REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

****

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR, DE LA RECHERCHE ET DE L'INNOVATION

****

UNIVERSITE GASTON BERGER DE SAINT-LOUIS

U.F.R DE SCIENCES APPLIQUEES ET DE TECHNOLOGIE

SECTION INFORMATIQUE

Mémoire de fin d'études pour l'obtention du diplôme de

Master en Réseaux Sécurité et Systèmes Distribués (R2SD)

Sujet : Étude d'une solution d'accès distance terminal serveur, déploiement et hybridation de la messagerie.

Présenté le 01/04/2021 par :

M. Moustapha Ndao

Sous la direction de :

Dr. Chérif Diallo

Jury :

Président :	M. Maissa MBAYE
Examinateur :	El Hadji Serigne Mamour DIOP
Examinateur :	M. Mahamadou TRAORE
Encadrant :	M. Chérif DIALLO

Année Académique 2019/2020

Remerciements

"si j'ai pu voir aussi loin, c'est que j'étais debout

sur des épaules de géants"

Issac Newton

Mes plus sincères remerciements vont :

À mes très chers parents qui n'ont lésinés sur aucun moyen durant tout notre cursus scolaire.

Mon encadreur pédagogique, **Pr Chérif Diallo** pour son soutien moral et scientifique, pour sa disponibilité et ses conseils.

Mon maître de stage, **M. Mor Talla Gueye** ainsi qu'au directeur d'EXPERT IS **M. Ismaël MERICO** de par leur disponibilité, leur conseil et la confiance envers mon humble personne tout au long de ce travail.

À tous les membres du jury qui m'ont fait l'honneur de prendre mon modeste travail en considération pour le juger.

À tout le personnel et le corps enseignant de la section informatique de l'UFR SAT.

À mes collègues du département système et réseaux d'EIS.

Je tiens à remercier aussi tous ceux qui m'ont prêté main forte, et ceux qui ont contribué de près ou de loin à l'élaboration de ce travail.

Dédicaces

Je dédie ce mémoire à :

Mon père

Ma mère

Mon grand-père

Ma Famille

M. Alboury Ndao Expert-Comptable

Mes professeurs

Dr Moussa Soidridine Moindze

Mes collègues d'EXPERT IS

À tous mes camarades promotionnaires

Et à tous mes camarades que j'ai pu rencontrer au cours de mon cursus scolaire, …

Avant-propos

L'UGB, l'Université Gaston Berger de Saint-Louis, Sénégal a été créée officiellement par la loi n° 90-03 du 02 Janvier 1990 et est dotée d'un statut définitif par le décret n° 096-597 du 10 Juillet 1996, d'un nom par le décret n°096-1016 du 04 Décembre 1996.

Se trouvant à une dizaine de kilomètres de la ville de Saint-Louis, l'université est composée de l'Institut polytechnique de Saint-Louis et de huit unités de formation et de recherche que sont :

- Lettres et sciences humaines
- Sciences juridiques et politique
- Sciences économiques et de gestion
- Sciences de la santé
- Sciences agronomiques, d'aquaculture et de technologie alimentaire
- Civilisations, religions, arts et communication
- Sciences Appliquées et de technologie

L'unité de formation et de recherche des sciences appliquées et de technologie (UFR- SAT) est composée de trois sections : Mathématiques, Physique appliquée et Informatique. Dans la section informatique sont dispensés des cours de la Licence au Master en informatique pour une polyvalence dans les métiers du numérique. La formation en master dure deux années et est sanctionnée par un mémoire de fin d'études soutenu devant un jury.

C'est dans cette optique que pour l'obtention du diplôme de master en informatique spécialité réseaux, sécurité et systèmes distribués (**M2S2SD**), les étudiants doivent présenter un mémoire à la fin de la formation ou un rapport de stage.

C'est dans ce dessein que j'ai intégré EXPERT-IS, structure dans laquelle j'ai été chargé de mener un projet informatique dont la teneur est consignée dans ce rapport.

Sigles et Abréviations

AD-DS: Active Directory Domain Services
API: Application Programming Interface
AWS: Amazon Web Services
CAL: Client Access License
CPU: Central Process Unit
CRM: Customer Relationship Management
DDoS: Distributed Denial of Service
DHCP: Dynamic Host Control Protocol
DNS: Domain Name System
EAC: Exchange Administration Console
ERP: Enterprise Resource Planning
ETSI: European Telecommunications Standards Institute
EVD: Enterprise for Virtual Desktop
FQDN: Full Qualified Domain Name
HTTPS: HyperText Transfer Protocol Secure
IA: Intelligence Artificielle
IaaS: Infrastructure as a Service
IDS: Intrusion Detection System
IMAP: Internet Message Access Protocol
IoT: Internet of Things
URL: Uniform Resource Locator
IP: Internet Protocol
IPS: Intrusion Prevention System
ISO: International Organization for Standardization
IT: Information Technique
LAN: Local Area Network
NFV: Network Functions Virtualization
NIST: National Institute of Standards and Technology
OWA: Outlook Web Access
OS: Operating System
PaaS: Platform as a Service
PC: Personal Computer
PHP: HyperText Pre-processor
PME: Petite/Moyenne Entreprise
POP: Post Office Protocol
RAM: Random Access Memory
RDC: Remote Desktop Client
RDP: Remote Desktop Protocol
RDS: Remote Desktop Services
RDSH: Remote Desktop Session Host
RPC: Remote Procedure Control
SaaS: Software as a Service
SAV: Service Après Vente
SMTP: Simple Mail Transfer Protocol
SQL: Structured Query Language
TL: Terminal Léger
TLS: Transport Layer Secure
TPE: Très Petite Entreprise
UIT: Union Internationale des Télécommunications
VDI: Virtual Desktop Infrastructure
VLAN: Virtual Local Area Network
VCPU: Virtual Central Processing Unit
VPN: Virtual Private Network
VGPU: Virtual Graphics Processing Unit
WAN: Wide Area Network

Liste des Figures et des tableaux

Figure 1.2-1 : Organigramme EXPERT-IS 6
Figure 2.1-1 Hyperviseur de type 1 8
Figure 2.1-2 Hyperviseur de type 2 9
Figure 2.1-3 virtualisation données 9
Figure 2.1-4 Virtualisation serveur 9
Figure 2.1-5 Virtualisation des postes de travail 10
Figure 2.1-6 Virtualisation des systèmes d'exploitation 10
Figure 2.1-7 Virtualisation réseau 11
Figure 2.2-1 Cloud computing 11
Figure 2.2-2 Couches Cloud computing 13
Figure 2.2-3 Infrastructure IaaS 13
Figure 2.2-4 Infrastructure PaaS 14
Figure 2.2-5 Infrastructure SaaS 15
Figure 2.2-6 AWS Serverless computing 16
Figure 2.2-7 Datacenter 17
Figure 2.2-8 Microsoft Azure 18
Figure 2.2-9 Amazon Web Services 18
Figure 2.2-10 Google Cloud Platform 18
Figure 3.1-1 Architecture EXPERT IS 22
Figure 3.1-2 Microsoft Azure 24
Figure 4.1-1 Architecture déploiement 27
Figure 4.2-1 Architecture ferme RDS 29
Figure 4.2-2 Sélectionner le Serveur Cible 33
Figure 4.2-3 Confirmation des services RDS 34
Figure 4.2-4 Installation des services RDS 35
Figure 4.2-5 Services et rôles 35
Figure 4.2-6 Installation service Broker 36
Figure 4.2-7 Choix du mode Licence CAL 36
Figure 4.2-8 Création collection 37
Figure 4.2-9 Spécification serveur hôte de session 37
Figure 4.2-10 Autorisations des utilisateurs 38
Figure 4.2-11 Connexion aux RemoteApp 39
Figure 4.2-12 Ressources publiées 39

Figure 4.2-13 Client RDC 40
Figure 4.2-14 Bureau à distance 41
Figure 4.2-15 Configuration multisessions 42
Figure 4.2-16 Nombre de sessions 43
Figure 4.2-17 Flux Messagerie 45
Figure 4.2-18 Mode Installation 50
Figure 4.2-19 Services Exchange 51
Figure 4.2-20 Interface EAC 53
Figure 4.2-21 User Mailbox 55
Figure 4.2-22 création groupe dynamique 57
Figure 4.2-23 Groupe dynamique 57
Figure 4.2-24 Types de contacts 58
Figure 4.2-25 User Mailbox 59
Figure 4.2-26 Office 365 61
Figure 4.2-27 Serveur AD 68
Figure 4.2-28 Serveur Azure AD Connect 69
Figure 4.2-29 Installation Azure AD Connect 69
Figure 4.2-30 Composants Azure AD Connect 70
Figure 4.2-31 Authentification Azure AD Connect 70
Figure 4.2-32 Connexion à Azure AD 71
Figure 4.2-33 Connexion annuaire 71
Figure 4.2-34 Compte de forêt AD 72
Figure 4.2-35 Suffixes UPN 72
Figure 4.2-36 Identification des utilisateurs 73
Figure 4.2-37 Configurations Azure AD Connect 73
Figure 4.2-38 Synchronisation Azure AD et AD Local 74
Figure 4.2-39 Connexion à Office 365 75
Figure 4.2-40 Assistant hybridation 75
Figure 4.2-41 Configuration des paramètres hybridation 76
Figure 4.2-42 spécification serveur cible 77
Figure 4.2-43 Types d'hybridation 78
Figure 4.2-44 Topologie 79
Figure 4.2-45 Finalisation paramètres 79
Figure 4.2-46 Hybridation messagerie 80

Tableau 4.2-1 Prérequis matériels et logiciels 29
Tableau 4.2-2 Conditions matérielles et logicielles 47
Tableau 4.2-3 Types de destinataires 54

Tables des matières

Remerciements i
Dédicaces ii
Avant-propos iii
Sigles et Abréviations iv
Liste des Figures et des tableaux v
Introduction Générale 1
CHAPITRE 1 : Présentation EXPERT-IS 4
1.1 Activités 5
1.1.1 Système 5
1.1.2 BI et BIG DATA 5
1.1.3 Cybersécurité 6
1.1.4 Réseaux Télécommunications 6
1.2 Organisation 6
1.3 Les métiers du technicien au sein d'EXPERT-IS 7
CHAPITRE 2 : Généralités sur la Virtualisation et le cloud computing 8
2.1 Définition de la virtualisation 8
2.1.1 Les différentes ressources virtualisées 9
2.2 Définition du cloud computing 11
2.2.1 Les différents modèles de déploiement cloud 12
2.2.2 Les différents types de services Cloud 12
2.2.3 Les acteurs du cloud computing 17
2.2.4 La sécurité informatique et le cloud computing 19
CHAPITRE 3 : Etude de l'existant et Objectifs de la mission technique 22
3.1 Étude de l'infrastructure existante 22
3.1.1 Présentation de Microsoft Azure 23
3.1.2 Services Azure 24

3.2 Objectifs de notre mission 25
3.3 Moyens mis à disposition du stagiaire 26
CHAPITRE 4 : Réalisation du projet 27
4.1 Conception générale 27
4.2 Conception détaillée 28
4.2.1 Accès Terminal Serveur 28
4.2.2 Déploiement des rôles Remote Desktop Service 32
4.2.3 Configuration de connexions simultanées 41
4.2.4 Hybridation de la messagerie 43
4.2.5 Configuration Office 365 60
4.3 Conclusion 81
Conclusion Générale 82
Bibliographie 83

Introduction Générale

Aujourd'hui les chaines de valeur des entreprises sont composées d'environ 20 entreprises, l'avènement de Consumer IT ou du Web2.0, des réseaux sociaux et l'internet des objets transforment la façon dont nous vivons, dont nous apprenons, dont nous collaborons, travaillons, consommons et jouons. Ces changements dans la société transforment également la façon dont nous concevons, gérons nos entreprises et notre chaine de valeur afin de les adaptées aux changements du monde extérieur.

Selon le « National Institut of Standards and Technology » le cloud computing est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurables (par exemple, réseau, serveurs, stockage, application et services) qui peuvent être mises à disposition et libérées avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services [1].

Tous les cloud ne sont pas identiques et aucun type de cloud ne convient à tout le monde. Plusieurs modèles, types et services différents ont évolués au fil des années pour répondre aux besoins des entreprises, et structures commerciales.

C'est pour cela que nous étions chargés de faire une étude pour l'optimisation d'une infrastructure hybride répartie comme suit :

Nous allons dans une première partie faire une présentation de la structure d'accueil. Dans la deuxième partie sera consacrée à l'étude de la virtualisation et du cloud computing. Nous procéderons ensuite dans la troisième partie à l'étude de l'existant et les objectifs de notre mission et finir par la mise en œuvre dans la quatrième partie des solutions d'optimisation de l'infrastructure.

1. Problématique

Avec la demande croissante des besoins, de la disponibilité des ressources, de stockage des données et de l'élasticité des ressources. Beaucoup d'entreprises se voient obliger de trouver une solution non seulement qui permettra d'avoir une infrastructure évolutive, d'accéder à n'importe quelle ressource informatique à la demande, de pouvoir réduire ou

augmenter la consommation des ressources mais aussi de pouvoir payer seulement les ressources consommées.

Ainsi pour résoudre ces problèmes, grâce à aux nouvelles technologies de l'information et de la communication, les entreprises doivent opter des solutions qui leur permettront d'être en phase avec l'évolution technologique.

C'est le cas du cloud computing qui apporte des solutions concernant l'évolutivité de l'infrastructure informatique, d'accéder aux ressources à la demande n'importe où et permet aussi un stockage beaucoup plus important et moins coûteuse.

2. Objectifs

L'objectif de ce travail consiste à faire une étude afin d'optimiser une infrastructure hybride, d'identifier les évolutions notées dans le domaine technologique comme services et applications grâce au cloud computing. Afin de proposer une solution appropriée à nos besoins. D'identifier aussi les différentes possibilités et conditions de migration que nous pouvons faire pour aller vers les services offerts par le cloud computing.

3. Contexte et Intérêt du sujet

Avec l'avènement du Big Data caractérisé par les trois V qui sont :

- Le volume
- La variété
- Et la vélocité

Mais aussi l'IoT, L'IA et la collaboration avec des partenaires, les entreprises se retrouvent dans un monde dans laquelle la quantité d'informations devant être traitée et stockée les obligent à adopter une solution qui leur permettra non seulement de pouvoir satisfaire ces besoins mais aussi d'avoir une infrastructure informatique flexible et facilitant de même une meilleure gestion des ressources.

C'est dans cette optique que nous optons de mettre en place une solution d'optimisation de cloud hybride afin de répondre aux besoins comme la flexibilité de l'infrastructure, la possibilité de traiter de grosses données, la conservation des données sensibles en interne et aussi de procéder à des sauvegardes pour éviter les temps d'arrêt.

4. Démarche méthodologique

Dans le cadre de ce travail, nous allons dans une première partie procéder par une présentation de la structure d'accueil, la deuxième partie sera consacrée à la présentation de la virtualisation et du cloud computing, la troisième à l'étude de l'existant et des objectifs de la mission technique. Dans la quatrième partie les réalisations des solutions.

CHAPITRE 1 : *Présentation EXPERT-IS*

EXPERT IS est une startup créée en 2016, par un Ingénieur en Informatique avec une forte expérience dans l'expertise et la gestion des projets informatiques. L'objectif de **E.IS** est de se positionner dans le secteur informatique au Sénégal, en apportant un niveau d'expertise et en proposant des Ingénieurs experts et pointus dans leur domaine d'activité.

E.IS jouit de l'expérience et du savoir-faire de son partenaire principal MCI EXPERT France dont EIS est la filiale Sénégalaise.
Les collaborateurs d'EXPERT IS sont triés sur le volet, ils sont issus de formation de haut niveau et sont certifiés dans leur domaine d'intervention. L'expertise locale est privilégiée mais **E.IS** peut faire appel à des experts provenant de ses partenaires étrangers si l'expertise locale fait défaut pour le besoin du client.
EXPERT IS comporte quatre pôles d'activités :

- Système,
- BI et BIG DATA,
- Cybersécurité,
- Réseaux et Télécommunications.

Pour répondre aux besoins des clients correspondants aux départements précités. Les chefs de ces trois départements présentent des expériences d'une quinzaine d'années d'expertise dans ces secteurs.

Le groupe compte parmi ses clients en France l'entreprise EDENRED, ECOMETERING, CEAT ELECTRONICS, LOREAL, POINT P, pour ne citer que ces structures. Le groupe a mise en place pour ses clients des systèmes d'information, de messagerie d'entreprise, de solution de centralisation des données, et de prestation en mode régie ou forfait. EIS est partenaires de :

- Microsoft, revendeur de leur solution notamment sur la partie CLOUD avec l'office 365 ou AZURE
- DELL
- Kaspersky

- FORTINET
- 3CX Téléphonie
- VEEAM Backup
- SimplyDesk : Solution de gestion de parc informatique
- EIS est aussi partenaire **Overland Storage**, pour ne citer que ceux-là.

1.1 Activités

Pour répondre aux besoins des clients, E.IS dispose de quatre Business Unit (BU) dont les chefs présentent une quinzaine d'années d'expérience dans ces d'activités :

1.1.1 Système

- Déploiement de votre environnement système Microsoft (Mise en place d'un système de messagerie avec Microsoft Exchange) et Linux.
- Déploiement Solution cloud à travers Office365 / AZURE.
- Déploiement de solution de gestion de parc informatique
- Sécurisation de l'infrastructure réseaux avec les solutions Fortinet.
- Vente de matériel informatique sur la partie serveur, stockage, d'équipement réseau.

1.1.2 BI et BIG DATA

- Conseil en technologie – Choix d'outils – Intégration – Migration.
- Une expertise fonctionnelle, méthodologique, technique et sectorielle (Télécoms, Public, Banque et Assurance).
- Etude et mise en œuvre des schémas directeurs décisionnels, nouveaux usages, réurbanisation, rationalisation d'outils.
- Audit et dimensionnement, choix d'architecture.
- Intégration de logiciel et de base de données (SAS, SPAD, SPSS, BO, ORACLE).

Formation/ Renforcement de capacités / Transfert de compétence :

- Formations aux logiciels SAS, SPAD, BO, IBM SPSS Modeler….
- Formations à l'administration ORACLE.
- Formations personnalisées**.** Études & transfert de compétences.
- Développement d'applications web, mobile.
- Conseil en Business Intelligence, solution ERP, finance & fiscalité.

1.1.3 Cybersécurité

- Cyber stratégie et SMSI. Gouvernance par les risques.
- Gestion des incidents et de la continuité d'activité
- Expertise technique en cybersécurité.
- Conformité et audits fonctionnels/techniques, Ethical Hacking et tests d'intrusion.
- Formation et sensibilisation.
- Normes internationales : ISO 27001, ISO 27002, NIST, PCI-DSS, etc.
- Veille technologique

1.1.4 Réseaux Télécommunications

- Déploiement de réseaux LAN, WAN.
- Mise en place de PBX et autres réseaux téléphoniques d'entreprise.
- Installation et configuration d'équipements Télécoms.
- Audit réseaux et sécurité.
- Optimisation de réseaux.

1.2 Organisation

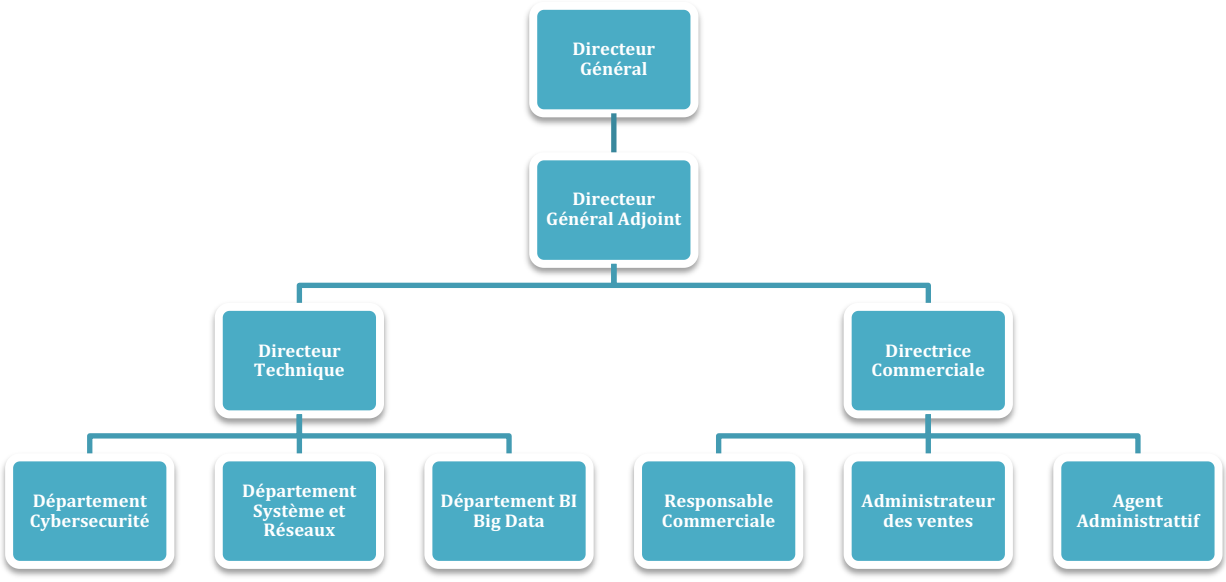


Figure 1.2-1 : Organigramme EXPERT-IS

1.3 Les métiers du technicien au sein d'EXPERT-IS

- Administrateur système et réseau :
  - Apporter son expertise technique en système, réseaux et télécoms
  - Gérer les projets des clients et les projets internes dans son département
  - Maintenir en condition opérationnelle l'infrastructure système et réseaux de l'entreprise
  - Conseiller et être support des clients d'EIS
  - Conseiller et être support du service commercial dans les réponses techniques aux clients
  - Transférer des compétences et faire des formations techniques
  - Assurer la veille technologique

CHAPITRE 2 : *Généralités sur la Virtualisation et le cloud computing*

Ce chapitre nous permettra de se familiariser avec la virtualisation et le cloud computing. Nous y donnerons, les définitions, les différents concepts qui existent entre ces deux technologies et parler des intervenants du cloud computing et aussi des aspects de la sécurité dans le cloud computing.

2.1 Définition de la virtualisation

La virtualisation est une technologie qui vous permet de créer des services informatiques utiles à l'aide de ressources physiques. Elle permet d'exploiter toute la capacité d'une machine physique en le répartissant entre de nombreux utilisateurs ou environnements différents [2].

Pour fonctionner la virtualisation utilise des logiciels du nom d'hyperviseur.

1. Hyperviseur de type 1

Un hyperviseur de type 1 est une plateforme qui s'installe directement sur la couche matérielle du serveur. Il est privilégié lorsque l'on souhaite garder les performances de la machine physique et utilisé pour virtualiser des serveurs de fichiers, des bases de données, etc...

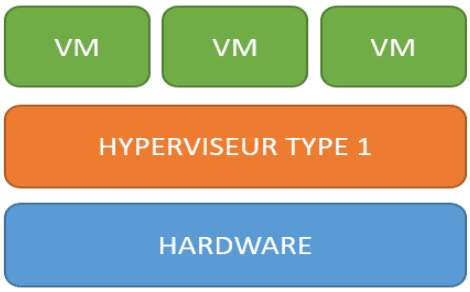


Figure 2.1-1 Hyperviseur de type 1 [2]

2. Hyperviseur de type 2

Un hyperviseur de type 2 est assez comparable à un émulateur dans la mesure où il s'installe sur le système d'exploitation. Ils sont utilisés pour virtualiser des OS sur des postes de travail.

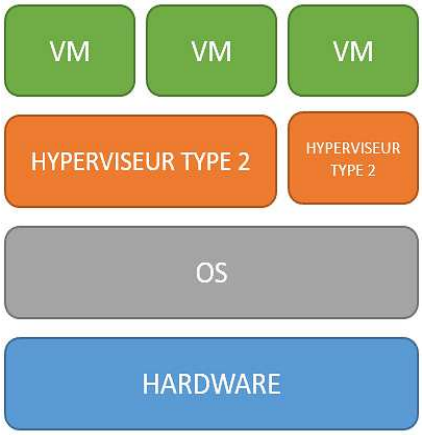


Figure 2.1-2 Hyperviseur de type 2 [2]

2.1.1 Les différentes ressources virtualisées

1. Virtualisation des données

Virtualisation des données consiste à rassembler des données éparpillées dans un environnement. Elle permet l'utilisation des données comme source dynamique [2].

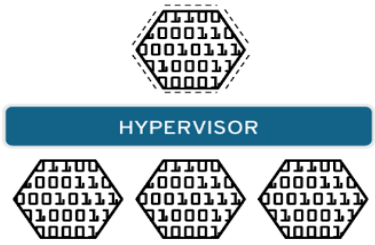


Figure 2.1-3 virtualisation données [2]

2. Virtualisation des serveurs

La virtualisation des serveurs permet d'optimiser les performances d'exécution des fonctions et de traiter un volume élevé de tâches spécifiques afin de permettre aux utilisateurs (ordinateurs portables et de bureau) d'effectuer plusieurs tâches [2].

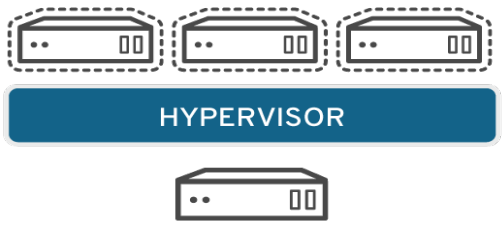


Figure 2.1-4 Virtualisation serveur [2]

3. Virtualisation des postes de travail

Souvent confondue avec la virtualisation des systèmes d'exploitation, la virtualisation des postes de travail permet de centraliser la configuration, la gestion et les mises à jour de plusieurs postes simultanément par un seul administrateur [2].

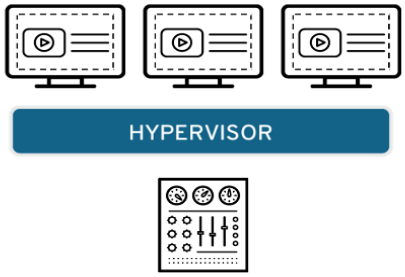


Figure 2.1-5 Virtualisation des postes de travail [2]

4. Virtualisation des systèmes d'exploitation

Elle permet l'exécution en parallèle deux systèmes d'exploitation différents dans une seule et même machine permettant ainsi la réduction des coûts, le renforcement de la sécurité et la réduction du temps alloué aux mises à jour de logiciel.

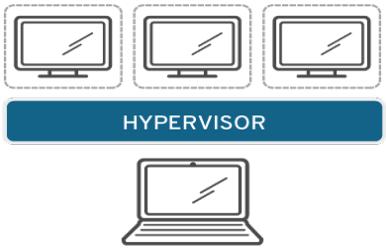


Figure 2.1-6 Virtualisation des systèmes d'exploitation [2]

5. Virtualisation des fonctions réseau

La virtualisation des fonctions réseau (NFV) permet à l'opérateur de déployer des fonctions réseaux en tant qu'instances virtualisées au lieu d'entités matérielles dédiées. L'approche NFV s'appuyant sur la virtualisation informatique qui permet la création de partition réseau isolée sur une infrastructure réseau partagée permettant ainsi à de multiples réseaux virtuels hétérogènes de coexister simultanément sur les mêmes équipements matériels.

L'approche NFV a été initié par l'organisme ETSI dans l'objectif de virtualiser les services et fonctions du réseau et de gérer les machines virtuelles en fonction des demandes des utilisateurs.

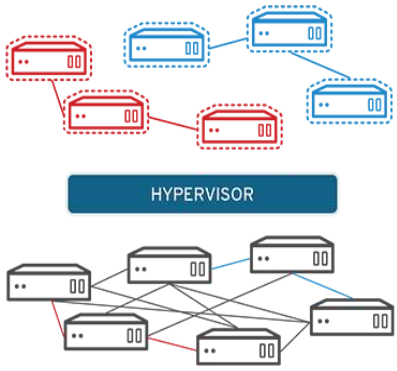


Figure 2.1-7 Virtualisation réseau [2]

2.2 Définition du cloud computing

La définition suivante du cloud computing est un extrait de la définition du National Institut of Standards and Technology (NIST, États-Unis) et du groupe spécialisé de l'UIT.

« Le cloud computing est un modèle qui offre aux utilisateurs du réseau un accès à la demande, à un ensemble de ressources informatiques partagées et configurables, et qui peuvent être rapidement mises à la disposition du client sans interaction directe avec le prestataire de service. »

Autrement dit les utilisateurs louent des ressources informatiques déjà opérationnelles sans se soucier de comment elles ont été implantées, du stockage et de la gestion selon une solution bien définie.



Figure 2.2-1 Cloud computing [3]

2.2.1 Les différents modèles de déploiement cloud

Tous les cloud ne sont pas identiques et aucun type de cloud computing ne convient à tout le monde. Plusieurs modèles, types et services différents ont évolués pour aider les entreprises à choisir la solution adaptée à leurs besoins. En effet, pour un déploiement optimal, l'entreprise se doit d'abord de définir le type d'architecture de cloud computing sur lequel ses services cloud seront implantées.

1. Cloud public

Un cloud public est une infrastructure informatique dans laquelle un fournisseur de services met des ressources à la disposition du public à travers internet. Les ressources peuvent être des capacités de stockage, des machines virtuelles ou des applications.

2. Cloud privé

Les cloud privés offrent des niveaux de :

- Sécurité supérieure aux pare-feu de l'entreprise
- Hébergement interne
- Et une confidentialité qui garantisse que les fournisseurs tiers ne peuvent pas accéder aux données sensibles

3. Cloud Communautaire

Le cloud communautaire qui est récent, est similaire à un cloud privé, mais où les ressources sont partagées entre les membres d'une communauté fermée ayant des intérêts similaires. L'infrastructure peut être gérée par ces organisations ou par un tiers. Elle peut leur être interne ou externe.

4. Cloud hybride

C'est une solution qui associe un cloud privé, un ou plusieurs services cloud public et un logiciel propriétaire permettant la communication entre chaque service.

2.2.2 Les différents types de services Cloud

Il y a différents services proposés dans le cloud qui répondent chacun à des besoins spécifiques. Chacun d'eux fournissent des services bien appropriés à la demande de l'utilisateur.

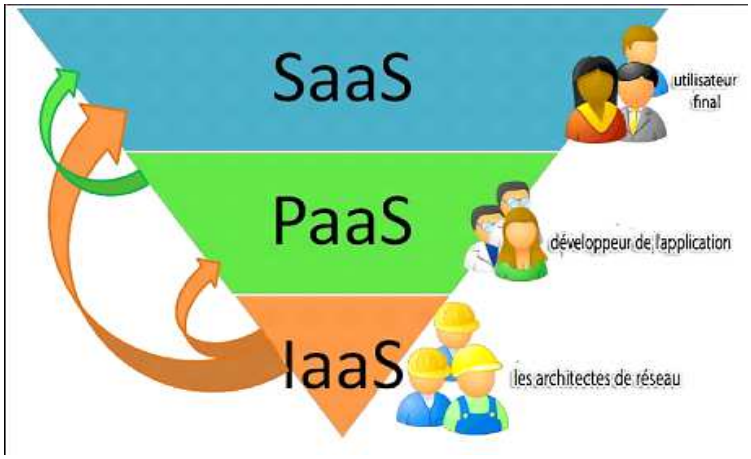


Figure 2.2-2 Couches Cloud computing

1. Infrastructure as a Service

Les fournisseurs d'IaaS proposent des machines virtuelles, des bibliothèques d'images de machines virtuelles, un stockage brut et basé sur des fichiers, des pare-feu, des équilibreurs de charge, des adresses IP, des réseaux locaux virtuels (VLAN), des logiciels et autres ressources informatiques nécessaires. Avec ce service, le consommateur est capable de déployer et d'exécuter des logiciels arbitraires, qui peuvent inclure des systèmes d'exploitation et des applications et il ne gère ni ne contrôle l'infrastructure, mais il a le contrôle des systèmes d'exploitation, du stockage, des applications déployées, et éventuellement un contrôle limité de certains composants réseau (par exemple, les pare-feu hôtes).

Types de IaaS

Exemples d'IaaS : Amazon EC2, GoGrid, iland, Rackspace Cloud Servers, ReliaCloud.

Toutes les infrastructures sont fournies à la demande du client.

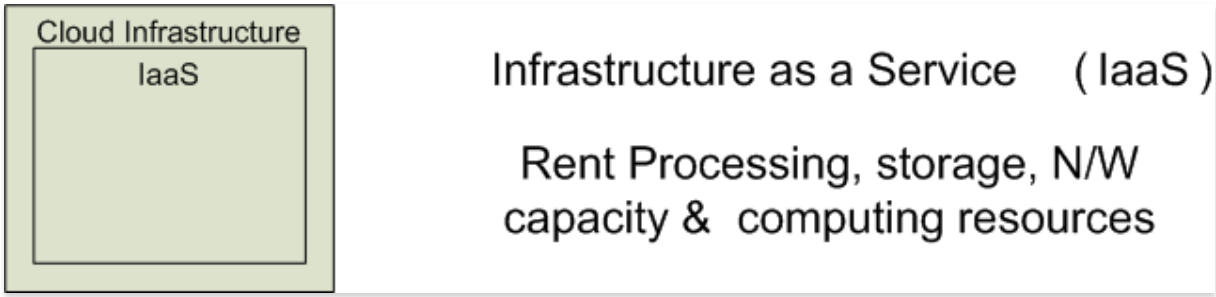


Figure 2.2-3 Infrastructure IaaS

Il y a différents types de fournisseurs de cloud IaaS, cela dépend selon le besoin du client :

- Stockage et la bande passante
- Développement et test
- Haute performance
- Partage des ressources

2. Platform as a Service

Le PaaS fournit une plate-forme informatique et une pile de solutions en tant que service. Elle offre la possibilité de déployer sur l'infrastructure en nuage des applications créées ou acquises par le consommateur et créées à l'aide de langages de programmation, d'outils et de bibliothèque pris en charge par le fournisseur. L'utilisateur ne gère ni ne contrôle la plate-forme. Le fournisseur fournit les réseaux, les serveurs, le stockage et les autres services par contre le consommateur a le contrôle sur les applications déployées et éventuellement sur les configurations de l'environnement d'hébergement de ces dernières.

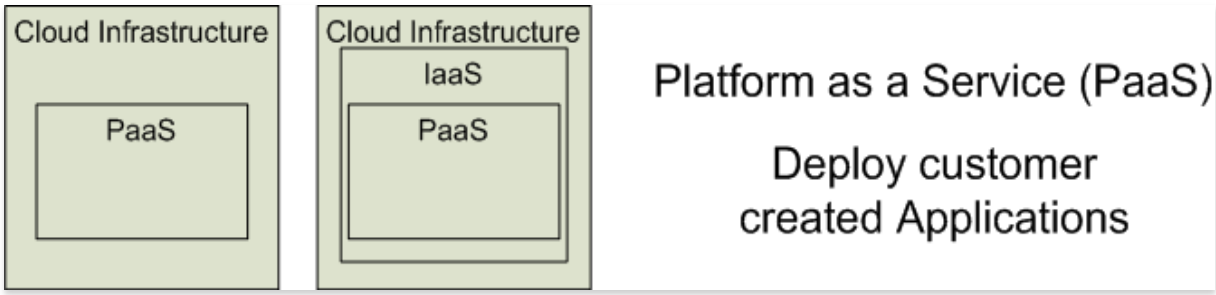


Figure 2.2-4 Infrastructure PaaS

Types de PaaS

Toutes les plateformes PaaS ne fournissent pas les mêmes services :

Plateformes d'applications sociales, plateformes comme Facebook fournissent des API que des tiers puissent écrire de nouvelles applications. Une fonctionnalité qui est mise à la disposition de tous les utilisateurs.

Plateformes informatiques comme Amazon Web services, Rackspace, Opsource fournissent le stockage, le processeur et la bande passante comme un service.

Plateformes d'applications Web comme Google Apps fournit des API et des fonctionnalités permettant aux développeurs de créer des applications qui tirer parti de sa cartographie, de son calendrier et de ses tableurs, ainsi que YouTube et d'autres services.

Plateformes d'applications commerciales comme WOLF permettent une meilleure abstraction des complexités techniques et est orienté vers les applications commerciales transactionnelles telles que les bases de données, l'intégration, le flux de travail et les applications utilisateur service d'interface.

Par exemple de **plateforme cloud** nous pouvons citer Windows Azure, Google App.

3. Software as a Service

Le SaaS est un système dans lequel une application est hébergée en tant que service fourni aux clients sur l'internet. La possibilité offerte aux consommateurs est d'utiliser les applications du fournisseur fonctionnant sur une infrastructure en nuage. Elles sont accessibles à partir de divers dispositifs clients tels qu'un navigateur web (par exemple, le courrier électronique basé sur le web). Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation et le stockage, etc....

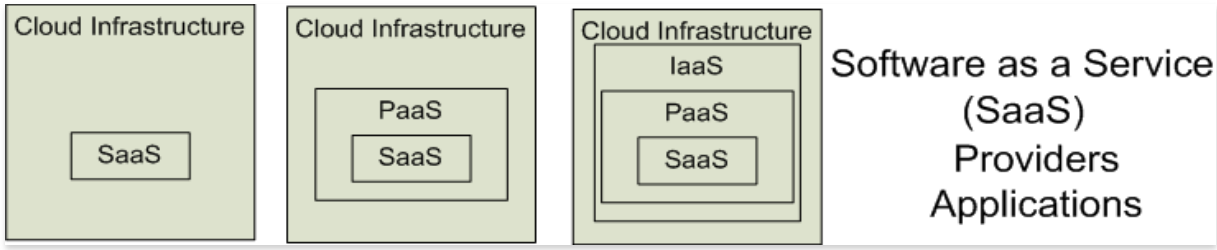


Figure 2.2-5 Infrastructure SaaS

Types de Saas

Le SaaS allège le fardeau de la maintenance des logiciels. Les types de services offertes par les cloud de types SaaS sont :

- Business Utility SaaS : des applications telles que l'automatisation de Saleforce sont utilisées par les entreprises et les particuliers pour gérer et collecter des données, la rationalisation des processus de collaboration et la fourniture d'analyse exploitable. Les utilisations les plus populaires sont : la gestion de la relation client (CRM), ressources humaines et comptabilité.
- Social Network SaaS : des applications comme Facebook sont utilisées par les entreprises pour se mettre en réseau et partager des informations, photos, vidéos, etc.

4. Informatique Serverless

Se chevauchant avec le PaaS, l'informatique serverless se concentre sur la création de fonctionnalités applicatives sans perdre de temps en lien avec la gestion permanente des serveurs et de l'infrastructure requise. Le fournisseur cloud se charge de la configuration, de la planification et de l'administration du serveur. Les architectures serverless sont hautement scalables et basées sur des évènements. Autrement dit elles consomment les ressources que si une activité est en cours. Comme fournisseur de plateforme sans serveur il y a AWS Lambda [3].

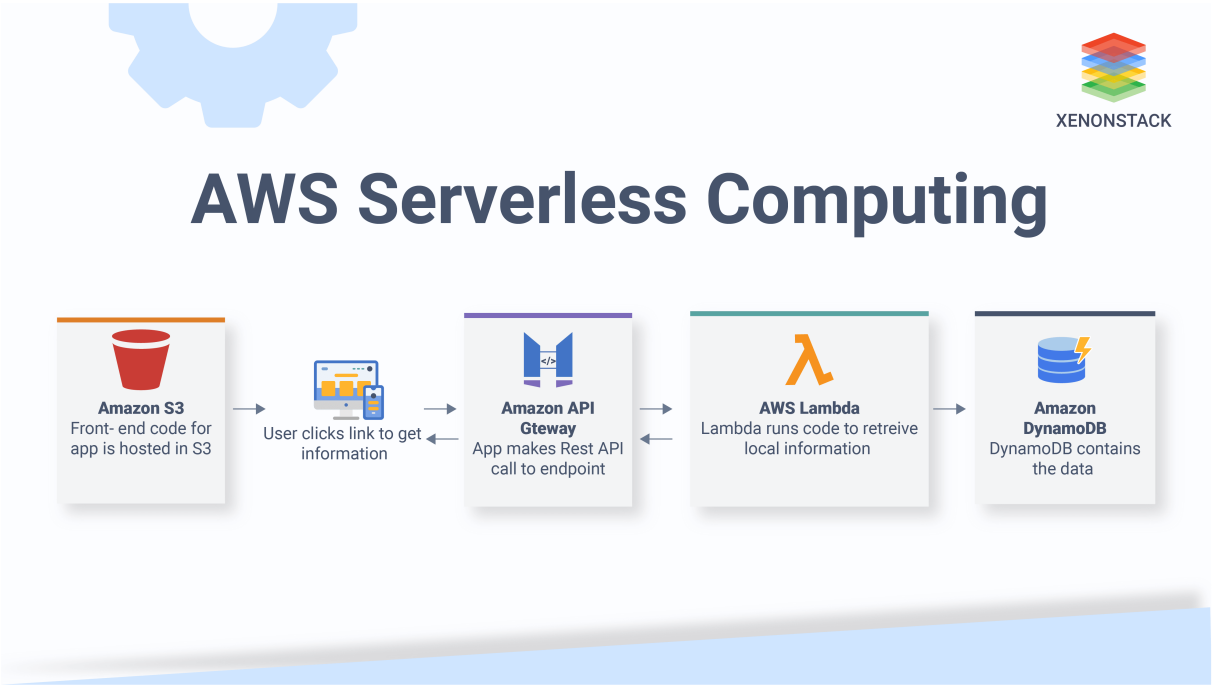


Figure 2.2-6 AWS Serverless computing [3]

5. Datacenter

Datacenter ou centre de données est un site regroupant des installations informatiques (serveurs, routeurs, commutateurs, disques durs, etc.) chargés de stocker et de distribuer des données à travers un réseau ou via accès par Internet.



Figure 2.2-7 Datacenter [3]

2.2.3 Les acteurs du cloud computing

Parmi les intervenants au niveau du cloud computing nous avons les fournisseurs, qui mettent à la disposition des organisations des services informatiques fonctionnels et les éditeurs qui proposent à ses clients un service cloud comprenant l'infrastructure et l'accès à l'ERP.

Parmi les plus grands fournisseurs qui occupent presque le marché du cloud computing nous avons :

1. Microsoft Azure

Lancée en 2010, Microsoft Azure est la plateforme cloud de Microsoft. Elle regroupe divers services de cloud computing en passant par des solutions open-source et des technologies propriétaires de Microsoft ou d'autres entreprises [4]. Elle permet de profiter de ressources de cloud computing à la demande, simplifier l'utilisation et l'administration de technologies Microsoft comme Windows serveur, SharePoint et Active Directory.

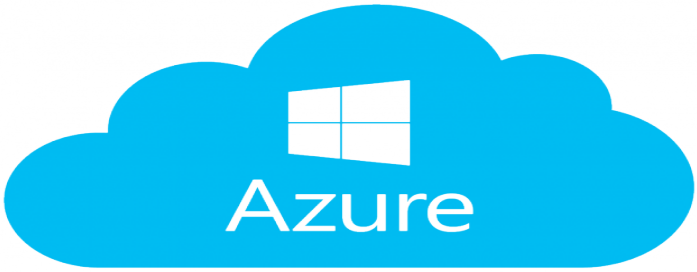


Figure 2.2-8 Microsoft Azure

2. Amazon Web Services

Amazon Web Services est une division du groupe américain de commerce électronique Amazon, spécialisée dans les services de cloud computing à la demande pour les entreprises et les particuliers [5].



Figure 2.2-9 Amazon Web Services

3. Google Cloud Platform

Google Cloud Platform est une plateforme de cloud computing fournie par Google, proposant un hébergement sur la même infrastructure que celle que Google utilise en interne pour des produits tels que son moteur de recherche. Cloud Platform fournit aux développeurs des produits permettant de construire une gamme de programmes allant de simples sites web à des applications complexes [6].

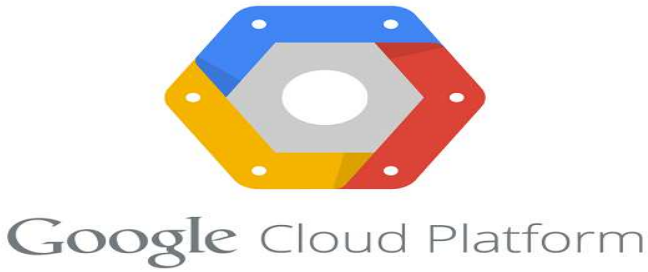


Figure 2.2-10 Google Cloud Platform

2.2.4 La sécurité informatique et le cloud computing

1. La sécurité informatique

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mise en place pour conserver, rétablir et garantir la sécurité de l'ensemble des ressources (matériels, logiciels, personnels, données et procédures) de l'organisme.

Elle peut s'évaluer suivant plusieurs critères parmi lesquels :

- **La disponibilité** : garantie que les ressources considérées seront accessibles au moment voulu par les personnes ayant droit.
- **L'intégrité** : garantie que les données sont exactes et complètes.
- **La confidentialité** : garantie que seules les personnes autorisées ont accès aux éléments considérés.

D'autres aspects peuvent également faire l'objet d'évaluation de la sécurité au sein d'un système d'information :

- **La non-répudiation** : garantie qu'une transaction ne peut être niée.
- **La traçabilité** : garantie que l'accès et les tentatives d'accès aux données sont tracés et que ces traces sont conservées et exploitables.
- **L'authentification** : consistant à assurer que seules les personnes autorisées aient accès aux ressources.

2. Sécurité dans le cloud

L'utilisation de plus en plus fréquente du cloud computing fait apparaître de nouveaux risques de sécurité. Augmentant ainsi l'intérêt des attaquants à trouver de nouvelles vulnérabilités et exposant les utilisateurs à voir leurs données compromises.

D'après une étude de l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) les risques plus importants qui surviennent dans le cloud sont liés directement ou indirectement à la confidentialité des données : l'échec de l'isolation, la gestion des interfaces compromises, la protection des données, la suppression non sécurisée ou incomplète des données et les attaques de l'intérieur [7].

Le problème d'isolation réside dans le fait que l'environnement (machine virtuelle) d'un attaquant peut potentiellement se retrouver sur la même machine physique d'un utilisateur cause que cette dernière héberge de multiples machines virtuelles. Cela lui permet de mettre en place différentes attaques matérielles ou logicielles pour écouter ou perturber les autres machines virtuelles. [8]. Les problèmes recensés concernant la sécurité au niveau du cloud sont nombreux et devraient être traités par le fournisseur de service de cloud afin de convaincre les utilisateurs d'utiliser cette technologie.

Le plus important, à notre avis, est de garantir l'intégrité et la confidentialité des données des utilisateurs pendant qu'elles sont stockées dans le nuage. Dans une longue chaîne de fournisseurs non transparente, il est difficile pour un utilisateur final de déterminer quels mécanismes de sécurité sont appliqués aux données dans le cloud [9]. Nous allons maintenant voir quelques mécanismes utilisés pour garantir la sécurité surtout la confidentialité et l'intégrité des données des organisations dans le cloud computing.

a. La dissimulation de données

Cette technique consiste à garantir l'intégrité et la confidentialité des données en réalisant une injection dans la base de données des informations artificielles en respectant certaines propriétés [7] :

- Pas de perte de données réelles
- Récupération facile des données par le propriétaire légitime
- La génération des données artificielles doit tenir compte de l'évolution naturelle du nombre d'entrées.
- Impossible qu'une tierce personne trouve les données d'une autre
- La dissimulation doit se faire tout en partie ou en temps réel.
- Les données artificielles doivent paraître identiques que les données à insérer

b. Services Level Agreements

Les Service Level Agreements précisent les niveaux minimums de performance que le client peut attendre, par exemple : 99,99% de disponibilité du système par an [9]. Les SLAs n'ont pas couvert les aspects de sécurité tels que la confidentialité et l'intégrité.

c. VPN

Les réseaux privés virtuels permettent de garantir une connexion sécurisée entre un utilisateur et un site distant dans le cas d'un cloud privé.

d. Les contrôles de sécurité

L'objectif des contrôles de sécurité du cloud est de réduire les vulnérabilités à un niveau tolérable et de minimiser les effets d'une attaque. Pour ce faire, une organisation doit déterminer quel impact pourrait avoir une attaque, et la probabilité de perte. C'est-à-dire de faire une analyse des risques qui pourraient se produire.

Parmi les moyens utilisés pour assurer la sécurité dans un cloud:

- **Azure Security Center :** qui assure les fonctionnalités de gestion de la sécurité et permet la protection avancée contre les menaces dans l'ensemble des charges de travail cloud hybrides [10].
- **Application Gateway :** permet de créer des serveurs web frontaux sécurisés, scalables et à haut niveau de disponibilité dans Azure [10].
- **Protection DDos Azure :** assure la protection des applications contre les attaques de types DDos 5Distributed Denial of Service)
- **Azure Advanced Threat Protection :** c'est une solution de sécurité cloud qui identifie les menaces avancées, les identités compromises et les actions malveillantes initiés contre l'entreprise [10].

  Il est aussi capable de détecter les attaques et techniques malveillantes connues, les problèmes de sécurité et les risques encourus par votre réseau.

Conclusion

Dans cette partie il a été question de faire une étude sur la virtualisation et le cloud computing en parlant de leurs définitions, les différents types de virtualisation qui existent et hyperviseurs mais aussi les possibles architectures de déploiement cloud et les services cloud existants avant de passer à la sécurité informatique et le cloud computing.

CHAPITRE 3 : *Etude de l'existant et Objectifs de la mission technique*

Dans cette partie nous allons faire la présentation en détaille de l'infrastructure existante d'EXPERT IS c'est-à-dire parler de ses différents composants et la solution cloud que l'on utilise et donner les raisons pour lesquelles nous faisons une optimisation de l'infrastructure.

3.1 Étude de l'infrastructure existante

Il faut noter que au sein d'EIS, nous avons une infrastructure Hybride c'est-à-dire une partie sur site et l'autre dans le cloud, représentée par le figure ci-dessous :

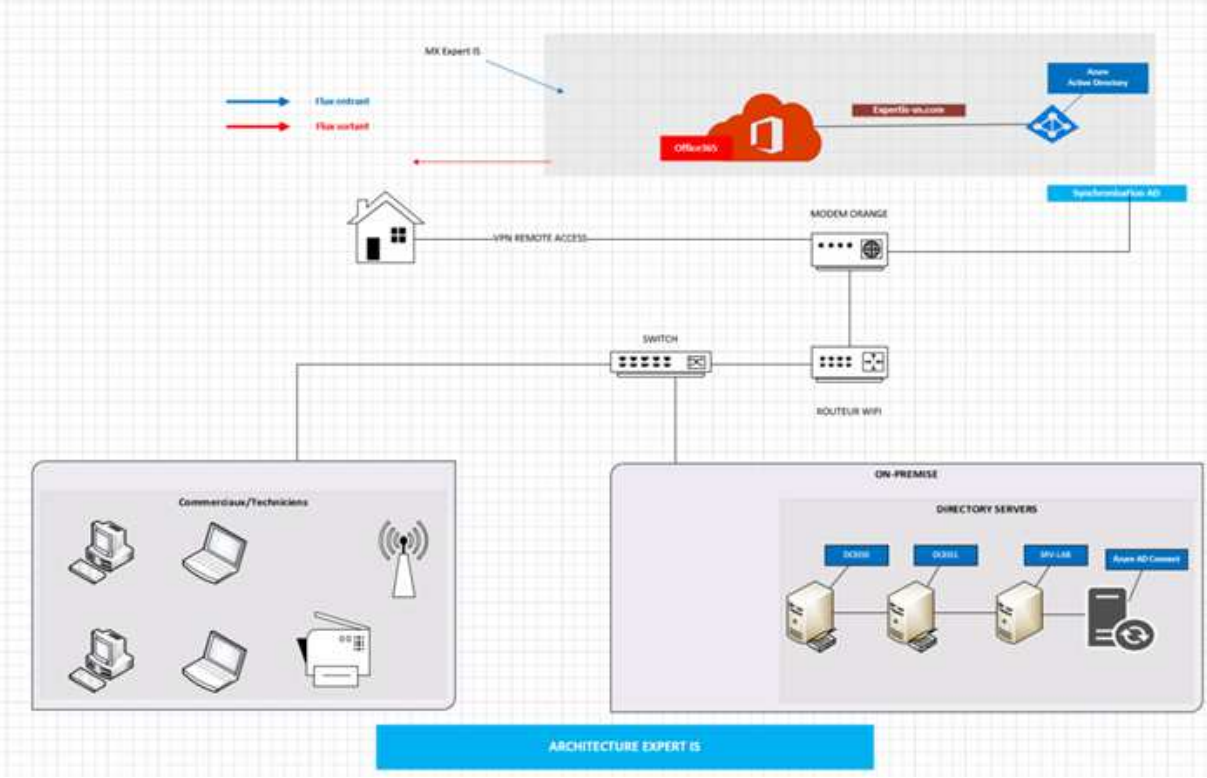


Figure 3.1-1 Architecture EXPERT IS

D'après l'architecture ci-dessus, l'entreprise dispose de plusieurs serveurs et services dont les détails sont ci-après :

- Un serveur AD primaire : qui est le serveur Active Directory primaire stocke les données d'annuaires et gère les communications entre les utilisateurs et les

domaines, y compris les processus d'ouverture de session d'utilisateur, l'authentification et les recherches dans l'annuaire ;

- Un serveur DNS primaire : qui est un système de nom hiérarchique et décentralisé pour les ordinateurs, services, ou d'autres ressources connectées à Internet ou à un réseau privé. Il associe différentes informations avec un nom de domaine assigné à chaque participant d'une entité du réseau.
- Un serveur AD secondaire : son rôle est de prendre le relai en cas de panne ou dysfonctionnement noté au niveau du serveur principal. Il est tout le temps en parfait synchronisation avec le serveur primaire pour enregistrer toutes modifications apportées sur le réseau.
- Un serveur de test : ce serveur est destiné pour les test sur des applications et systèmes de collaboration.
- Un serveur de synchronisation : qui permet de faire la synchronisation de l'annuaire entre le cloud (office 365) et le serveur active directory.
- SIMPLYDESK : c'est un serveur hébergeant une solution support qui nous permet de mettre très rapidement en œuvre un helpdesk adapté à un environnement que vous soyez un service client (SAV, Hotline, ...) ou un service interne ayant besoin de gérer toute question, incident, demande de service....
- Un service DHCP qui gère l'allocation dynamique des adresses IP aux différents composants réseau de l'organisation.
- Un service VPN Remote Access qui met à disposition aux utilisateurs en déplacement des connexions sécurisées pour faire du télétravail.

3.1.1 Présentation de Microsoft Azure

Lancée en 2010, Microsoft Azure est la plateforme cloud de Microsoft. Elle regroupe divers services de cloud computing en passant par des solutions open-source et des technologies propriétaires de Microsoft ou d'autres entreprises [4]. Elle permet de profiter de ressources de cloud computing à la demande, simplifier l'utilisation et l'administration de technologies Microsoft comme Windows serveur, SharePoint et Active Directory.

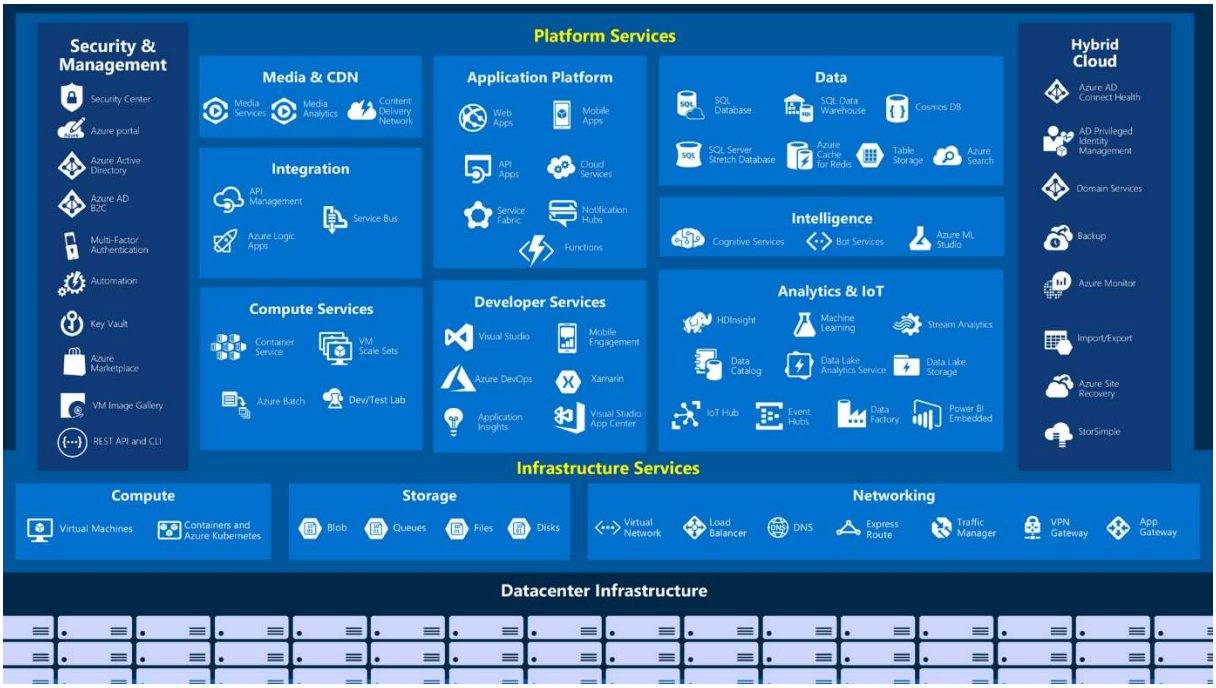


Figure 3.1-2 Microsoft Azure

3.1.2 Services Azure

En tant que plateforme de services cloud, Microsoft Azure propose différents services afin d'améliorer l'organisation, l'usage et la gestion des infrastructures informatiques.

3.1.2.1 Azure Active Directory

Il permet de synchroniser les répertoires de l'annuaire locale et assure l'authentification unique comme multifacteur aussi afin d'aider les utilisateurs à se protéger contre des attaques de cybersécurité.

3.1.2.2 Mise en réseaux

Avec Azure DNS, les entreprises pourront héberger leur système de noms de domaine dans azure qui prend en charge tous types d'enregistrement DNS Courants avec une garantie de la très haute disponibilité et une mise à jour rapide des enregistrements DNS.

3.1.2.3 Stockage

Avec ce service, Azure offre une possibilité de stocker tous les type de données. Il peut stocker jusqu'à 64 To d'informations sur des disques offrant également la sauvegarde et la récupération des données.

3.1.2.4 Base de données SQL

Avec cette fonctionnalité, les services de bases de données SQL Azure simplifient les opérations telles que :

- La migration des charges de travail SQL avec SQL Server sur des machines virtuelles Azure.
- Prise en charge d'applications modernes avec Azure SQL Database.
- Modernisation de vos applications existantes avec Azure SQL Managed Instance

3.1.2.5 Services Kubernetes

Azure Kubernetes Services offre la création, la mise à l'échelle et la mise à niveau pour permettre une efficacité beaucoup plus accrue aux développeurs. Autrement dit c'est un outil d'orchestration avec des architectures distribuées sur plusieurs conteneurs.

3.1.2.6 App Services

Cette fonctionnalité dans Azure permet de mettre en place rapidement des applications conçues avec les langages (.NET, .NET Core, Node.js, java, Python ou PHP) dans des conteneurs ou les exécutées sur Windows ou Linux.

3.2 Objectifs de notre mission

Aujourd'hui les chaines de valeur des entreprises sont composées d'environ 20 entreprises, l'avènement de Consumer IT ou du Web2.0, des réseaux sociaux et l'internet des objets transforment la façon dont nous vivons, dont nous apprenons, dont nous collaborons, travaillons, consommons et jouons. Ces changements dans la société transforment également la façon dont nous concevons, gérons nos entreprises et notre chaine de valeur afin de les adaptées aux changements du monde extérieur.

Ainsi pour être en phase avec l'évolution dans le domaine des technologies de l'information et de la communication, les organisations doivent mettre en place des solutions d'infrastructure informatique flexible, évolutive avec la possibilité d'accéder aux ressources de l'organisation depuis n'importe où, n'importe quand avec tout type d'appareil et une gestion centralisée de l'infrastructure tout en garantissant la haute disponibilité, l'intégrité et la confidentialité des ressources.

C'est dans ce contexte que nous sommes chargés d'optimiser l'infrastructure existante d'EIS en mettant en place une solution d'accès terminal serveur, configurer une solution d'office 365 et la mise en place d'un serveur messagerie exchange en interne afin de

pouvoir garantir les critères qui sont la disponibilité et la confidentialité de certaines ressources sensibles.

L'optimisation de l'infrastructure d'EIS a pour but de mettre en place une solution qui garantira la disponibilité des services, des performances adaptables en fonction de nos besoins et aussi garder le contrôle sur des applications et des données sensibles.

3.3 Moyens mis à disposition du stagiaire

Pour la réalisation de cette tâche, EIS a mis à notre disposition toutes les ressources matérielles et humaines nécessaires afin d'y parvenir :

- Une Licence Office 365 Business E3
- L'accès au portail Microsoft Azure
- L'accès à la documentation officielle des services Microsoft
- L'autorisation d'accéder aux ressources techniques de l'entreprise
- L'accès à la documentation officielle de l'entreprise

Conclusion

Au cours de ce chapitre nous avons eu à faire une présentation de l'infrastructure d'EIS, en parlant des différentes entités qui la compose, la présentation de la solution Azure de Microsoft qu'ils utilisent et ses services et finir par décrire les objectifs de la mission qui nous a été confiée.

CHAPITRE 4 : *Réalisation du projet*

Durant cette partie nous parlerons de l'architecture a déployée après une étude des besoins soulevés. Nous finirons ensuite par une présentation et la configuration de chaque sous-système que nous allons déployer, de la solution d'accès terminal serveur en passant par la configuration d'office 365 à la configuration de Microsoft Exchange Serveur.

4.1 Conception générale

D'après une étude de l'architecture existante et des besoins exprimés, nous avons pu faire une description des différents services présents et quelles solutions optées afin de répondre aux exigences formulées. Raison pour laquelle nous choisissons d'ajouter des serveurs à l'architecture existant afin de mettre en exécution la mission qui nous été confiée.

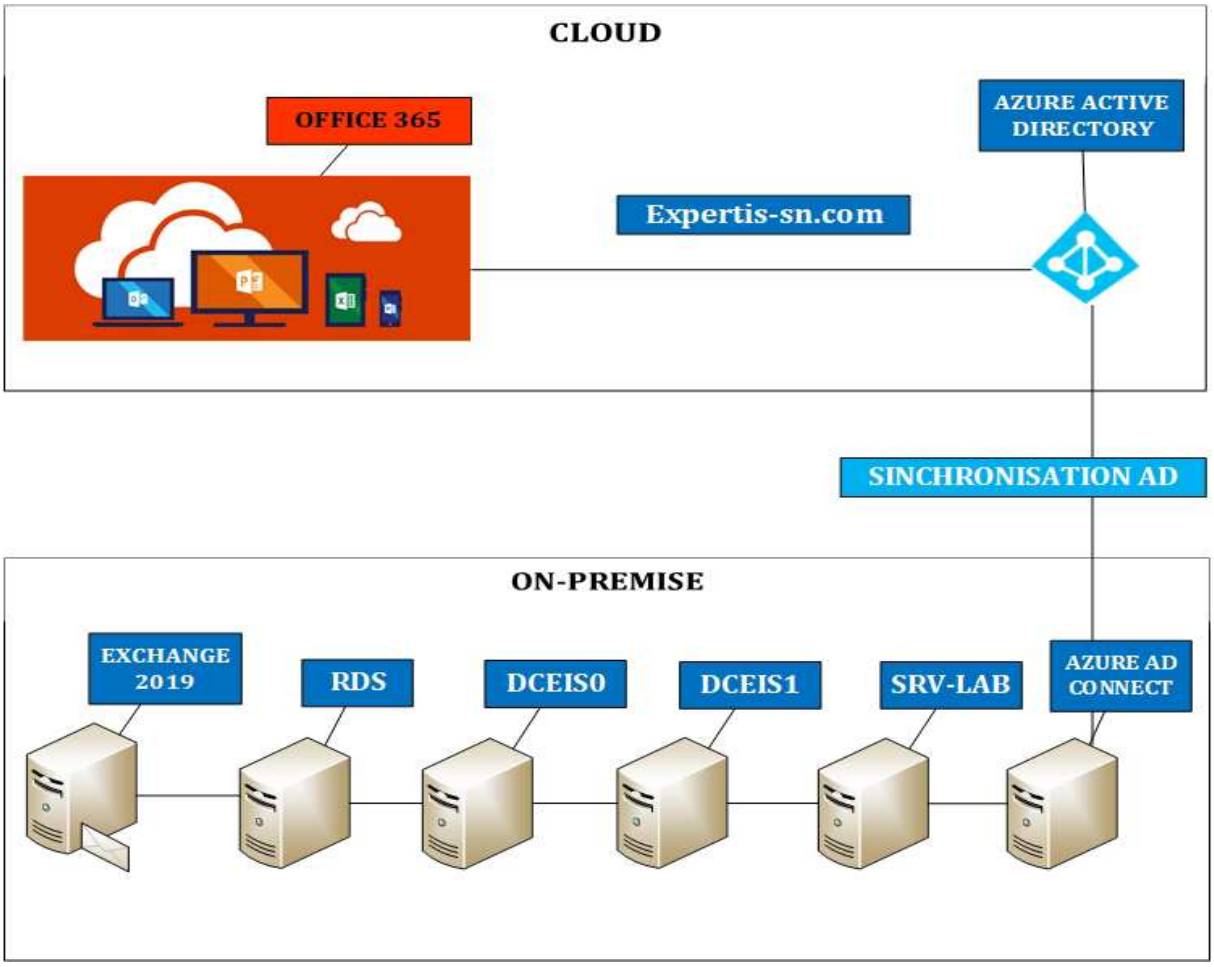


Figure 4.1-1 Architecture déploiement

Cette architecture est composée de deux parties :

Coté On-premise nous avons :

- Un serveur de contrôleur de domaine primaire qui stocke les données d'annuaire et assure l'authentification des utilisateurs.
- Un serveur de contrôleur de domaine secondaire pour la redondance
- Un serveur Azure AD connect pour assurer la synchronisation entre le site local et le cloud
- Une ferme de serveurs de Bureau à distance
- Un serveur Microsoft Exchange pour la messagerie locale synchronisé aussi avec Exchange online.

Au niveau du Cloud nous avons :

- Office 365 est ses différents composants et services comme la suite office, Teams, etc.
- Azure Active Directory qui assure la synchronisation des répertoires de l'annuaire locale et l'authentification des utilisateurs.

4.2 Conception détaillée

Dans cette partie nous allons aborder plus en détail l'ensemble des différentes fonctionnalités que nous ajouterions sur l'architecture déjà existante.

4.2.1 Accès Terminal Serveur

Remote Desktop Services (**RDS**) ou Services Bureau à distance est une architecture centralisée qui permet à des utilisateurs de se connecter sur un ordinateur distant utilisant Microsoft Terminal Services. Il utilise Remote Desktop Protocol (RDP) pour l'affichage sur le Terminal Léger (TL) ainsi que la communication des périphériques. Il a été implémenté à partir de la version R2 de Windows Server 2008.

En somme, RDS permet la virtualisation d'un poste en séparant l'environnement utilisateur de l'ordinateur (appelé TL) le résumant à un simple terminal. Un élément permet de gérer les machines virtuelles, et de répartir la charge des sessions utilisateur (en renvoyant la connexion utilisateur vers la machine virtuelle concernée) : le Connexion Broker. RDS fait partie de la Virtual desktop infrastructure (VDI) mise en place par Microsoft.

4.2.1.1 Prérequis

Tableau 4.2-1 Prérequis matériels et logiciels

Prérequis matériels	
RAM	Le minimum recommandé est que les serveurs doivent avoir 2Go de RAM au moins qui peuvent aller jusqu'à 8 Go dans certains environnements de travail [11].
CPU	Un virtuel processeur dual-Core au moins
DISQUE DUR	Un disque dur virtuel de 50 Go minimum
RESEAU	Une carte réseau virtuel et une adresse IP statique pour tous les serveurs
Prérequis logiciels	
Windows 2012 R2	Les serveurs doivent avoir comme système minimum requis serveur 2012 R2 édition Datacenter
Domaine active Directory	Domaine active directory est obligatoire

4.2.1.2 Architecture de déploiement

Il faut noter que l'environnement devant accueillir les rôles RDS doit obligatoirement déployer auparavant le rôle Active Directory Domain Services et un serveur de fichiers qui est optionnel. Tous les serveurs de l'infrastructure doivent être dans le même domaine.

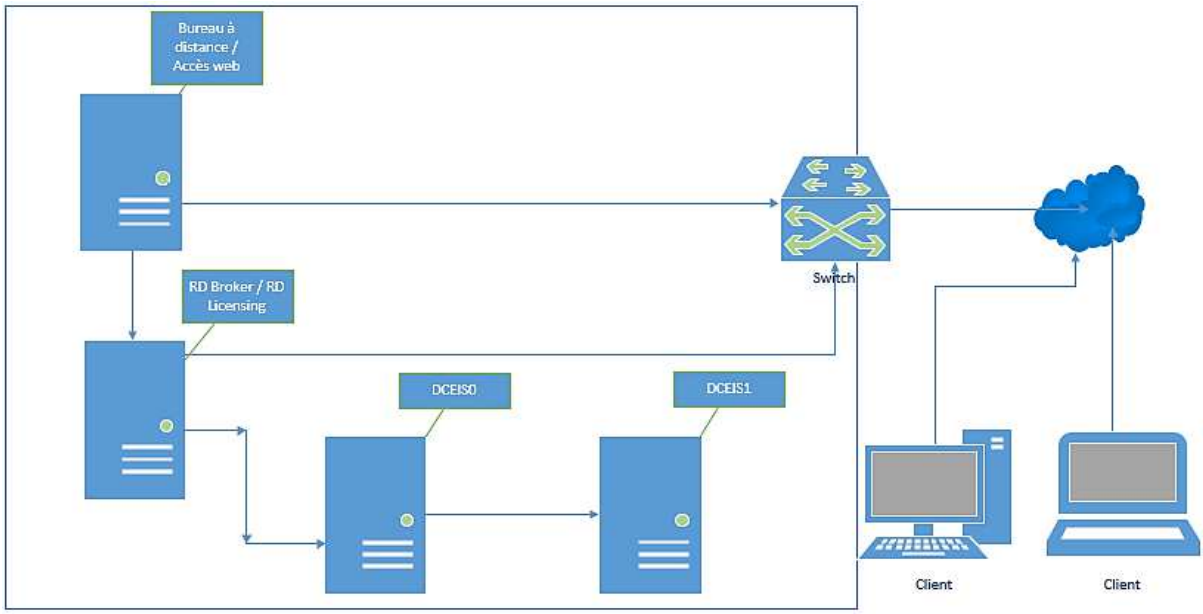


Figure 4.2-1 Architecture ferme RDS

- Le rôle accès web ou passerelle d'accès à distance : permet aux différents utilisateurs qui ne sont pas dans l'environnement interne de l'entreprise de pouvoir y accéder de manière sécurisée grâce au protocole HTTPS ;
- Hôte de session bureau à distance : les utilisateurs se connecteront sur ce serveur ;
- RDS Broker : il gère les différents serveurs sur lesquels vont se connecter les utilisateurs de façon à répartir la charge de ces derniers ;
- Gestionnaire de licences : assure la distribution des licences (CAL RDS).
- Par défaut les serveurs hôte de la session bureau à distance autorisent un nombre illimité de sessions de service bureau à distance,
- Le bureau à distance pour administration autorise deux sessions de service bureaux à distance.
    - Il est aussi possible de mutualiser les deux rôles RD Broker et RD Licensing sur un unique et même serveur sachant que ces derniers ne prennent pas en charge directement la sollicitation des utilisateurs. Il est évidemment permis d'installer tous les rôles sur une même machine mais pour garantir la Haute disponibilité on peut installer les rôles sur différents serveurs.
    - Une plateforme RDS sans serveur de licences valide pourra fonctionner pendant une durée de 180 jours.

4.2.1.3 Multisession simultanées sous Windows

Avec Windows server, le droit d'utiliser le système d'exploitation après avoir acheté une licence n'est pas tout à fait le cas. Deux utilisateurs distants simultanés peuvent se faire avec le protocole Remote Desktop Protocol (RDP) de Windows.

Pour autoriser la connexion simultanée de plusieurs utilisateurs il faut obligatoirement les licences CAL de Windows Remote Desktop Services soumis par utilisateur ou par machine.

1. Windows Multisession

Anciennement appelé Windows 10 Enterprise pour Virtuel Desktop (EVD), est un hôte de session bureau à distance qui permet plusieurs sessions interactives simultanées. Cette fonctionnalité offre aux utilisateurs la réduction des coûts concernant l'achat de licences d'accès client RDS (CAL) [12]. Il faut noter qu'aussi le nombre de sessions interactives dépend des ressources matérielles du système utilisé :

- VCPU : le nombre de processeur virtuel alloué à la machine ;
- Mémoire : la quantité de mémoire RAM ;
- Disque : le stockage pour être en phase avec ces besoins ;
- VGPU : la capacité de la mémoire graphique à permettre aux utilisateurs de travailler avec beaucoup d'efficacité et de productivité.

Mais également le nombre de session de peut-être limité de la façon dont les utilisateurs exploitent les ressources matérielles et logicielles disponibles lorsqu'ils sont connectés.

NB : Il faut préciser que cette solution ne fonctionne pas dans un environnement de production en local mais seulement pour le service de Windows Virtual Desktop pour Microsoft Azure.

2. RDWRAP

L'objectif de ce logiciel est d'activer la prise en charge de Remote Desktop host et des sessions RDP simultanées sur des systèmes à fonctionnalités réduites pour une utilisation à domicile. Il fonctionne comme une couche entre le Service Control Manager et les services Terminal Server, de sorte que le fichier termsrv.dll d'origine reste intact.

3. Logiciels tiers

Parmi les logiciels tiers pouvant offrir la possibilité de faire du bureau à distance il y a :

- TeamViewer
- Anydesk
- NoMachine

4.2.1.4 Mise en œuvre de la solution Terminal serveur de Windows

Le déploiement des rôles de services bureau à distance requiert des prérequis dans l'environnement destiné. Parmi les prérequis dont leur configuration ne se trouve pas dans ce document nous avons :

- La création d'une machine virtuelle ;
- Déploiement de Windows Serveur 2019 Datacenter ;
- Configuration du réseau ;
- Jonction du serveur au domaine active directory ;
- Déploiement d'un domaine active directory ;

- Une adresse IP fixe pour le serveur RDS et être membre aussi du domaine AD.

Après la vérification de l'ensemble de ces prédispositions nécessaires pour le bon déroulement du déploiement des services RDS, nous passons maintenant à leur installation.

4.2.2 Déploiement des rôles Remote Desktop Service

Comme Windows Server 2016, Windows Server 2019 utilise une nouvelle façon d'installer les services bureau à distance basée sur des scénarios simplifiant ainsi l'installation des différents services de rôle bureau à distance sur un ou plusieurs serveurs. Ce mode d'installation installe et configure également le service de déploiement du Bureau à distance qui permet de gérer le serveur avec la nouvelle interface de gestion des services bureau à distance.

Nous avons différentes possibilités pour installer les services bureau à distance [13] :

- Installation des services bureau à distance : également appelé mode scénario, il permet de déployer sur un plusieurs serveurs les services de rôle Bureau à distance via un assistant d'installation graphique. Il permet aussi d'installer et de configurer les services de rôle RDS nécessaires au scénario choisi (par exemple : les services de rôle RDS Session Host, RD web et RD connection Broker seront installés pour un scénario en mode Hôte de session)
- Installation basée sur un rôle ou une fonctionnalité : ce mode d'installation permet d'installer chaque service de rôle d'une manière unique.
- PowerShell : avec PowerShell, il est possible de reproduire les deux types d'installation ci-dessus.

Pour le type d'installation, nous avons opté le mode d'installation des services Bureau à distance qui nous permettra d'installer les rôles Bureau à distance sur un ou plusieurs serveurs, permettant aussi de définir le type de scénario qui convient à nos besoins.

Depuis le serveur devant accueillir les services de rôles Bureau à distance, ouvrez le **Gestionnaire de serveur** cliquer sur le menu **Gérer** puis sur **Ajouter des rôles et fonctionnalités**

- La fenêtre de **l'Assistant Ajout de rôles et de fonctionnalités** s'ouvre et vous affiche à l'écran **Avant de commencer,** cliquez sur le bouton **Suivant.**

- Choisir **l'option installation de service bureau à distance** pour définir **le type d'installation** a adoptée et cliquez sur **Suivant.**
- Sur la page **Sélectionner le type de déploiement,** choisissez **Démarrage rapide** puis cliquez sur **Suivant.**
- Sur la page **Sélectionner le scénario de déploiement**, Choisissez **Déploiement de bureaux basées sur une session** puis cliquez sur **Suivant**.
- Sur la page **Sélectionner un serveur**, sélectionnez le nom du serveur pour l'installation des services de rôle Bureau à distance dans la colonne **Pool de serveurs,** cliquez sur la **flèche** au centre pour le définir en tant que serveur **Sélectionné.** Si l'installation se fait à partir d'un autre serveur, il se pourrai que le nom du serveur n'apparaisse pas, dans ce cas il faudra annuler l'installation, revenir au **Gestionnaire de serveur**, ouvrir le menu **gérer** et **Ajouter des serveurs** afin d'ajouter le serveur. Cliquez ensuite sur **Suivant.**

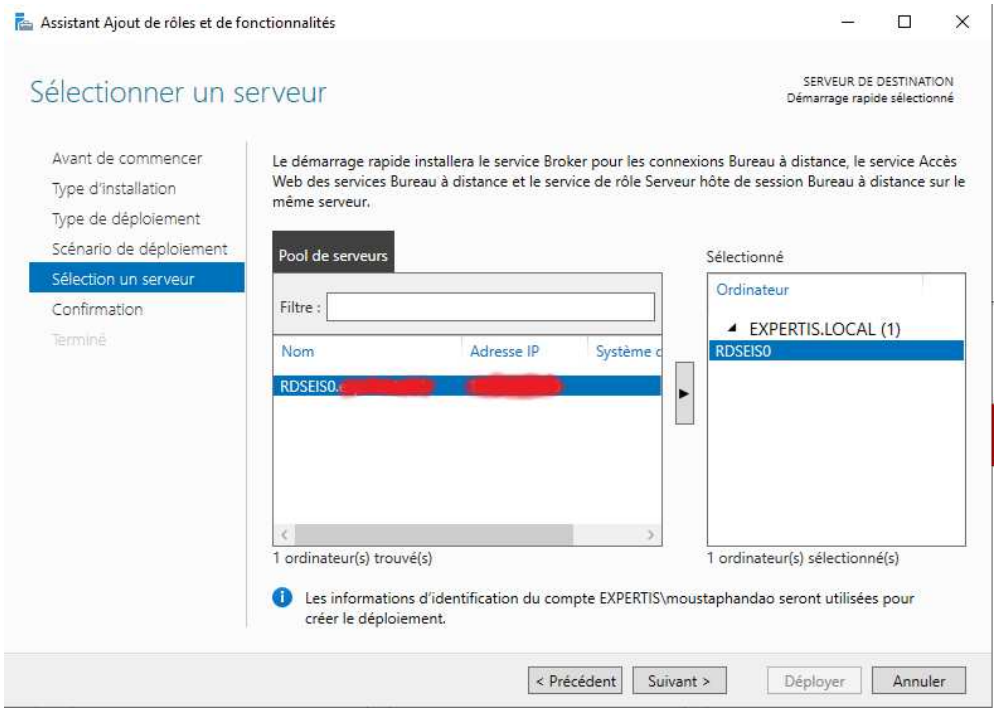


Figure 4.2-2 Sélectionner le Serveur Cible

- **Sur la page Confirmer les sélections,** Après la sélection du serveur devant accueillir les services de rôles de Bureau à distance, nous pouvons maintenant passer à une vérification des services choisis et n'oublier pas de cocher la **case redémarrer automatiquement le serveur de destination si nécessaire** et cliquez sur **Déployer.**

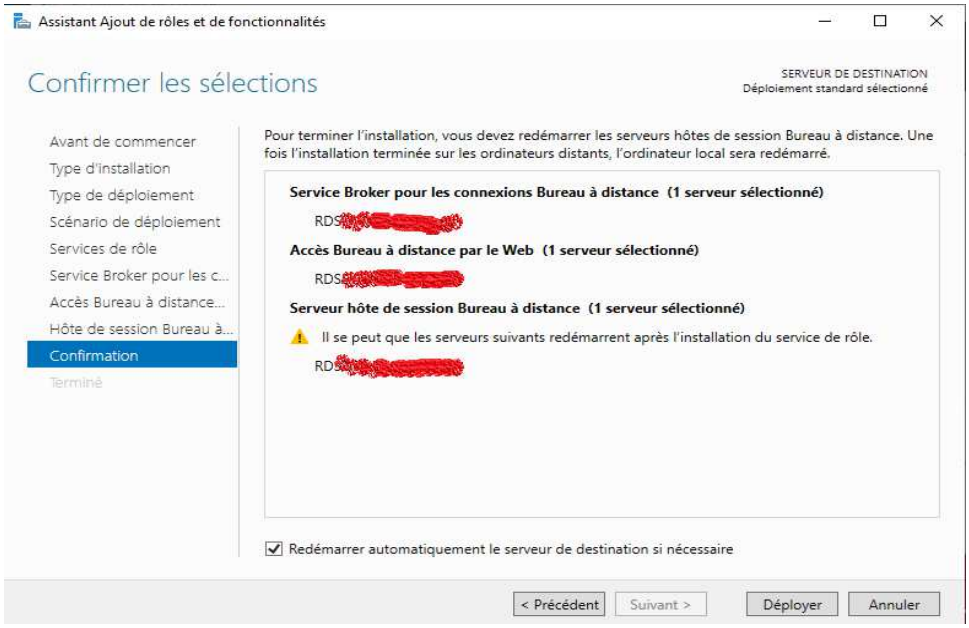


Figure 4.2-3 Confirmation des services RDS

Ainsi nous pouvons voir l'installation des différents services que nous allons installer sur notre serveur qui sont :

- Le **service Broker** qui permet la répartition des sessions dans une infrastructure RDS et gère aussi l'équilibrage de la charge entre les serveurs d'une même collection.
- Le **service de rôle Accès Web** permet de présenter les applications et bureau à distance des utilisateurs via un simple site web.
- Le **service de rôle serveur hôte de session** : permet à serveur d'héberger des applications ou le bureau complet de Windows. Avec ce service la limitation des deux utilisateurs est levée.

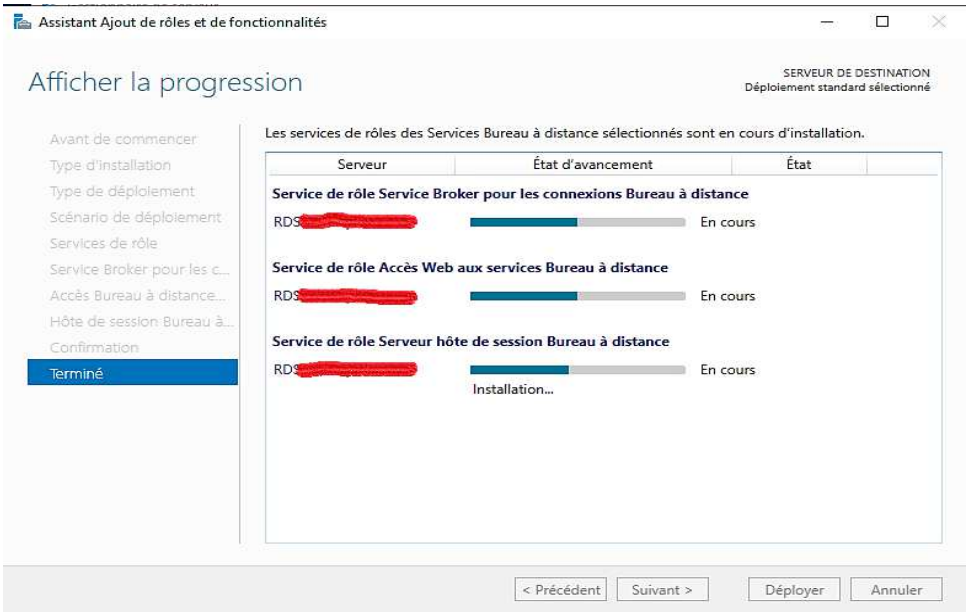


Figure 4.2-4 Installation des services RDS

Après que l'installation des différents services de rôles Bureau à distance ont été installés sur notre serveur. Nous pouvons voir maintenant depuis **Gestionnaire de serveur** sur le **Tableau de bord** les rôles ou fonctionnalités installés sur le serveur.

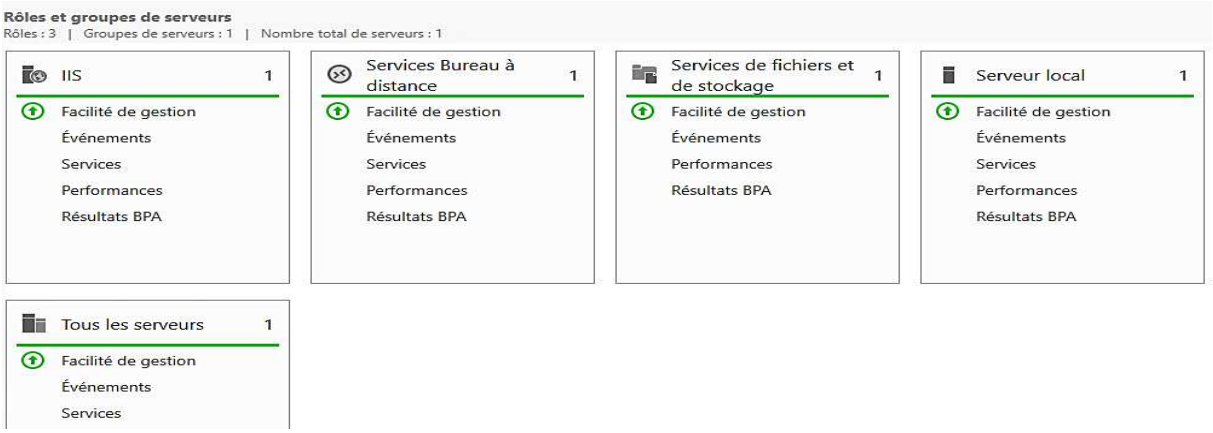


Figure 4.2-5 Services et rôles

Nous allons maintenant installer le **service de rôle Gestionnaire de licences** : qui gère l'attribution des licences CAL par périphérique ou utilisateur afin de se connecter au serveur RDSH.

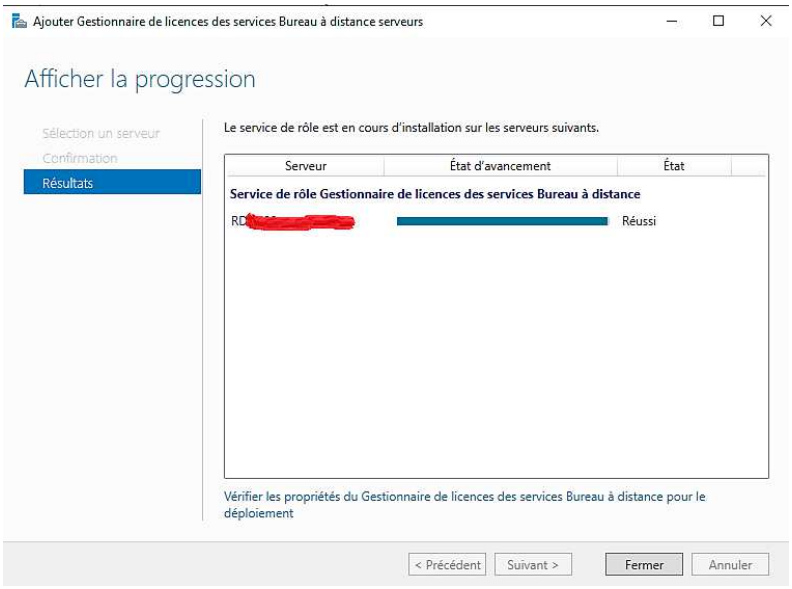


Figure 4.2-6 Installation service Broker

Après l'installation du gestionnaire de licence nous allons définir le mode de licences appropriée à notre besoin et choisir l'ordre des serveurs si toutefois plusieurs serveurs ont été installés. Nous avons opté le mode de licence par utilisateur qui permet à l'utilisateur concerné d'accéder au serveur afin d'utiliser des services tel que le stockage ou l'impression et il pourra aussi se connecter depuis plusieurs appareils.

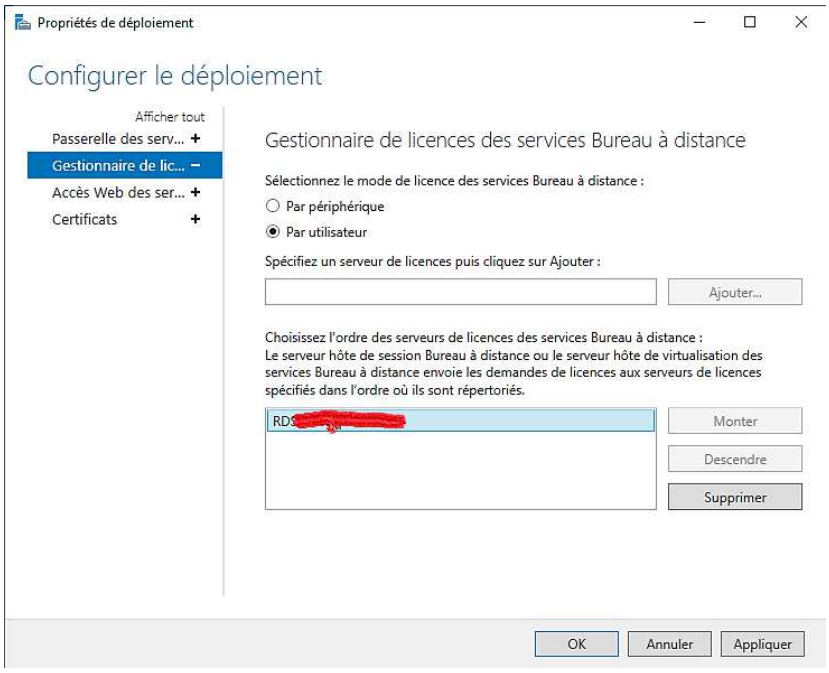


Figure 4.2-7 Choix du mode Licence CAL

Nous allons maintenant passer à la création d'une collection. Elle permet de configurer les services de rôles Bureau à distance en spécifiant les hôtes qui composent la collection et

qui peut y accéder. Depuis le **gestionnaire de serveur** sur la page de **gestions des collections**, cliquer **TACHES** et **Créer une collection de sessions.**

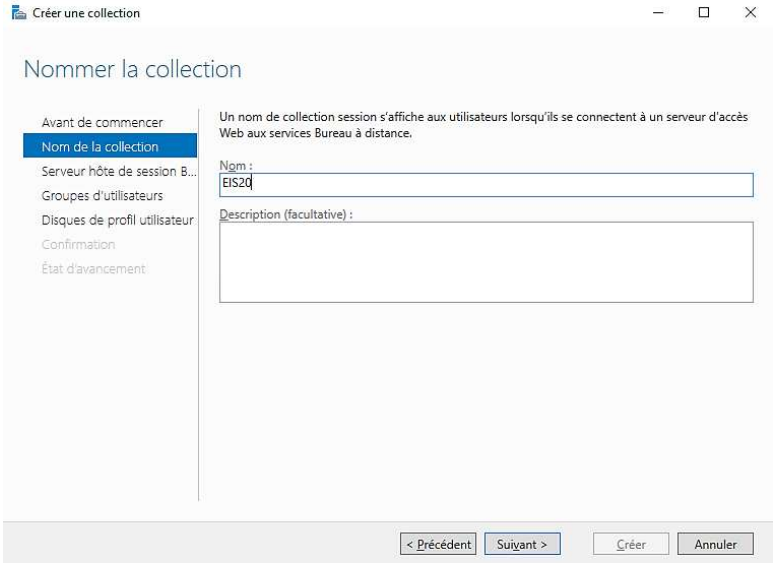


Figure 4.2-8 Création collection

Ajouter le(s) serveur(s) hôte(s) de sessions bureau à distance en cliquant sur la flèche pour spécifier le(s) serveur(s) qui doivent faire office de serveur hôte de sessions Bureau à distance.

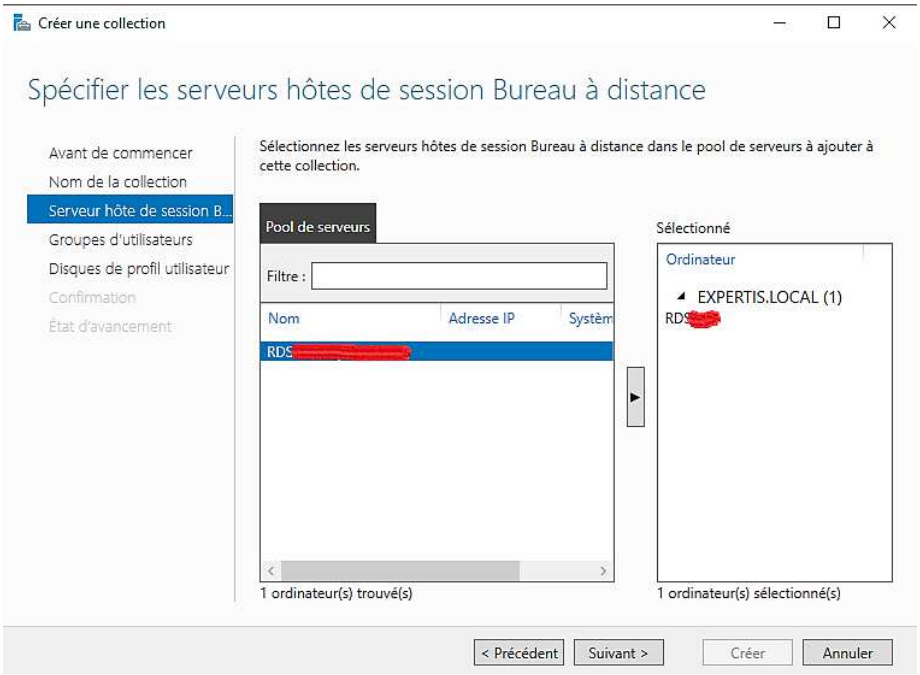


Figure 4.2-9 Spécification serveur hôte de session

A présent vu que le serveur a été sélectionné, nous allons définir les groupes d'utilisateur qui auront l'autorisation d'accéder au serveur afin de pouvoir utiliser ces services.

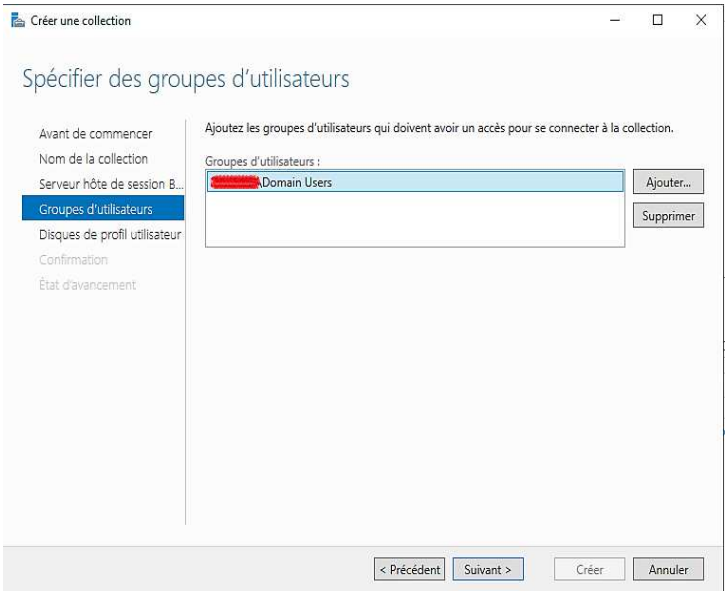


Figure 4.2-10 Autorisations des utilisateurs

Ainsi nous pouvons maintenant créer la collection de service hôte de session Bureau à distance en cliquant **Suivant** avec tous ces paramètres que nous avons pu faire jusque-là à savoir définir le serveur cible pour les licences CAL, sélectionner les utilisateurs qui auront accès au serveur et ces services.

1. Test des services RDS déployés

Il faut noter que les programmes publiés en RemoteApp permettent de lancer des programmes depuis le(s) serveur(s) hôte(s) de session bureau à distance en donnant l'impression à l'utilisateur que celui-ci est exécuté depuis son poste de travail mais seule la fenêtre du programme est affichée.

Depuis un poste client nous pouvons **lancer un navigateur** mais de préférence **internet explorer** et spécifier l'URL de connexion **https://fqdn/rdweb** de l'accès web. Le FQDN (Full Qualified Domain Name) est le nom complet de la machine serveur composé du nom du serveur plus le domaine dont il est joint, indiquer les informations d'identification d'un utilisateur autorisé à accéder au serveur pour se connecter.

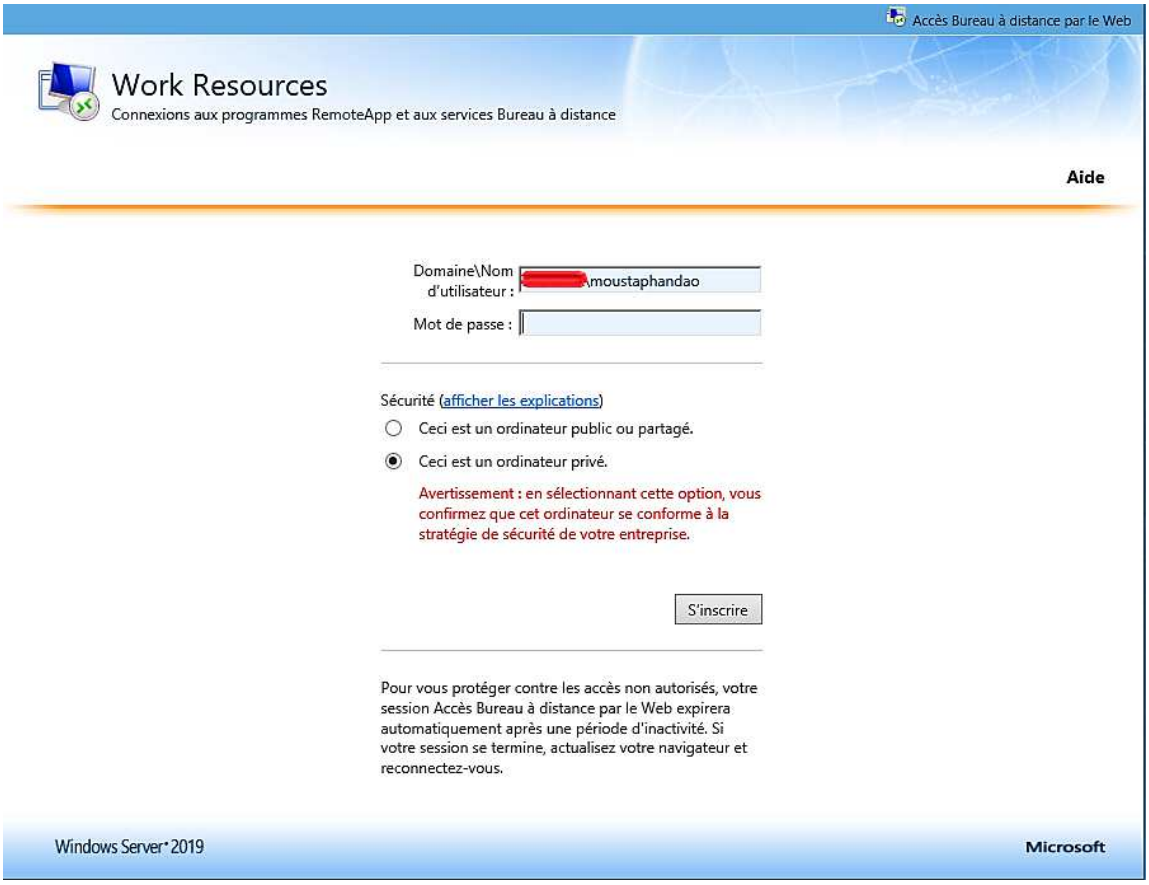


Figure 4.2-11 Connexion aux RemoteApp

Si les informations d'indentifications fournies durant la phase d'authentification sont correctes l'utilisateur pourra alors accéder aux programmes publiés dans RemoteApp. Ainsi l'utilisateur bénéficiera d'un accès total aux ressources publiés



Figure 4.2-12 Ressources publiées

À part l'accès bureau à distance par le web on peut utiliser le client Remote Desktop Connexion RDC pour se connecter au serveur. Indiquer le nom ou l'adresse IP de la ferme RDS.

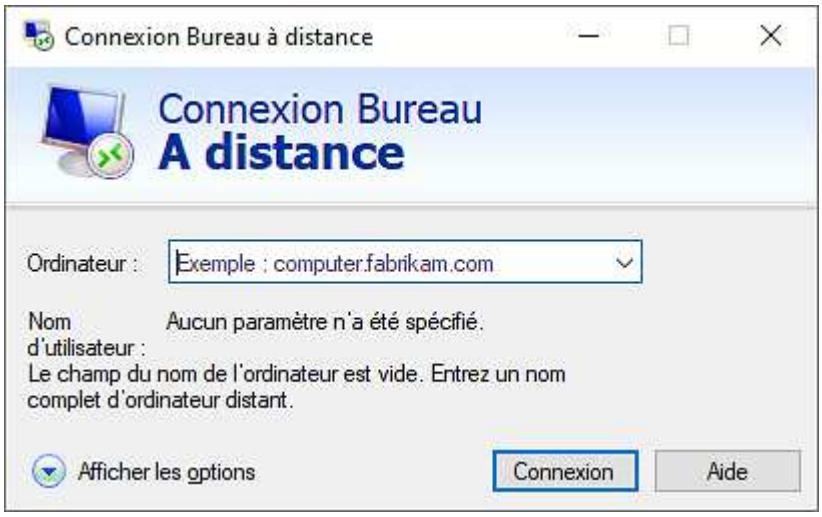


Figure 4.2-13 Client RDC

Sur la fenêtre d'identification donner le nom d'utilisateur et le mot de passe d'un utilisateur ayant les privilèges requis pour se connecter à une session de bureau à distance. Ensuite valider la demande indiquant l'identité de la machine distante n'est pas reconnue. Le certificat de sécurité est géré par le service de gestionnaire de licence dont nous avons une version d'évaluation d'une période de 180 jours.

Après toutes ces vérifications nous pouvons accéder désormais à l'ordinateur distant comme indiquer en haut de la fenêtre nous avons **l'adresse IP / connexion bureau à distance**.

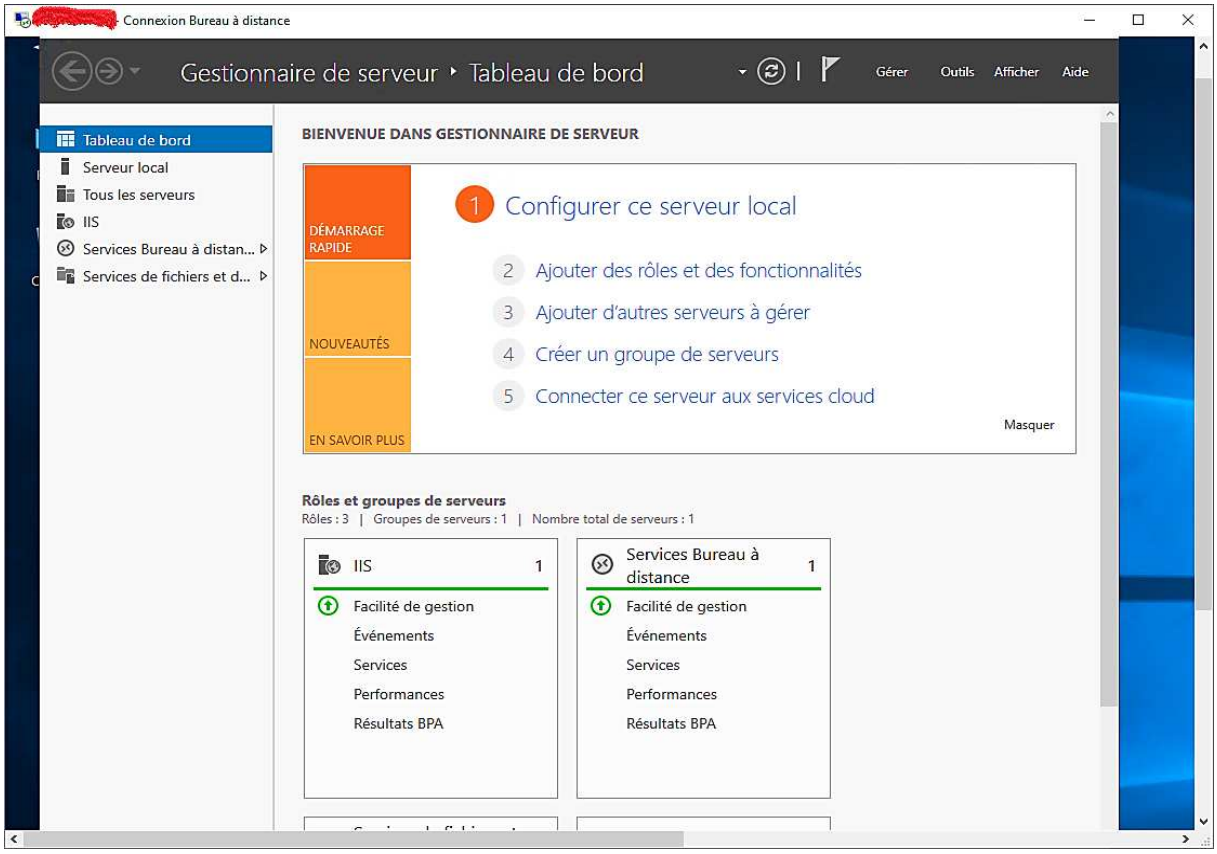


Figure 4.2-14 Bureau à distance

4.2.3 Configuration de connexions simultanées

Les connexions simultanées permettent à plusieurs utilisateurs d'une même machine de se connecter en même temps sans interruption de l'une des sessions ouvertes sur l'ordinateur.

Sur les serveurs

Par défaut les Windows serveurs n'autorisent qu'une seule session bureau à distance. Pour activer plusieurs sessions simultanées il faudra modifier quelques paramètres du système et éventuellement avoir à sa disposition les licences CAL RDS.

Pour activer plusieurs sessions bureau à distance :

- Appuyer sur la touche Windows puis taper **gpedit.msc,**
- Accéder à **Configuration ordinateur>Modèles d'administration>Composants Windows>Services Bureau à distance>Hôte de session Bureau à distance>Connexions ;**

- Définir **limiter l'utilisateur des services Bureau à distance à une seule session des services Bureau à distance sur Désactivé** ou **Disabled ;**

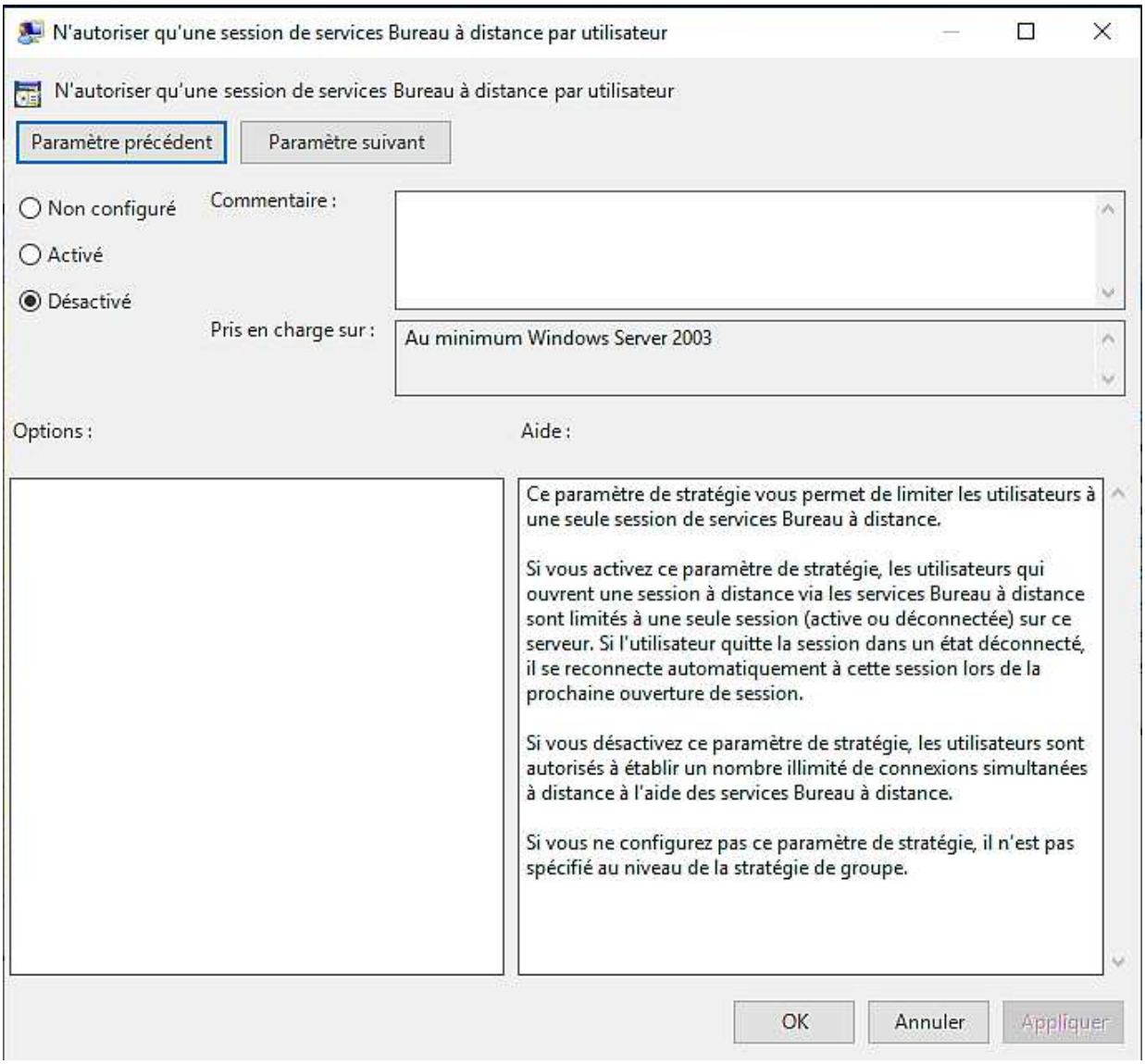


Figure 4.2-15 Configuration multisessions

Définir **Limiter le nombre de connexions à sa valeur maximale 999999** de connexions autorisées cela permettra d'autoriser ou de limiter le nombre de sessions des services bureau à distance qui peuvent être activées sur le serveur.

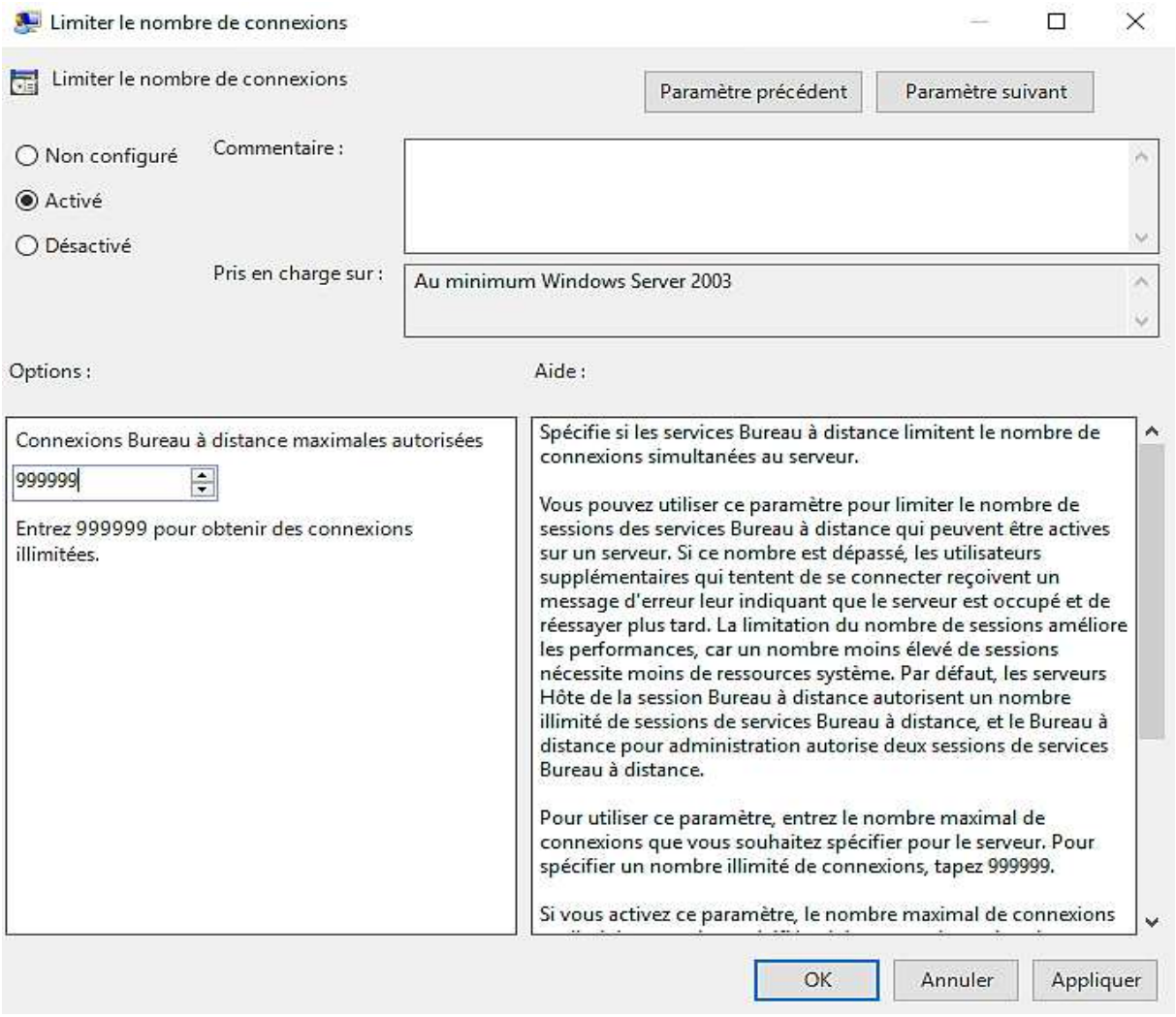


Figure 4.2-16 Nombre de sessions

Sur les postes

L'option multisession ne peut pas être exécutée sur les postes de travail. Mais Microsoft a apporté une solution, l'image ISO de Microsoft Windows 7/10 Entreprise multisessions, qui permet d'ouvrir des sessions simultanées et interactives, le nombre de sessions dépend des ressources matérielles du système et de la manière dont les utilisateurs utilisent les applications et aussi de la charge de travail [12]. Il faut noter que cette solution ne peut pas être déployée dans un environnement de production local car elle optimisée pour le service de machine virtuelle de Windows pour Azure.

4.2.4 Hybridation de la messagerie

Microsoft Exchange Server est un logiciel de travail pour serveur de messagerie électronique créé par Microsoft. Il est aussi pour la gestion d'agenda, de contacts et de tâches, qui assure le stockage des informations et permet des accès à partir de clients

mobiles (Outlook Mobile Access, Exchange Active Sync) et de clients web (navigateurs tels que Microsoft Edge, Internet Explorer 11, Mozilla Firefox, Safari, Google Chrome) [15] .

Avec la dernière version de Microsoft Exchange Server 2019, beaucoup de nouveautés ont été apportés afin d'améliorer l'utilisation et la sécurité des données qui y transitent.

1. **Sécurité**

- Windows Server Core permet de réduire la surface d'attaque des personnes malveillantes.
- Suivi et prévention de la perte de données de migration
- Bloquer l'accès externe au centre d'administration Exchange et à Exchange Management Shell
- La prise en charge automatique du chiffrement TLS 1.2

2. **Performance**

- Infrastructure de recherche amélioré
- Basculements plus rapides et plus fiables entre les serveurs
- Prise en charge jusqu'à 256 Go de mémoire et 48 cœurs de processeur.

3. **Clients**

- Une gestion plus sécurisé des droits relatifs à l'information avec l'option Calendrier Ne pas transférer.
- Acheminement en mode natif des adresses e-mails contenant des caractères non anglais
- Prise en charge d'annulation de réunion créée auparavant par un utilisateur qui a quitté l'organisation.

4.2.4.1 Architecture Logique Exchange Serveur

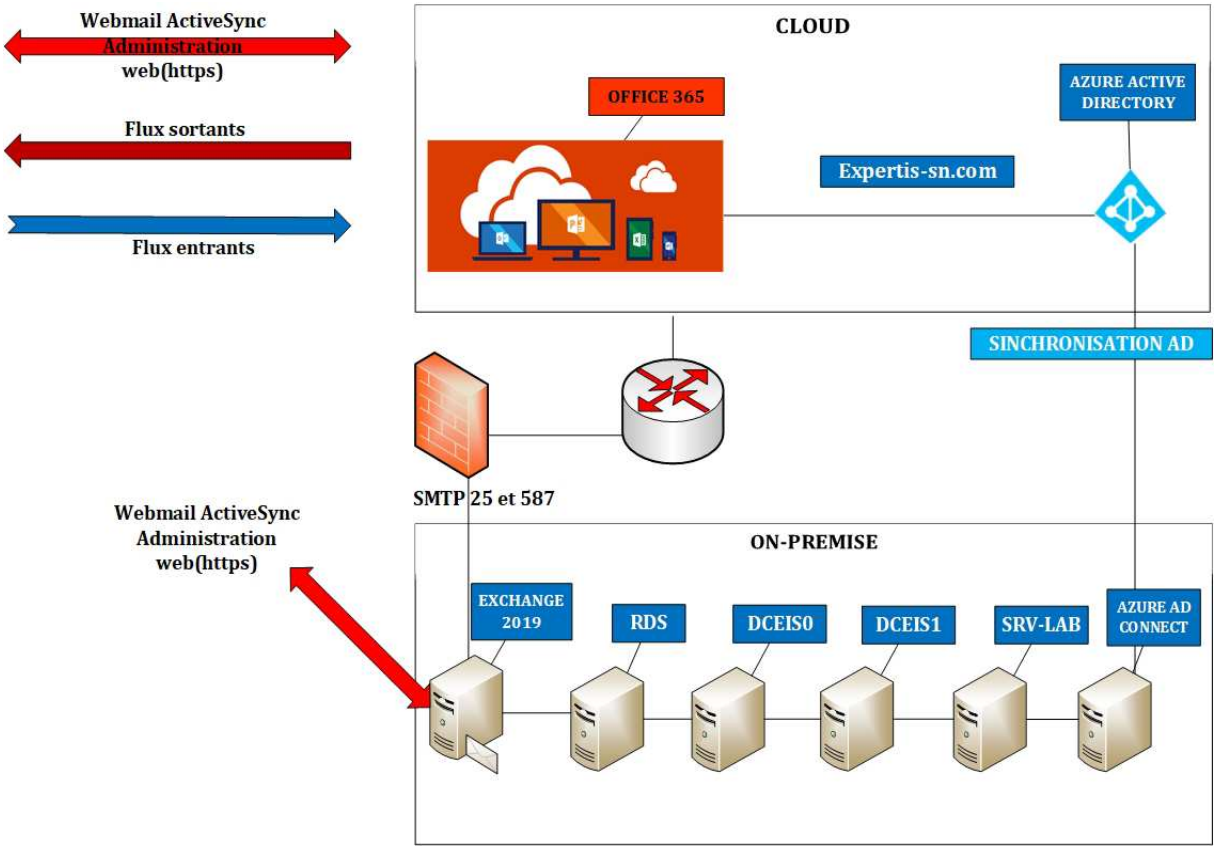


Figure 4.2-17 Flux Messagerie

1. Rôles d'Exchange serveur 2019

Avec Microsoft Exchange 2013, il y avait trois rôles qui sont :

- Le rôle accès client
- Le rôle serveur de boîtes aux lettres
- Le transport Edge qui gère le flux de messagerie, assure la protection contre les spam et les règles de transport de Edge.

Mais avec Exchange 2019, le nombre de rôles de serveur est réduit à deux : les rôles de serveur de boîte aux lettres et le transport Edge. La messagerie unifiée a été retiré de l'Exchange 2019 [16].

- Les services d'accès client fournissent des services d'authentification, de redirection limitée et de proxy. Les services d'accès client ne font pas de rendu de données et offrent tous les protocoles d'accès client habituels : HTTP, POP et IMAP, et SMTP.

- <Les services de boîte aux lettres comprennent tous les composants de serveur traditionnels que l'on trouve dans le rôle de serveur de boîte aux lettres d'Exchange 2013, à l'exception de la messagerie unifiée : les protocoles d'accès client en arrière-plan, le service de transport et les bases de données de boîte aux lettres. Le serveur de boîtes aux lettres gère toutes les activités des boîtes aux lettres actives sur ce serveur.

Exchange 2019 permet aussi :

- D'enregistrer des fichiers dans OneDrive Entreprise
- De partager et lier des documents stockés dans OneDrive Entreprise ou dans un site SharePoint.
- Téléchargement de fichier depuis OneDrive Entreprise
- Lister les éléments récemment utilisés remplies de fichiers locaux et en ligne.

Un autre avantage est que le nombre de boîtes aux lettres qu'on peut rechercher à la fois passe de 5000 à 10 000 pour les boîtes aux lettres et les boîtes aux lettres d'archivage.

2. Rôle Mailbox

Le rôle Mailbox regroupe les mêmes fonctionnalités compare au rôle Mailbox sur Exchange 2013 mais comporte en plus des fonctionnalités de Transport et de Messagerie unifiée. Il est semblable à un **Back End** qui assure le traitement.

a. Messagerie Unifiée

La messagerie Unifié est maintenant un composant du rôle Mailbox. La Messagerie Unifiée apporte à l'entreprise la centralisation et l'accessibilité des informations depuis partout dans le monde. Les avantages d'une telle solution sont les suivants :

- **Réponse aux appels :** les appelants peuvent laisser leurs messages vocaux directement sur la boîte aux lettres de l'utilisateur.
- **Réception des télécopies :** le serveur peut recevoir des télécopies et les transmettre directement dans les boîtes aux lettres des utilisateurs.
- **Accès des abonnés :** les utilisateurs peuvent accéder aux informations de leurs boîtes aux lettres à l'aide d'Outlook Voice Access. Ils peuvent, entre autres, accéder

à leurs messages vocaux, écouter des informations de leur calendrier ou encore accepter ou annuler une demande de réunion.

Une fois l'utilisateur activé pour la messagerie unifiée, vous pouvez gérer, modifier et configurer les propriétés de la messagerie unifiée pour cet utilisateur.

b. Managed Store

La Managed Store est le nom des processus de la magasin d'informations dans Exchange 2016 et Exchange 2019. Il utilise un modèle de processus de contrôleur/de travail qui permet d'isoler les processus de stockage et d'accélérer le passage à la base de données. La Managed Store utilise également un mécanisme de mise en cache de base de données statique qui remplace l'algorithme de tampon dynamique dans les versions précédentes d'Exchange [17].

Le modèle à processus multiples utilisé par la Managed Store se compose des processus :

- Processus de contrôle de service de magasin unique pour l'ensemble du serveur.

Microsoft.Exchange.Store.Service.exe, également appelé MSExchangeIS

- Processus de travail d'âne pour chaque base de données.

Microsoft.Exchange.Store.Worker.exe

3. Rôle de transport

Le rôle EDGE 2016 est similaire au rôle EDGE que nous avions avec les versions précédentes d'exchange il assure les fonctions de transport SMTP.

Cette architecture ci-dessus symbolise le trafic des flux de messagerie entre les mails venant de l'extérieur et le site on-premise et l'office 365. Les utilisateurs peuvent aussi depuis leur navigateur web consulté leurs E-mails avec le Webmail qui est une interface web permettant l'émission et la réception de courriers électroniques.

4.2.4.2 Déploiement Microsoft Exchange Server

Tableau 4.2-2 Conditions matérielles et logicielles

Prérequis matériels

Processeur	Processeurs Intel 64-bits (Intel EM64T) Processeurs AMD qui supporte la plateforme AMD64 **NB :** les processeurs Intel Itanium IA64 ne sont pas pris en charge.
Mémoire de travail	Boîte aux lettres : 128 Go minimum recommandé par Microsoft Transport Edge : 64 Go minimum recommandé par Microsoft
Espace disque	30 Go pour l'installation 200 Mo libre pour sur le disque système 500 Mo libre avec le messages queue Database
Résolution de l'écran	1024 x 728 pixels ou plus
Types de fichiers	NTFS sur les partitions qui contiennent : ➢ Partition système ➢ Binaires d'Exchange ReFS sur les partitions qui contiennent : ➢ La base de données Mail box ➢ Logs des transactions
Prérequis logiciels	
Domaine active Directory	➢ Windows serveur 2019 Standard ou Datacenter ➢ Windows serveur 2016 Standard ou Datacenter ➢ Windows serveur 2012 R2 Standard ou Datacenter
Niveau de la forêt de l'AD	Minimum Windows serveur 2012 R2
Serveur DNS	Pouvant résoudre les enregistrement MX, A, CNAME. Routage des mails à l'extérieur, résolution des noms et services (MX)

Concernant l'installation nous allons procéder avec la méthode **recovery** afin de récupérer les informations de configurations qui étaient présentes dans le serveur de messagerie antérieure.

Pour cela certains prérequis sont aussi nécessaires pour le bon fonctionnement de la messagerie exchange :

- NET Framework 4.8

- Visual C++ Redistributable Package for Visual Studio 2012 [18]
- Visual C++ Redistributable Package for Visual Studio 2013 [18]
- Unified Communications Managed API 4.0 [18]

4.2.4.3 Procédure d'installation

1. La préparation du contrôleur de domaine nécessitant l'outil AD-RSAT-ADDS qu'il faut exécuter sur le serveur devant accueillir le serveur exchange avec la commande :

Install-WindowsFeature RSAT-ADDS

2. Installation des composants Windows :

Les deux rôles obligatoires dans Microsoft Exchange serveur 2019 sont le rôle de boites aux lettres et le rôle de transport EDGE.

Rôle Mailbox sur Windows 2019

Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS

Rôle EDGE sur Windows 2019

Install-WindowsFeature ADLDS

Ces lignes de commande sont à exécuter sur PowerShell avec les niveaux de privilèges requis.

Cette récupération n'est possible que si le nouveau serveur ait le même nom, les mêmes temps de performances et la même configuration matérielle que le serveur perdu pour pouvoir retrouver certaines informations et paramètres enregistrés dans le contrôleur de domaine.

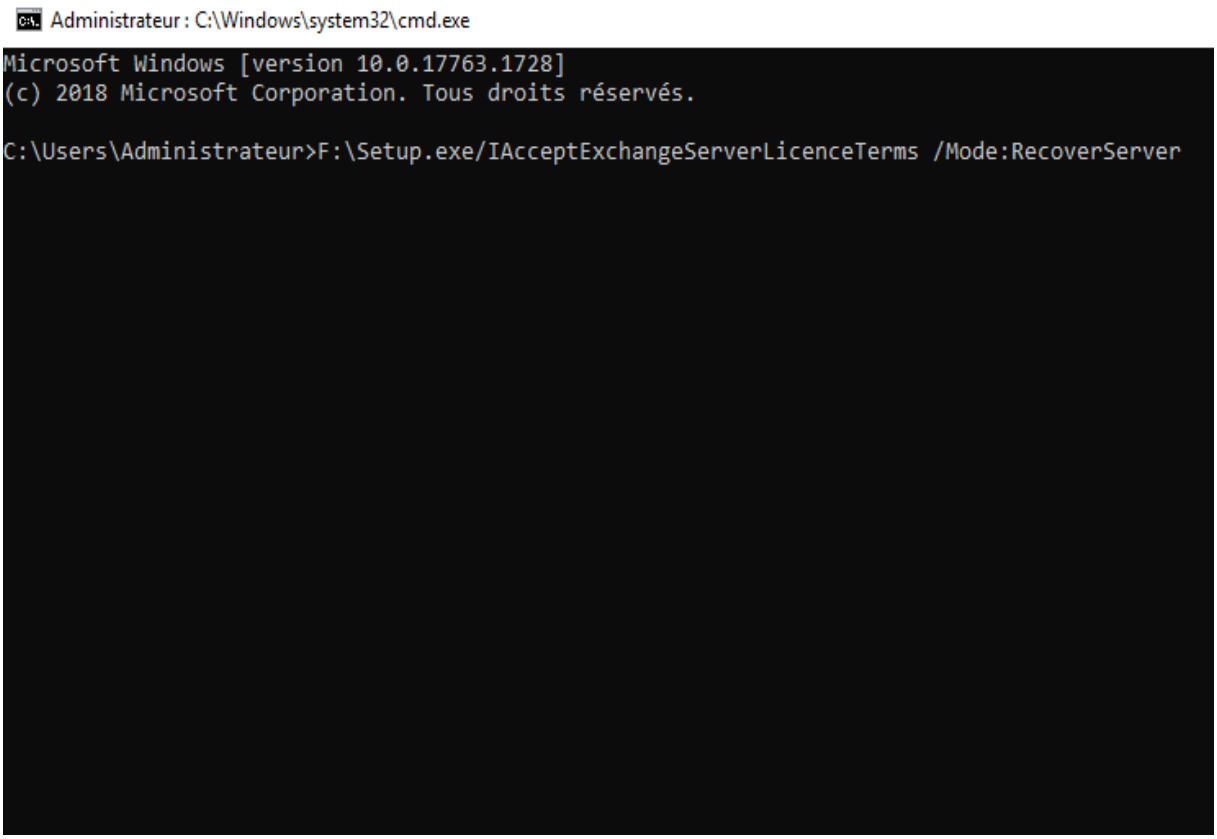


Figure 4.2-18 Mode Installation

Comme décrit précédemment nous allons procéder une récupération du serveur exchange perdu en mode sans assistance dont les commandes figurent sur l'image ci-dessus. Pour parvenir à récupérer un serveur de messagerie exchange, il faut obligatoirement que le nouveau serveur ait le même nom que le serveur à récupérer, d'être membre du même domaine et qu'ils présentent les mêmes caractéristiques en terme de ressources matérielles. Avant de lance le mode **RecoverServe**r, nous avons réinitialisé l'objet de l'ancien serveur présent dans l'active directory. Concernant ce mode d'installation il faut spécifier la lettre du lecteur qui contient le setup d'Exchange, accepter les contrats de licences et définir avec **RecoverServer** une récupération du serveur perdu.

4.2.4.4 Configuration Post-récupération

Après une installation en mode recovery du serveur exchange, nous allons passer maintenant à une vérification que tous les services exchanges sont installés et fonctionnels.

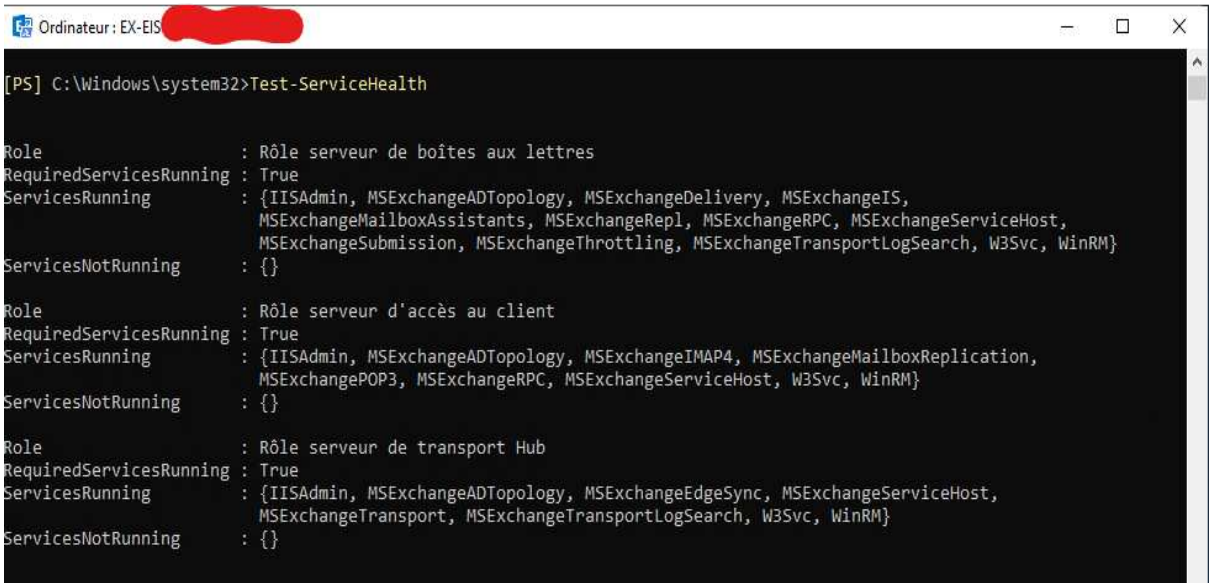


Figure 4.2-19 Services Exchange

Ainsi d'après l'image ci-dessus on peut constater sont bien installés et fonctionnels :

- Serveur de boîtes aux lettres
- Serveur d'accès au client
- Serveur de transport Hub

4.2.4.4.1 Configuration service Web

Bon nombre de fonctionnalités Exchange sont des services web notamment l'accès Webmail, l'Exchange Administration Console, l'Outlookanywhere, l'Autodiscover, les Informations de disponibilités etc. L'accès aux web services se fait à travers le protocole HTTPS et nécessite par conséquent un certificat. Lors de l'installation d'Exchange des certificats Auto signés sont installés sur les serveurs ce qui permet le fonctionnement des services web dès l'installation mais génère des warnings lors de certains accès. Les accès à travers un nom DNS publique nécessite de disposer un certificat fourni par une autorité de certification publique. Pour les accès interne un certificat fourni par une autorité de certification interne peut suffire, mais nécessite un certificat qui inclus les noms internes.

1. **Certificat**

Pour mettre en place le certificat sur le serveur Exchange il faut au préalable avoir installé l'autorité de certification sur le contrôleur de domaine Active Directory.

2. **Url Web Services**

Pour la configuration des services web voir annexe.

4.2.4.4.2 Les accès clients

Depuis la version Microsoft Exchange 2016 les accès clients fournis sont les suivants :

- Outlook Anywhere
- Outlook Web Access
- Exchange active Sync
- POP3 (Post Office Protocol Version 3)
- IMAP4 (Internet Message Access Protocol version 4)

Il faut aussi préciser que Exchange ne prenne plus en charge la possibilité d'établir une connexion MAPI pure, seule la connexion Outlook Anywhere est possible entre le client Outlook et le serveur exchange.

1. **Outlook Anywhere**

L'Outlook Anywhere est le protocole de connexion par défaut du client Outlook avec Exchange 2016. L'Outlook Anywhere est une encapsulation du protocole MAPI à travers le protocole de transport http. L'OA permet également au client Outlook de se connecter en dehors du réseau local. L'Outlook Anywhere correspond à deux types de connexions le RPC/Http et le MAPI/Http.

RPC/Http : Le RPC/Http est une encapsulation du protocole MAPI via le protocole de transport RPC avec une connexion http. Le MAPI est doublement encapsulé par le RPC et le http.

MAPI/http : Le MAPI over Http est une encapsulation du protocole MAPI via le protocole de transport http. Une véritable connexion web http est établie entre le client et le serveur Exchange. Un des avantages du MAPI/http est que lors d'une perte de sa connexion du poste du fait de sa déconnexion du réseau, la session n'est réinitialisée qu'après une déconnexion de plus de 15mn et le client peut simplement se reconnecter à sa session précédente. Ce qui est assez intéressant pour des connexions de faible qualité. Le MAPI/http est activé par défaut sur Exchange 2016.

2. **Outlook Web Access**

Le client OWA permet l'accès à l'interface web de la boîte de messagerie. L'accès peut se faire par l'URL **: https://<nom du serveur>/OWA.**

La console d'administration ou EAC Exchange administration Console permet d'accéder à l'interface graphique de management du serveur.

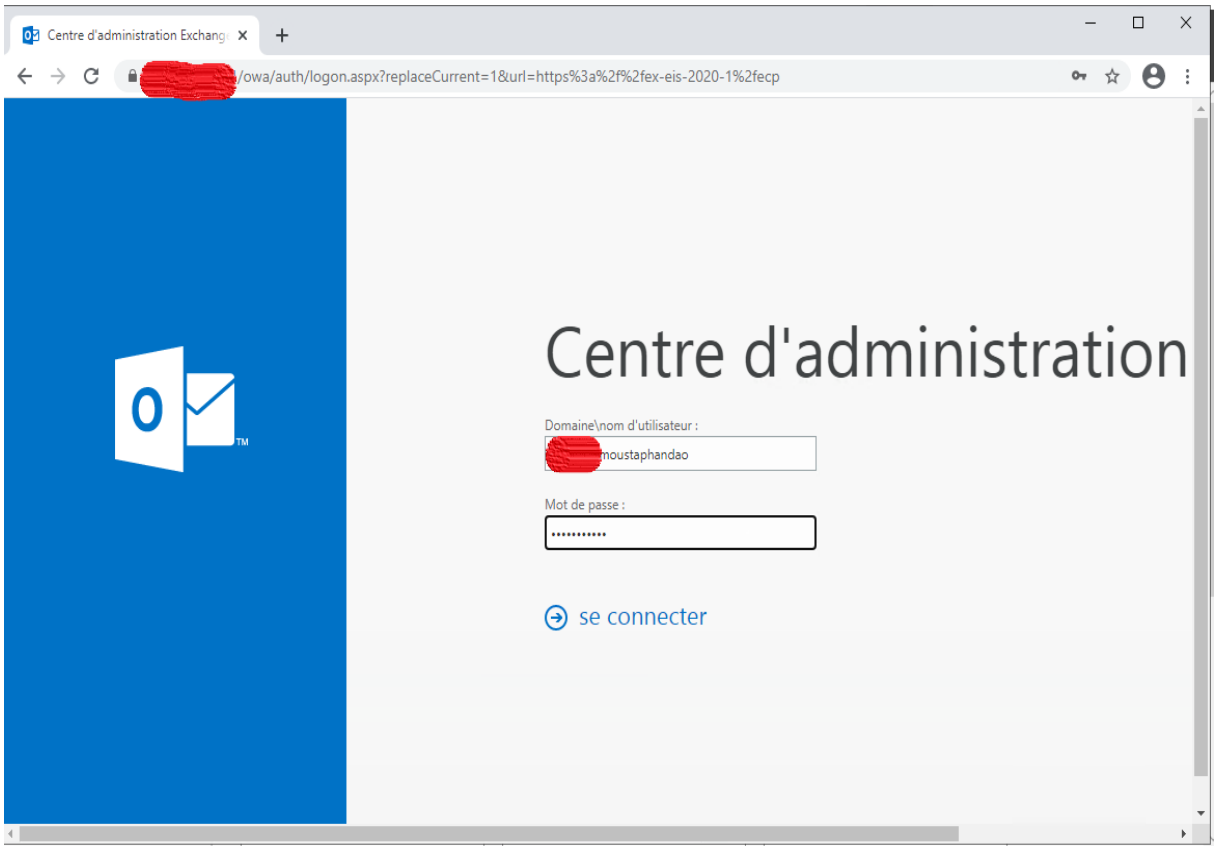


Figure 4.2-20 Interface EAC

3. Exchange active Sync

EAS (Exchange ActiveSync) permet l'accès à sa messagerie via un mobile tel qu'un smartphone. Des solutions tierces se basent aussi sur ActiveSync comme la version 10 de BlackBerry.

4. POP3

Le protocole POP3 permet de synchroniser ses mails avec un client POP (exemple Outlook Express).

5. IMAP4

IMAP (Interactive Mail Access Protocol) est un autre protocole permettant de consulter les mails sur un serveur en les synchronisant sans les retirer de la boîte aux lettres du serveur.

4.2.4.4.3 Administration des destinataires

Depuis exchange 2016, la gestion des destinataires se fait à partir de l'interface EAC et grâce aussi à la console PowerShell de Exchange.

1. Les destinataires

Les destinataires sont composés entre autres, des utilisateurs avec ou sans boîte aux lettres, les groupes et les contacts.

Tableau 4.2-3 Types de destinataires

Destinataires	Types
Boîte aux lettres	Utilisateur Salle Équipement Liée Partagée Public Folder
Groupe de distribution	Groupe de distribution Groupe de distribution dynamique
Contact	Contact Messagerie – utilisateur messagerie

a. Les types de boîtes aux lettres

Les boîtes aux lettres sont destinées pour différentes tâches. Les boîtes aux lettres que nous retrouvons sur Exchange sont :

- **User Mailbox (Boîte aux lettres utilisateur)** : ce type de destinataire correspond à la mailbox classique d'un utilisateur. L'utilisation des boîtes aux lettres permet d'envoyer ou de recevoir des mails, la boîte aux lettres est stockée dans la base de

donnée du serveur mailbox. Il faut noter aussi qu'un utilisateur en peut avoir qu'une seule user mailbox et une user mailbox ne peut être liée qu'à un seul et unique utilisateur mais un utilisateur peut en outre avoir une boîte aux lettres d'archives.

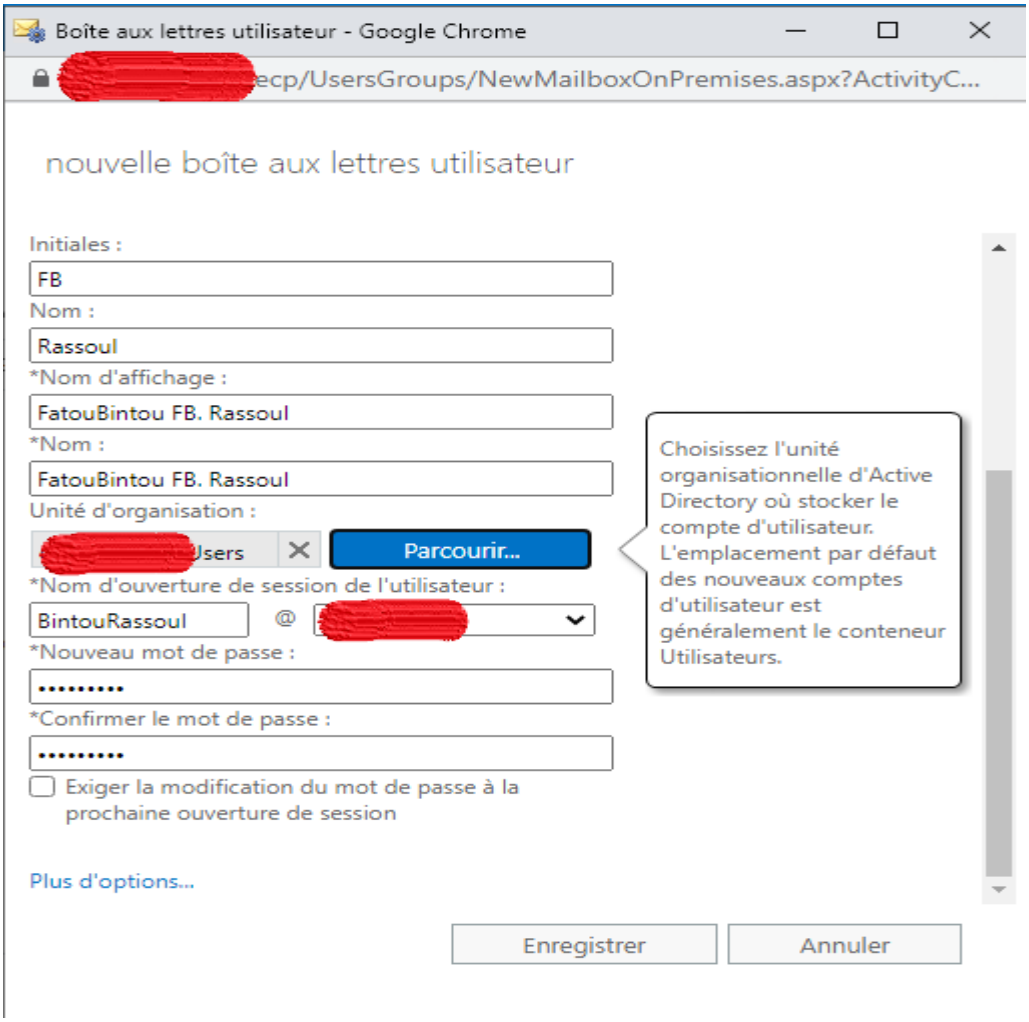


Figure 4.2-21 User Mailbox

Lors de la création d'un user mailbox pour utilisateur, il est possible de le faire pour un utilisateur existant ou de créer un nouvel utilisateur, procédure que nous avions utilisée pour créer l'utilisateur ci-dessus.

- **Room Mailbox (Boîte aux lettres de salle)** : permet de planifier des réunions ou des formations tout en réservant des salles. La création d'une boîte aux lettres de salle entraine la création d'un compte utilisateur désactivé.

- **Equipement Mailbox (Boîte aux lettres d'équipement)** : permet de réserver par exemple une vidéo projecteur, une voiture, etc. La création d'une boîte aux lettres d'équipement entraine la création d'un compte utilisateur désactivé.
- **Boîtes aux lettres liées** : Les boîtes aux lettres liées permettent à un compte d'une forêt approuvée de bénéficier de la messagerie. Ce type de boîtes fonctionne exactement comme une boîte aux lettres utilisateur standard. Ces boîtes aux lettres sont utilisées pour des structures complexes telles que des architectures multi forêts. IL faut pour cela établir des relations d'approbations inter forêts et autoriser les comptes d'une forêt à accéder à leur compte de messagerie sur l'autre forêt.
- **Shared Mailbox (Boîte aux lettres partagées)** : Les boites à lettres partagées sont utilisées par plusieurs utilisateurs. Lors de la création un compte AD désactivé va être créé. Après création il faut accorder les droits aux utilisateurs ou groupes concernés, il faut accorder en fonction du besoin les droits Full et ou Send As.

b. Les groupes de distribution

Les groupes sont des comptes de messagerie utilisés pour envoyer simultanément à plusieurs utilisateurs avec extension de messagerie. Les groupes de distributions sont créés sur l'active directory à partir d'exchange ou de la console utilisateurs et ordinateurs actives directory. Il y a deux étendues de groupes :

- Groupe universel de distribution à extension de messagerie destiné à l'envoie en masse qui ne peut se voir affecter d'autorisations pour des ressources.
- Groupe universel de sécurité à messagerie activée destiné à l'envoie en masse qui peut se voir affecter des autorisations pour des ressources.

Il est possible de créer deux types de groupe que sont :

- Groupe standard avec ajout suppression manuelle des utilisateurs
- Groupe dynamique avec une gestion automatique des appartenances au groupe.



Figure 4.2-22 création groupe dynamique

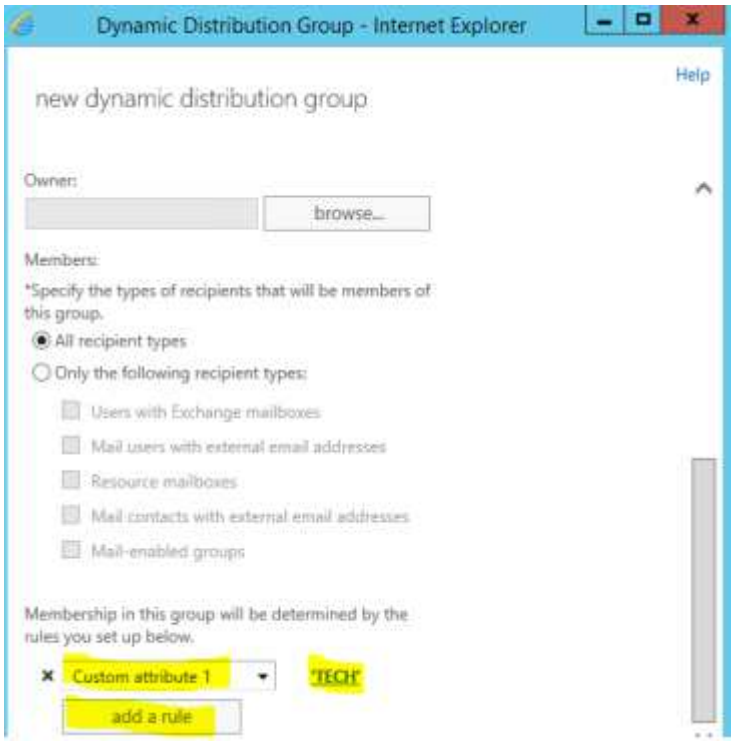


Figure 4.2-23 Groupe dynamique

c. Les contacts de messagerie

Les contacts de messagerie sont très utilisés par les entreprises pour leurs partenaires ou sous-traitants réguliers qui utilisent leurs propres serveurs de messagerie. En effet, nombre d'entreprises ont besoin que leurs clients envoient des messages à leurs partenaires ou sous-traitants, tout en faisant en sorte que cela soit transparent pour le client expéditeur. Ainsi, le client recevra un mail du partenaire et pensera qu'il s'agit d'une personne chez son fournisseur. Pour cela, vous allez créer un contact avec une adresse de messagerie externe, et tous les mails destinés à l'adresse du partenaire ou du sous-traitant

seront routés vers sa boîte aux lettres externe. Cela peut être aussi un moyen d'assurer une cohérence de tous les contacts de l'entreprise plutôt que de passer par les contacts Outlook via les dossiers publics.

Deux types de contacts sont présents sur exchange :



Figure 4.2-24 Types de contacts

- Les contacts de messagerie servent uniquement à créer des contacts avec une adresse de messagerie mais n'ont aucun accès à votre organisation puisqu'ils ne possèdent pas de compte d'utilisateur.
- Les utilisateurs de messagerie, ils fonctionnent comme les utilisateurs standards : ils peuvent se connecter sur un domaine mais n'ont pas de boîte aux lettres.

Les contacts de messagerie sont utilisés pour des prestataires externes ou pour des contacts d'entreprises alors que les utilisateurs de messagerie sont utilisés par des sous-traitants ayant besoin d'un accès aux ressources de l'entreprise pour laquelle ils travaillent.

2. La gestion des boîtes aux lettres

a. Le déplacement des Mailbox

IL est possible de déplacer les Mailbox d'une base de données vers une autre. Le cas le plus usuel est lors des migrations Exchange après installation du nouveau serveur Exchange on migre les boites en faisant des déplacements de boite (Move Mailbox). Lorsque vous déplacez une boîte aux lettres, vous la déplacez depuis une base de données de boîtes aux lettres source vers une base de données de boîtes aux lettres cible. La base de données de boîtes aux lettres cible peut se trouver sur le même serveur, sur un serveur différent, dans un domaine différent, sur un site Active Directory différent et même vers une organisation exchange différente.

b. La récupération des Mailbox supprimées

Une mailbox utilisateur est composé d'un compte AD et d'une mailbox contenant les données et stockée dans la base de données Exchange.

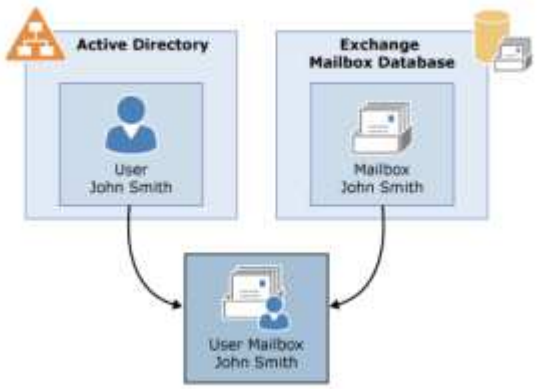


Figure 4.2-25 User Mailbox

La suppression d'une boîte aux lettres utilisateur peut être une désactivation, dans ce cas, juste la mailbox utilisateur est supprimée et le compte AD est conservé, la boîte aux lettres est conservée pendant le temps de conservation défini au niveau de la base de données ; s'il s'agit d'une suppression de la boîte aux lettres utilisateur et le compte AD sont supprimés et la mailbox est conservée pendant le temps de conservation défini au niveau de la base de données.

La récupération de la boîte aux lettres permet de restaurer une boîte aux lettres supprimée malencontreusement sans avoir à utiliser une restauration via une sauvegarde.

Ce délai est de 30 jours par défaut et vous pouvez le changer selon les stratégies de l'entreprise. Par contre, le fait de conserver des boites aux lettres supprimées implique que vous devez, dans certains cas, prévoir un espace disque suffisant pour conservant toutes ces boites aux lettres.

Enfin, ce paramètre est propre à chaque base de données de boîtes aux lettres. Cela signifie que si vous voulez paramétrer des stratégies différentes en fonction d'utilisateurs particuliers, vous êtes obligés de créer plusieurs bases de données de boîtes aux lettres.

Le processus de gestion des boîtes aux lettres permet de nettoyer les bases de données en supprimant les boîtes aux lettres supprimées dont le délai de rétention a été atteint. Ce processus se gère à partir des propriétés de la base de données des boîtes aux lettres dans la planification de la maintenance. Une fois le délai atteint et dépassé, vous ne pouvez plus récupérer la boîte aux lettres simplement mais vous êtes contraint de passer par une restauration classique.

c. L'activation des archives pour les Mailbox

Exchange 2013 permet de définir une boite d'archive en plus de sa boite classique. La boite d'archive permet à l'utilisateur de conserver un bon nombre de mails sans dépasser son quota de boite et sans faire recours à de l'archivage locale sous forme de fichier PST. Les archives Exchange répondent à l'ensemble de ces questions en :

- Centralisant les archives sur un seul point d'accès.
- Rendant accessible l'archive depuis n'importe où.
- Proposant une stratégie de rétention de l'archive associée à la boîte.

Enfin, vous pouvez, comme sur la boîte aux lettres principale, activer un quota sur la boîte d'archive.

4.2.5 Configuration Office 365

Microsoft Office 365 est un service de type SaaS (Software as a Service) qui offre un ensemble complet d'outils logiciels et de services à partir d'un serveur Cloud de Microsoft. Office 365 est proposé sous forme d'abonnement (annuel et mensuel). Selon l'offre d'abonnement choisie, les utilisateurs disposeront d'une messagerie en ligne, d'un agenda, d'un espace de stockage et de partage, des applications Office Online (Excel, Word, PowerPoint et OneNote...). Certaines offres incluent la suite bureautique Office 2016 à installer sur un ou plusieurs supports (PC, Mac, tablette, smartphone...).

De plus, Microsoft a ajouté dans ces nouvelles offres d'Office 365, de nouvelles applications : **Sway**, une application de narration et **Delve**, un agrégateur de contenus permettant à l'utilisateur de retrouver plus facilement certaines informations (documents partagés, profils, e-mails, conversations, personnes...).

Office 365 est un espace de travail centralisé sur Internet vous permettant de travailler à plusieurs dans un environnement sécurisé et depuis n'importe quel endroit à partir d'une connexion Internet. Toutes les applications et services proposés par Office 365 ont été conçus pour fonctionner dans cet environnement collaboratif.

Il est essentiellement dédié aux TPE et PME. Son objectif est de mettre à votre disposition différents services afin d'optimiser votre organisation et celle de vos collaborateurs, qu'elle soit sédentaire ou mobile.



Figure 4.2-26 Office 365

Microsoft Office 365 peut être divisée en deux groupes [14]:

- Microsoft Office 365 Business pour les entreprises pas plus 300 employés
- Microsoft Office 365 Enterprise pour les entreprises de plus de 300 employés

4.2.5.1 Microsoft Office 365 Business

Pour l'offre Microsoft Office 365 Business, il y plusieurs formules :

- Microsoft 365 Business Basic idéal pour les entreprises recherchant des solutions simples pour le travail à distance. Cette offre inclut Microsoft Teams (plateforme collaborative), Microsoft OneDrive (espace de stockage en ligne sécurisé) et Office pour le web (cette offre n'inclut pas les versions des produits installables sur ordinateur).
- Microsoft 365 Business Standard conçue pour les entreprises recherchant une gamme complète d'outils pour le télétravail et la collaboration. Elle inclut Microsoft Teams (plateforme collaborative), Microsoft OneDrive (espace de stockage en ligne sécurisé), Microsoft Outlook et Microsoft Exchange (des services

de messagerie professionnelle) ainsi que les logiciels Office Premium pour tous types d'appareils (smartphones, tablettes, etc.).

- Microsoft 365 Business Premium : cette offre est idéale pour les entreprises recherchant des solutions sécurisées pour le télétravail, avec tous les avantages de l'offre Business Standard, ainsi que des fonctionnalités avancées pour la gestion des appareils et la protection contre les cyber menaces.
- Microsoft 365 Apps conçue pour l'utilisation des logiciels Office sur différents appareils, et recherchant une solution de stockage de fichiers dans le cloud. Cette offre n'inclut pas ni la solution de messagerie professionnelle, ni Microsoft Teams.

4.2.5.2 Microsoft Office 365 Entreprise

Comme le Pack Business nous avons aussi différentes offres concernant le pack Microsoft Office 365 Enterprise :

- Microsoft 365 Apps for enterprise, version complète des logiciels et applications Office, avec stockage et partage de fichiers dans le cloud. Le service de courrier professionnel n'est pas inclus.
- Office 365 E1, services professionnels : courrier, stockage et partage de fichiers, Office pour le web, réunions et messagerie instantanée, etc. Les logiciels office ne sont pas inclus.
- Office 365 E3 permet aux entreprises de bénéficier de toutes les fonctionnalités incluses dans Microsoft Apps365 for enterprise et Office 365 E1, ainsi que de fonctionnalités de sécurité et de conformité.
- Office 365 E5, bénéficiez de toutes les fonctionnalités d'Office 365 E3, ainsi que de fonctionnalités avancées de sécurité, d'analyse et de gestion des communications vocales.

Les applications et services diffères selon l'offre choisie, Microsoft Office 365 vous donne accès à tous vos outils du quotidien sur une seule plateforme de travail :

1. **OneDrive Entreprise**

Une solution de partage, de stockage et de sauvegarde en ligne des données depuis n'importe quel appareil. Il permet aussi de coéditer des documents avec ces collaborateurs. OneDrive peut être utilisé de deux manières : à travers un navigateur web

ou à travers le logiciel OneDrive qui permet une synchronisation entre OneDrive et les supports informatiques compatibles.

OneDrive Entreprise, c'est...

Un espace de stockage personnel accessible 24h/24

Accéder à vos fichiers n'importe où, n'importe quand et depuis n'importe quel appareil (même hors connexion).

Une collaboration en temps réel

Partagez et coéditez des documents avec vos collaborateurs où qu'ils soient ou même des personnes extérieures à votre organisation.

Une solution fiable

Sécurité intégrée, conformité continue, confidentialité, sauvegarde des données, accessibilité... profitez d'une solution fiable et performante.

2. La suite Office

Microsoft Office est une suite bureautique fonctionnant avec les plateformes fixes et mobiles. Elle peut être installée sur ordinateur et fournit les logiciels tels que : Word, Excel, PowerPoint, OneNote, Outlook, Access et/ou Publisher selon les suites choisies.

3. SharePoint

C'est une plateforme collaborative favorisant le travail d'équipe grâce à des sites d'équipe dynamiques et productifs dédiés à chaque équipe de projet, service et division. Il renforce l'efficacité organisationnelle en permettant le partage des ressources et des applications communes sur des sites d'accueil et des portails.

Un espace de travail commun

Créez et personnalisez facilement un site d'équipe pour accéder à vos documents et données en ligne sans surcharger le service informatique ni investir en infrastructure.

Un espace de travail permettant de collaborer en temps réel

Stocker vos documents, partagez et coéditez-les avec vos collaborateurs ou des personnes extérieures à votre organisation où qu'ils soient. L'idéal pour favoriser le travail d'équipe et améliorer votre productivité.

Une plateforme sécurisée et accessible 24h/24

Partagez des informations avec des collaborateurs, des partenaires ou encore des clients de façon stable et en toute sécurité. Accédez aux informations dont vous avez besoin à toute heure, en tout lieu et depuis n'importe quel appareil.

4. Microsoft Teams

Microsoft Teams est une application de communication collaborative. Il s'intègre à la suite Microsoft Office 365 et Skype et propose des extensions pouvant intégrées à des produits autres que Microsoft.

Avec Teams, vous aussi discuter, participer à des réunions, émettre ou recevoir des appels. Permet de même la création d'équipe favorisant ainsi une équipe opérationnelle.

5. Skype Entreprise

Skype Entreprise est une solution de Microsoft qui est disponible de façon autonome ou dans le cadre de l'offre Office 365. Il y a des fonctionnalités supplémentaires dans Office 365 : enregistrement de réunion, applications Office (Word, Excel, Outlook...), réunion jusqu'à 250 participants, etc.

Tous vos contacts dans un seul outil conçu pour répondre à tous vos besoins

Téléphonie IP ou classique, messagerie instantanée, conférences vidéo, audio et web...

Un accès sur tous vos appareils

Communiquez facilement avec vos collaborateurs où que vous soyez à partir de n'importe quel appareil (PC/Mac, IPHONE, Android, iPad...)

L'intégration de vos services et applications Microsoft

Exchange Online, SharePoint Online, Word, Excel, PowerPoint...

Des communications sécurisées

6. Exchange Online

Exchange online est une offre de messagerie professionnelle. Accessible grâce aux abonnements Microsoft Office 365, il est le serveur de messagerie en ligne et Outlook le client de messagerie permettant de s'y connecter.

Elle offre des fonctionnalités de Microsoft Exchange Serveur comme service cloud. Il permet aux utilisateurs d'accéder aux e-mails, au calendrier, aux contacts et aux tâches à partir de PC, du Web et d'appareils mobiles. Il s'intègre entièrement à Active Directory, permettant aux administrateurs d'utiliser des stratégies de groupe, ainsi que d'autres outils d'administration, pour gérer les fonctionnalités d'Echange Online dans l'environnement local. Avec Echange Online, les entreprises n'ont pas la charge opérationnelle des logiciels de serveur sur leur site par contre, gère les services de messagerie qu'elles offrent aux utilisateurs. Les serveurs d'Echange Online sont hébergés dans les centres de données de Microsoft et sont accessibles aux utilisateurs depuis le réseau de l'entreprise ou sur internet.

Un moteur de recherche performant

Retrouvez rapidement vos emails, vos pièces jointes, vos rendez-vous ou encore vos contacts.

Une navigation aisée et intuitive

Gérez facilement et plus rapidement toutes vos communications avec cette solution.

Plus qu'une messagerie

Bénéficiez d'un antivirus et d'un anti-spam performant et de 50Go de stockage par utilisateur.

Gagnez ainsi en efficacité pendant vos déplacements en restant connecté à tout moment et aussi en efficacité avec une interface claire et unifiée de vos mails, calendriers, contacts, tâches et fichiers. Organisez-vous et travaillez où que vous soyez avec votre tablette ou smartphone (Android ou Apple).

4.2.5.3 Hybridation de la messagerie

Le composant Exchange Online d'Office 365 prend en charge les déploiements uniquement dans le cloud. Avant de configurer votre environnement Exchange sur site existant pour vous connecter à Office 365, prévoyez d'évaluer l'état actuel de votre organisation Exchange. En vous assurant que vous remplissez toutes les conditions préalables avant de passer aux étapes de coexistence ou de migration pour réduire le risque d'échec.

4.2.5.3.1 Concepts Exchange Online

Exchange Online fonctionne de la même manière que Exchange On-premise. Tout comme Exchange on-premise utilise un environnement Active Directory pour stocker les attributs et les propriétés des objects de configuration et des destinataires, Exchange Online stocke également ses informations de configuration dans Active Directory. Dans le cas d'Exchange Online, le composant Active Directory est Azure Active Directory, un service d'annuaire multi-locataires conçu pour s'adapter à des milliards d'objects.

L'administration d'Exchange Online peut se faire soit sur le centre d'administration Office 365 soit avec Windows PowerShell. Pour se connecter à Exchange Online par Windows PowerShell, vous aurez besoin d'importer les cmdlets d'Exchange Online dans votre session.

$Credential = Get-Credential

$ExchangeSession = New-PSSession –ConfigurationName Microsoft.Exchange –ConnectionUri https://outlook.office365.com/powershell-lived -Authentication Basic -AllowRedirection -Credential $ Credential

4.2.5.3.2 Méthodes de Migration et de coexistence

Lorsque vous planifier une coexistence ou une migration vers Exchange Online, vous devez tenir compte de vos objectifs à court et à long terme, en plus de votre AD Exchange, de la configuration de votre bureau et de la topologie de votre réseau. En fonction de l'entreprise et l'environnement, vous pourrez peut-être choisir une ou plusieurs de ces stratégies de coexistence migratoire :

1. **Cutover migration** : si votre environnement on-premise fonctionne avec Exchange 2003, 2007, 2010 ou Exchange 2013, et vous avez moins de 2000 mailbox, vous pouvez utiliser une migration de transition. En raison de la nature d'une migration de remplacement, vous devez migrer tout le monde en même temps. Bien que 2000 boîtes aux lettres soit le nombre maximum d'utilisateur pouvant être migrés avec cette méthode, il est plus réaliste de la limiter aux environnements comportant 150 mailbox ou moins.
2. **Staged migration :** si votre environnement sur site fonctionne avec Exchange 2003 ou 2007 et que vous disposez de plus de 150 boîtes aux lettres, vous pouvez

effectuer une migration par étapes. Les migrations échelonnées nécessitent l'utilisation d'Azure Active Directory Connect.

3. **Express migration :** si votre de travail fonctionne avec Exchange 2010, Exchange 2013 ou 2016, vous ne prévoyez pas d'utiliser de technologies de synchronisation d'annuaire pour faire migrer vos utilisateurs, et n'avez pas besoin de maintenir la possibilité de rechercher le statut libre ou occupé entre Office 365 et les utilisateurs sur site, vous pouvez utiliser la migration express.
4. **Hybrid migration :** si votre environnement on-premise fonctionne avec Exchange 2010, 2013 ou 2016, vous pouvez utiliser une migration hybride mais aussi dans les environnements Exchange 2003 ou 2007 si vous déployer un serveur Exchange 2010 ou Exchange 2013. Les migration hybrides soutiennent l'idée de migrations de boîtes aux lettres en ligne si les boîtes aux lettres sont hébergées sur des serveurs Exchange 2007 ou ultérieurs, ce qui signifie que la boîte aux lettres de l'utilisateur reste montée et en ligne jusqu'au moment de la coupure, puis le profil Outlook de l'utilisateur peut être redirigé vers Office 365. Si les boîtes aux lettres sont hébergées sur Exchange 2003, la mailbox est verrouillée et indisponible jusqu'à ce que la migration pour cette boîte aux lettres soit terminé. Les dossiers publics hébergés sur Exchange 2003 doivent être migrés vers Exchange 2007 avant que la coexistence ou la migration hybride puisse être effectuée.
5. **IMAP migration :** si votre environnement source exécute une version d'Exchange antérieure à 2003 ou un système de messagerie électronique étranger, vous pouvez utiliser une migration IMAP. Les migrations IMAP ne permettent généralement pas de migrer le calendrier et les contacts. La plupart des organisations qui doivent effectuer des migrations à partir de plateformes autres que Microsoft ou hébergées travaillent avec un partenaire spécialisé dans les migrations.

4.2.5.3.3 Prérequis hybridation de la messagerie

Pour déployer une infrastructure de messagerie hybride, il faudra respecter certains prérequis :

- Un serveur contrôleur de domaine : stocke les données d'annuaires et gère les communications entre les utilisateurs et les domaines, y compris les processus

d'ouverture de session d'utilisateur, l'authentification et les recherches dans l'annuaire local ;

- Un serveur Azure AD Connect : Azure AD Connect synchronise le nom UPN et le mot de passe de vos utilisateurs afin que ceux-ci puissent se connecter avec les mêmes informations d'identification que celles utilisées sur leur site ;
- Un serveur Exchange pour la messagerie interne au sein de l'organisation ;
- Un abonnement Office 365 pour l'utilisation et la configuration des services d'Office 365 ;
- **Compte d'administrateur local** : l'administrateur qui installe Azure AD Connect et qui a des autorisations d'administrateur local sur la machine ;
- **Compte d'administrateur d'entreprise AD DS**. Utilisé de façon facultative pour créer le « compte de connecteur AD DS »
- **Compte d'administrateur général Azure AD**. Utilisé pour créer le compte de connecteur Azure AD et configurer Azure AD.

Concernant la configuration matérielle nous avons

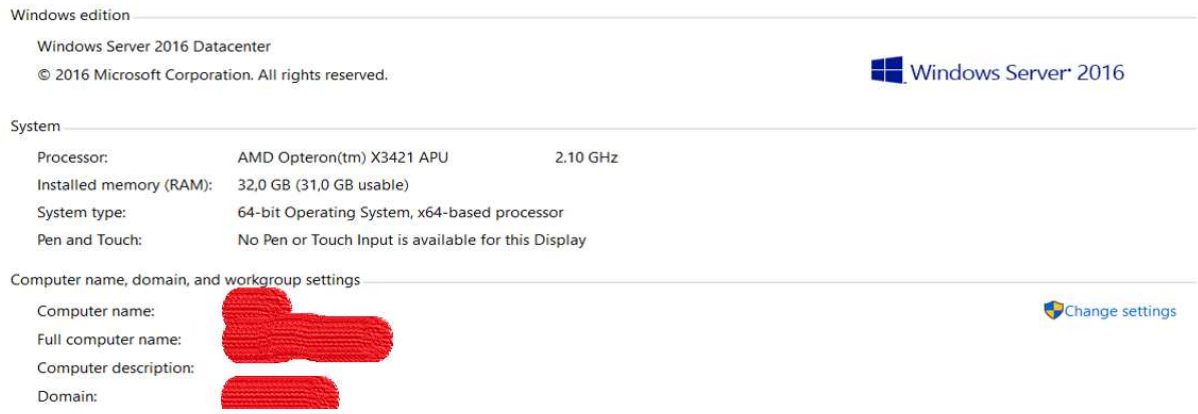


Figure 4.2-27 Serveur AD

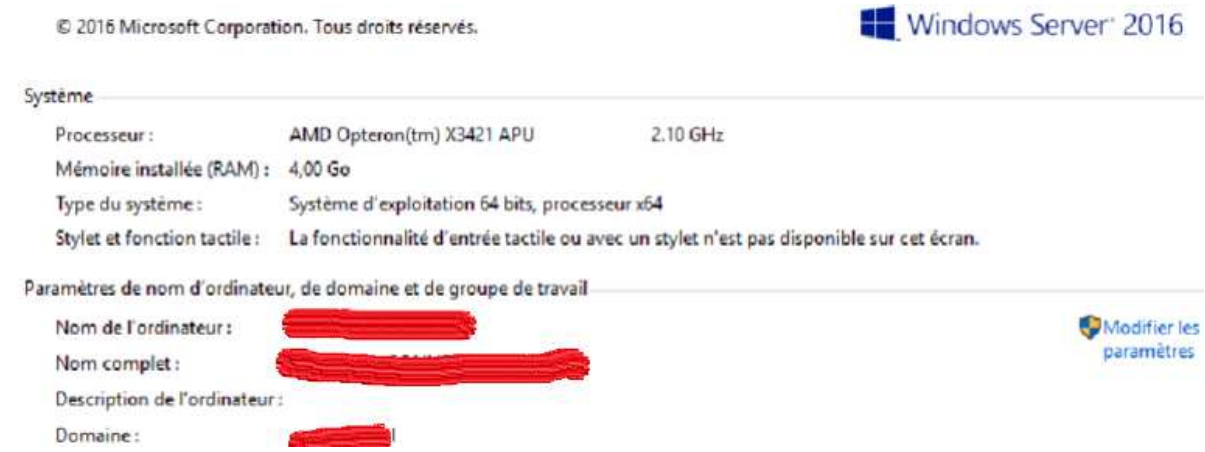


Figure 4.2-28 Serveur Azure AD Connect

4.2.5.3.4 Installation et Configuration de Azure AD Connect

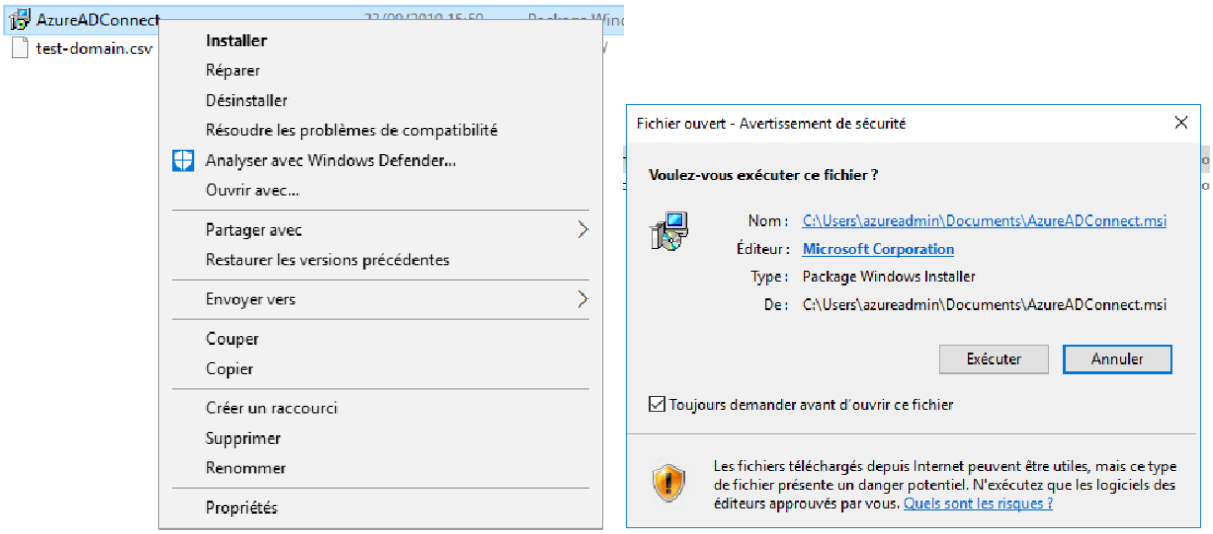


Figure 4.2-29 Installation Azure AD Connect

Après téléchargement de Microsoft Azure AD Connect et lancer l'installation nous allons maintenant spécifier les différents composants nécessaires pour assurer la synchronisation que sont :

- Un emplacement d'installation personnalisé
- Un compte de service
- Les groupes de synchronisation personnalisés

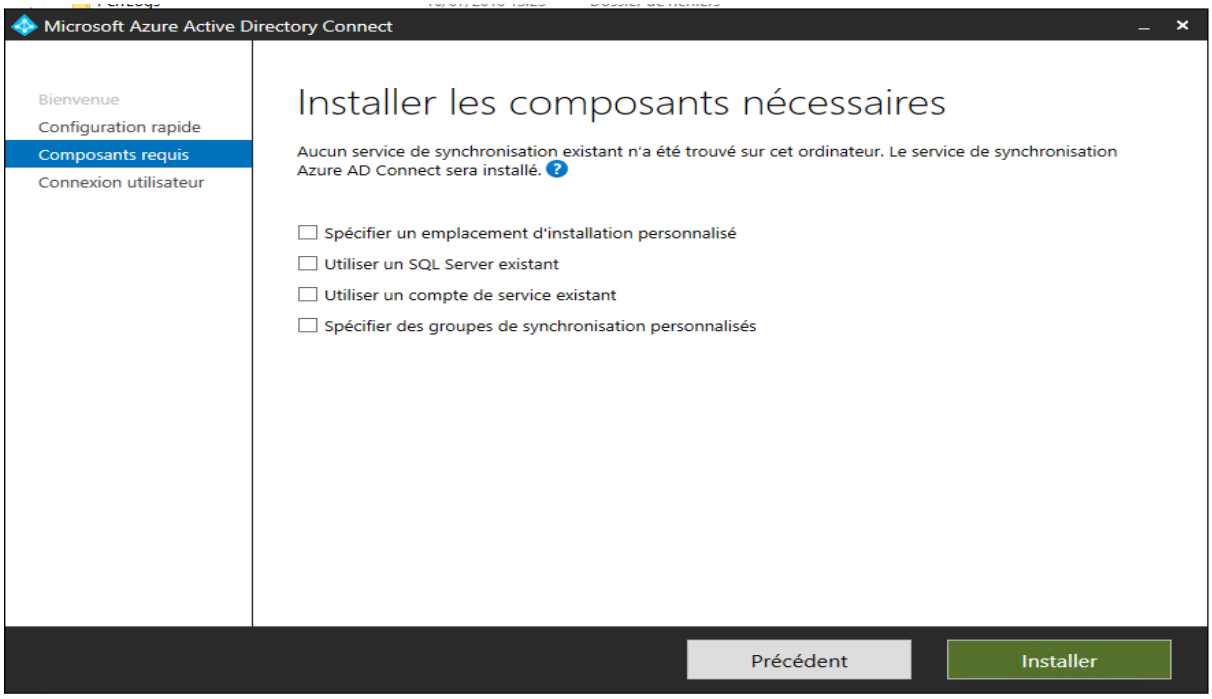


Figure 4.2-30 Composants Azure AD Connect

Si la vérification sur les composants nécessaires est terminée nous indiquerons la méthode a utilisé pour l'authentification des utilisateurs

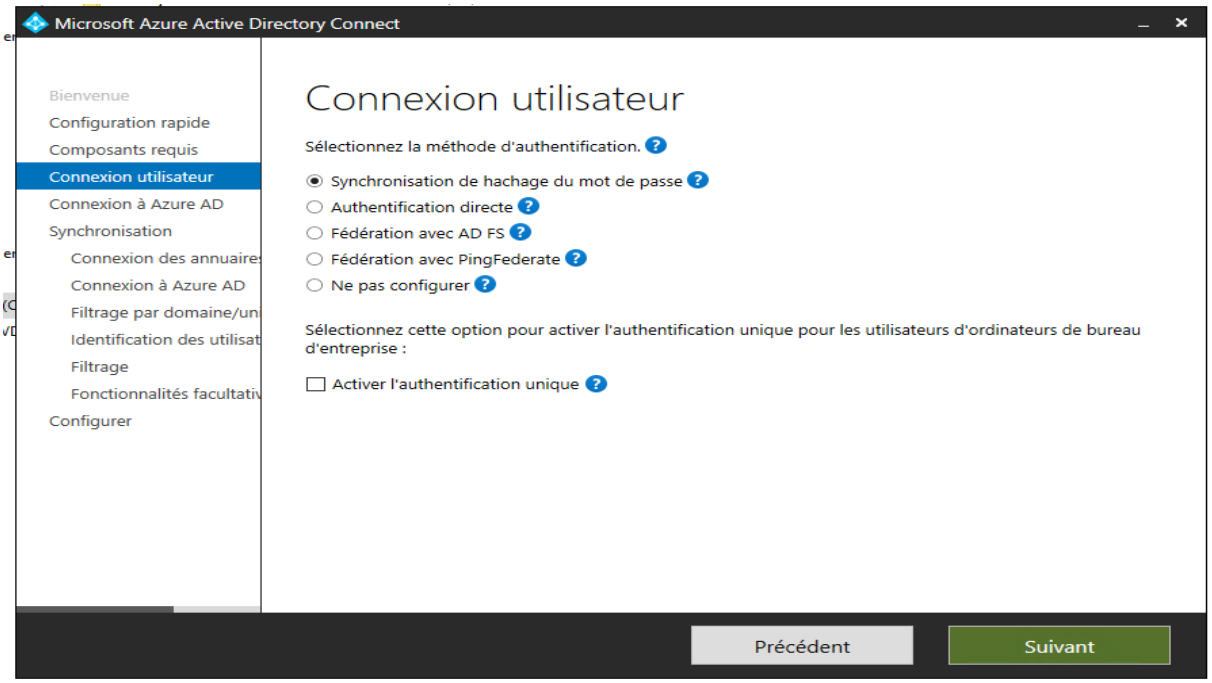


Figure 4.2-31 Authentification Azure AD Connect

Indication des informations d'identification pour administrateur général Azure AD Connect

- Nom d'utilisateur
- Mots de passe

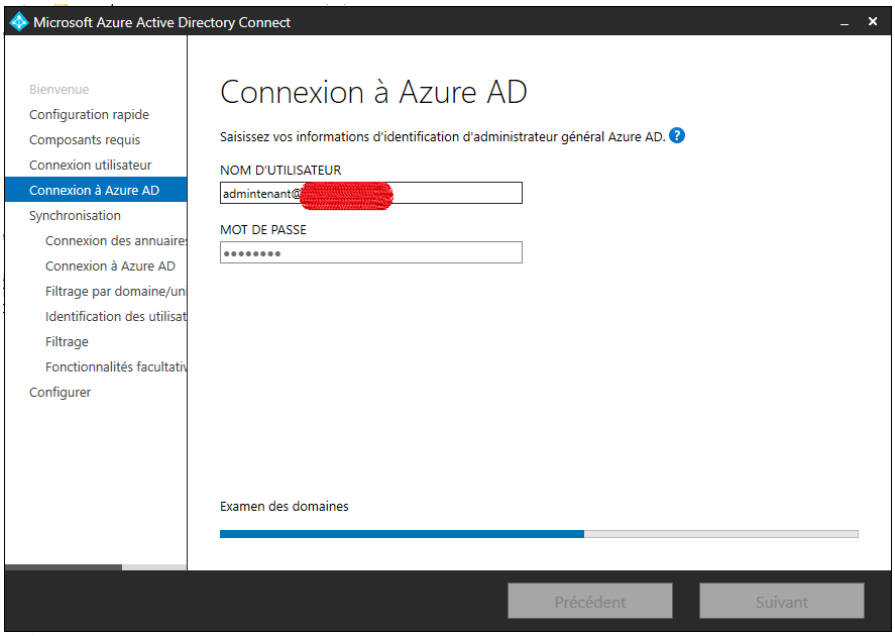


Figure 4.2-32 Connexion à Azure AD

Nous définirons ensuite le type d'annuaire a utilisé notre serveur de contrôleur de domaine et le nom de la forêt du contrôleur de domaine.

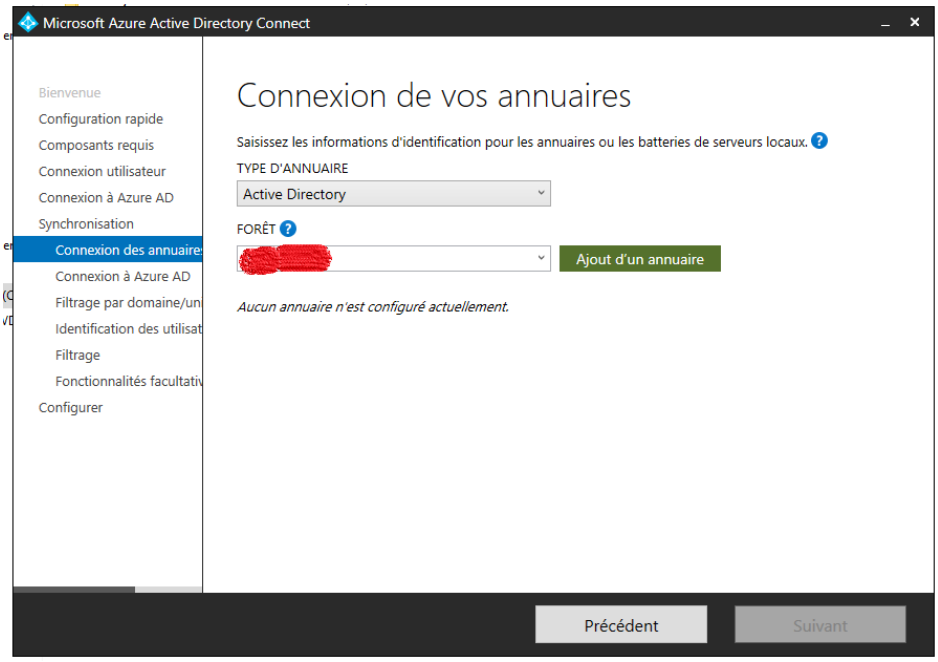


Figure 4.2-33 Connexion annuaire

Nous définirons le compte que nous utiliserons pour faire la synchronisation, il doit être membre du domaine et avoir les autorisations nécessaires pour la synchronisation comme indiquer au niveau des prérequis.

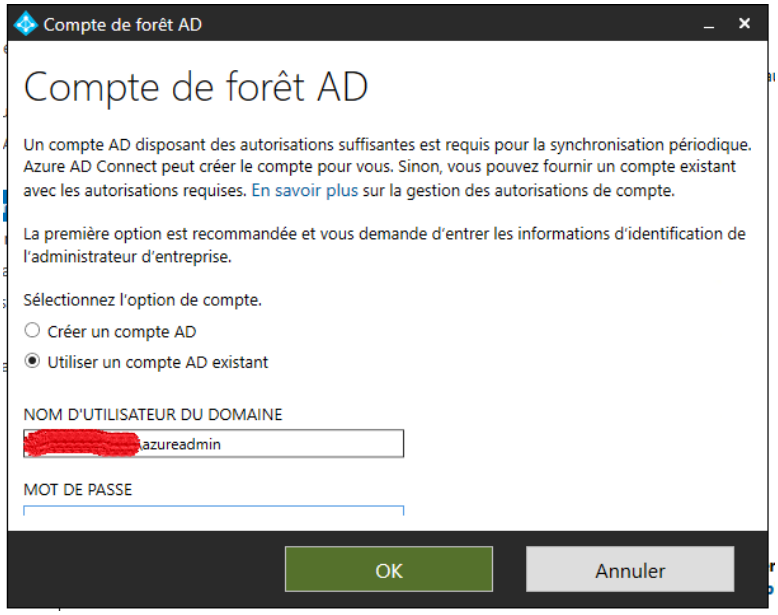


Figure 4.2-34 Compte de forêt AD

Nous allons ensuite donner le nom des suffixes UPN pour que les mêmes informations d'identifications qui soient sur notre AD local se trouvent sur l'AD Azure configuré.

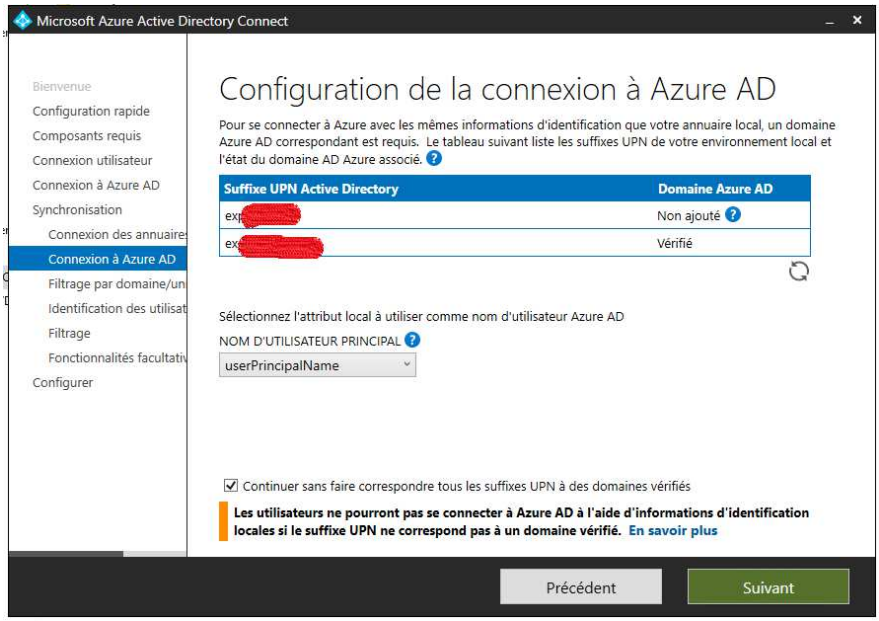


Figure 4.2-35 Suffixes UPN

Définition de la manière d'identification des utilisateurs par AD Azure

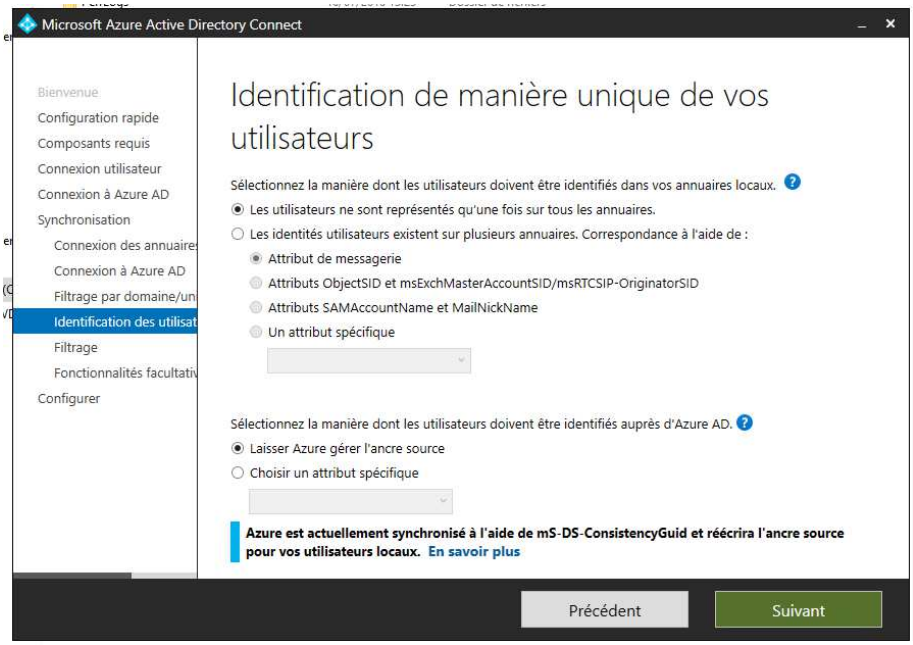


Figure 4.2-36 Identification des utilisateurs

Ainsi après ces différentes étapes, un filtrage des utilisateurs et appareils c'est-à-dire de donner le groupe qui contient les utilisateurs à synchroniser et de définir la synchronisation par hachage de mots de passe pour renforcer la sécurité des comptes d'utilisateur nous aurons l'image ci-dessous nous indiquant une récapitulatif des différentes configurations faites.

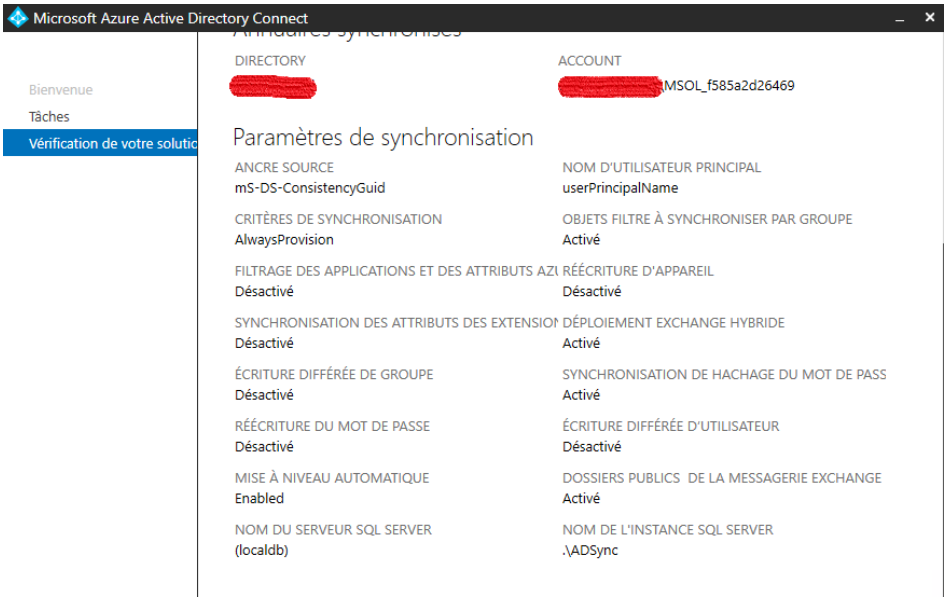


Figure 4.2-37 Configurations Azure AD Connect

Après une vérification de l'ensemble de ces configurations que nous avons fait, nous pourrons alors lancer la synchronisation entre notre AD local et Azure Active Directory.

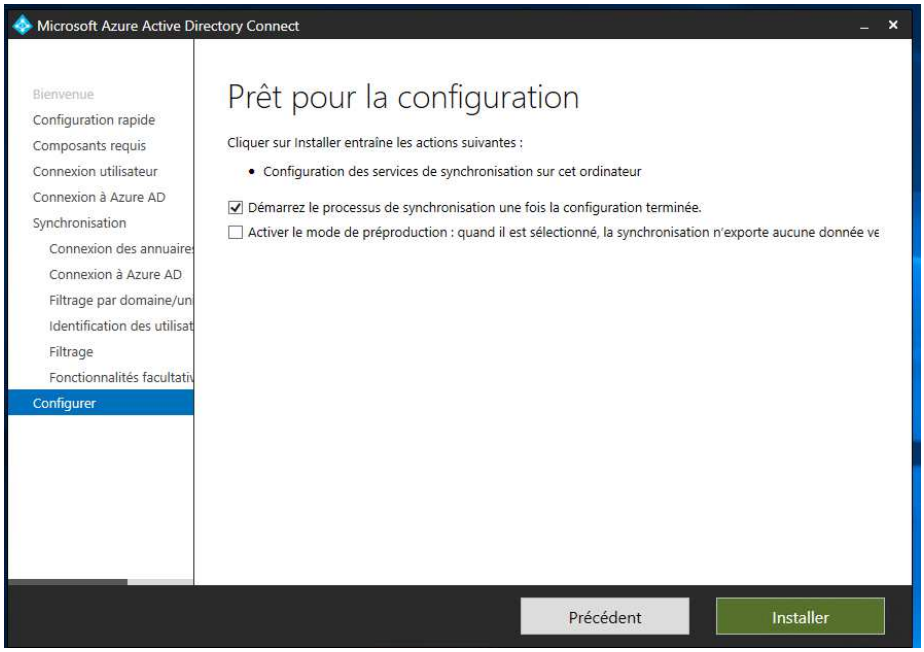


Figure 4.2-38 Synchronisation Azure AD et AD Local

4.2.5.3.5 Mise en œuvre de l'hybridation de la messagerie

D'après une installation et vérification des prérequis matériels et logiciels pour le déploiement de l'hybridation de la messagerie exchange, nous pouvons maintenant déployer l'assistant d'hybridation.

Nous avons opté de faire une hybridation complète de la messagerie parce qu'elle prenne en charge les fonctionnalités comme :

- Partage de disponibilité
- Flux de courrier amélioré
- Etc.

Se connecter au **centre d'administration exchange** -> sélectionnez le sous menu **hybride -> Modifier** pour se connecter ensuite à **Office 365**

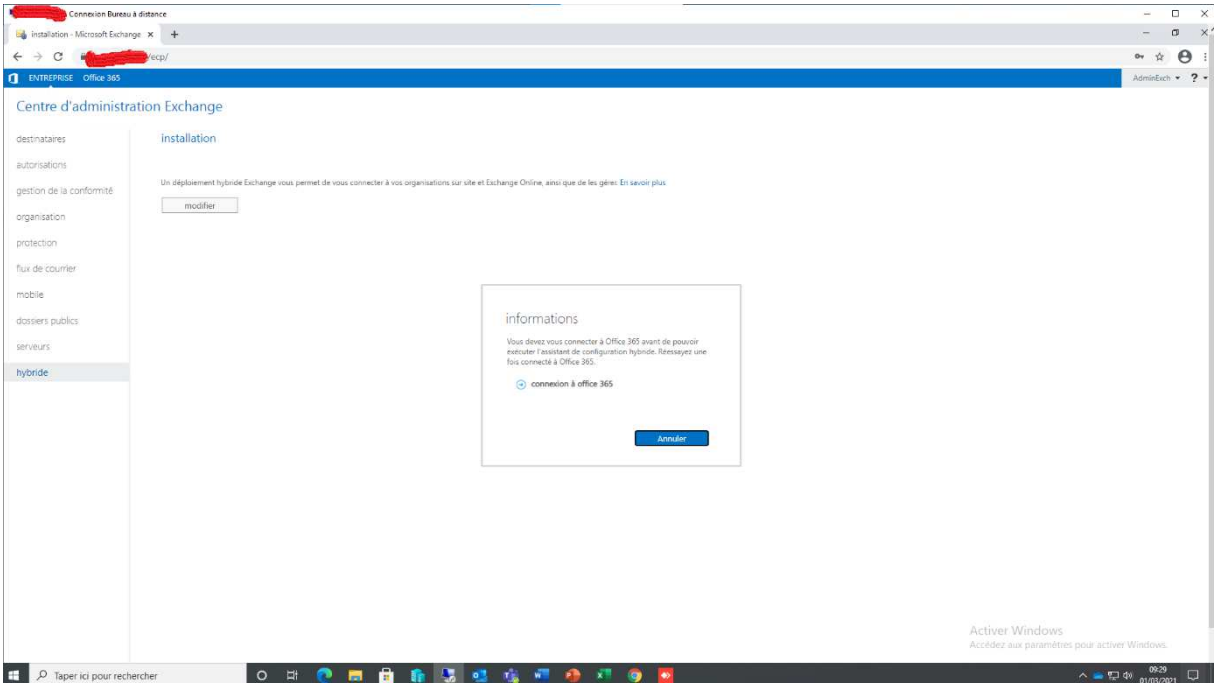


Figure 4.2-39 Connexion à Office 365

Si la connexion passe vous serez redirigé sur exchange online.

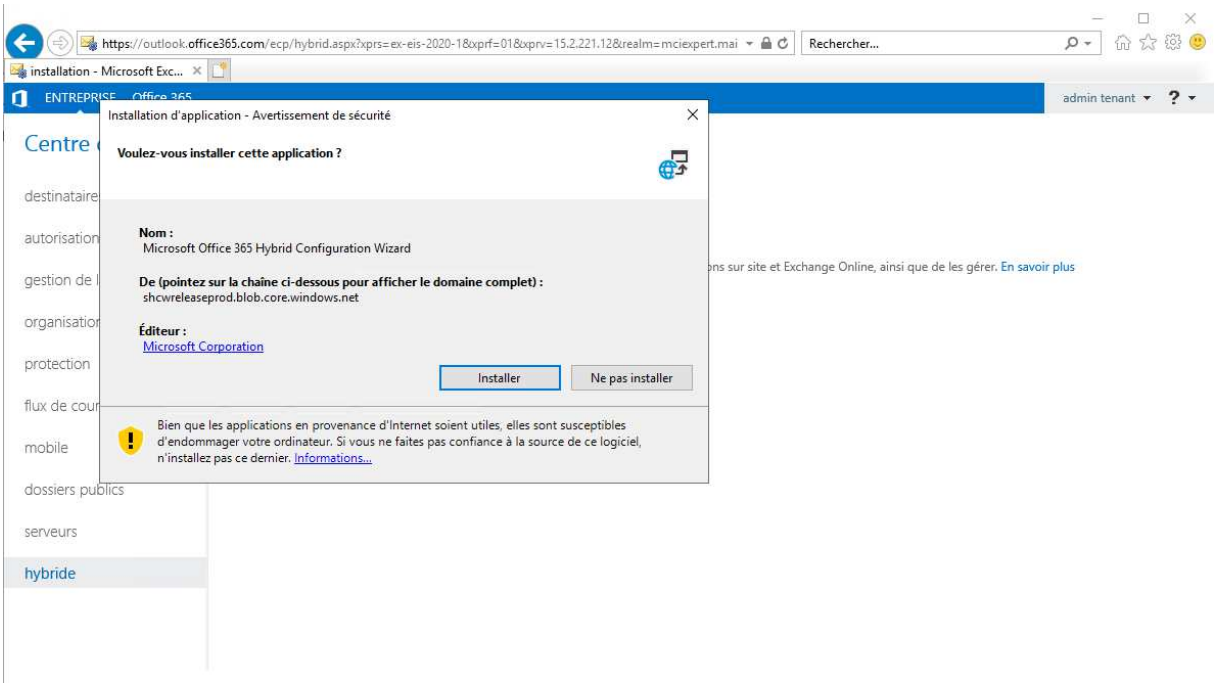


Figure 4.2-40 Assistant hybridation

Si le téléchargement et l'installation terminaient nous allons maintenant passer au paramétrage avancés.

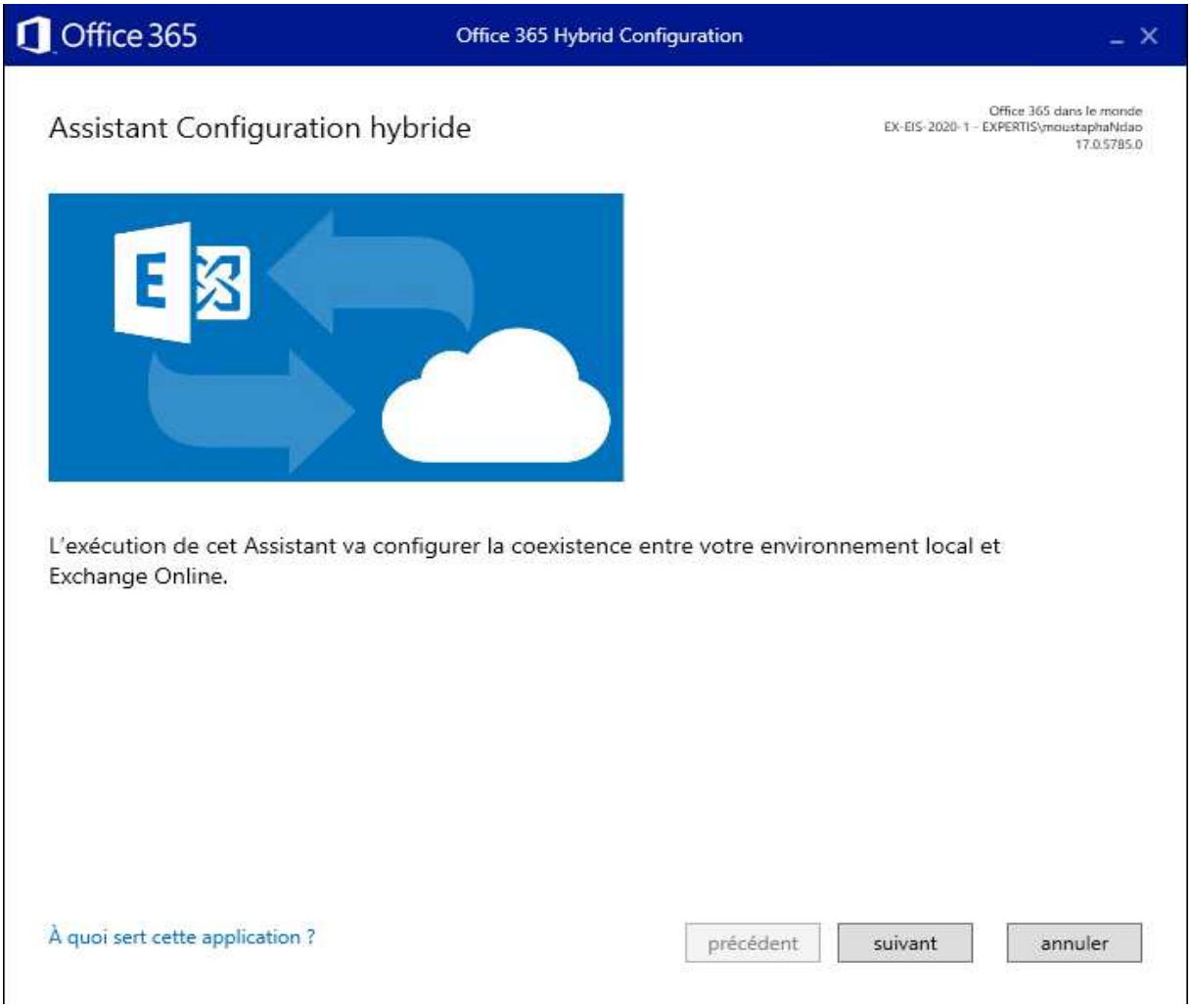


Figure 4.2-41 Configuration des paramètres hybridation

Ainsi alors nous avons les détails :

- Le nom du serveur exchange
- Domaine dans lequel il est joint
- La version du serveur de messagerie
- Les rôles installés
- Etc.

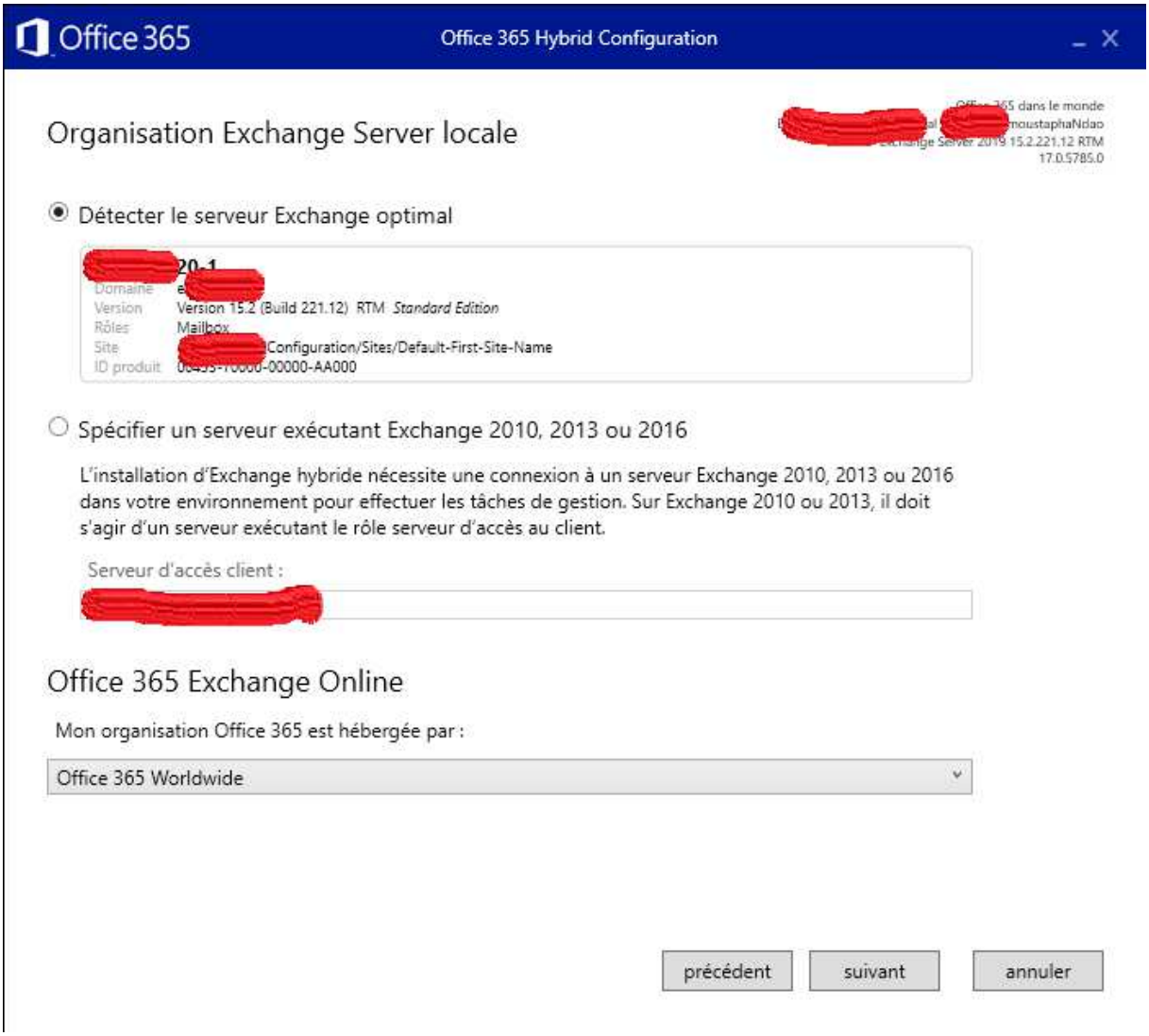


Figure 4.2-42 spécification serveur cible

Après nous définirons le type d'hybridation à choisir. Dans notre cas nous avons choisi de faire une hybridation complète de la messagerie qui permettra à l'organisation de profiter de l'ensemble des fonctionnalités comme le partage de la disponibilité, le flux de courrier amélioré, eDiscovery (découverte électronique)

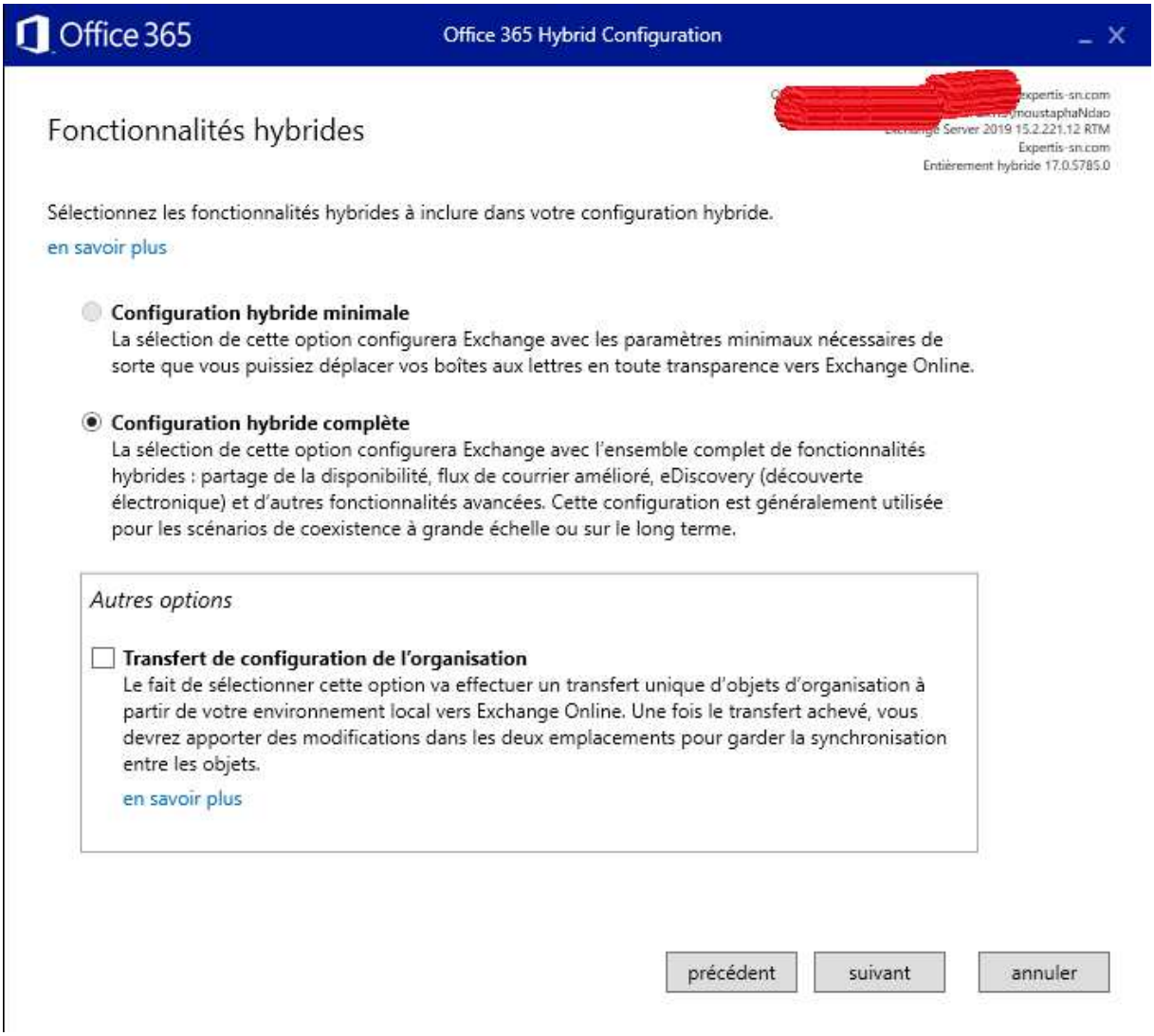


Figure 4.2-43 Types d'hybridation

Donner ensuite le type de la topologie

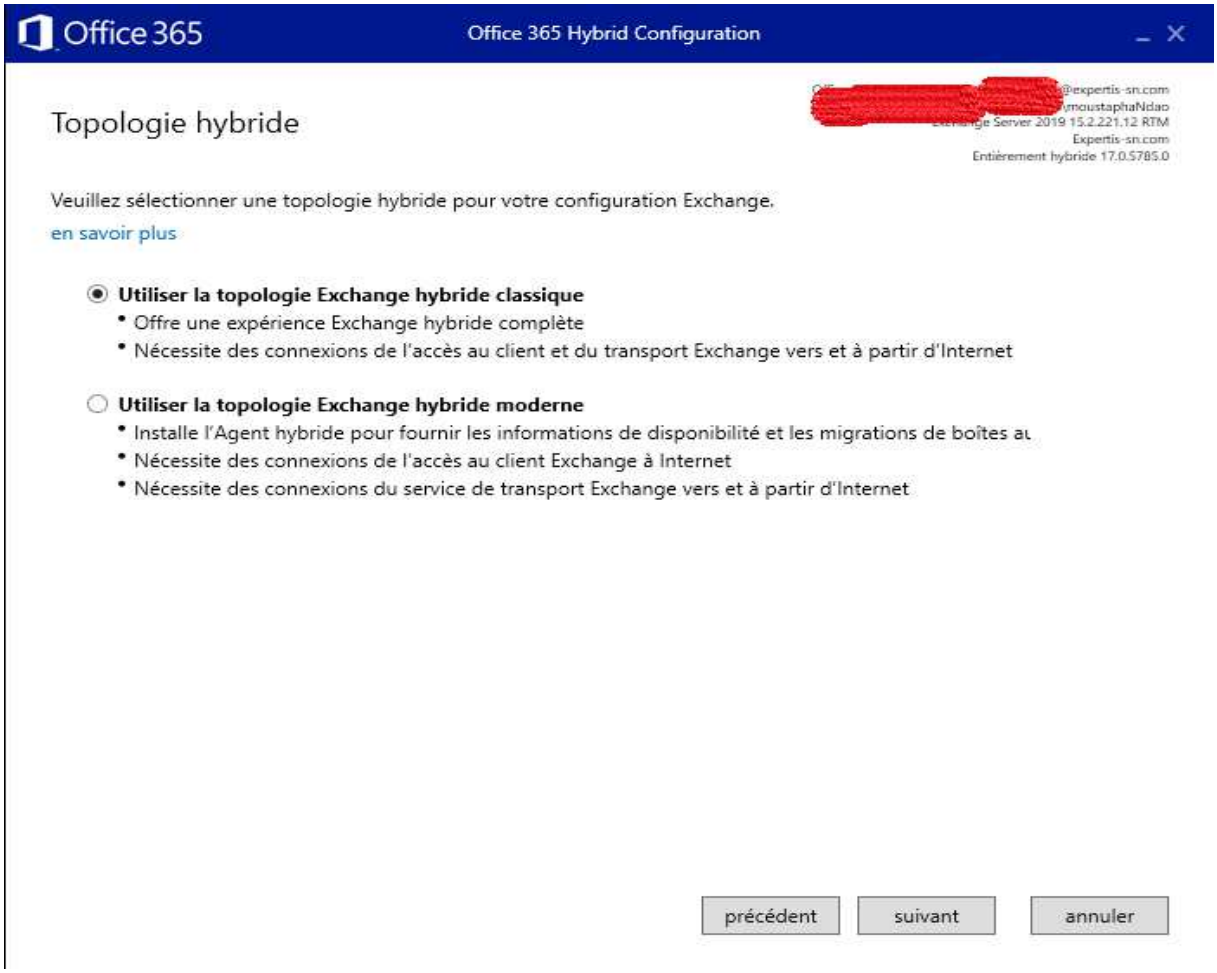


Figure 4.2-44 Topologie

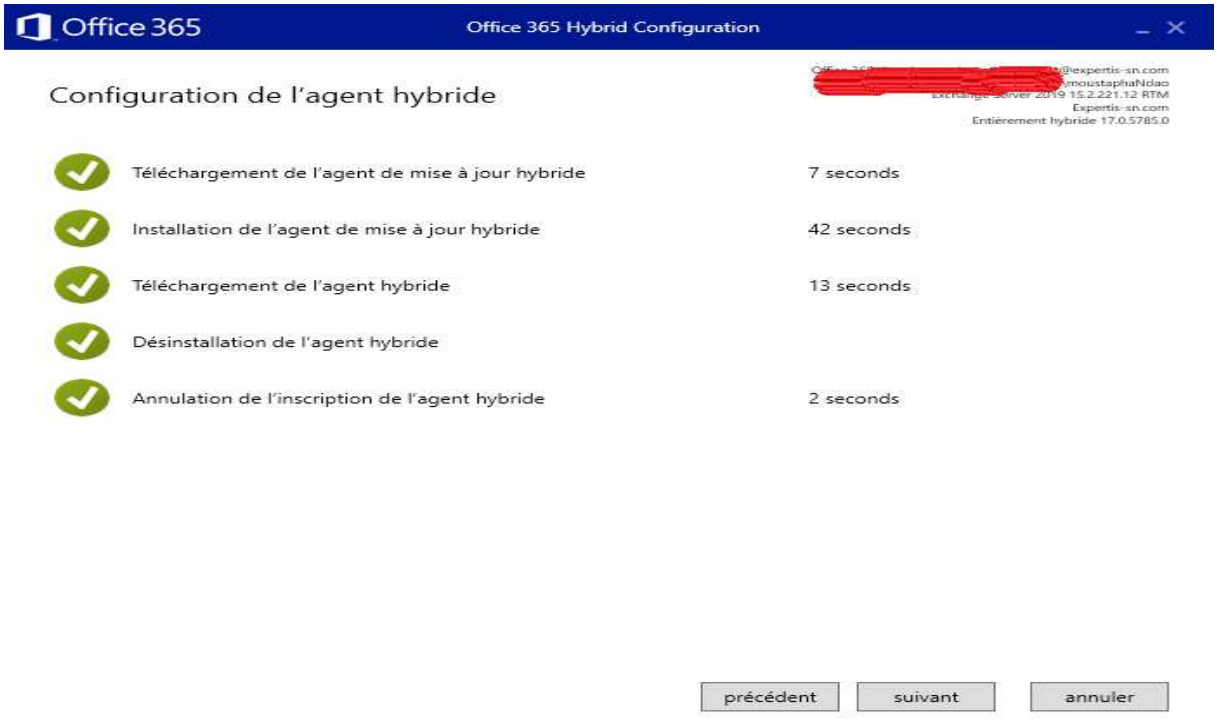


Figure 4.2-45 Finalisation paramètres

Ainsi après un déploiement de l'assistant d'hybridation et toutes les configurations apportées nous voilà maintenant arriver à terme de ce projet mais tout ayant quelques erreurs et sont résolus par l'installation et le paramétrage d'une autorité de certification ADCS sur le contrôleur de domaine principale.

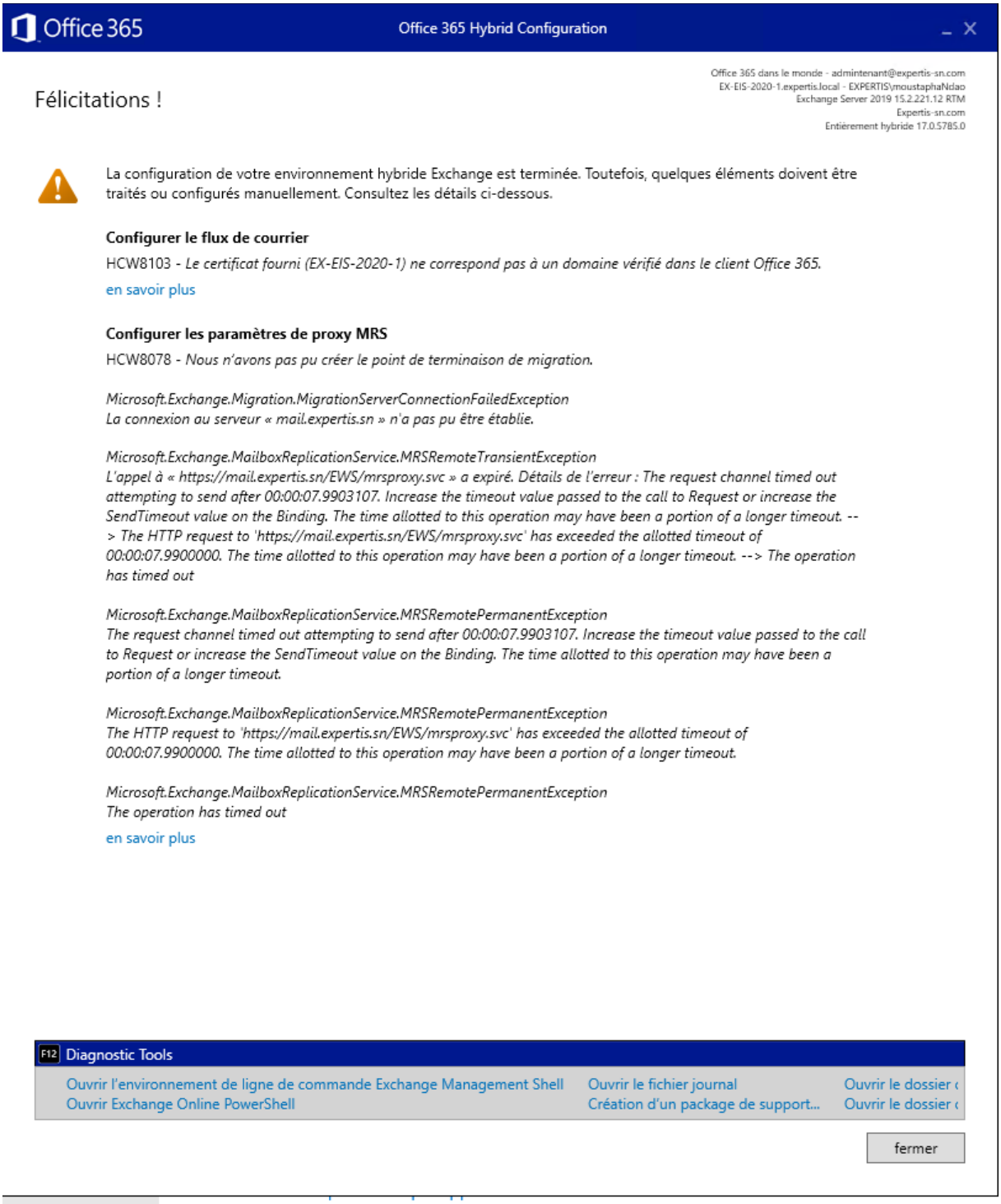


Figure 4.2-46 Hybridation messagerie

Conclusion

Dans cette partie nous avons pu faire une présentation des différentes solutions déployées au niveau de l'infrastructure d'EIS pour apporter des solutions à des problèmes qui ont été soulevés.

Conclusion Générale

L'objectif de ce travail était de faire une étude afin d'optimiser une infrastructure hybride. De ce fait, nous avons fait une étude du cloud computing c'est-à-dire ces différents systèmes de déploiement et services et la sécurité dans le cloud computing mais aussi plus précisément la solution Azure de Microsoft qui est déployée auparavant au sein de l'entreprise. D'après cette étude faite, nous avons pu déployer les solutions que nous avons jugés optimales et qui nous ont été proposées c'est-à-dire l'hybridation de la messagerie et le déploiement d'une solution d'accès terminal serveur, tout en respectant les spécifités techniques de l'entreprise. Cependant avec la cybercriminalité qui prend de l'ampleur dans le monde des technologies de l'information et de la communication, la mise au point de stratégies techniques et des matériels (pare-feu, logiciel de détection et de préventions d'intrusions IDS et IPS) afin de lutter contre ce mal mais aussi une politique de sécurité interne pour mieux protéger l'organisation et ses employés vis-à-vis des risques et menaces informatiques.

Ce stage nous a donné l'occasion de nous familiariser avec les différents solutions cloud qui existent dans le marché mais également d'être plus autonome, méthodique et rigoureux pour réaliser ce travail.

Bibliographie

[1] Peter Mell, Timothy Grance, "*Recommendations of the National Institut and Technology",* special publication 800-145

[7] Christian Delettre, Karima Boudaoud et Michel Riveill, « *Cloud Computing, Sécurité et Dissimulation de Données »* 7ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information – Cabourg 22-25 mai 2012

[8] Yanpei Chen, Vern Paxson et Randy H. Katz, "*What's New About Cloud Computing Security*" Edition University of California, 2010

[9] Rong C et al. "*Beyond lightning: A survey on security challenges in cloud computing"*. Comput Electr Eng. (2012)

[10] Mémoire de Mor Talla Gueye, "*Étude et Mise en place d'une infrastructure Hybride*" 2019

[13] Mouhamed Athie *"Services Bureau à distance"* Editions ENI

Webographie

[2] https://www.redhat.com/fr/topics/virtualization/what-is-virtualization consulté le 13/11/2020

[3] https://blog.ippon.fr/2017/06/09/les-architectures-serverless/ consulté le 22/12/2020

[4] https://www.lebigdata.fr/microsoft-azure-tout-savoir consulté le 08/01/2021

[5] https://fr.wikipedia.org/wiki/Amazon_Web_Services consulté le 22/12/2020

[6] https://fr.wikipedia.org/wiki/Google_Cloud_Platform consulté le 22/12/2020

[11] https://hichamkadiri.wordpress.com/2015/04/22/guide-pas-a-pas-mise-en-place-dune-infrastructure-rds-2012-r2-hautement-disponible-part-1/ consulté le 16/11/2020

[12] https://docs.microsoft.com/en-us/azure/virtual-desktop/windows-10-multisession-faq consulté le 12/11/2020

[14] https://www.microsoft.com/fr-ww/microsoft-365/enterprise/compare-office-365-plans?market=sn consulté le 23/12/2020

[15] https://fr.wikipedia.org/wiki/Microsoft_Exchange_Server consulté le 15/01/2020

[16] https://docs.microsoft.com/en-us/exchange/new-features/new-features?view=exchserver-2019 consulté le 15/01/2020

[17] https://docs.microsoft.com/fr-fr/exchange/architecture/mailbox-servers/managed-store/managed-store?view=exchserver-2019#:~:text=The%20Managed%20Store%20is%20the,isolation%20and%20faster%20database%20failover. Consulté le 15/02/2021

[18] https://docs.microsoft.com/fr-fr/exchange/recover-an-exchange-server-exchange-2013-help consulté le 28/01/2021