrouverez ce document en première partie des Annexes à la fin de ce rapport.

4 Installation et Configuration des Projets

4.1 Le serveur d'applications

4.1.1 SOLUTION 1 : Ulteo OVD 3.0.4 (release 7/2013 → disponibilité OVD 4 Beta 10/2013)

Ulteo est une société qui édite des solutions libres pour le marché du bureau virtuel. Elle a été créée par Gaël Duval, cofondateur de Mandriva. En 2009, la société a reçu un Open Source Innovation Award décerné par l'Open World Forum pour sa solution Open Virtual Desktop.

Histoire

Gaël Duval travaillait déjà sur le projet Ulteo alors qu'il était encore employé par Mandriva, mais après avoir été licencié, il fonda une nouvelle compagnie appelée Ulteo pour se concentrer sur son projet.

- **Définition du VDI**

Le Virtual Desktop Infrastructure est une dissociation de la machine utilisateur d'une part et de la machine physique d'autre part.

L'objectif de cette technologie réside dans l'implémentation de la machine virtuelle dans un serveur distant du système ce qui permet à l'utilisateur d'accéder à l'intégralité de ses programmes, applications, processus et données et ce quel que soit le client matériel qu'il utilise.

Pourquoi utiliser Ulteo ?

C'est une solution Open source développée en France (14000 CAEN) qui rencontre actuellement un grand succès international.

Voici donc la procédure d'installation de la version 3.0.4 d'Ulteo OVD

- **Présentation de cette solution**

Avant de rentrer dans le vif du sujet, il me semble préférable que j'explique ici les différents serveurs nécessaires pour faire fonctionner cette solution.

Ulteo OVD utilise différents serveurs avec différents rôles. Certains sont obligatoires, d'autres optionnels.

- **Session Manager**

C'est le serveur central de l'architecture Ulteo OVD. Il gère le lancement des sessions utilisateurs et héberge la console d'administration. C'est le premier logiciel à installer.
Pour l'instant, il ne tourne que sous Linux mais, il est possible de le faire tourner sous Windows en l'installant via les sources.

- **Application Server**

Il permet de fournir les applications et les bureaux. Il faudra donc plusieurs de ces serveurs pour héberger les applications et accéder aux bureaux à distance en fonction du nombre d'utilisateurs connectés.
Ce ou ces serveurs peuvent tourner sous Linux et Windows. Cela dépend de vos besoins. Evidemment si vous avez besoin d'application Linux et d'applications Windows, vous aurez besoin au minimum d'un Application Server Linux et un Windows.

- **Web Client**

Cela permet de démarrer une session sans avoir à installer quoique ce soit sur la machine cliente. Seul le navigateur web est nécessaire. Ce n'est pas le seul moyen de démarrer une session, vous pouvez utiliser le client natif d'Ulteo. Ce module n'est donc pas obligatoire.

- **File Server**

Il permet de centraliser les fichiers des utilisateurs. Notamment, il assure que les utilisateurs puissent accéder aux mêmes fichiers alors qu'ils utilisent des applications hébergées sur serveurs différents. Il stocke les profils utilisateurs et les répertoires partagés.

- **Gateway**

La solution Ulteo OVD utilise plusieurs ports lors d'une session active, principalement le 443 et 3389 (HTTPS et RDP). Mais, selon la politique de sécurisation du réseau établissement/entreprise, certains de ces ports peuvent être bloqués. (lorsqu'un utilisateur essaye de travailler depuis un réseau extérieur notamment).
Ce module « tunnelise » toutes les connexions OVD en liens HTTPS. De ce fait, de n' importe où, vous pourrez démarrer une session distante.
Ce module est donc optionnel.

- Performances requises pour faire tourner la solution

  - **Session Manager**

- Tests : 1 CPU et 512 Mb de RAM minimum,
- Production : 2Gb de RAM et 2 CPU minimum.

  - **Application/File Server**

- Tests : 1 CPU et 1Gb de RAM minimum,
- Production : 4Gb de RAM et 2 CPU minimum.

  - **Web Client**

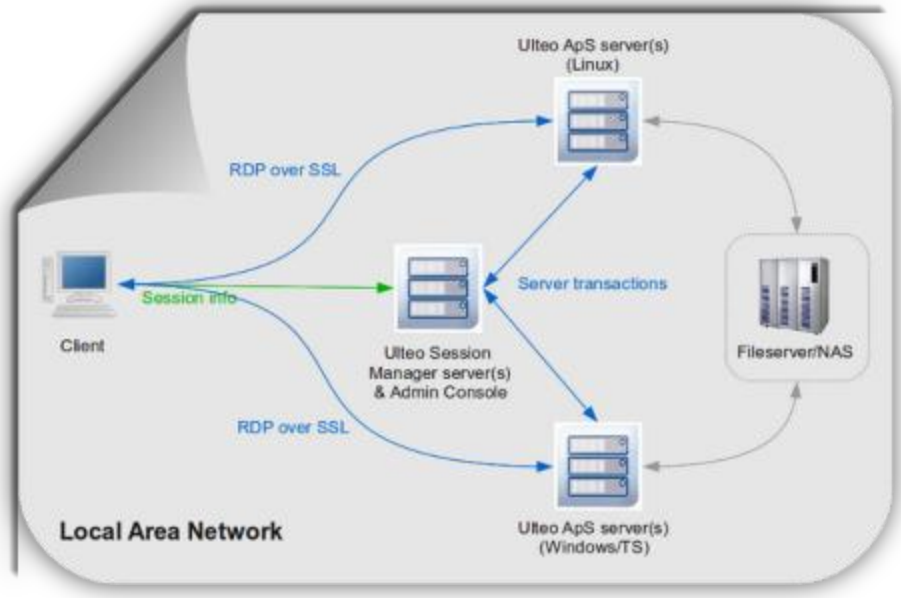
- Tests : 1 CPU et 512Mb de RAM minimum,
- Production : 1Gb de RAM minimum.

Pour ce premier projet, 2 serveurs sont mis à ma disposition au sein du Datacenter de Montpellier.
Nous avons mis en place deux VM sous VMWARE ESX 5 :

- Le **session Manager** avec 1 processeurs Xeon à 2 Ghz / 1 Go de RAM et 20 Go d'espace disque.
  Le système d'exploitation installé sera Debian 6 Squeeze.
- L'**Application Server** avec 2 processeurs Xeon à 2 Ghz / 4 Go de RAM et 20 Go d'espace disque.
  Le système d'exploitation installé sera Windows server 2008 R2 Standard

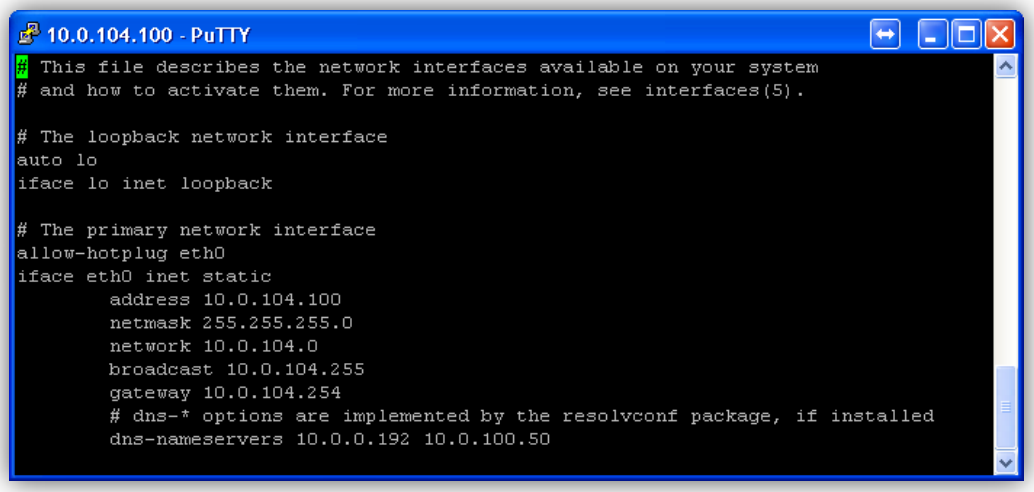
Les accès distants aux VM pour l'installation se feront à l'aide des logiciels **Putty** et **SSH Secure Shell Client**.

Principe de fonctionnement d'Ulteo



4.1.1.1 Installation du Serveur Session Manager

Je passe en détail l'installation du système d'exploitation Debian 6, il faudra juste faire attention a bien configurer les paramètres réseau en éditant le fichier **/etc/network/interfaces** :



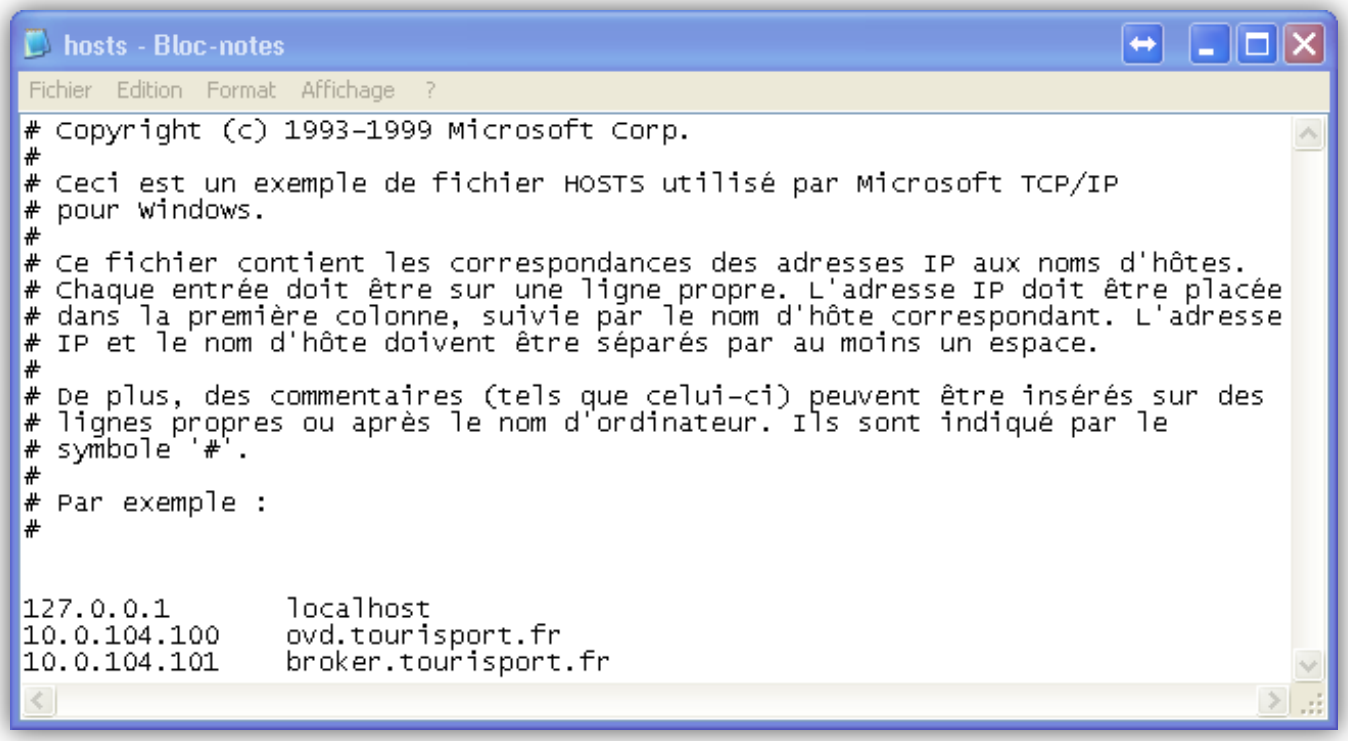
Et à déclarer correctement le nom du serveur dans le fichier **/etc/hosts**

Après configuration, il suffira de tester les accès à la VM.

```
P:\>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

P:\>ping ovd.tourism-it.com

Envoi d'une requête 'ping' sur ovd.tourism-it.com [10.0.104.100] avec 32 octets
de données :

Réponse de 10.0.104.100 : octets=32 temps=38 ms TTL=62
Réponse de 10.0.104.100 : octets=32 temps=38 ms TTL=62
Réponse de 10.0.104.100 : octets=32 temps=36 ms TTL=62
Réponse de 10.0.104.100 : octets=32 temps=37 ms TTL=62

Statistiques Ping pour 10.0.104.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 36ms, Maximum = 38ms, Moyenne = 37ms

P:\>
```

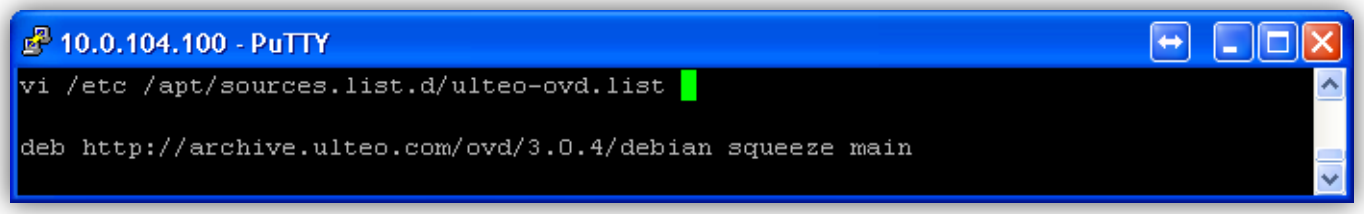
A propos de la commande **\ > ipconfig /flushdns**

- Cette commande sert à purger le cache DNS de votre poste Windows. Mes projets étant encore au stade expérimental et avec des noms et adresses IP temporaires, ils ne sont pas déclarés au niveau des serveurs DNS.
  Pour pouvoir y accéder avec un nom FQDN, il faudra les déclarer dans le fichier **C:\WINDOWS\system32\drivers\etc\hosts**

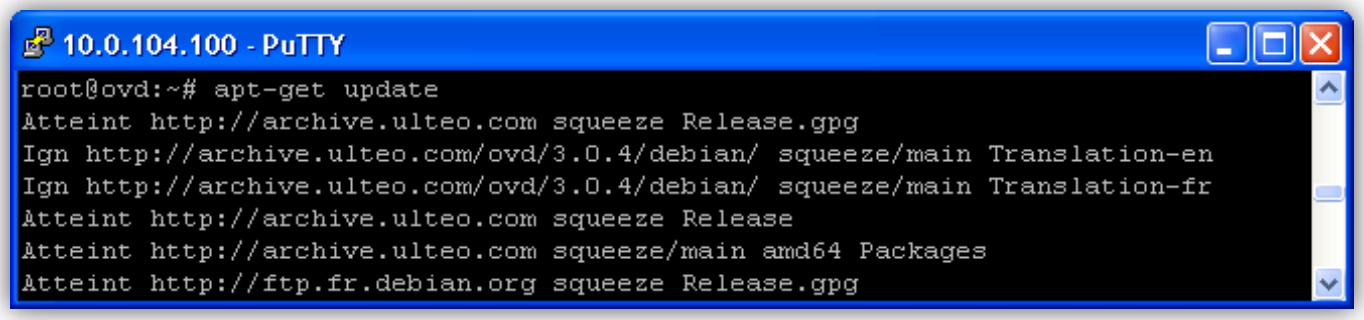


Debian Squeeze (6.0) est un système basé sur Debian qui utilise le système de récupération : **apt-get**. Il faudra donc avoir une connexion Internet sur le système Debian Squeeze (6.0) pour pouvoir ajouter un dépôt Debian Ulteo.

Créer et modifier le fichier **/etc/apt/sources.list.d/ulteo-ovd.list** fichier et ajouter cette ligne:



Effectuer ensuite la commande **# apt-get update**



L'option update met à jour la liste des fichiers disponibles dans les dépôts APT présents dans le fichier de configuration **/etc/apt/sources.list.** L'exécuter régulièrement est une bonne pratique, afin de maintenir à jour votre liste de paquets disponibles.

Un message d'erreur apparaitra, en fait la clef GPG du dépôt n'est pas encore intégrée.
Pour y remédier il faut l'installer en tapant la commande suivante :

```
# sudo apt-get install ulteo-keyring
```

Et de nouveau

```
# sudo apt-get update
```

Installation de MySQL

Le gestionnaire de sessions est un système LAMP (Linux Apache MySQL PHP) et peut être utilisé sur un serveur LAMP déjà existant

Installer le paquet **mysql-server**

```
# Apt-get install mysql-server
```

-→ Un mot de passe **root** sera demandé.

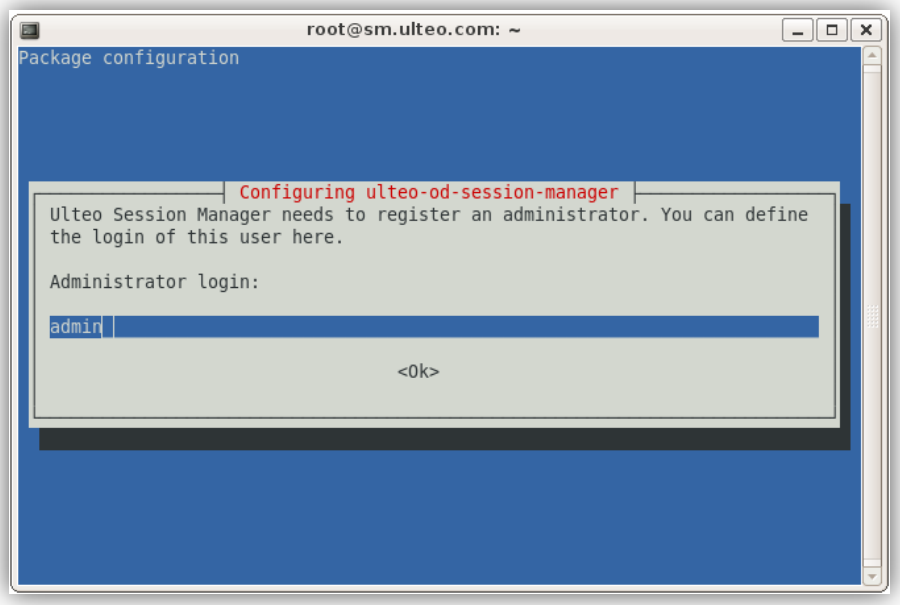
Maintenant créer la base de données nécessaire à OVD

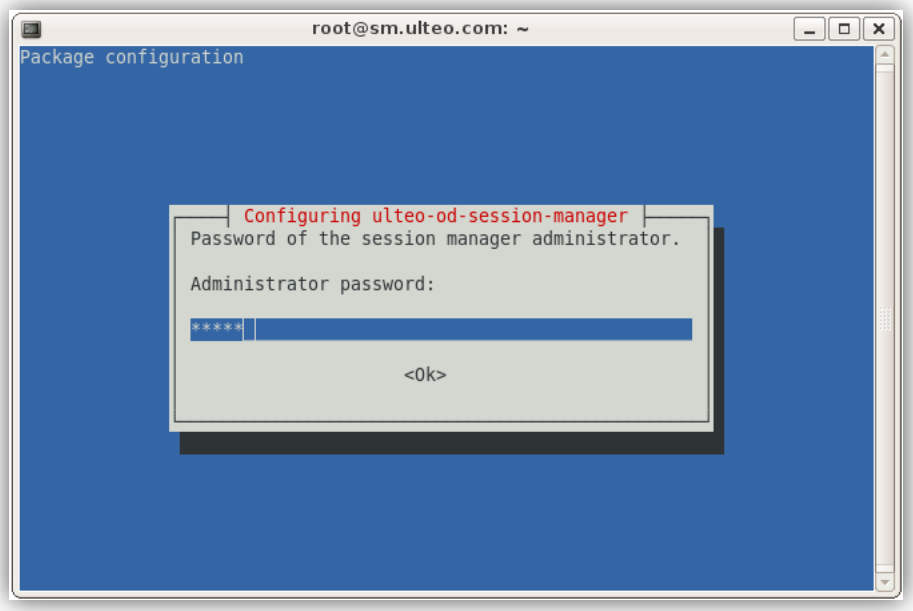
```
# Mysql-u root-p-e 'CREATE DATABASE ovd'
```

Installez le paquet Ulteo OVD-session-manager:

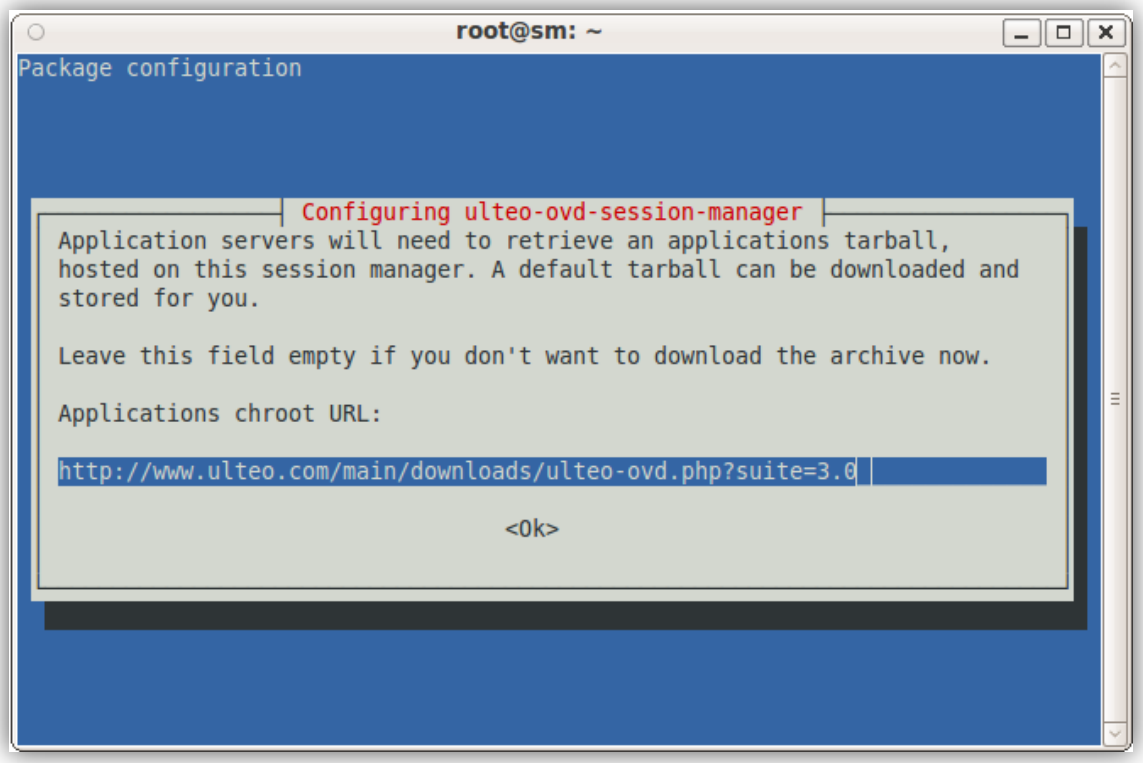
```
# Apt-get install Ulteo OVD-session-manager
```

Le programme d'installation requiert un login et un mot de passe administrateur.





Nous allons également préinstaller un serveur d'application Linux sur le Session Manager

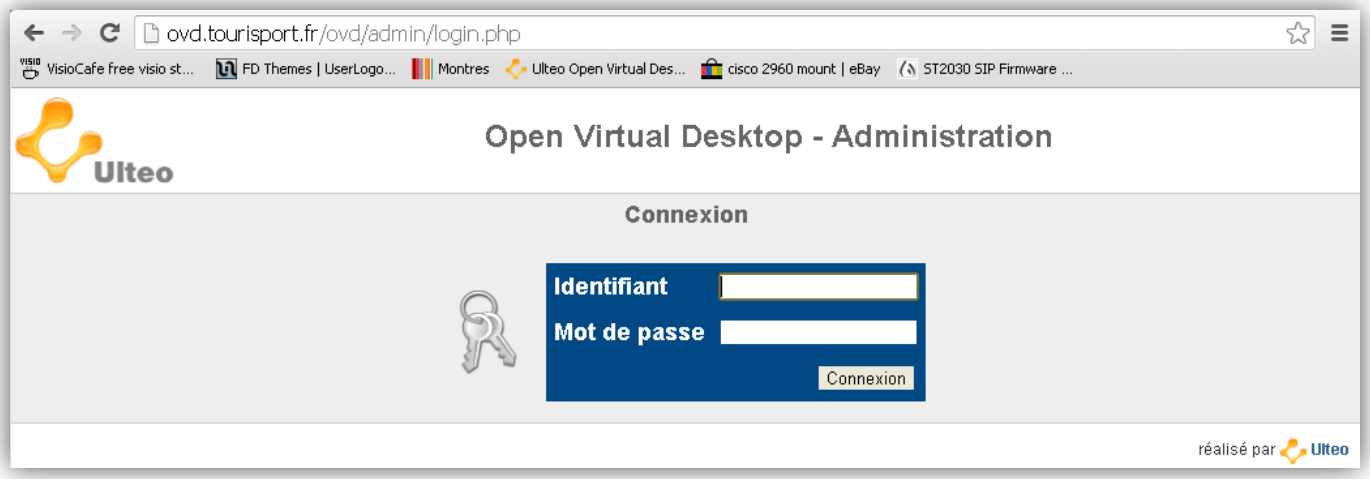


Voilà notre serveur est presque opérationnel.

Le plus compliqué sera bien entendu la configuration de ce logiciel pour l'intégrer dans le SI.

Sur la page suivante, nous allons configurer le session-manager et gérer les utilisateurs.

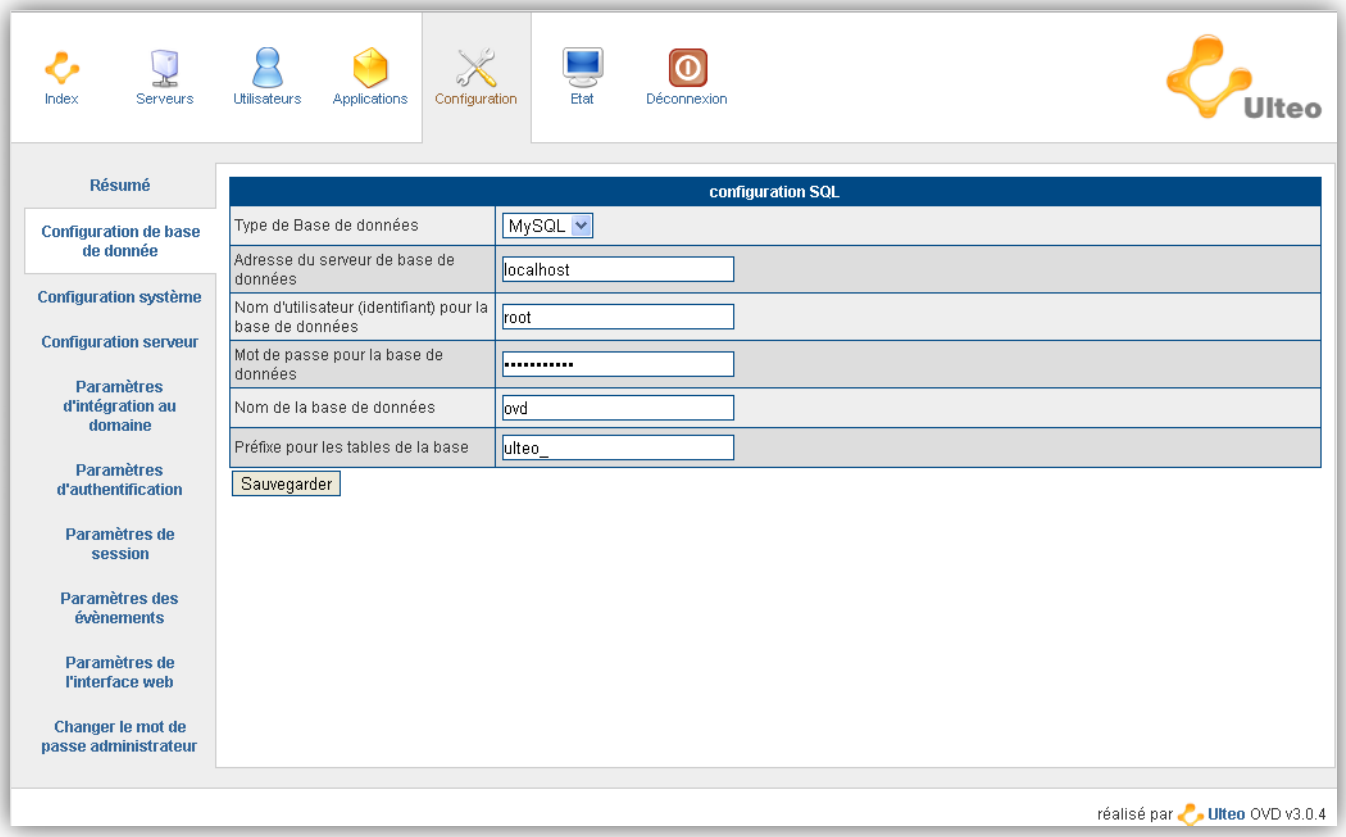
Ouvrez une page web et tapez l'url suivante : **http://votre_serveur/ovd/admin**.
Identifiez-vous avec le compte administrateur créé lors de l'installation du paquet **ovd-session-manager.**



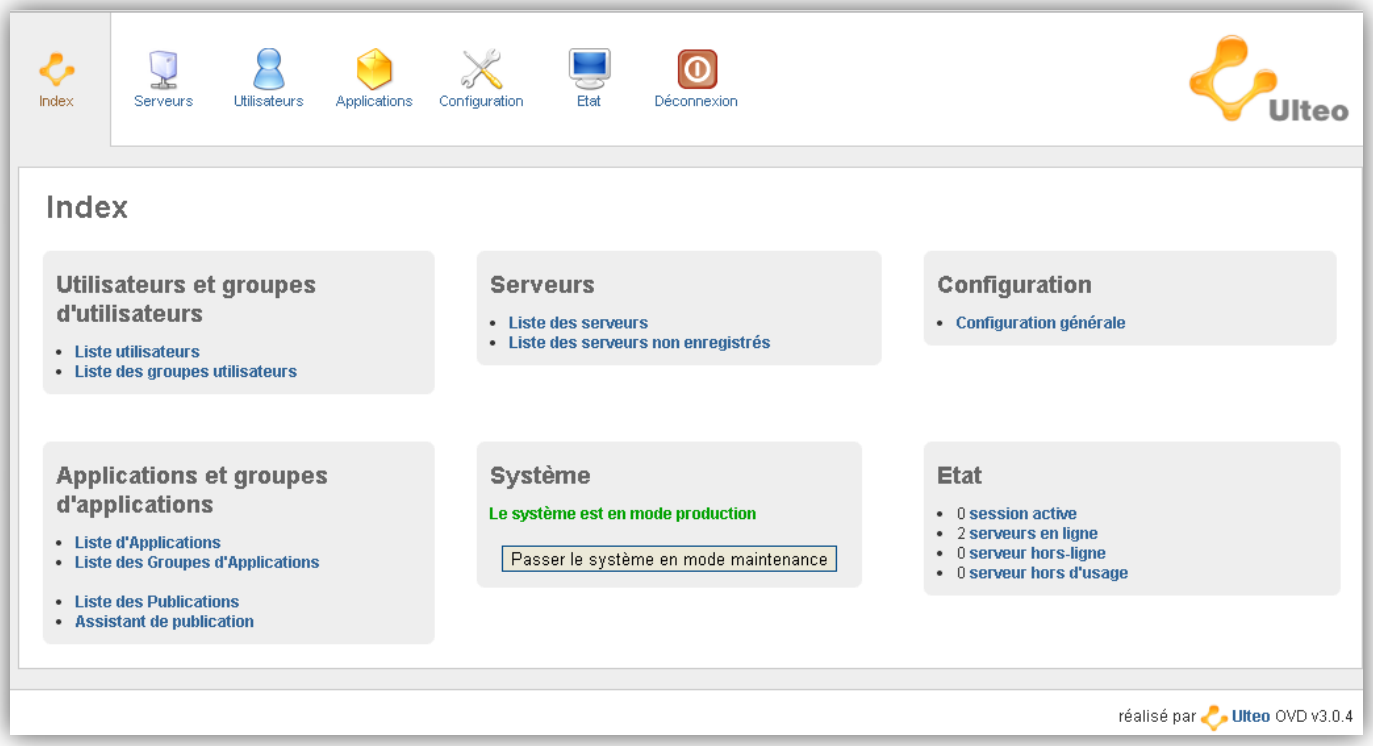
Configuration de la base de données

Pour la première fois que vous vous connectez, le système détecte que la configuration n'est pas encore effectuée de sorte que vous êtes redirigé vers une page de configuration de base qui permettra de sauver une configuration par défaut.

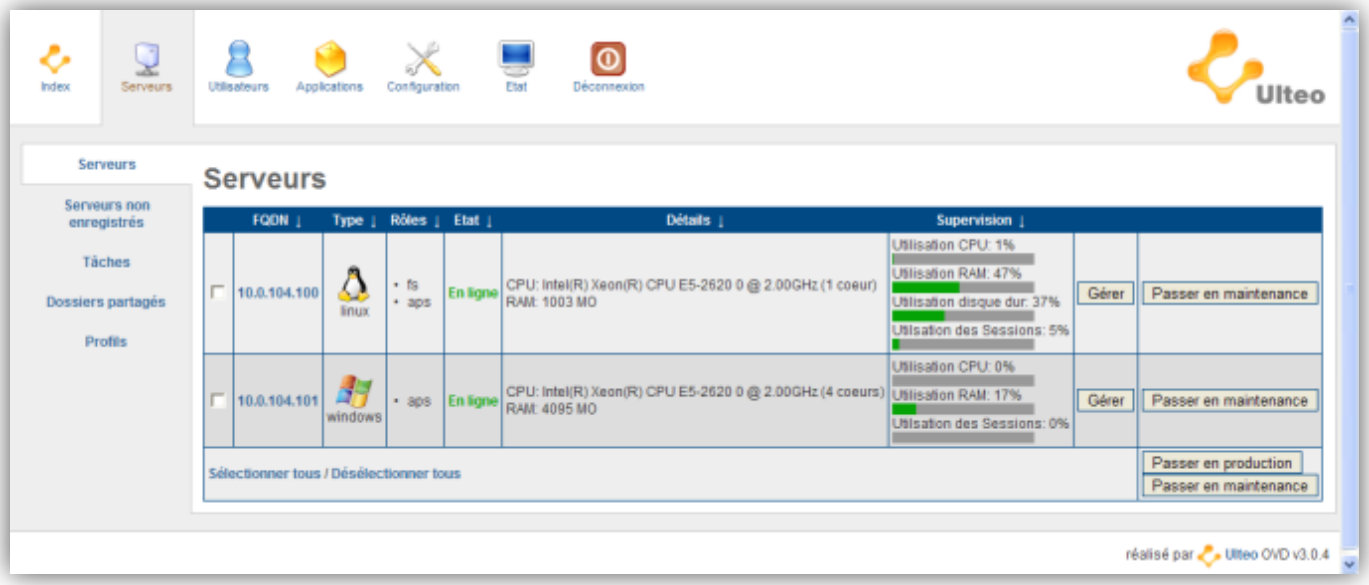
Vous devez définir la configuration de MySQL. Par exemple, si vous installez MySQL sur le même hôte comme décrit précédemment, voici la configuration, il vous faudra renseigner les informations comme ci-dessous: (le mot de passe est le même qui a été utilisé tout à l'heure pour créer la base).



On est ensuite redirigé vers la page d'accueil de la console d'administration

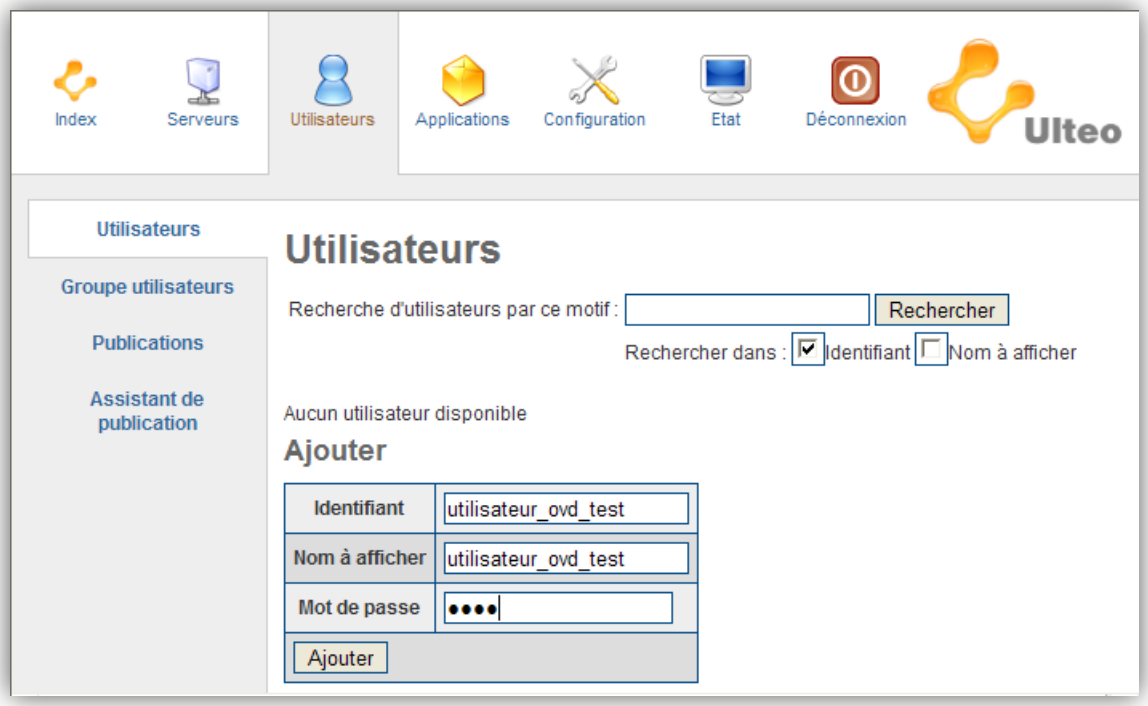


Lors du premier lancement, dans l'onglet serveur, il faudra enregistrer les nouveaux serveurs qui apparaissent dans cette section pour pouvoir les passer en mode production.



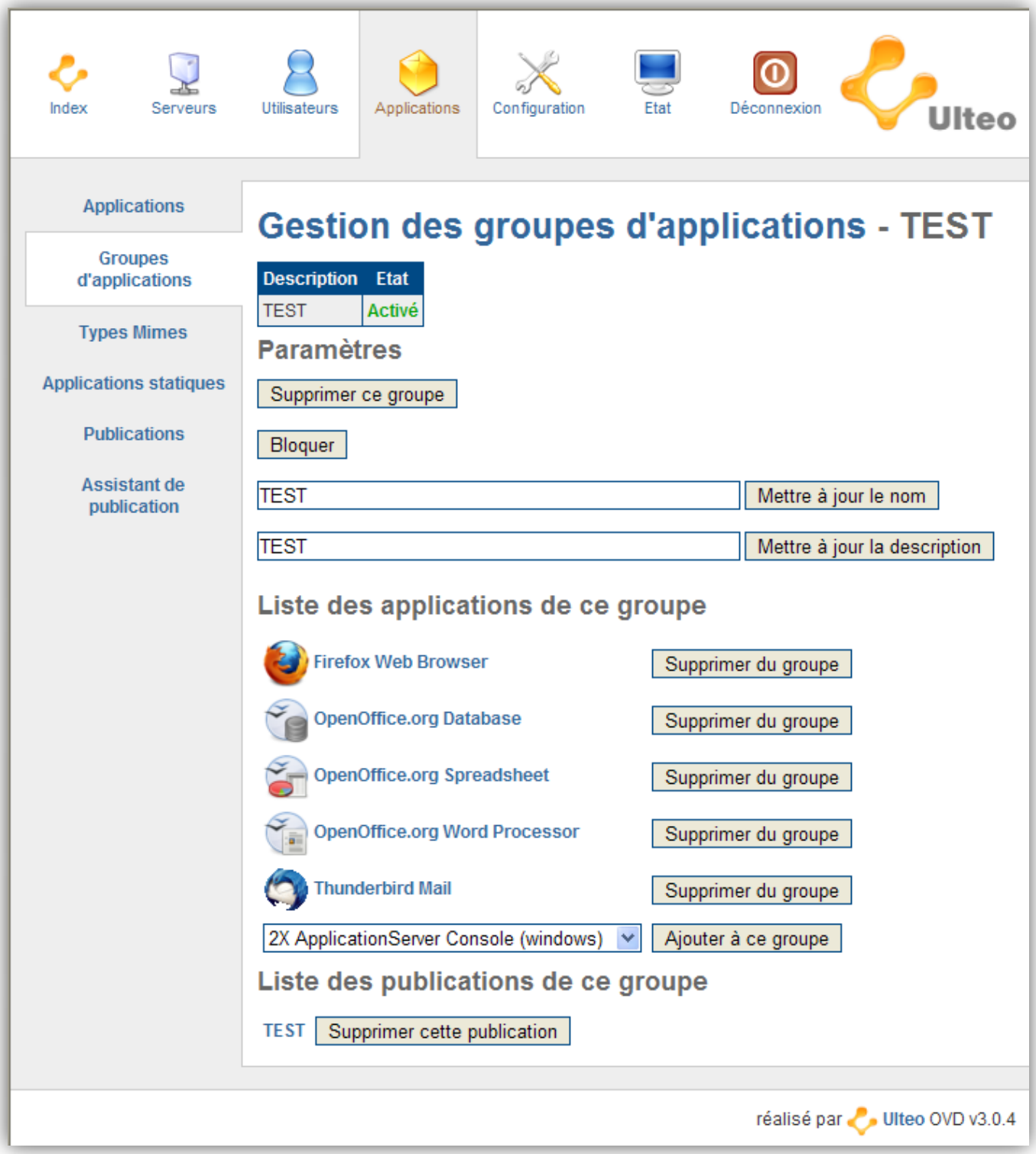
Sur cette copie d'écran nous voyons notre serveur management (10.0.104.100) ainsi qu'un second serveur Windows dont je détaillerais l'installation plus tard.

A ce stade nous pouvons tester l'accès à un bureau virtuel.
Nous devons d'abord créer un utilisateur que nous nommerons : **utilisateur_ovd_test**

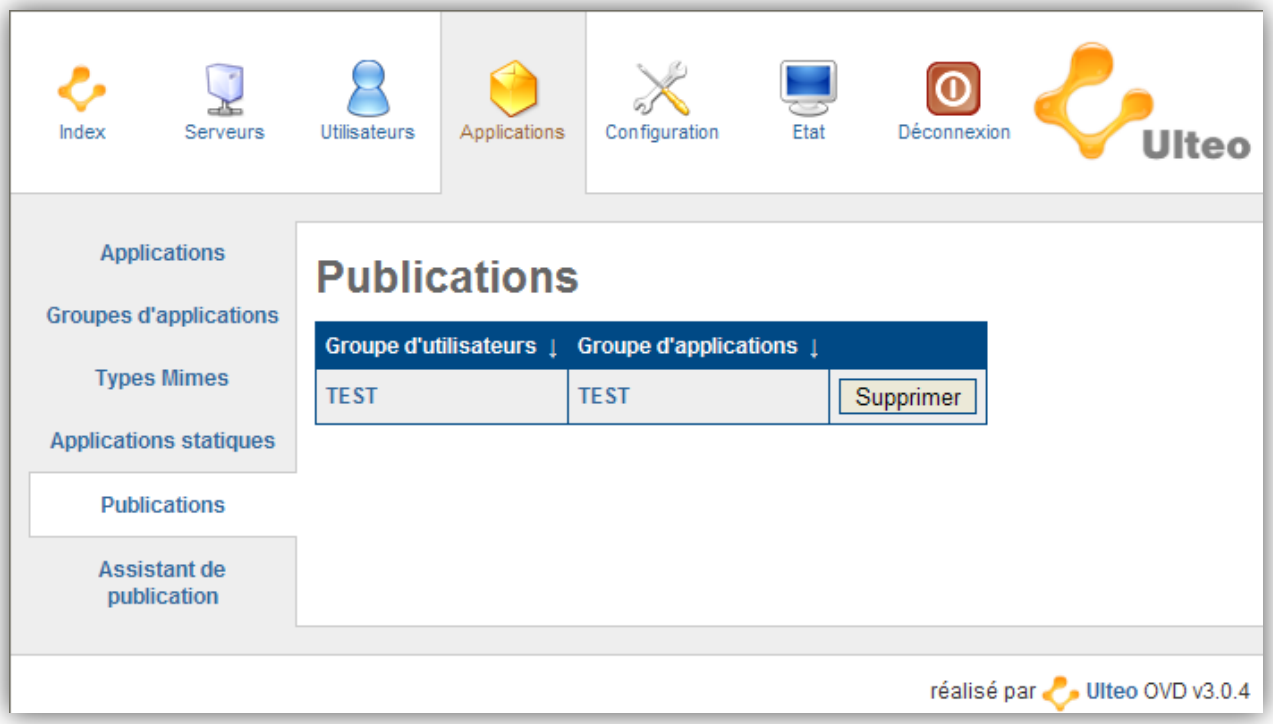


Nous devons ensuite créer un groupe utilisateur et y intégrer celui nouvellement créé.

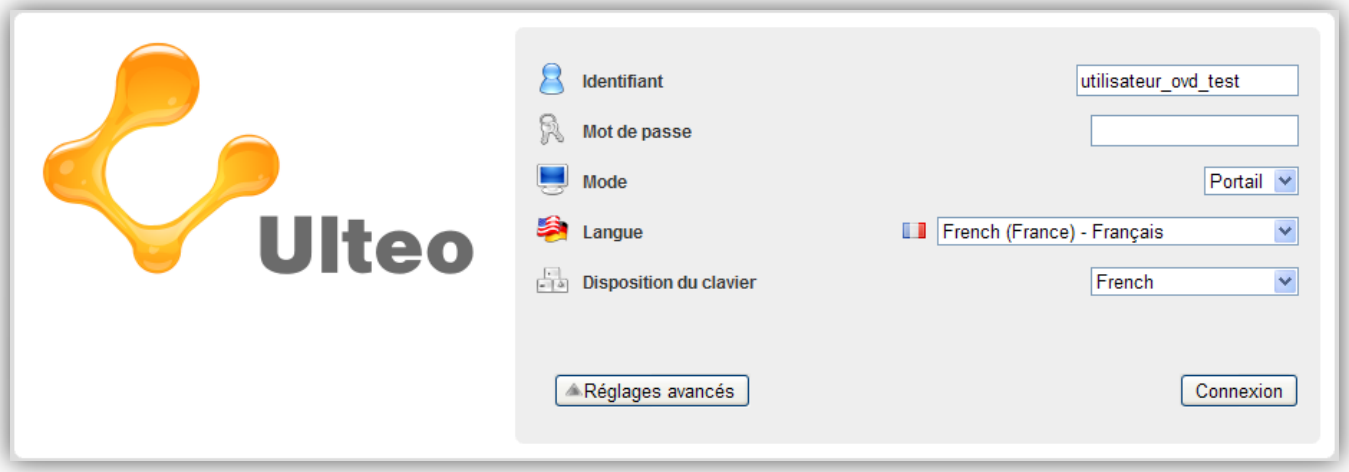
Nous devons ensuite créer un groupe d'application en y intégrant quelques logiciels présents sur le serveur d'application Linux intégré au Session Manager.



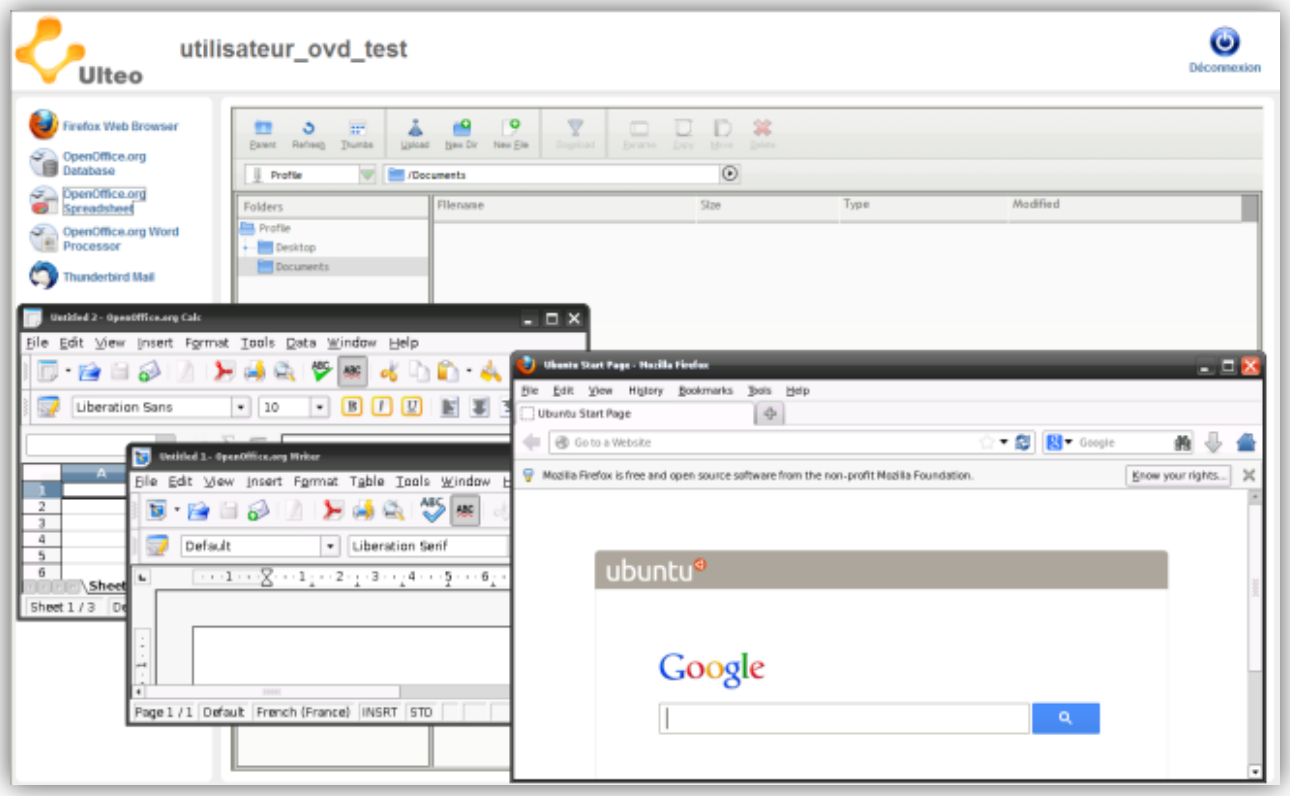
Il faudra ensuite créer une publication liant notre groupe d'utilisateurs à notre groupe de publication.



A partir de maintenant nous pouvons nous loguer sur une session avec notre profil utilisateur à l'adresse :
http://votre_serveur/ovd/



En mode portail les applications disponibles apparaissent sur le côté gauche de la page web, la partie droite de l'écran est constituée des différents disques et espaces de stockages accessibles à l'utilisateur.
Pour lancer une application il suffira de cliquer sur l'icône, toutes les applications peuvent fonctionner en même temps.



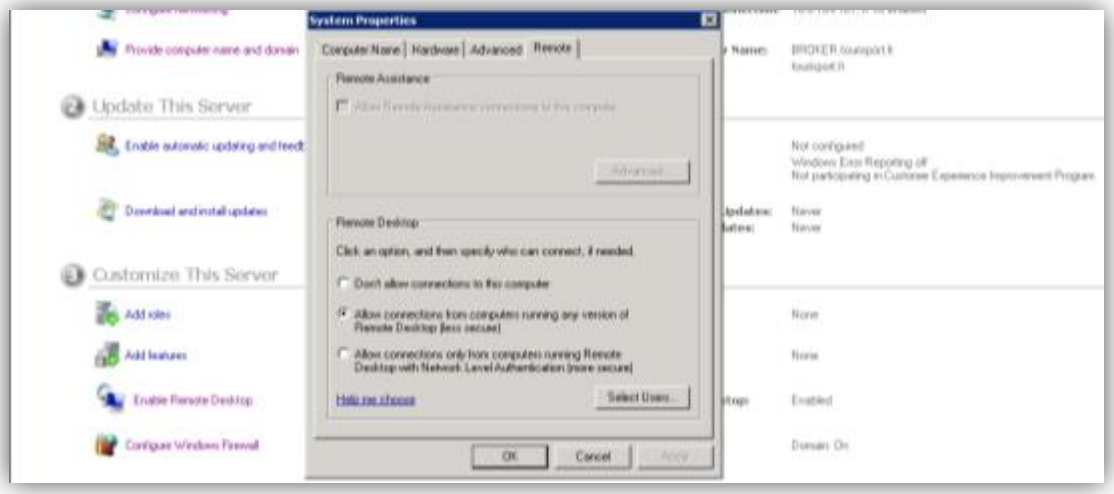
4.1.1.2 Installation du Serveur d'applications Windows

Nous allons maintenant procéder à l'installation du serveur d'application Windows.
Pour cela nous installerons une version de Windows Server 2008 R2 sur notre deuxième Vm.

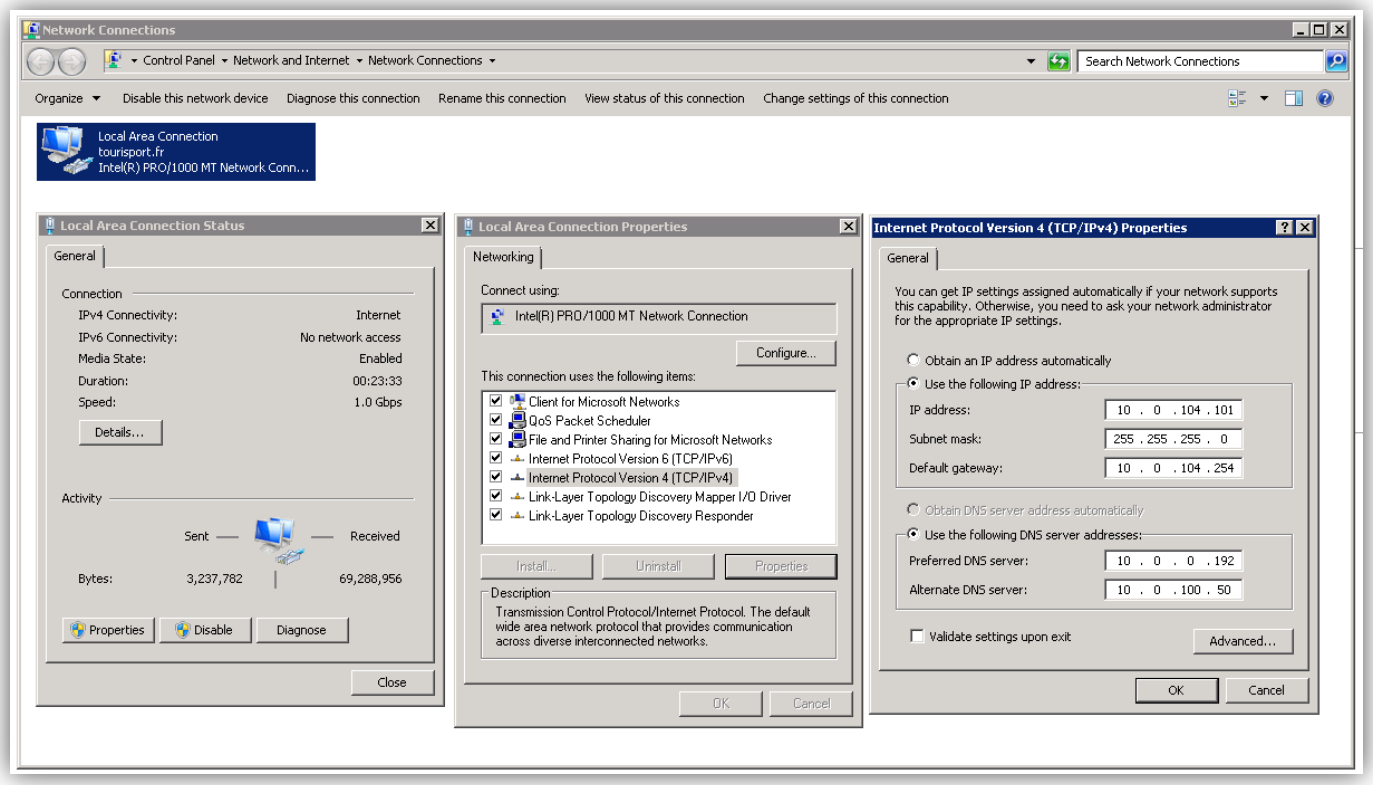
Important

Le serveur Windows peut fonctionner en groupe de travail ou être membre d'un domaine AD, **mais ne doit pas** fonctionner comme un contrôleur de domaine.

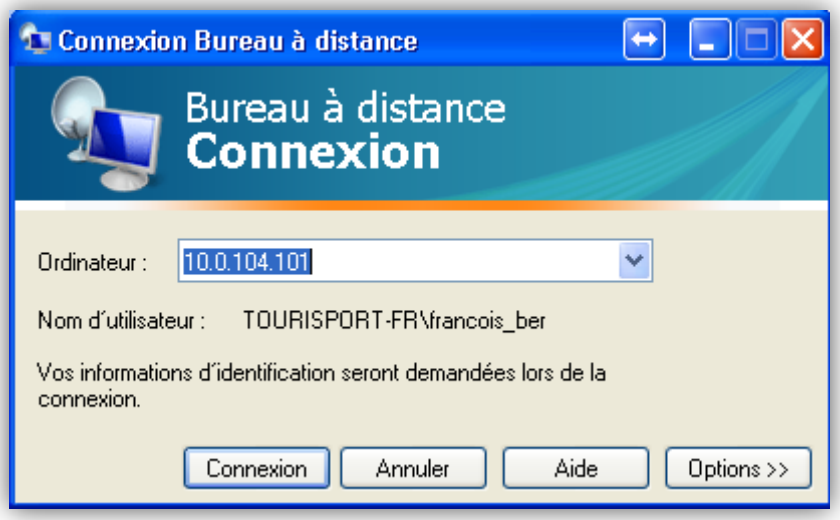
Nous veillerons à activer le service REMOTE DESKTOP, la Vm étant installée au Datacenter de Montpellier



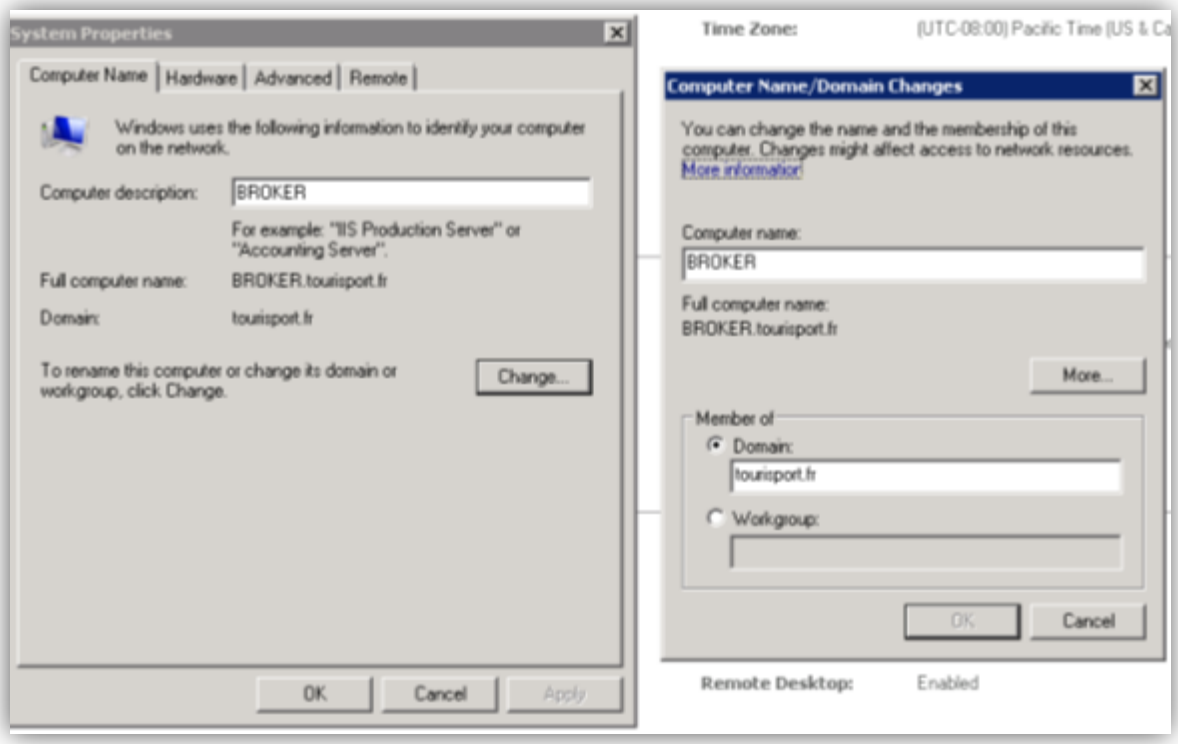
Régler les différents paramètres réseaux



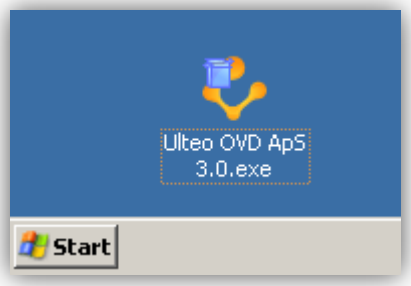
Nous pouvons dorénavant accéder à notre Serveur Windows avec l'agent de connexion à distance.

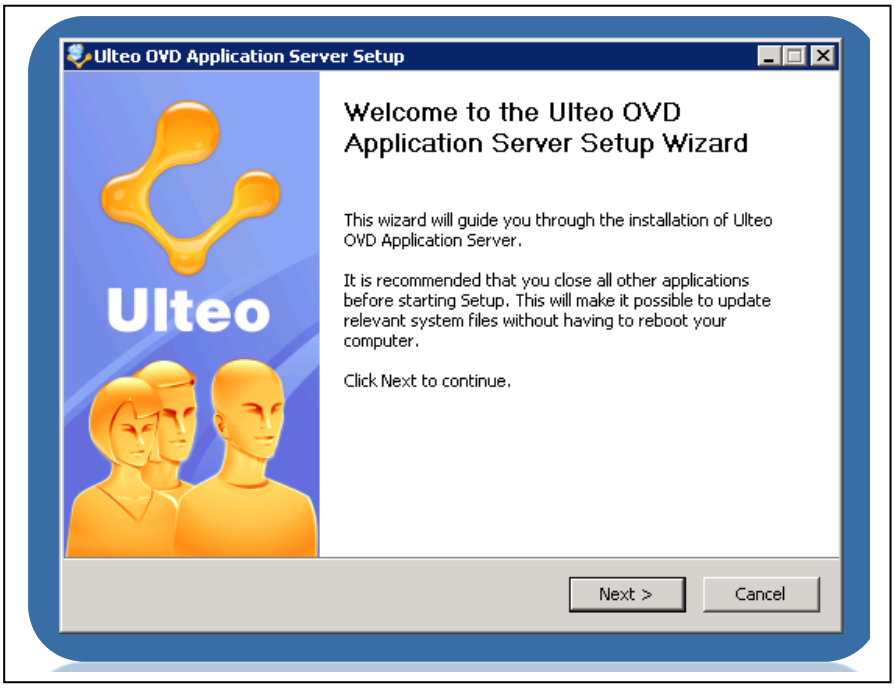


Nous devons maintenant donner un nom à notre serveur (BROKER) et l'intégrer au domaine tourisport.fr. Celui-ci devra ensuite être accepté manuellement sur le contrôleur de domaine.

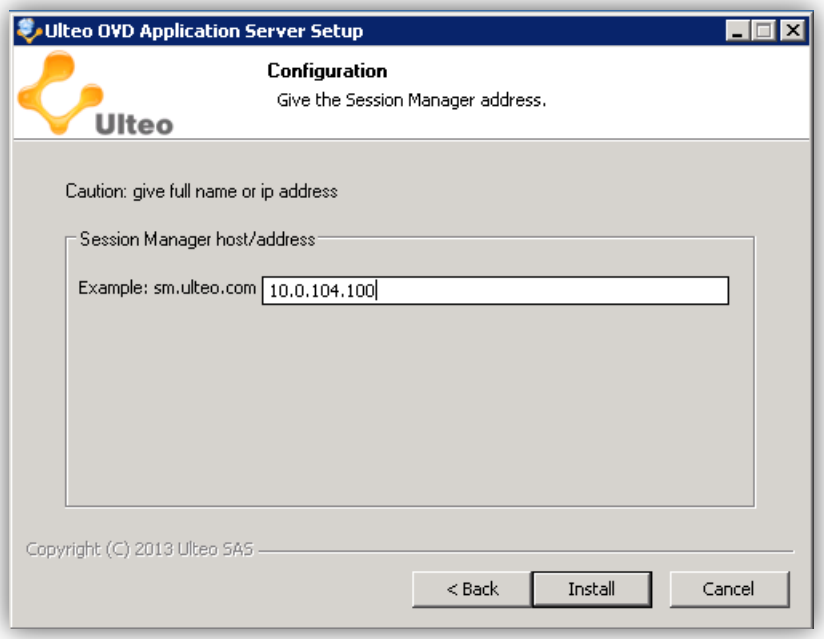


Copier et lancer le Setup d'installation du Serveur d'application Windows

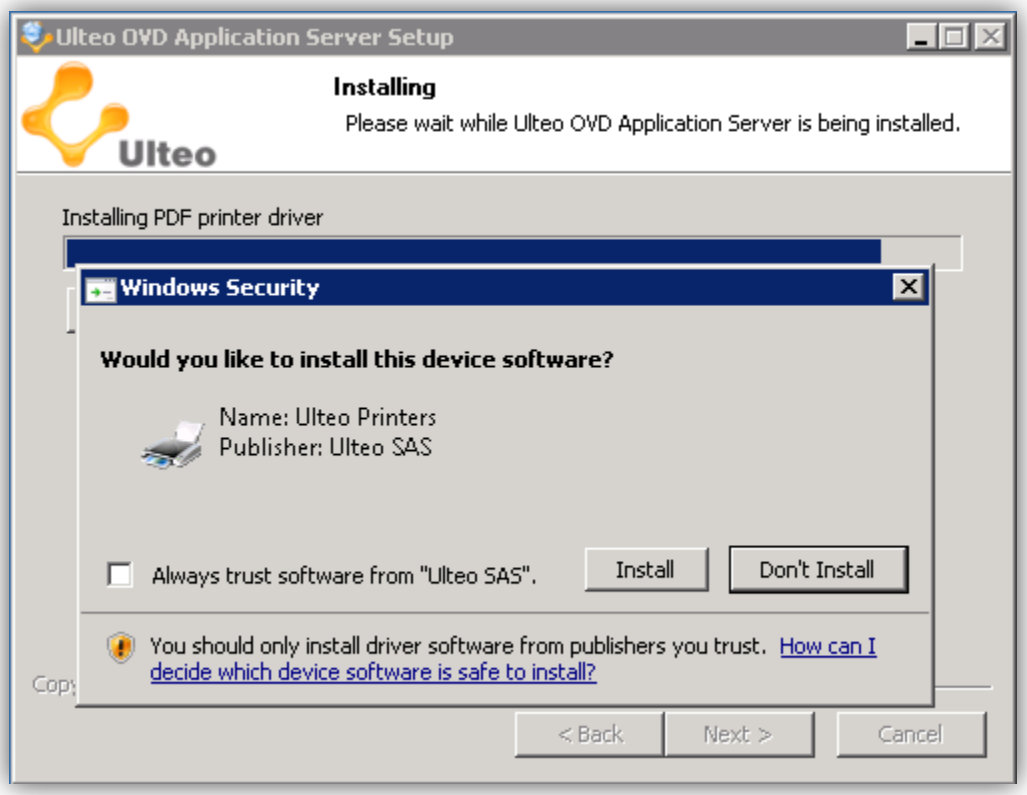




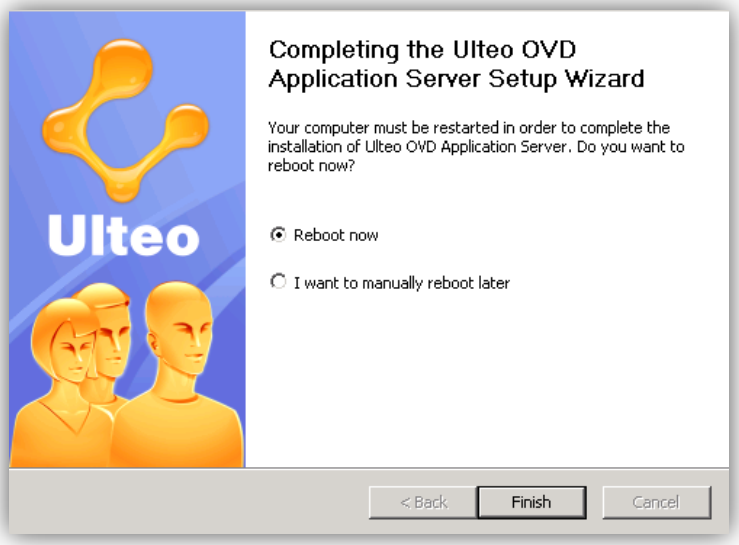
Il faudra déclarer l'adresse IP du Serveur Session Manager



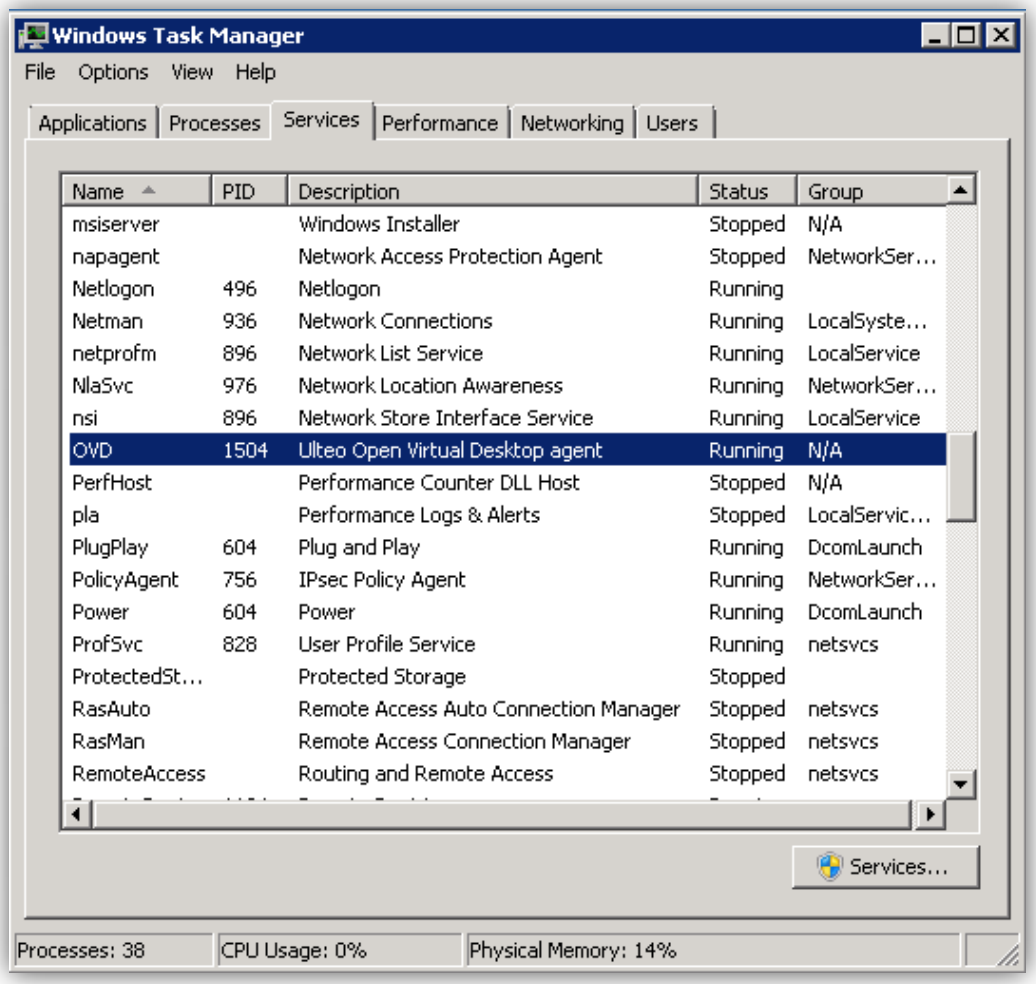
Un driver d'impression est également installé qui fera la jonction avec les imprimantes réseaux présentes.



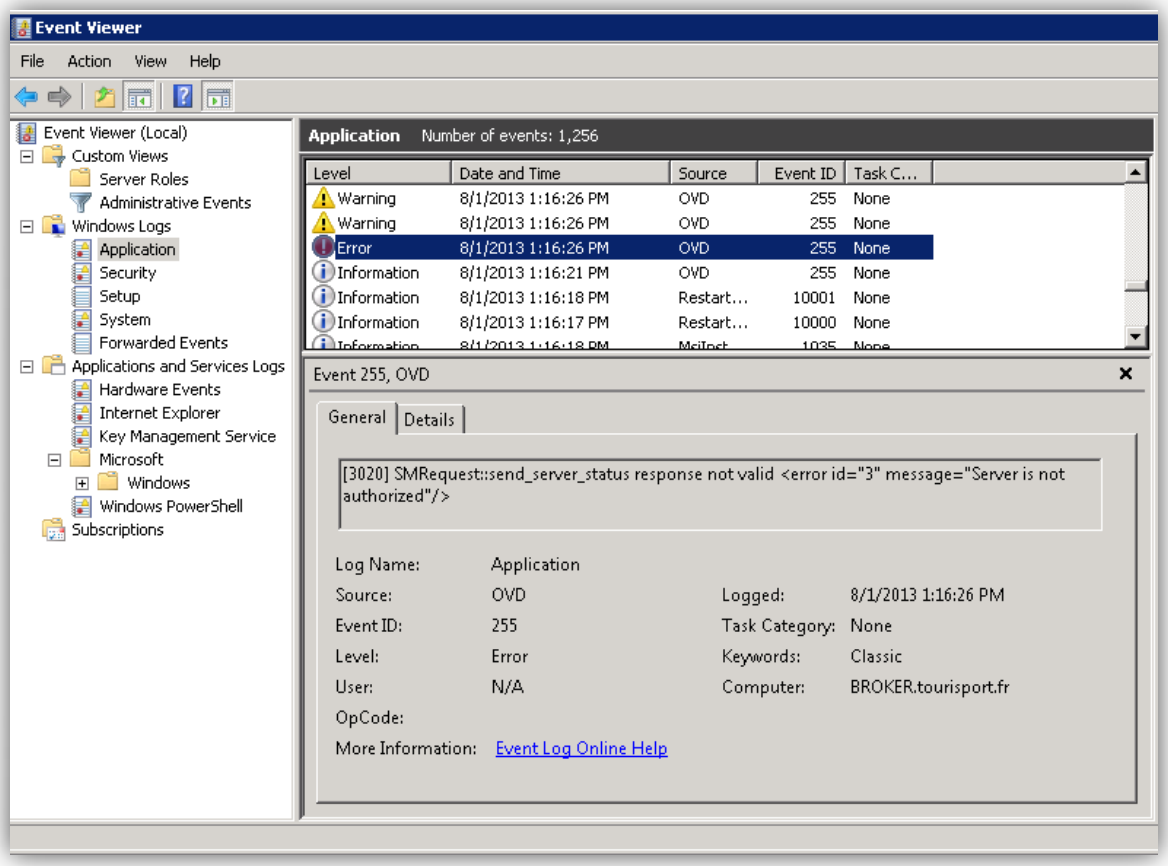
A la fin de l'installation, il faudra redémarrer le serveur



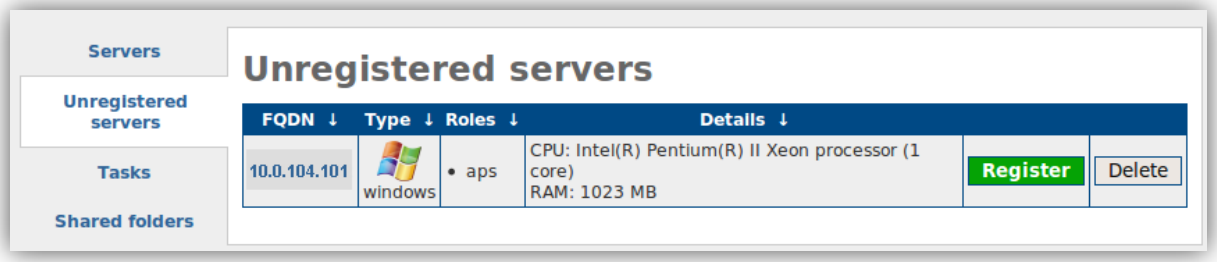
Après redémarrage, nous pourrons contrôler le fonctionnement du serveur d'application en vérifiant que le service OVD est bien apparent dans le gestionnaire de taches.



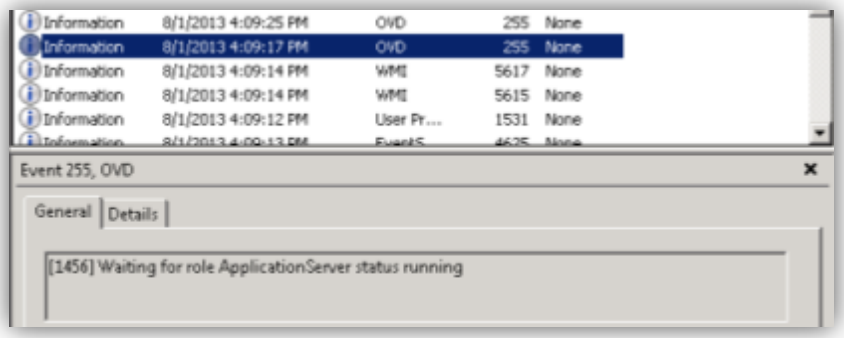
Un code erreur apparaitra dans le gestionnaire d'évènements de Windows Server 2008.

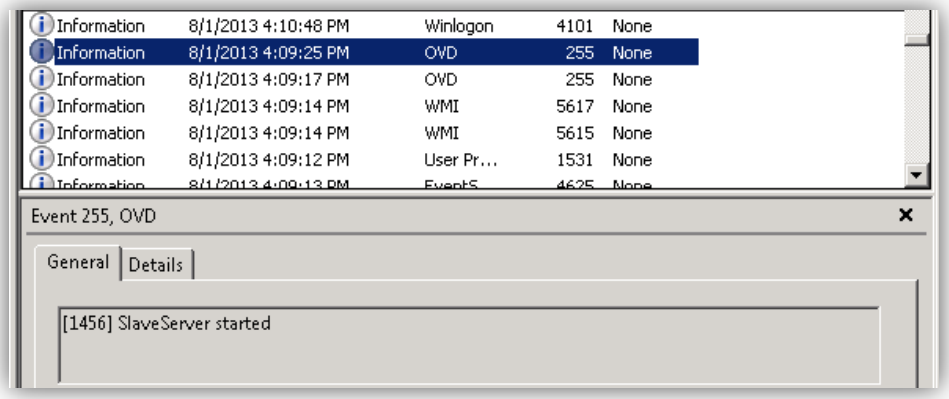


Ce code erreur est renvoyé car le Serveur d'application Windows n'est pas encore autorisé dans le Serveur Session manager.

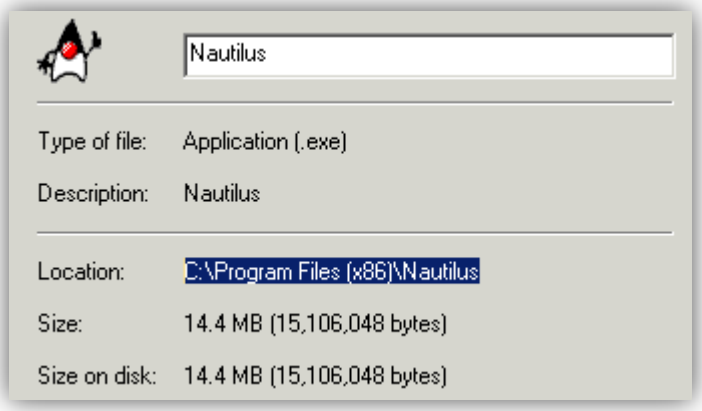


Un fois enregistré dans le Session Manager, le gestionnaire d'évènement devrait afficher les éléments suivants.



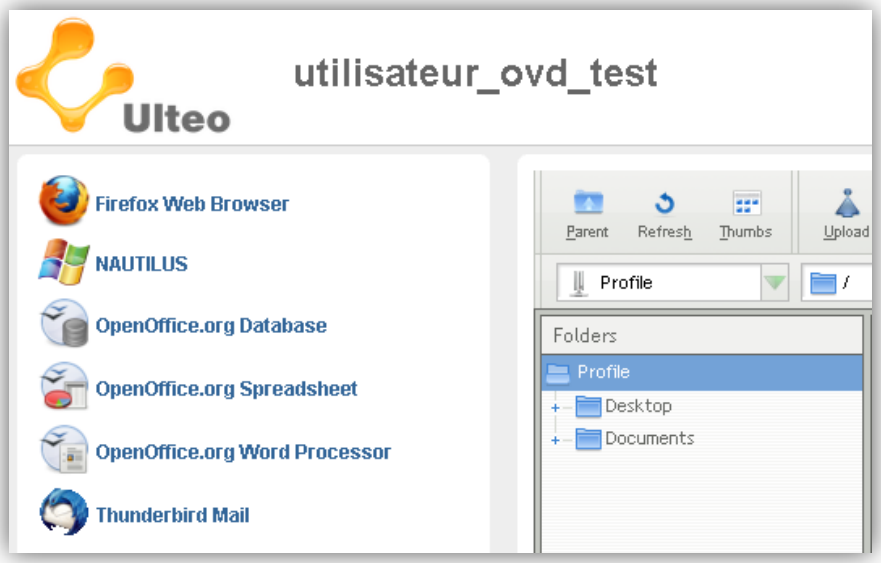


Sur notre serveur Windows nous installons maintenant notre logiciel métier, il s'agit juste d'un exécutable qui se connecte à divers serveurs de base de données.
Celui-ci sera installé dans **C:\Program Files (x86)\Nautilus**



Pour pouvoir le rendre accessible à nos utilisateurs il faudra l'intégrer dans le groupe d'applications que nous avons créé précédemment sur le Serveur Session Manager.

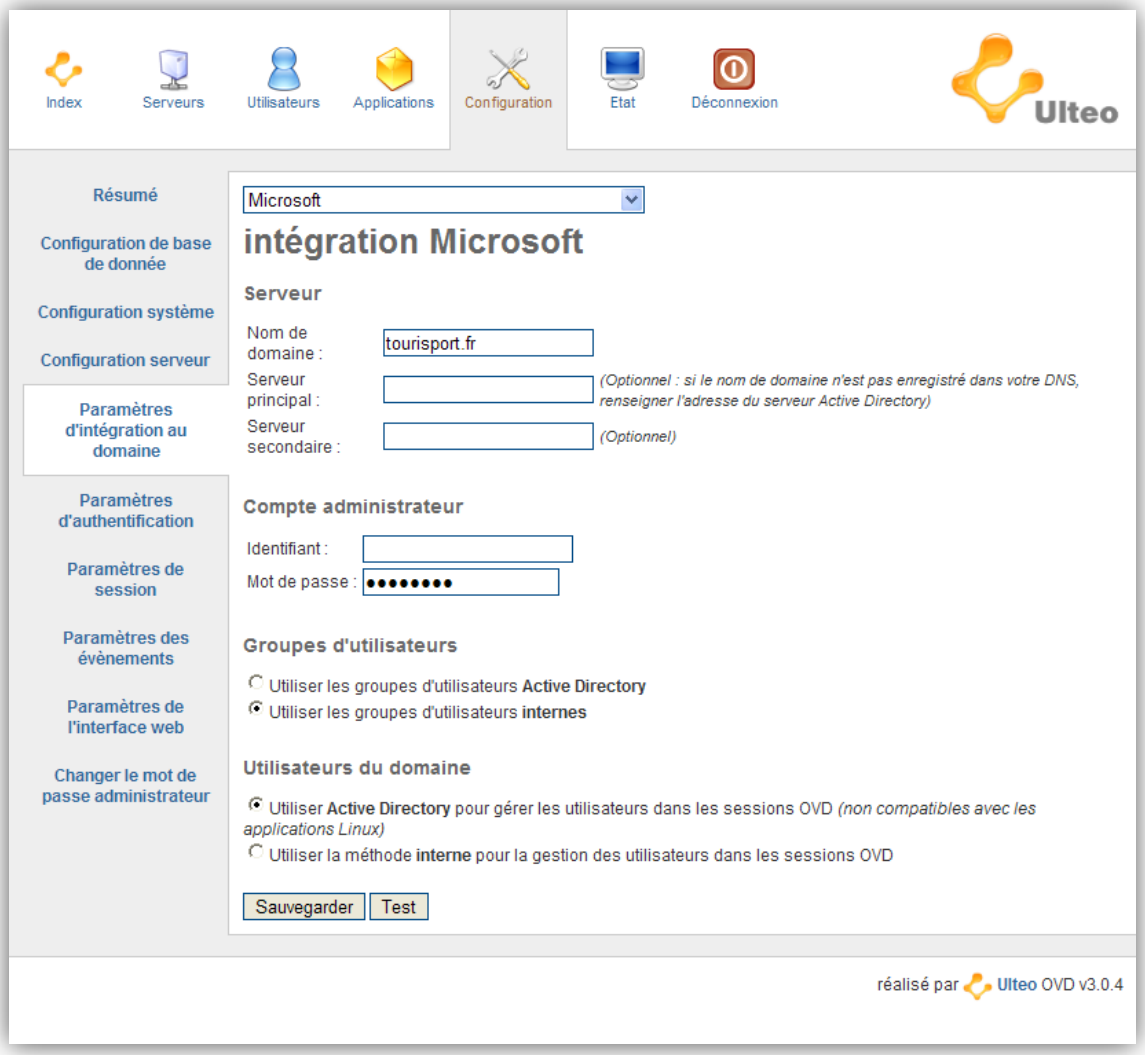
Le programme **Nautilus** apparait maintenant disponible pour notre utilisateur

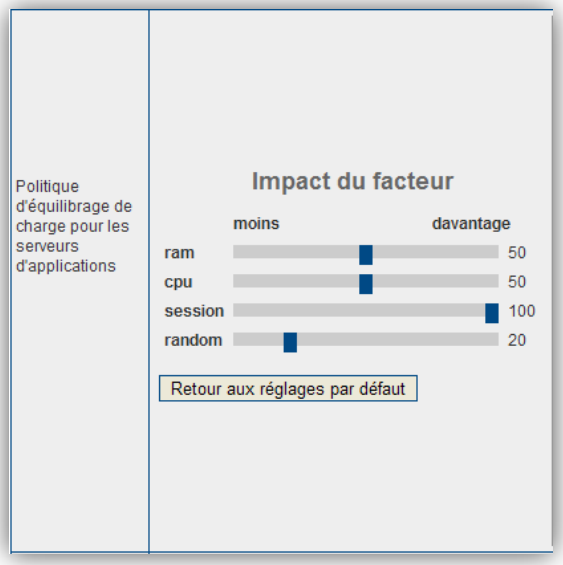


Configuration additionnelle du Serveur Session Manager

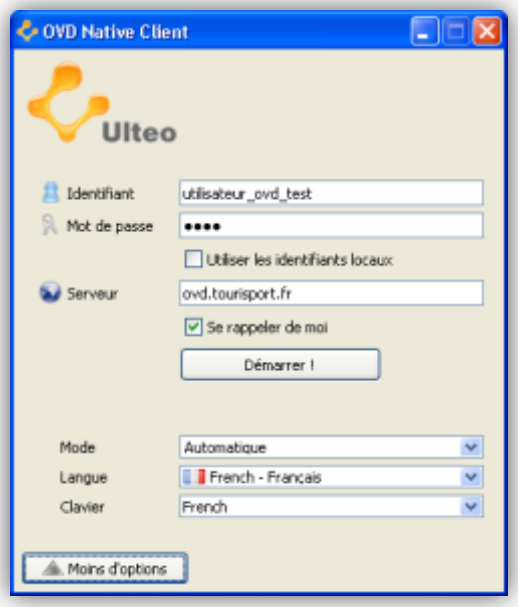
Le Serveur Session Manager peut être directement relié aux contrôleurs de domaines Windows pour l'authentification des utilisateurs.

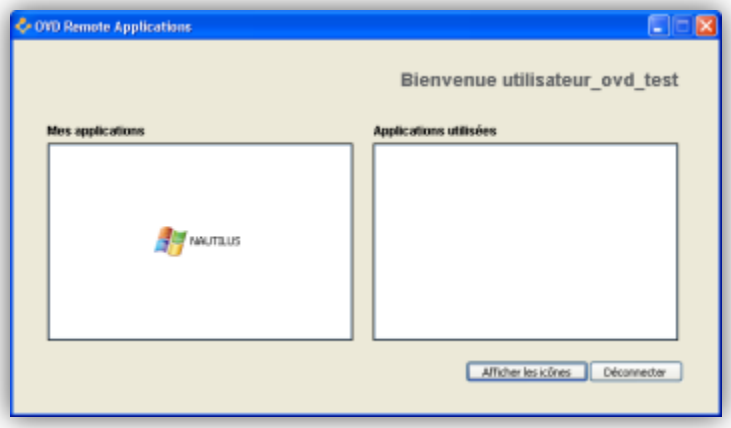
Il peut également effectuer de l'équilibrage de charge pour la distribution des sessions aux utilisateurs.


Index
Serveurs
Utilisateurs
Applications
Configuration
Etat
Déconnexion
Ulteo
Résumé
Configuration de base de donnée
Configuration système
Configuration serveur
Paramètres d'intégration au domaine
Paramètres d'authentification
Paramètres de session
Paramètres des évènements
Paramètres de l'interface web
Changer le mot de passe administrateur
Microsoft
intégration Microsoft
Serveur
Nom de domaine :
tourisport.fr
Serveur principal :
(Optionnel : si le nom de domaine n'est pas enregistré dans votre DNS, renseigner l'adresse du serveur Active Directory)
Serveur secondaire :
(Optionnel)
Compte administrateur
Identifiant :
Mot de passe :
Groupes d'utilisateurs
Utiliser les groupes d'utilisateurs Active Directory
Utiliser les groupes d'utilisateurs internes
Utilisateurs du domaine
Utiliser Active Directory pour gérer les utilisateurs dans les sessions OVD (non compatibles avec les applications Linux)
Utiliser la méthode interne pour la gestion des utilisateurs dans les sessions OVD
Sauvegarder
Test
réalisé par Ulteo OVD v3.0.4


Politique d'équilibrage de charge pour les serveurs d'applications
Impact du facteur
moins
davantage
ram 50
cpu 50
session 100
random 20
Retour aux réglages par défaut

La connexion des utilisateurs à leur session peut également être effectuée grâce à un « Client » installé sur le poste utilisateur.
Cette option est uniquement présente dans la version payante d'Ulteo et correspond à un module Gold que nous a permis de tester l'équipe d'Ulteo.





4.1.1.3 Conclusions de la solution Ulteo OVD 3.0.4

Cette solution est intéressante et fonctionne correctement pour la version Opensource. Le Native Client apporte un plus pour les utilisateurs se connectant directement à partir du réseau local.
Un autre avantage permettant d'augmenter la sécurité et de mieux gérer les flux est apparu au moment de tests. Le logiciel Nautilus ouvre certaines pages web qui permettent d'interagir avec des formulaires hébergés sur des sites web des agences, ainsi l'ouverture des pages web se fait via Ulteo à partir du serveur d'application (Windows 2008 R2) permettant d'encapsuler toutes les données dans la même connexion.

Les prix que nous a fournis l'équipe commerciale d'Ulteo sont les suivants :

Pour un projet de 160 utilisateurs, le prix est compose différemment que le programme quick start, voici les composants:

- Le coût de souscription annuel est de 45 euros par utilisateur.
- Le coût TechSupport annuel est de 20 euros. Ceci est un service qui assure un niveau 2 et 3, vous avez un Service Level Agreement(SLA) envers vos utilisateurs directement assuré par Ulteo. L'idéal est de prendre le Level 1 et si possible le L2, ce qui réduit le coût du support technique.
- Training(optionnel), deux jours de formation pour obtenir une certification. Nous demandons à ceux qui préfèrent faire leur niveau de support 1 et 2 d'avoir cette certification. Le coût est de 3000 euros et nous demandons un minimum de deux participants.
- Pré Production (optionnel, mais fortement recommande pour le premier projet), soit 2 à 4 jours d'aide en "remote" pour préparer et éventuellement mettre la solution en production.

ULTEO QUICK START PROGRAM OVERVIEW

PRICING*

25 users: € 2305

50 users: € 3430

100 users: € 5680

Summary

One year subscription plans for 25, 50 or 100 (max.) active users for the Ulteo OVD Premium Edition. Subscription provides one year eligibility for new software release updates and fixes.

Production support[1] and implementation offers requirements gathering to collect and define success criteria followed by remote deployment of OVD Premium Edition on your servers.

Two hours online administrator training.

Setup of remote monitoring to ensure agile and proactive support of your implementation.

*excluding VAT and any other third party licenses

WHAT IS ULTEO OPEN VIRTUAL DESKTOP?

Ulteo OVD is a delivery platform that provides on-demand access to private and public cloud hosted applications and virtual desktops enabling organizations to integrate and seamlessly deliver them as a secure service to users. Ulteo OVD supports SaaS, Windows Remote Desktop Services and Linux hosted applications and full desktop sessions to clients based on Windows, Linux, MacOS, Android and iOS platforms.

ULTEO OVD PREMIUM EDITION

OVD Premium Edition is a comprehensive application delivery and virtual desktop platform designed to deliver solutions for workforce mobility, BYO initiatives, virtual desktop projects and more. It comprises advanced features such as an SSL VPN and two factor authentication support for enhanced security, Microsoft SharePoint and Alfresco integration. It delivers seamless applications and desktop sessions from Windows and Linux servers to native Windows and Linux clients, HTML5 enabled browsers and mobile devices. A fully featured administrator web console provides for configuration of server settings, user management, application publishing and server monitoring along with server load balancing for optimum performance and scalability.

QUICK START PROGRAM

The Ulteo OVD Quick Start Program is a one-stop solution providing everything you need to get your application delivery project off the ground. The program features comprehensive packaged solutions of OVD Premium Edition subscriptions, support and education services to ensure success of your project.

GET STARTED TODAY

To find out more go to www.ulteo.com/quick-start

About Ulteo

Ulteo is a commercial open source company, combining the advantages of open source and the commercial enterprise allows us to efficiently and rapidly develop technology, delivering independent and open solutions. Ulteo was founded by veteran entrepreneurs Gaël Duval, CTO and Co-founder of MandrakeSoft / Mandriva and Thierry Koehrlen, CEO and Co-founder of intalio.com with the mission of enabling organizations to benefit from the open source ethos of a non-proprietary open platforms built on innovation, independence and an open architecture.

Terms and Conditions

This document is for informational purposes only. Ulteo makes no warranties, express or implied, in the document. Service engagements direct with Ulteo are governed by the Ulteo Professional Services General Terms and Conditions. Ulteo SAS. 5 rue Charles Léandre, F-14000 CAEN, France www.ulteo.com Copyright © 2013 Ulteo SAS. All rights reserved.

sales@ulteo.com | partners@ulteo.com | www.ulteo.com

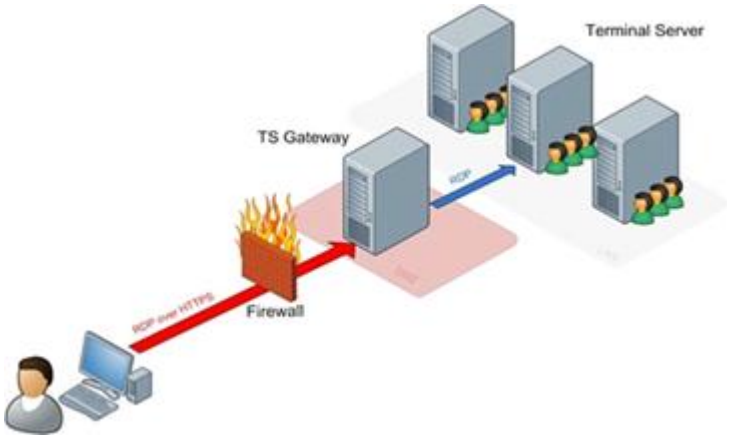
4.1.2 SOLUTION 2 : REMOTE-APP TERMINAL SERVER WINDOWS 2008 R2

Terminal Server

Description technique des environnements Terminal Server

Technologie d'accès distant via :

- RDP (port : 3389)
- RDP over HTTP SSL (port : 443) aussi appelé HTTPS



Bénéfices :

- Un moyen d'administrer des Serveurs à distance pour les IT PRO
- Une mise en place d'un serveur hébergeant des applications centralisées
- Un point d'accès à des bureaux ou applications pour des utilisateurs nomades

Application coté poste client requise pour se connecter à distance

- Remote desktop client (RDC)
- Version 6.0 (native depuis : Windows Vista et Windows Server 2008)

Pour les utilisateurs de Windows XP, la version 6 est intégrée au service pack 3(Une version redistribuable de RDC 6.0 est disponible si vos clients sont antérieurs à XP SP3).

Comment lancer un RDC en mode console :

- Commande : **mstsc /admin** (la version 6.0 n'emploi plus le « /console »).

Récapitulatif des évolutions technologiques

Description des composants de la nouvelle Infrastructure Terminal services

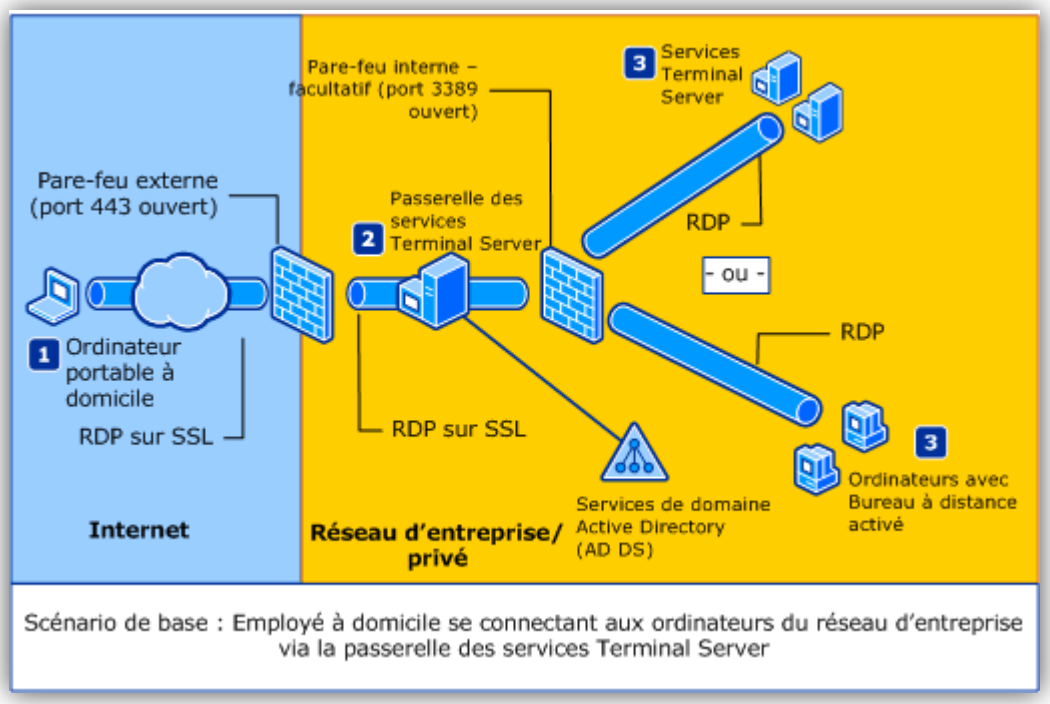
Windows Server 2008 R2

Les rôles Terminal Services :

- TS Server (Serveur hébergeant les sessions à distance et Applications)
- TS Gateway (Encapsule le protocole RDP dans un flux * numéro de port modifiable.
- TS Session Broker (BALANCEUR DE CHARGE/GESTIONNAIRE DE SESSION RDP)
- TS Remote APP (Permet de donner accès à des applications distantes au viaTSE)
- TS Licensing (Système de gestion des licences)

Les rôles Remote Desktop Services :

- Remote Desktop Session Host
- Remote Desktop Gateway
- Remote Desktop Connections Broker
- Remote App Manager
- Remote Desktop Licensing
  Nouveau scénario apporté par l'intégration de la virtualisation à Remote Desktop Service :
- Remote Desktop Virtualization Host (Permet d'étendre les environnements RDS vers les modèles Virtual Desktop Infrastructure)



Les étapes de mise en œuvre d'un environnement Terminal Server

Rôles du sous-composant Terminal Server : **Remote APP**

Cette fonctionnalité est disponible sur un serveur de Session Terminal Server, elle permet de mettre à disposition des utilisateurs un panel d'applications.

Ces applications pourront par la suite, être redistribuées sous forme de fichiers .RDP, ou publiées à travers un serveur : TS Web Access.

Il y a une consigne à prendre en compte, si vous redistribuez votre application sur un serveur TSE autonome ou membres d'une batterie de serveurs TSE. Il va falloir installer et autoriser l'application sur chaque Serveurs TSE auxquels vos utilisateurs pourront se connecter.

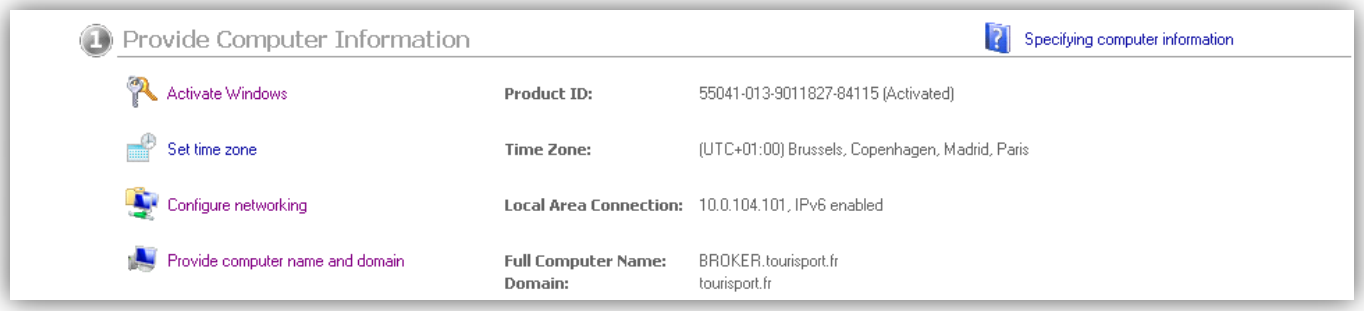
Dans le cas contraire vous aurez un message d'erreur vous indiquant que l'application n'est pas disponible sur le serveur de session auxquels vous tentez d'accéder.

Le mode d'installation d'une application sur un serveur de Session Terminal Server est particulier.
En effet il faut indiquer au serveur de Session Terminal Server qu'il va exécuter une application partagée par plusieurs utilisateurs en même temps.

4.1.2.1 INSTALLATION ET CONFIGURATION TERMINAL SERVEUR – APPREMOTE SUR WINDOWS Server 2008 R2

Terminal Server (TSE) est un composant de Microsoft Windows qui permet à un utilisateur d'accéder à des applications et des données sur un ordinateur distant. Nous allons voir comment mettre en œuvre cette solution.

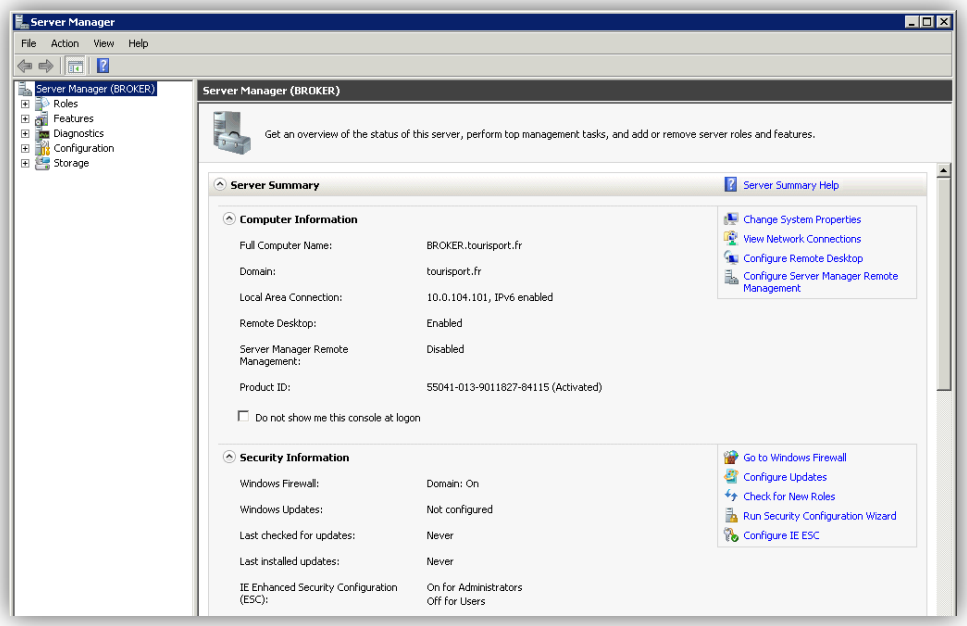
Prérequis : Microsoft Windows 2008 R2 Installé, mis à jour et rejoint au domaine.



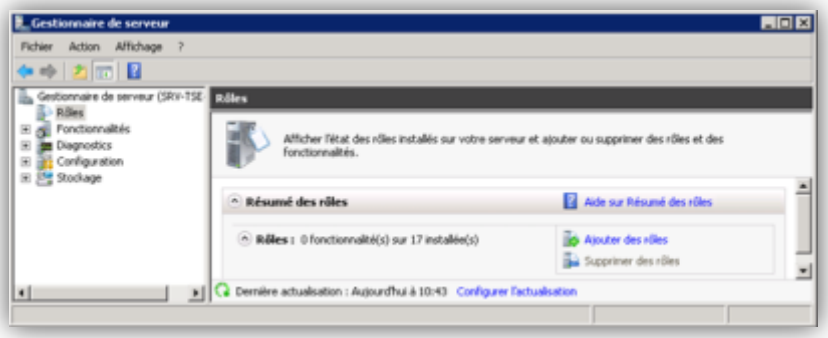
4.1.2.1.1 Installation des services TSE

Ouvrir le Gestionnaire de serveur.
Démarrer > Outils d'Administration > Gestionnaire de serveur

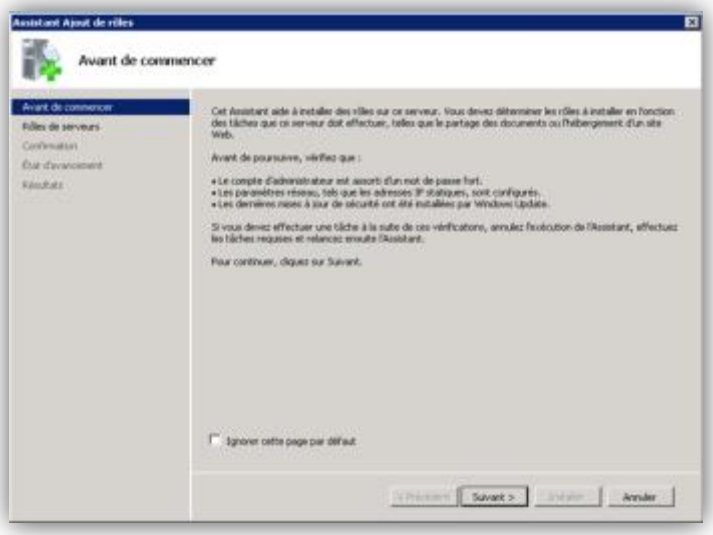
La fenêtre suivante s'ouvre



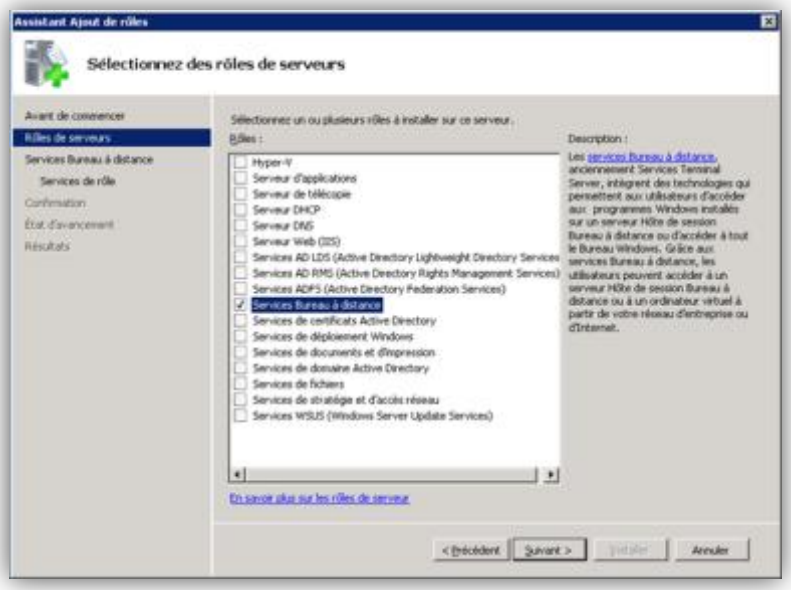
Cliquer sur Rôles puis Ajouter des rôles



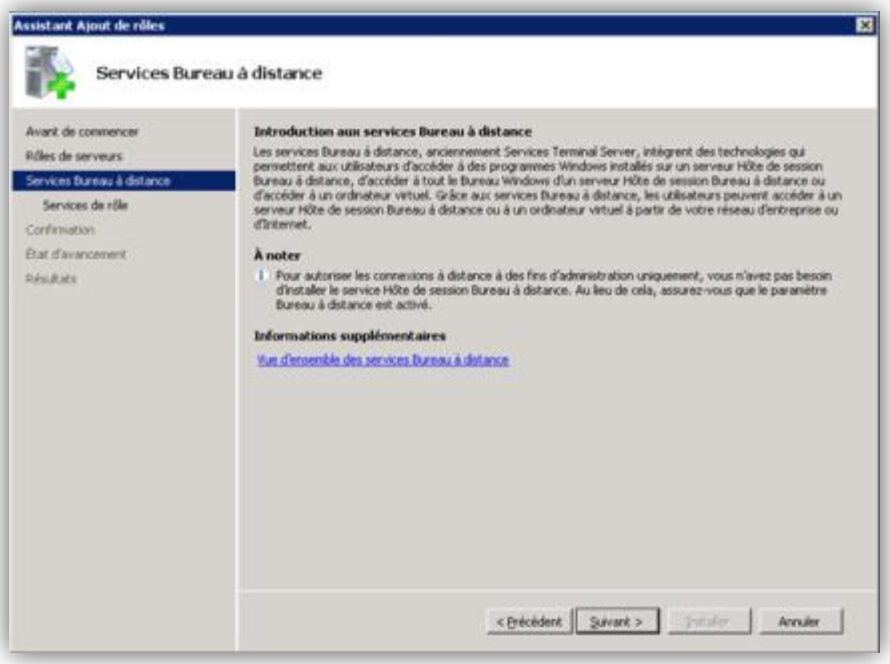
Cliquer sur Suivant



Cocher Services Bureau à distance puis cliquer sur Suivant

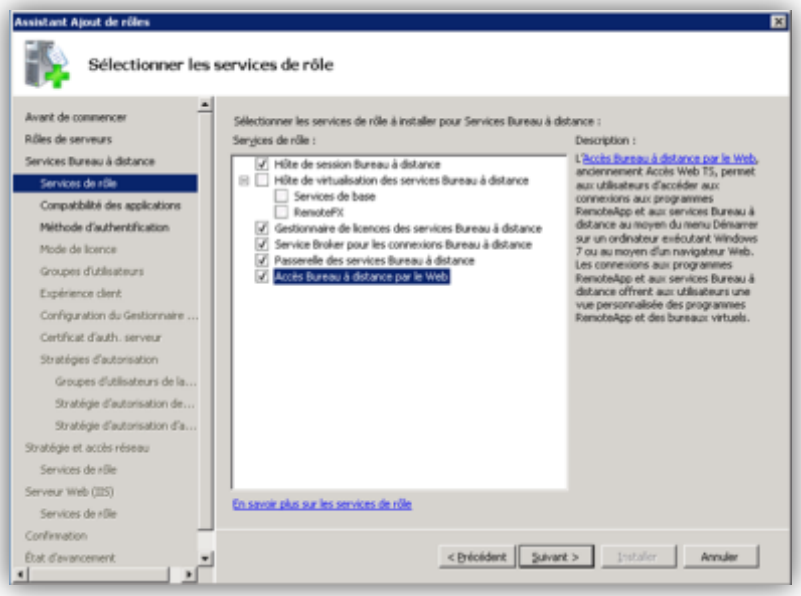


Cliquer sur Suivant

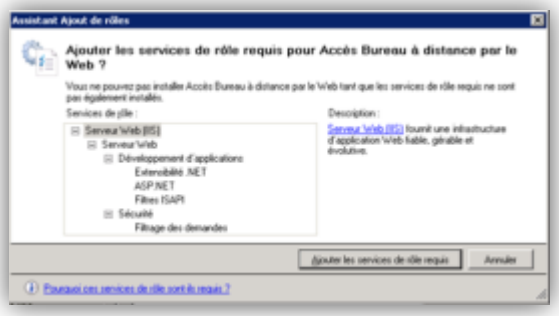


Cocher les lignes suivantes puis cliquer sur Suivant

- **Hôte de session Bureau à distance :** Serveur hôte de session Bureau à distance qui héberge les programmes Windows
- **Gestionnaire de licence des services Bureau à distance** : Gère les licences TSE que vous avez acquis
- ***Service Broker pour les connexions Bureau à distance*** : Équilibrage de charge et accès aux RemoteApp
- ***Passerelle des services Bureau à distance*** **:** Permet aux utilisateurs de se connecter depuis Internet
- ***Accès Bureau à distance par le Web :*** Permet aux utilisateurs d'accéder aux RemoteApp et aux services Bureau à distance depuis un navigateur web

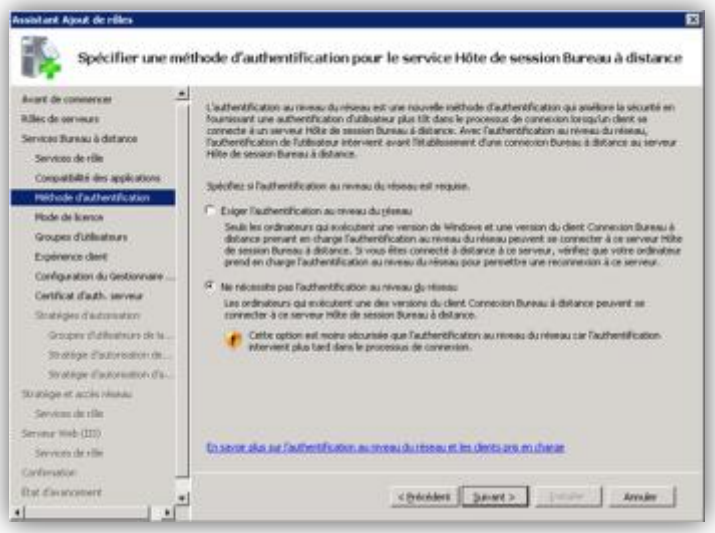


En cliquant sur Passerelle des services Bureau à distance et Accès Bureau à distance par le Web la fenêtre suivante s'ouvre, cliquer sur Ajouter les services de rôle requis

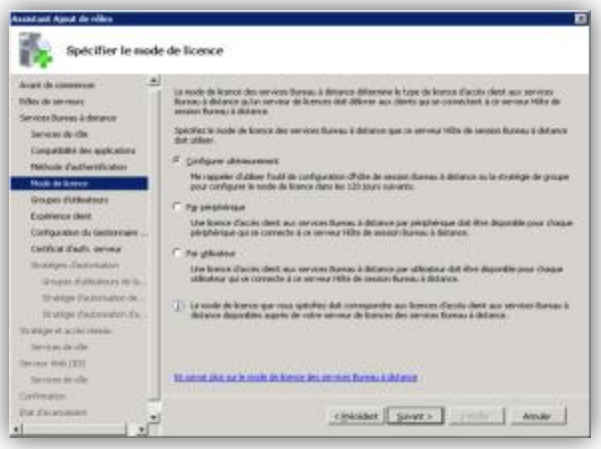


Cliquer sur Suivant

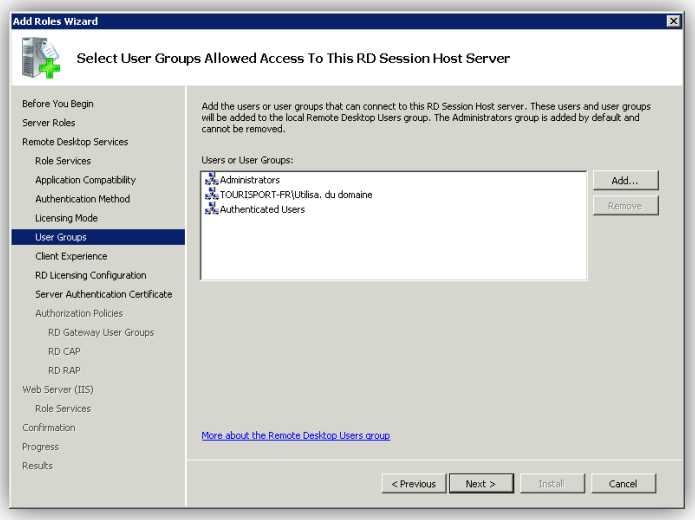
Choisir la méthode d'authentification, dans notre cas, Ne nécessite pas l'authentification au niveau du bureau. Cela permettra aux anciennes versions de se connecter au serveur.



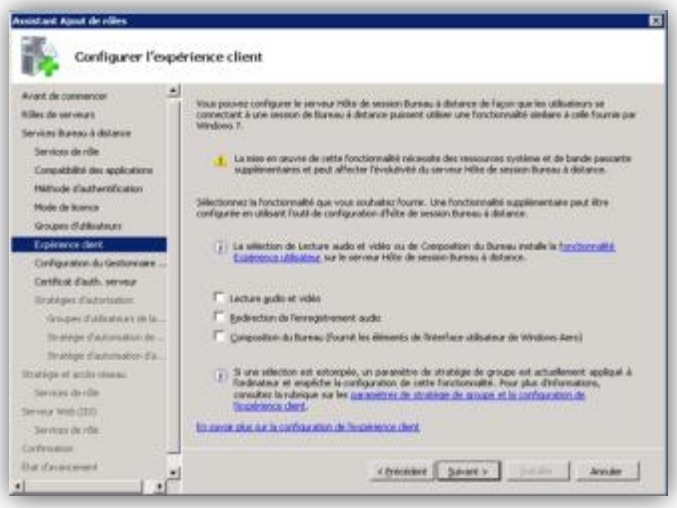
Choisir le mode de licence, dans mon cas je suis sur un serveur de test donc je choisis de le configurer ultérieurement (Période d'essai de 120j), sinon choisir le mode de licence en fonction de ce que vous avez acheté et actif.



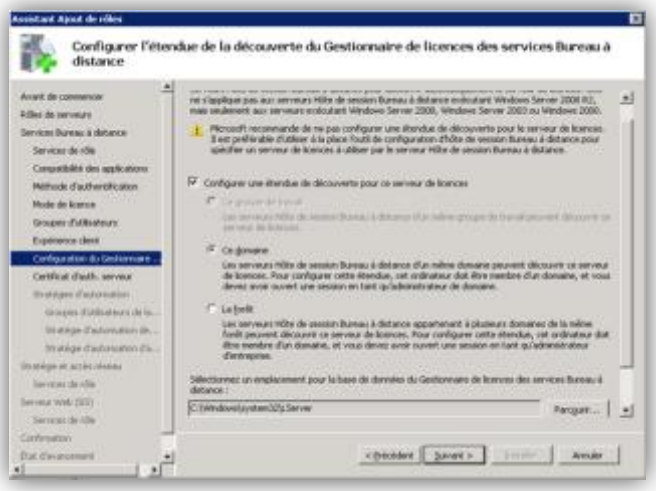
Choisir les groupes d'utilisateurs autorisés à accéder aux services TSE puis cliquer sur Suivant

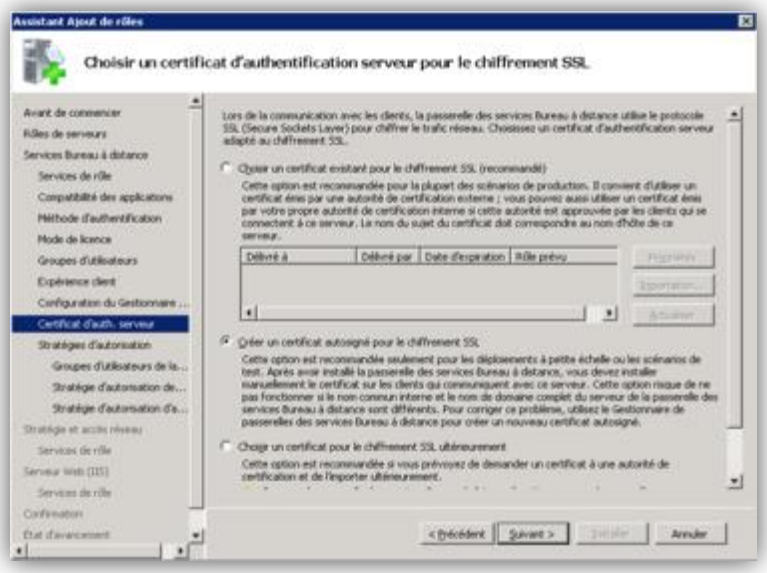


Afin de ne pas consommer trop de bande passante, dans mon cas je ne coche rien. Cliquez sur Suivant



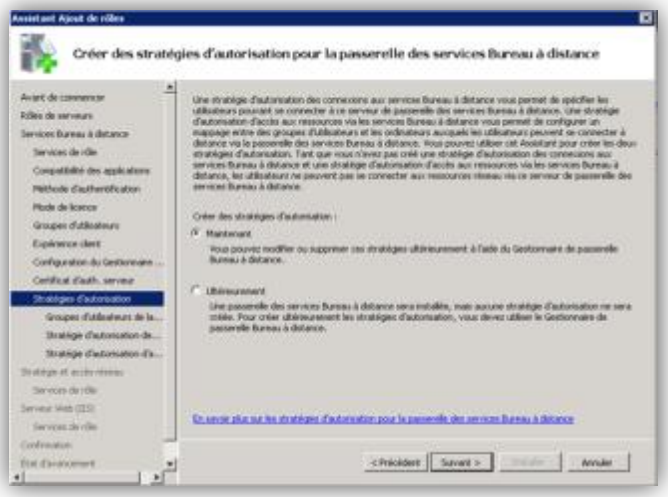
Définir l'étendue de découverte, dans mon cas, ce domaine, puis cliquer sur Suivant



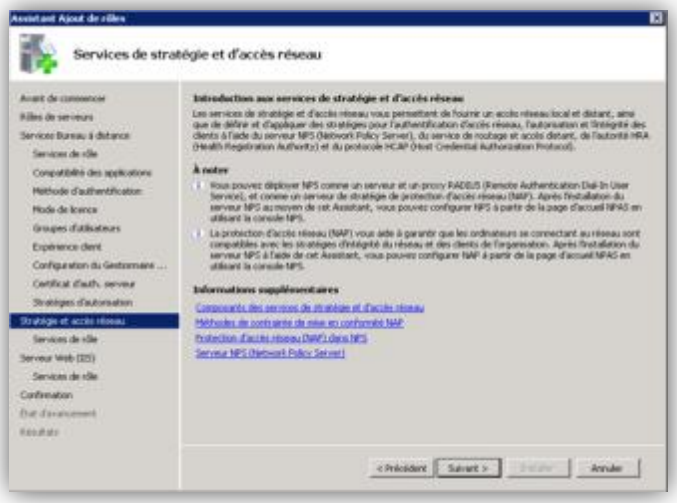


Dans mon cas, sur mon serveur, un serveur de test, je n'ai pas installé l'autorité de certification, dans un environnement de production, il serait préférable de passer par une autorité de certification.
Cocher créer un certificat auto-signé pour le chiffrement SSL puis cliquer sur Suivant

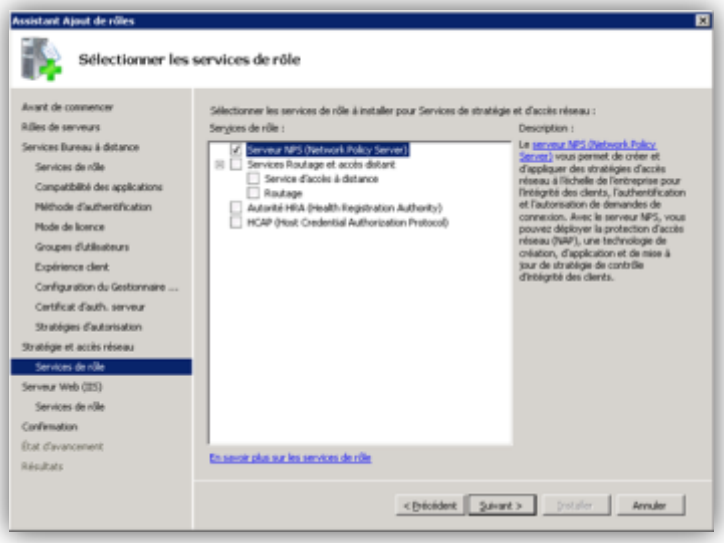
Créer une stratégie d'autorisation ultérieurement puis cliquer sur Suivant



Cliquer sur Suivant

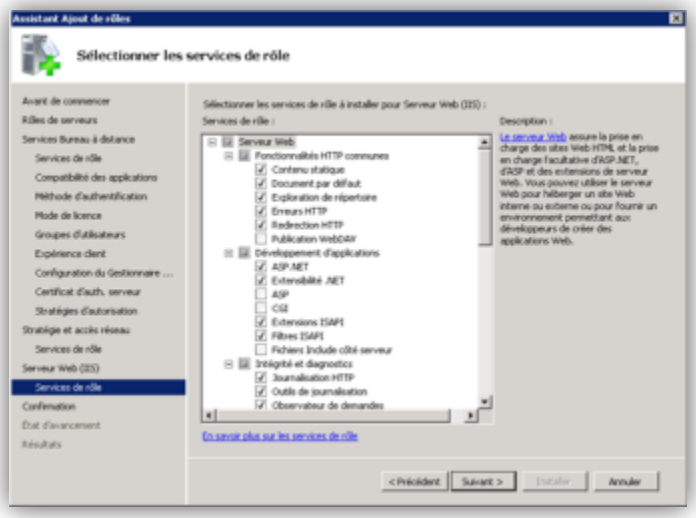


Cliquer sur Suivant

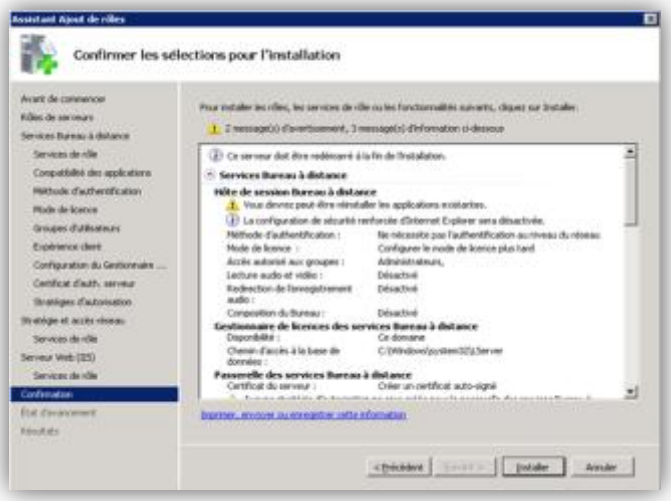


Cliquer sur Suivant

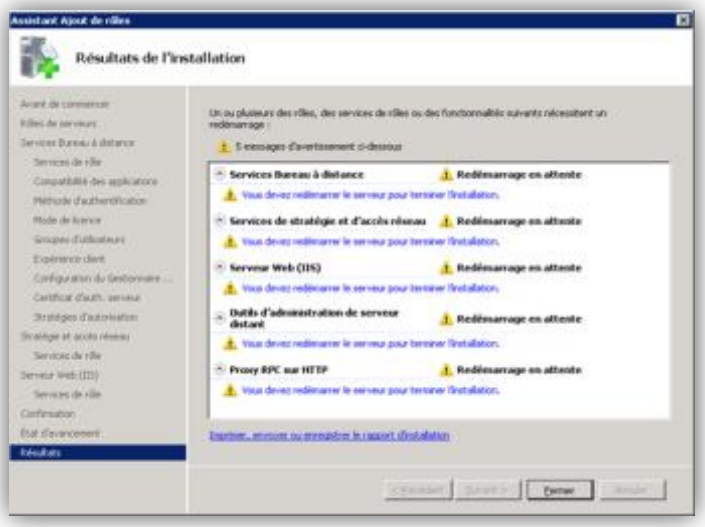
Cliquer sur Suivant



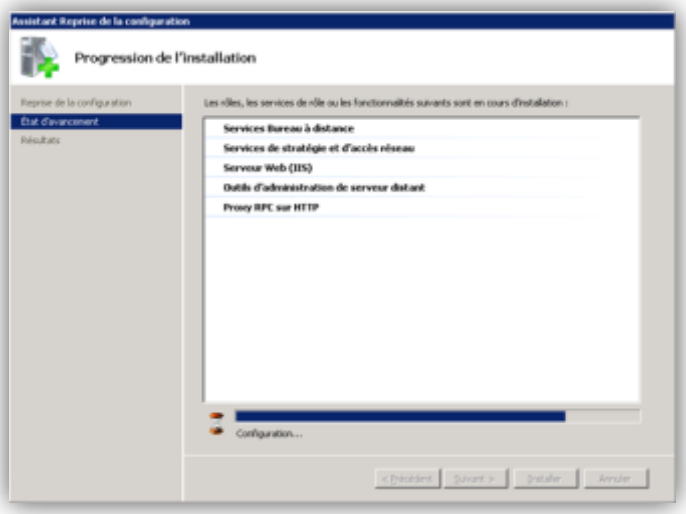
Cliquer sur Installer



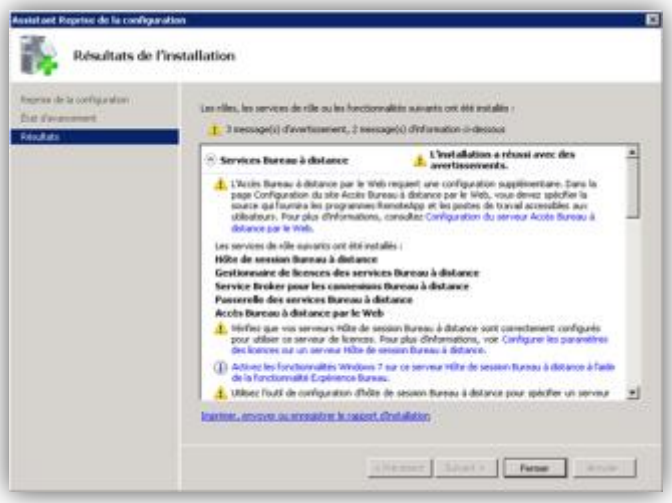
Cliquer sur Fermer pour redémarrer le serveur



Après avoir redémarré, l'installation continue



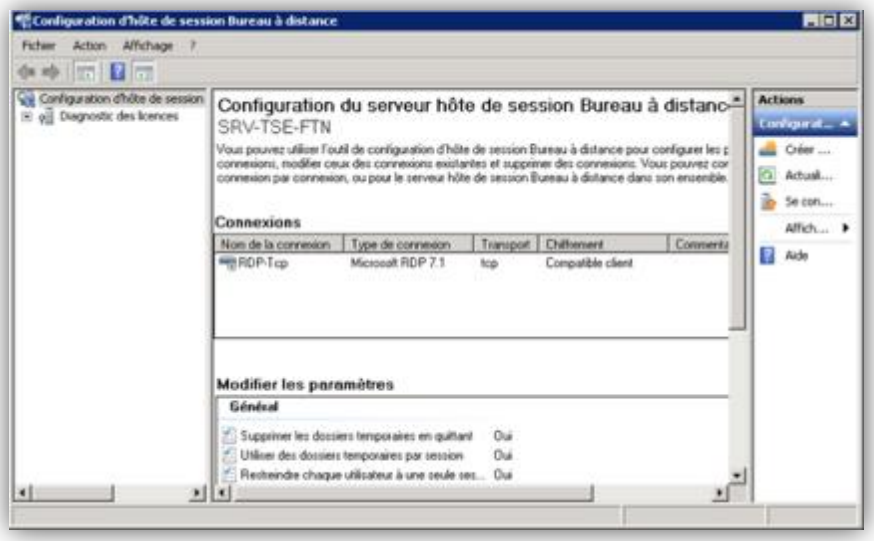
Cliquer sur Fermer pour terminer l'installation



Redémarrer le serveur. Le rôle TSE est maintenant installé.

4.1.2.1.2 Configuration de TSE

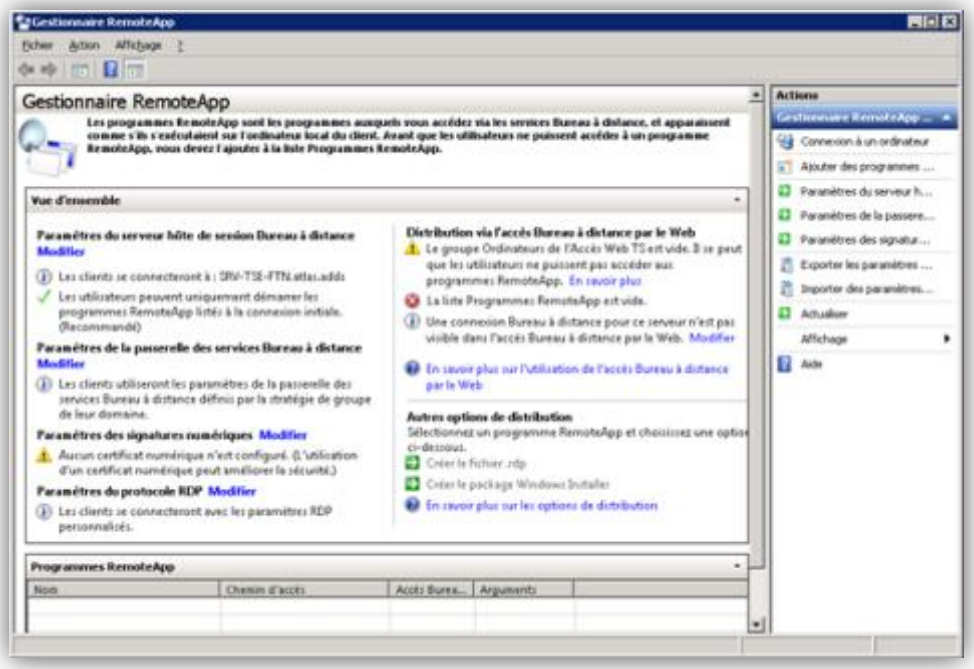
Cliquer sur Démarrer > Outils d'administration > Services Bureau à distance > Configuration d'hôte de session Bureau à distance
Faire un clic droit sur RDP-Tcp > Propriétés



Afin d'éviter l'utilisation inutile de licences, modifier les paramètres suivants. Cliquer sur Sessions puis Cocher Remplacer les paramètres de l'utilisateur, choisir les paramètres souhaité. Coché, Remplacer les paramètres de l'utilisateur puis choisir ce que vous souhaitez.

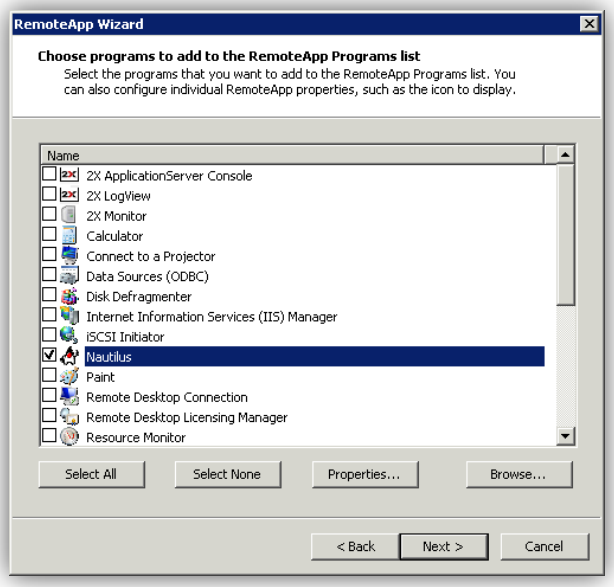
4.1.2.1.3 Configuration Remote App

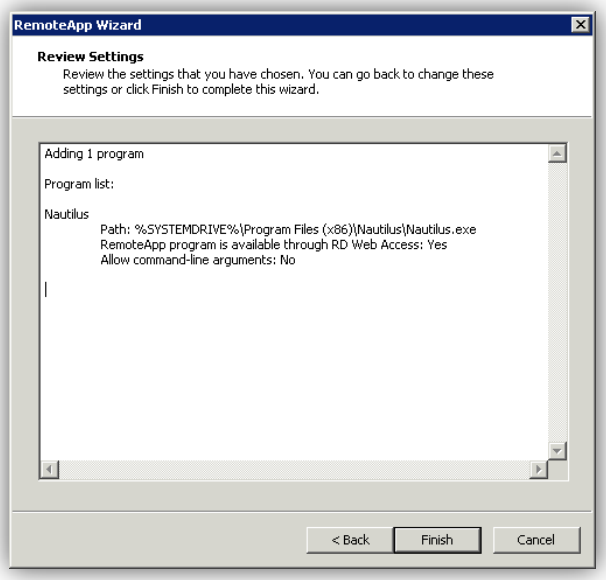
Les programmes **RemoteApp** sont des programmes auxquels vous pouvez accéder à distance par le biais des services Terminal Server et qui apparaissent comme s'ils étaient exécutés sur l'ordinateur local de l'utilisateur final. Les utilisateurs peuvent exécuter côte à côte des programmes **RemoteApp** et leurs programmes locaux.
La configuration minimale doit être Windows XP SP2 sur lesquels le nouveau client Connexion bureau à distance a été installé.
Dans ce cas, je vais configurer la calculette en **RemoteApp**.
Cliquer sur Démarrer > Outils d'Administration > Services Bureau à distance > Gestionnaire **RemoteApp**
La fenêtre suivante s'ouvre. Cliquer sur Ajouter des programmes.



Cliquer sur Suivant

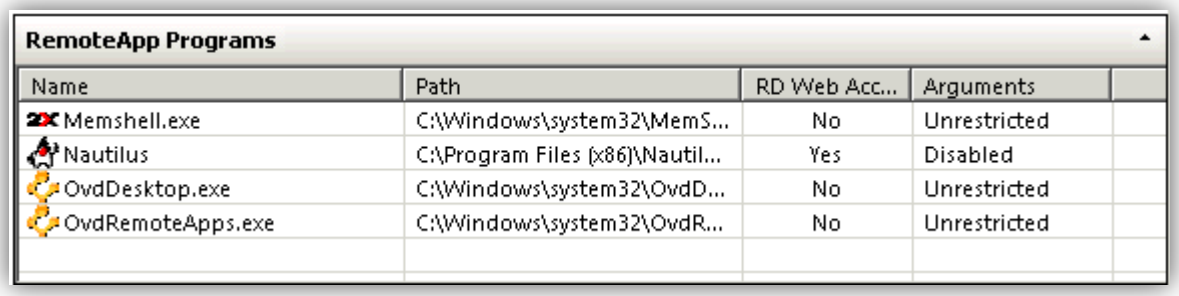
Cocher le programme que vous souhaitez, dans mon cas, Nautilus. Puis cliquer sur Suivant



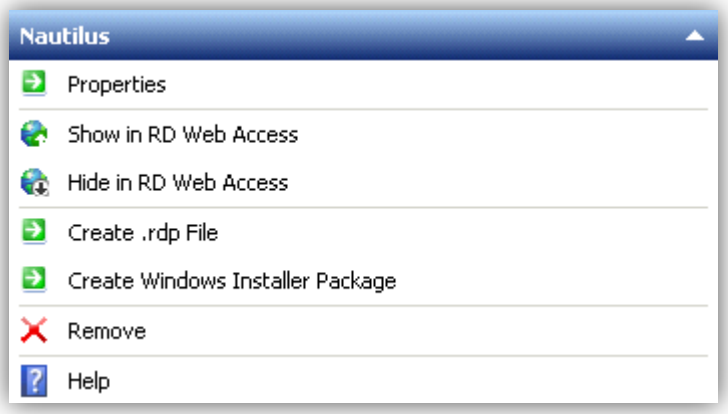


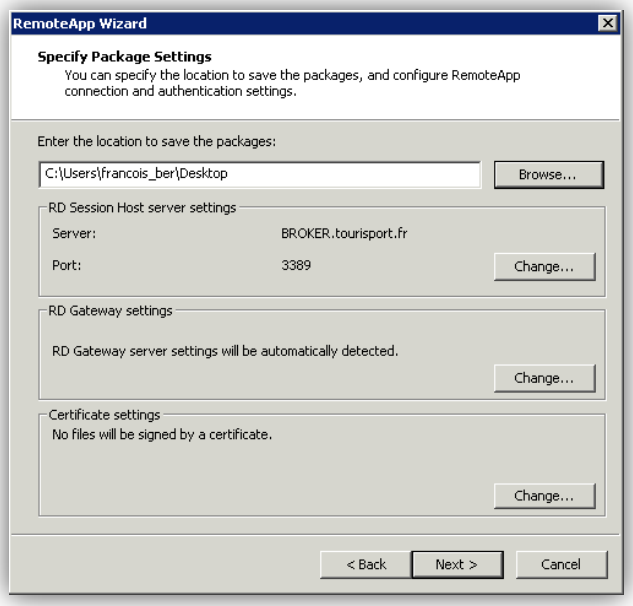
Cliquer sur Terminer

On peut maintenant voir le programme Nautilus apparaitre dans la liste des programmes RemoteApp.



Cliquer ensuite sur Nautilus, puis dans le menu à droite, Créer le fichier **.rdp**





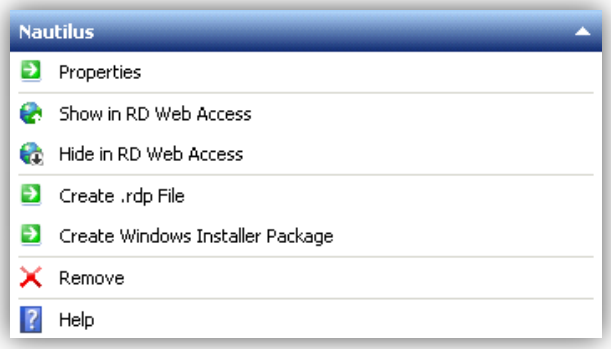
Cliquer sur Suivant. Le fichier **.rdp** sera créé sur le bureau

Cliquer sur Terminer

Le fichier **.rdp** est créé. Il suffit simplement de le mettre sur un poste client, pour que celui-ci ait accès au logiciel Nautilus en Remote.

Il est aussi possible de créer un fichier **.msi** afin par exemple de le déployer via GPO.

Cliquer sur Créer le package Windows

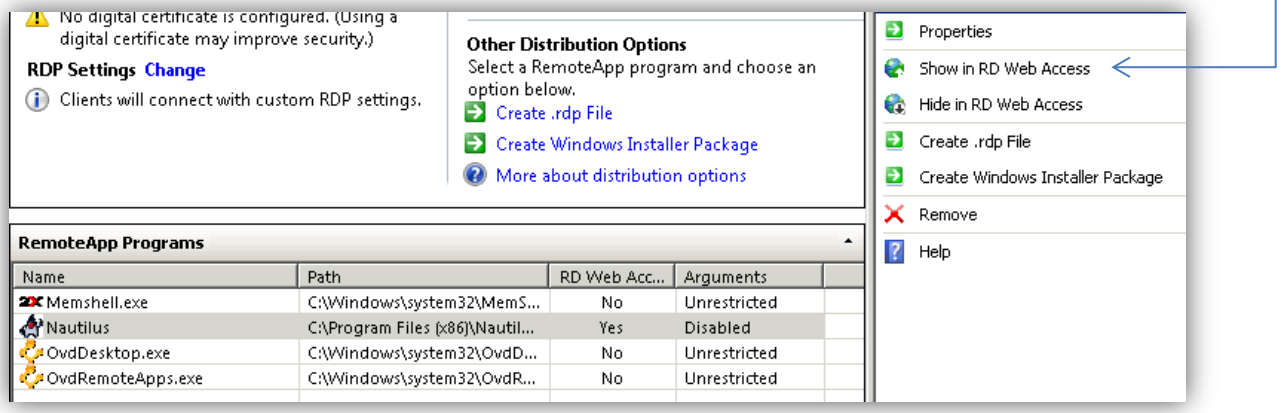


Avec les mêmes paramètres que précédemment un fichier exécutable sera créé sur le bureau

Cliquer sur Suivant. Le fichier **.msi** sera créé sur le bureau

Le programme d'installation placera le raccourci dans le menu → Démarrer → Remote Programme→ Nautilus

Pour pouvoir utiliser le logiciel via une interface web, sélectionner l'application puis cliquer sur « Afficher dans l'accès Bureau à distance par le web »

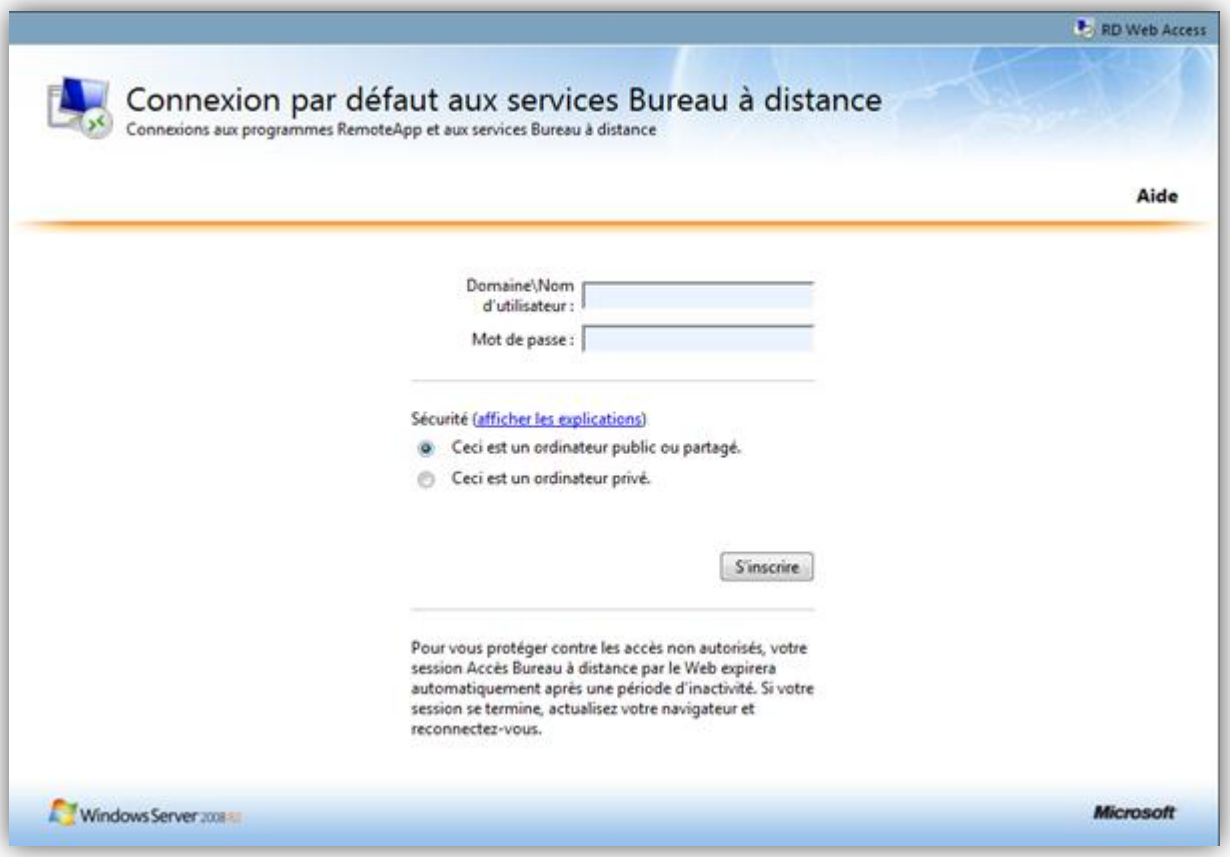


4.1.2.1.4 Les modes de connexions aux logiciels

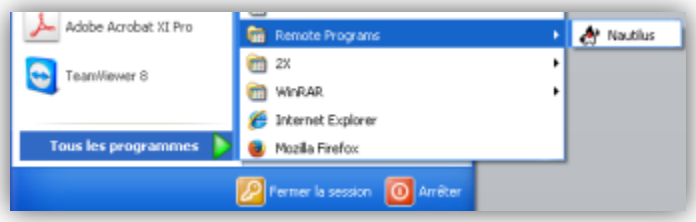
Dans un navigateur internet (De préférence Internet Explorer) saisir l'adresse suivante

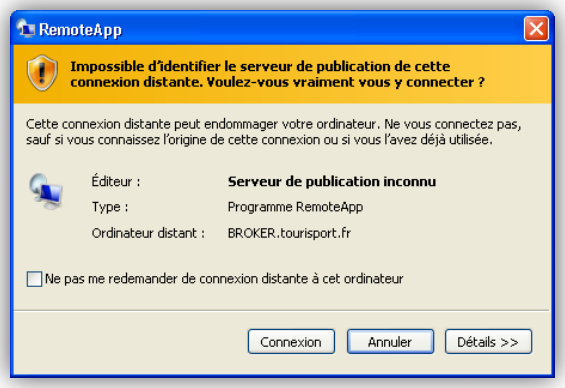
https://**NomDeVotreServeur**/RDWeb/

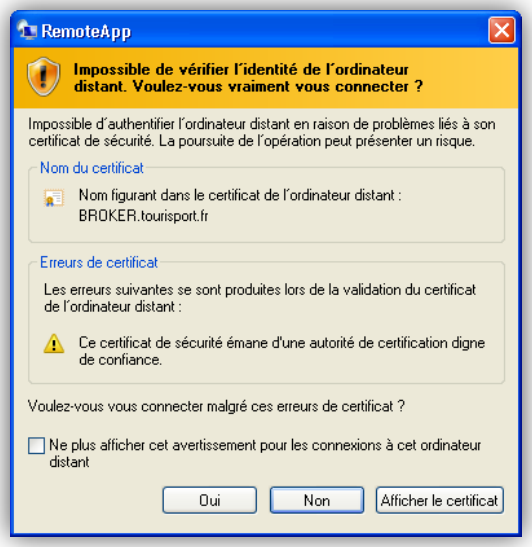
La fenêtre suivante s'ouvre, saisir un nom d'utilisateur et un mot de passe autorisé à se connecter aux services Bureau à distance, puis cliquer sur s'inscrire.



Accès via le menu démarrer en RDP







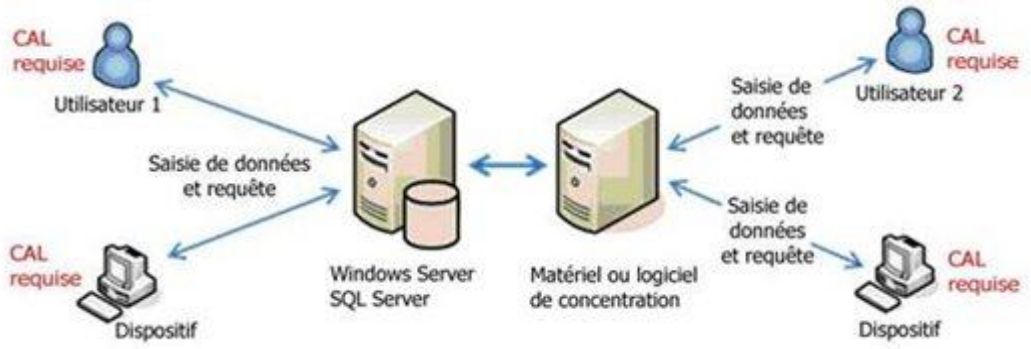
4.1.2.1.5 A propos des serveurs de licences Windows

Il existe deux types de licences d'accès pour Windows server 2008. Il y a souvent confusion entre licences d'accès au serveur, et licences d'accès à distance (RDS).

Les licences d'accès au serveur (CAL Users):

Il s'agit de licences permettant aux utilisateurs d'accéder aux ressources du serveur.

Les CALs User sont obligatoire, dès qu'il y a "authentification" d'un poste (device) ou d'un utilisateur (user) pour accéder aux services de base de Windows Server: Active Directory, partage de fichiers et/ou d'imprimante etc. (voir exemple en image ci-dessous)



En général, les versions OEM de Windows server proposent au minimum 5 licences utilisateurs (5 CAL User)

Les licences d'accès Bureau à distance (CAL RDS):

Il s'agit de licences permettant aux utilisateurs d'ouvrir une session de bureau à distance (avec la commande Mstsc) au serveur RDP (Remote Desktop Protocol).

Par défaut, aucune version de Windows server ne contient de CAL RDS.

Pour laisser tout le temps nécessaire au déploiement d'un serveur de licences, les Services Bureau à distance fournissent une période de grâce des licences pour le Serveur de session Bureau à distance au cours de laquelle aucun serveur de licences n'est requis. Au cours de cette période, un Serveur de session Bureau à distance peut accepter des connexions de clients non licenciés sans avoir à contacter un serveur de licences. La période de grâce débute la première fois que le Serveur hôte de session Bureau à distance accepte une connexion cliente. Elle prend fin dès lors que l'un des événements suivants se produit :

- **Une licence d'accès client aux services Bureau à distance permanente est émise par un serveur de licences sur un client qui se connecte au Serveur hôte de session Bureau à distance.**
- **Le nombre de jours de la période de grâce est dépassé. (120 jours), après ceci l'achat de licence RDS est obligatoire ainsi que l'installation d'un serveur RDL.**

4.1.2.1.6 Installation et configuration du serveur de licences des services Bureau à distance

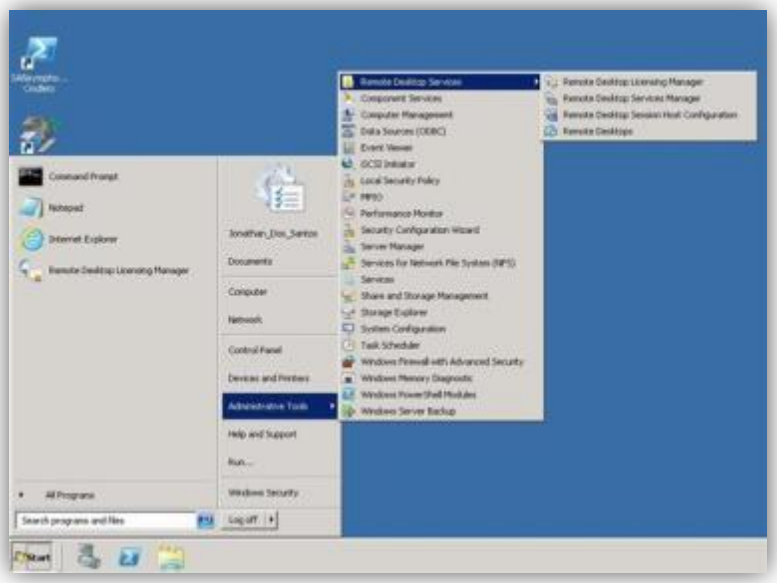
Mise en place d'un serveur de licences pour les services Bureau à Distance (RDL).

I- Installer le service de rôle licences des services Bureau à distance

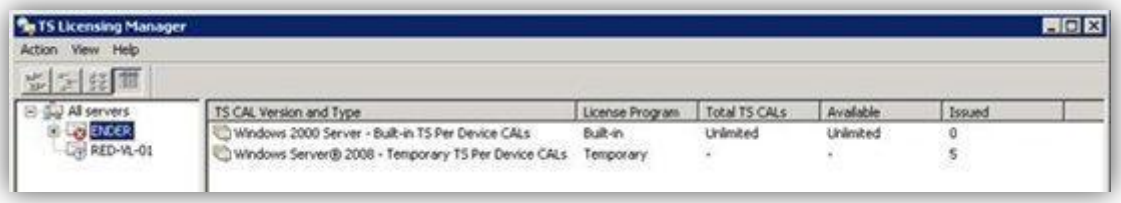
1. Ouvrez une session sur votre serveur en tant qu'Administrateur.
2. Sur le serveur où installer le service de rôle Gestionnaire de licences des services Bureau à distance, ouvrez Gestionnaire de serveur. (Pour ouvrir le Gestionnaire de serveur, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez **Gestionnaire de serveur**.)
3. Sous **Résumé des rôles**, cliquez sur **Ajouter des rôles**.
4. Dans la page **Avant de commencer** de l'**Assistant Ajout de rôles**, cliquez sur **Suivant**.
5. Dans la page **Sélectionnez des rôles de serveurs**, activez la case à cocher **Services Bureau à distance**, puis cliquez sur **Suivant**.
6. Dans la page **Services Bureau à distance**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner les services de rôle**, activez la case à cocher **Gestionnaire de licences des services Bureau à distance**, puis cliquez sur **Suivant**.
8. Dans la page **Configurer l'étendue de la découverte du Gestionnaire de licences des services Bureau à distance**, activez la case à cocher **Configurer une étendue de découverte pour ce serveur de licences**, cliquez sur **Ce domaine**, puis sur **Suivant**.
9. Dans la page **Confirmer les sélections pour l'installation**, vérifiez que le service de rôle Gestionnaire de licences des services Bureau à distance sera installé et cliquez sur **Installer**.
10. Dans la page **Progression de l'installation**, vous pouvez suivre le déroulement de la procédure.
11. Dans la page **Résultats de l'installation**, vérifiez que l'installation du service de rôle Gestionnaire de licences des services Bureau à distance a réussi, puis cliquez sur **Fermer**.

II. Activation du serveur de licences des services Bureau à distance

1. Ouvrir le Gestionnaire de licences des services Bureau à distance sur le serveur de licences. (Pour ouvrir le Gestionnaire de licences des services Bureau à distance, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, **Services Bureau à distance** puis cliquez sur **Gestionnaire de licences des services Bureau à distance**.)



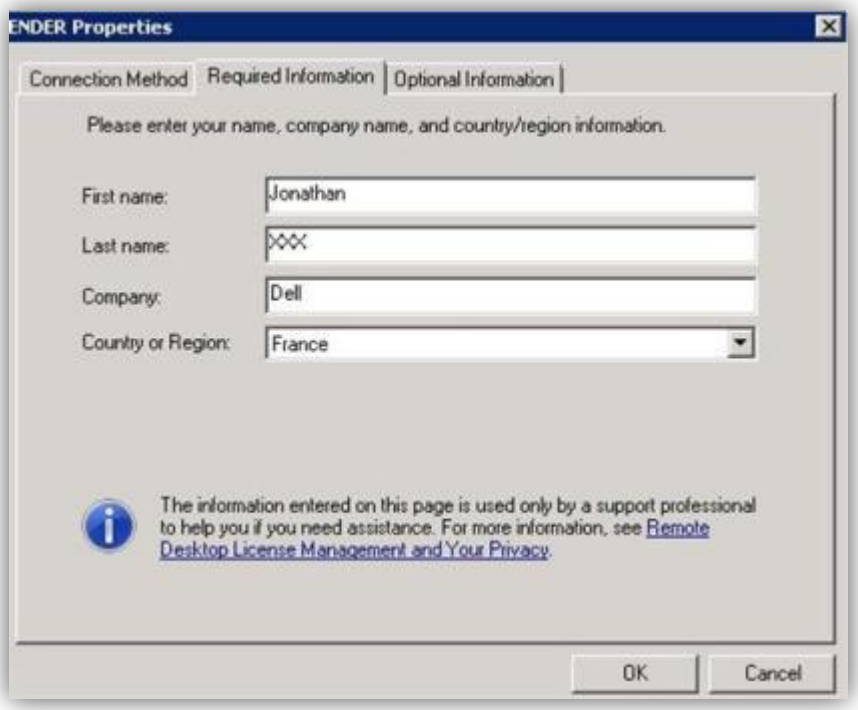
2. Cliquez avec le bouton droit sur le serveur de licences puis cliquez sur **Activer le serveur**. L'Assistant Activation du serveur démarre.



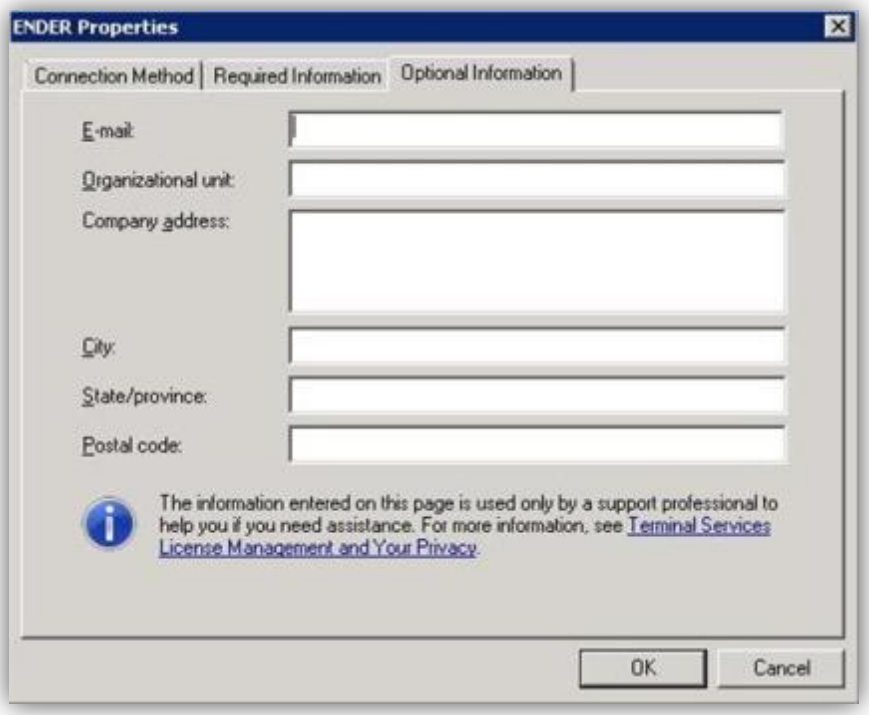
3. Dans la page **Assistant Activation du serveur**, cliquez sur **Suivant**.

4. Dans la page **Méthode de connexion**, dans la liste **Méthode de connexion**, sélectionnez **Connexion automatique (recommandé)**, puis cliquez sur **Suivant**.

5. Dans la page **Informations sur la société**, tapez votre nom et le nom de la société, indiquez votre pays ou votre région, puis cliquez sur **Suivant**.



6. Dans la page d'informations facultative **Informations sur la société**, spécifiez les informations que vous souhaitez éventuellement fournir, telles qu'une adresse de messagerie et l'adresse de la société, puis cliquez sur **Suivant** pour activer votre serveur de licences.



7. Dans la page **Fin de l'Assistant Activation du serveur**, veillez à ce que la case à cocher **Démarrer l'Assistant Installation de licences** soit activée, puis cliquez sur **Suivant**.

Ensuite, utilisez l'**Assistant Installation des licences** pour installer les licences d'accès client aux services Bureau à distance sur le serveur de licences des services Bureau à distance

III. Installation des licences d'accès client aux services Bureau à distance sur le serveur de licences des services Bureau à distance

1. Ouvrir le Gestionnaire de licences des services Bureau à distance sur le serveur de licences. Pour ouvrir le Gestionnaire de licences des services Bureau à distance, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, **Services Bureau à distance** puis cliquez sur **Gestionnaire de licences des services Bureau à distance**.
2. Cliquez avec le bouton droit sur le serveur de licences**,** puis cliquez sur **Installer les licences**.
3. Dans la page **Assistant Installation de licences**, cliquez sur **Suivant**.
4. Dans la page **Programme de licence**, sélectionnez le programme de licence sous lequel vous avez acquis vos licences d'accès client aux services Bureau à distance, puis cliquez sur **Suivant**.
5. Le **programme de licence** sélectionné à la page précédente de l'Assistant détermine les informations que vous devez fournir dans cette page. Généralement, vous devez indiquer un code de licence ou un numéro de contrat. Consultez la documentation qui vous a été fournie lors de l'achat de vos licences d'accès client aux services Bureau à distance.
6. Lorsque vous avez entré ces informations obligatoires, cliquez sur **Suivant**.
7. Dans la page **Version du produit et type de licence**, sélectionnez la version appropriée du produit et le type de licence ainsi que la quantité de licences d'accès client aux services Bureau à distance de votre environnement en vous aidant de votre contrat d'achat, puis cliquez sur **Suivant**.

Microsoft Clearinghouse est contacté automatiquement et traite votre demande. Les licences d'accès client aux services Bureau à distance sont installées automatiquement sur le serveur de licences.

1. Pour achever l'installation, cliquez sur **Terminer**. Le serveur de licences peut maintenant distribuer les licences d'accès client aux services Bureau à distance sur les clients qui se connectent à un serveur Hôte de session Bureau à distance.

Configurez ensuite l'Hôte de session Bureau à distance, pour prendre en charge la gestion de licences des services Bureau à distance.

IV. Configuration du serveur Hôte de session des services Bureau à distance pour la prise en charge du Gestionnaire de licences des services Bureau à distance

Pour spécifier le mode de licence des services Bureau à distance

1. Ouvrir la Configuration d'hôte de session Bureau à distance sur le serveur hôte de session Bureau à distance. Pour ouvrir la Configuration d'hôte de session Bureau à distance, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, **Services Bureau à distance** puis cliquez sur **Configuration d'hôte de session Bureau à distance**.
2. Si la boîte de dialogue **Contrôle de compte d'utilisateur** apparaît, confirmez que l'action affichée est celle que vous souhaitez, puis cliquez sur **Continue**r.
3. Dans la zone **Modifier les paramètres**, sous l'onglet **Gestionnaire de licences**, double-cliquez sur **Mode de licence des services Bureau à distance**.
4. Sous l'onglet **Gestionnaire de licences** de la boîte de dialogue **Propriétés**, cliquez sur le paramètre **Par périphérique** ou **Par utilisateur** le plus approprié à votre environnement.
5. Cliquez sur **OK** pour enregistrer les modifications apportées aux paramètres de licence.

Après avoir spécifié un mode de licence des services Bureau à distance, vous devez indiquer le serveur de licences que le serveur Hôte de session Bureau à distance utilisera.

Pour spécifier le serveur de licences que le serveur Hôte de session des services Bureau à distance doit utiliser

1. Ouvrir la Configuration d'hôte de session Bureau à distance sur le serveur hôte de session Bureau à distance. Pour ouvrir la Configuration d'hôte de session Bureau à distance, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, **Services Bureau à distance** puis cliquez sur **Configuration d'hôte de session Bureau à distance**.

2. Si la boîte de dialogue **Contrôle de compte d'utilisateur** apparaît, confirmez que l'action affichée est celle que vous souhaitez, puis cliquez sur **Continue**r.
3. Dans la zone **Modifier les paramètres**, sous **Gestionnaire de licences**, double-cliquez sur **Serveurs de licences des services Bureau à distance**.
4. Dans la fenêtre **Configuration d'hôte de session des services Bureau à distance**, cliquez sur **Fermer**.
5. Sous l'onglet **Gestionnaire de licences** de la boîte de dialogue **Propriétés**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Ajouter un serveur de licences**, sélectionnez **RDL-SRV** dans la liste de serveurs de licences connus, puis cliquez sur **Ajouter**.
7. Cliquez sur **OK** pour fermer la boîte de dialogue **Ajouter un serveur de licences**, puis cliquez sur **OK** pour enregistrer les modifications apportées aux paramètres de licence.

4.1.2.1.7 Conclusions sur la solution RemoteApp de Windows Server 2008 R2

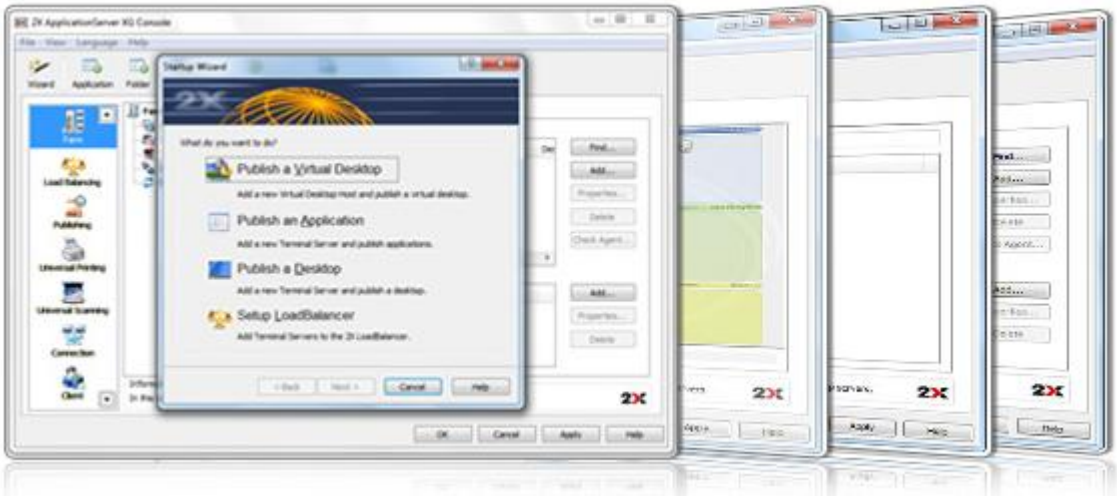
Solution fonctionnelle qui apporte certains avantages :

- Le raccourci d'exécution de l'application est un simple lien « **rdp** »
- Connexion possible à partir d'une interface web

Mais apporte aussi beaucoup d'inconvénients :

- L'interface web fonctionne uniquement avec Internet Explorer
- Obligation d'installer un serveur de licences et d'obtenir des licences CAL-RDS

4.1.3 SOLUTION 3 : 2X Application Serveur



L'application 2X ApplicationServer XG étend Windows Terminal Services en utilisant un shell personnalisé et des applications distribuées via des canaux virtuels, en s'appuyant sur le protocole RDP.

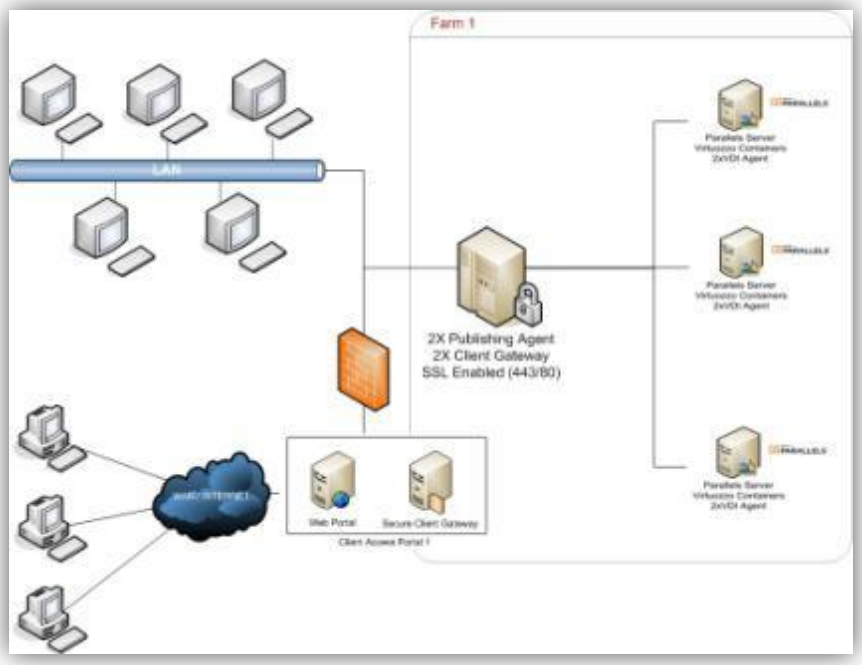
Les applications fonctionnent de façon isolée, dans leurs propres sessions distinctes sans affecter les autres applications, économisant ainsi les ressources.

Les applications sont parfaitement intégrées dans les bureaux locaux et les barres de tâches. Les applications virtuelles et les bureaux sont accessibles via le client 2X, disponibles dans une large gamme de clients mobiles ou fixes.

De nombreux clients de connexion à distance (PC, Tablette ou mobile) : Windows, Linux, MAC, Android, IPhone, IPad.

Principales fonctions de 2X Application Server XG :

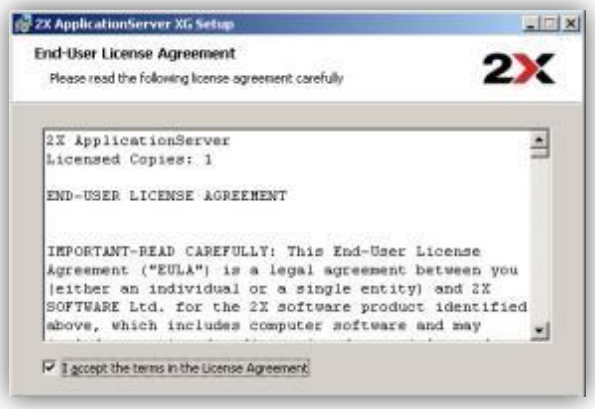
- Publication, présentation des applications
- Intégration au poste de travail local & à la barre des tâches
- Portail Web et Cloud
- Compatible Terminal Server et RDS
- Intégration avec 2X LoadBalancer, répartition de la charge entre plusieurs serveurs
- Connexion sécurisée SSL aux applications
- Universal Printing - Driver d'imprimante universel
- Single Sign-On
- Support de moniteurs multiples
- VDI Connexion Broker
- Compatible hyperviseurs Microsoft Hyper-V, Citrix XenServer, VMware vSphere
- Support multimédia RemoteFX et RDP7



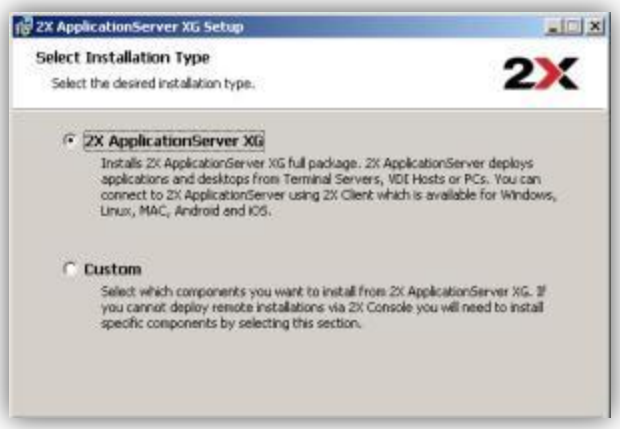
4.1.3.1 Installation 2xApplicationServer XG sur Windows Server 2008 R2

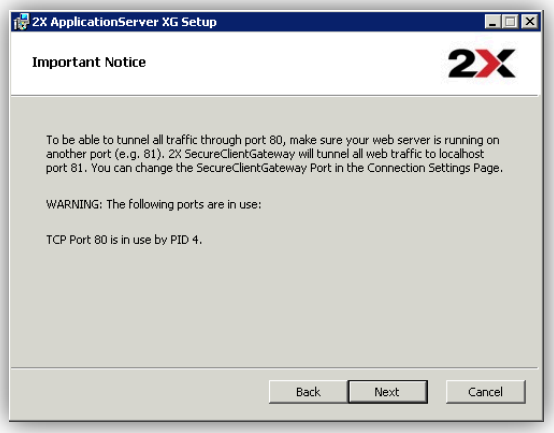
Tout d'abord, ce logiciel est gratuit mais limité à 3 clients. En fait, lorsque vous le téléchargez sur leur site, vous devez mentionnez une adresse mail valide à laquelle vous recevrez un numéro de série pour pouvoir enregistrer le logiciel gratuitement une fois la version d'évaluation de 30 jours expirée.
Pendant ces 30 jours vous pourrez utiliser un nombre illimité de clients mais ce nombre sera limité à 3 à la fin de cette durée.
Par contre la licence gratuite est valable à vie comme indiqué sur la page de téléchargement de ce logiciel "**2X ApplicationServer XG**".
Ensuite, ce logiciel est compatible avec Windows Server 2000, 2003, 2008 et 2008 R2.

1. Installation Serveur



Sélectionnez le dossier dans lequel installer 2X puis sélectionner "2X ApplicationServer XG".

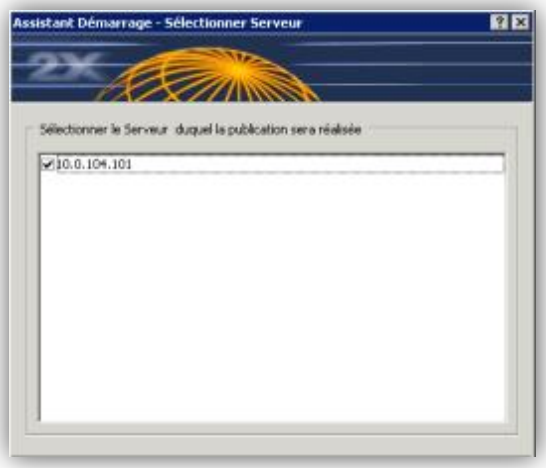




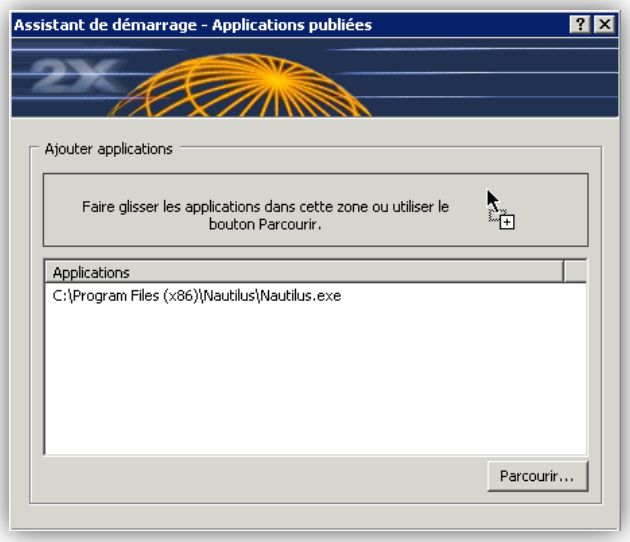
Le port 80 étant déjà utilisé par le serveur web d'accès à REMOTEAPP précedement installé nous devrons changé plus tard le port de connection dans la configuration.

2. Configuration Serveur

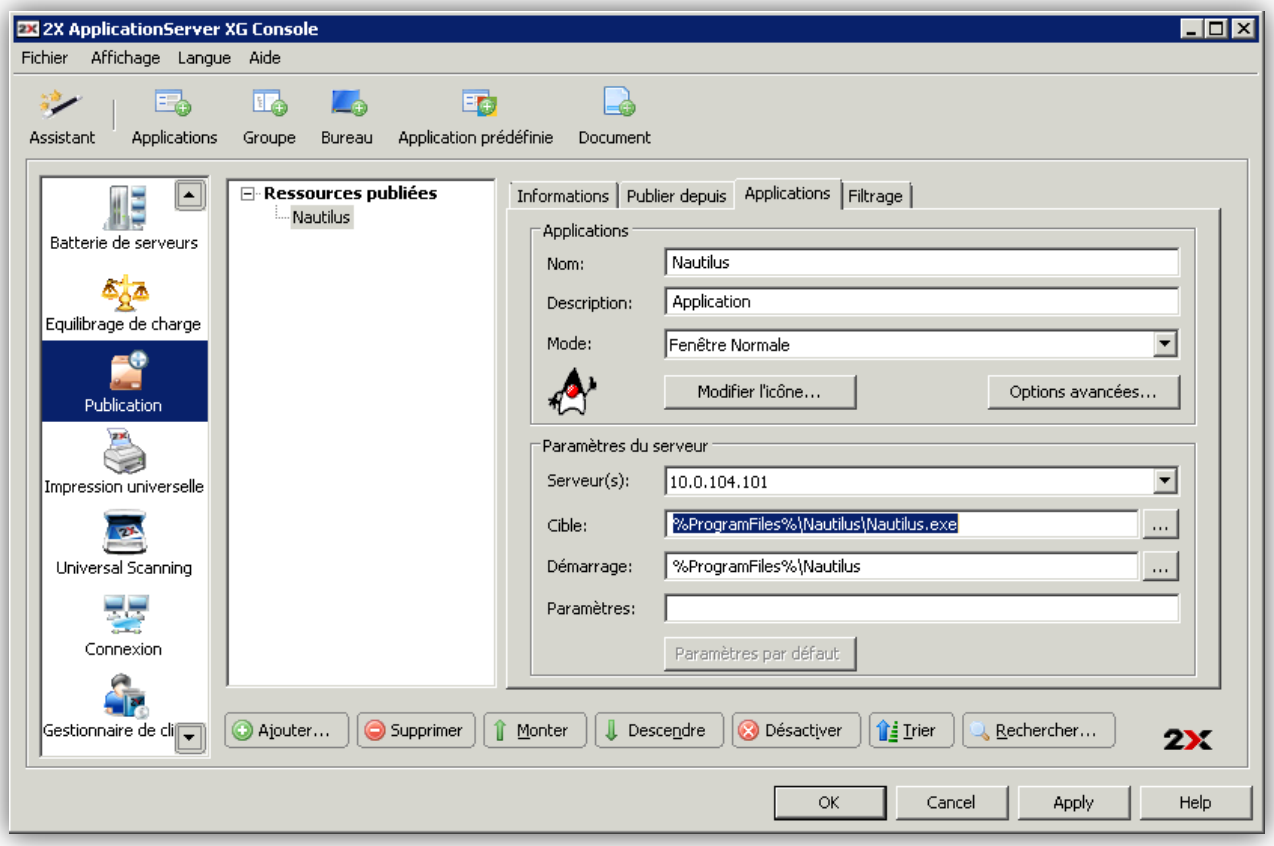
Sélectionnez "Publier une seule application"puis sélectionner le serveur à ajouter à la batterie.



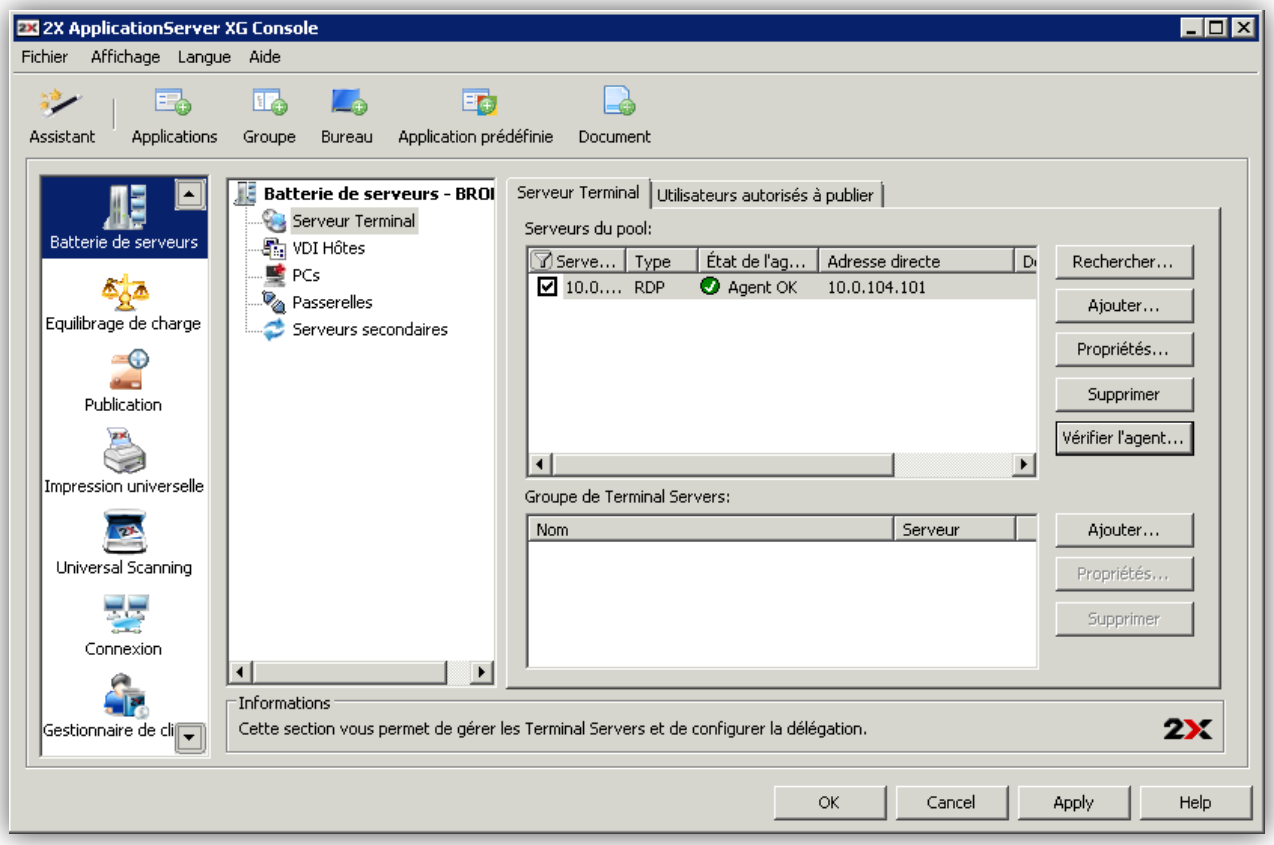
Cliquez sur "Parcourir" et sélectionner le fichier "**exe**" principal du programme à ajouter.

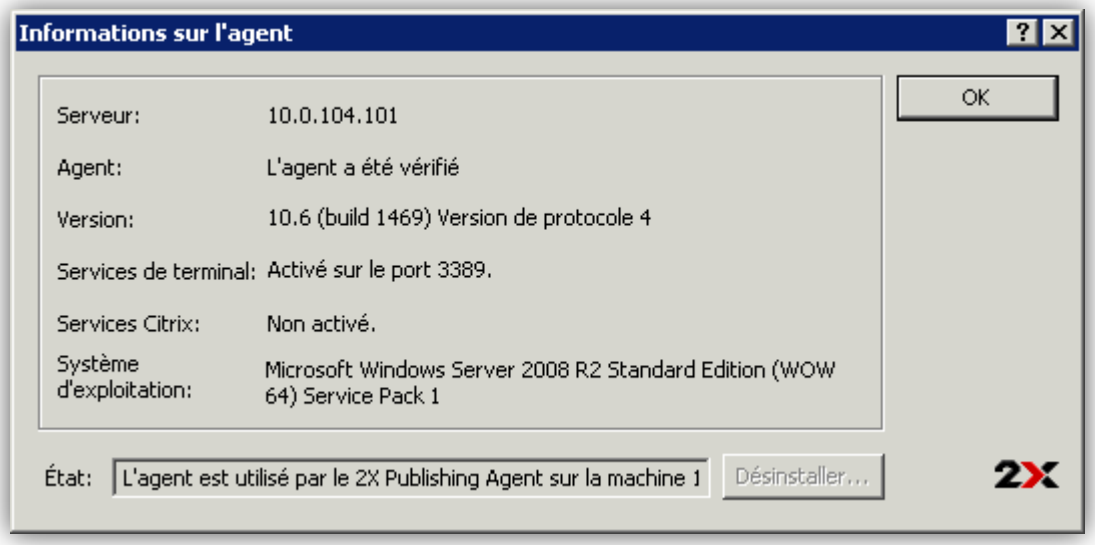


Les applications à publier se trouve dans l'onglet "Publication". Cliquez sur "Appliquer" pour sauvegarder les changements.

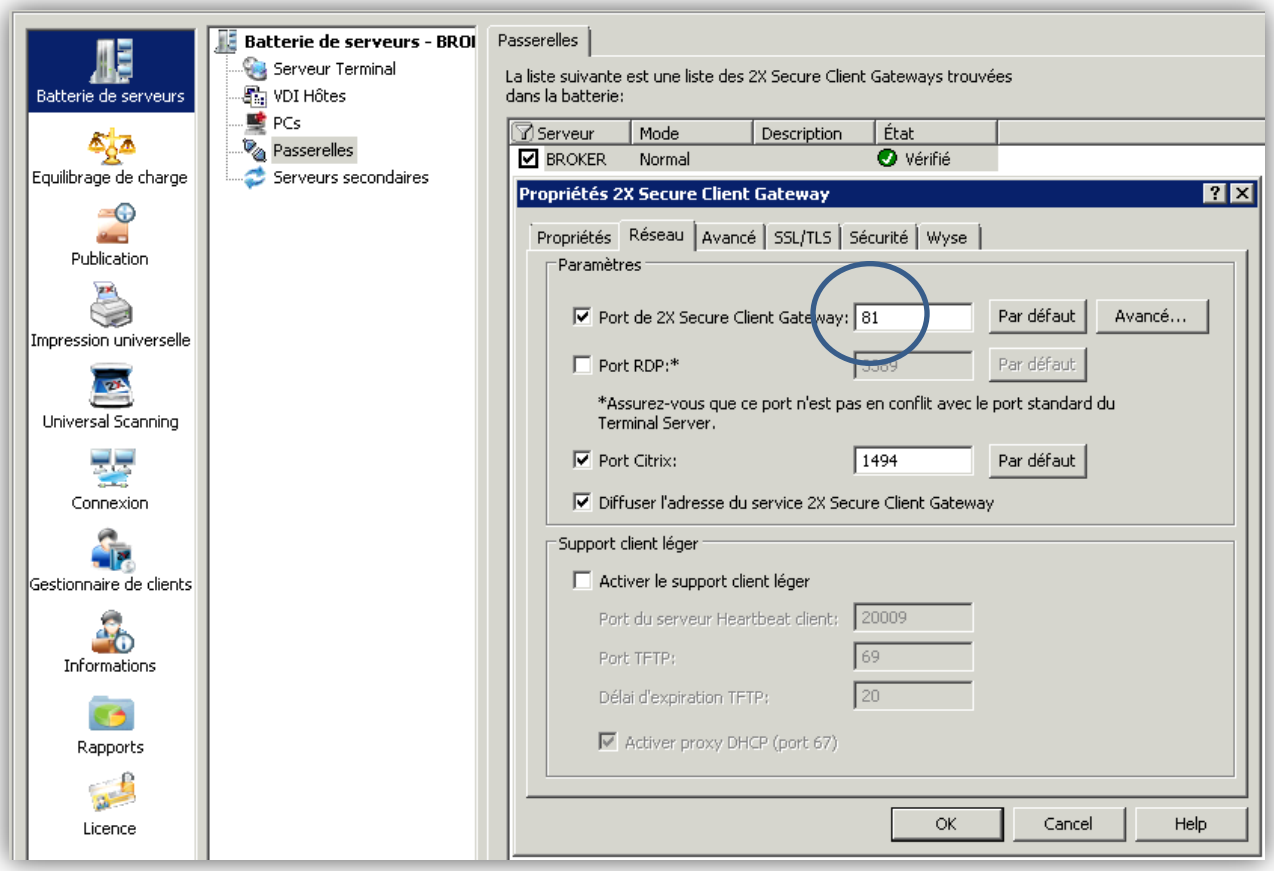


Aller dans l'onglet "Batterie de serveurs et cliquer sur "Serveur Terminal". Dans l'onglet "Serveur Terminal", il doit y avoir un **"v"** vert dans la colonne "Etat de l'agent". Si ce n'est pas le cas cliquer sur le bouton "Vérifier l'agent".





Nous devons maintenant changer le port de connexion de la passerelle pour le Client 2x au serveur.
Configurer le port 81



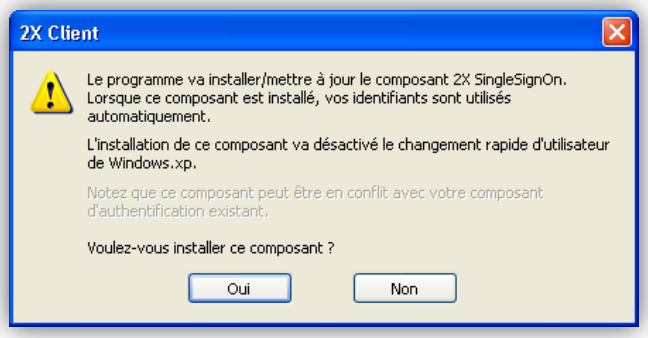
2 modes de connexions à distance au logiciel sont dorénavant possibles par l'utilisateur :

- Avec un agent 2x client installé sur le poste utilisateur
- A partir d'un portail web à l'adresse : http://adresse-du-serveur/2xwebportal/login.aspx

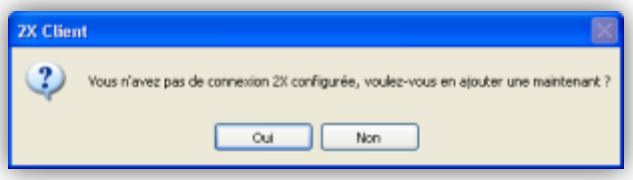
Je vais maintenant détailler ces 2 modes de connexion.

4.1.3.2 Installation 2X client sur un poste Utilisateur

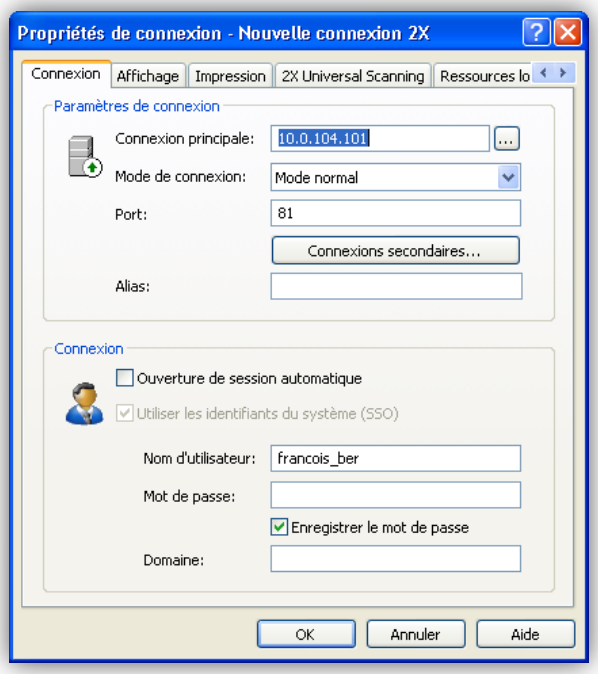
Le logiciel client pour "Windows" est compatible 32 et 64 Bits.



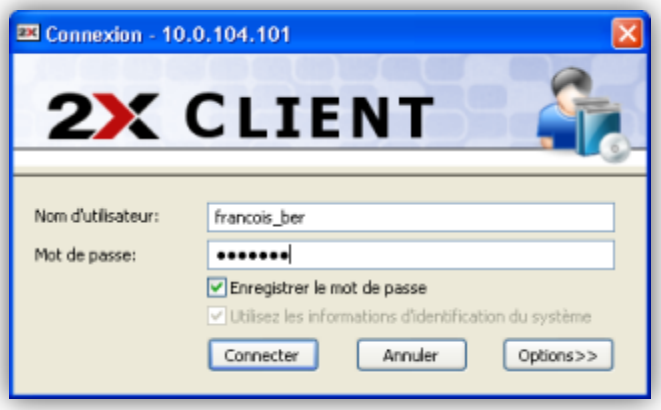
Cliquez sur non, car sinon l'écran d'accueil Windows avec la liste de vos session utilisateur ne s'affichera plus et vous serez obligé de vous connecter en indiquant votre nom d'utilisateur / mot de passe manuellement.



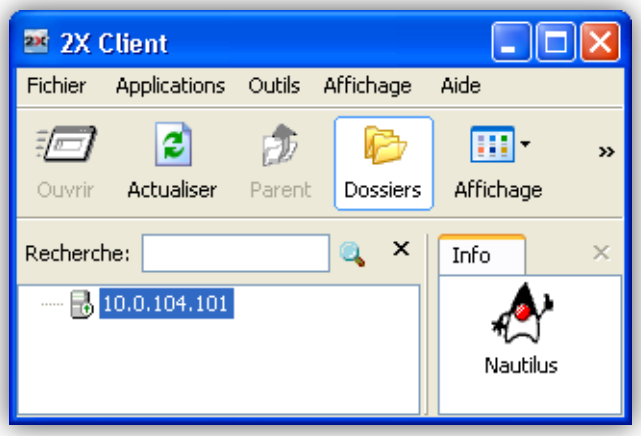
Le client vous signale qu'aucune connexion 2X n'est configurée, cliquez sur "**Oui**" pour en configurer une.



Entrer ensuite les données de connexion du serveur puis cliquer sur OK pour tester la communication avec le serveur d'application.



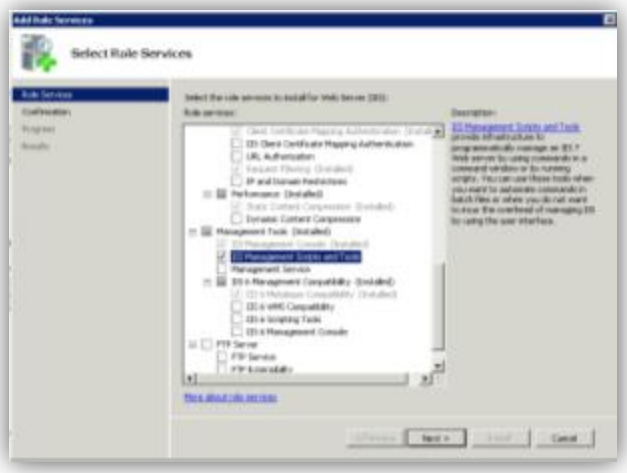
Le client initie une connexion vers le serveur , le serveur est détecté et l'application patagée est bien disponible.

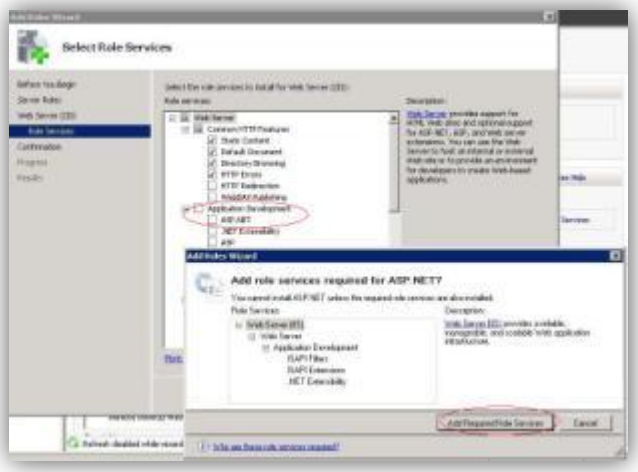


Pour pouvoir utiliser le logiciel, il suffit de double-cliquer dessus

4.1.3.3 Installation de l'interface WebPortal 2X client (Windows Server 2008 R2)

Avant de procéder à l'installation, le rôle « Web Server IIS » doit être installé ainsi que les services IIS Management Scripts and Tools et ASPNET sur le serveur.



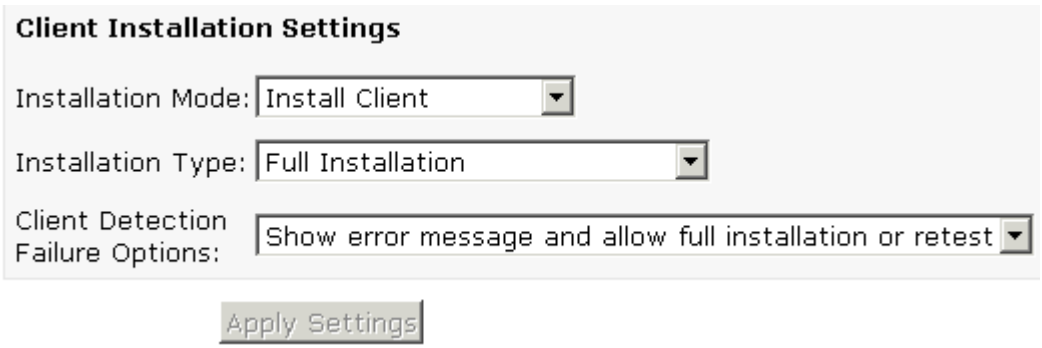


Nous pouvons maintenant procéder à l'installation du portail web. Le port du serveur web doit être diffèrent des autres, nous le configurerons sur le port : 100

A la fin de l'installation nous nous loggons sur l'interface d'administration à l'adresse :

http://adresse_du_serveur:100/2xwebportal/Admin.aspx

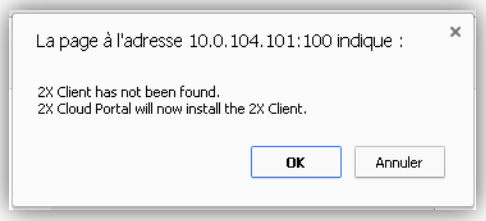
Dans le menu → « General Settings puis → System Settings , il faut veillez à configurer l'installation du client via l'interface web.



Nous allons maintenant acceder au portail web à partir d'un poste client à partir de l'adresse :

http://adresse _du_serveur :100/2xwebportal/Logon.aspx

Accepter les avertissements de sécurité de Java , l'installation recherche si le client 2X est déjà installé sur le poste utilisateuret procedera à son installation.



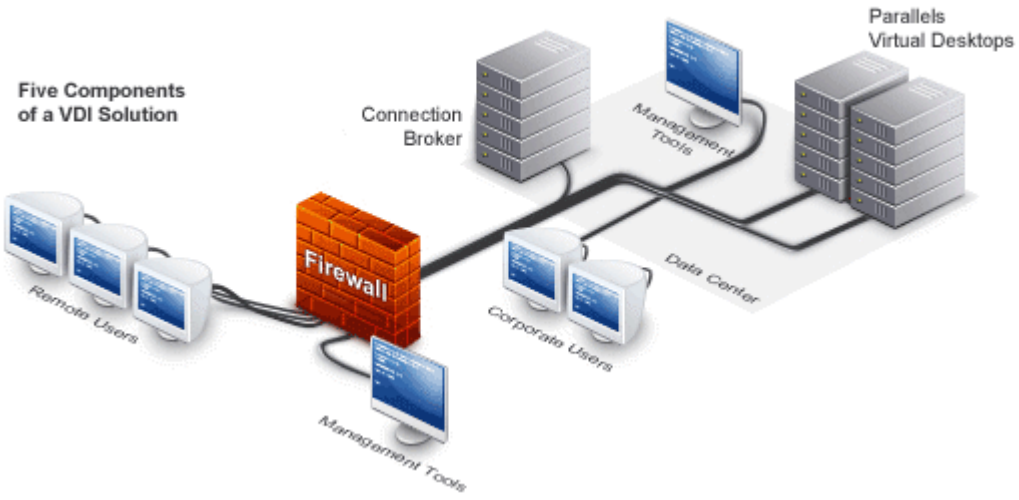
Nous pouvons dorénavant nous authentifier avec un utilisateur du domaine.

4.1.3.4 Conclusion sur la Solution 2X ApplicationServer XG

La plateforme d'administration est très intuitive à utiliser et le déploiement des applications distantes est très simple à effectuer.

Mais l'installation du client « Java » au moment de la première connexion d'un utilisateur sur le portail web est assez longue et difficilement compréhensible pour l'utilisateur.

5 Installation et Configuration d'un Connexion Broker



Actuellement chaque utilisateur se connecte à distance sur une machine virtuelle qui se trouve localisée dans les serveurs du Datacenter de Montpellier où sur les serveurs de Marseille.

Un Connexion Broker centralise les accès et alloue une machine virtuelle disponible à un utilisateur authentifié. Il assure également l'indépendance des utilisateurs vis-à-vis d'un terminal et la possibilité dans certains cas de créer des groupes pour du provisionning de VM.

L'accès à distance peut se faire au travers de différents matériels : un PC traditionnel, un portable, un terminal léger, voir un téléphone de type Smartphone sans rien avoir à configurer sur le poste client.

Les bureaux à distance sont donc fournis par la solution des Contenaires Parallels Virtuozzo
Chaque contenaires est configuré pour être accessible à partir d'une adresse IP.

121	marseille-vm407	MARSEILLE-VM407	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
139	MARSEILLE-VM662	MARSEILLE-VM662	[redacted]	Starting	windows_2003_std_sp2-5.2.3790/20071017 x86_64
153	marseille-vm145	MARSEILLE-VM145	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
166	marseille-vm164	MARSEILLE-VM164	[redacted]	Down	windows_2003_std_sp2-5.2.3790/20071017 x86_64
236	TALEND-MRS	TALEND-MRS	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
239	marseille-vm234	MARSEILLE-VM234	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
245	MARSEILLE-VM242	MARSEILLE-VM242	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
251	marseille-vm250	MARSEILLE-VM250	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
252	marseille-vm251	MARSEILLE-VM249	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
255	marseille-vm255	MARSEILLE-VM255	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
256	MARSEILLE-VM256	MARSEILLE-VM256	[redacted]	Starting	windows_2003_std_sp2-5.2.3790/20071017 x86_64
415	MARSEILLE-VM415	MARSEILLE-VM415	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
426	MARSEILLE-VM426	MARSEILLE-VM426	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
427	MARSEILLE-VM427	MARSEILLE-VM427	[redacted]	Starting	windows_2003_std_sp2-5.2.3790/20071017 x86_64
600	MARSEILLE-VM600	MARSEILLE-VM600	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
601	MARSEILLE-601	MARSEILLE-601	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
658	MARSEILLE-VM658	MARSEILLE-VM658	[redacted]	Down	windows_2003_std_sp2-5.2.3790/20071017 x86_64
864	marseille-vm865	MARSEILLE-VM865	[redacted]	Running	windows_2003_std_sp2-5.2.3790/20071017 x86_64
13088	GCLOUD13088	GCLOUD13088	[redacted]	Starting	windows_2003_std_sp2-5.2.3790/20071017 x86_64

Adresses IP

Actuellement les utilisateurs peuvent se connecter à leur contenaires à partir 'une adresse IP publique + un n° de port --→xxx.xxx.xxx.xxx :xxx

Des règles de redirection NAT sont enregistrées dans un routeur redirigeant la correspondance entre le numéro de port et l'adresse IP privée du contenaires

XXX.XXX.XXX.XXX : XXX ROUTEUR → XXX.XXX.XXX.XXX
→ XXX.XXX.XXX.XXX

Adresse Publique + n° de port

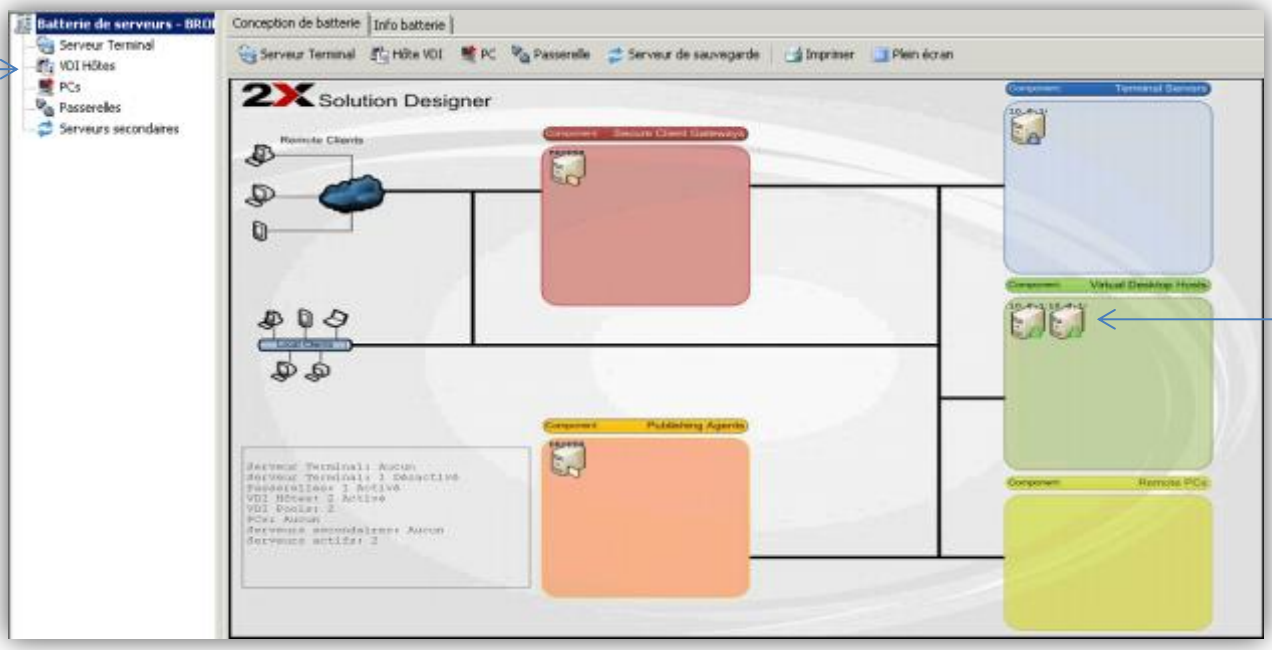
Adresse Privée du contenaire

L'administrateur Cloud désirerait que l'utilisateur puisse accéder à son contenaire Parallels via une passerelle web ou un client installé sur son poste.

5.1 SOLUTION 1 : 2XAPPLICATION SERVER

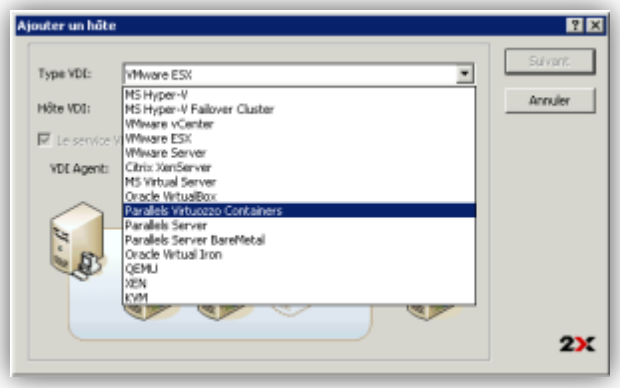
La procédure d'installation reste la même que précédemment, le connexion broker faisant partie des fonctions disponibles proposés dans la solution 2X ApplicationServer XG .

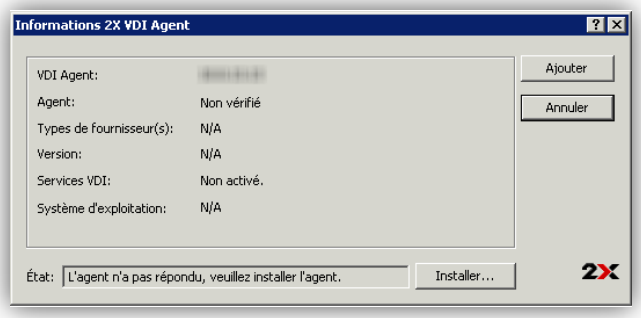
Dans la console d'administration de 2XApplicationSERVER , nous allons ajouter 2 nouveaux serveurs dans les hôtes VDI dans notre batterie de serveurs.



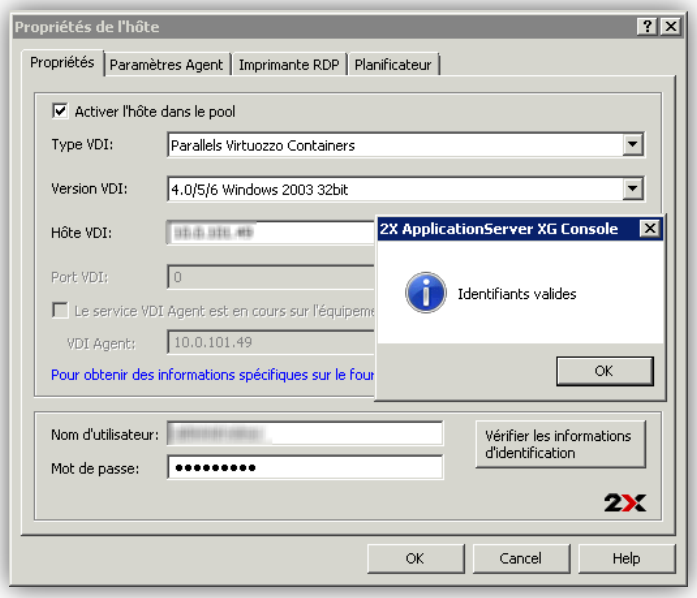
Dans l'onglet « Hôtes de client virtuels », sélectionner « Ajouter », dans notre cas sélectionner le type de type de VDI Parallels Virtuozzo Containers puis renseigner la partie Hôte VDI avec l'adresse IP du server.

Effectuer ensuite l'installation à distance de l'agent.

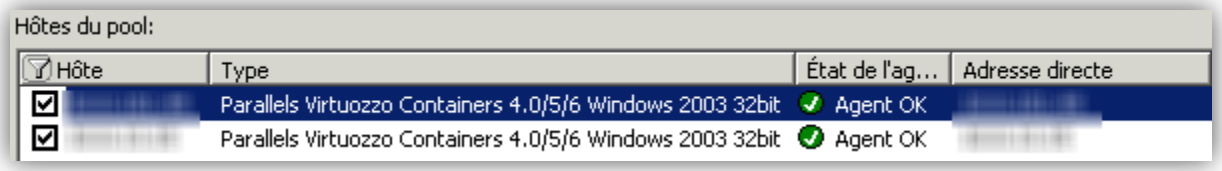




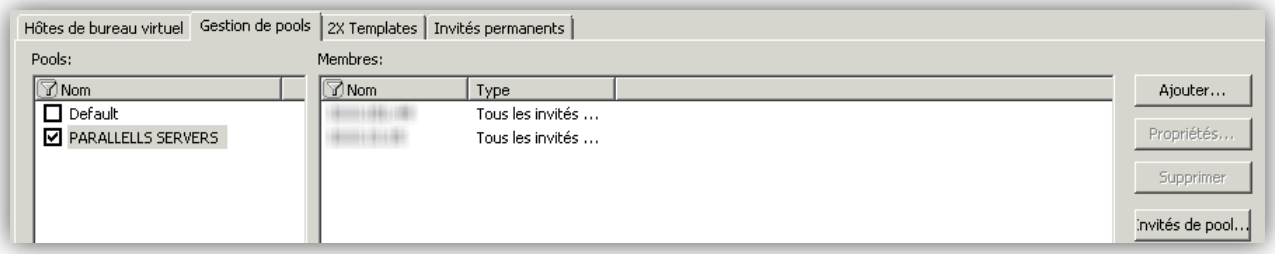
Il faut ensuite saisir les identifiants de l'administrateur du serveur Parallels et effectuer un test d'authentification.

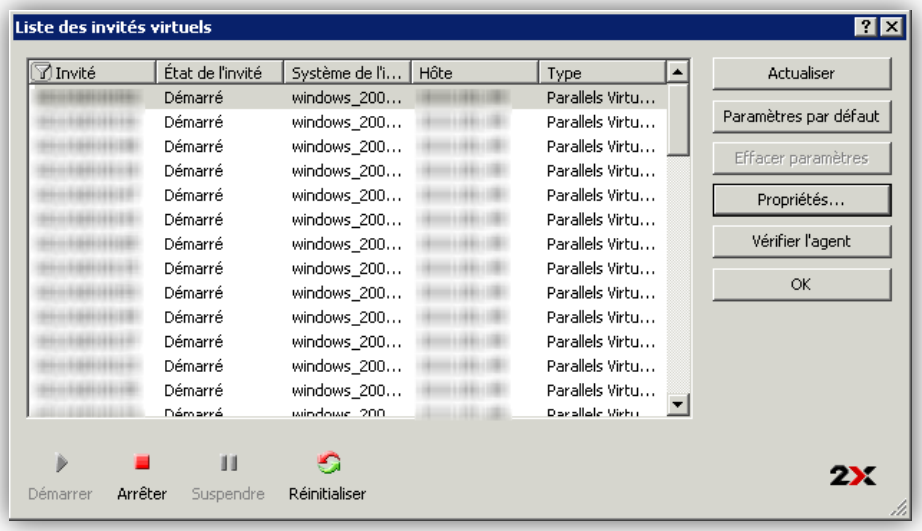


L'administrateur Cloud ayant mis à ma disposition 2 serveurs Parallels (1-Marseille+1-Montpellier) ainsi que 4 containers, je vais donc configurer ces 2 serveurs sur ma ferme de serveurs VDI.

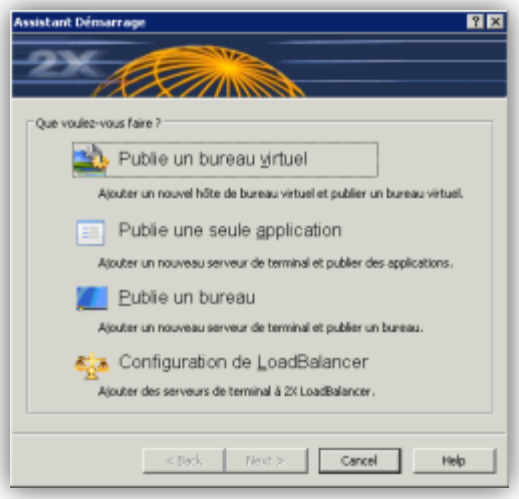


Dans l'onglet suivant « Gestion de pools » nous avons dorénavant nos 2 serveurs Parallels et en cliquant sur le bouton « Invité de pool » nous verrons apparaître tous les containers disponibles sur les 2 serveurs.



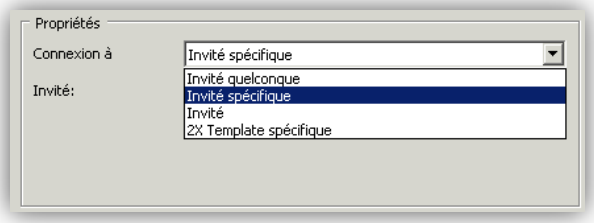


Nous pouvons maintenant publier un bureau virtuel :

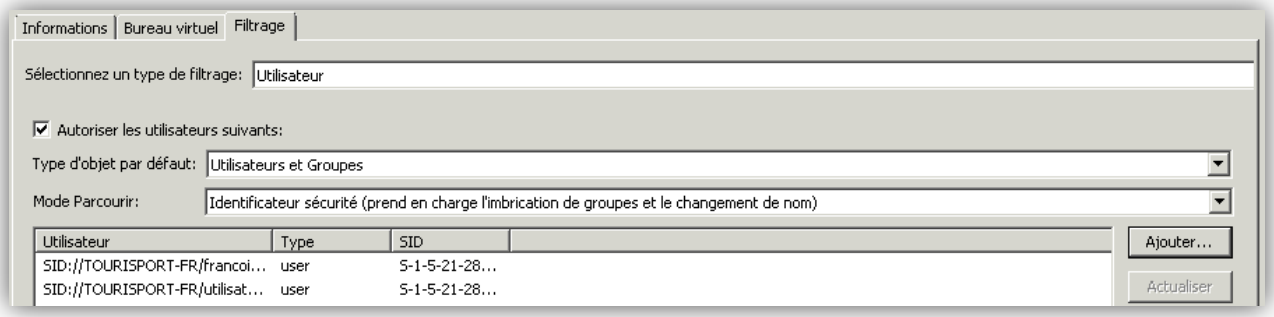


3 modes de connexion ont configurables :

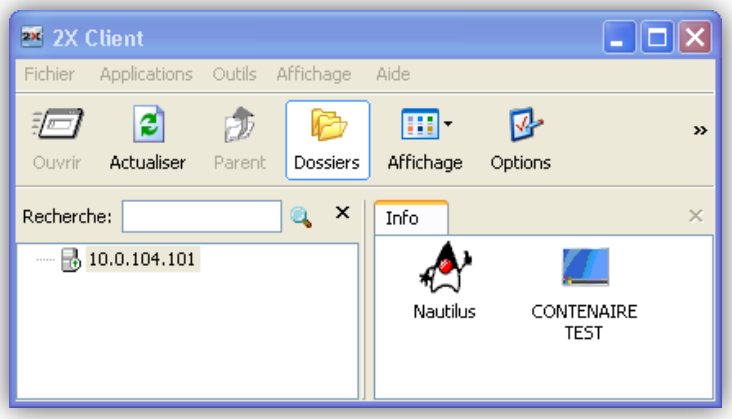
- Invité quelconque : un contenaire disponible sera attribué à l'utilisateur
- Invité spécifique : un certain contenaire lui sera attribué
- Invité : un contenaire attribué devra être spécifié dans la configuration de l'utilisateur au niveau du contrôleur de domaine



En choisissant « **invité spécifique** », nous pouvons autoriser l'utilisation du contenaire à un certain utilisateur ou à un groupe.

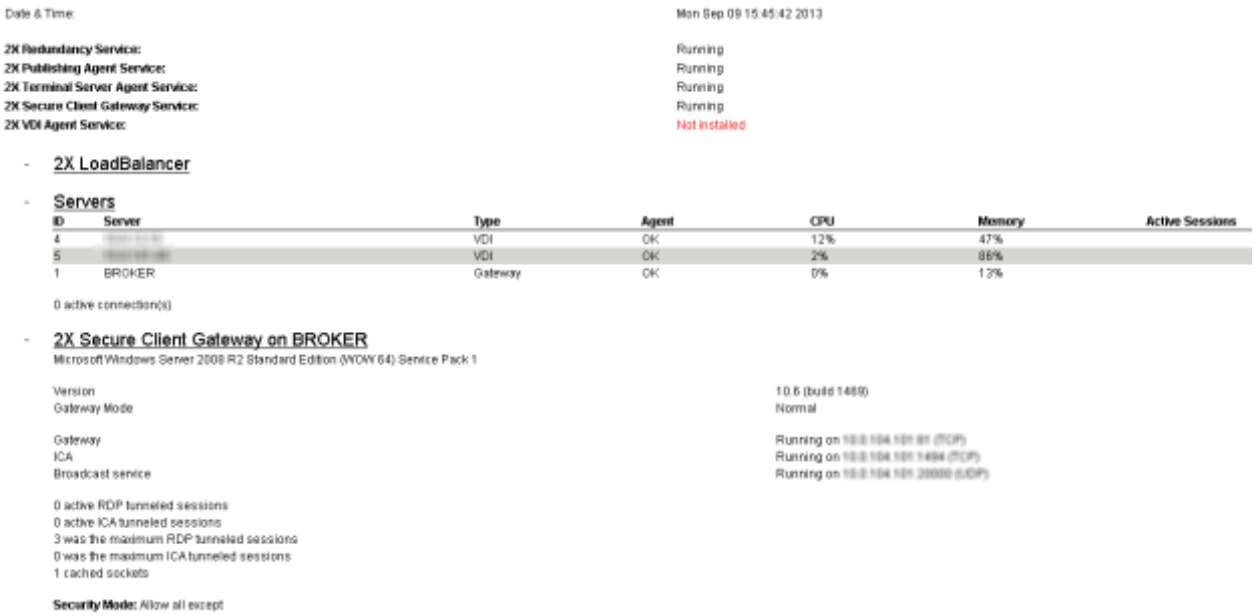


Notre bureau virtuel est dorénavant publié, nous pouvons effectuer un test de connexion avec les méthodes détaillées en page 72 et page 75.



A partir de notre client nous avons dorénavant notre application précédemment publiée et notre bureau virtuel.
Il suffira de double-cliquer sur l'icône pour ouvrir une session sur le contenaire dédié.

Dans la partie information, nous pourrons visualiser les différentes sessions actives ainsi que l'utilisateur connecté.



Guests on [redacted]

Microsoft Windows Server 2008 R2 Standard Edition (x64)

0 active connection(s)

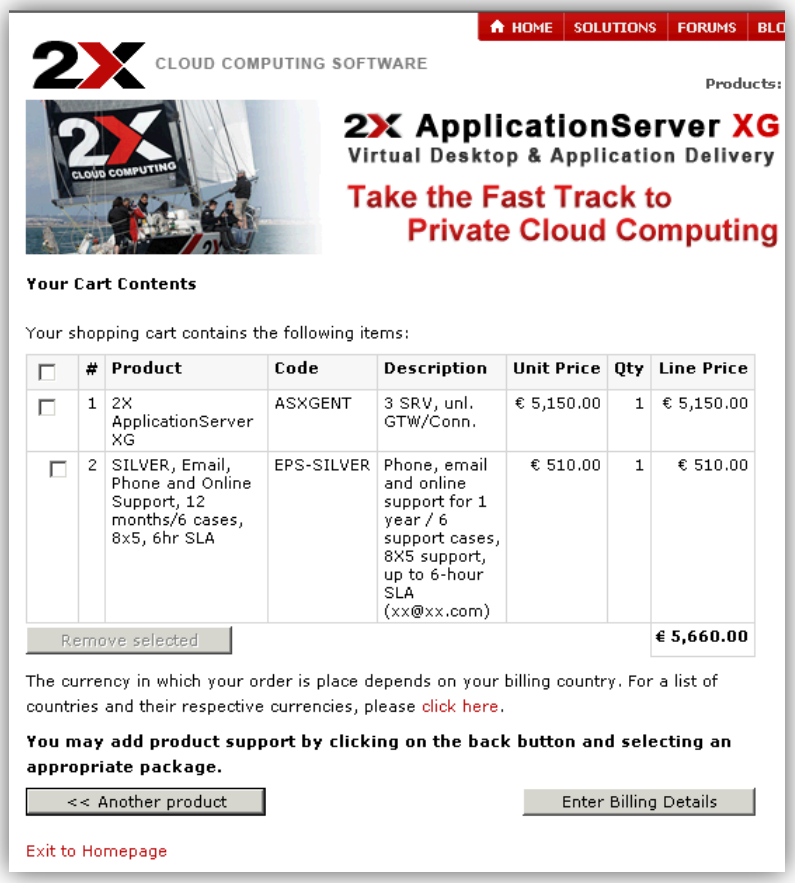
ID	Guest	State	Connection	Template	User
0	[redacted]	On	Disconnected	N/A	francois_ber
1	[redacted]	On	Disconnected	N/A	[redacted]
10	[redacted]	On	Disconnected	N/A	
11	[redacted]	On	Disconnected	N/A	
12	[redacted]	On	Disconnected	N/A	
13	[redacted]	On	Disconnected	N/A	
14	[redacted]	On	Disconnected	N/A	
15	[redacted]	On	Disconnected	N/A	
16	[redacted]	On	Disconnected	N/A	
17	[redacted]	On	Disconnected	N/A	
18	[redacted]	On	Disconnected	N/A	
19	[redacted]	On	Disconnected	N/A	
2	[redacted]	On	Disconnected	N/A	utilisateur_ovd_test

5.1.1 Conclusions de la Solution BROKER 2XApplicationsServer

Les conclusions restent les mêmes que pour la solution de serveur d'application, l'installation du client 2X en java à partir de l'interface web reste assez lourde pour l'utilisateur.

La mise en place et la prise en main de l'interface d'administration reste assez simple.

Cette solution reste payante avec les tarifs décrits dans les propositions que j'ai donné à la direction du SI (Annexes). Voici le prix de la proposition qui comprend la licence pour 3 serveurs avec Gateway et utilisateurs illimités ainsi qu'un support Gold par téléphone, email et online pour une année.



5.2 SOLUTION ERICOM POWERTERM WEBCONNECT REMOTEVIEW

Ericom propose une solution correspondant aux besoins de Tourim-It et à l'infrastructure existante.

La solution Powerterm Webconnect RemoteView propose les options suivantes :

- Serveur d'application
- Connexion Broker
- Compatibilité avec les serveurs VDI Parallels Virtuozzo
- Contrôle total des contenaires à partir de l'interface
- Possibilité de dédier un ou plusieurs VDI par Utilisateur

POWERTERM WEBCONNECT SERVER PLATFORMS	Microsoft® Windows 2003, 2003 x64, 2008, 2008 x64, 2008 R2 and 2008 R2 x64
CLIENT DEVICES	Windows XP, Vista and Windows 7 (32-bit and 64-bit), Windows CE, Linux (Ubuntu, Red Hat and Novell), Mac OS X (Intel & PowerPC), Novell SLED 10 client, Locked-Down Kiosks, Wyse S10, Teradici PCoIP client, Google Chrome OS, and any other device with an HTML5-capable browser
MOBILE DEVICES	iPhone (3 and later); iPad (any); iPod Touch (3 and later); Android 1.5 and later; Chromebook; RIM Playbook and BlackBerry OS 7 or newer
HOST PLATFORMS	Windows XP, Vista, Windows 7, 2003; 2003 x64; 2008; 2008 x64; 2008 R2 *All can be physical or virtual*
VIRTUALIZATION PLATFORMS	VMware VirtualCenter, 4/vSphere 4.0, VMware vSphere Hypervisor/VMware ESX/ESXi (without VirtualCenter), VMware Server (without VirtualCenter), Microsoft Hyper-V, Microsoft Hyper-V R2 SP1, and Microsoft System Center (SCVMM), XenServer, Parallels Virtuozzo, Oracle VM, Enomaly ECP, Red Hat KVM, Xen Community
SECURITY	SSL, SFTP, Kerberos, SSL VPN integration and interoperability, RSA® SecurID® and RADIUS two-factor authentication

A noter qu'Ericom propose une version gratuite proposant uniquement le serveur d'application Windows :

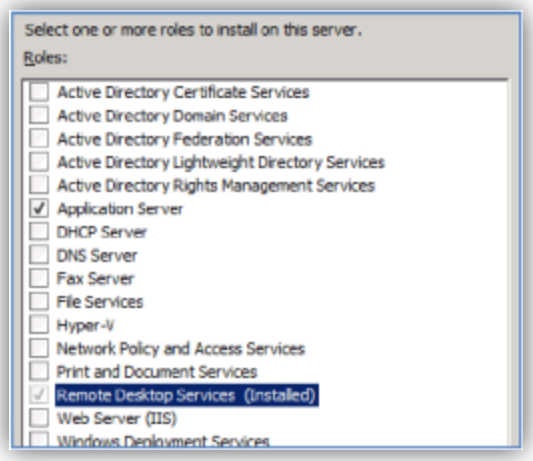
http://www.ericom.com/WS08_R2.asp

Composants nécessaires à l'installation de cette solution :

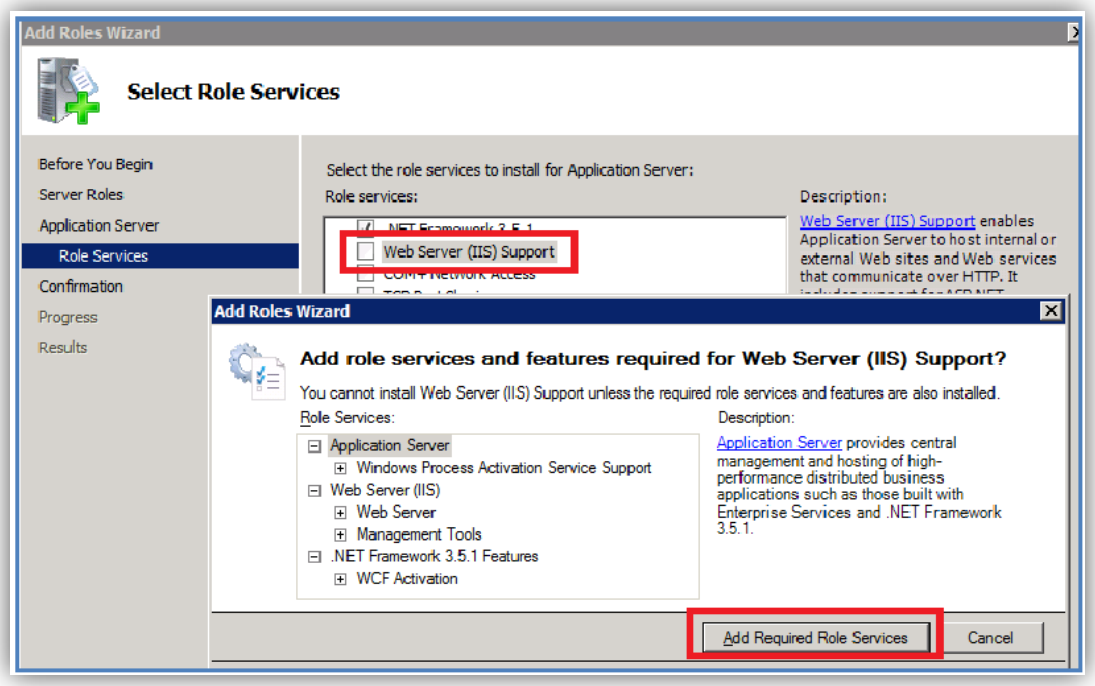
- Un serveur préinstallé avec Windows Server 2008 R2
- Le logiciel d'installation Ericom Secure Gateway permettant aux utilisateurs de se connections sans la mise en place d'un VPN
- Le pack d'installation Powerterm Webconnect Remoteview

5.2.1 Pré configuration du serveur Windows 2008 R2

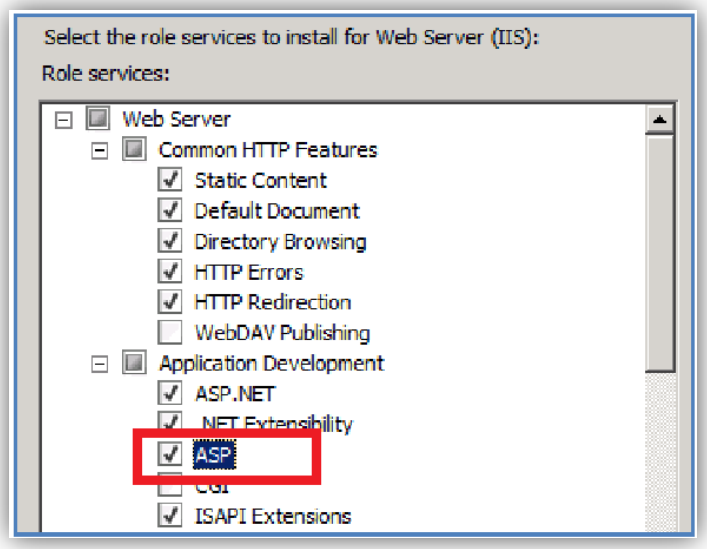
En premier il faudra installer les rôles suivants : ***Application Server*** et ***Remote Desktop Services***



Ensuite dans les services de rôle d'Application Server, il faudra sélectionner ***Web Server (IIS Support)***

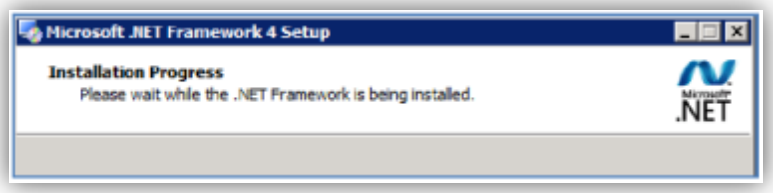


Et dans les options ***Add Required Role Services***, il faudra sélectionner **ASP**



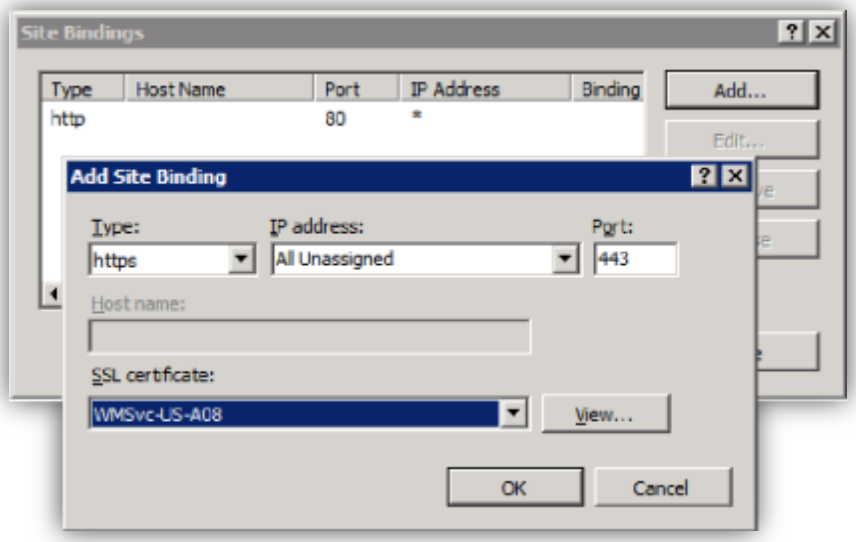
Après l'installation de ces rôles, il faudra redémarrer le serveur.

Il faut maintenant effectuer l'installation de Microsoft NetFrameWork 4



Il faut maintenant configurer WebIIs en HTTPS.
Dans le service WebIIS activé HTTPS sur le port 443
Aller sur "Web Site" et cliquer sur ***Bindings***.

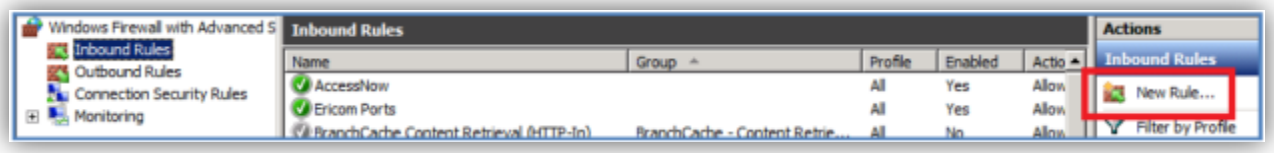
Cliquer sur ***Add*** et changer le mode en ***https*** puis choisir un certificat SSL dans la liste déroulante.

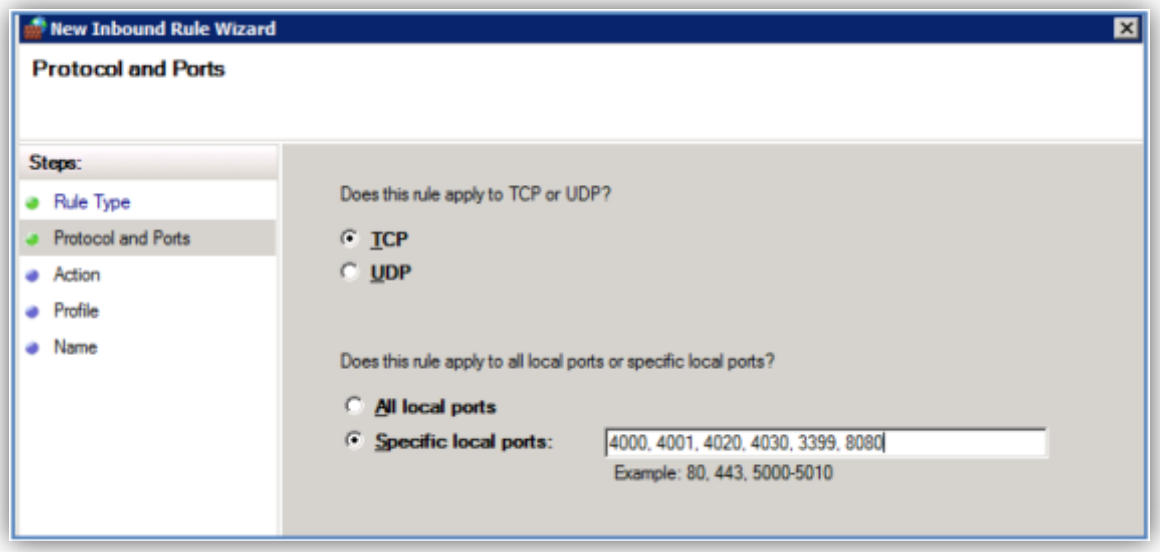


Cliquer ok pour que Web IIS soit actif en HTTPS.

Il faut maintenant configurer le pare-feu pour autoriser les ports utilisés par Powerterm Webconnect.
Il faudra créer une nouvelle règle autorisant les ports **4000,4001,4020,4030,3399,8080** et le **4045**.

Nommer cette nouvelle règle *Ericom Ports*.





5.2.2 Installation d'Ericom Secure Gateway

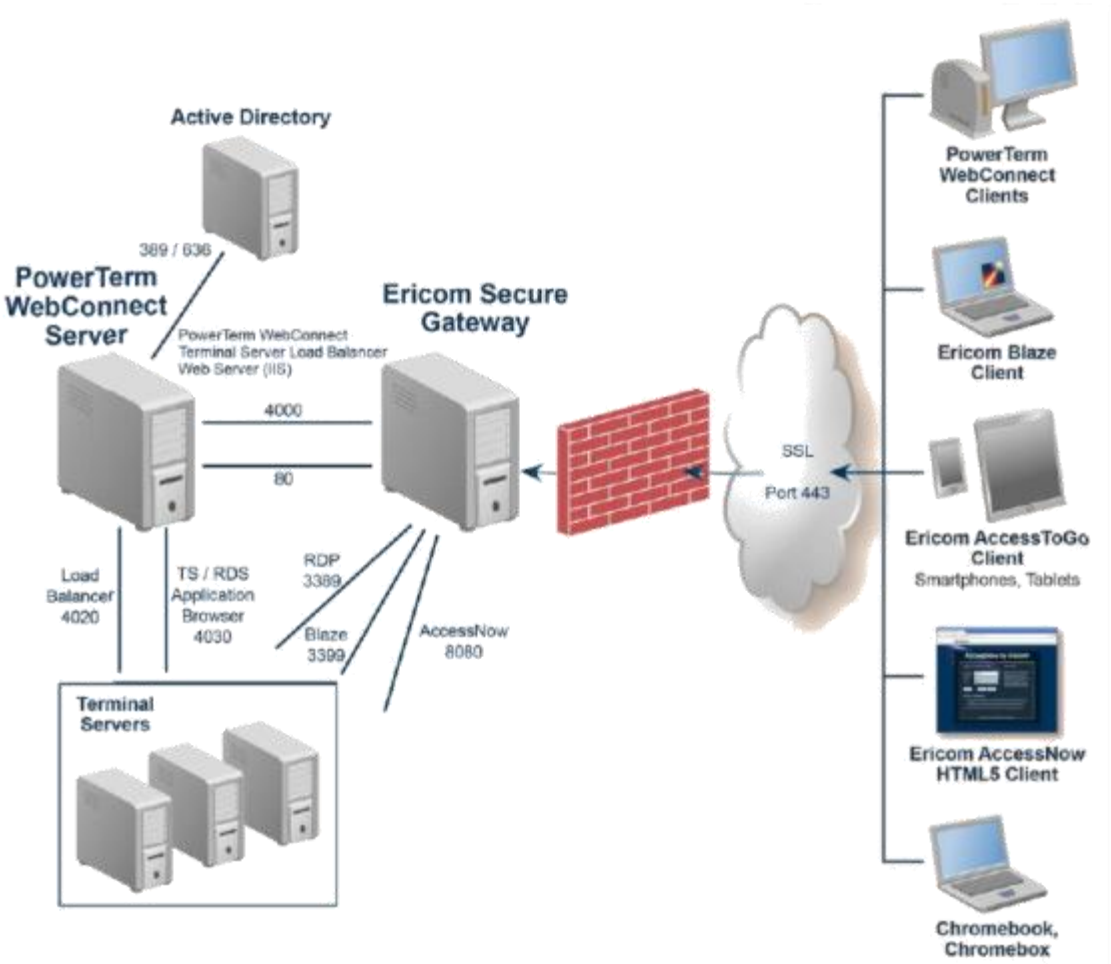
PowerTerm WebConnect inclut une passerelle sécurisée pour gérer et centraliser les accès sur les différents serveurs Ericom et les clients distants.

Secure Gateway est généralement installé dans la DMZ et agit comme un relais proxy unique pour toutes les communications liées à PowerTerm WebConnect.

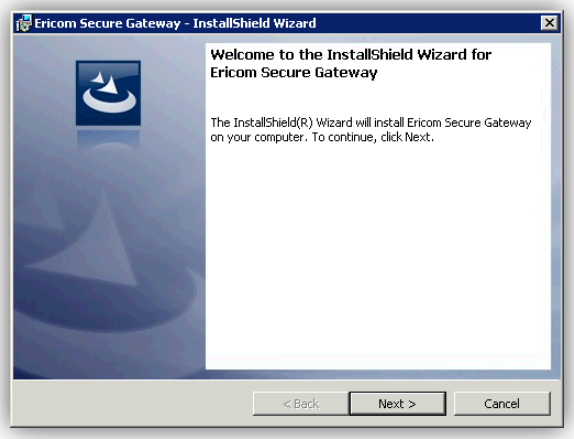
Cela signifie qu'un seul port doit être ouvert sur le pare-feu externe. Secure Gateway « tunellisera » toutes les communications liées à travers son port: PowerTerm WebConnect (4000), RDP (3389), Blaze (3399), Access Now (8080), HTTP (80), HTTPS (443), l'émulation (80), SSH (22), et plus.

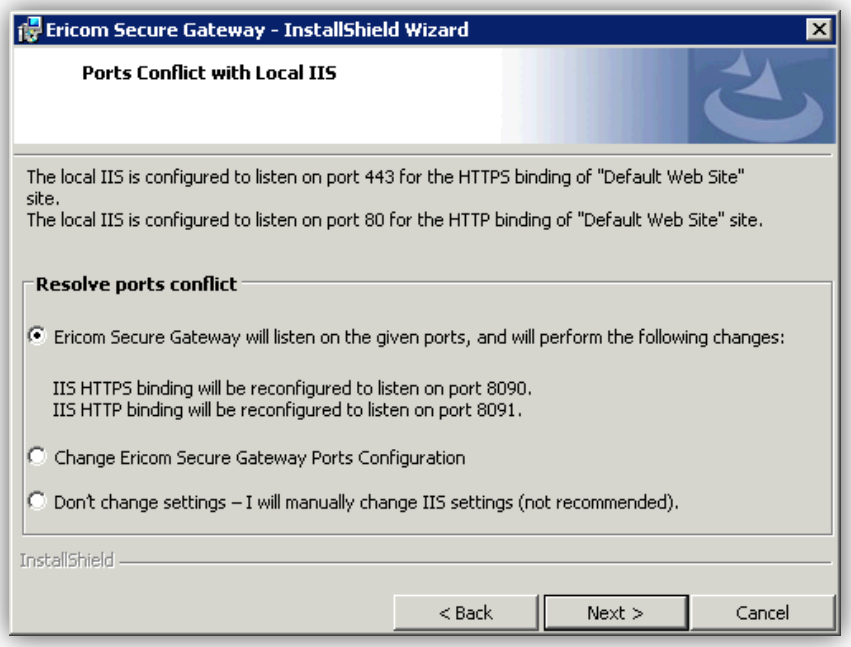
Le serveur Secure Gateway est généralement installé dans la DMZ, tandis que le serveur PowerTerm WebConnect est installé sur le LAN.

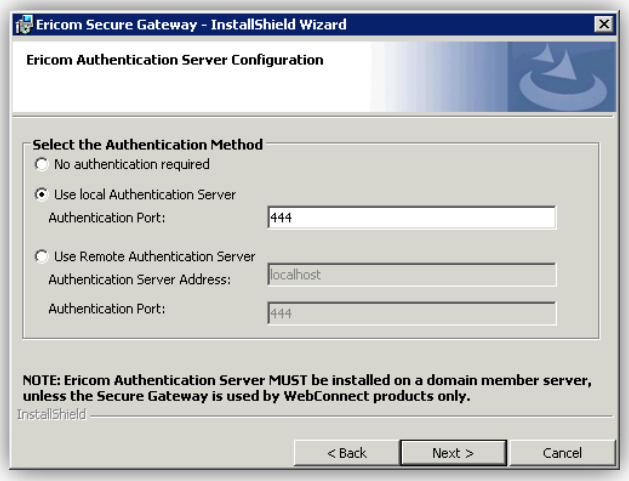
Le schéma suivant illustre le flux de communication des utilisateurs à des connexions à distance à travers l'environnement de PowerTerm WebConnect avec l'utilisation du Secure Gateway.

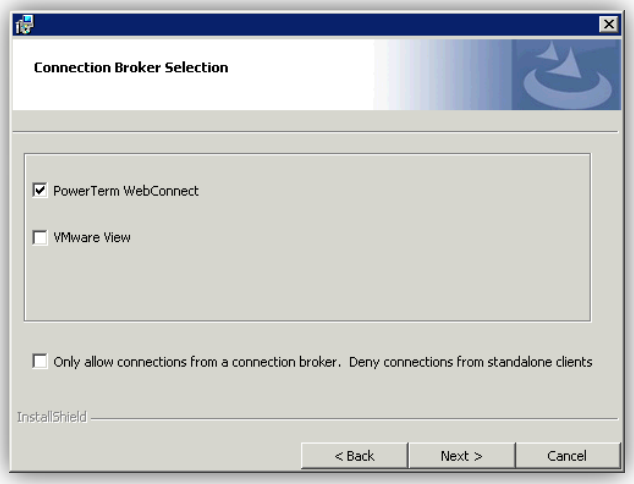


Dans le cadre de mes essais en interne, j'installerais le Secure Gateway sur le même serveur que Powerterm Webconnect.




Ericom Secure Gateway - InstallShield Wizard
Ports Conflict with Local IIS
The local IIS is configured to listen on port 443 for the HTTPS binding of "Default Web Site" site.
The local IIS is configured to listen on port 80 for the HTTP binding of "Default Web Site" site.
Resolve ports conflict
Ericom Secure Gateway will listen on the given ports, and will perform the following changes:
IIS HTTPS binding will be reconfigured to listen on port 8090.
IIS HTTP binding will be reconfigured to listen on port 8091.
Change Ericom Secure Gateway Ports Configuration
Don't change settings – I will manually change IIS settings (not recommended).
InstallShield
< Back
Next >
Cancel

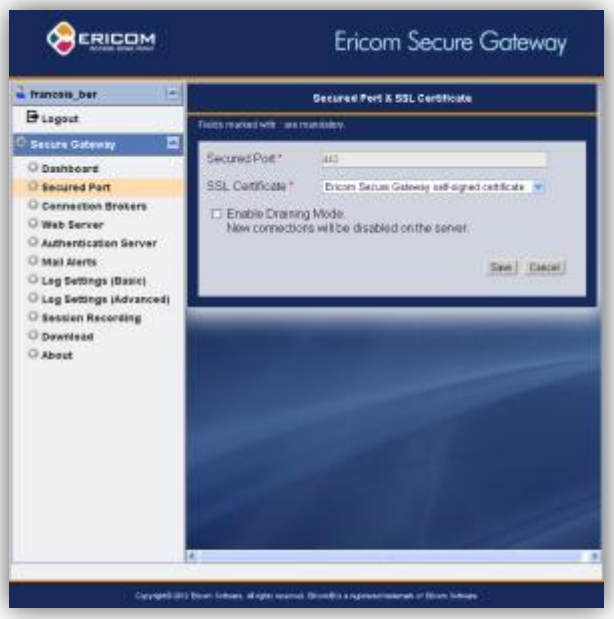

Ericom Secure Gateway - InstallShield Wizard
Ericom Authentication Server Configuration
Select the Authentication Method
No authentication required
Use local Authentication Server
Authentication Port:
444
Use Remote Authentication Server
Authentication Server Address:
localhost
Authentication Port:
444
NOTE: Ericom Authentication Server MUST be installed on a domain member server, unless the Secure Gateway is used by WebConnect products only.
InstallShield
< Back
Next >
Cancel

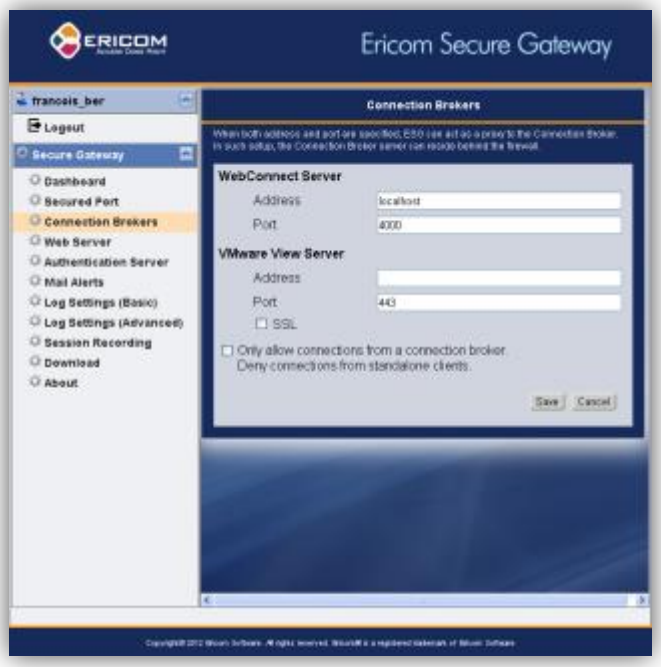

Connection Broker Selection
PowerTerm WebConnect
VMware View
Only allow connections from a connection broker. Deny connections from standalone clients
InstallShield
< Back
Next >
Cancel

Après l'installation nous pouvons accéder à l'interface d'administration du Secure Gateway à l'adresse du serveur en **https**

➔ https://10.0.0.99/Admin/Login.html

Nous retrouvons ici toutes les informations que nous avons précédemment configurées, l'activité moyenne du Secure Gateway ainsi que tous les logs de connexion

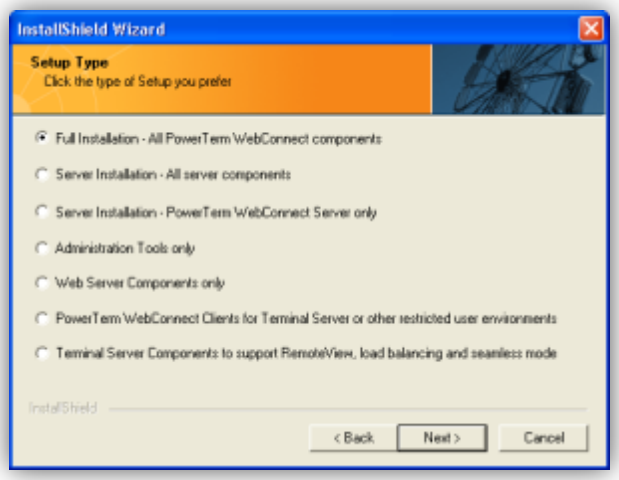

ERICOM
Ericom Secure Gateway
francois_ber
Logout
Secure Gateway
Dashboard
Secured Port
Connection Brokers
Web Server
Authentication Server
Mail Alerts
Log Settings (Basic)
Log Settings (Advanced)
Session Recording
Download
About
Secured Port & SSL Certificate
Secured Port *
SSL Certificate *
Enable Draining Mode
New connections will be disabled on the server.
Save
Cancel


ERICOM
Ericom Secure Gateway
francois_ber
Logout
Secure Gateway
Dashboard
Secured Port
Connection Brokers
Web Server
Authentication Server
Mail Alerts
Log Settings (Basic)
Log Settings (Advanced)
Session Recording
Download
About
Connection Brokers
WebConnect Server
Address
localhost
Port
4000
VMware View Server
Address
Port
443
SSL
Only allow connections from a connection broker
Deny connections from standalone clients.
Save
Cancel

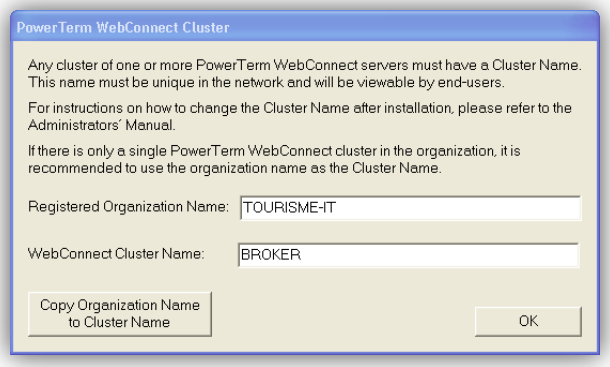
ERICOM
Ericom Secure Gateway
francois_ber
Logout
Secure Gateway
Dashboard
Secured Port
Connection Brokers
Web Server
Authentication Server
Mail Alerts
Log Settings (Basic)
Log Settings (Advanced)
Session Recording
Download
About
Authentication Server
Enabled
Address
localhost
Port
444
Save
Cancel

5.2.3 Installation du Server Powerterm Webconnect

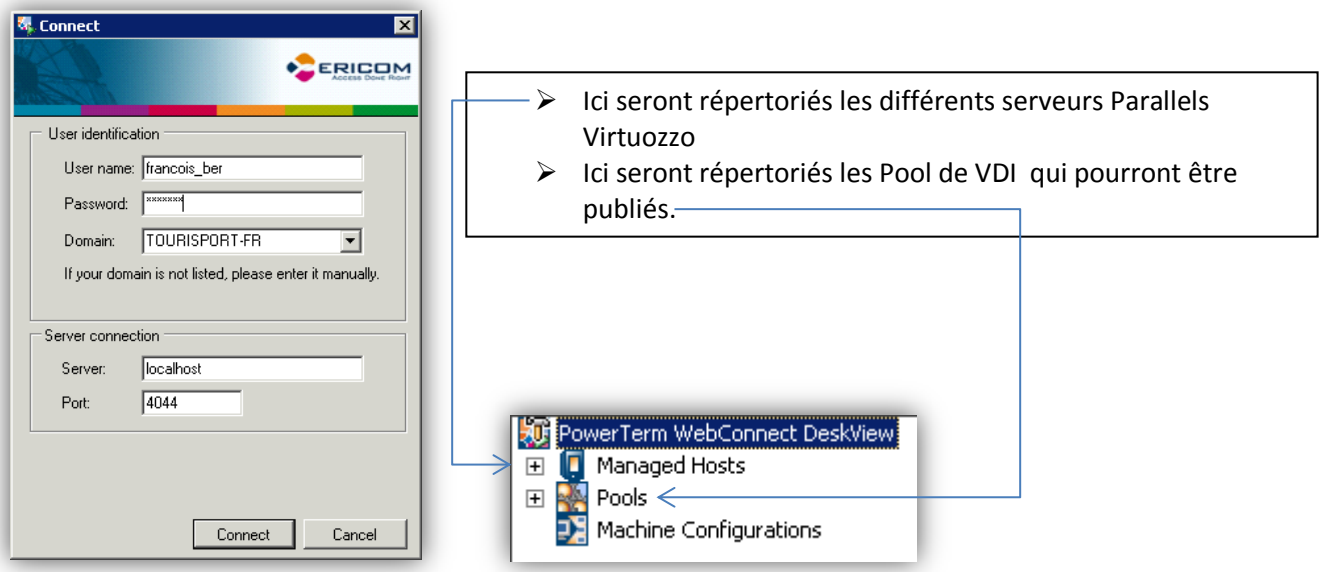
L'installation se fait à partir de l'exécutable **ptdj.exe** téléchargeable sur le site web d'Ericom.
Cliquer sur « **Evaluate** » pour utiliser le serveur sans licence, puis choisir installation complète.



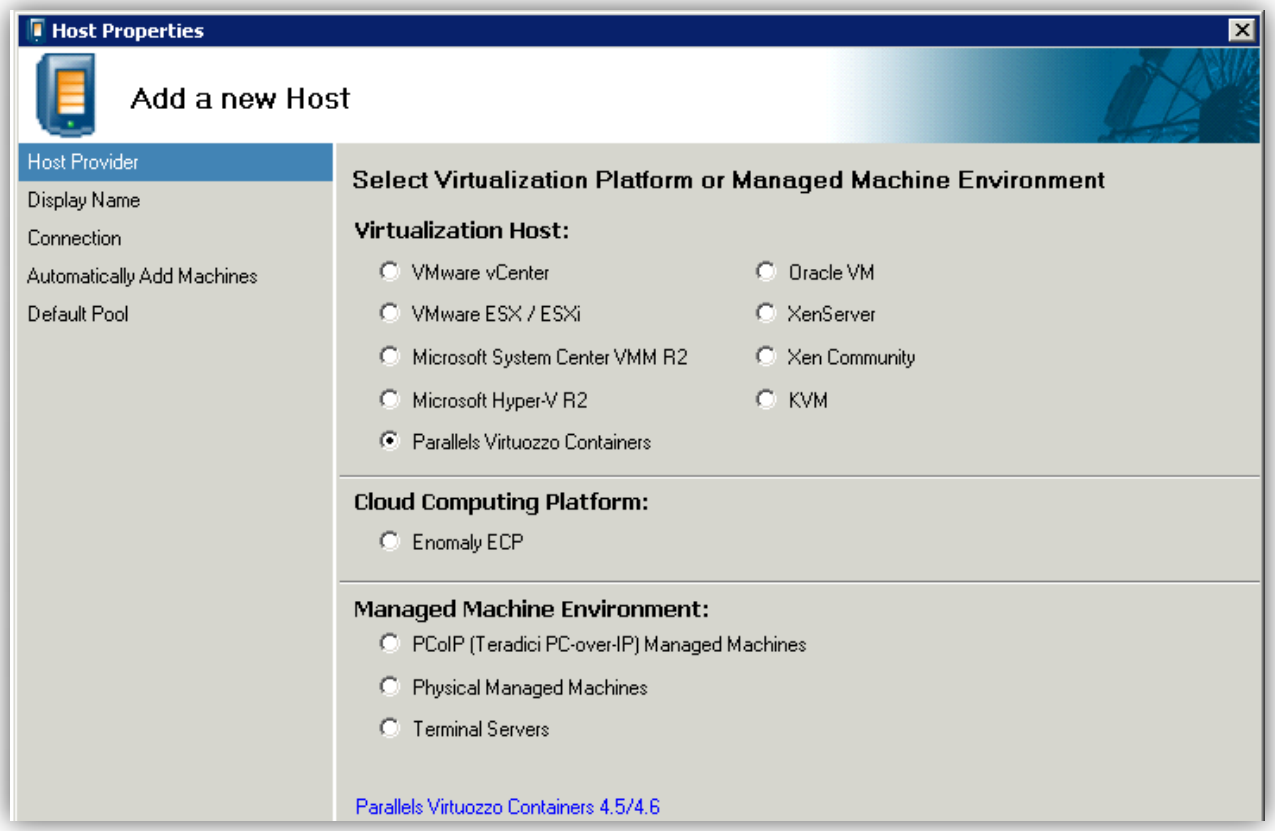
Le setup d'installation demandera ensuite d'activer ASP, puis configurer ensuite le nom du cluster.



Nous allons en premier démarrer sur la console d'administration du Broker, ici nous allons devoir créer notre « Ferme » de serveurs VDI.

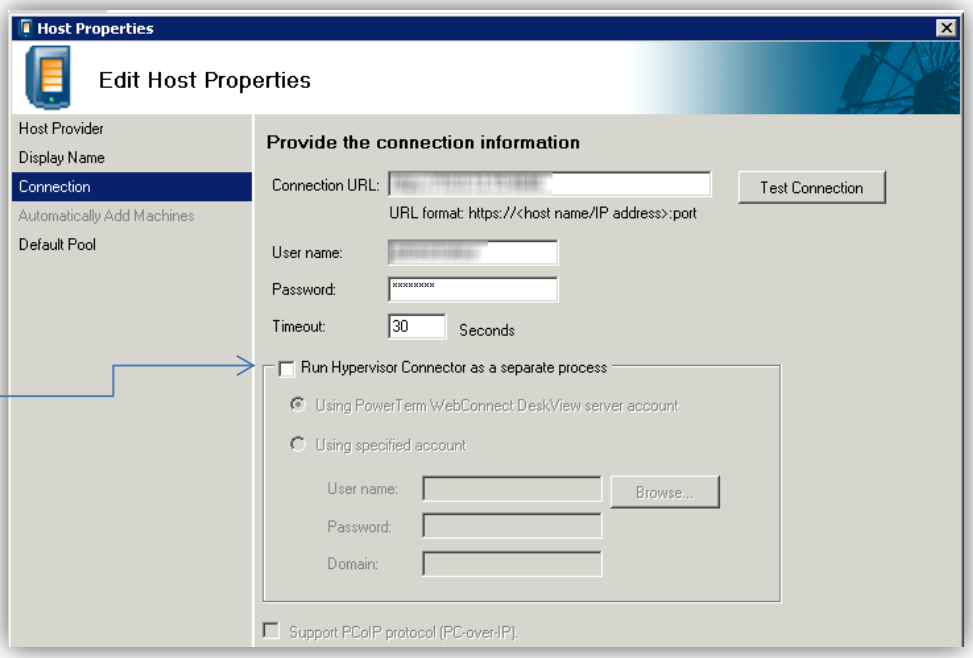


Nous allons ajouter 2 serveurs Parallels (1 Marseille + 1 Montpellier)

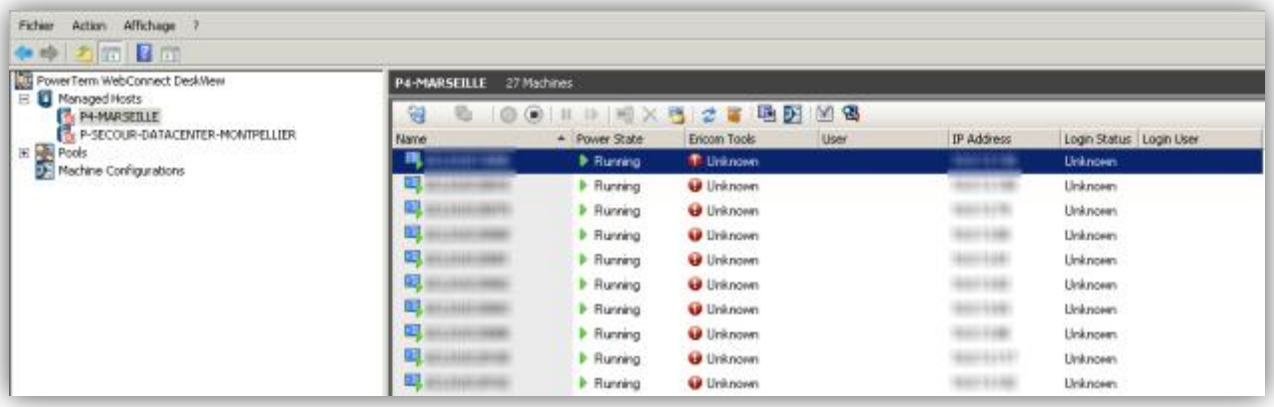


Il faut ensuite configurer les paramètres réseaux du serveur ainsi que l'authentification de l'administrateur.

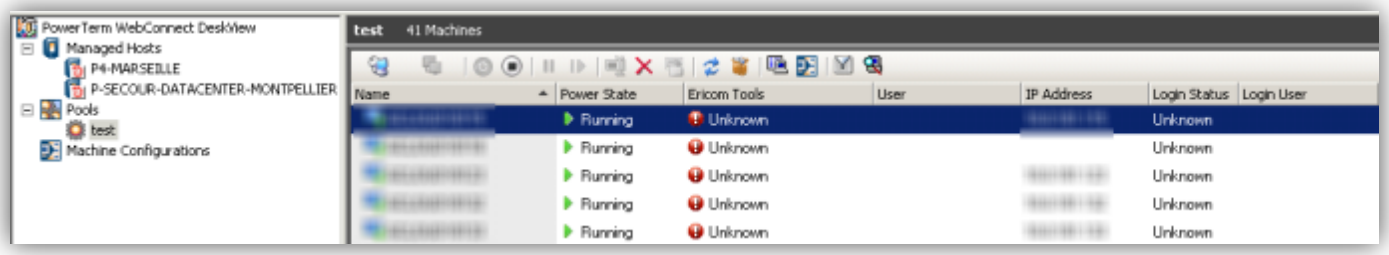
Ne pas cocher « Run Hypervisor …» en effet après les premiers tests, cette fonction empêche la remontée des informations du client installé sur chaque contenaire.



Nous avons maintenant nos deux serveurs de VDI ainsi que les différents contenaires actifs sur chacun d'eux.

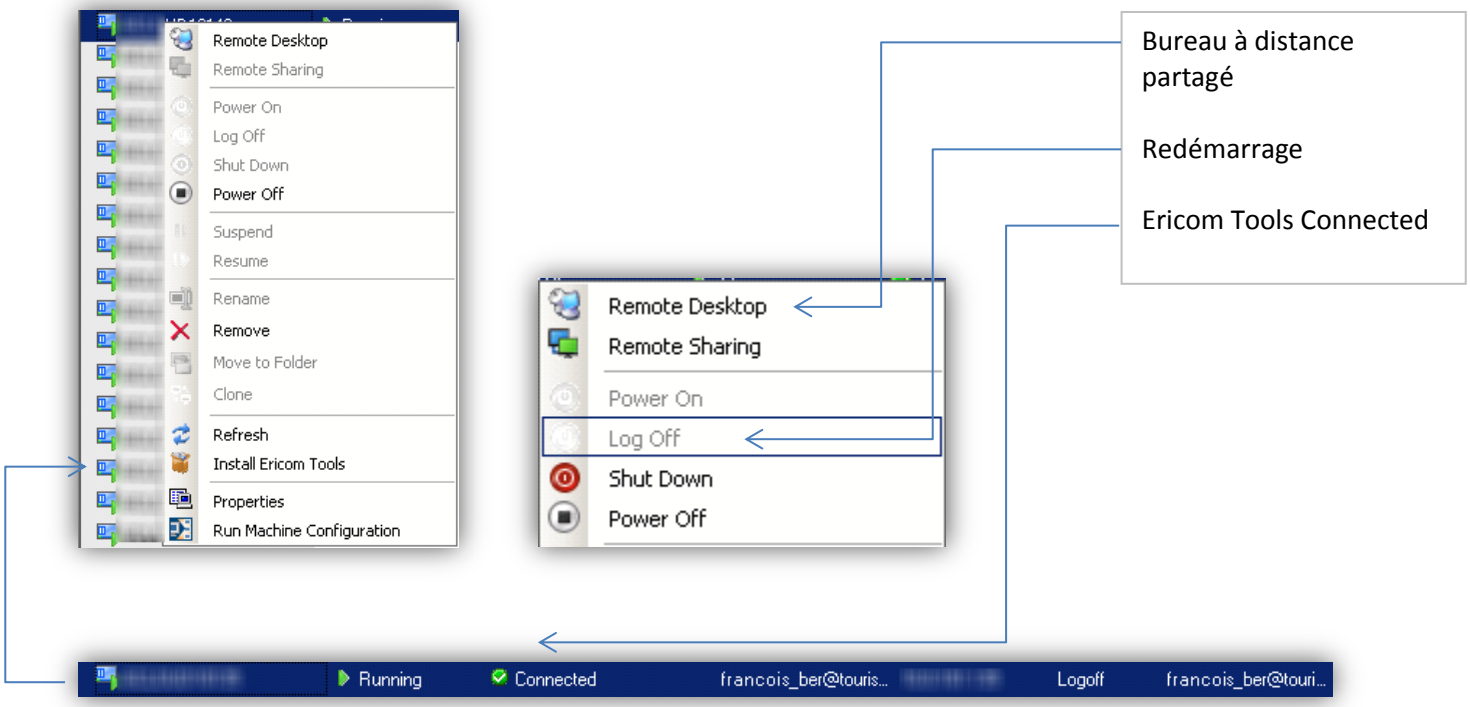


Nous allons maintenant créer un pool test qui comprendra tous les contenaires des 2 serveurs.

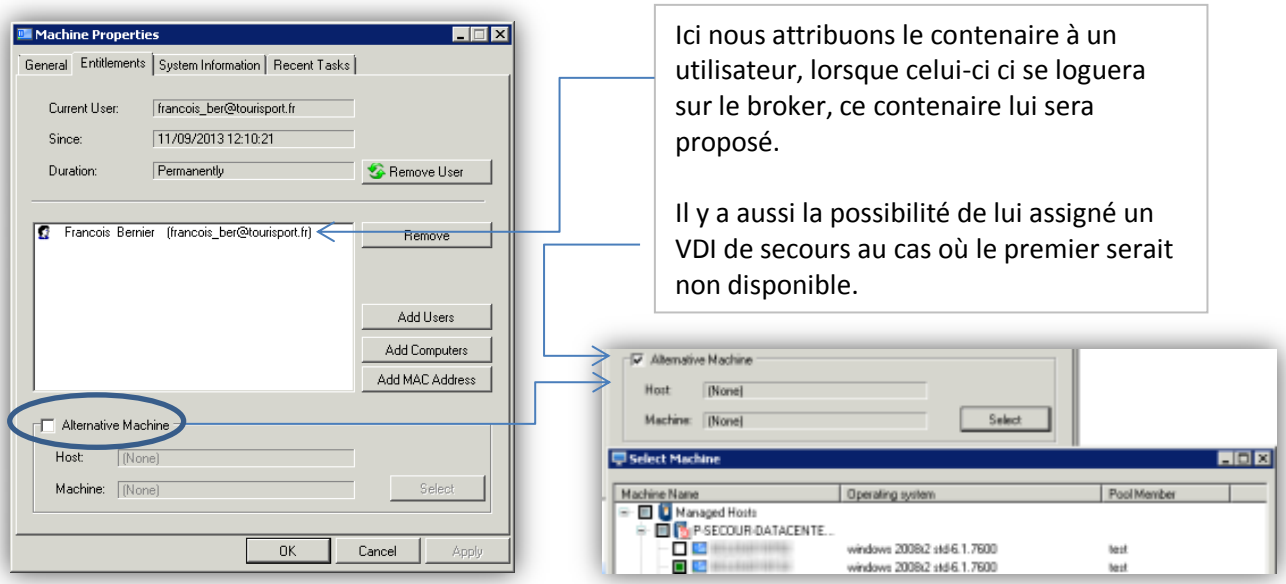


Pour pouvoir avoir un contrôle total sur les contenaires, nous devons y installer un agent, ce qui nous permettra d'obtenir :

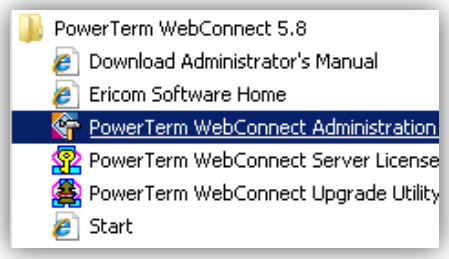
- Les informations de connexion des utilisateurs
- La possibilité d'arrête ou de redémarrer un contenaire
- La possibilité de prendre en main à distance en partagé le contenaire à partir de l'interface du Broker



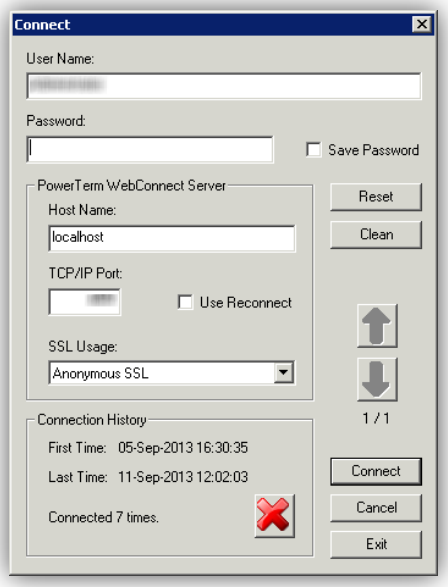
Nous pouvons dorénavant attribuer un contenaire à un utilisateur, cliquer sur l'option « propriété » du contenaire.

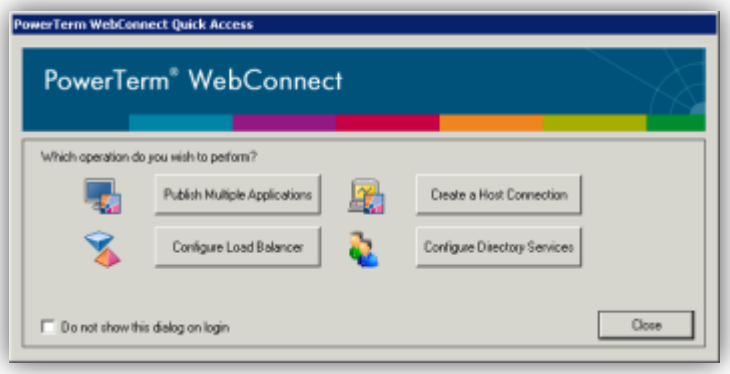


Nous allons maintenant publier ce contenaire, pour cela nous devons nous rendre sur l'interface Powerterm Webconnect.

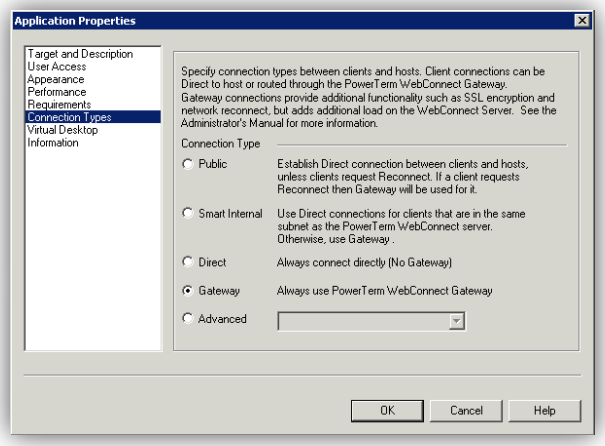


Nous devons d'abord nous authentifier, puis fermer la fenêtre d'accueil.

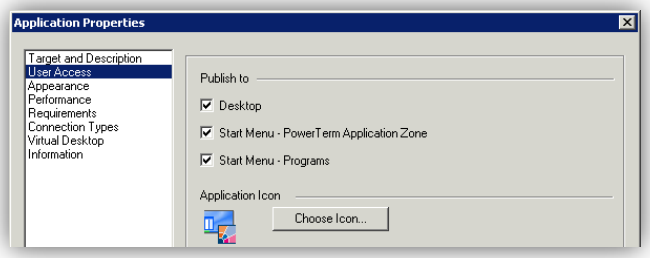




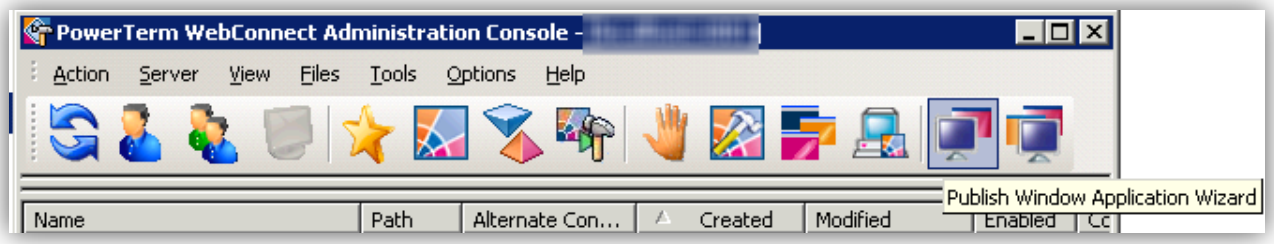
Nous voyons apparaitre notre pool test, cliquer sur ses propriétés et sélectionner le mode de connexion Gateway



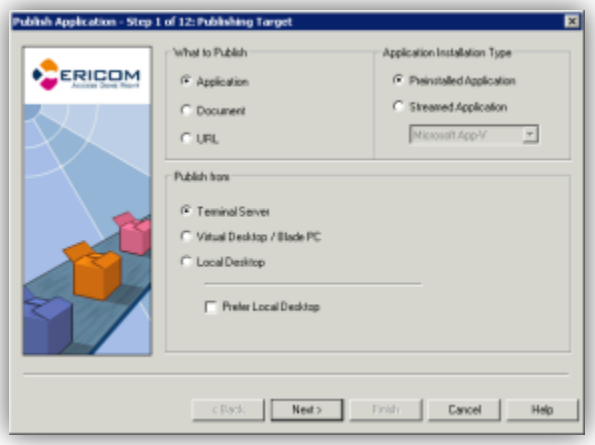
Sélectionner également User Access et cocher les trois options, ce qui permettra de créer le raccourci direct vers le contenaire et les applications dans le menu démarrer et le bureau de l'utilisateur.

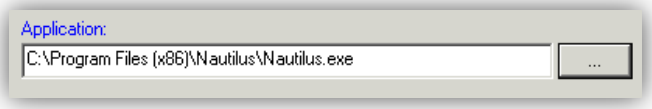


Nous allons également pouvoir publier une application avec cette solution.
Dans le menu principal nous allons sélectionner l'option « Publish Window Application Wizard »

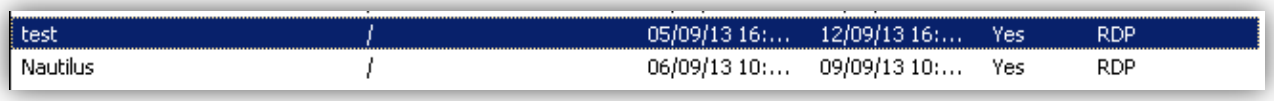


Sélectionner Application et Terminal Server, puis choisir l'emplacement de l'application à publier et le mode de connexion par « Gateway » comme précédemment.



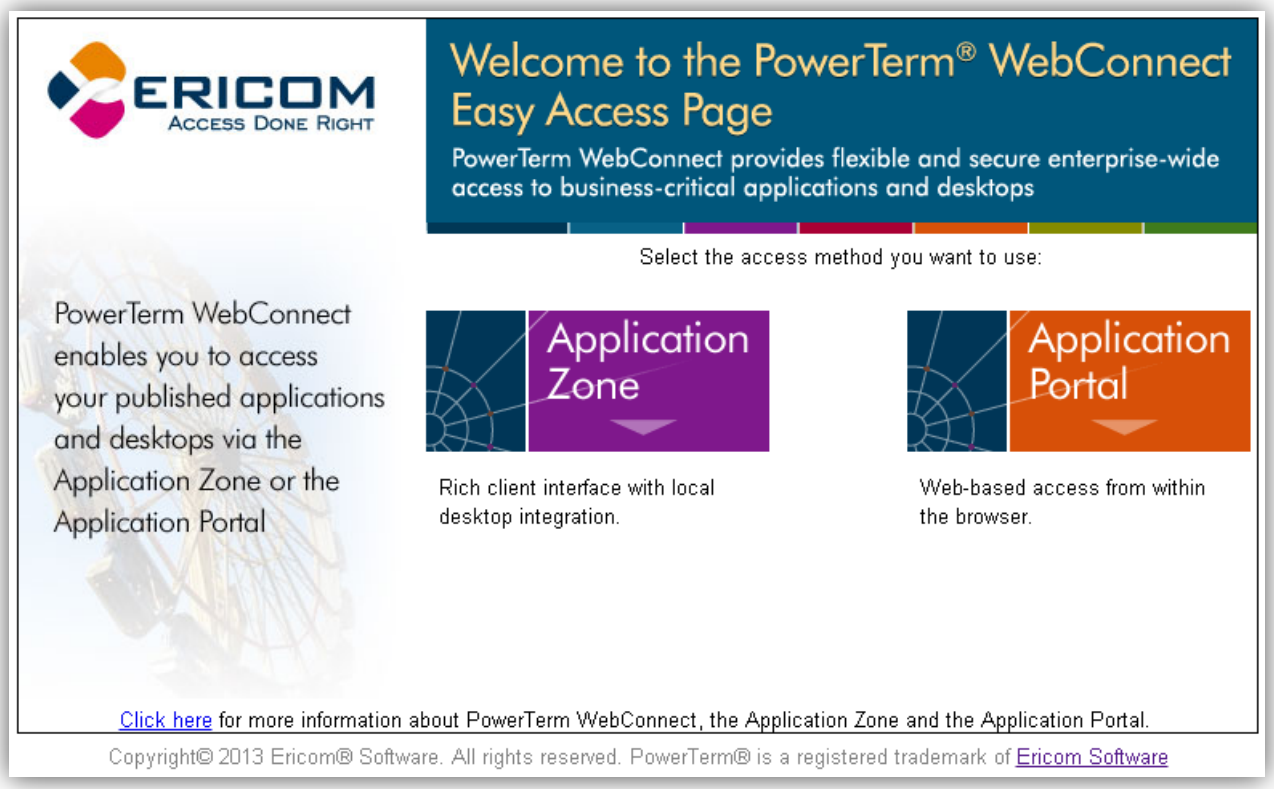


L'application est maintenant disponible dans la liste des publications.

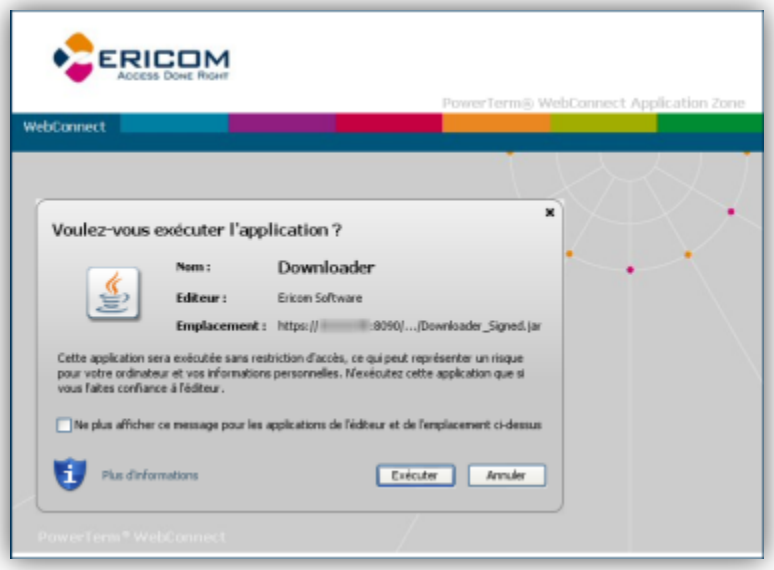


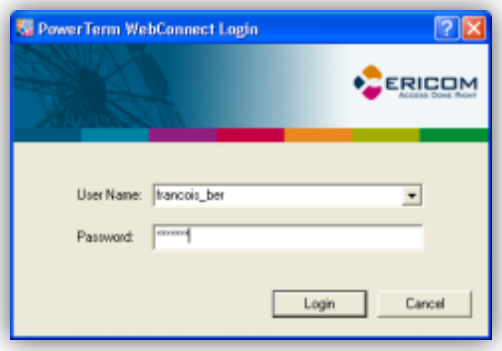
test	/	05/09/13 16:...	12/09/13 16:...	Yes	RDP
Nautilus	/	06/09/13 10:...	09/09/13 10:...	Yes	RDP

Nous pouvons maintenant tester l'accès à notre portail à l'adresse **https://serveur:8090/WebConnect5.8**

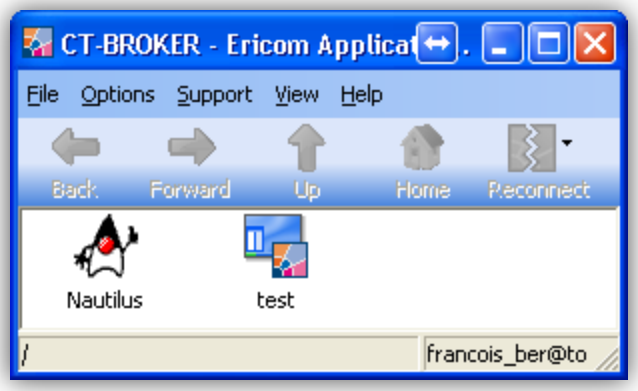


Cliquez sur application Zone, les paramètres de sécurité vous demanderont d'autoriser l'exécution de l'applet Java.





Et nous accédons au client Powerterm Webconnect, nous pouvons tester si le contenaire disponible correspond bien à celui programmé pour cet utilisateur.



La connexion est bien établie sur le contenaire que nous avions dédié à cet utilisateur.

Nous pouvons également tester l'accès à l'application Nautilus

5.2.4 Conclusion sur la Solution ERICOM Powerterm Webconnect

Cette solution semble la plus mature de toute et fournis les besoins nécessaires au SI de Tourism-It.
Le client Ericom s'installe en tache de fond sans la moindre intervention de la part de l'utilisateur.
La compatibilité avec l'infrastructure est totale et les consoles d'administration sont très bien conçues apportant une grande facilité de gestion pour l'administrateur.
Après avoir pris contact avec le service Commercial d'Ericom voici le devis qu'il m'a fourni pour 100 utilisateurs.

Hello Francois,

Thank you for your interest in Ericom's solution.

The specific Ericom solution you require is called PowerTerm WebConnect (PTWC) RemoteView which supports your requirement of Parallels Virtuozzo, RDP acceleration, and seamless mode. (the free version of PTWC WS08 R2 does not support the above)

Our offer for 99 concurrent users:

PowerTerm WebConnect RemoteView			
Quantity	**Upgrade price per license**	**annual maintenance per user**	**Total**
99	€ 113.00	€ 20.34	€ 13,200.66

A valid maintenance contract allows you to receive technical support as well as free upgrades to latest versions of the purchased product.

Please advise when you would like to place the order?

Good luck,
Malka

Malka Wormser
Regional Sales Manager EMEA
Ericom Software Ltd.
http://www.ericom.com

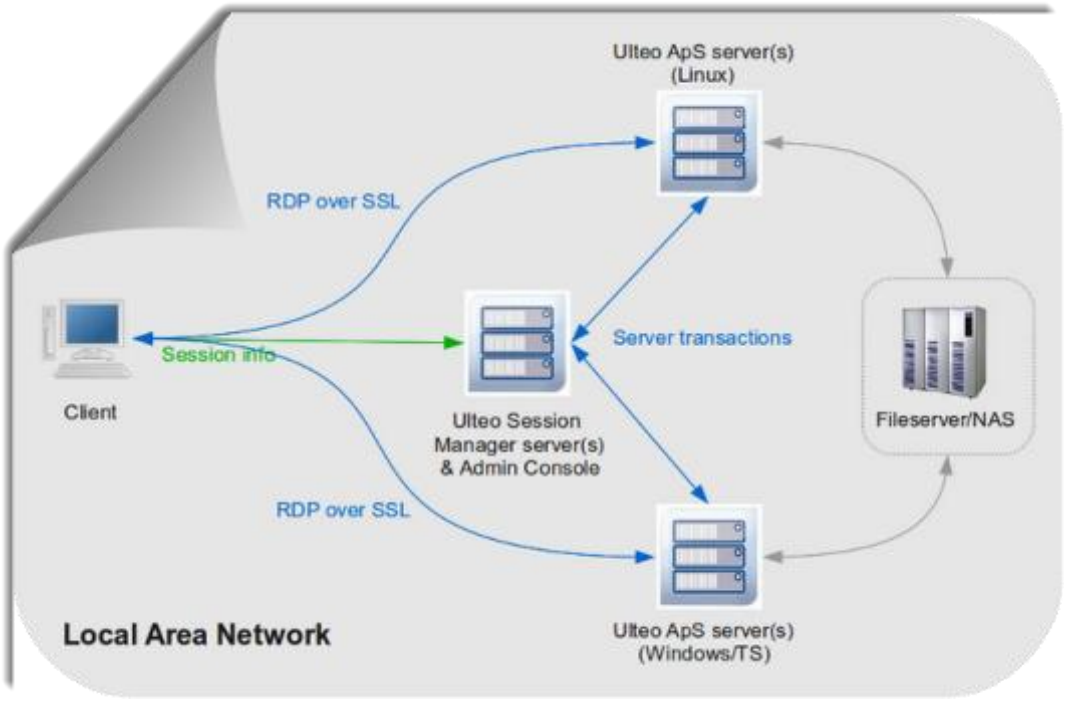
5.3 Compte rendu de Réunion de présentation des solutions à l'administrateur Cloud le 11 Septembre 2013

J'ai pu présenter l'ensemble de mon travail à l'Administrateur Cloud, nous avons ainsi évalué les pours et les contres de chaque solution et avons décidé de mettre en **Pré-production** la version Ulteo pour le serveur d'application.

Concernant le RDP BROKER les solutions 2xApplicationServeur et Ericom Powerterm correspondent aux besoins de l'administrateur Cloud, ces solutions représentants un investissement important, elles seront soumises à un futur projet sur 2014.

6 Mise en Pré-Production de la solution Ulteo

Comme nous avons vu précédemment, l'infrastructure de la version OpenSource Ulteo est la suivante



Pour pouvoir accéder de l'extérieur aux deux serveurs, nous devons créer des règles NAT de redirection sur un des routeurs de l'infrastructure pour le serveur Session Manager et pour le serveur Windows/TS.

Le serveur Linux → Session Manger sera accessible à partir de l'adresse **go.geophyle-XXX:XXXXX**
Le trafic arrivant sur cette adresse sera donc routé vers notre serveur sur le port **443**, correspondant à l'adresse **https://session-manager/**

Pour arriver sur la page d'authentification il faudra donc saisir l'adresse : **http://go.geophyle-XXX:XXXXX/ovd**

Après différents tests approfondis, la solution ULTEO fonctionne correctement en adéquation avec le cahier des charges qui m'a été donné.

La **mise en production** finale a été décidée le **19 Septembre 2013** et doit ainsi être opérationnelle le **25 Septembre** pour être livrable aux différentes agences du groupe Geophyle.

L'administrateur Cloud m'a donc demandé de préparer les éléments suivants :

- Rédiger une documentation de l'installation des serveurs Session Manager et Serveur d'application TSE (Procédure d'installation en annexe des documents fournis)
- Réaliser une procédure de sauvegarde via un script des bases de données du Session Manager ainsi que de l'interface Web.

6.1 Procédure de sauvegarde des données du Serveur Session Manager

Le script ci-dessous permet de sauvegarder l'ensemble des bases de données d'ULTEO Manager ainsi que le répertoire ou est stockée l'interface web.

Nous créons un Script exécutable qui génèrera le fichier compressé :

```
root@ovd:/# mkdir BACKUP
```

```
root@ovd:/# cd /etc/init.d
```

```
root@ovd:/etc/init.d# vi backup-ulteo.sh
```

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin

date1=$(date +%d-%m-%y--%Hh%M)

tar -cvf /BACKUP/ulteo-backup.$date1.tar /usr/share/ulteo

mysqldump -u root -p[redacted] --all-databases | gzip > /BACKUP/ulteo-databases.$date1.sql.gz
~
~
~
```

Mot de passe **root** MysQl

Créer maintenant une commande de programmation du service « **crontab** »

En mode terminal éditer le fichier « **crontab** » de l'utilisateur **root**

Crontab –e

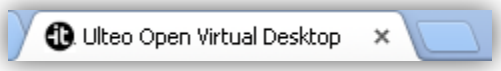
Insérer le code suivant :

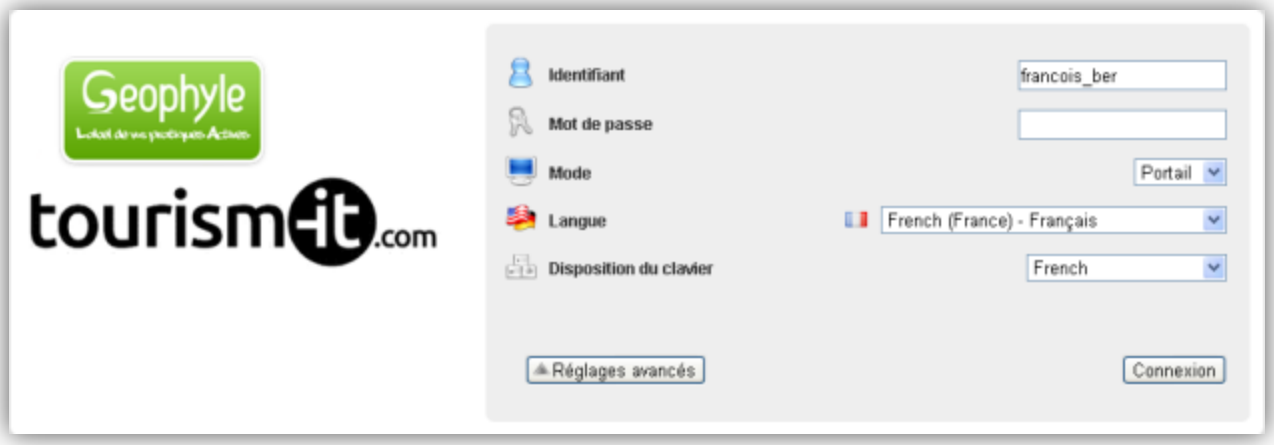
0 3 * * * sh /etc/init.d/backup-ulteo.sh

Le script que nous avons effectué précédemment sera exécuté tous les jours à 3h00

Le nom des fichiers sera formaté comme ci-dessous :

J'ai pu également modifier les logos de la page d'accueil du client web pour qu'ils correspondent à la société :





7 Annexes

7.1 Propositions des solutions de projet au SI de Tourism-It

Propositions de solutions de Connection Broker et de Serveur d'applications

Projets de Stage BERNIER Francois AFPA TSGERI 2013

BERNIER Francois Projet de stage TSGERI 2013 francois@bernier-family.fr
TEL :06-10-31-68-93 http://superghost.fr

Table des matières

I. **Synthèse** 2

II. **Description des offres présentes sur le marché** 4

Contraintes

Offres

III. **Solutions Préconisées** 5

Synthèse

Avec l'avènement de la virtualisation, l'idée est de porter le poste de travail sur des environnements virtuels pour obtenir le meilleur des deux mondes.
Cela permet de centraliser la gestion des postes, de réduire le TCO (*Total Cost of Ownership*, traduisez *Coût total de possession*) , d'avoir une meilleure sécurité des données et de réduire les ressources employées.

Afin de pousser la corrélation entre les deux architectures (poste physique et serveur de terminaux), le VDI (Virtual Desktop Infrastructure) intègre un composant permettant de désolidariser la gestion de l'utilisateur du au poste de travail virtuel.

Ce composant est une application chargée d'associée un poste de travail virtuel lambda à un utilisateur précis. Appelée Connection broker, elle permet de faire le lien entre les profils utilisateurs (stockés dans l'annuaire) et un pool de postes de travail virtualisés. Il n'est donc pas nécessaire d'attribuer un poste de travail virtuel à chaque utilisateur (bien que cela reste faisable).

Connexion Broker

Le but de Connection Broker est de répartir la charge au sein d'une ferme TSE (Terminal Server) en redirigeant au besoin les nouvelles connexions vers le serveur le moins chargés.

On distingue 2 parties pour le fonctionnement de Connexion Broker:

- La partie équilibrage de charge avec (NLB (Network Load Balancing , le tourniquet DNS, où des produits tiers)
- L'orientation de la session utilisateur en fonction de la charge des serveurs où si c'est une session déconnectée

Serveur d'applications

Un serveur d'applications est un logiciel d'infrastructure offrant un contexte d'exécution pour des composants applicatifs. Le terme est apparu dans le domaine des applications web. Dans un sens strict les composants hébergés par le serveur d'applications ne sont pas de simples procédures ou scripts mais de réels composants logiciels conformes à un modèle de composants (EJB, COM, Fractal, etc.).

Les clients des serveurs d'application sont : des programmes autonomes (stand alone application), des applets ou d'autres composants.

La structuration en couches des différents composants mis à disposition par le serveur d'application permet une prise en compte des besoins métier, des interactions avec les utilisateurs, des connexions avec les bases de données, etc.

Les serveurs d'applications sont des logiciels occupant la couche centrale dans une architecture multicouche, qu'elle soit classique 3-tiers (postes clients, serveur d'applications, serveur de données) ou étendue (n-tiers) lorsqu'elle intègre par exemple des serveurs d'acquisition (données de terrain, données de process, de back-office, etc.) et/ou des serveurs d'interface (gateways, systèmes coopérants externes, etc.).

Dans un sens plus large, un serveur d'application peut être une machine servant à héberger des applications soit pour permettre leur exécution depuis un poste client (mode client serveur de données, généralement partage de fichiers et politiques de gestion des accès) ou pour déporter l'affichage sur le poste client (mode client serveur d'affichage).

Tourniquet DNS : technique **tourniquet DNS (Round robin) qui vous** permet d'inscrire dans le DNS plusieurs adresses IP pour un même nom d'hôte. Une fois cette fonction activée, le serveur DNS va séquentiellement renvoyer aux clients faisant une demande de résolution de nom sur cet hôte une adresse réseau différente.

Description des offres présentes sur le marché

Contraintes

- Compatibilité Windows Server 2008 R2

- Compatibilité Authentification ACTIVE DIRECTORY WINDOWS

- Compatibilité possible avec Parallels Vituozzo (déploiement des conteneurs à partir du Broker)

- Répartition des conteneurs et LoadBalancing (Répartition de charge)

- Coût réduit

- Monitoring, Reporting

- Prise en charge des Imprimantes, disques locaux….(Local Desktop Interactions)

Offres

Voici la description des différentes offres rencontrées

Connexion Broker

	Support Windows Server 2008 R2	LDAP	Compatibilité Parallels Virtuozzo	Monitoring Reporting	Load Balancing	Local Desktop Interactions	Coûts Licenses
Powerterm Webconnect connection broker	OUI	OUI	OUI	OUI	OUI	OUI	139$ / Utilisateurs ~ 42000 €
Ulteo OVD3	OUI	OUI	NON	OUI	OUI	OUI	Gratuit /Open Source
2X Applications Server	OUI	OUI	OUI	OUI	OUI	OUI	Pour serveur < 160 utilisateurs 5150 € à 16000 €
vWorkspace	OUI	OUI	OUI	OUI	OUI	OUI	169$ / Utilisateurs ~ 51000 $
Windows Session **Broker** TS	OUI	OUI	NON	NON	OUI	OUI	CAL Windows
PROPALMS VDI	OUI	OUI	OUI	OUI	OUI	OUI	???????

Serveurs d'applications

	Support Windows Server 2008 R2	LDAP	Compatibilité Parallels Virtuozzo	Monitoring Reporting	Load Balancing	Local Desktop Interactions	Coûts Licenses
Ulteo OVD3	OUI	OUI	NON	OUI	OUI	OUI	Gratuit /Open Source
2X Applications Server	OUI	OUI	OUI	OUI	OUI	OUI	Pour serveur < 160 utilisateurs 5150 € à 16000 €
WINDOWS REMOTE APP	OUI	OUI	NON	NON	OUI	OUI	CAL WINDOWS

Solutions Préconisées

Les Quatre solutions retenues sont :

- **Windows Remote App Server** pour sa parfaite compatibilité avec l'infrastructure existante et les licences utilisateurs déjà acquises. (Uniquement pour le serveur d'applications)
- **Ulteo OVD3** pour sa solution Open source incluant les futures évolutions des ressources offertes aux utilisateurs (Serveurs d'applications pour Nautilus et Locomotion).
  Actuellement en négociation avec la société Ulteo pour pouvoir tester certains module de la solution nécessaires à nos besoins. (Serveur d'applications et eventuellement Connection Broker)
- **2X Applications Server** Pour le faible coût de la licence , sa compaibilité avec Parallels Virtuzzo et la possibilité de faire fonctionner le Connection Broker et le serveur d'application avec la même solution. (Serveur d'applications et Connetion Broker)
- **Powerterm Webconnect** pour sa compatibilité avec la technologie de contenaires Virtuozzo. (Connection Broker et eventuellement Serveur d'applications)

7.2 Missions en cours de stage

Dans le cadre de mon stage au sein de Tourisme et Services j'ai eu à effectuer seul ou en collaboration avec l'administrateur réseau, Nicolas Paugam, divers missions.

Dans cette section, je détaillerais les actions suivantes :

- Installation d'un serveur ProLiant DL360P G8 au sein du Datacenter de Montpellier
- Pré configuration et installation d'un SWICTH CISCO Catalyst 2960
- Installation et Configuration d'un Téléphone IP THOMSON ST2030
- Installation et Configuration d'un poste Client DELL OPTIPLEX 3010

7.2.1 Datacenter

Installation d'un Serveur Proliant DL360P G8

DATACENTER NEO TELECOMS Montpellier

Dès mon entrée en stage, Nicolas Paugam, Administrateur Cloud m'a invité à effectuer l'installation d'un nouveau serveur au sein du Datacenter NEO TELECOM de Montpellier. Ce nouveau serveur sera dédié à la délivrance de contenaires Parallels Virtuozzo aux utilisateurs du groupe Geophyle.

Le Datacenter

Depuis 2008, le Neo Center de Montpellier est le Datacenter privilégié des hébergeurs du Languedoc-Roussillon. Réputé pour sa haute disponibilité, sa connectivité et son bilan énergétique, il répond aux contraintes d'exploitation des entreprises les plus exigeantes.

Le Datacenter a été conçu autour de la norme Tier III+ (entre la norme Tier III et la norme Tier IV). L'ensemble de la conception, des installations techniques et de la maintenance répondent aux contraintes techniques de cette norme.

Elle garantit aux clients que les services fournis par le Data Center ont un niveau de disponibilité de 99,99% (garantit contractuellement).

Le serveur

Serveur HP ProLiant DL360p Gen8

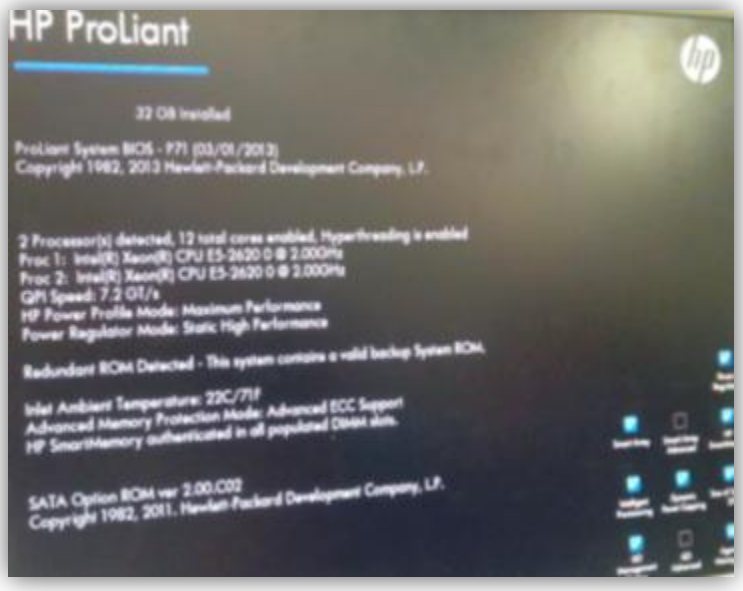
Serveur de classe d'entreprise, le serveur HP ProLiant DL360p Gen8 offre des performances de pointe 2 sockets dans l'industrie et une grande efficacité dans un format 1U peu encombrant. Avec la facilité améliorée et la flexibilité de configuration de Gen8, ce serveur est idéal pour des applications générales comme fichier/imprimer ou web, ainsi que pour les charges de travail dynamiques, la virtualisation et les solutions Cloud.

Les machines intègrent maintenant sur un stockage dédié tous les éléments nécessaires au déploiement, ce qui permet de réduire par trois le temps de mise en route, et affranchit l'administrateur de la contrainte des CD ou DVD d'installation (Intelligent Provisioning). Les ProLiant Gen8 embarquent par ailleurs un nouveau système de monitoring, appelé HP Active Health, permettant de surveiller en temps réel quelque 1 600 paramètres systèmes et donc d'accélérer le diagnostic s'il n'est pas possible de résoudre automatiquement le problème.

Caractéristiques techniques :

- Processeurs: 2x Intel® Xeon® E5-2620 (6 cœurs, 2,00 GHz, 15 Mo, 95 W)
- Mémoire, standard: 32 Go (4x8 Go) RDIMM
- 4 x Disque dur SAS: SFF HP 600 Go, 6 Gb/s, 10 000 tr/min à petit facteur de forme (2,5 pouces) SC Enterprise

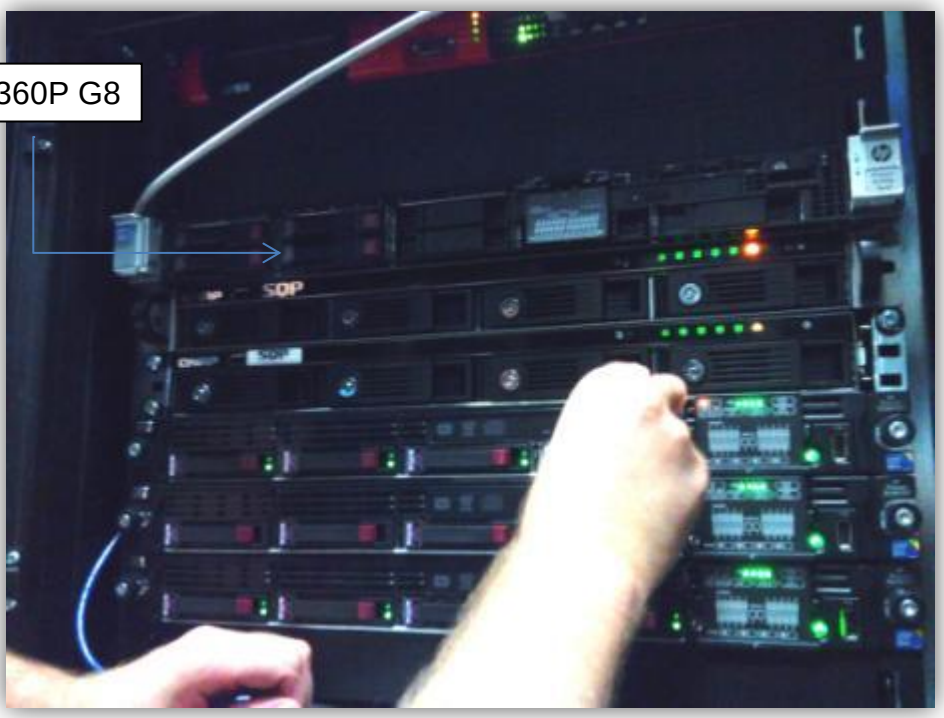
Démarrage du serveur



En premier l'administrateur a effectué la configuration réseau du serveur en 10.0.xxx.xxx/24 et ensuite installé le système d'exploitation Windows Server 2008 R2 Standard.

Il m'a ensuite demandé de câbler les sorties Ethernet du serveur sur le switch présent en respectant l'ordre de sortie du serveur vers le switch pour que les techniciens du Datacenter puissent créer les connexions aux VLANS.

DL360P G8



Port ILO

Connections coté Serveur

Connections coté Switch

J'ai ensuite relié le port ILO du serveur au Switch.

Le produit HP iLO Management Engine est un ensemble complet de fonctionnalités de supervision qui permet de gérer le cycle de vie intégral du serveur, à partir du déploiement initial, jusqu'aux alertes de service et à la prise en charge à distance, en passant par la gestion continue.
HP iLO est une fonctionnalité du moteur de gestion HP iLO.
Le sous-système HP iLO est un composant standard des serveurs HP ProLiant, qui simplifie la configuration du serveur initial, la surveillance du bon fonctionnement du serveur, l'optimisation de l'alimentation et de la température, ainsi que l'administration du serveur à distance. Le sous-système HP iLO comprend un microprocesseur intelligent, une mémoire sécurisée et une interface réseau dédiée. Cette conception permet à HP iLO d'être indépendant du serveur hôte et de son système d'exploitation.
HP iLO permet d'activer et de gérer le système de santé actif et offre une gestion sans agent.
HP iLO surveille tous les sous-systèmes clés internes.
Une fois activées, les alertes SNMP sont directement envoyées à HP iLO, quel que soit le système d'exploitation de l'hôte ou si un tel système est installé.
Le logiciel HP Insight Remote Support est également disponible sur les serveurs HP ProLiant Gen8 avec iLO 4, quel que soit le logiciel du système d'exploitation et sans nécessiter d'autre logiciel, driver ou agent de l'hôte.

Fonctions de HP iLO

HP iLO permet de réaliser les tâches suivantes :

• Accès à la console sécurisée hautes performances Integrated Remote Console (Console distante intégrée) par le serveur depuis n'importe quel endroit dans le monde si vous disposez d'une connexion réseau au serveur.

Il existe deux versions de la console distante intégrée :

- IRC .NET
- IRC Java

Les références générales à la console distante s'appliquent à la fois à .NET IRC et Java IRC, sauf indication contraire.

• Utilisation de la solution .NET IRC partagée pour collaborer avec jusqu'à quatre administrateurs de serveur.
• Montage distant de périphériques Virtual Media hautes performances sur le serveur.
• Contrôle sécurisé et distant de l'état d'alimentation du serveur supervisé.
• Implémentation d'une vraie supervision sans agent avec des alertes SNMP depuis HP iLO, quel que soit l'état du serveur hôte.
• Accès aux fonctions de résolution des problèmes d'Active Health System au moyen de l'interface Web HP iLO.
• Inscription au logiciel HP Insight Remote Support sans installer de drivers ou d'agents.
• Utilisation de Virtual Power (Alimentation virtuelle) et Virtual Media (Support virtuel) à partir de l'interface graphique, de l'interface de ligne de commande (CLI) ou de la boîte à outils de génération de scripts iLO pour de nombreuses tâches, y compris l'automatisation du déploiement et de l'approvisionnement.
• Contrôle de l'état du serveur. iLO surveille les températures au niveau du serveur et envoie des signaux de correction aux ventilateurs afin de maintenir un niveau de refroidissement correct du serveur. iLO surveille également les versions de microprogramme, ainsi que l'état des ventilateurs, de la mémoire, du réseau, des processeurs, des alimentations et du stockage interne.
Fonctions de HP iLO 13• Utilisation de comptes d'utilisateurs locaux ou basés sur le répertoire pour connexion à iLO.
• Utilisation de modules de langue iLO pour basculement entre l'anglais et une autre langue prise en charge.
• Configuration de l'authentification Kerberos, ce qui ajoute le bouton HP Zero Sign In à l'écran de connexion.
• Surveillance de la consommation d'énergie et des paramètres d'alimentation du serveur

Configuration Windows Server 2008

- Réglage de la mémoire virtuelle à 50 Go
- Jonction au domaine tourisport.fr et configuration du nom du serveur

Configuration HP Lights Out Online

- Ajout d'un utilisateur Administrateur
- Configuration de l'interface ILO :
  - IP
  - Netmask
  - Gateway
  - DNS name
- Connexion ILO en **https**

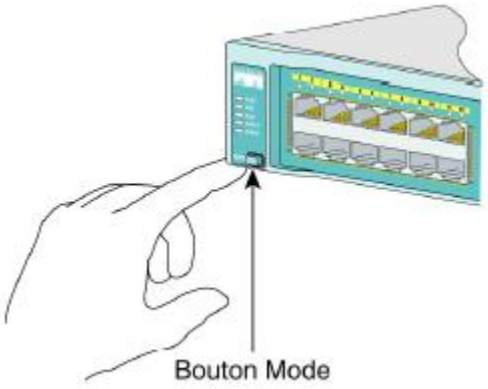
Le serveur est dorénavant prêt, l'administrateur devra installer à distance un serveur Parallels Virtuozzo dès notre retour à Marseille.

7.2.2 Pré configuration et installation d'un SWICTH CISCO Catalyst 2960

Afin de remettre à niveau une baie de brassage de la société Huwans , l'administrateur Cloud m'a donné pour mission de reconfigurer un switch CISCO Catalyst 2960 et de le mettre en production .

7.2.2.1 Configuration

Le switch ayant déjà été utilisé, les paramètres d'accès à celui-ci (adresse, login et mot de passe) , il me faut totalement le réinitialiser.
Réinitialiser le commutateur supprime les configurations et redémarre le commutateur en mode de configuration express.



Les leds du commutateur commencent à clignoter lorsque j'appuie sur le bouton Mode (ce qui signifie que le commutateur est déjà configuré avec des renseignements IP).

Pour le réinitialiser, appuyer sur le bouton Mode et le maintenir enfoncé. Après environ 3 secondes, les leds du commutateur commencent à clignoter. Continuer de maintenir le bouton Mode enfoncé. Les leds arrêtent de clignoter après 7 secondes supplémentaires et le commutateur redémarre ensuite.

Le commutateur agit maintenant comme un commutateur non configuré. Nous pouvons entrer les renseignements IP du commutateur en utilisant le Configurateur express.

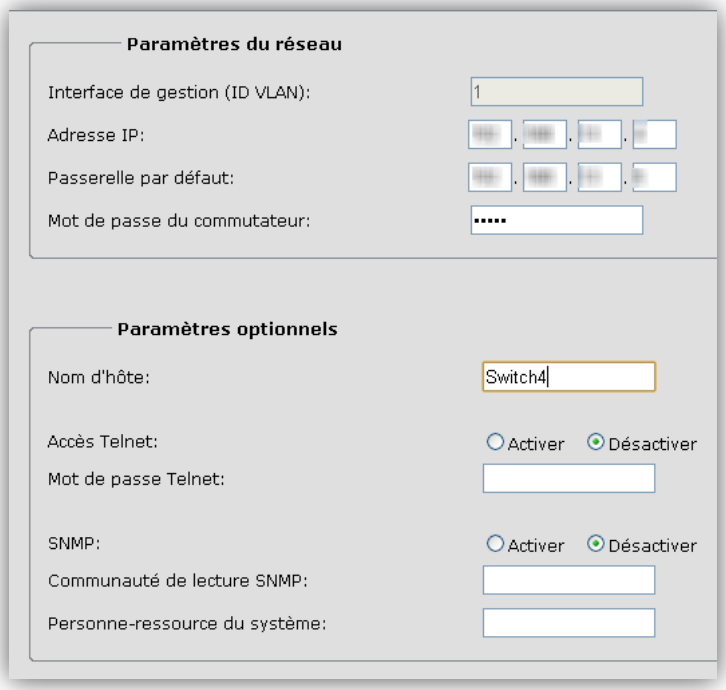
L'accès de base au switch se fait à partir d'un navigateur internet sur l'adresse 10.0.0.1, mon pc étant connecté sur un réseau 192.168.xxx.xxx avec une adresse IP fixe, il me faut donc reconfigurer ma carte réseau en mode DHCP et brancher mon pc sur le switch à reconfigurer.

Accès au switch :

La page Configuration express apparaît.

Il me faut ensuite rentrer les renseignements suivants :

- Dans le champ Interface de gestion (ID VLAN), le chiffre par défaut est 1. Entrez un nouvel ID VLAN seulement si vous voulez modifier l'interface de gestion par laquelle vous gérez le commutateur et à laquelle vous attribuez les renseignements IP. L'étendue de l'ID VLAN est de 1 à 1001.
- Dans le champ Adresse IP, entrez l'adresse IP du commutateur. Dans le champ Masque de sous-réseau, cliquez sur la flèche déroulante et sélectionnez Masque de sous-réseau.
- Dans le champ Passerelle par défaut, entrez l'adresse IP pour la passerelle par défaut (routeur).
- Entrez votre mot de passe dans le champ Mot de passe de commutation. Le mot de passe peut comporter de 1 à 25 caractères alphanumériques, peut commencer avec un chiffre, est sensible aux minuscules et majuscules, permet les espaces intercalés, mais ne permet pas les espaces au début ou à la fin. Entrez le mot de passe de nouveau dans le champ Confirmer le mot de passe de commutation.



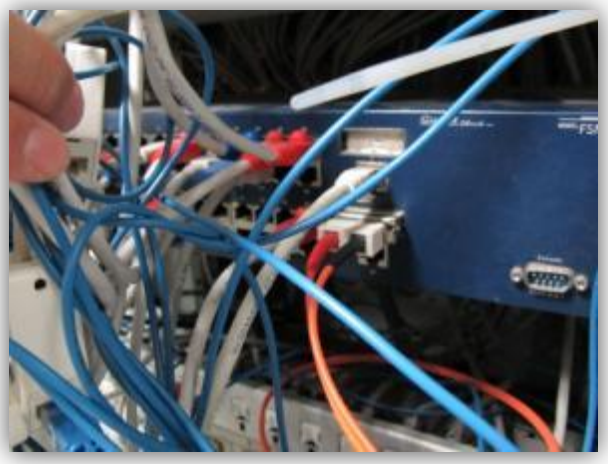
Je peux maintenant redémarrer le switch et reconfigurer mes paramètres réseaux précédents pour pouvoir accéder à celui-ci à partir du réseau existant.

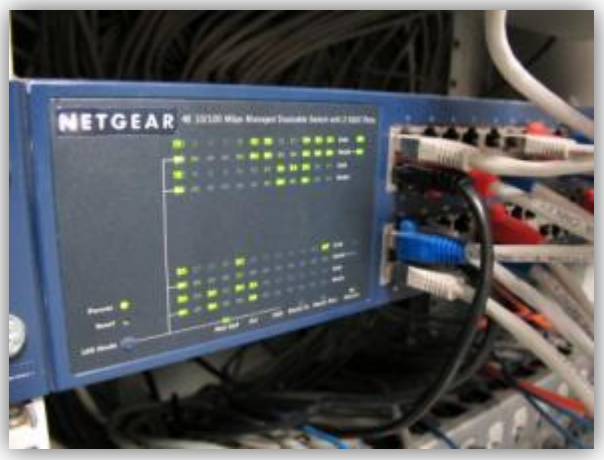
Renseignments du commutateur	
Nom d'hôte:	Switch
ID du produit:	WS-C2960-48TT-S
Adresse IP:	
Adresse MAC:	
ID Version:	V04
Numéro de série:	FOC1442V3BE
Logiciel:	12.2(50)SE4
Personne-ressource:	
Emplacement:	

7.2.2.2 Mise en production

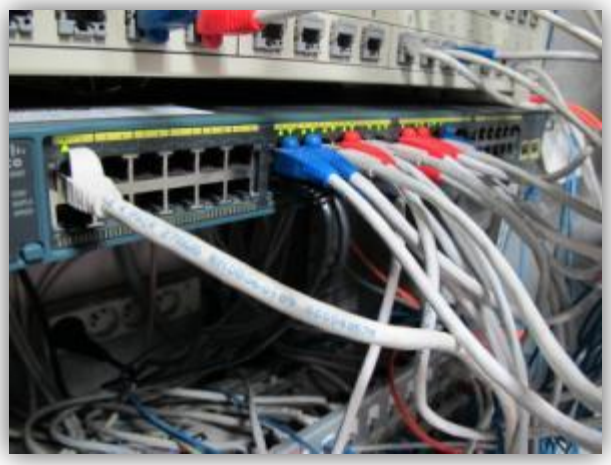
Afin de ne pas perturber le fonctionnement de la société Huwans, j'ai effectué le remplacement de celui-ci avant l'ouverture et l'arrivée du personnel.

Voici la baie existante avec un Switch Netgear surdimensionné pour les besoins en Hôtes IP.



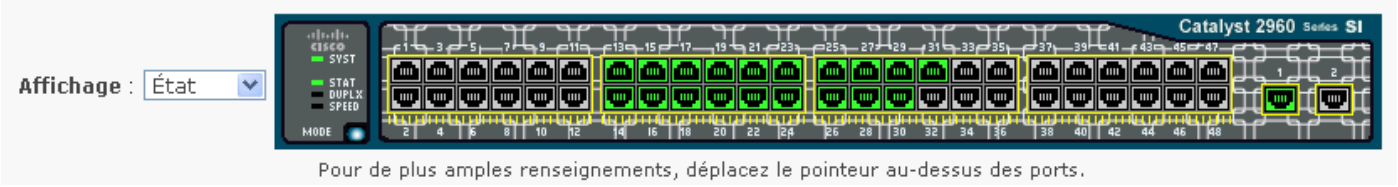


Mise en place et branchements du nouveau switch



Mise en place de l'étiquette permettant d'identifier le switch avec son adresse IP et l'adresse email de l'administrateur en cas de problème.

Vérification du bon fonctionnement du switch à partir de l'interface web.



7.2.3 Configuration et Installation d'un Téléphone IP THOMSON ST2030

L'administrateur m'a donné pour mission de tenter de remettre à jour deux téléphones IP.
En effet ceux ci possèdent une configuration propriétaire non modifiable effectuée par un ancien fournisseur.
Ces téléphones n'étant plus fabriqués et suivis par la marque, il m'a fallu rechercher les firmwares correspondant sur internet, trouvés sur un site web de réparateur de téléphonie aux états unis.

Il m'a d'abord fallu reconfigurer manuellement à partir des menus d'administration du téléphone les paramètres IP pour pouvoir y accéder à partir d'un navigateur web.

La mise à jour est assez longue à effectuer, 3 firmwares sont nécessaires pour reconfigurer totalement le téléphone.

Voici les informations, en anglais à suivre afin d'effectuer la mise à jour complète :

ST2030 SIP fw upgrade via http
==========

1. Web access:

http://<ip>/admin.html
usr: administrator
pwd: 784518

2. Application upgrade:

2.1. Go to Utility section, select Firmware upgrade (via http)
2.2. Browse to select the application file v2030SG.R11.1.SED.120313.2.78.1.zz, then press Apply
2.3. When you are prompted to, click "Reboot and restart main application". Wait until you are back in the home page

3. Boot code upgrade (Optional, only if your phone does not show Boot Version 1.11 in homepage and you want to do MGCP-SIP swap)

3.1. If your homepage already shows Boot Version 1.11, go directly to step 4 below
3.2. Go to Utility section, select Firmware upgrade (via http)
3.3. Browse to select the boot code file "v2030_boot_v111.zz", then press Apply
3.4. When you are prompted to, click "Reboot and restart main application". Wait until you are back in the home page

4. DSP fw upgrade (Optional, if your dsp code is older than 3.20).

4.1. If your home page already shows DSP version 3.20, go directly to step 5 below
4.2. Go to Utility section, select Firmware upgrade (via http)
4.3. Browse to select the dsp fw file "v2030_dsp_R11.1_SED_v320.zz", then press Apply
4.4. When you are prompted to, click "Reboot and restart main application". Wait until you are back in the home page.

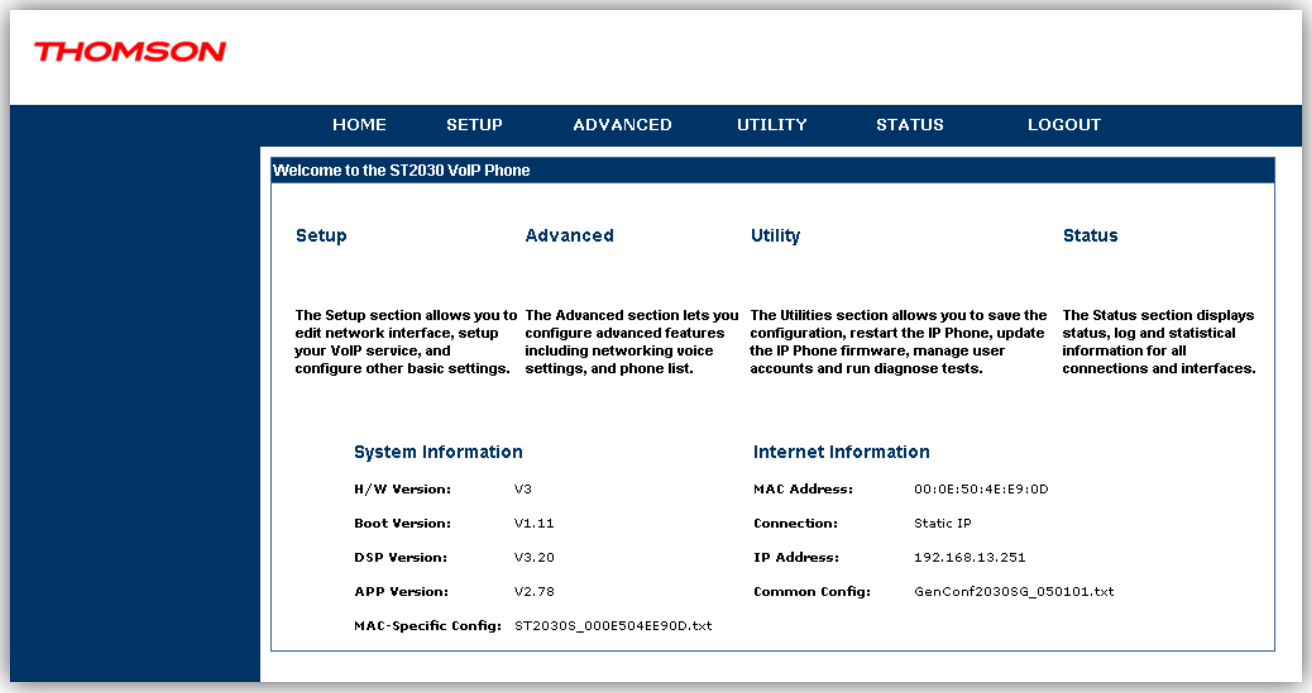
5. Telephone configuration upgrade. This step is mandatory.

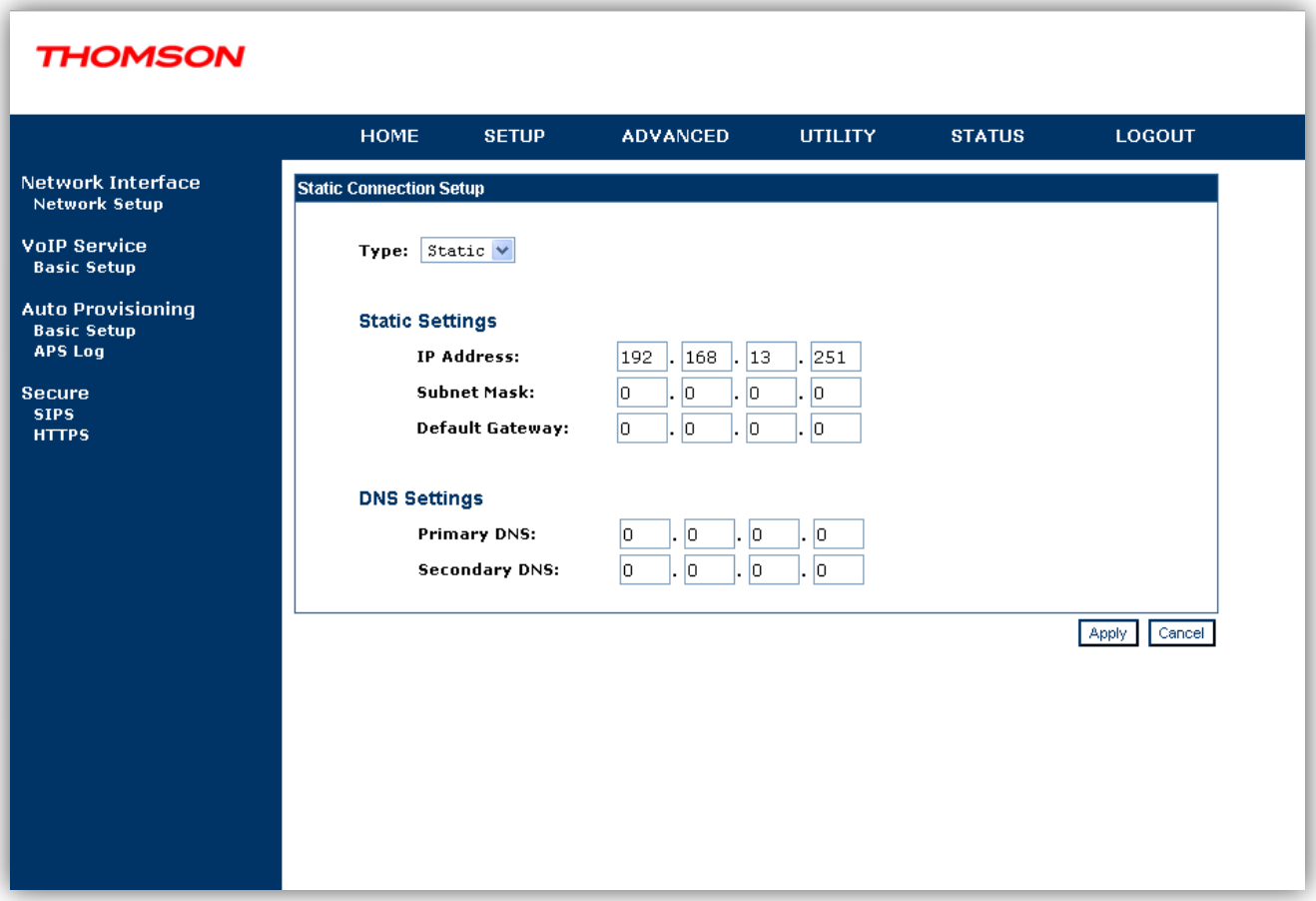
5.1. Go to Utility section, select Telephone Configure
5.2. Browse to select the configuration file TelConf2030SG.R11.1.SED.120313.2.78.1.txt, then press Apply
5.3. When you are prompted to, click "Reboot and restart main application"

6. Check in Home page, that
DSP version is 3.20
Boot Version is 1.11
Application version has changed according to your intended release package

7. Your phone should be ready to work in your environment since it will keep the previous configuration.

Après mis à jour nous pouvons vérifier la bonne installation des firmwares et la possibilité de pouvoir reconfigurer le téléphone avec les informations correspondantes à notre infrastructure de téléphonie IP.





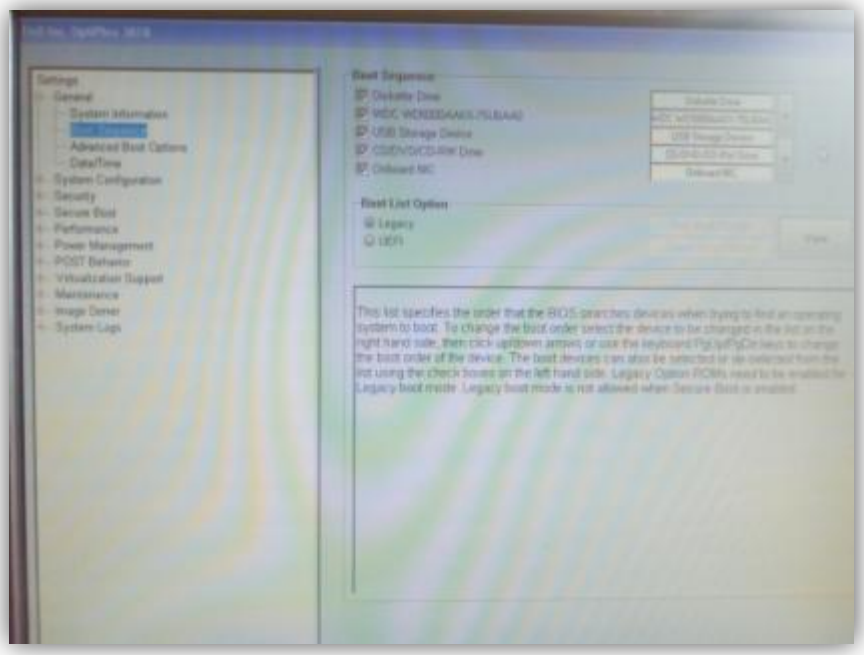
7.2.4 Installation et Configuration d'un poste Client DELL OPTIPLEX 3010

Lors de mon stage au sein de Tourism-It, j'ai eu régulièrement pour mission de préparer des postes de travail pour les utilisateurs, que ce soit pour une remise à niveau d'un poste existant ou la configuration et l'installation d'un nouveau poste.

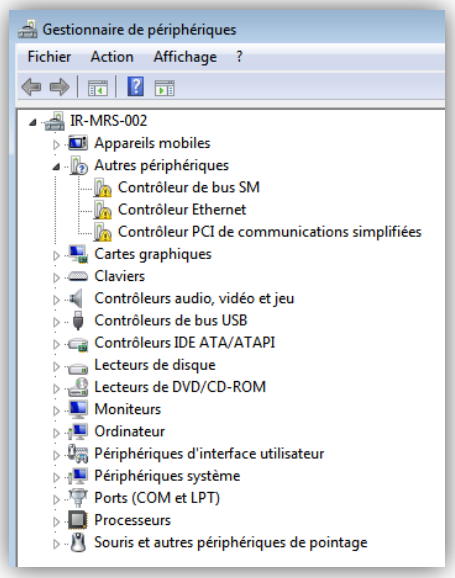
Je vais détailler ici l'installation d'un nouveau poste.

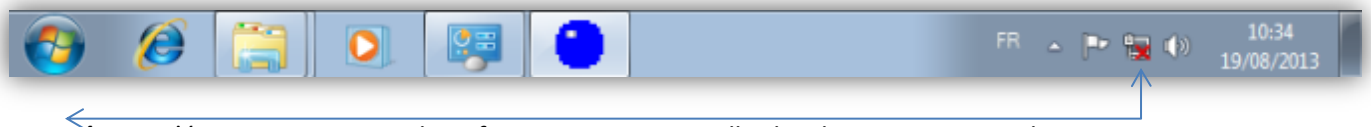
7.2.4.1 Installation du système d'exploitation

J'ai dû en premier réaliser l'installation du système d'exploitation Microsoft Windows 7 64 bits.
Pour pouvoir lancer l'installation à partir du lecteur DVD il faut modifier le Bios de la carte mère pour que celui-ci puisse effectuer son boot à partir du lecteur DVD.

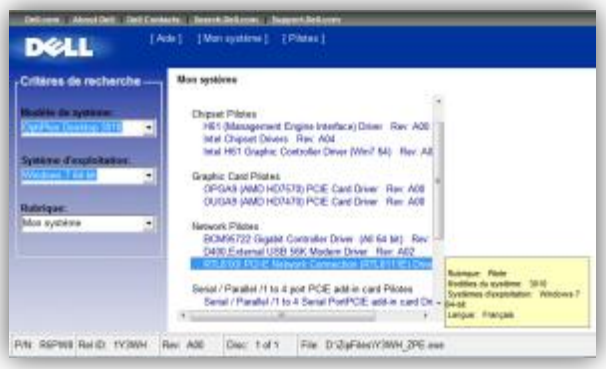


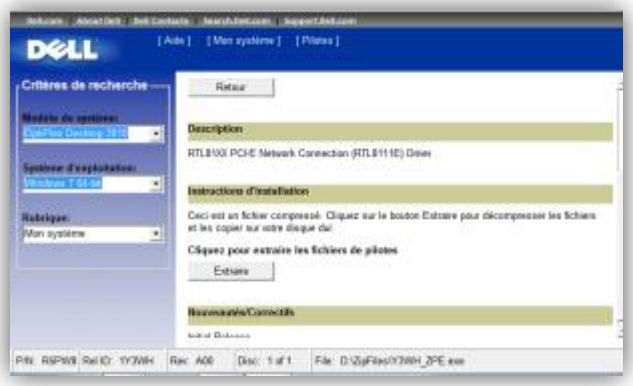
Au redémarrage, il faut appuyer sur la touche F12 et sélectionner le périphérique de BOOT.

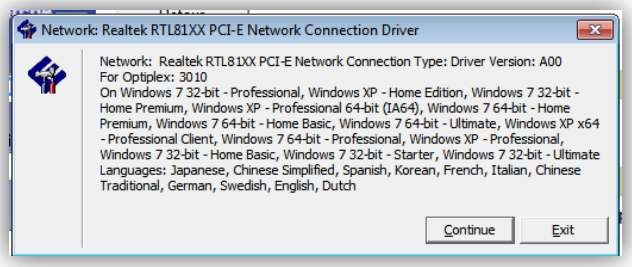




La **carte réseau** n'étant pas reconnu, il me faut en premier installer les drivers correspondants pour pouvoir effectuer ensuite la configuration des paramètres réseaux.

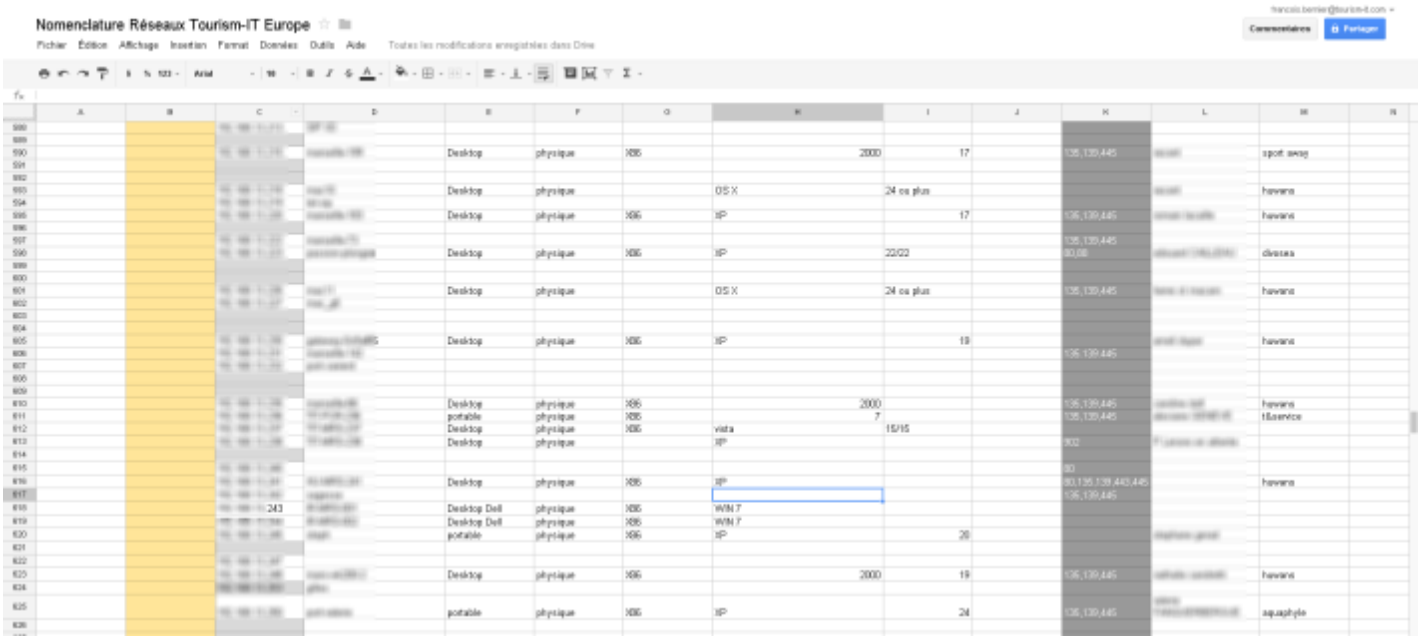




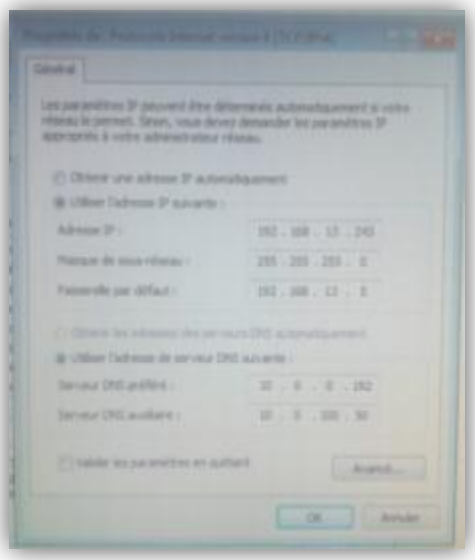


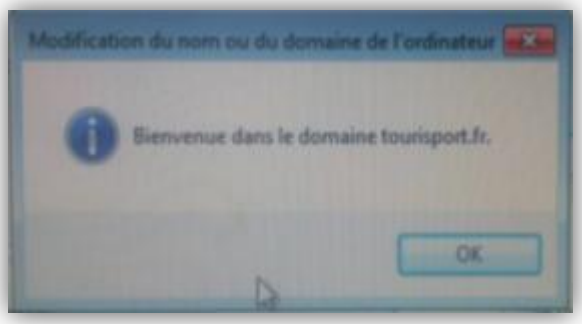
Après installation du système d'exploitation, il faut assigner un nom au poste, une adresse IP et le joindre au domaine.

Le nom et l'adresse IP respecte une norme de nommage qui doit être répertoriée dans un tableau.

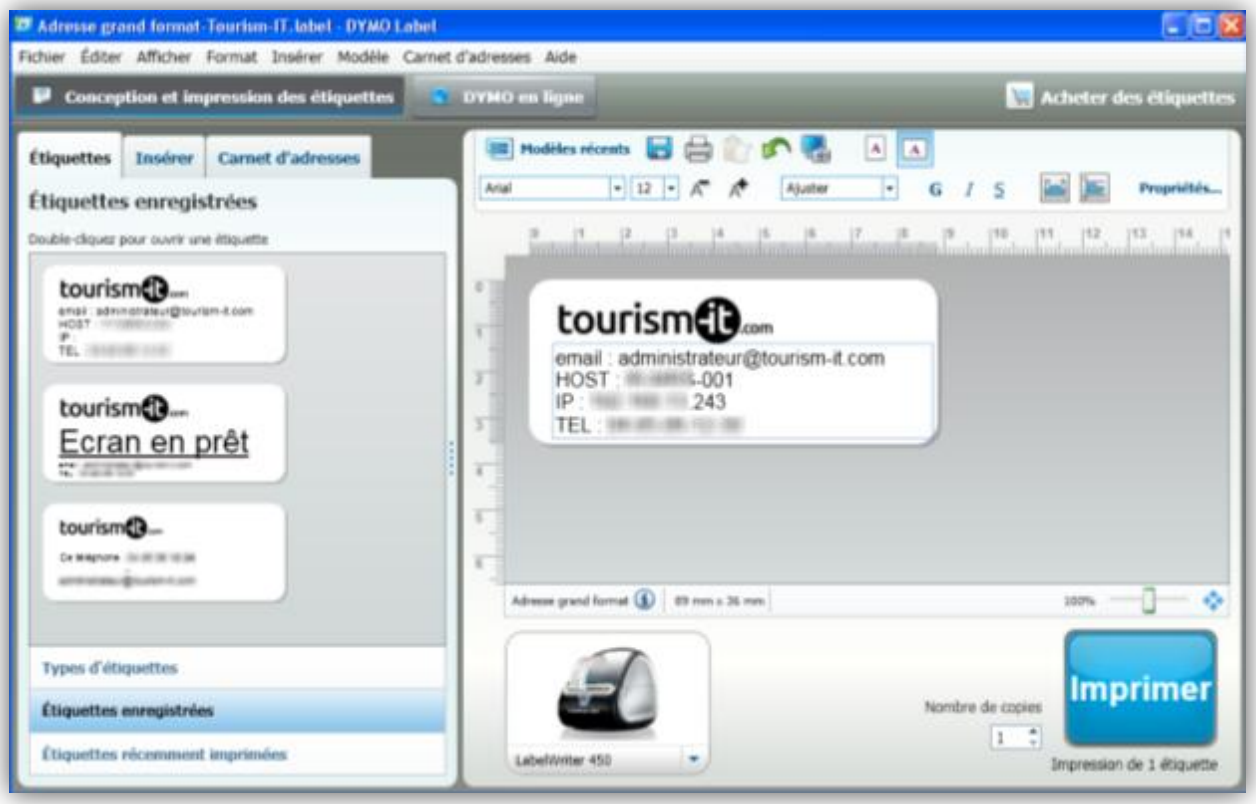


Nommage et jonction au domaine





Il faut également apposer une étiquette sur le poste utilisateur permettant de retrouver rapidement son nom en cas de crash et également afficher l'adresse email de l'administrateur en cas de problème sur le poste.



Pour chaque poste en permanence une série de logiciels est installée.
Avant leur installation il faudra effectuer les mises à jour du système avec Windows Update et installer ensuite les logiciels suivants :

- TeamViewer
- LogMeIn
- L'agent AntiVirus Kapersky Endpoint Securit 10
- Google Chrome
- Java
- Adobe Flash Player
- Microsoft Office 2010

Avant livraison à l'utilisateur, il faudra vérifier le Gestionnaire de périphérique et installer éventuellement les drivers manquants.

7.3 Schéma Infrastructure Tourism-It Format A3

SCHEMA A3

8 Bibliographie et Webographie

Webographie :

- http://technet.microsoft.com/en-us/library/dd560648(v=ws.10).aspx
- http://technet.microsoft.com
- http://www.parallels.com/fr/products/pvc/
- http://www.labo-microsoft.org/articles/server/
- http://www.indexel.net/infrastructure/virtualisation-de-pc-six-alternatives-a-vmware-view-3-2841.html#
- http://www.itpro.fr/a/implementer-infrastructure-vdi/
- http://www.virtualizationadmin.com/search/?q=Remote+Desktop+Server+farms+explained+%28Part+1%29
- http://www.ulteo.com/home/
- http://www.2x.com/fr/applicationserver/
- http://www.ericom.com/
- http://syskb.com/implementer-un-serveur-remote-desktop-gateway-rdg-rd-gateway/
- http://www.labo-microsoft.org/articles/Microsoft-VDI/
- http://7.supinfo.com/post/Windows-7-applications-et-bureaux-distants-(Virtual-Desktop-Infrastructure).aspx
- http://tiennot.fr/romain/index.php?post/2012/06/18/Windows-Server-2012-Virtual-Desktop-Infrastructure-%28VDI%29#content

Logiciels et système d'exploitation mis en œuvre lors du stage:

- Microsoft Office 2010
- Microsoft Server 2008 R2
- Microsoft Server 2003
- Microsoft Windows XP Professionnel
- Microsoft Windows 7 Pofessionnel/Ultimate
- Parallels Virtuozzo
- Office Visio Professional 2007
- Debian 6 Squeeze
- Ulteo OVD 3.04
- 2xApplicationServer
- Ericom Powerterm Webconnect
- Quest Vworkspace
- Teamviewer
- LogMeIn
- Kaspersky Endpoint Security 10
- PhpMyAdmin
- MySqlServer
- Adobe Acrobat Pro
- The Gimp 2
- Vmware Esxi / Vsphere