

Sécurité, organisation et performance désignent les trames essentielles à la mise en place de serveurs en milieu professionnel. Ces 3 thématiques conduiront l'entreprise BSD tout au long du livrable.

Projet EVOLUTION

Déploiement des serveurs
Windows et Debian

LEONEL DROUHARD
SEBASTIEN SOMBRET
WILLIAM BERQUET

I. Avant-propos

Ce livrable s'inscrit dans le cursus de la formation *Gestionnaire de Maintenance et Support Informatique*, et se déroulant au CESI de Reims. Il portera sur l'administration d'un parc informatique, dans le cadre d'une intégration de serveurs et du déploiement de services de communication. Ce projet continue la démarche pédagogique des précédents projets « SAS » et « START », visant l'acquisition des compétences nécessaires à l'environnement professionnel.

Dans la continuité de l'installation du réseau câblé puis du déploiement des systèmes d'exploitation lors du projet START, l'amélioration de l'environnement numérique en milieu professionnel nécessite l'intégration de serveurs, qui permettront une gestion centralisée de l'ensemble du parc informatique.

Ce travail veut mettre en relief une conduction efficace de cette initiative. Les éléments nécessaires à cette fin seront confrontés aux impératifs imposés dans l'énoncé de l'exercice, aux grilles d'évaluations, ainsi qu'aux suggestions des intervenants.

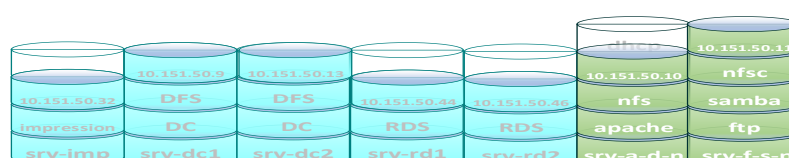
Plusieurs obstacles ont demandé un examen approfondi de la part de notre groupe. Tout d'abord, assimiler une grande quantité d'information en un temps limité fut un défi. Ensuite, la réactivité des serveurs de test, malgré les performances de la plateforme de virtualisation, s'est révélée parfois pesante. Enfin, quelques initiatives à propos des stratégies de groupes ou de l'affichage de la base de données furent des investissements riches mais stressant dans leurs réalisations.

II. Remerciement

En premier lieu, nous tenons à remercier M. Frederic LEROUX, pilote du projet Evolution pour la qualité de ses conseils, sa disponibilité et son enthousiasme à nous faire progresser dans le domaine de l'administration informatique.

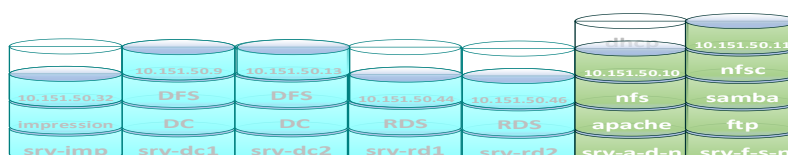
Nous souhaitons également gratifier les efforts et la patience de M. Jason Mahdjoub, intervenant lors de ce projet pour son apport dans notre compréhension de l'algorithmie et de la gestion des bases de données relationnelles

Enfin, nous exprimons notre reconnaissance pour l'ensemble de l'équipe pédagogique du CESI de Reims pour son soutien et sa bienveillance tout au long de ce travail.



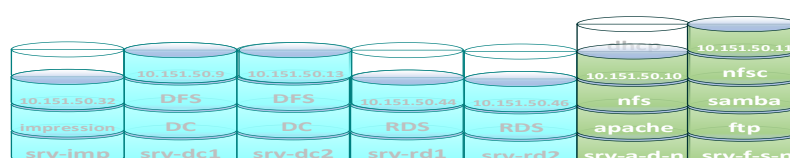
III. Table des matières

<p>I. Avant-propos2</p> <p>II. Remerciement.....2</p> <p>III. Table des matières.....3</p> <p style="padding-left: 20px;">A. Table des illustrations4</p> <p style="padding-left: 20px;">B. Liste des abréviations5</p> <p style="padding-left: 20px;">C. Glossaire.....6</p> <p>IV. Introduction8</p> <p>V. Cadrage8</p> <p style="padding-left: 20px;">A. Présentation entreprise9</p> <p style="padding-left: 20px;">B. Cahier des charges10</p> <p>VI. Conception10</p> <p style="padding-left: 20px;">A. Méthode de pilotage10</p> <p style="padding-left: 20px;">B. Stratégie informatique – Stratégie IT12</p> <p style="padding-left: 20px;">C. Planification13</p> <p style="padding-left: 20px;">D. Plan de communication.....13</p> <p>VII. Windows Server 201614</p> <p style="padding-left: 20px;">A. Choix des serveurs14</p> <p style="padding-left: 20px;">B. Topologie réseau.....14</p> <p style="padding-left: 20px;">C. Système d’exploitation et licence15</p> <p style="padding-left: 20px;">D. Rôle ADDS et DC.....15</p> <p style="padding-left: 20px;">E. Rôle DFS - Système de fichiers distribués 16</p> <p style="padding-left: 20px;">F. Rôle RDS - Services Bureau à distance17</p> <p style="padding-left: 20px;">G. Rôle DHCP.....17</p> <p style="padding-left: 20px;">H. Permission NTFS.....17</p> <p style="padding-left: 20px;">I. Stratégies de groupe18</p> <p style="padding-left: 20px;">J. Serveur d’impression18</p> <p>VIII. Serveurs Debian18</p> <p style="padding-left: 20px;">A. SSH19</p> <p style="padding-left: 20px;">B. Webmin.....19</p> <p style="padding-left: 20px;">C. Serveurs de fichiers.....19</p> <p style="padding-left: 40px;">❖ ProFTPD19</p> <p style="padding-left: 40px;">❖ SAMBA20</p>	<p style="padding-left: 40px;">❖ NFS.....20</p> <p style="padding-left: 40px;">❖ Apache20</p> <p>IX. Budget prévisionnel21</p> <p>X. Conclusion.....21</p> <p>XI. Charte graphique22</p> <p>XII. Webographie23</p> <p>XIII. Annexes.....26</p> <p style="padding-left: 20px;">A. Planification26</p> <p style="padding-left: 40px;">❖ Le tableau RACI.....26</p> <p style="padding-left: 40px;">❖ Trello.....26</p> <p style="padding-left: 40px;">❖ Microsoft Project Pro 201927</p> <p style="padding-left: 20px;">B. Installation serveurs.....30</p> <p style="padding-left: 40px;">❖ Licences Microsoft Windows.....30</p> <p style="padding-left: 40px;">❖ Devis Serveurs30</p> <p style="padding-left: 20px;">C. Topologie serveurs BSD.ADDS33</p> <p style="padding-left: 20px;">D. Active Directory.....33</p> <p style="padding-left: 40px;">❖ Topologie DFS Réplication33</p> <p style="padding-left: 40px;">❖ Topologie Active directory35</p> <p style="padding-left: 20px;">E. Tableau des permissions NTFS.....36</p> <p style="padding-left: 20px;">F. Rôle DHCP36</p> <p>Base de données relationnelles.....38</p> <p style="padding-left: 20px;">G. Scripts PowerShell.....48</p> <p style="padding-left: 20px;">H. Script Rds.....54</p> <p style="padding-left: 20px;">I. Procédure Windows56</p> <p style="padding-left: 20px;">J. Procédure Linux95</p> <p style="padding-left: 40px;">❖ Installation95</p> <p style="padding-left: 40px;">❖ Webmin98</p> <p style="padding-left: 40px;">❖ Nfs.....100</p> <p style="padding-left: 40px;">❖ Apache100</p> <p style="padding-left: 40px;">❖ Samba104</p> <p style="padding-left: 40px;">❖ Proftpd.....106</p> <p style="padding-left: 20px;">K. Dhcp.....110</p>
--	---



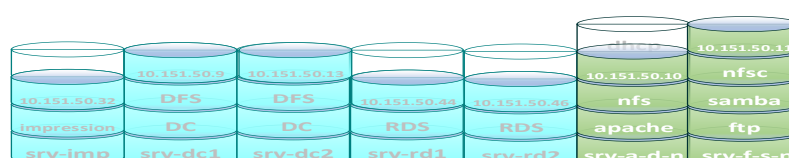
A. Table des illustrations

Figure XIII-1 : Découpage projet via Trello	27	Figure XIII-19 : Power Shell UO	48
Figure XIII-2 : Planification Gantt maquetage ...	27	Figure XIII-20 : Power Shell users csv.....	48
Figure XIII-3 : Planification Gantt déploiement ..	28	Figure XIII-21 : Power Shell script user	49
Figure XIII-4 : Planification calendrier	28	Figure XIII-22 : Power Shell ISE création ordinateurs	51
Figure XIII-5 : Planification taches en cours	29	Figure XIII-23 : Power Shell ISE creation users ...	52
Figure XIII-6 : Planification tache en retard	29	Figure XIII-24 : Samba passwd false	Erreur ! Signet non défini.
Figure XIII-7 : Capture d'écran prix licences	30	Figure XIII-25 : Proftpd filezilla.....	106
Figure XIII-8 : Liaisons switches-serveurs bsd.adds	33	Figure XIII-26 : ftp filezilla sav	107
Figure XIII-9 : Vignettes DFS + Informations domaine	34	Figure XIII-27 : ftp produitb	107
Figure XIII-10 : Arborescence des UO	35	Figure XIII-28 : ftp script de comptage archive nettoyage	Erreur ! Signet non défini.
Figure XIII-11 xampp	39	Figure XIII-29 : apache cron	108
Figure XIII-12 Base de données users	40	Figure XIII-30 : Script_ftp_log.sh.....	108
Figure XIII-13 ODBC.....	42	Figure XIII-31 : Client Windows lien ftp SAV et produitB	108
Figure XIII-14 : Table relationnel Access	42	Figure XIII-32 : Client windows ftp sav.....	109
Figure XIII-15 : Access tables imbriqués	43	Figure XIII-33 : Client Windows ftp produitb	Erreur ! Signet non défini.
Figure XIII-16 : Access tables imbriquées 2.....	43	Figure XIII-34 : Serveurs	111
Figure XIII-17 : Access Requête	44		
Figure XIII-18 : Requête Access	Erreur ! Signet non défini.		



B. Liste des abréviations

<i>AD</i> : Active Directory	<i>NTDS</i> : New Technology Directory Services
<i>ADDS</i> : Active Directory Domain Services	<i>OS</i> : Operating System
<i>BDD</i> : Base de données	<i>OSI</i> : Open Systems Interconnection
<i>BOTM</i> : But, Objectifs, Tactiques, Mesures	<i>PC</i> : Post Computer
<i>CAL</i> : Client Access License	<i>PS</i> : PowerShell
<i>Cmdlet</i> : Command-Let	<i>RACI</i> : Responsible, Accountable, Consulted et Informed
<i>CSV</i> : Comma-Separated Values	<i>RAID</i> : Redundant Array of Independent Disks
<i>DFS</i> : Distributed File System	<i>RD</i> : Remote Desktop
<i>DNS</i> : Domain Name System	<i>RDS</i> : Remote Desktop Services
<i>ESXi</i> : Elastic Sky X integrated	<i>RH</i> : Ressources Humaines
<i>FTP</i> : Files Transfer Protocol	<i>SAV</i> : Service Après-Vente
<i>GC</i> : Global Catalog	<i>SI</i> : Service Informatique
<i>GPO</i> : Group Policy Object	<i>SMB</i> : Server Message Block
<i>IMP</i> : Impression	<i>SSH</i> : Sécure SHell
<i>IP</i> : Internet Protocol	<i>SSII</i> : Société de Services en Ingénierie Informatique
<i>ISE</i> : integrated scripting environment	<i>SW</i> : Switch (commutateur)
<i>IT</i> : Information Technology	<i>SYSVOL</i> : Volum System
<i>LDAP</i> : Light Directory Access Protocol	<i>TCP</i> : Transmission Control Protocol
<i>NFS</i> : Network File System	<i>UO</i> : Unité Organisationnelle
<i>NFSC</i> : NFS Client	
<i>NTFS</i> : New Technology Files System	





Requête : Instruction envoyée par un terminal, en attendant une réponse du destinataire

Script : Programme automatisant les actions d'un ordinateur

Serveur : Entité informatique fournissant des services à destination de clients

Service : Dans un réseau informatique, application fournie par un serveur et utilisé par un client

SMB : Protocole permettant aux utilisateurs de lire et d'écrire des fichiers sur un serveur connecté sur le réseau

Stratégie de groupe (ou GPO) : Fonctionnalité contrôlant l'environnement des utilisateurs et les ordinateurs au sein d'un domaine Microsoft

Super Utilisateur ou Root : Utilisateur Unix disposant de tous les droits d'administration du système

Système de fichier : Méthode de stockage et de récupération de données

Terminal : Equipement permettant l'exploitation de données

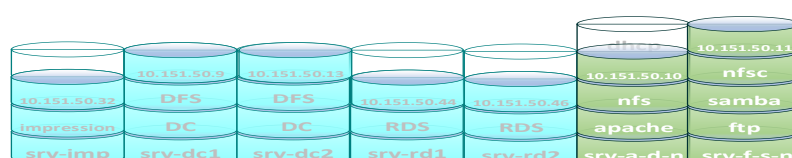
TCP-IP : Protocole de transmission dédié à l'intégrité des données transmises

Thread : En relation avec un processeur, unité de traitement virtualisée

UNIX : Système d'exploitation ayant inspiré la création du noyau Linux

User : Utilisateur d'une ressource informatique

Unité organisationnelle : Espace dans un domaine où l'on peut stocker et influencer les objets d'un domaine Microsoft



IV. Introduction

- En été 2019, l'utilitaire web Webmin dédié à la gestion à distance des systèmes Unix/Linux fut l'origine d'attaques contre des VPN d'entreprises comme Pulse Secure et Fortinet FortiGate, compromettant la sécurité des infrastructures touchées.
- L'étude de Kroll On Track de 2017 estime que la perte de données en entreprise est une cause de faillite majeure. Parmi ses chiffres, 60% des entreprises perdant leurs données ferment dans les 6 mois.

Ces deux extraits de l'actualité numérique cristallisent le défi de toute entreprise moderne : allier les avantages d'un réseau basé sur des serveurs centralisateurs tout en veillant activement à leur intégrité. Sans s'arrêter à cette dichotomie, nous pouvons enrichir la problématique sous-jacente.

Dans quelles mesures répondre aux exigences fonctionnelles, sécuritaires, de qualité et d'évolution de la disponibilité des données de l'entreprise BSD

Tout d'abord, nous construirons notre réflexion dans l'analyse de la situation actuelle et l'organisation qui en découlera. Une répartition du temps et des ressources sera nécessaire à l'aboutissement du projet dans les délais souhaités.

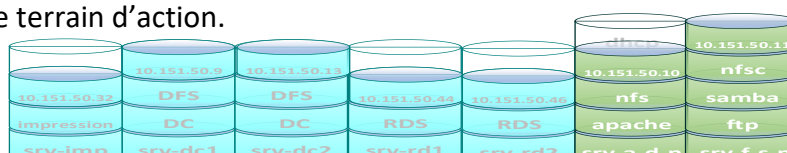
Suivant le plan préétabli, nous documenterons les prérequis et la mise en place d'une solution de centralisation des données (choisir une date en fonction de l'activité de l'entreprise), ainsi que des services réseau.

Une fois les serveurs installés et configurés, il s'agira de dresser une cartographie de l'espace utilisateurs via la création de bases de données. Enfin, décider de stratégies de groupes fixeront les environnements dans lesquels évolueront les salariés de l'infrastructure BSD.

V. Cadrage

Pour débuter cette étude de faisabilité, il convient d'en déterminer l'envergure, ses principaux acteurs, sa durée estimée, ses méthodes et ses buts. Pour cela, décrivons point par point les variables principales du projet :

- L'objet de cette étude porte sur le parc informatique de l'entreprise BSD, aussi bien les matériels, les utilisateurs et les données internes de l'entreprise
- Parmi ces utilisateurs, nous distinguons le directeur général, le directeur administratif et financier, le service informatique, les responsables de chaque service et les utilisateurs en général
- Les réflexions porteront uniquement sur le réseau interne de l'entreprise BSD
- Les échéances prévues sont les suivantes :
 - Lancement du projet :
 - Présentation de l'étude de faisabilité :
 - Phase de réalisation :
 - Aboutissement du projet :
- Les mises en œuvre se dérouleront selon l'ordonnement suggéré par le découpage du projet. Il sera question d'établir une planification des étapes, de l'achat de nouveaux matériels, de maquetages permettant le suivi des installations logicielles, de construire une structure réseau cohérente en fonction des services et des utilisateurs présents. La qualité, les coûts et les délais délimiteront le terrain d'action.



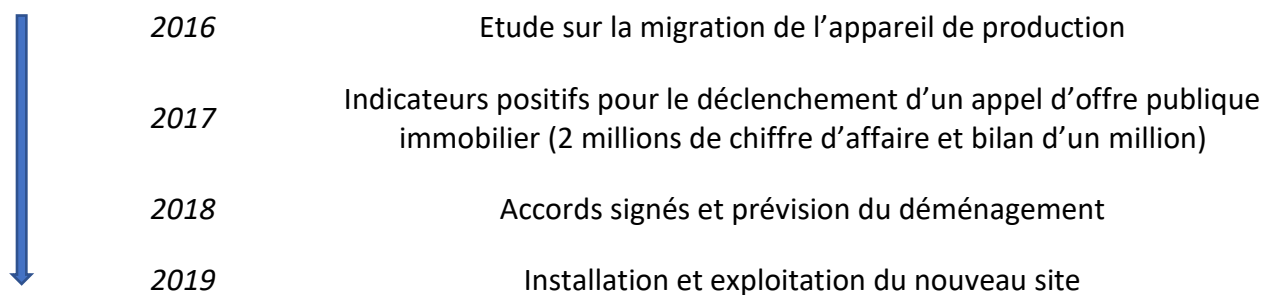
- Enfin, l'amélioration de l'administration système par la centralisation des données et des services vise une meilleure maîtrise du coût total de possession, une augmentation du retour sur investissement et un gain de temps sur toutes les opérations afférentes à l'infrastructure (communication locale, sécurité, stabilité, maintenance).

Ces thématiques dirigeront le fil conducteur de cette étude.

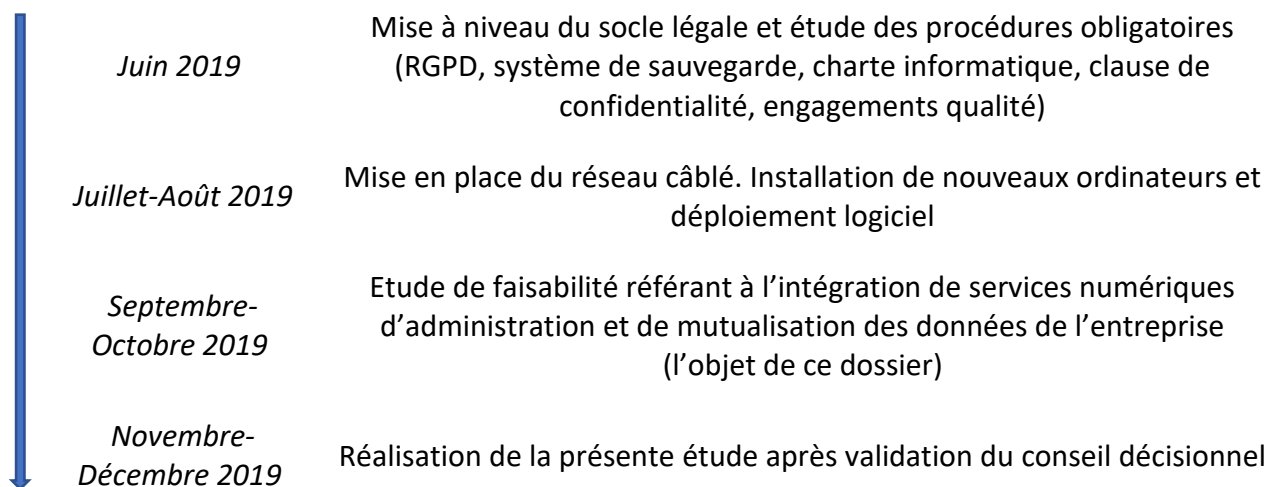
A. Présentation entreprise

L'entreprise BSD, spécialisée dans l'import et le reconditionnement de produits manufacturés, officie sur Reims depuis 2007. De forme juridique SARL regroupant moins de 100 salariés, BSD connaît une croissance importante depuis 2014. Ces résultats prometteurs, combinés à la vétusté des installations originelles, motivent le conseil décisionnel dans le renouveau et l'agrandissement des infrastructures.

Dans ce contexte, rappelons les évènements notables :



Concernant l'évolution des systèmes numériques de l'entreprise pendant la période 2019, nous relevons aujourd'hui quatre périodes de progression :



L'organigramme présente les ressources humaines mises en œuvre afin de délivrer la prestation BSD auprès de nos clients. Les services de l'entreprise BSD sont répartis comme suit :



productions, SAV, SI, et direction. Ces acteurs suivent par défaut le rythme d'accès officiel des locaux (7h-20h). Ces informations seront exploitées lors de l'installation des serveurs.

B. Cahier des charges

Pour réduire les incompréhensions entre exécutants et commanditaires, une formulation du cahier des charges doit être établie par les deux parties. Ci-dessous, l'interprétation par le service informatique des demandes de la direction :

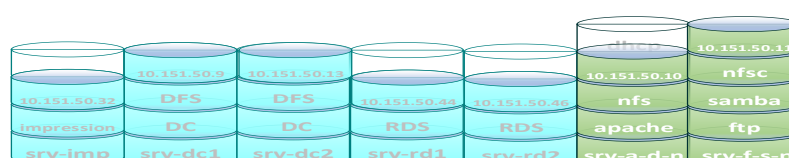
- Réduction des délais d'intervention et des sollicitations du support technique.
- Elaboration d'un inventaire regroupant les informations importantes du système d'information. Cette tâche comprendra la création numérique de cet inventaire (base de données) ainsi que ses moyens d'exploitation (affichage, filtrage, modification des informations)
- Mise en place d'un serveur FTP sous un système Linux. Le siège social étant extérieur aux locaux concernés, la connexion entre les terminaux sera assurée en extranet ou via Internet.
- Chaque utilisateur de l'entreprise dispose par défaut de privilèges d'administration système pouvant compromettre l'infrastructure numérique de BSD. Réduire la surface d'attaque d'une erreur humaine ou d'un piratage par une limitation des accès augmentera la résilience du parc informatique et la sécurité des données de l'entreprise
- Bien que cette gestion de droit utilisateur puisse s'effectuer poste par poste (Windows Workgroups), l'audit SSII conforte l'avis du service informatique sur l'implémentation **Erreur ! Source du renvoi introuvable.** Comme environnement centralisateur. Il permettra non seulement un contrôle des actions utilisateurs mais aussi des services à disposition (accès distant, partage d'espace disque, etc.)
- Des indicateurs organisationnels seront présentés pour apprécier la progression des étapes de réalisation du projet. Ils regrouperont la répartition des responsabilités, les temps de travail de chaque tâche, le découpage du projet, etc.
- Ce livrable répondra aux exigences d'information réclamée par le commanditaire. En tant qu'étude de faisabilité, y seront harmonisés des obligations envers le cahier des charges et les limitations de mise en œuvre (contrainte d'ordonnancement des tâches, prix)

VI. Conception

A. Méthode de pilotage

Contrairement aux précédents projets, où le cahier des charges était défini sans modification ultérieure, le projet EVOLUTION subira des conditions additionnelles de la part du commanditaire. Il convient donc d'adapter une autre forme de méthodologie de projet.

Parmi les gestions applicables, nous utiliserons une version adaptée de la méthode Agile. Rappelons que cette méthode découpe en mini-projets la trame principale de progression. Le directeur administratif posant des exigences supplémentaires comme des ajouts de services et un contrôle hebdomadaire de l'évolution du projet, nous distinguerons chaque semaine de la planification.



Semaine 0 : 27 au 30 août

Formation du groupe et premières concertations : prise de connaissance du projet et des échéances. Choix des premiers moyens de communications

Semaine 1 : 2 au 6 septembre

Remise du cahier des charges. Premières analyses des problématiques à résoudre. Découpage primitif du projet, mise en commun des connaissances (précédents livrables), confirmation de la formation du groupe, entretien avec le directeur administratif et financier pour synchroniser les attentes et les prévisions de l'équipe informatique, construction virtuelle de l'Active Directory

Semaine 2 : 9 au 13 septembre

Formulation problématique/besoins/enjeux. Planification. Début de maquettage Windows Server 2016 et installation des services ADDS, DC (DNS+GC), DNS, DFS. Définition des partitions NTDS/SYSVOL/DATA. Décision sur les spécificités physiques pour les serveurs.

Semaine 3 : 16 au 20 septembre

Choix du fournisseur et du modèle de serveur. Début de la rédaction de l'étude de faisabilité. Manipulation de la base de données et export Access

Semaine 4 : 23 au 27 septembre

Montage et configuration RDS. Script de connexion RDS. GPOs. Cliché instantané. Serveur d'impression.

Semaine 5 : 30 septembre au 4 octobre

Finition des configurations Microsoft.

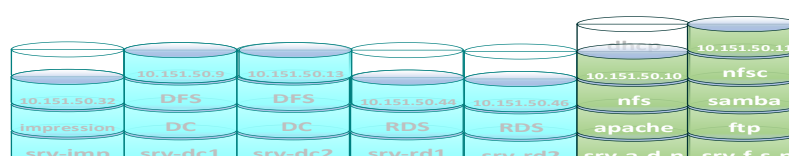
Montage serveurs Linux. Rôles SSH, NFS, Apache, ProFTPd, Samba. Script enregistrement personnalisé des connexions.

Semaine 6 : 7 au 11 octobre

Tri des notes et des captures d'écran. Rédaction du livrable

Semaine 7 : 14 au 18 octobre

Rédaction, mise en page et corrections



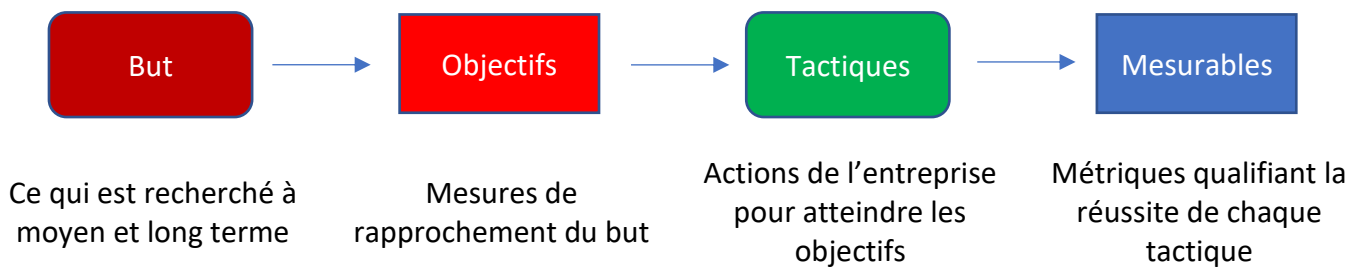
B. Stratégie informatique – Stratégie IT

Une stratégie d’entreprise vise à augmenter les revenus en jouant sur les délais et les perspectives de profit. Cependant, ce type de stratégie propose des objectifs vagues, basés sur les possibilités des divisions opérationnelles.

Ces approximations ne peuvent convenir à un environnement critique et transversale tel que le système d’information. Il importe donc d’établir une méthodologie propre à cette interface afin de situer, pour chaque besoin, les ressources à proposer. Ce soin particulier apporté à la stratégie IT est justifié par la capacité du service IT à distinguer les priorités fonctionnelles de tous les services (ressources, processus, outils).

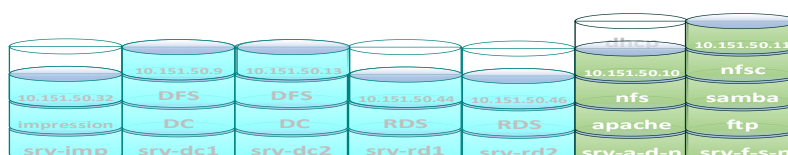
La méthode BOTM a été pensée pour répondre à cette exigence du « sur-mesure ». Elle repose sur la communication entre les cadres des différents services et l’équipe informatique, idéalement au plus tôt dans l’établissement des plans stratégiques. L’avantage de cette méthode est de désigner concrètement les rôles des acteurs. L’équipe IT définit la manière de procéder (ex : attribuer les ressources serveur) ; les cadres désignent l’objet de la stratégie (ex : exploiter une nouvelle application).

BOTM est l’acronyme de But – Objectifs – Tactiques – Mesurables et chaque lettre correspond à un paramètre dépendant du précédent.



Ci-dessous, la stratégie choisie par le SI pour mener à bien le projet Evolution.

But	Exploiter le système d’information de manière sécurisée et performante
Objectifs	Réduire le taux d’interruption de l’activité de l’entreprise Contrôler les actions/opérations des utilisateurs du parc informatique de BSD
Tactiques	Planifier et répartir des tâches du projet Choisir les machines serveurs adaptés Installer 5 à 6 Windows Serveur 2016 Ajouter leurs rôles (AD, DC, RDS, DFS, impression) Structurer les données utilisateurs (AD, BDD) Définir les groupes utilisateurs (sécurisation NTFS) Mettre en place les stratégies de groupe Installer 2 serveurs Linux et leurs rôles (Samba, Apache, etc.)



Mesures

Pour chaque tactique, une justification et un maquetage commenté guidera la lecture de ce livrable

C. Planification

Project Pro 2019 est un logiciel Microsoft regroupant des outils de gestion comme le calcul des salaires ou le taux de sollicitation des employés. Nous utiliserons uniquement l'interface Gantt améliorée introduisant, en plus du calendrier prévisionnel, le taux de progression et la quantification horaire de chaque tâche.

Ce diagramme de Gantt (avec le tableau RACI) marque la première étape de la stratégie IT de BSD. Malgré son rapport indirect aux objectifs initiaux de performance et de sécurité, la planification est un prérequis comportant l'ordonnement du projet en fonction des délais.

Considérons le postulat que tout projet complexe exige un objectif organisationnel. Sur cette base, l'usage de Project Pro se justifie pour documenter les charges de travail, constater l'état d'avancement, ajuster l'allocation des ressources en conséquence.

Enfin, le tableau RACI dresse la liste complète des parties prenantes et leur niveau d'implication dans le projet. Les collaborations et le responsable de chaque processus y sont mentionnés.

D. Plan de communication

L'ampleur du projet influence les risques de pertes d'informations, de manque de clarté dans les échanges ou encore des défauts dans la progression des travaux (estimations hasardeuses des temps de réalisation).

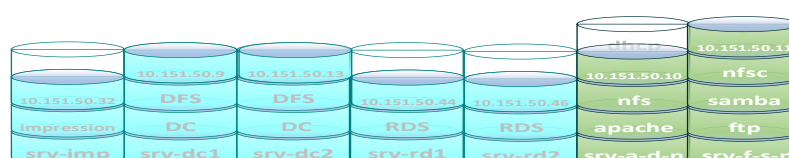
Ainsi les objectifs d'une communication : suivi de l'avancée des projets, relevé des difficultés jalonnant la réalisation, disponibilité des ressources de l'équipe, adaptation des échanges selon les destinataires.

Les moyens de communications se diversifient par des logiciels dédiés :

- La suite Microsoft Office pour la création des supports d'information (livrable sur Word, PowerPoint, schéma Visio, etc.)
- Microsoft Teams met à disposition un client de messagerie, ainsi que le travail collaboratif sur les logiciels de la suite Microsoft Office
- SharePoint offre le travail collaboratif sur des formats Microsoft spécifiques comme Project Pro et un espace de stockage.
- Trello pour composer collectivement la division des activités et leurs attributions
- Application Web vCenter pour hyperviseur ESXi permet au service informatique de mutualiser les opérations de test

En outre, les interactions les autres parties prenantes restent essentielles dans une optique de compréhension maximale :

- Réunion hebdomadaire avec le directeur administratif et financier sur l'avancée du projet
- Mise au point journalière au sein du service informatique sur les difficultés rencontrées et les objectifs du lendemain



VII. Windows Server 2016

A. Choix des serveurs

Les possibilités offertes par une centralisation des données et des services à l'aide de serveurs seront conditionnées par les caractéristiques de ces derniers. Aussi importe-t-il de choisir une machine capable de supporter la charge engrangée par le trafic des requêtes au sein du réseau de BSD.

Nous nous tournerons donc vers les solutions spécifiquement dédiées aux serveurs professionnels. Les Xeon Cascade Lake d'Intel et les EPYC d'AMD sont les dernières générations de processeurs serveur actuellement sur le marché. A la vue du rapport performance/prix entre les deux architectures et en fonction des offres constructeurs, nous avons choisis AMD et le constructeur Dell pour leurs prix attractifs, le configurateur en ligne et la qualité de son support technique dans le monde professionnel.

Nous considérerons une machine type pouvant remplir les limitations imposées par l'infrastructure à savoir :

Nombre de terminaux locaux considérés : 100

Nombre de serveurs : 7

Pour chaque serveur, nous obtenons

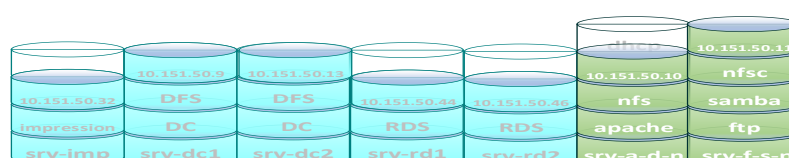
Stockage (dont 700 GB système)	5 GB par utilisateur (cahier des charges) 5*100=500 GB réservés users pour chaque serveur 500 + 700 = 1.2 To < 2 To pour un volume serveur 4 To pour RAID 1
Mémoire vive	64 Go RAM
Licence Windows Server 2016	Pour 5 serveurs
Processeur	Au moins 10 cœurs et 20 threads récent

Chaque composant de la configuration proposée est modifiable (sauf contraintes constructeur) dans le configurateur

B. Topologie réseau

Après avoir choisi les spécificités et la quantité des serveurs, nous localiserons leur emplacement au sein du réseau câblé.

Dans l'idéal, il importe de réduire les distances de transmission de données. A l'inverse, la disponibilité des données et des services implique un positionnement centralisé, parfois au détriment d'une possible proximité avec les postes clients. Afin de répondre à ces contraintes, nous nous baserons sur l'arrivée internet du fournisseur d'accès. Cette dernière n'étant pas modifiable dans l'immédiat, nos serveurs seront donc placés au plus proche de ce nœud stratégique.



Dans ce schéma, nous avons un premier aperçu (schéma Visio) des différents rôles que joueront ces nouveaux appareils. Afin d'assurer que tous les PC raccordés soient reconnus comme membres du domaine BSD.ADDS. Les contrôleurs dudit domaine (voir chapitre « Rôle ADDS et DC ») sont ici l'interface entre les routeurs et le reste de l'architecture.

Tous les autres serveurs membres sont conséquemment disposés après les DC et la première batterie de commutateurs (SWA et SWB). Ce positionnement offre une tolérance de panne nécessaire en cas de dysfonctionnement sur un switch, le câblage ou une carte réseau d'un serveur. Chacun de ses serveurs (RD et IMP) est relié aux deux switches, eux-mêmes placés comme carrefours liant toute la structure.

C. Système d'exploitation et licence

Conjointement à l'achat matériel, le choix du système d'exploitation s'appuie sur des critères similaires comme une architecture récente et dimensionnée pour la gestion d'une centaine de PC sous Windows 10 Pro.

L'exigence de BSD concernant l'adoption de Windows Server 2016 Standard s'explique en 3 points :

- Support technique étendu jusqu'en 2027
- Pas de limite de connexions client et suffisante en RDS
- Maturité de l'interface, peu de recul sur la version 2019

L'installation de Windows Server nécessite l'obtention et l'enregistrement de licences. Ces dernières assurent l'authenticité de l'OS ou du service associé et se présente ici dans 4 formats :

- Les licences d'activation des clients Windows (déjà enregistrées)
- Les licences CAL (Client Access License) autorisant la connexion des clients aux serveurs
- Les licences CAL RDS spécifiques au service Bureau à Distance
- Les licences d'activation des serveurs

Actuellement, les licences serveurs imposent des limitations sur le nombre de processeur et de leurs cœurs physiques. Chacun de nos serveurs Windows étant équipés d'un processeur 24 cœurs, ce calcul s'applique :

- 1 licence WS 2016 16 cœurs + 4 licences additionnelles 2 cœurs ; ceci pour chaque serveur (5 au total)

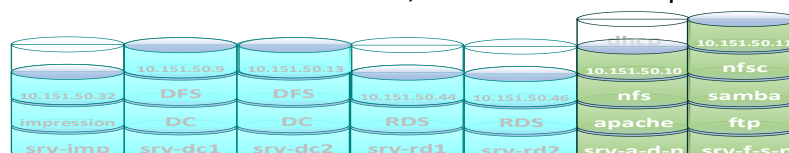
Concernant les CAL, étant donné que la majorité des salariés sont postés (non itinérants), les CAL périphériques (attribués aux terminaux) sont à préférer au CAL utilisateurs plus coûteuses en termes de prix et de sécurité (plusieurs terminaux par utilisateurs)

Au contraire, les CAL RDS seront affiliées aux utilisateurs car les sessions Bureau à Distance sont nettement plus restreintes par les stratégies de groupe prévues (notamment les interdictions d'accès à une session locale ou aux outils de configuration du serveur)

D. Rôle ADDS et DC

Active Directory est, à la fois, l'appellation Microsoft de l'annuaire et du domaine dans un réseau Windows.

Cet annuaire est un système de stockage centralisant des données dans un objectif de durabilité, tout au long de l'activité réseau au sein du domaine. En effet, ces données n'ont pas vocation à subir d'importantes



et/ou fréquentes modifications. Cette stabilité autorise une structure hiérarchique (fixée par la norme LDAP) dans laquelle des objets s'intégreront. Dans notre étude, ces objets (ordinateurs, utilisateurs, imprimantes, unités organisationnelles et autres conteneurs) seront répartis dans l'arborescence du domaine nommé BDS.ADDS.

La notion de domaine symbolise l'espace dans lequel évolue les objets du réseau Windows. Dans cet espace, l'annuaire lie l'emplacement de ces objets à leur nom unique. Ainsi, nul besoin d'inscrire le chemin complet d'une ressource pour y accéder. Ce confort de navigation s'organise autour d'un contrôleur de domaine (DC=Domain Controller). C'est à ce serveur Windows que revient la charge de gérer toutes les requêtes concernant son domaine, comme identifier les objets AD, mais également authentifier les utilisateurs ou appliquer les stratégies de groupe (source : ITconnect.fr).

A titre informatif, les noms d'utilisateurs pourront s'écrire ainsi :

testeur@bsd.adds ou bsd.adds\testeur

ID du compte séparateur de champs domaine

Autre visuel, les chemins réseaux acceptent également plusieurs syntaxes

\\nomduPC\... \\IPduPC\...

Par ces accès multiples, nous constatons la prise en charge des requêtes opérée par le DC. La conversion entre adresse IP et le nom du PC améliore l'ergonomie logicielle (résolution DNS). Même remarque pour l'authentification des comptes. Grâce à la présence de l'annuaire, l'emplacement exact de l'utilisateur dans l'arborescence bsd.adds n'est pas nécessaire pour ouvrir une session (le salarié n'écrit que son nom).

Une opération de support technique courante consiste à réinitialiser le mot de passe d'un compte. Le DC concentre cette manipulation pour tous les utilisateurs intégrés au domaine bsd.adds. Le service informatique n'a ainsi besoin que d'un accès au DC pour enclencher la procédure, le poste utilisateur pouvant se situer dans un autre bâtiment. Conséquentement, une réduction des déplacements physiques du SI augmente la disponibilité de l'appareil de production.

E. Rôle DFS - Système de fichiers distribués

Dans un environnement Microsoft Windows, DFS (Distributed Files System) est un ensemble de services pour clients et serveurs permettant d'organiser des partages de fichiers.

Pour ce maquetage, il est installé avec

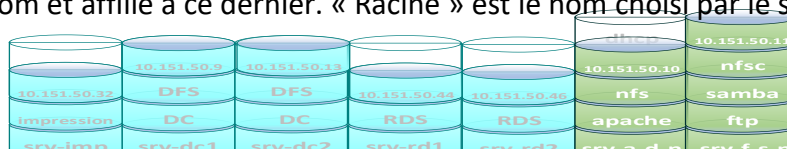
- L'espace de nom DFS, qui offre une visibilité des partages sur le réseau
- La réplication DFS, créant une redondance des fichiers

Les deux services étant déployés dans le domaine bsd.adds, le chemin de partage se présentera de la façon suivante.

\\bsd.adds\racine\exemple\123

Espace de nom DFS Chemin du fichier

Cette requête concentre tous les accès aux PC concernés, c'est-à-dire membres du domaine, disposant du service d'espace de nom et affilié à ce dernier. « Racine » est le nom choisi par le service informatique.



Windows Server déterminera, pour chaque interaction dans cet espace, le chemin optimal en fonction de l'état des serveurs et du trafic réseau.

Ces rôles sont installés sur les contrôleurs de domaines dans un souci de répartition des charges. En effet, DFS nécessite moins de ressources, comparé aux services Bureaux à distance et Impression.

Au vu de ces possibilités, le système de fichiers distribués correspond aux exigences fonctionnelles et sécuritaires de BSD concernant la disponibilité des données et la tolérance de panne.

F. Rôle RDS - Services Bureau à distance

Les services de bureau à distance sont un composant Windows permettant à un utilisateur de prendre le contrôle d'un ordinateur via un accès réseau. Il utilise le protocole TCP/IP dans la version actuelle.

BSD exploite un programme collaboratif entre les deux secteurs de production. Afin d'exploiter pleinement ce programme, l'entreprise mettra à disposition deux serveurs RDS pour assurer des performances satisfaisantes. Ce supplément vise également à prévenir les défaillances d'une machine source unique.

La mise en place des serveurs RDS est disponible en annexe

G. Rôle DHCP

Ce rôle permet l'attribution automatique d'adresses IP aux machines clientes de notre domaine avec un bail réglable et les informations nécessaires comme le serveur DNS et la passerelle réseau. Le réglage machine sera DHCP (Dynamic Host Configuration Protocole) pour l'attribution d'adresse (voir Annexes).

Les IP serveurs et imprimantes ne seront pas allouées dynamiquement pour la stabilité requise par ce type d'équipement.

L'hyperviseur ESXi ne permettant pas l'installation du DHCP (risque de perturbation au sein de la plateforme), le maquettage de cette partie sera effectué sur une machine virtuelle isolée Windows Server.

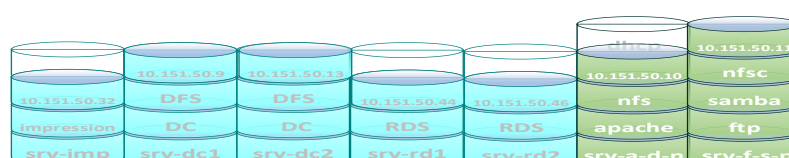
H. Permission NTFS

Les informations circulant au sein du réseau BSD se destinent rarement à tous les employés. Sans aller jusqu'à gérer tous les échanges de façon individuelle (ex : courriels), le système de fichiers NTFS accorde, à des groupes dits « de sécurité », des autorisations d'accès dans n'importe quel dossier sous Windows.

Il est alors possible par ce système de filtrer les personnes et les actions sur les données partagées. Pour clarifier la répartition des permissions, il importe donc de les organiser. En annexe, le tableau des permissions NTFS représente les actions disponibles des groupes de sécurité sur des dossiers partagés.

Rappelons que l'intérêt de cette délimitation renforce la sécurité (erreur ou intrusion) et la confidentialité des données.

Le choix de ces entités fit l'objet d'une réflexion collégiale du service informatique (le 6 et 9 septembre). Le nommage et la quantité de ces entités doivent suivre les exigences des chartes en termes de contrôle d'accès, d'efficacité et de compréhension.



I. Stratégies de groupe

Un utilisateur peut causer des pannes, volontairement ou non, sur un ordinateur. Installation de pilotes incompatibles, téléchargement de fichiers infectés, suppression inopinée de données... Autant de situations risquant de compromettre, non seulement le fonctionnement du poste informatique, mais parfois l'intégralité de son réseau local.

Pour se prémunir de tels accidents, le contrôle de l'interface utilisateur/PC est indispensable. Certes, une sensibilisation des usagers aux bonnes pratiques numériques constitue un prérequis. Mais en complément de cette mesure, l'administration centralisée des objets AD offre des possibilités de paramétrage en ce sens.

La gestion des environnements client dans un domaine Microsoft est appelé stratégie de groupe ou GPO.

Les GPO représentent un vaste catalogue de réglages prédéfinis (ex : supprimer clic droit, masquer les lecteurs, etc.) et configurables (ex : déployer des raccourcis ou des programmes). Un autre exemple représentatif est l'accès au panneau de configuration. Les personnes autres que le SI n'ont pas vocation à modifier des paramètres comme l'adresse IP ou le nom de la machine.

Influençant ainsi les sessions Windows des employés, les objectifs sécuritaires et fonctionnels rendent favorable l'instauration des GPO.

J. Serveur d'impression

Sans serveur, les imprimantes sont partagées par un appareil client dédié ou par leur logiciel intégré. Ces solutions, à l'échelle de l'entreprise BSD, ne sont viable qu'avec une faible fréquence d'impression.

Un encombrement à ce niveau rend l'imprimante lente (voire inopérante) lors de son tirage papier ou de la modification de la file d'attente (suppression, pause d'une requête).

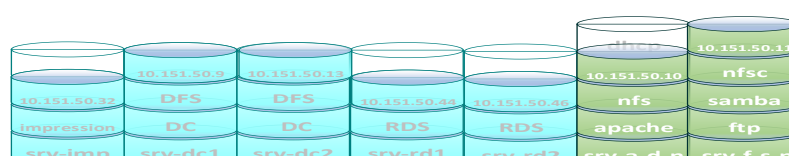
Bien meilleurs que les performances des machines client, notre serveur sera plus adapté à l'exploitation des imprimantes réseau. Son installation comblera, en partie, les interruptions de l'appareil de production.

VIII. Serveurs Debian

Debian 9.6 n'est pas le système d'exploitation le plus récent de cette distribution. Néanmoins, le SAV manipule un logiciel métier dépendant de cette version. Cette situation doit faire l'objet d'un examen car cet OS bénéficie de correctifs de sécurité jusqu'en juin 2022. Il s'agira de comparer les solutions proposées par le fournisseur actuel du logiciel métier, ou, à défaut, d'autres chemins de réflexions.

L'installation de l'OS sur les deux serveurs concernés fut jugée acceptable à court terme par le SI pour les points suivants :

- L'infrastructure réseau de BSD est majoritairement sous environnement Windows
- Les rôles Linux (proFTPd, Apache ...) ont des équivalents installables sur Windows Server
- Interdépendance faible concernant l'AD (pas de rôle DC ni serveur membre de BSD.ADDS)
- Seul le personnel du SI et du SAV seront fortement touchés par une réinstallation des serveurs Linux (5 personnes dont 3 professionnels IT)



A. SSH

Dans notre étude, SSH sera l'un des rôles à installer sur tous les serveurs Debian. Cette propension s'explique par la criticité de son usage.

En effet, SSH crée des connexions chiffrées entre deux terminaux. Basé sur la cryptographie asymétrique (clés privée et publique), ce programme empêche les interceptions lors d'une connexion distante et authentifie le serveur pendant une requête de communication.

Les administrateurs peuvent ainsi modifier à distance des fichiers de configurations en super utilisateur de manière sécurisée. Le protocole SSH et le programme associé s'insèrent donc dans la stratégie IT de BSD (objectif de sécurité)

B. Webmin

Webmin est une interface d'administration pour serveur Unix/Linux. Par défaut, elle s'utilise via un navigateur web à cette adresse : <https://ipduserveur:10000>. S'ensuivra une demande de connexion en super utilisateur (local) du terminal ciblé.

La faille de sécurité abordée en introduction fut corrigée sur les dernières versions de l'interface.

Configurer un serveur Debian grâce à des menus et des zones de saisie facilite le travail d'un administrateur, lui épargnant la manipulation en ligne de commande.

Cette interface centralise les interactions possibles avec les fichiers de configuration du PC. Citons notamment la gestion des utilisateurs et du planificateur de tâche CRON qui sont installés d'origine. Les rôles ajoutés comme Samba ou Apache (que nous verrons plus loin) sont également configurables sans préciser manuellement le chemin des fichiers à modifier.

Cette ergonomie augmente la réactivité et l'exactitude des techniciens informatiques dans leurs opérations administratives courantes.

C. Serveurs de fichiers

Un serveur de fichiers permet le partage de données sur un réseau.

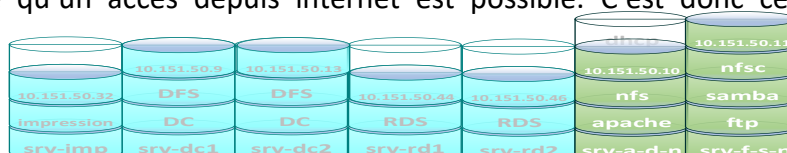
3 logiciels délivrant cette fonctionnalité seront intégrés sur les serveurs Linux de BSD. Leurs distinctions offrent différents niveaux de cloisonnement. Ainsi, selon l'étendue de partage voulue, les protocoles de communication joueront le rôle de filtres dans la couche application du modèle OSI.

Par exemple, une intrusion distance via le protocole FTP ne peut atteindre directement le réseau local de l'infrastructure. Autre cas de figure, une perturbation logicielle des échanges Samba ne peut affecter directement les liaisons NFS (alors même que les 2 protocoles cohabitent dans le même réseau local).

Cette granularité du partage limite les interactions utilisateurs sur les fichiers du réseau BSD. Les serveurs de fichiers Linux, par leur diversité de fonctionnement, s'insère nécessairement dans la stratégie IT et son objectif de contrôle de l'infrastructure.

❖ ProFTPD

Comme son nom l'indique, ProFTPd est un serveur de fichier exploitant le protocole FTP. Ce protocole est routable, c'est-à-dire qu'un accès depuis internet est possible. C'est donc ce service qui assurera la



connexion avec le siège social de BSD. Cependant, les tests présentés dans ce livrable n'affectent que le réseau local. Par conséquent, la sécurisation des échanges FTP avec l'extérieur ne sera pas décrite (changement de ports, chiffage de transmission) et fera l'objet d'une étude séparée.

La sécurité et l'anonymisation des consultations FTP au sein du réseau local passera par la configuration des login Unix (mot de passe), les permissions de partage des données (écriture, lecture, etc.) et de la connexion anonyme (sans authentification).

❖ SAMBA

Samba est un logiciel implémentant en environnement Linux le protocole réseau SMB. L'exploitation de ce protocole permet de déclarer notre machine Debian comme serveur de fichiers.

SMB fait également partie des ressources utilisées par le domaine AD. Ce point commun entre les univers Microsoft et Linux place Samba comme un acteur évident pour les partages inter plateformes.

Le SI doit atteindre certains fichiers sur ce serveur Debian depuis les trois OS du parc informatique de BSD (Microsoft Windows 10 Pro, Microsoft Windows Server 2016 et Debian 9.6)

La création d'un utilisateur Samba (avec son mot de passe) conditionne l'accès à ce type de partage. Nous retrouvons ainsi, au travers des fonctionnalités de Samba, le but de la stratégie IT de BSD.

❖ NFS

Contrairement à Samba, qui authentifie les « users », NFS autorise un partage grâce aux informations du serveur (nom ou IP de l'hôte). Vu que plusieurs personnes connaîtront les logs du serveur, NFS sera choisi pour le partage de ressources communes.

Autre différence avec Samba, NFS n'est pas compatible nativement avec Windows. En l'état, ce protocole concerne uniquement l'environnement Linux, donc le SI et le SAV. Dans le cas où le logiciel du SAV (voir début du chapitre VIII) profiterait d'une machine puissante, un partage NFS du programme se justifie.

Au moment de choisir comment partager des données, les administrateurs système devront identifier ressources communes et ressources individuelles. Cette analyse associera les serveurs de fichiers aux partages correspondants.

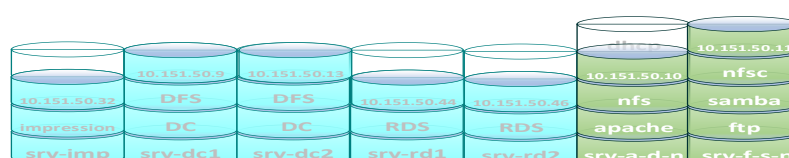
Sur le site BSD, l'exploitation de NFS est exclusive aux machines sous Debian, ce qui limite logiquement son accès. Cette division dans les partages de fichiers pourra combler des besoins spécifiques à cet environnement.

❖ Apache

Apache est un serveur web. Il permet l'accès en ligne (ici en intranet) de pages html.

Sa mise en place sur une machine Linux se justifie par les besoins en ressources. Les serveurs Windows remplissant déjà des rôles considérables, ne pas les surcharger s'avère important dans une optique de disponibilité des données.

De plus, l'affichage des sites web est dépendant d'un navigateur web. Toutes les machines du parc informatique disposent de ce type de logiciel (Windows comme Linux). La consultation est accessible sur n'importe quel poste. La disponibilité des données est donc renforcée par la vitesse du serveur et l'accessibilité du service.





XI. Charte graphique

Une charte graphique est le support fondamental d'une communication externe et interne. Elle représente graphiquement les valeurs et l'univers de l'entreprise.

Une identité visuelle est bâtie grâce à son logo que l'on retrouve sur tous les supports de communication de l'entreprise.

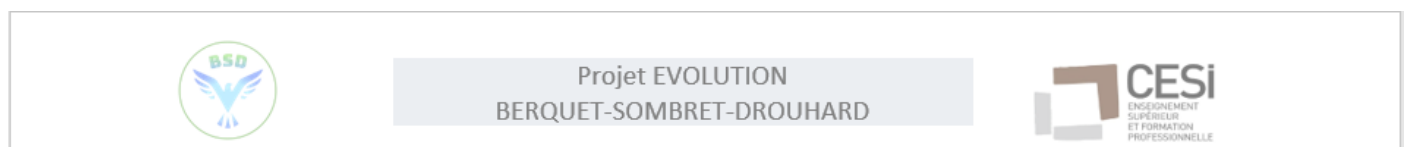
Ce logo doit refléter l'image de l'entreprise.



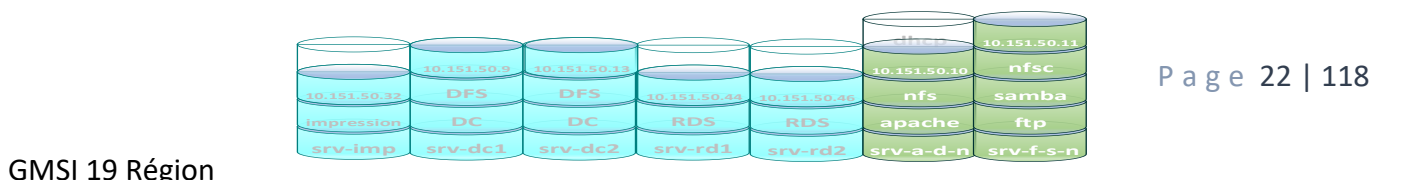
	Type de police	Taille
Titre 1	Calibri light gras	18
Titre 2	Calibri light gras	16
Titre 3	Calibri light gras	14
Texte	Calibri en justifier	12

L'en-tête et le pied de page sont utilisés sur toutes les pages du document sauf sur la page de garde.

L'en-tête est composé du logo BSD, du nom du projet avec les noms des auteurs du livrable et du logo du CESI.



Le pied de page est quant à lui composé du nom de la promo GMSI 19 Région, les piles des serveurs et du numéro de page.



XII. Webographie

Introduction

<https://www.zdnet.fr/actualites/les-pirates-informatiques-s-attaquent-aux-serveurs-webmin-pulse-secure-et-fortinet-vpn-39889509.htm>

<https://www.undernews.fr/reseau-securite/sauvegardes-stockage-donnees/infographie-les-chiffres-de-la-perde-de-donnees.html>

Cadrage

<http://www.ih2ef.education.fr/conseils/commande/operations/formuler-une-problematique/>

Conception

<https://www.planzone.fr/blog/methodologies-gestion-projet>

<https://www.manager-go.com/gestion-de-projet/dossiers-methodes/matrice-raci>

<https://www.linkedin.com/learning/implementer-sa-strategie-it/bienvenue-dans-implementer-sa-strategie-it>

Serveurs Windows

<https://www.dell.com/learn/fr/fr/frbsdt1/sb360/what-type-of-server-do-i-need>

https://www.dell.com/fr-fr/work/shop/cty/pdp/spd/poweredge-r6415/emea_r6415_vi_vp

<https://www.anandtech.com/show/11544/intel-skylake-ep-vs-amd-epyc-7000-cpu-battle-of-the-decade>

Licences :

<https://docs.microsoft.com/fr-fr/windows-server/remote/remote-desktop-services/rds-client-access-license>

<https://social.technet.microsoft.com/Forums/fr-FR/d5a192c3-e695-48f0-ba07-9c821efe90fd/cal?forum=windowsserver2008fr>

<https://adeo-informatique.fr/bien-choisir-ses-cal-windows-serveur-2012/>

https://www.youtube.com/watch?time_continue=57&v=XGI69EwIQfE

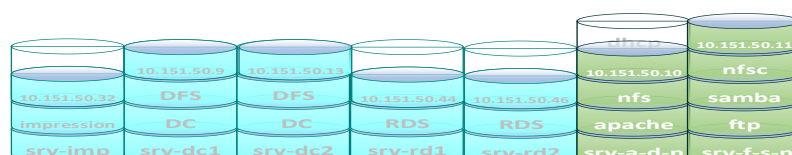
Permissions NTFS

<http://info-technologie-cours.blogspot.com/2013/02/permissions-et-droits.html>

Active Directory :

<https://www.fr.paessler.com/it-explained/active-directory>

<http://www.tontonfred.net/blog/?p=95>



<https://forsenergy.com/fr-fr/dsadmin/html/dce5a1c3-3e98-46ab-ae10-1304712b0c85.htm>

<https://www.it-connect.fr/chapitres/a-la-decouverte-du-catalogue-global/>

<https://docs.microsoft.com/en-us/windows/win32/ad/global-catalog>

<https://openclassrooms.com/fr/courses/2257706-presentation-du-concept-dannuaire-ldap/2260186-differences-avec-une-base-de-donnees>

https://fr.wikipedia.org/wiki/Annuaire#En_informatique

<https://medium.com/@yoursproductly/understanding-active-directory-4e7508372b80>

<https://blog.varonis.fr/controleur-de-domaine/>

<https://a201165.wordpress.com/2013/05/21/active-directory-advantages-and-disadvantages/>

<https://www.cubittech.com/blog/2015/03/what-are-the-benefits-of-a-windows-domain/>

RDS

<https://docs.microsoft.com/fr-fr/learn/modules/create-windows-virtual-machine-in-azure/5-exercise-connect-to-a-windows-vm-using-rdp>

<https://www.youtube.com/watch?v=08m42Bqerbo&list=PLJA4l0PkoJnGLVj0GFRqLM5t1cBErD5DF&index=1>

<http://www.metsys.fr/blog/securisation-des-serveurs-remote-desktop-servers-windows-2008-r2/>

PowerShell

<https://openclassrooms.com/fr/courses/3664366-creez-votre-premier-script-avec-powershell>

<https://www.linkedin.com/learning/l-essentiel-de-powershell-5/installer-windows-powershell>

<https://www.supinfo.com/articles/single/4015-script-powershell-creation-ous-importation-comptes-creation-groupes>

<https://whatis.techtarget.com/fr/definition/cmdlet>

Stratégies de groupe

<https://www.supinfo.com/articles/single/984-gpo-mappage-lecteur-reseau-avec-windows-serveur-2012>

<http://www.tontonfred.net/blog/?p=599>

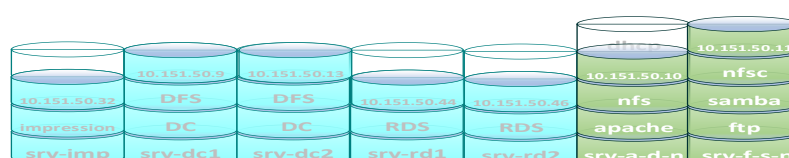
<https://akril.net/comment-masquer-ou-restreindre-laces-a-une-partition-sous-windows/>

<https://www.top-password.com/blog/disable-run-command-in-windows-10/>

<https://social.technet.microsoft.com/Forums/fr-FR/294f4142-cdee-4257-bba8-6a70d998e47e/comment-interdire-louverture-dune-session-windows-en-environnement-multidomaines-active-directory?forum=windowsserver2008fr>

<https://activedirectorypro.com/gpresult-tool/>

Imprimantes





<https://www.youtube.com/watch?v=2zsEa0hV9a4>

Logiciel

<https://www.microsoft.com/en-us/download/details.aspx?id=13380>

Base de données relationnelle

<https://www.youtube.com/watch?v=VFHVNA8xgK0>

<https://www.briandunning.com/sample-data/>

Rédaction livrable

<https://www.scribbr.fr/France/avant-propos-France/>

Serveur Debian :

<https://wiki.debian.org/fr/LTS>

<http://www.tontonfred.net/blog/?p=2790>

<http://www.tontonfred.net/blog/?p=1364>

<https://wodric.com/commande-grep/>

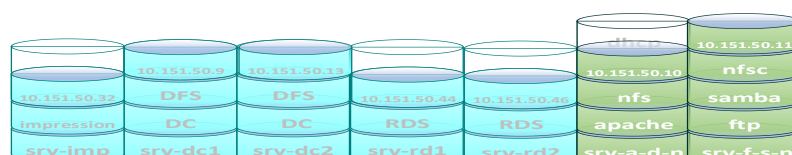
<http://www.linux-France.org/~ohoarau/article/ohoarau/cours-unix-10.htm>

https://doc.ubuntu-fr.org/samba_smb.conf

<http://www.tontonfred.net/blog/?p=1401>

<http://techno.firenode.net/article.sh?id=d201608040826134297>

<https://forum.ubuntu-fr.org/viewtopic.php?id=192890>



XIII. Annexes

A. Planification

Plusieurs outils ont été utilisés afin de planifier l'organisation du dossier d'étude

❖ Le tableau RACI

Il définit les différents rôles et responsabilités de chacun.

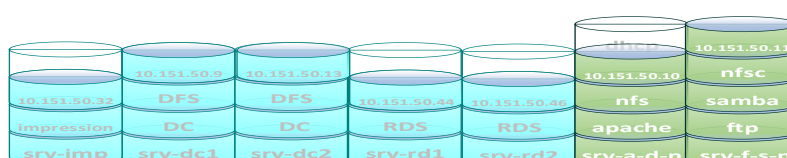
Définissant le niveau d'information, consultation, d'approbation et de réalisation de chacun.

qui \ quoi	BERQUET William	SOMBRET Sébastien	DROUHARD Léonel	Utilisateurs	Direction Générale	Administration
Cadrage	C	R	C		A	C
Choix méthode de pilotage	C	AR	C		I	I
Planification	C	R	AR	I	C	C
Choix des serveurs	R	AR	R		I	C
Maquettage des rôles Windows	AR	C	R		I	I
Structure Active Directory	R	R	AR		I	C
Base de données	C	C	AR		I	C
Stratégie de groupe	AR	R	R	I	I	C
Permissions	R	AR	R	I	I	C
Maquettage des rôles Linux	AR	C	R		I	I

Réalisation	R
Approbation	A
Consultation	C
Information	I

❖ Trello

Logiciel de gestion de projet collaboratif. Il permet d'ébaucher collectivement les premiers découpages du projet et de la répartition des tâches. Sa maniabilité en ligne et son intégration dans plusieurs outils fut appréciée (Teams et application Android notamment).



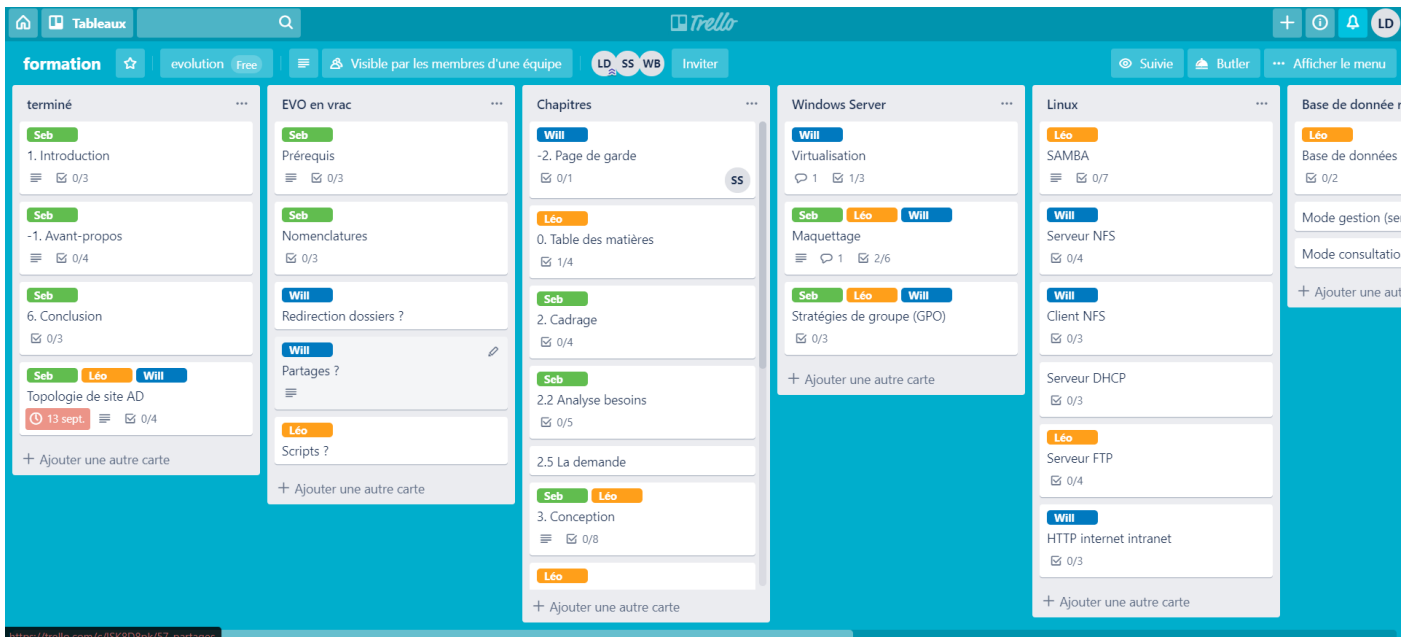


Figure XIII-1 : Découpage projet via Trello

❖ Microsoft Project Pro 2019

Logiciel permettant la planification des tâches et la visualisation du projet final

Suivi et validation des impératifs de temps

Le pourcentage de progression des tâches les limites de temps si nécessaire

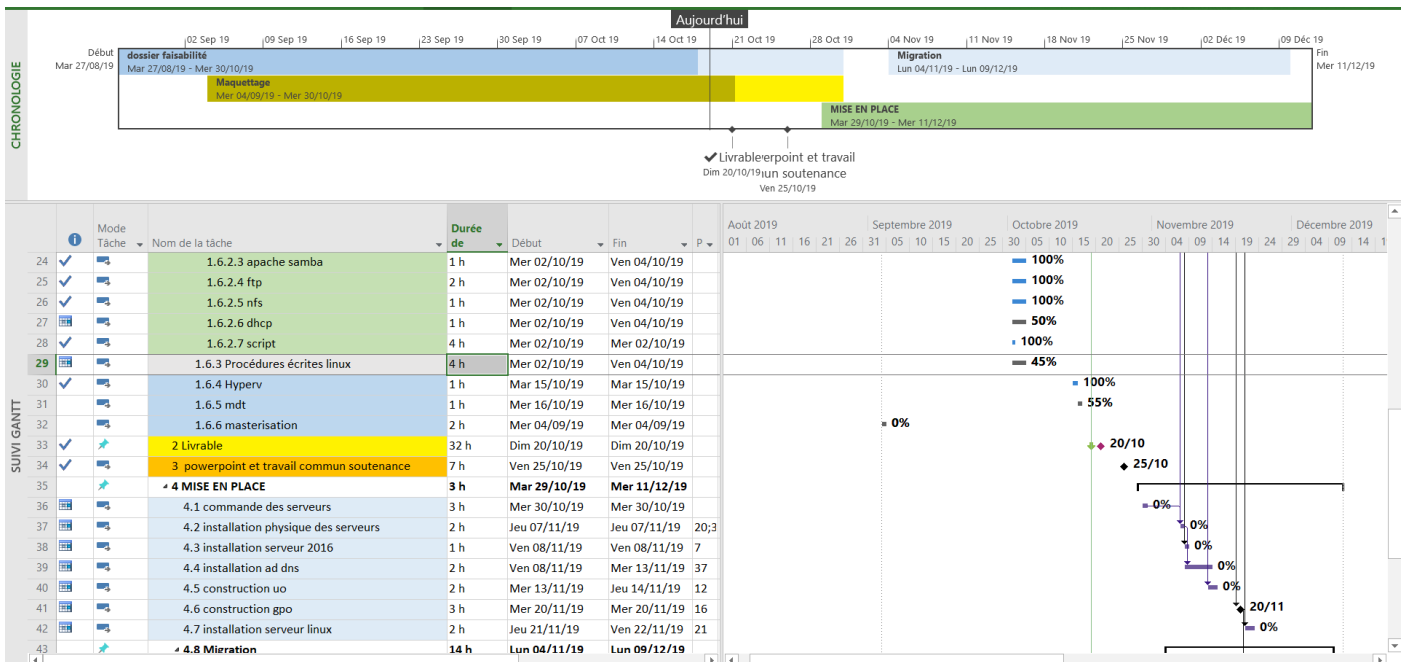
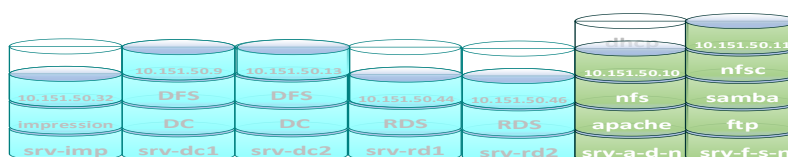


Figure XIII-2 : Planification Gantt maquettage



La chronologie et la planification du projet après acceptation du directeur administratif et financier

- Achats des serveurs
- Installation
- Migration
- Déploiement par service de la nouvelle image Windows si nécessaire

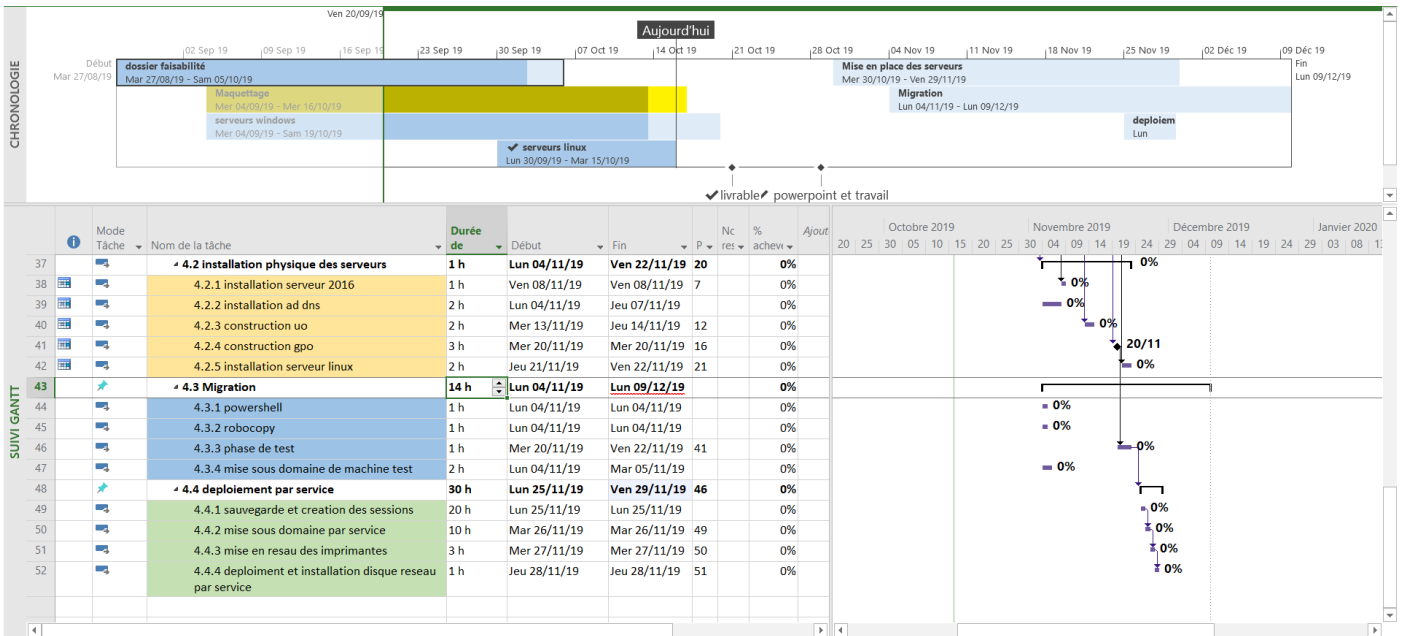


Figure XIII-3 : Planification Gantt déploiement

Le calendrier prévisionnel

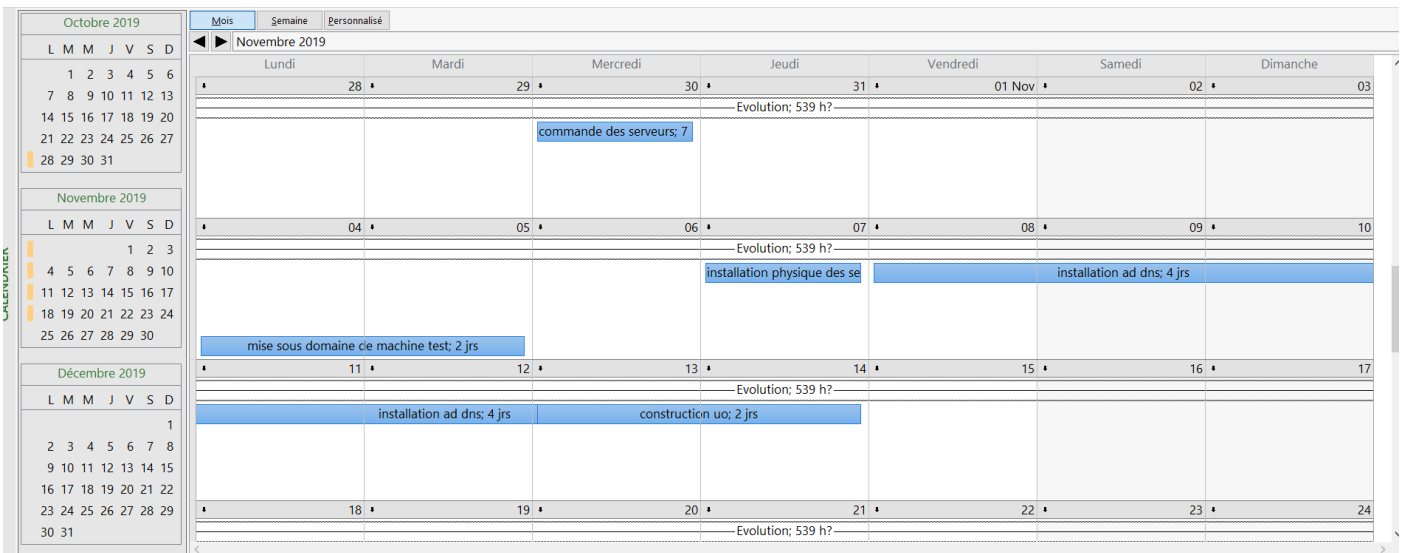
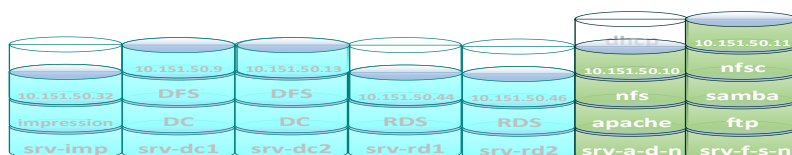


Figure XIII-4 : Planification calendrier



Ci-dessous, un autre aspect graphique du découpe projet, fourni par Project Pro

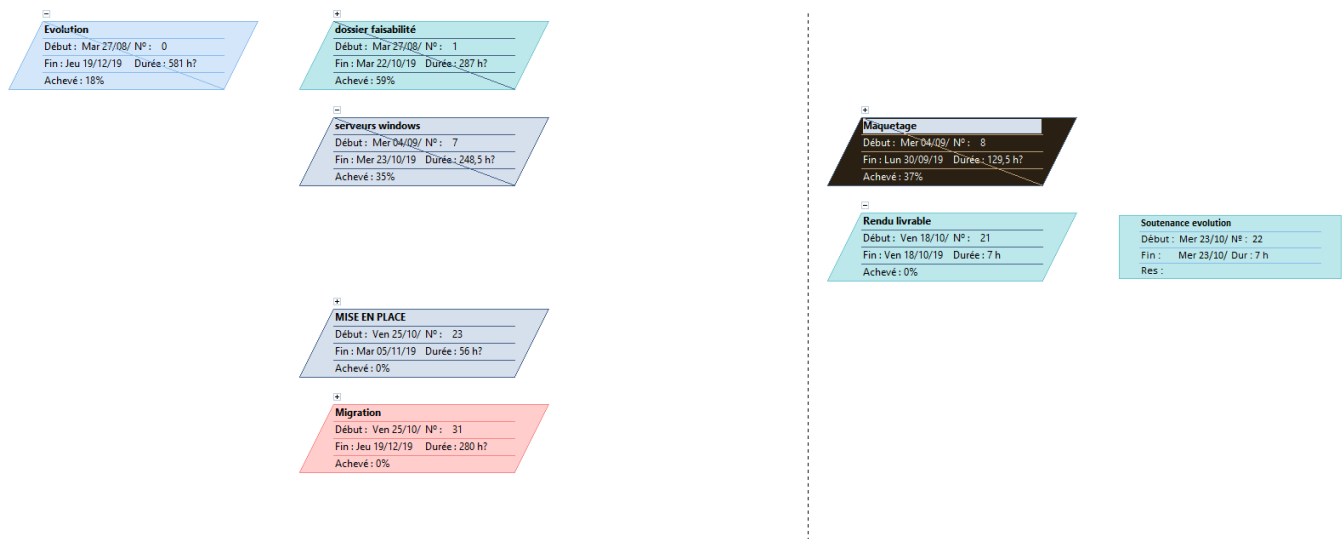
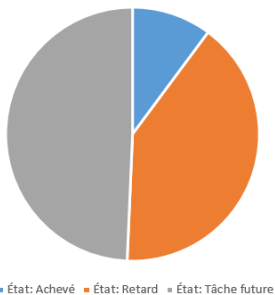


Figure XIII-5 : Planification tâches en cours

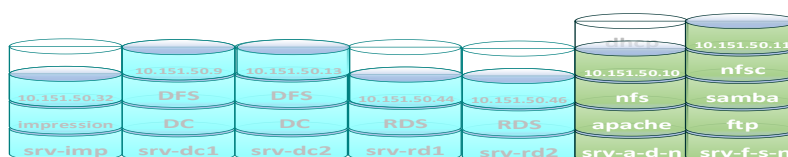
TÂCHES EN RETARD



Tâches en retard par rapport à la date d'état. Une tâche est en retard si sa date de fin est échue ou si elle ne progresse pas comme prévu.

Nom	Début	Fin	% achevé	Travail restant	Noms ressources
plan	Mer 04/09/19	Jeu 05/09/19	90%	0,7 h	sebastien sombret
menu	Jeu 05/09/19	Ven 06/09/19	60%	2,8 h	leonel drouhard
nom et logo charte graphique	Jeu 05/09/19	Jeu 05/09/19	75%	1,75 h	william berquet
choix des serveurs windows	Mar 27/08/19	Mer 11/09/19	60%	0 h	
presentation	Mer 04/09/19	Jeu 05/09/19	14%	0 h	
installation AD	Mar 10/09/19	Mar 10/09/19	80%	4,2 h	leonel drouhard;sebastien sombret;william berquet
RDS	Ven 20/09/19	Ven 20/09/19	0%	0 h	
DFS répliqué	Ven 13/09/19	Ven 13/09/19	75%	0 h	
gpo multiples	Lun 16/09/19	Lun 16/09/19	60%	1,1 h	william berquet
script powershell plusieurs	Jeu 19/09/19	Jeu 19/09/19	80%	1,4 h	leonel drouhard
base de donnée sql	Lun 16/09/19	Lun 16/09/19	5%	0 h	
<Nouvelle tâche>	Mer 04/09/19	Mer 04/09/19	0%	0 h	
installation 2016	Lun 23/09/19	Lun 23/09/19	50%	0 h	
installation AD + documentation	Lun 23/09/19	Lun 23/09/19	45%	0 h	
deuxieme serveurs AD + documentation	Lun 23/09/19	Lun 23/09/19	35%	0 h	
structure AD +	Lun 23/09/19	Lun 23/09/19	50%	0 h	

Figure XIII-6 : Planification tâche en retard



B. Installation serveurs

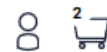
❖ Licences Microsoft Windows

Figure XIII-7 : Capture d'écran prix licences

Panier | lizengo France

<https://www.lizengo.fr/checkout/cart>

Conseils gratuits au : 0800 90 53 44



VOTRE PANIER



Windows Server 2016 RDS - 10 User CALs

10 ▾

6 799,90 €

TTC

Prix unitaire **679,99 €**



Windows Server 2016 - 10 Device CALs

10 ▾

2 699,90 €

TTC

Prix unitaire **269,99 €**

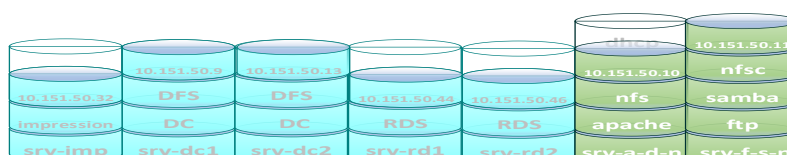
❖ Devis Serveurs

Ce modèle de serveur lame est compatible avec le format des armoires de brassage.

Ce devis est spécifique pour chaque contrôleur de domaine. Les autres serveurs n'ont besoin que d'une carte réseau (2 ports) pour remplir les conditions de connexion de la topologie réseau BSD.

Dans le même esprit, les serveurs Debian, moins consommateurs de ressources, pourront subir des ajustements physiques selon le budget alloué.

Le configurateur reste pratique pour ce genre de modifications.



PowerEdge R6415 - Full Configuration Résumé

Prix 11 558,62 €

[Ajouter au panier](#)

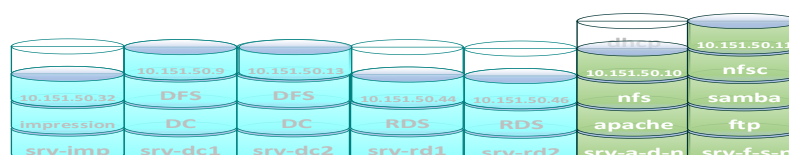
Hors TVA, Éco-contribution incluse, livraison gratuite
[Expédition et livraison](#)

Expédition en 12 à 14 jours ouvrés



Other options

Option	Sélection	Référence SKU/code produit	Quantité
Basique	PowerEdge R6415 Server	[210-ANJO] / R6415	1
Chassis Configuration	2.5" Chassis with up to 8 Hot Plug Hard Drives	[321-BDBB] / 5107995	1
Module TPM (Trusted Platform Module)	No Trusted Platform Module	[461-AADZ] / NTPM	1
Processeur	AMD EPYC™ 7401P 2.0GHz/2.8GHz, 24C/48T, 64M Cache (155W/170W) DDR4-2400/2666	[338-BNCT] / 5108563	1
Configuration thermique du processeur	Standard Heatsink	[412-AALH] / 5108352	1
Type de configuration de la mémoire	Performance Optimized	[370-AAIP] / PEOPT	1
Memory DIMM Type and Speed	2666MT/s RDIMMs	[370-ADNU] / 5099278	1
Mémoire	32GB RDIMM, 2666MT/s, Dual Rank	[370-ADNF] / 5098890	2
Système d'exploitation	Windows Server® 2016,Standard,16CORE,Factory Inst,No MED,NO CAL	[634-BILL] / WS2FI	1
Virtualisation activée	None		
Secondary OS	None		
OS Media Kits	Windows Server® 2016,Standard,16CORE, Media Kit	[634-BILD] / WS20S	1
Module SD interne	None		
Cartes de stockage optimisées pour le démarrage	None		
Licences	Windows Server® 2016,Standard Ed, Add License,2CORE,NO MEDIA/KEY	[634-BILK] / MS202	4
RAID Configuration	C3, RAID 1 for 2 HDDs or SSDs (Matching Type/Speed/Capacity)	[780-BCDN] / 5098871	1
RAID Controller	PERC H330 RAID Controller, Minicard	[405-AAEF] / H330	1
Disque dur	1.92TB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD, 3504 TBW	[400-AXSD] / GGMU1EX	2
BIOS and Advanced System Configuration Settings	Performance BIOS Setting	[384-BBBL] / HPBIOS	1
Configuration avancée du système	UEFI BIOS Boot Mode with GPT Partition	[800-BBDM] / UEFIB	1
Fans	None		
Bloc d'alimentation	Dual, Hot Plug, Redundant Power Supply (1+1), 550W	[450-AGZB] / G8NPRID	1
Cordon d'alimentation	Rack Power Cord 2M (C13/C14 10A)	[450-AADY] / 518051	2
PCIe Riser	No PCIe Riser	[800-BBLC] / NOPCIE	1
Motherboard	PowerEdge R6415/R7415 Motherboard	[384-BBSR] / 5107909	1



Other options

Option	Sélection	Référence SKU/code produit	Quantité
Embedded Systems Gestion (Multi)	iDRAC9 Enterprise with OpenManage Enterprise Advanced	[385-BBKT][528-BIYY] / 5100750	1
Carte réseau supplémentaire	On-Board Broadcom 5720 Dual Port 1Gb LOM	[542-BBBP] / OBNIC	1
Carte réseau supplémentaire	Broadcom 57416 Dual Port 10 GbE BaseT Network LOM Mezz Card	[540-BBYT] / 5104798	1
Bezel	No Bezel for x4 and x8 chassis	[350-BBBW][350-BBMD] / 5109234	1
Quick Sync	Quick Sync 2 (At-the-box mgmt)	[350-BBKQ] / 5104112	1
Rails pour rack	ReadyRails™ Static Rails for 2/4-post Racks	[770-BBBM] / STATIC	1
CacheCade SSD	None		
Password	iDRAC,Factory Generated Password	[379-BCSF] / 5101343	1
iDRAC Server Manager	iDRAC Service Module (ISM), Pre-Installed in OS	[379-BCQW] / 5102435	1
Group Manager	iDRAC Group Manager, Enabled	[379-BCQV] / 5100925	1
Lecteur optique interne	No Internal Optical Drive for 4/8 HD Chassis	[429-ABBF] / 5101077	1

Other options

Option	Sélection	Référence SKU/code produit	Quantité
Microsoft SQL Server	None		

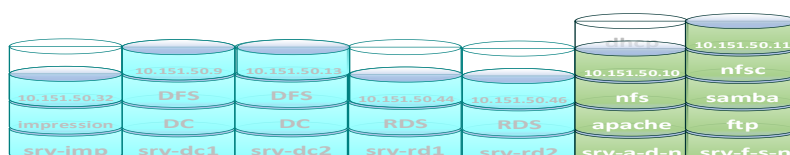
Other options

Option	Sélection	Référence SKU/code produit	Quantité
Documentation du système	No Systems Documentation, No OpenManage DVD Kit	[631-AACK] / NODOCS	1
Emballage d'expédition	PowerEdge R6415 x8 Drive Shipping Material	[343-BBGM] / G7XZ9OQ	1
Expédition	PowerEdge R6415 Shipping EMEA1 (English/French/German/Spanish /Russian/Hebrew)	[340-CBFT] / G2RMJ5Z	1

Other options

Option	Sélection	Référence SKU/code produit	Quantité
Garantie de base	Basic Next Business Day 36Months, 36 Mois	[709-BBIL] / G2L3ABJ	1
Garantie	ProSupport Plus and Next Business Day Onsite Service, 36 Mois	[865-BBND] / GU08IG4	1
Dell Services:Extended Service	Keep Your Hard Drive, 36 Mois	[711-BBBR] / GB5Q0ZY	1
Service de diagnostic sur site	None		
Services de déploiement	Basic Deployment Dell Server R Series 1U/2U	[683-19200] / GJCST0V	1
Dell Services : Solution Services	None		

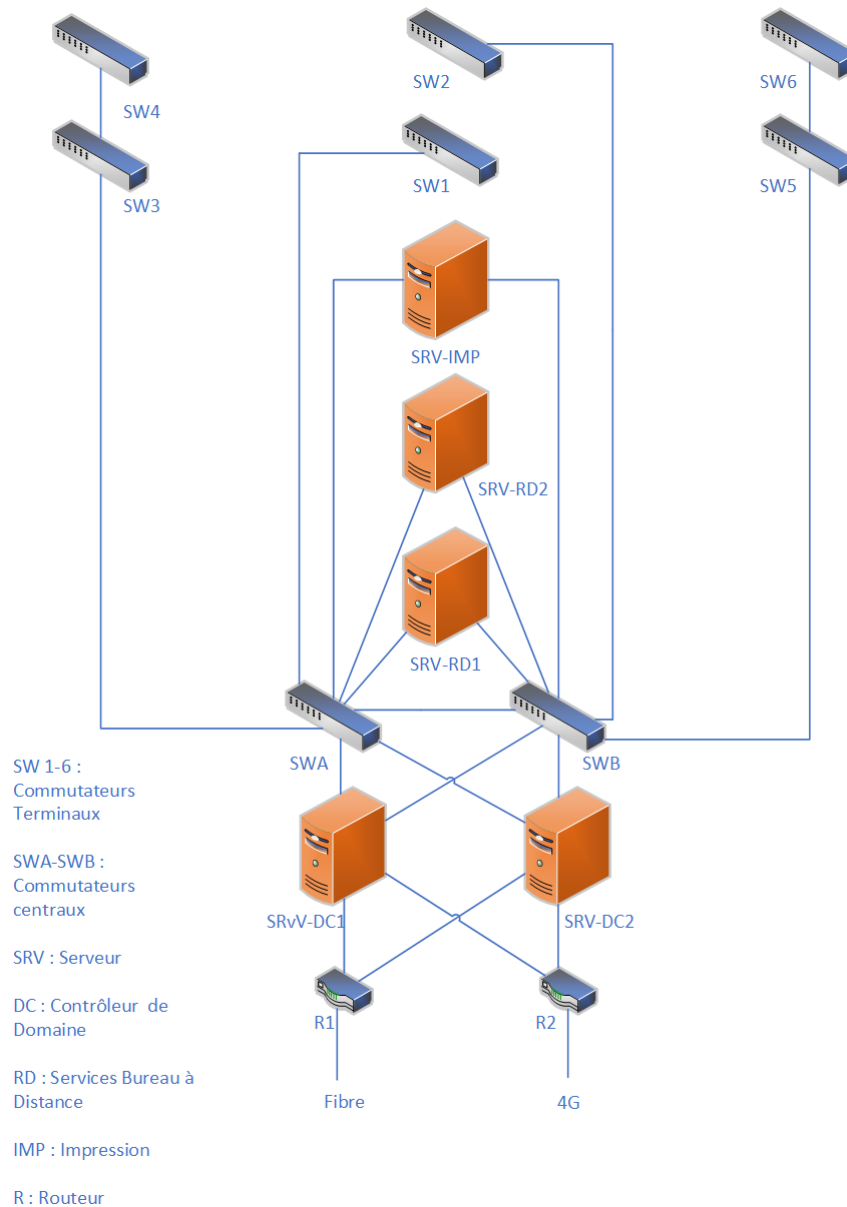
Tous les serveurs se présentent avec une agrégation RAID 1 pour une tolérance de panne accrue



C. Topologie serveurs BSD.ADDS

Le schéma ci-dessous concerne exclusivement les serveurs faisant partie de l'environnement Windows

Figure XIII-8 : Liaisons switchs-serveurs bsd.adds



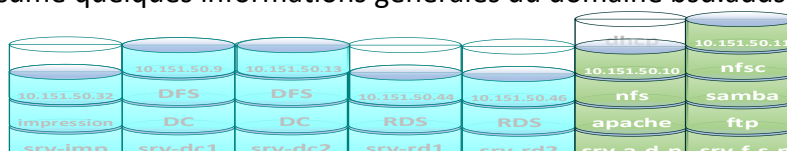
Les 2 contrôleurs de domaine, disposant de 4 ports Ethernet, sont connectés aux 2 routeurs et aux 2 commutateurs centraux afin d'assurer le plus haut niveau d'accès Internet.

D. Active Directory

❖ Topologie DFS Réplication

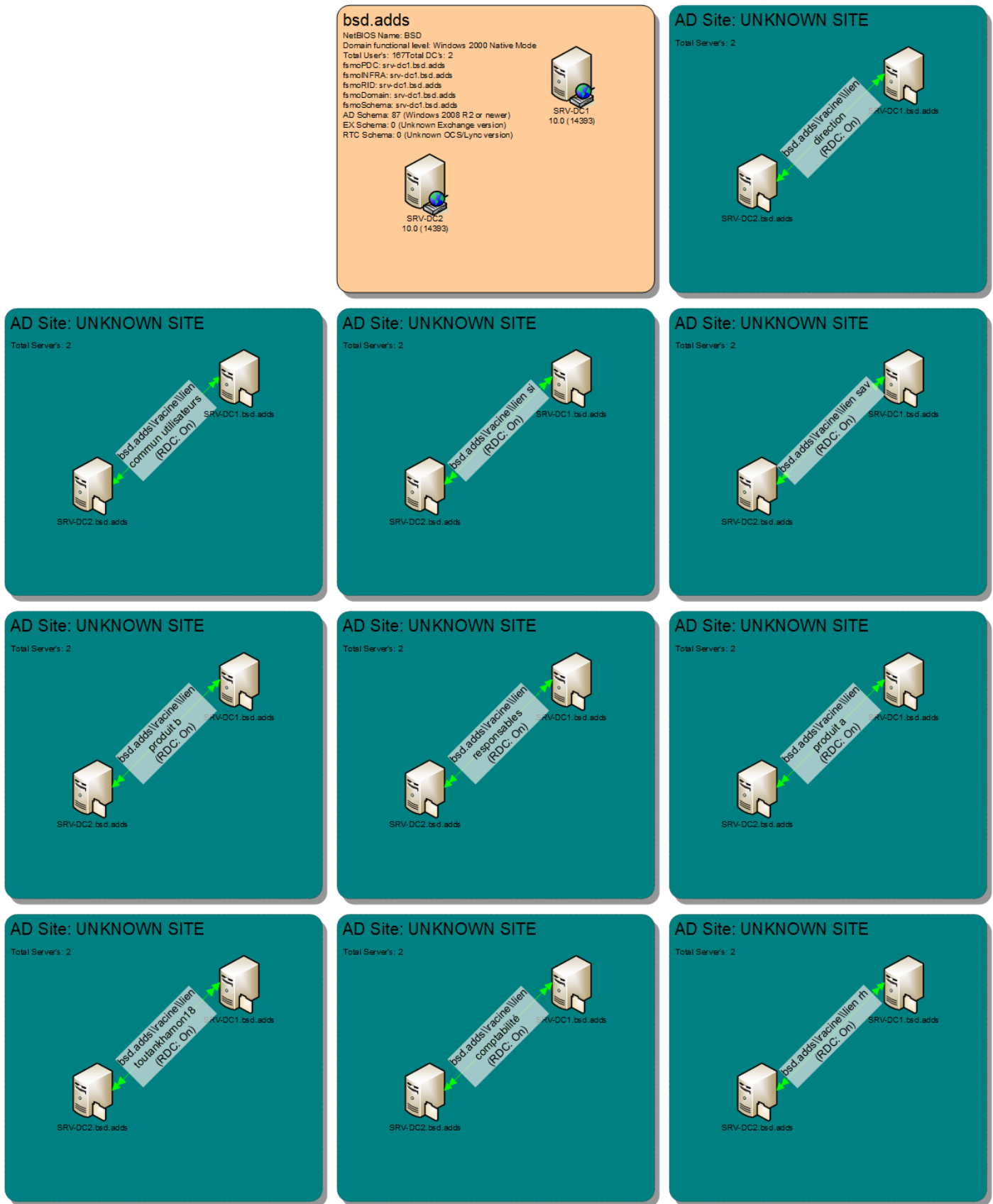
Les vignettes ci-dessous décrivent le nom des liens et l'état de la réplication des fichiers distribués.

La vignette orange résume quelques informations générales du domaine bsd.adds



La mention « UNKNOWN SITE » fait référence à un site géographique, non déployé pour cette étude.

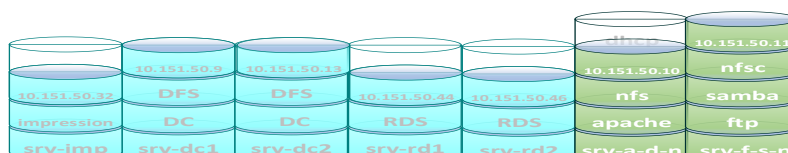
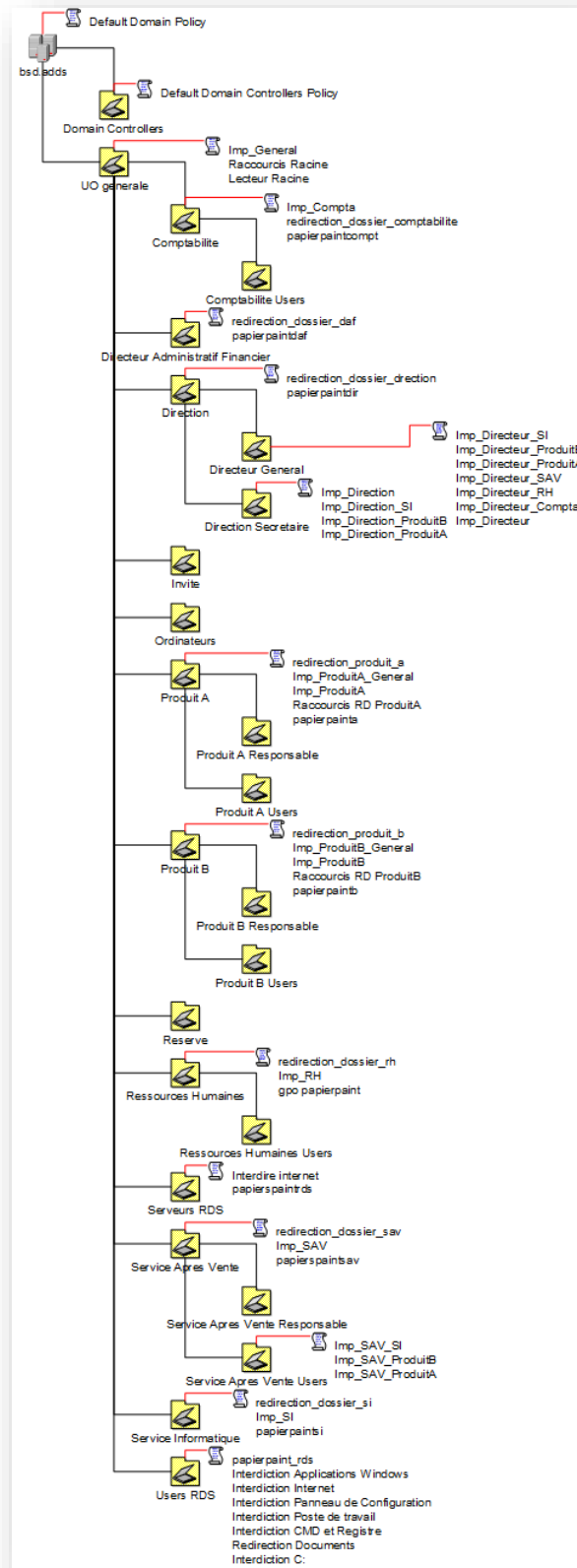
Figure XIII-9 : Vignettes DFS + Informations domaine



❖ Topologie Active directory

Les listes GPO sont liées en rouge à leur OU respectives, c'est-à-dire leurs environnements d'application

Figure XIII-10 : Arborecence des OU



E. Tableau des permissions NTFS

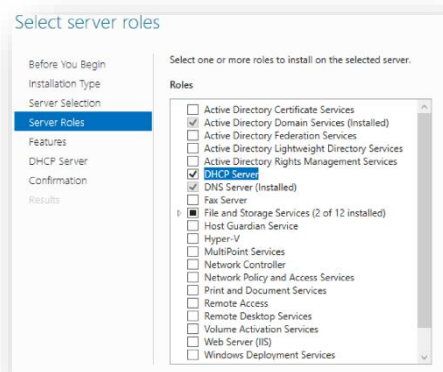
Groupes	Direction	Compta	RH	SAV	ProduitA	ProduitB	Responsables	SI	Invités
Dossiers									
Direction	E	NA	NA	NA	NA	NA	NA	NA	NA
Compta	L	E	NA	NA	NA	NA	NA	NA	NA
RH	L	NA	E	NA	NA	NA	NA	NA	NA
SAV	L	NA	NA	E	NA	NA	NA	NA	NA
ProduitA	L	NA	NA	NA	E	NA	NA	NA	NA
ProduitB	L	NA	NA	NA	NA	E	NA	NA	NA
Commun	E	E	E	E	E	E	E	E	L
Responsables	L	NA	NA	NA	NA	NA	E	NA	NA
SI	L	NA	NA	NA	NA	NA	NA	E	NA

L	Lecture
E	Ecriture
NA	Non autorisé

Composition des groupes	Direction	Responsable 0 + utilisateurs	Responsable 0 Directeur général
	Compta	Responsable 1 + utilisateurs	Responsable 1 Directeur Administratif et Financier
	RH	Responsable 1 + utilisateurs	Responsable 2 Responsable SAV
	SAV	Responsable 2 + utilisateurs	Responsable 3 Responsable Produit A
	ProduitA	Responsable 3 + utilisateurs	Responsable 4 Responsable Produit B
	ProduitB	Responsable 4 + utilisateurs	
	Responsables	Responsable 0+1+2+3+4	
SI			

- Le groupe Invités rassemble les utilisateurs temporaires
- Le groupe Responsables n'a pas de permission sur le dossier Direction
- Le groupe Responsables peut lire les données des autres dossiers
- Chaque groupe (sauf Invités) peut écrire à l'intérieur du dossier partagé correspondant à son service
- Le groupe Direction peut lire les données de l'ensemble des dossiers partagés
- Le groupe Commun autorise tous les groupes (sauf Invités) en écriture
- Les absences de permissions NTFS (Non autorisé) sont considérées comme des interdictions non explicites (pas de refus d'accès spécifique)

F. Rôle DHCP



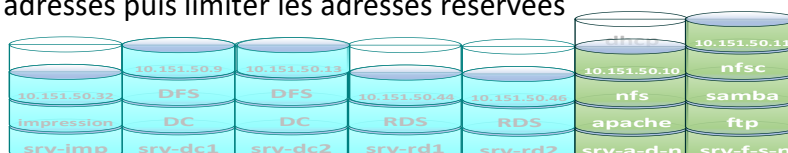
Installation du rôle DHCP
Activer l'autorisation du serveur

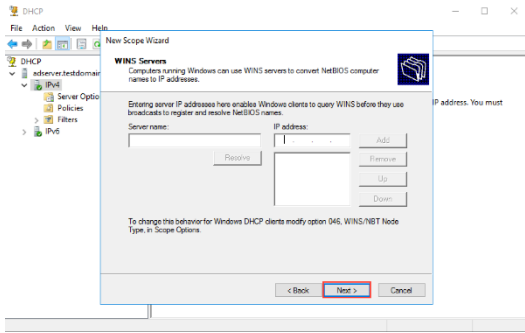
Sur Ipv4 en vert on demande l'assistant nouvelle étendue

La nommée puis la configurer

Plage d'adresse deux solutions :

- soit limiter la plage pour protéger les adresses que l'on veut réserver
- soit ouvrir toutes les adresses puis limiter les adresses réservées





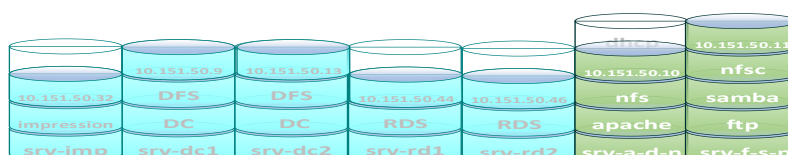
Le choix présent sera d'ouvrir toute la plage puis d'exclure les adresses réservées.

Plage 10.151.50.2 à 10.151.50.250 ouverte à l'attribution d'adresses

Et donc les adresses réservées : les serveurs, switch, imprimantes, passerelle

Liste non exhaustive vu qu'il suffit d'ajouter une adresse de réservation au serveur.

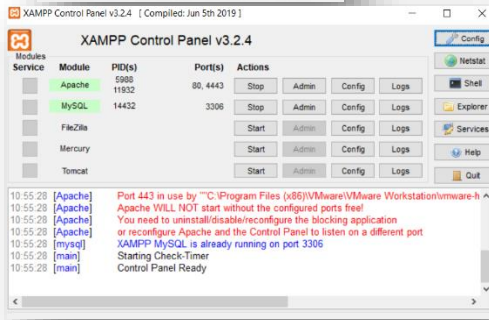
10.151.50.9	10.151.50.13	10.151.50.32
10.151.50.10	10.151.50.11	10.151.50.44
10.151.50.50 10.151.50.57	à 10.151.50.1	10.151.50.46



Plusieurs choix possibles, le plus simple pour tester a été de télécharger Xampp qui intègre un serveur Apache et un serveur sql facile à manipuler.



XAMPP
 X Multiplateforme
 A Apache
 M Mariabd (Mysql)
 P Perl
 P PHP



Les outils sont déjà préprogrammés.

Nous avons dû modifier le port sécurisé 443 natif à apache en 4443 (vmware workstation a déjà réservé le port 443)

Figure XIII-11 xampp

Phpmysqladmin

Pas d'interface d'accueil dans les configurations de xampp root sans mot de passe

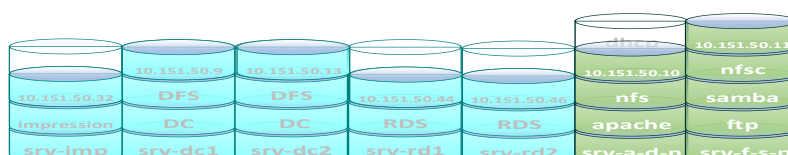
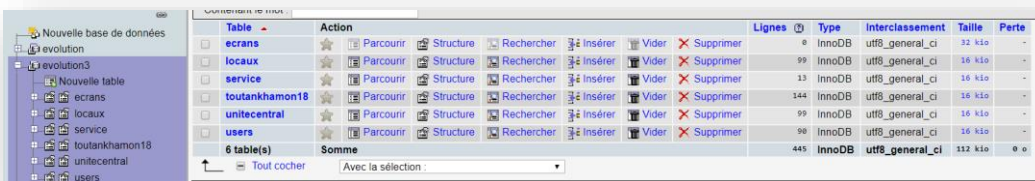
Directement sur une arborescence de base et de table.

Donc création de la base evolution3 et des tables en suivants le MCD.

Soit en mode graphique, soit en mode SQL (sigle de Structured Query Language, en français langage de requête structurée)

L'interface graphique ne permet qu'une action à la fois, le SQL peut en faire plusieurs voir même la création complète d'une base si aucune faute de syntaxe ou incohérence ne vient arrêter le processus.

Donc soit on crée la base et les tables puis on peut importer des fichier csv pour remplir les données existantes dans les tables par le service d'importation.



Ou la création en sql

```

CREATE TABLE service(
  idservice VARCHAR(30) NOT NULL PRIMARY KEY
  ,services VARCHAR(33) NOT NULL
);

INSERT INTO service(idservice,services) VALUES ("","Service Informatique");
INSERT INTO service(idservice,services) VALUES ("","Ressources Humaines Users");
INSERT INTO service(idservice,services) VALUES ("","Comptabilite Users");
INSERT INTO service(idservice,services) VALUES ("","Directeur Administratif Financier");
INSERT INTO service(idservice,services) VALUES ("","Directeur General");
INSERT INTO service(idservice,services) VALUES ("","Direction secretaire");
INSERT INTO service(idservice,services) VALUES ("","Toutankhamon18");
INSERT INTO service(idservice,services) VALUES ("","Produit A Users");
INSERT INTO service(idservice,services) VALUES ("","Produit B Users");
INSERT INTO service(idservice,services) VALUES ("","Toutankhamon18");
INSERT INTO service(idservice,services) VALUES ("","Service Apres Vente Responsable");
INSERT INTO service(idservice,services) VALUES ("","Service Apres Vente Users");
  
```

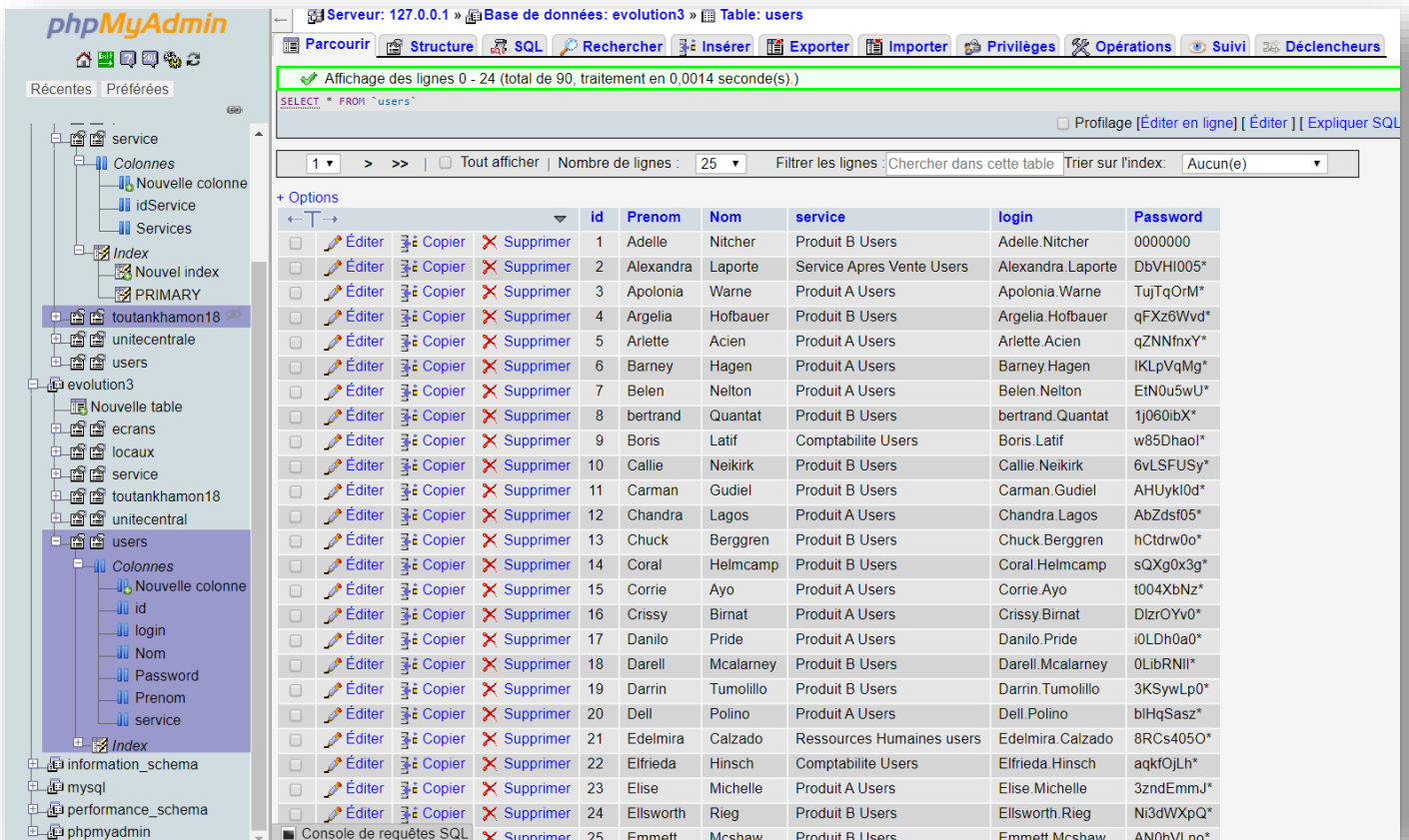
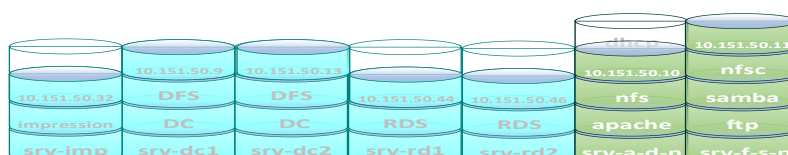


Figure XIII-12 Base de données users

Voilà la base sur la gauche et l'affichage de la table users sur la droite




```
-----  
#  
# Table: PossederToutankhamon18  
#-----  
  
CREATE TABLE PossederToutankhamon18 (  
    idService          Int NOT NULL ,  
    idToutankhamon18 Int NOT NULL  
    ,CONSTRAINT  
    PossederToutankhamon18_PK PRIMARY KEY  
    (idService,idToutankhamon18)  
  
    ,CONSTRAINT  
    PossederToutankhamon18_Service_FK FOREIGN KEY  
    (idService) REFERENCES Service(idService)  
    ,CONSTRAINT  
    PossederToutankhamon18_Toutankhamon180_FK  
    FOREIGN KEY (idToutankhamon18) REFERENCES  
    Toutankhamon18 (idToutankhamon18)  
    )ENGINE=InnoDB;
```

Exemple de création de table avec id primaire et les contraintes relationnelles

La table MySQL sur PHP admin est fonctionnelle.

Le but sera d'installer sur le serveur linux en complément d'Apache de faire une exportation SQL

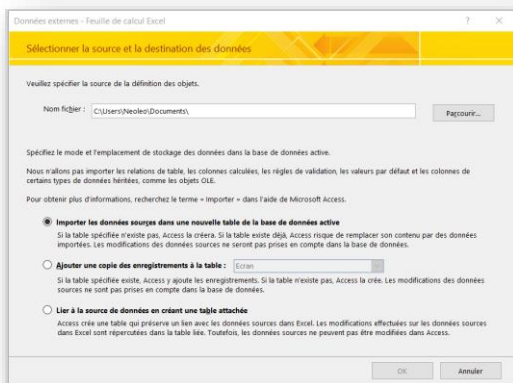
Puis une importation sur MySQL du serveur linux après avoir fait les configurations nécessaires.

Interface user sans permission et root avec toutes les permissions pour l'accès à la base qui remplit les demandes du cahier des charges mais limitatif dans son utilisation.

Il manque un outil d'interface, le code PHP, html, ccs pourrait être une bonne solution alliée à la base déjà créée sur un délai plus important.

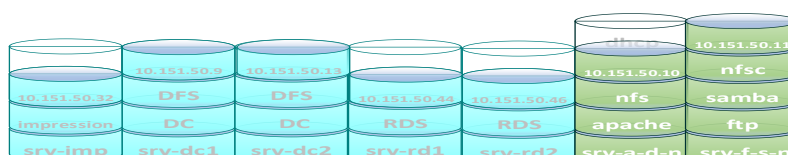
Donc Access paraît être la meilleure alternative pour nous.

Lancement du programme Access.



Création des bases par importation, deux choix, soit par les fichiers Excel (fichier importation source extérieur)

Copier ou lier



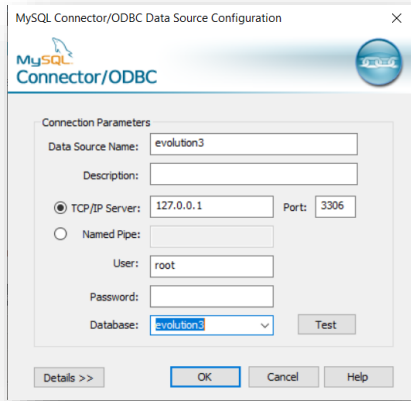


Figure XIII-13 ODBC

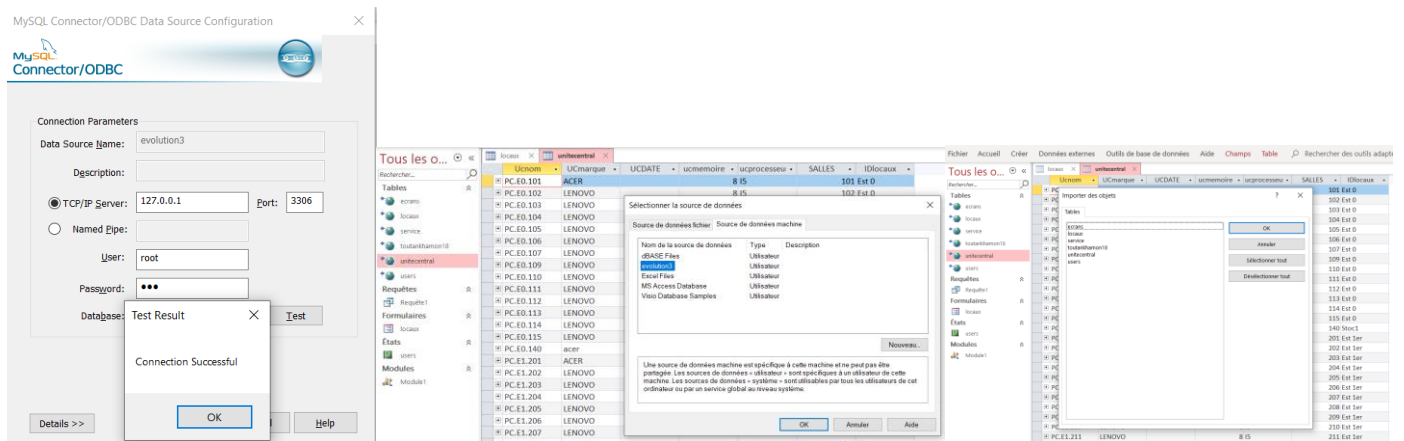
Soit importer ou lier depuis la base MySQL.

La problématique de compatibilité peut être réglé par les drivers ODBC

Donc installation et configuration des pilotes, attentions aux versions 32b et 64b, nous avons dû mettre la version 32bit.

Donc connexion à l'IP du serveur MySQL et son port, login et mdp de la base de données.

Nous voilà en lien avec la base et la possibilité de lier les tables ou de les exporter. Nous avons exporté pour tester la connectivité et travailler ensuite hors connexion pour préserver les tables. Le but dans l'installation sera bien de lier les tables au serveurs SQL pour une interactivité complète.



Voilà les tables sont exportées et liées.

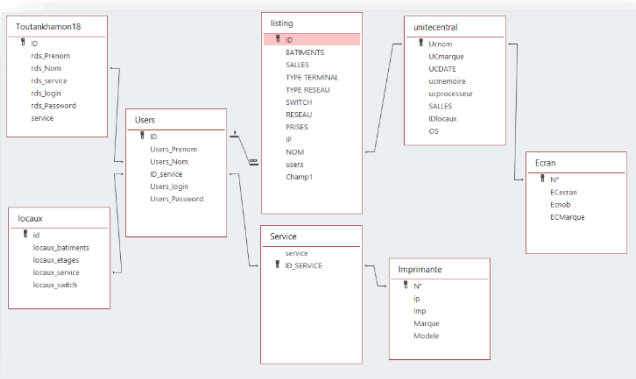


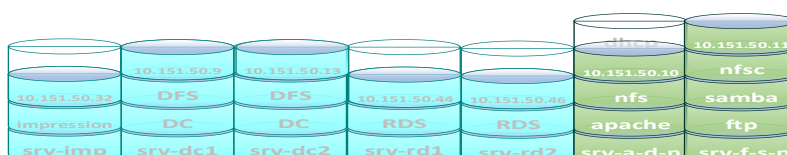
Figure XIII-14 : Table relationnel Access

Une table relationnelle est aussi nécessaire à Access pour fonctionner.

Nous avons recréé un mcd pour Access.

Le suivi du premier Merise n'a pas été concluant.

Celui-ci laisse les tables d'Access travaillé.



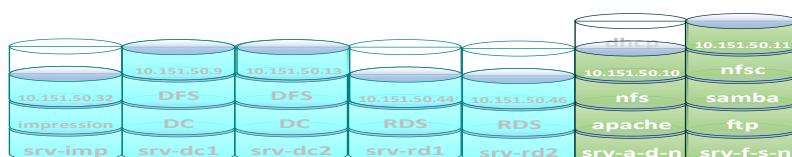
Access génère des tables dans les tables suivant les jointures du mcd

Figure XIII-15 : Access tables imbriqués

ip	Imp	Marque	Modele	Cliquer pour ajouter					
10.10.3.1	IMP.1								
10.10.3.2	IMP.2								
10.10.3.3	IMP.3								
10.10.3.4	IMP.4								
10.10.3.5	IMP.5								
10.10.3.6	IMP.6								
service		Cliquer pour							
Produit A Responsable									
ID	Prenom	Nom	Login	Password				Cliquer pour	
84	Frederic	Leroux	Frederic.Leroux	NrdyUGIZ*					
ID	BATIMENTS	SALLES	TYPE TERMI	TYPE RESEAL	SWITCH	RESEAU	PRISES	IP	NOM
105	Est 1er		201 PC	reseau est	E1		4 E1/201/4	10.10.4.201	PC.E1.201
		(Nouv.)							
		(Nouv.)							
10.10.3.7	IMP.7								

Figure XIII-16 : Access tables imbriquées 2

service	ID_SERVICE	Cliquer pour ajouter									
Gardien	1										
Comptabilite Users	2										
ID	Prenom	Nom	Login	Password				Cliquer pour			
43	Miss	Dunning	Miss.Dunning	1ks123tv*							
44	Elfrieda	Hinsch	Elfrieda.Hinsch	aqkfoJlh*							
53	Willis	Wylie	Willis.Wylie	3xTSPWOL*							
54	Maxima	Brzozowski	Maxima.Brzozowski	tvOGRzLV*							
55	Boris	Latif	Boris.Latif	w85Dhaol*							
		(Nouv.)									
		(Nouv.)									
Directeur Administratif Fina	3										
ID	Prenom	Nom	Login	Password				Cliquer pour			
87	Eric	POLFER	Eric.POLFER	0IQJJmo*							
		(Nouv.)									
Directeur General	4										
ID	Prenom	Nom	Login	Password				Cliquer pour			
83	Olivier	Kalusinsky	Olivier.Kalusinsky	ZUMO3PXY*							
		(Nouv.)									
Direction secretaire	5										
ID	Prenom	Nom	Login	Password				Cliquer pour			
42	Scarlette	Ada	Scarlette.Ada	BnCpwnVX*							
ID	BATIMENTS	SALLES	TYPE TERMI	TYPE RESEAL	SWITCH	RESEAU	PRISES	IP	NOM	Champ1	Cliquer pour
45	Principal 1er		203 PC	reseau principal P1			1 P1/203/1	10.10.1.203	PC.P1.203		
		(Nouv.)									
		(Nouv.)									
Produit A Responsable	6										
Produit A Users	7										
Produit B Responsable	8										
Produit B Users	9										
Ressources Humaines users	10										
Service Apres Vente Respor	11										
Service Apres Vente Users	12										
Informatique	13										
		(Nouv.)									



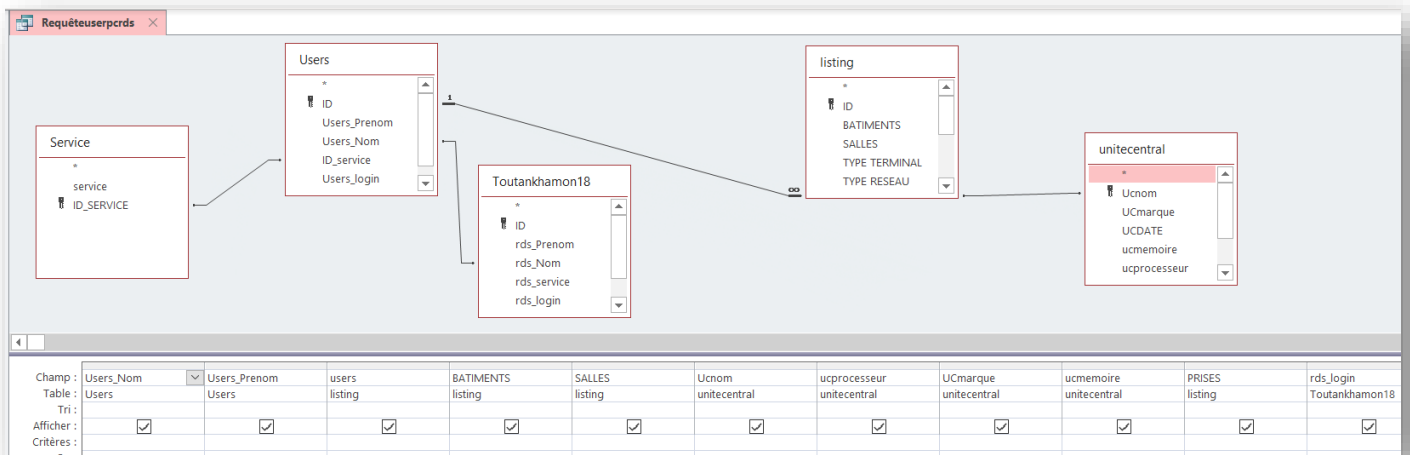


Figure XIII-17 : Access Requête

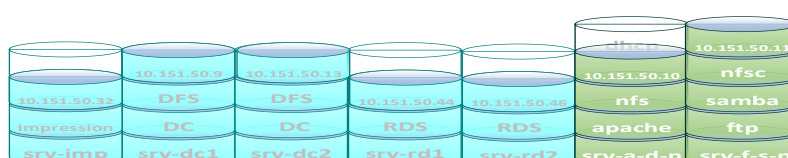
Voilà maintenant l'heure de créer des requêtes, trois modes permettent de mettre notre requête en place soit comme ci-dessus en mode création la possibilité de gérer la jointure entre les tables et qui l'on veut afficher.

La syntaxe SQL

```

SELECT Users.Users_Nom, Users.Users_Prenom, listing.users, listing.BATIMENTS, listing.SALLES, unitecentral.Ucnom, unitecentral.ucprocesseur, unitecentral.UCmarque, unitecentral.ucmemoire, listing.PRISES, Toutankhamon18.rds_login, Service.service
FROM (Service INNER JOIN (Users INNER JOIN Toutankhamon18 ON Users.Users_Nom = Toutankhamon18.rds_Nom) ON Service.ID_SERVICE = Users.ID_service) INNER JOIN (unitecentral INNER JOIN listing ON unitecentral.Ucnom = listing.NOM) ON Users.ID = listing.users
    
```

(Les instructions en sql seront les mêmes si la manipulation doit être faite depuis le serveur)



Le mode « feuille de données »

Toutes les tables sélectionnées pour l’affichage qui sont alignées à la jointure

Nom	Prenom	users	BATIMENTS	SALLES	Ucnom	ucprocesseur	UCmarque	ucmemoire	PRISES	rds_login	service
Beziat	Hannah	Hannah.Beziat	Est 0		103 PC.E0.103	I5	LENOVO	8	E0/103/4	Hannah.Beziat.rds	Produit A Users
Loeza	Tom	Tom.Loeza	Est 0		104 PC.E0.104	I5	LENOVO	8	E0/104/4	Tom.Loeza.rds	Produit A Users
krupps	Fabrice	Fabrice.krupps	Est 0		105 PC.E0.105	I5	LENOVO	8	E0/105/4	Fabrice.krupps.rds	Produit A Users
Portaro	Hui	Hui.Portaro	Est 0		106 PC.E0.106	I5	LENOVO	8	E0/106/4	Hui.Portaro.rds	Produit A Users
Opitz	Josefa	Josefa.Opitz	Est 0		107 PC.E0.107	I5	LENOVO	8	E0/107/4	Josefa.Opitz.rds	Produit A Users
Steinhaus	Lea	Lea.Steinhaus	Est 0		109 PC.E0.109	I5	LENOVO	8	E0/109/4	Lea.Steinhaus.rds	Produit A Users
Vielma	ola	ola.Vielma	Est 0		110 PC.E0.110	I5	LENOVO	8	E0/110/4	ola.Vielma.rds	Produit A Users
Harper	Quentin	Quentin.Harper	Est 0		111 PC.E0.111	I5	LENOVO	8	E0/111/4	Quentin.Harper.rds	Produit A Users
Tijerina	Leanna	Leanna.Tijerina	Est 0		112 PC.E0.112	I5	LENOVO	8	E0/112/4	Leanna.Tijerina.rds	Produit A Users
Pride	Daniilo	Daniilo.Pride	Est 0		113 PC.E0.113	I5	LENOVO	8	E0/113/4	Daniilo.Pride.rds	Produit A Users
Marcille	Huey	Huey.Marcille	Est 0		114 PC.E0.114	I5	LENOVO	8	E0/114/4	Huey.Marcille.rds	Produit A Users
Warne	Apolonia	Apolonia.Warne	Est 0		115 PC.E0.115	I5	LENOVO	8	E0/115/4	Apolonia.Warne.rds	Produit A Users
Warne	Apolonia	Apolonia.Warne	Est 0		101 PC.E0.101	I5	ACER	8	E0/101/4	Apolonia.Warne.rds	Produit A Users
Lagos	Chandra	Chandra.Lagos	Est 1er		207 PC.E1.207	I5	LENOVO	8	E1/207/4	Chandra.Lagos.rds	Produit A Users
Lagos	Chandra	Chandra.Lagos	Est 1er		202 PC.E1.202	I5	LENOVO	8	E1/202/4	Chandra.Lagos.rds	Produit A Users
Birnat	Crissy	Crissy.Birnat	Est 1er		203 PC.E1.203	I5	LENOVO	8	E1/203/4	Crissy.Birnat.rds	Produit A Users
Branin	Gianna	Gianna.Branin	Est 0		102 PC.E0.102	I5	LENOVO	8	E0/102/4	Gianna.Branin.rds	Produit A Users
Branin	Gianna	Gianna.Branin	Est 1er		204 PC.E1.204	I5	LENOVO	8	E1/204/4	Gianna.Branin.rds	Produit A Users
Billa	Valentin	Valentin.Billa	Est 1er		205 PC.E1.205	I5	LENOVO	8	E1/205/4	Valentin.Billa.rds	Produit A Users
Dudash	Ilona	Ilona.Dudash	Est 1er		206 PC.E1.206	I5	LENOVO	8	E1/206/4	Ilona.Dudash.rds	Produit A Users
Lablanc	Willard	Willard.Lablanc	Est 1er		208 PC.E1.208	I5	LENOVO	8	E1/208/4	Willard.Lablanc.rds	Produit A Users
Randol	Lauryn	Lauryn.Randol	Est 1er		209 PC.E1.209	I5	LENOVO	8	E1/209/4	Lauryn.Randol.rds	Produit A Users
Begin	Laurena	Laurena.Begin	Est 1er		210 PC.E1.210	I5	LENOVO	8	E1/210/4	Laurena.Begin.rds	Produit A Users
Armacost	Matthew	Matthew.Arma	Est 1er		211 PC.E1.211	I5	LENOVO	8	E1/211/4	Matthew.Armacost.r	Produit A Users
Wardle	lesha	lesha.Wardle	Ouest 0		101 PC.T0.101	I5	ACER	8	T0/101/6	lesha.Wardle.rds	Produit B Users
Sardou	jean	jean.Sardou	Ouest 0		102 PC.T0.102	I5	LENOVO	8	T0/102/6	jean.Sardou.rds	Produit B Users
Zarling	Louis	Louis.Zarling	Ouest 0		103 PC.T0.103	I5	LENOVO	8	T0/103/6	Louis.Zarling.rds	Produit B Users
Mcshaw	Emmett	Emmett.Mcsha	Ouest 0		104 PC.T0.104	I5	LENOVO	8	T0/104/6	Emmett.Mcshaw.rds	Produit B Users

Figure XIII-18 base de données requete users

Requêteuserpc

Nom:

Prenom:

BATIMENTS choix:

BATIMENTS:

SALLES:

Ucnom:

ucprocesseur:

UCmarque:

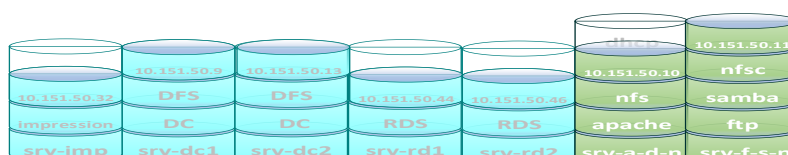
ucmemoire:

PRISES:

rds_login:

Qui nous permet de générer un formulaire basé sur la requête

Donc ici déjà nous pouvons choisir dans la liste déroulante le bâtiment et la salle et le formulaire va mettre toutes les occurrences à jours sur le formulaire en liens avec la requête.



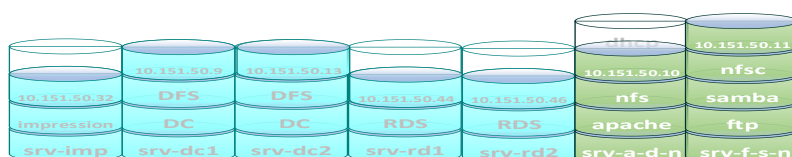




Maintenant, après la mise en forme ici recherche par login, nom, Bâtiments, Salle, Ordinateurs, Prises Services.

Requêteuserpcrds x Requêteuserpcrds x Requêteuserpctt x

Requête user pc complet

Choisir	Eric.POLFER
Nom	POLFER
Prenom	Eric
BATIMENTS	Principal 0
SALLES	101
PC	PC.P0.101
Processeur	I5
Marque PC	ACER
Memoire vive	16
PRISES	P0/101/1
service	Directeur Administratif Financier





Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



Voici d'autre exemple de requête transformée en formulaire modifiable par l'utilisateur qui sera le service informatique pour les besoins de suivi du parc.

Recherche par nom ou pc

Nom: loizel RECHERCHE par NOM

Prenom: Greg

Batiments: Ouest 1er

SALLES: 215

PC: PC.T1.215

Processeur: i5

Marque: LENOVO

Memoire vive: 8


PRISES: T1/215/6

Login RDS: Greg.loizel.rds

NOM: loizel

PC: []

RECHERCHE par PC



Le projet final en récapitulatif, le serveur linux apache mysql hébergera la base de données qui sera lié sur la base Access par connect ODBC, un accès users sans permission pour ceux qui veut consulter.

Au besoin un fichier html (pour placer en lien HyperText sur l'intranet ou Excel peut être éditer à la demande ou régulièrement depuis accès).

Users_Nom	Users_Prenom	BATIMENTS	SALLES	Ucnom	ucprocesseur	ucmarque	ucmemoire	PRISES	rds_login	Modifiable39	Modifiable37
Bezat	Hannah	Est 0	103	PC.E0.103i5	LENOVO	8	E0/103/4	Hannah.Bezat.rds			loizel
Losta	Tom	Est 0	104	PC.E0.104i5	LENOVO	8	E0/104/4	Tom.Losta.rds			loizel
Krupps	Fabrice	Est 0	105	PC.E0.105i5	LENOVO	8	E0/105/4	Fabrice.krupps.rds			loizel
Portaro	Hui	Est 0	106	PC.E0.106i5	LENOVO	8	E0/106/4	Hui.Portaro.rds			loizel
Opitz	Josefa	Est 0	107	PC.E0.107i5	LENOVO	8	E0/107/4	Josefa.Opitz.rds			loizel
Steinhaus	Lea	Est 0	109	PC.E0.109i5	LENOVO	8	E0/109/4	Lea.Steinhaus.rds			loizel
Vielma	ola	Est 0	110	PC.E0.110i5	LENOVO	8	E0/110/4	ola.Vielma.rds			loizel
Harper	Quentin	Est 0	111	PC.E0.111i5	LENOVO	8	E0/111/4	Quentin.Harper.rds			loizel
Tjerina	Leanna	Est 0	112	PC.E0.112i5	LENOVO	8	E0/112/4	Leanna.Tjerina.rds			loizel
Pride	Danilo	Est 0	113	PC.E0.113i5	LENOVO	8	E0/113/4	Danilo.Pride.rds			loizel
Marclie	Huey	Est 0	114	PC.E0.114i5	LENOVO	8	E0/114/4	Huey.Marclie.rds			loizel
Warne	Apolonia	Est 0	115	PC.E0.115i5	LENOVO	8	E0/115/4	Apolonia.Warne.rds			loizel
Warne	Apolonia	Est 0	101	PC.E0.101i5	ACER	8	E0/101/4	Apolonia.Warne.rds			loizel
Logos	Chandra	Est 1er	207	PC.E1.207i5	LENOVO	8	E1/207/4	Chandra.Logos.rds			loizel
Logos	Chandra	Est 1er	202	PC.E1.202i5	LENOVO	8	E1/202/4	Chandra.Logos.rds			loizel
Bimat	Crissy	Est 1er	203	PC.E1.203i5	LENOVO	8	E1/203/4	Crissy.Bimat.rds			loizel
Branin	Gianna	Est 0	102	PC.E0.102i5	LENOVO	8	E0/102/4	Gianna.Branin.rds			loizel
Branin	Gianna	Est 1er	204	PC.E1.204i5	LENOVO	8	E1/204/4	Gianna.Branin.rds			loizel
Billa	Valentin	Est 1er	205	PC.E1.205i5	LENOVO	8	E1/205/4	Valentin.Billa.rds			loizel
Dudash	Iiona	Est 1er	206	PC.E1.206i5	LENOVO	8	E1/206/4	Iiona.Dudash.rds			loizel
Lablanc	Willard	Est 1er	208	PC.E1.208i5	LENOVO	8	E1/208/4	Willard.Lablanc.rds			loizel
Randall	Lauryin	Est 1er	209	PC.E1.209i5	LENOVO	8	E1/209/4	Lauryin.Randall.rds			loizel
Begin	Laurena	Est 1er	210	PC.E1.210i5	LENOVO	8	E1/210/4	Laurena.Begin.rds			loizel
Armocost	Matthew	Est 1er	211	PC.E1.211i5	LENOVO	8	E1/211/4	Matthew.Armocost.rds			loizel
Wardle	Iesha	Ouest 0	101	PC.T0.101i5	ACER	8	T0/101/6	Iesha.Wardle.rds			loizel
Sardou	jean	Ouest 0	102	PC.T0.102i5	LENOVO	8	T0/102/6	jean.Sardou.rds			loizel
Zaring	Louis	Ouest 0	103	PC.T0.103i5	LENOVO	8	T0/103/6	Louis.Zaring.rds			loizel
Mcshow	Emmett	Ouest 0	104	PC.T0.104i5	LENOVO	8	T0/104/6	Emmett.Mcshow.rds			loizel
Sams	Tammy	Ouest 0	105	PC.T0.105i5	LENOVO	8	T0/105/6	Tammy.Sams.rds			loizel
Gudiel	Carman	Ouest 0	106	PC.T0.106i5	LENOVO	8	T0/106/6	Carman.Gudiel.rds			loizel
Hofbauer	Argella	Ouest 0	107	PC.T0.107i5	LENOVO	8	T0/107/6	Argella.Hofbauer.rds			loizel

Exportation - Document HTML

Sélectionner la destination pour les données à exporter

Spécifiez le nom et le format du fichier de destination.

Nom fichier: C:\Users\Neoleo\Documents\Requêteuserpc2.html

Spécifiez les options d'exportation.

Nous n'allons pas importer les relations de table, les colonnes calculées, les règles de validation, les valeurs par défaut et les colonnes de certains types de données héritées, comme les objets OLE.

Pour obtenir plus d'informations, recherchez le terme « Importer » dans l'aide de Microsoft Access.

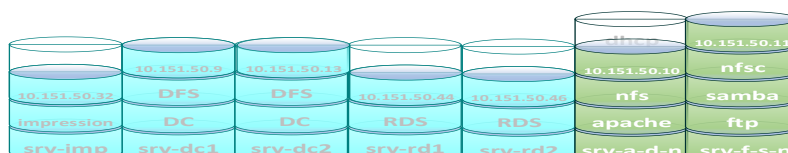
Exporter les données avec la mise en forme et la mise en page

Ouvrir le fichier de destination une fois l'exportation terminée

Exporter uniquement les enregistrements sélectionnés

OK Annuller

Voir les besoins réels puisqu'un autre accès peut être installé en mode consultation pour consulter un accès peut en consulter un autre.



H. Scripts PowerShell

Un prérequis important concerne le nommage des unités organisationnelles (UO). En effet, le script présenté dans cette sous-partie ne fonctionne qu'à la condition de choisir un nom différent pour chaque UO. Ceci permet d'exempter le PS de l'emplacement exact dans l'arborescence AD (voir chapitre « Comprendre Active Directory »), et ainsi d'épurer l'écriture du code. PowerShell utilise l'annuaire AD pour ce ciblage automatique (une seule occurrence UO ne permet qu'un seul ciblage).

Pour les 90 personnes officiant sur un ordinateur de BSD, il faudra ajouter 70 comptes pour administrer l'accès au serveur Bureau à Distance (voir topologie DFS : « 167 users »), les privilèges des sessions RDS et non-RDS ne comportant pas les mêmes privilèges utilisateurs.

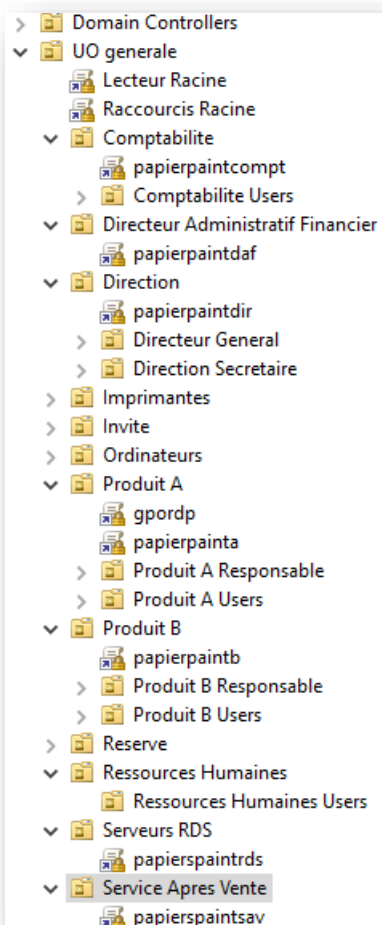


Figure XIII-19 : Power Shell UO

Les BDD (base de données) Excel des informations utilisateurs et ordinateurs a été fournie par le service RH

Une conversion en .CSV sera nécessaire pour son exploitation par le PS

L'organisation des UO fut préalablement décidée pour une répartition pertinente des objets AD. Le regroupement des users par service et au même niveau du domaine facilitera la compréhension globale et l'application des GPO désirées)

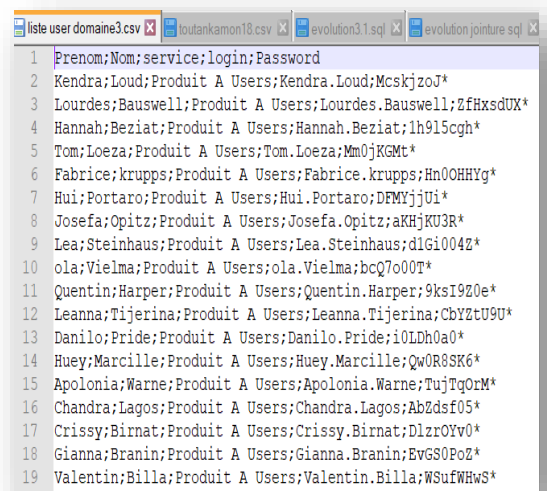
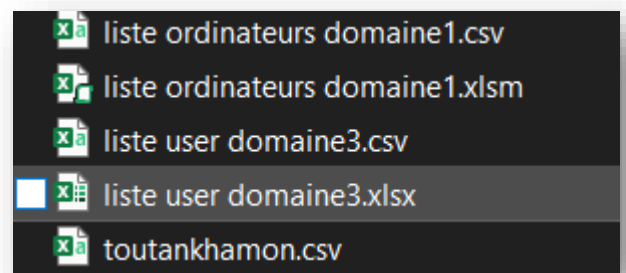
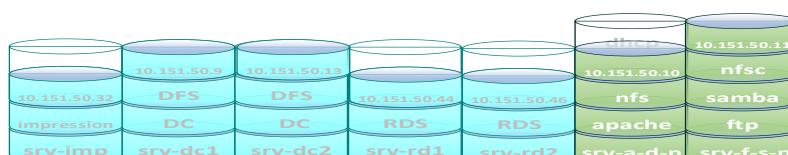


Figure XIII-20 : Power Shell users csv



La BDD en .CSV se présente comme le montre la figure XIII-20. L'entête de ce document (ligne 1) permet le nommage des champs et les points-virgules la séparation pour l'import dans PS

La première ligne est l'entête de colonne qui va être la référence pour Powell Shell dans son exportation. Puis les colonnes sont répétées avec nos informations.

A gauche un extrait de fichier .csv rassemblant des informations utilisateurs.

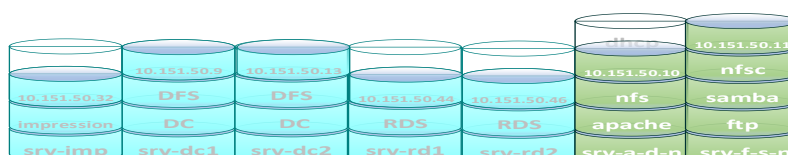
Ci-dessous le script Power Shell d'importation des utilisateurs du fichier .csv dans le domaine AD

```

1 ##### CREATE_USERS.ps1 #####
2
3 $ErrorActionPreference = "Continue"
4 Clear-Host
5
6 Write-Host "`n==== Script de création Utilisateurs =====`n" -BackgroundColor DarkGray
7
8 # Module AD
9 Import-Module ActiveDirectory
10
11 # Variables initiales
12 $File = "C:\Scripts\Utilisateurs.csv"
13 $Domain = (Get-AddDomain).DNSRoot
14
15 # Actions
16 Import-Csv $File -Delimiter ";" | Foreach-Object {
17
18 Write-Host "`n===== " -BackgroundColor DarkGray
19
20 # Variables fixes
21 $Nom = $_.Nom
22 $Prenom = $_.Prenom
23 $Login = $_.Login
24 $RawPassword = $_.Password
25 $Service = $_.Service
26
27 # Variables complémentaires
28 $DN = "$Prenom $Nom"
29 $UPN = "$Login@$Domain"
30 $OU = (Get-ADOrganizationalUnit -Filter "Name -like '*$Service*')."DistinguishedName
31
32
33
34 # Mot de passe
35 $Password = ConvertTo-SecureString -AsPlainText $RawPassword -Force
36
37 # Création de l'utilisateur
38 New-ADUser -GivenName $Prenom -Surname $Nom -SamAccountName $Login -Name $DN -DisplayName $DN -UserPrincipalName $UPN `
39 -Path $OU -AccountPassword $Password -Enabled $true -PasswordNeverExpires $false -ChangePasswordAtLogon $TRUE
40
41 # Vérification
42 if ($?) {Write-Host "Utilisateur $login créé avec succès !" -BackgroundColor DarkGreen}
43 else {Write-Host "Erreur avec l'utilisateur $login !" -BackgroundColor DarkRed}
44
45 Write-Host "=====" -BackgroundColor DarkGray
46
47 }
48
49 Write-Host "`n==== FIN du Script =====`n" -BackgroundColor DarkGray
50
51 ##### ----- #####

```

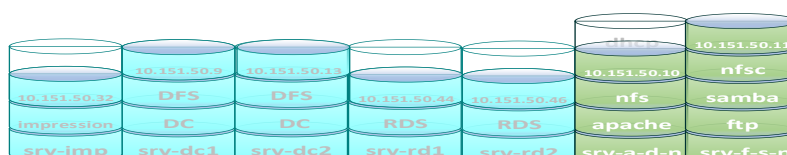
Figure XIII-21 : Power Shell script user



Une vue détaillée de l'action du script, le chiffre correspond au numéro de ligne de la figure ci-dessus :

- 1 -le # permet de placer des commentaires qui seront grandement intéressants à la compréhension du script
- 3 -`$file` variable qui permet à PS (Power Shell) de savoir comment se comporter au moment d'une erreur, « continue » il indique l'erreur et continue
- 6 18 45 49 - `Write-Host` permet d'écrire un texte pendant l'exécution du script début fin du script ou de nommer des étapes différentes par exemple
- 9 -importation du module active directory
- 12 -création de la variable ciblant le fichier .csv des utilisateurs que nous avons placé au préalable dans C:\scripts\
- 13 -variable domaine BSD
- 16 -commande d'importation du fichier cvs depuis l'adresse contenu dans la variable `$file` défini le délimiteur entre les colonnes. Le caractère « pipe » | joint à cette importation une boucle qui va s'exécuter pour chaque ligne du fichier .csv
- 20 à 29 -variables qui correspondent aux colonnes du csv pour l'enregistrement
- 30 -création de la variable UO. Dans les parenthèses, la cmdlet `Get-ADOrganizationalUnit` recherche dans l'active directory l'UO sous un format défini (ici « service »). Comme vu dans le chapitre « Rôle ADDS et DC », préciser le chemin complet de l'UO dans le script n'est pas nécessaire, à la condition que chaque UO soit unique
- 35 -force le chiffrement pour le mot de passe
- 38 -les variables injectent les informations du .csv dans les champs nécessaires à la création des utilisateurs
- 42 -un avertissement apparaîtra dans la console PS pour chaque création d'utilisateur (login) (échecs en rouge et succès en vert). Et cela en boucle jusqu'à la fin du fichier csv.
- 49 -cette instruction signifie la fin de la boucle demandée en écrivant la phrase entre guillemet

Donc s'il n'y a aucune erreur nous avons à l'écran uniquement des messages de création d'utilisateur en vert.



L'image ci-dessous montre ISE de PowerShell à droite le script à exécuter, à gauche le résultat des instructions est vert car il est positif. Ici c'est exactement le même principe pour le script mais pour les ordinateurs.

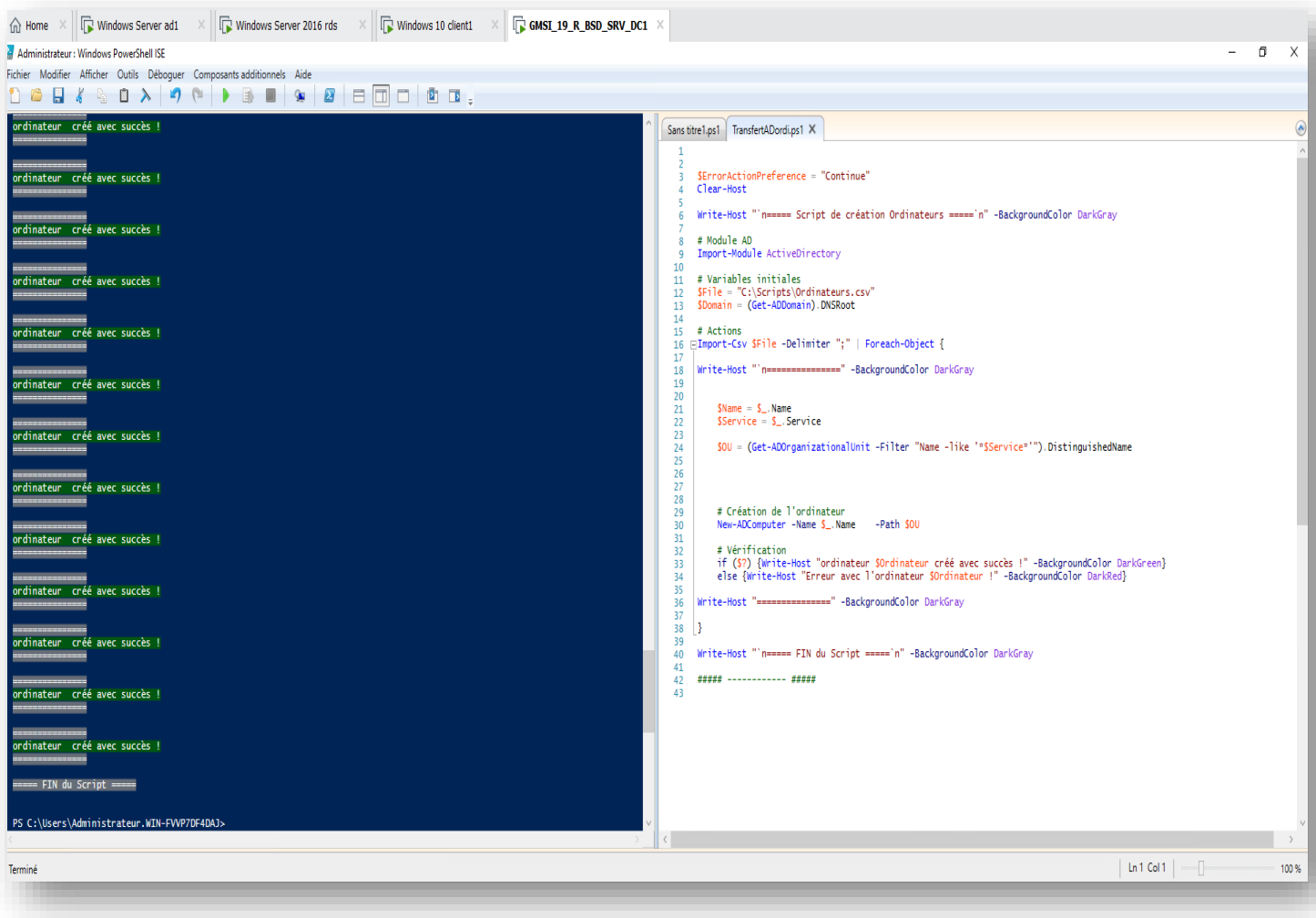
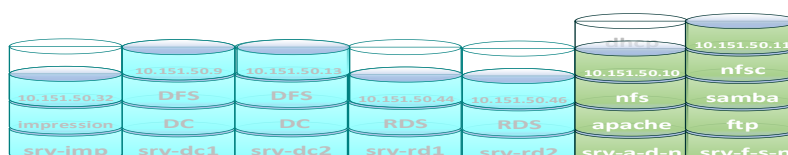


Figure XIII-22 : Power Shell ISE création ordinateurs



```

28     $DN = "$Prenom $Nom"
29     $UPN = "$Login@$Domain"
30     $OU = (Get-ADOrganizationalUnit -Filter "Name -like '*$Service*').DistinguishedName
31
32     # Mot de passe
33
34

```

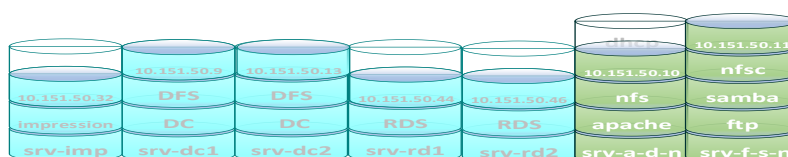
Utilisateur Arlette.Torchio créé avec succès !
Utilisateur Arlette.rds.Torchio créé avec succès !
Utilisateur Adolph.Krivanec créé avec succès !
Utilisateur Adolph.rds.Krivanec créé avec succès !
Utilisateur William.Brerquet créé avec succès !
Utilisateur Sebastien.Sombret créé avec succès !
Utilisateur leonel.Drouhard créé avec succès !

==== FIN du Script ====

PS C:\Users\Administrateur.SRV-AD>

Ici l'exécution du script de créations des utilisateurs avec la boucle et les écritures réussis dans les UO demandée.

Figure XIII-23 : Power Shell ISE creation users





Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



```

##### CREATE_USERS.ps1 #####
$ErrorActionPreference = "Continue"
Clear-Host

Write-Host "`n----- Script de création Utilisateurs -----`n" -BackgroundColor DarkGray

# Module AD
Import-Module ActiveDirectory

# Variables initiales
$File = "C:\Scripts\Utilisateurs.csv"
$Domain = (Get-ADDomain).DNSRoot

# Actions
Import-Csv $File -Delimiter "," | Foreach-Object {

Write-Host "`n-----" -BackgroundColor DarkGray

# Variables fixes
$Nom = $_.Nom
$Prenom = $_.Prenom
$Login = $_.Login
$RawPassword = $_.Password
$Service = $_.Service

# Variables complémentaires
$DN = "$Prenom $Nom"
$UPN = "$Login@$Domain"
$OU = (Get-ADOrganizationalUnit -Filter "Name -like '*$Service*').DistinguishedName

# Mot de passe
$Password = ConvertTo-SecureString $RawPassword -Force

# Création de l'utilisateur
New-ADUser -GivenName $Prenom -Surname $Nom -SamAccountName $Login -Name $DN -DisplayName $DN -UserPrincipalName $UPN `
-Path $OU -AccountPassword $Password -Enabled $true -PasswordNeverExpires $false -ChangePasswordAtLogon $true

# Vérification
if ($?) {Write-Host "Utilisateur $Login créé avec succès !" -BackgroundColor DarkGreen}
else {Write-Host "Erreur avec l'utilisateur $Login !" -BackgroundColor DarkRed}

Write-Host "-----" -BackgroundColor DarkGray
}

Write-Host "`n----- FIN du Script _toutankhamon18 -----`n" -BackgroundColor DarkGray

##### CREATE_USERS_Toutankhamon18.ps1 #####
$ErrorActionPreference = "Continue"

Write-Host "`n----- Script de création Utilisateurs Toutankhamon18 -----`n" -BackgroundColor DarkGray

# Module AD
Import-Module ActiveDirectory

# Variables initiales
$File = "C:\Scripts\Utilisateurs_Toutankhamon18.csv"
$Domain = (Get-ADDomain).DNSRoot

# Actions
Import-Csv $File -Delimiter "," | Foreach-Object {

Write-Host "`n-----" -BackgroundColor DarkGray

# Variables fixes
$Nom = $_.Nom
$Prenom = $_.Prenom
$Login = $_.Login
$RawPassword = $_.Password
$Service = $_.Service

# Variables complémentaires
$DN = "$Prenom $Nom"
$UPN = "$Login@$Domain"
$OU = (Get-ADOrganizationalUnit -Filter "Name -like '*$Service*').DistinguishedName

# Mot de passe
$Password = ConvertTo-SecureString $RawPassword -Force

# Création de l'utilisateur
New-ADUser -GivenName $Prenom -Surname $Nom -SamAccountName $Login -Name $DN -DisplayName $DN -UserPrincipalName $UPN `
-Path $OU -AccountPassword $Password -Enabled $true -PasswordNeverExpires $false -ChangePasswordAtLogon $true

# Vérification
if ($?) {Write-Host "Utilisateur $Login créé avec succès !" -BackgroundColor DarkGreen}
else {Write-Host "Erreur avec l'utilisateur Toutankhamon18 $Login !" -BackgroundColor DarkRed}

Write-Host "-----" -BackgroundColor DarkGray
}

Write-Host "`n----- FIN du Script _toutankhamon18 -----`n" -BackgroundColor DarkGray

##### ----- #####

##### CREATE_ordinateurs.ps1 #####
$ErrorActionPreference = "Continue"

Write-Host "`n----- Script de création Ordinateurs -----`n" -BackgroundColor DarkGray

# Module AD
Import-Module ActiveDirectory

# Variables initiales
$File = "C:\Scripts\Ordinateurs.csv"
$Domain = (Get-ADDomain).DNSRoot

# Actions
Import-Csv $File -Delimiter "," | Foreach-Object {

Write-Host "`n-----" -BackgroundColor DarkGray

$Name = $_.Name
$Service = $_.Service

# Variables complémentaires
$OU = (Get-ADOrganizationalUnit -Filter "Name -like '*$Service*').DistinguishedName

# Création de l'ordinateur
New-ADComputer -Name $_.Name -Path $OU

# Vérification
if ($?) {Write-Host "ordinateur $Ordinateur créé avec succès !" -BackgroundColor DarkGreen}
else {Write-Host "Erreur avec l'ordinateur $Ordinateur !" -BackgroundColor DarkRed}

Write-Host "-----" -BackgroundColor DarkGray
}

Write-Host "`n----- FIN du Script General -----`n" -BackgroundColor DarkGray
Write-Host "`n----- 90 users / 72 RDS / 99 pc ;) -----`n" -BackgroundColor DarkGray
##### ----- #####

```

Le script ci-contre regroupe plusieurs scripts

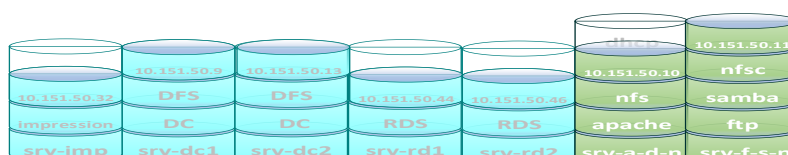
Pour fonctionner il a besoin des trois fichiers .csv sources :

- utilisateurs
- ordinateurs
- toutankhamon18

Rassemble les logins rds des utilisateurs du logiciel en question.

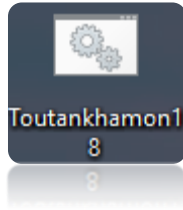
Le mode opération est le même que vu précédemment à la différence près qu'un message supplémentaire marque le passage à la boucle suivante.

L'exécution du script réunit les trois types de création, avec les fichiers .csv et les UO correspondants.



I. Script Rds

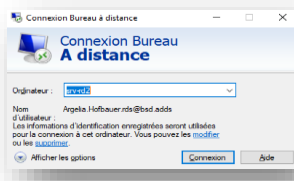
A la demande du directeur administratif et financier, nous avons recherché une solution pour que les utilisateurs du services produits A et B puissent avoir accès rapidement à la sessions RDS



(toutankhamons18).

Donc ouvrir par le biais d'un script une autre session sur le serveur RDS pour des raisons de sécurité une session rds de chaque utilisateur a été faites.

La problématique a été de pouvoir par GPO un script utilisable par les 72 sessions du rds.



Power shell a posé un problème dans la création de la variable d'environnement `%userprofile%.rds` qui se figeait dans le login comme nom et non comme variable.

Après plusieurs essais nous sommes revenu sur du batch. En testant la commande

```
cmdkey /add :<TargetName>/generic :<TargetName> /smartcard/user :<UserName> /pass :<Password>
```

nous avons garder la possibilité de générer la variable `%username%` et en prenant soin de ne pas mettre le password de manière pouvoir mettre le mot de passe à la première connexion puis rendre la connexion automatique jusqu'au prochain changement de mdp

```
cmdkey /generic:srv-rd2 /user:%username%.rds@bsd.adds
mstsc.exe /v:srv-rd2
```

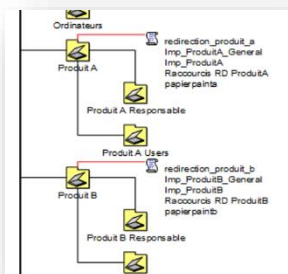
voici notre script batch il faut un espace avant le code. Windows génère la variable

`%username%.extension rds@nom de domaine.adds`

Puis active mstsc.exe (connection bureau a distance)

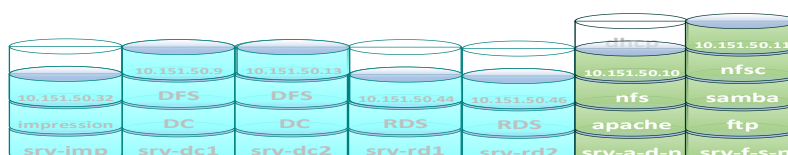
Avec les éléments serveur, login rds déjà renseigné !

Reste à enregistrer notre script et le rendre exécutable en lui ajoutant l'extension `.bat`



Une gpo a été crée pour generer ce toutankhamon18.bat sur

Le bureau de toutes les sessions utilisateur produitA et produitB.



```

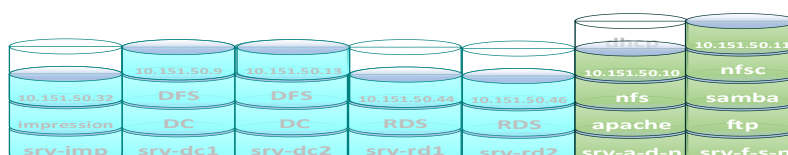
C:\Windows\system32\cmd.exe
C:\Users\Angelia.Hofbauer\Desktop>^
'^' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.
C:\Users\Angelia.Hofbauer\Desktop>cmdkey /generic:srv-rd2 /user:Angelia.Hofbauer.rds@bsd.adds
CMDKEY: les informations d'identification ont été ajoutées correctement.
C:\Users\Angelia.Hofbauer\Desktop>mstsc.exe /v:srv-rd2
  
```

Activation du toutankhamon18.bat

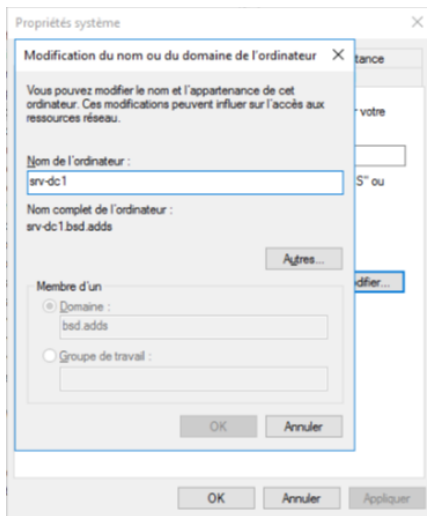
Depuis le poste client



Ouverture du bureau à distance du rds le mot de passe n'est rentrer que la première fois ou sur un changement donc la connexion est direct après le clique sur le fichier.bat



J. Procédure Windows



Tout d'abord, nous devons renommer les serveurs pour plus de facilité à reconnaître les différentes machines.

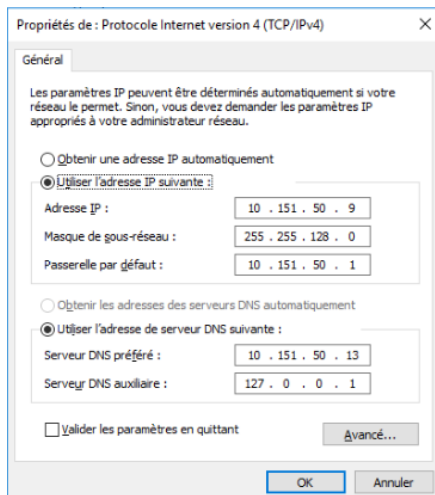
Redémarrage obligatoire des serveurs pour la prise en compte du changement de nom.



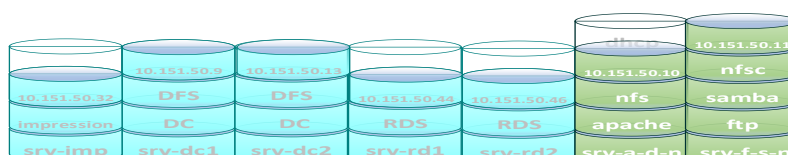
Puis, nous mettons un adressage IP fixe pour éviter que le DNS change.

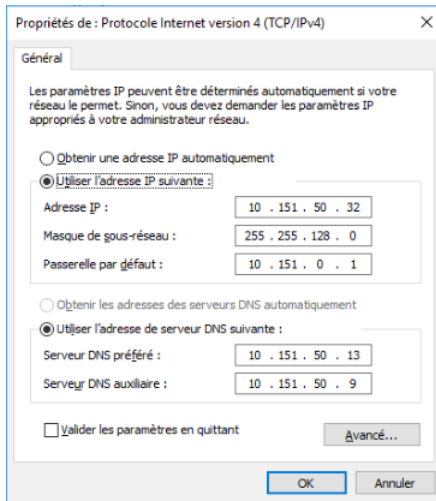
Pour le DNS, nous mettons en adresse préférée l'adresse IP du srv-dc2.

En adresse auxiliaire, nous mettons l'adresse IP locale du srv-dc1.



Nous devons réaliser la même démarche pour le srv-dc2.





Même chose pour les serveurs membres qui sont nommés :

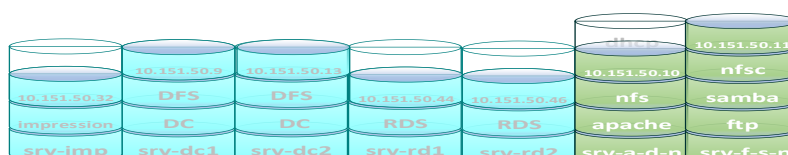
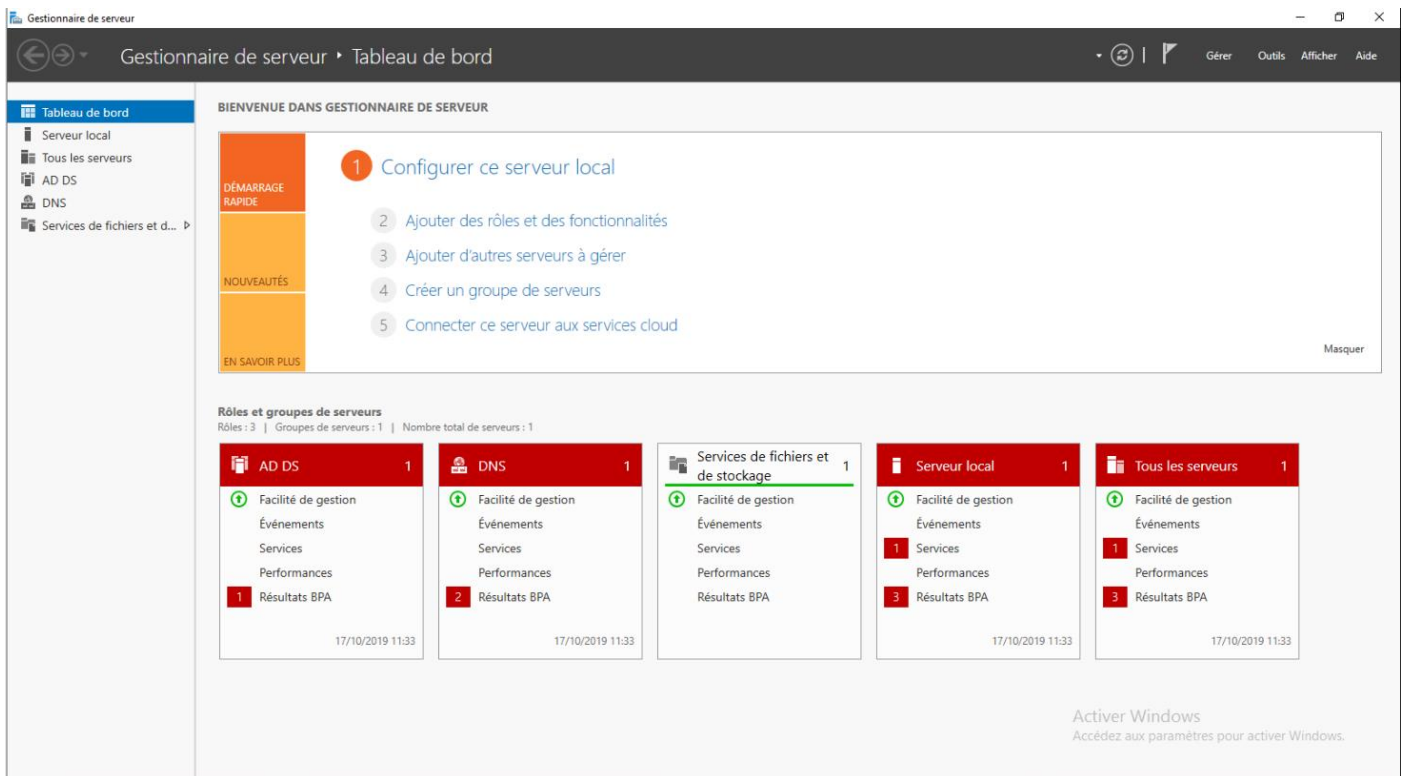
srv-imp

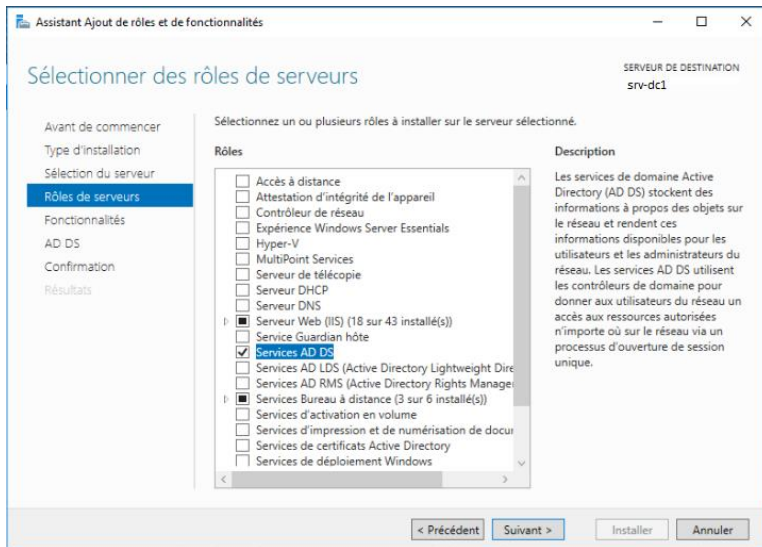
srv-rd1

srv-rd2

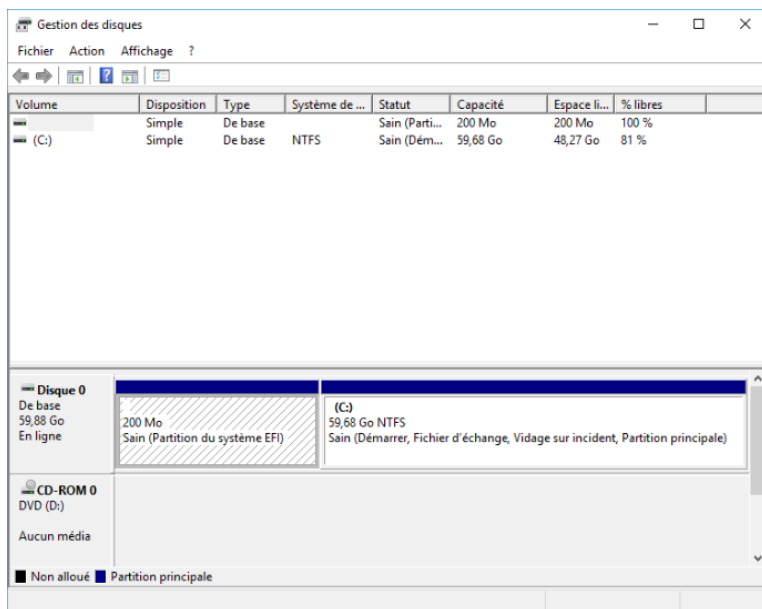
Sauf pour les DNS, nous attribuons les adresses IP des serveurs srv-dc1 et srv-dc2 pour pouvoir les joindre au domaine plus tard et ainsi avoir une tolérance de panne.

On s'intéresse maintenant au gestionnaire de serveur pour l'installation d'un Active Directory.

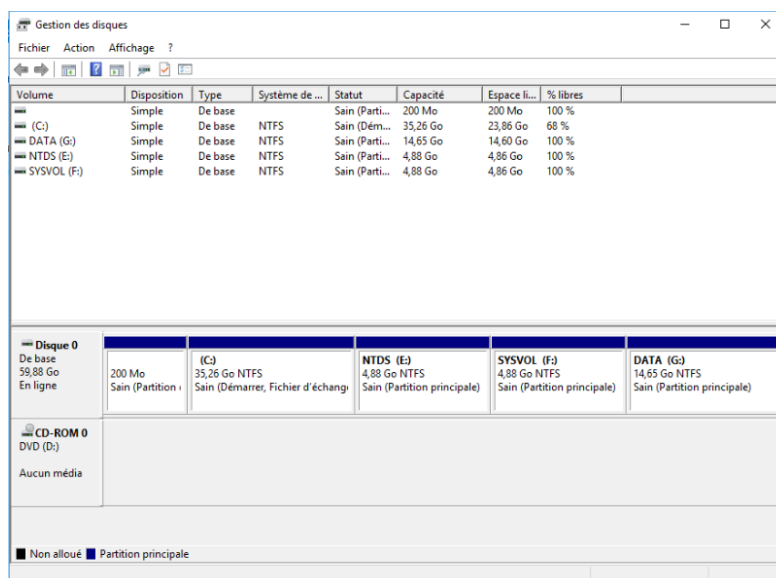




Dans l'assistant, nous ajoutons le rôle Services AD DS.



Une fois l'installation terminée, nous allons partitionner le disque dans la gestion des disques.

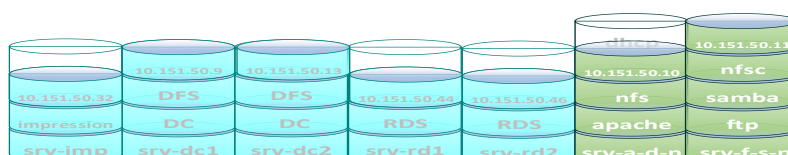


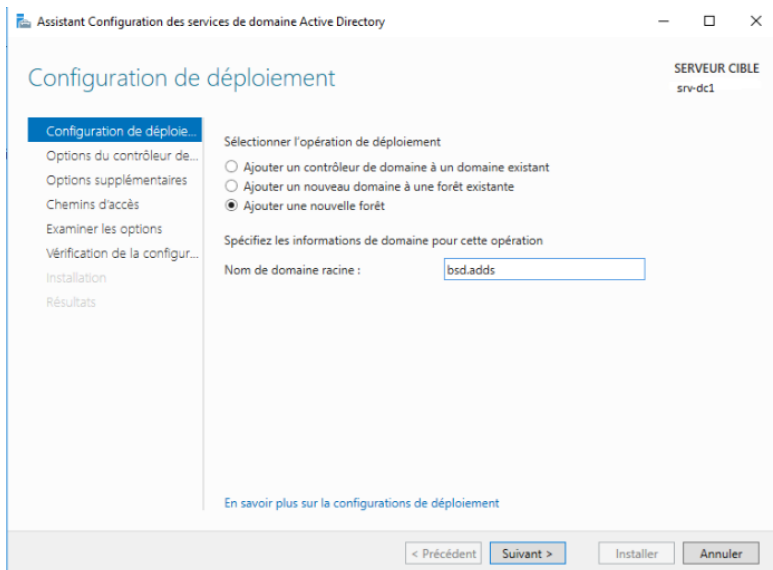
Nous avons donc créé 3 partitions supplémentaires.

NTDS contient l'annuaire de l'AD.

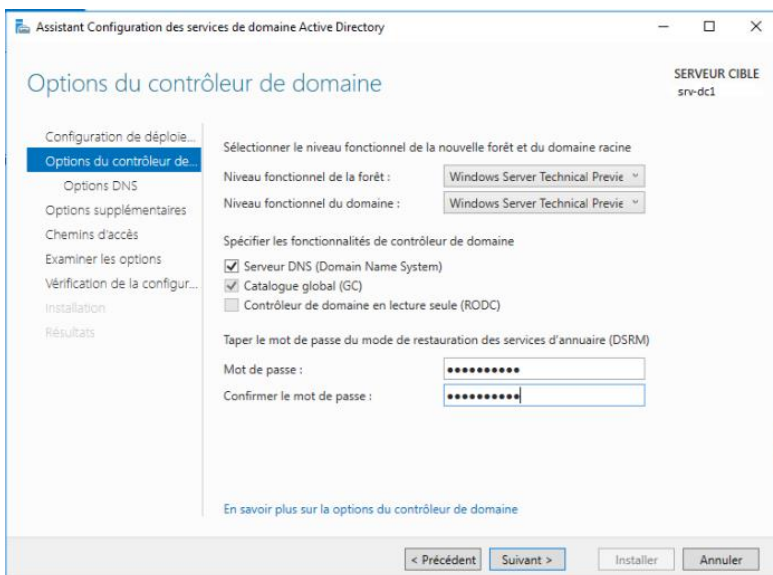
SYSVOL est le volume système du domaine.

DATA sera le volume de stockage des partages.

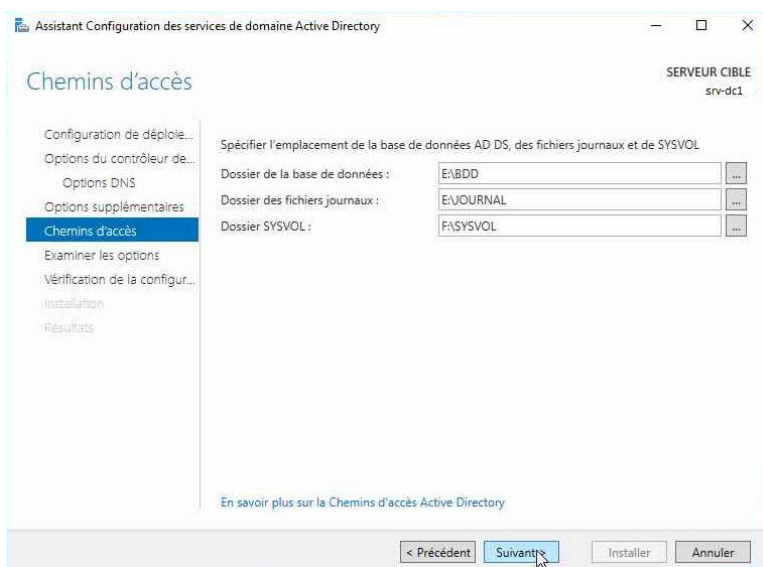




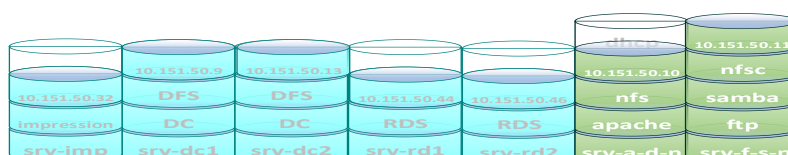
Dans l'assistant pour promouvoir le serveur au contrôleur de domaine, nous ajoutons une nouvelle forêt en donnant un nom de domaine. Ici notre nom de domaine est bsd.adds

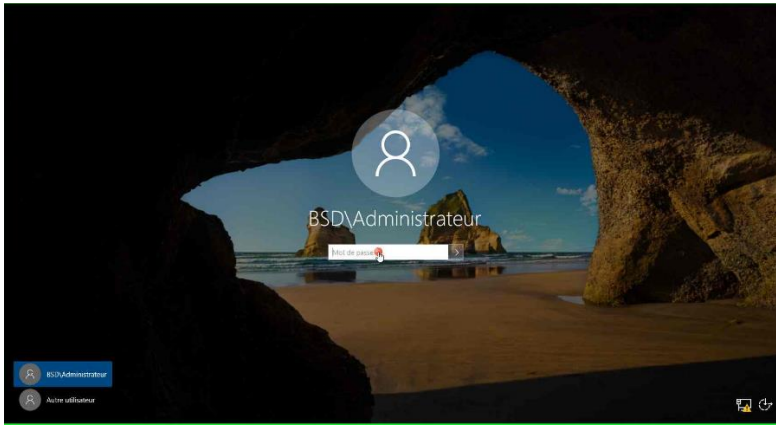


Pour le niveau fonctionnel de la forêt et du domaine, nous mettons notre version du windows server. Ici on installe le serveur DNS. Le srv-dc1 contiendra le catalogue globale (GC), annuaire de la forêt.

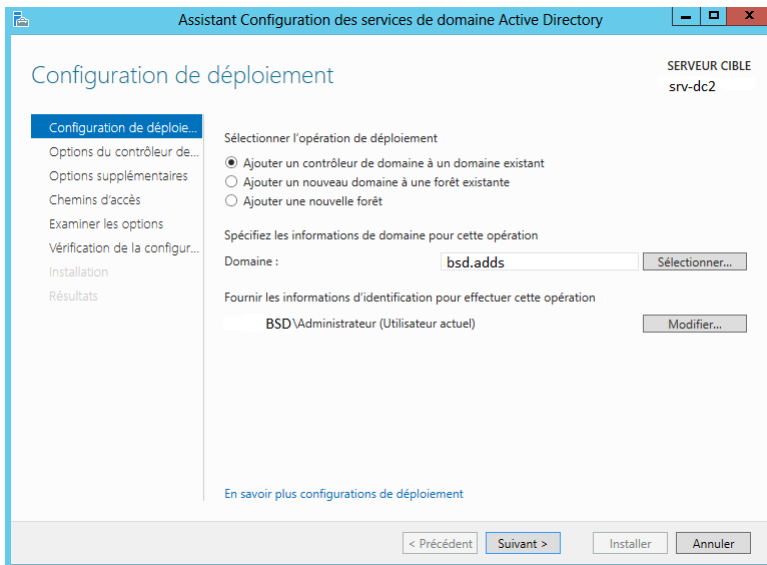


Ici nous choisissons le chemin où seront stockés la base de données, les fichiers journaux ainsi que le dossier SYSVOL. Une fois installé, il faut redémarrer le serveur.

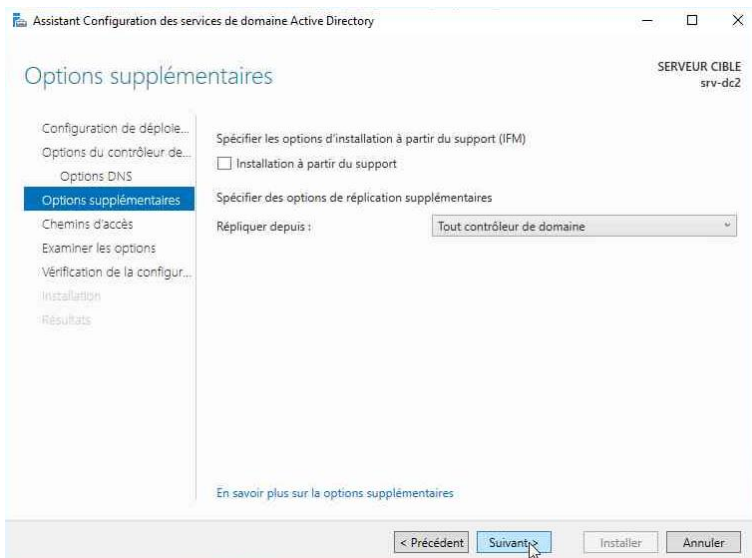




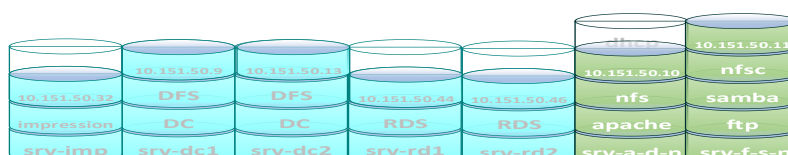
Nous pouvons maintenant nous connecter en tant qu'administrateur du domaine.

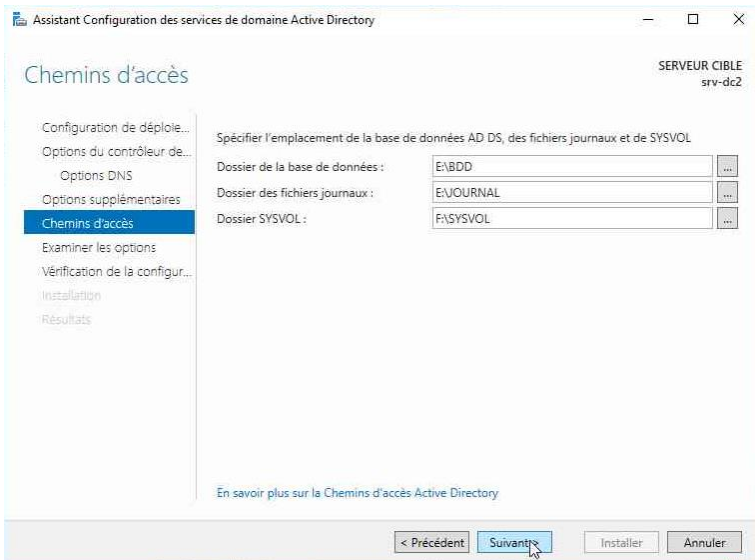


Après avoir installé L'AD DS et partitionné le disque sur le srv-dc2, nous ajoutons ce serveur en tant que contrôleur de domaine à un domaine existant. Nous indiquons seulement le nom du domaine.

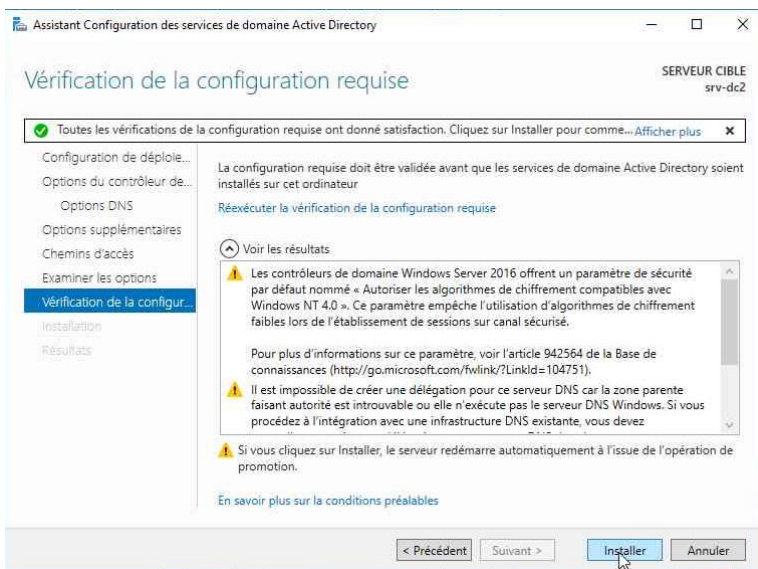


Nous indiquons que ce serveur doit être répliqué à tout contrôleur de domaine.





Comme pour le srv-dc1, nous choisissons le chemin pour la BDD, SYSVOL et les fichiers journaux.

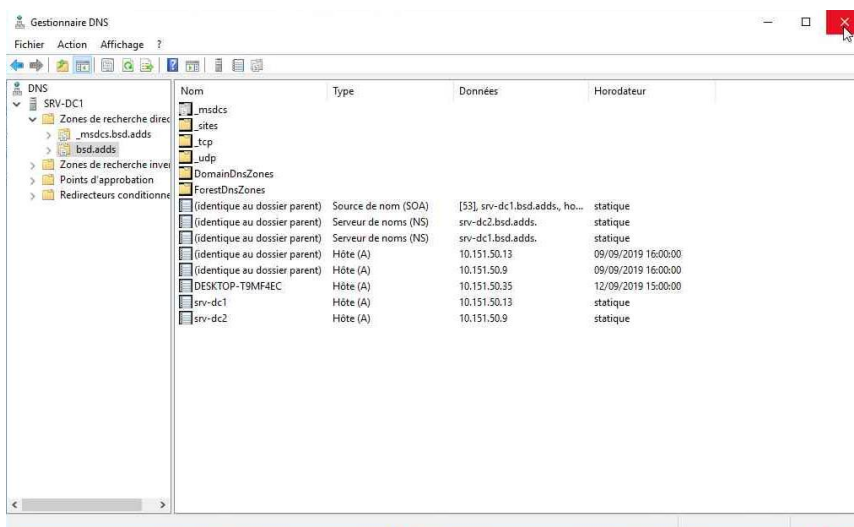


Une fois les vérifications faites, nous pouvons lancer l'installation.

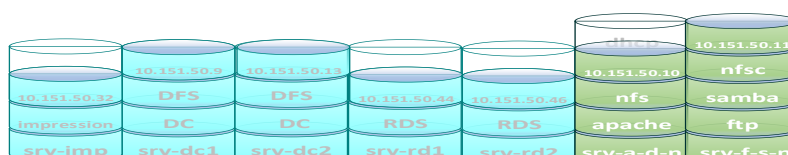
Redémarrage obligatoire après la fin de l'installation.

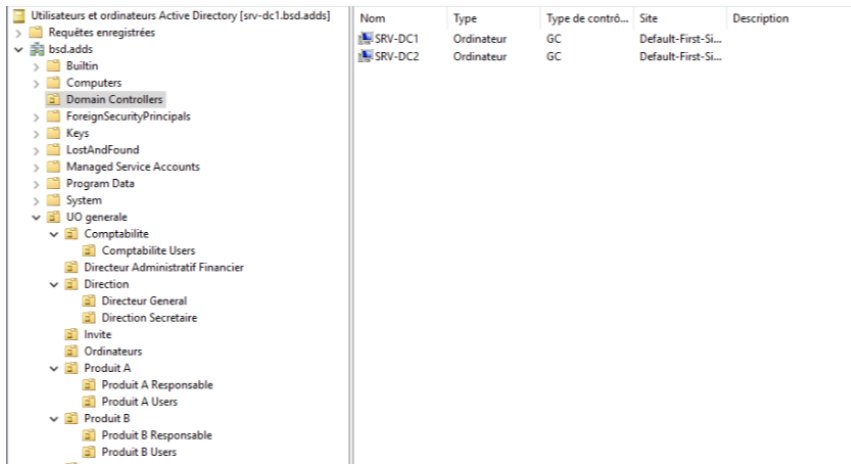
À partir de maintenant la redondance entre le srv-dc1 et le srv-dc2 est fonctionnelle.

Nous avons donc une tolérance de panne.



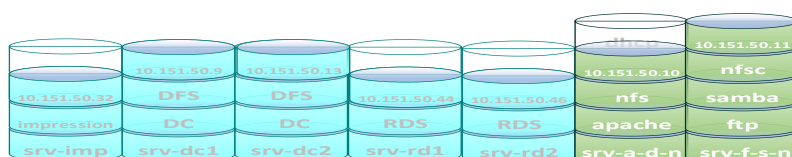
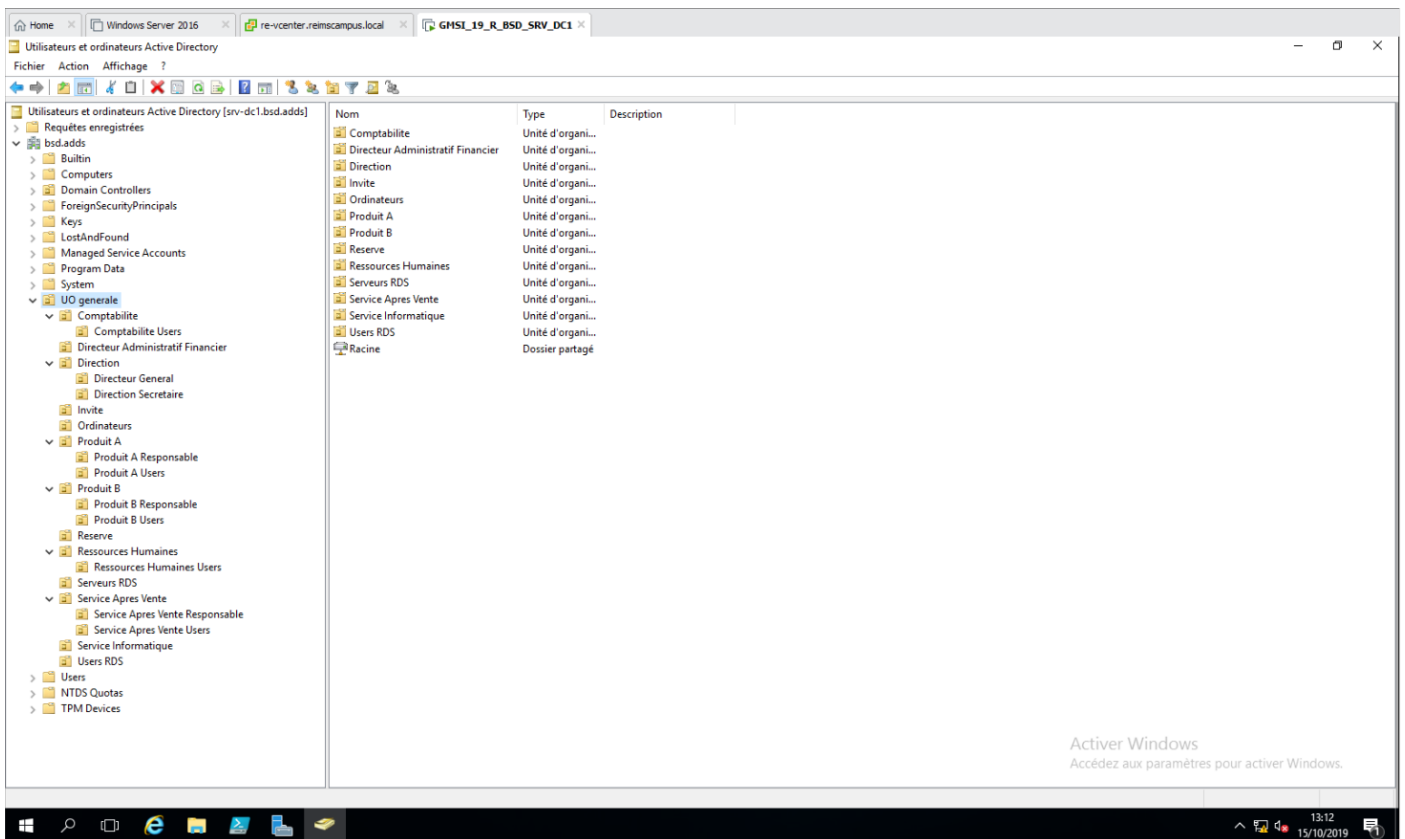
Après s'être connecté en tant qu'administrateur du domaine, nous vérifions dans le gestionnaire DNS si nos deux serveurs AD sont bien présents.





Même démarche dans Utilisateurs
et ordinateurs Active Directory,
section Domain Controller

Nous allons créer la structure de l'Active Directory. Pour cela, nous créons des Unités Organisationnelles (UO). Voici la structure de notre AD.



Voici un exemple de script pour créer les utilisateurs RDS.

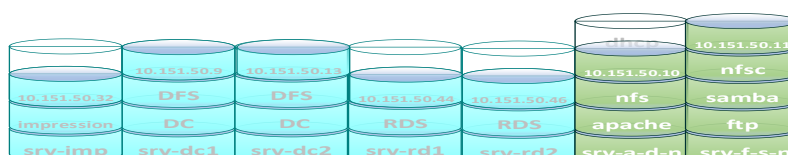
Nous avons un script global pour la création des utilisateurs, des groupes et des ordinateurs qui se rangent dans les UO correspondant à partir d'une base de données sur excel exportée en CSV.

```

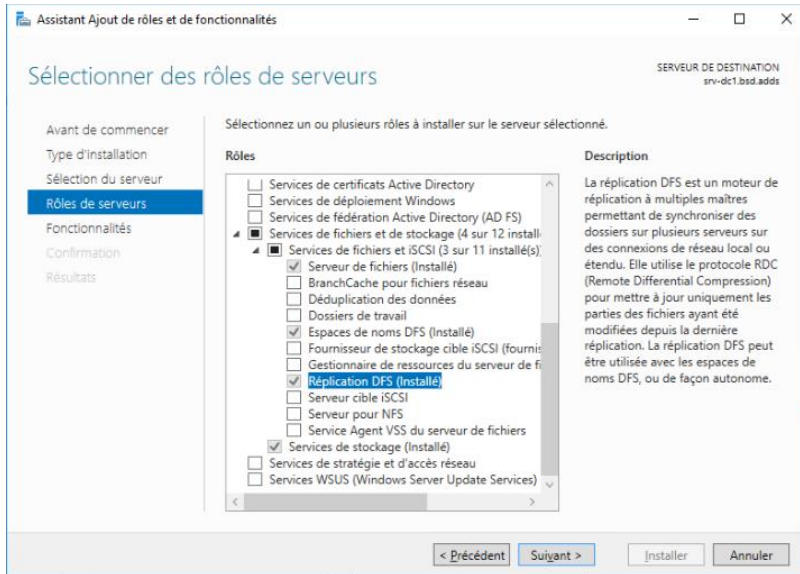
1 ##### CREATE_USERS.ps1 #####
2
3 $ErrorActionPreference = "Continue"
4 Clear-Host
5
6 Write-Host "##### Script de création Utilisateurs Toutankhamon18 #####" -BackgroundColor DarkGr
7
8 # Module AD
9 Import-Module ActiveDirectory
10
11 # Variables initiales
12 $File = "C:\Scripts\Utilisateurs_Toutankhamon18.csv"
13 $Domain = (Get-ADDomain).DNSRoot
14
15 # Actions
16 Import-Csv $File -Delimiter ";" | ForEach-Object {
17
18 Write-Host "#####" -BackgroundColor DarkGray
19
20 # Variables fixes
21 $Nom = $_.Nom
22 $Prenom = $_.Prenom
23 $Login = $_.Login
24 $RawPassword = $_.Password
25 $Service = $_.Service
26
27 # Variables complémentaires
28 $DN = "$Prenom $Nom"
29 $UPN = "$Login@$Domain"
30 $OU = (Get-ADOrganizationalUnit -Filter "Name -like '*$Service*') DistinguishedName
31
32 # Mot de passe
33 $Password = ConvertTo-SecureString $RawPassword -Force
34
35 # Création de l'utilisateur
36 New-ADUser -GivenName $Prenom -Surname $Nom -SamAccountName $Login -Name $DN -DisplayName $DN -L
37 -Path $OU -AccountPassword $Password -Enabled $true -PasswordNeverExpires $true -ChangePasswordA
38
39 # Vérification
40 if ($?) {Write-Host "Utilisateur $Login créé avec succès !" -BackgroundColor DarkGreen}
41 else {Write-Host "Erreur avec l'utilisateur Toutankhamon18 $Login !" -BackgroundColor DarkRed}
42
43 Write-Host "#####" -BackgroundColor DarkGray
44
45 }
46
47 Write-Host "##### FIN du Script #####" -BackgroundColor DarkGray
48
49 ##### ----- #####
50
  
```

```

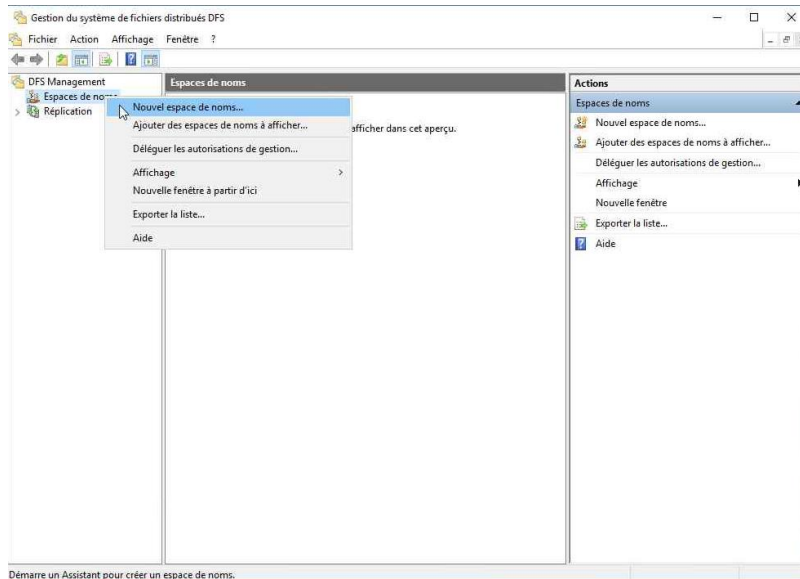
Utilisateur Farida.Saket.rds créé avec succès !
=====
Utilisateur Yan.Bubrig.rds créé avec succès !
=====
Utilisateur Maxime.testi.rds créé avec succès !
=====
Utilisateur bertrand.Quantat.rds créé avec succès !
=====
Utilisateur Wayne.Shivers.rds créé avec succès !
=====
Utilisateur Kristal.Bothe.rds créé avec succès !
=====
Utilisateur Florencia.Stadel.rds créé avec succès !
=====
Utilisateur Darrin.Tumolillo.rds créé avec succès !
=====
Utilisateur Freeman.Rudig.rds créé avec succès !
=====
Utilisateur Ellsworth.Rieg.rds créé avec succès !
=====
Utilisateur Greg.Ioizel.rds créé avec succès !
=====
Utilisateur Frederic.Leroux.rds créé avec succès !
=====
Utilisateur Arlette.Torchio.rds créé avec succès !
=====
===== FIN du Script =====
  
```



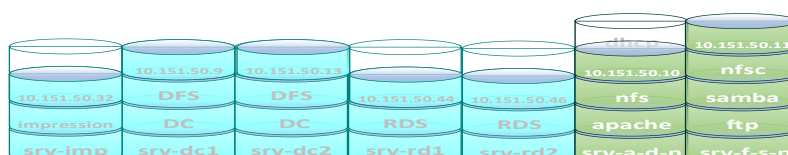
Nous allons nous intéresser sur le rôle DFS qui est un système de fichiers partagés.

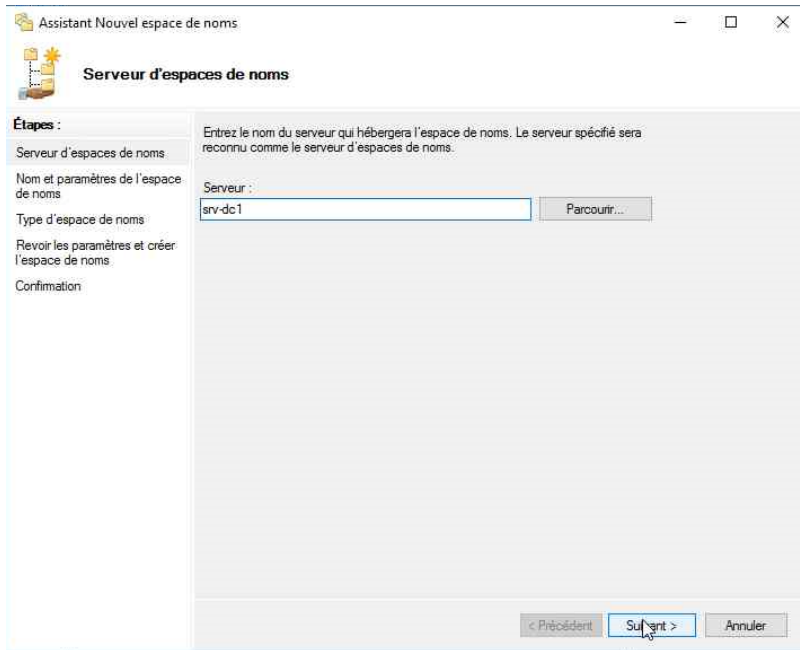


Nous choisissons Espaces de noms DFS ainsi que la réplication DFS.

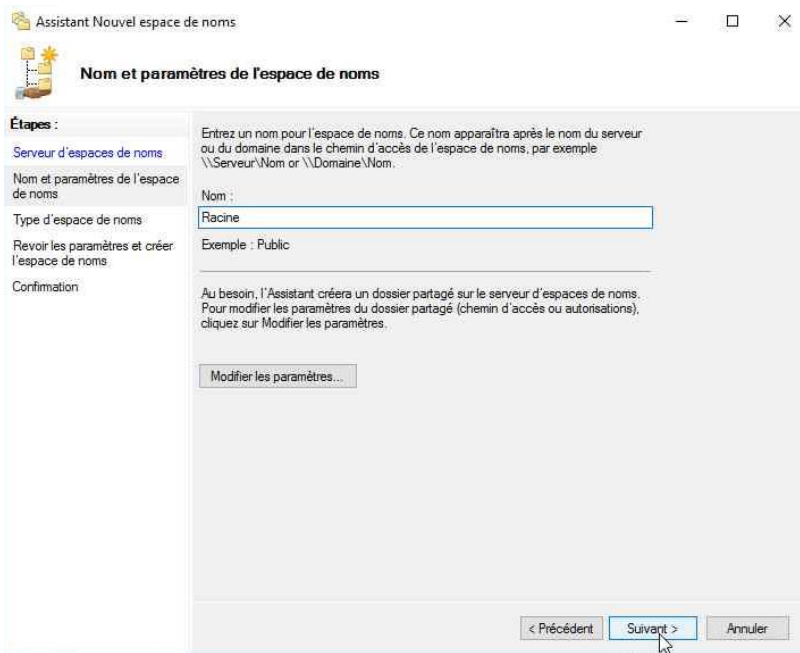


Une fois l'installation terminée, nous pouvons aller dans le gestionnaire DFS pour créer un nouvel espace de noms.

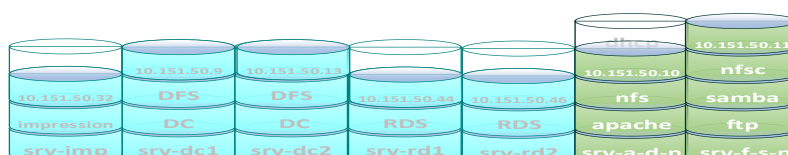


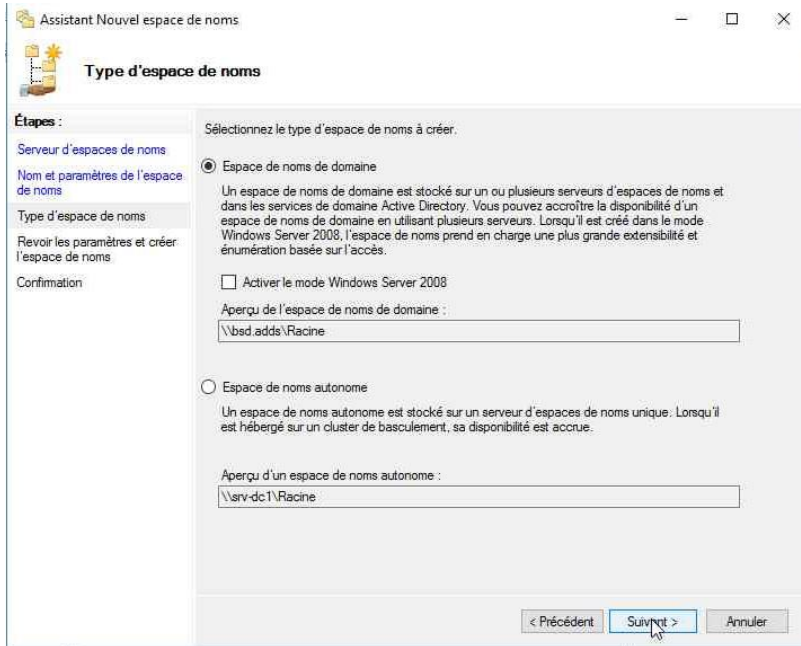


Nous indiquons le serveur qui hébergera l'espace de noms.
 Dans notre cas, ce sera srv-dc1.

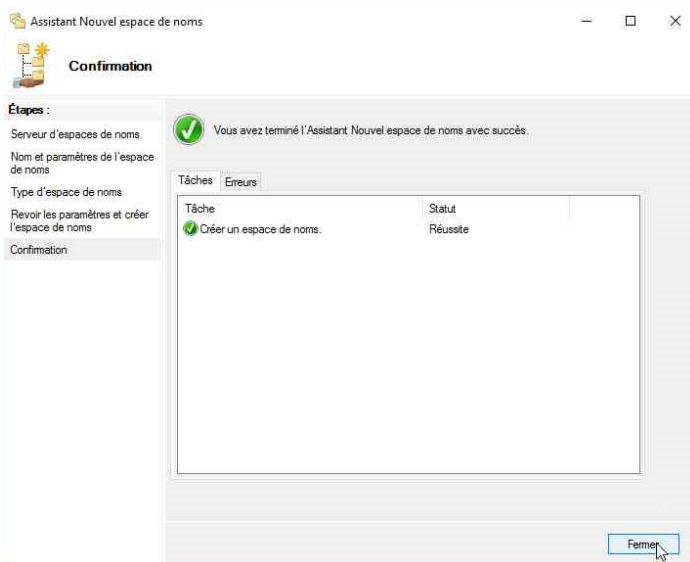


Nous donnons un nom à cet espace.
 Nous l'appelons « Racine »

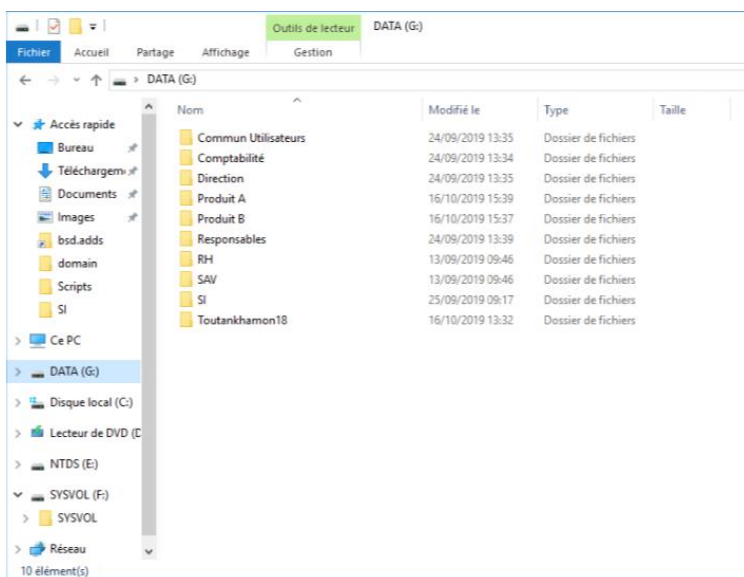




Nous sélectionnons « Espace de noms de domaine »

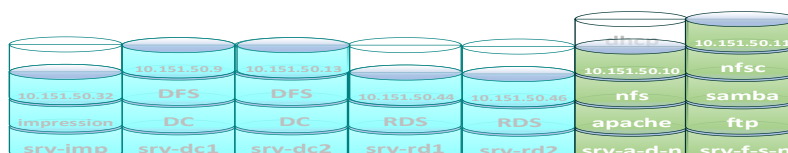


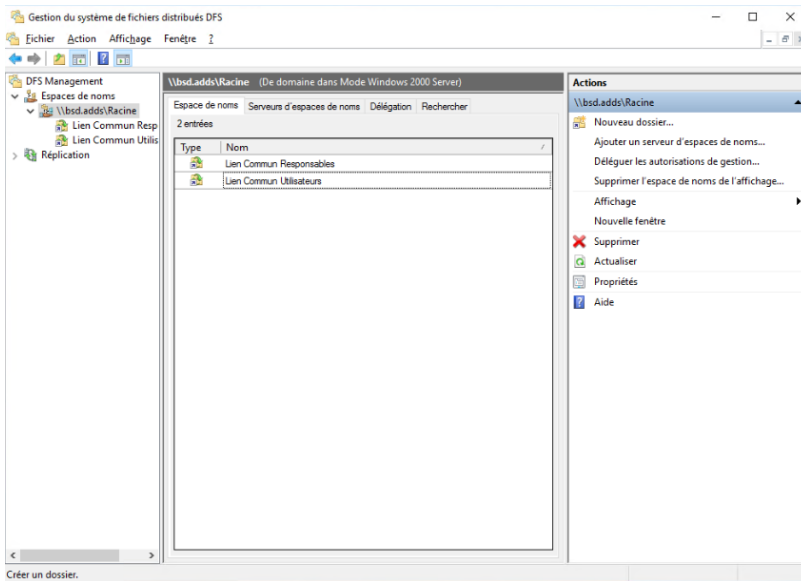
L'espace de nom est créé avec succès.



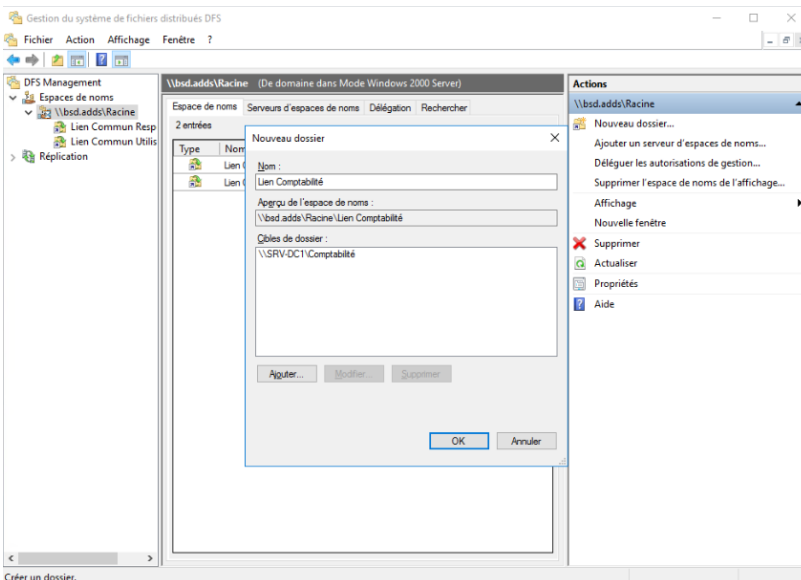
Nous allons créer les dossiers partagés sur le DATA pour les utilisateurs de l'entreprise sur srv-dc1.

Nous faisons de même sur srv-dc2 avec les mêmes noms suivis d'un bis.



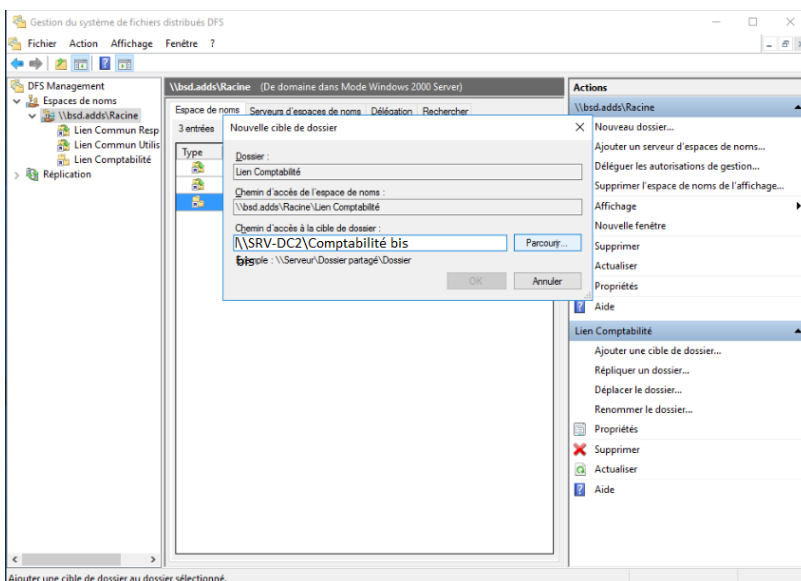


Nous pouvons dès à présent créer les liens pour la réplication des dossiers partagés.

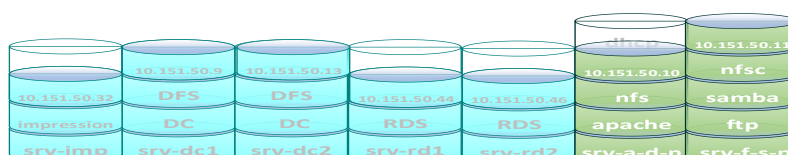


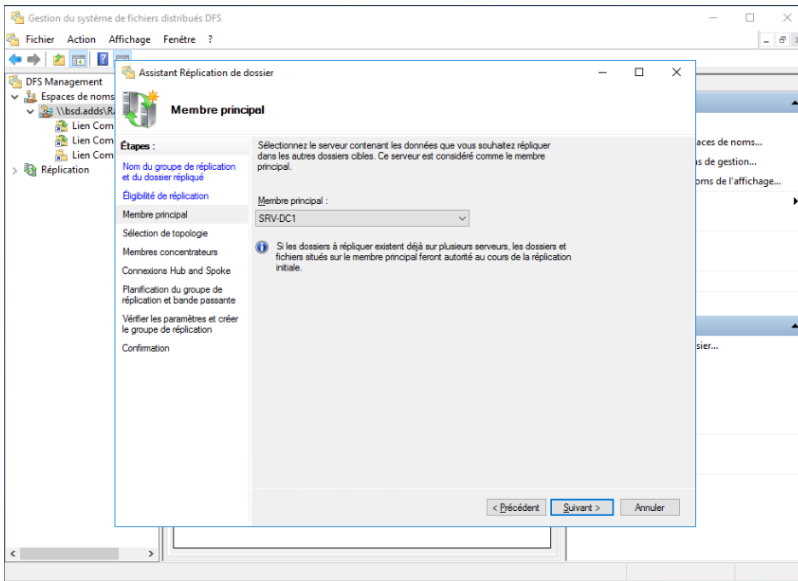
Nous mettons le nom du lien ainsi que la cible du dossier.

Ici nous choisissons le dossier partagé « Comptabilité » du srv-dc1.

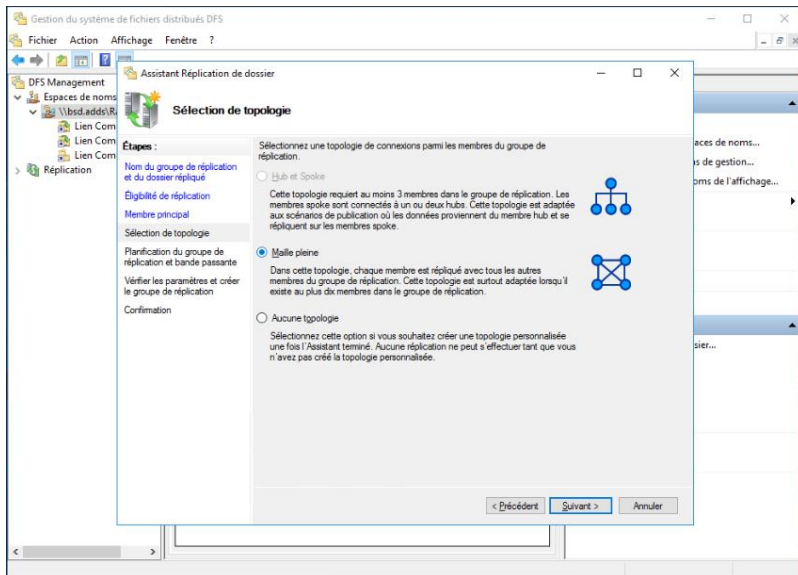


Nous effectuons le lien avec srv-dc2 du dossier partagé « Comptabilité bis » pour créer la réplication entre ces deux dossiers.

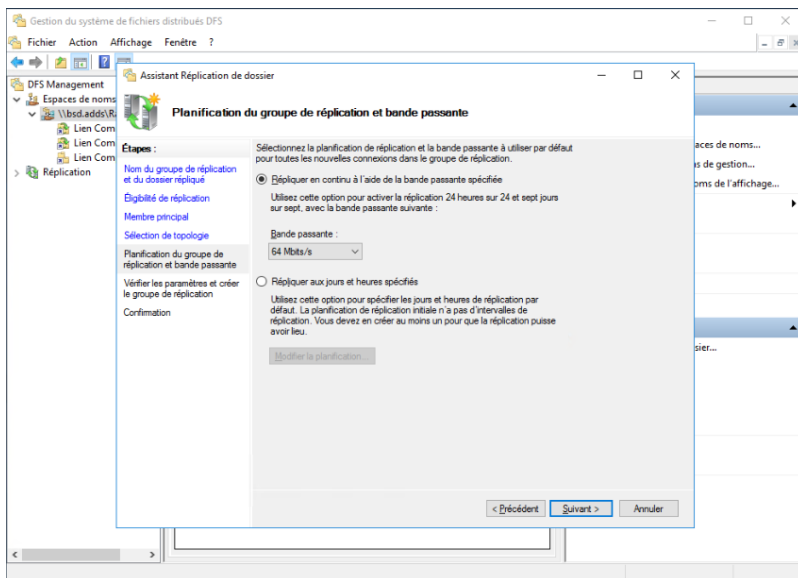




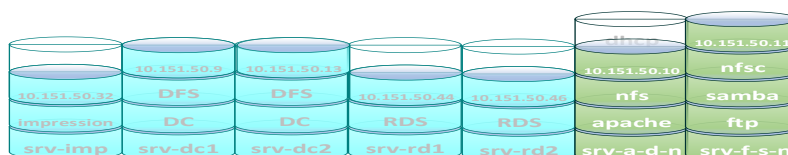
L'assistant se lance automatiquement.
 Nous choisissons le serveur membre principal.
 Ici ce sera « srv-dc1 ».

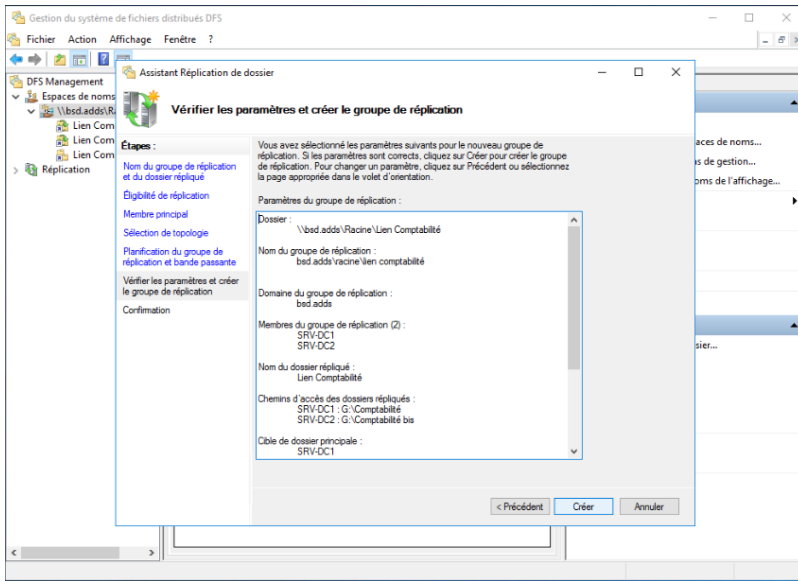


Pour la tolérance de panne, nous choisissons « Maille pleine » pour une réplication optimale.

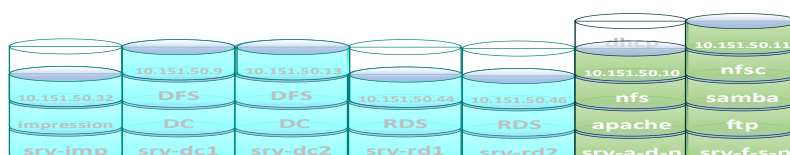


Nous choisissons la taille de la bande passante pour une réplication plus ou moins rapide suivant le débit.

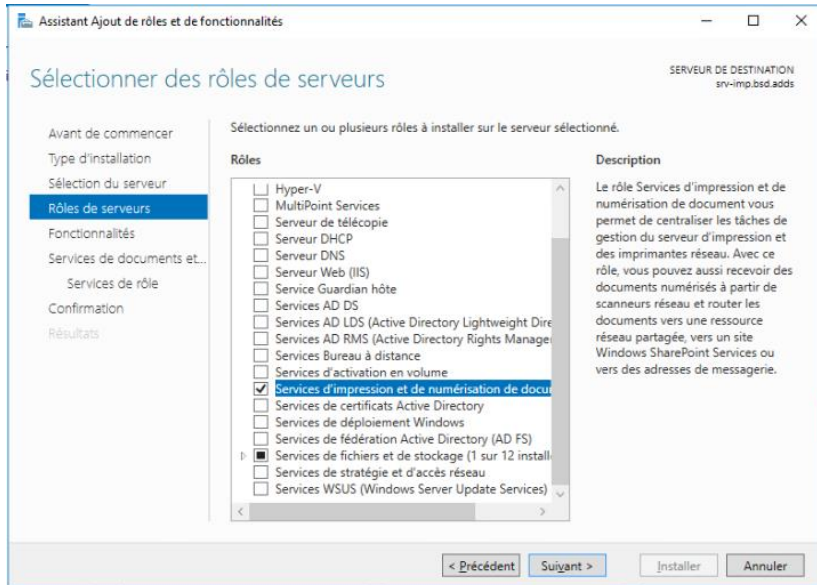




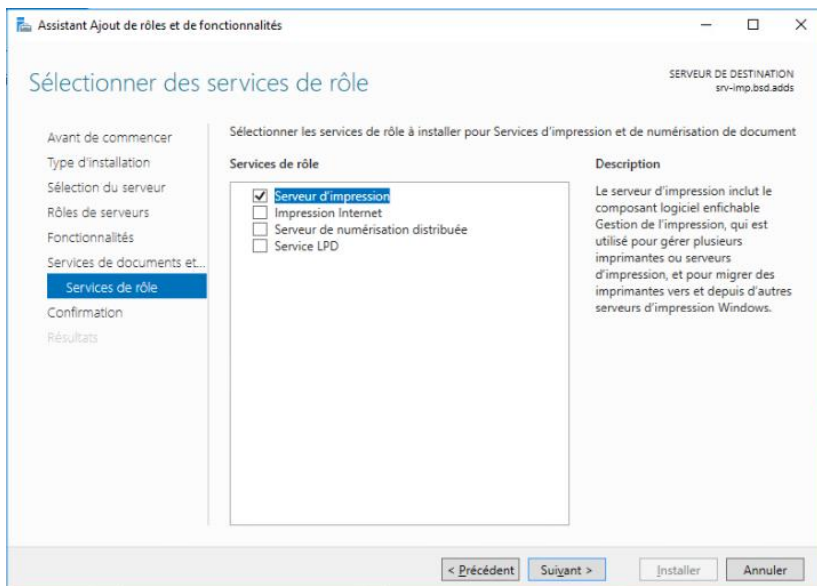
La réplication est bien créée.
Il faut répéter les précédentes étapes
pour chaque dossier partagé.



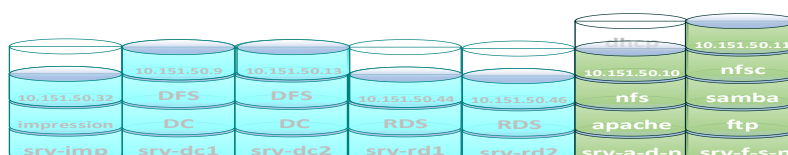
Passons maintenant à l'installation d'un nouveau serveur pour la gestion des imprimantes en réseau.

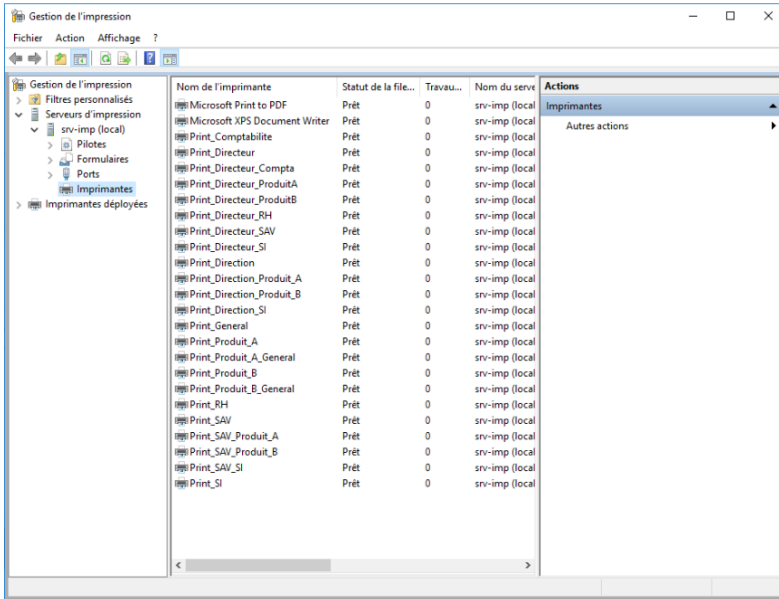


Après avoir renommé, adressé les IP et rejoint le serveur membre IMP au domaine, nous sélectionnons comme rôle les « services d'impression et de numérisation de documents »

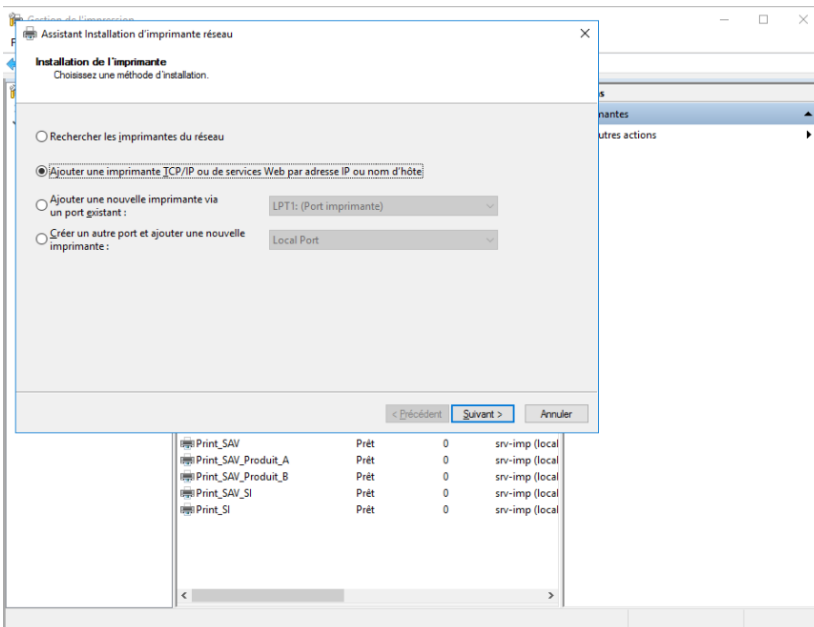


Dans la partie « Services de rôle » nous sélectionnons « Serveur d'impression »

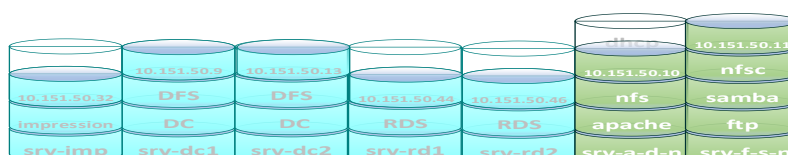


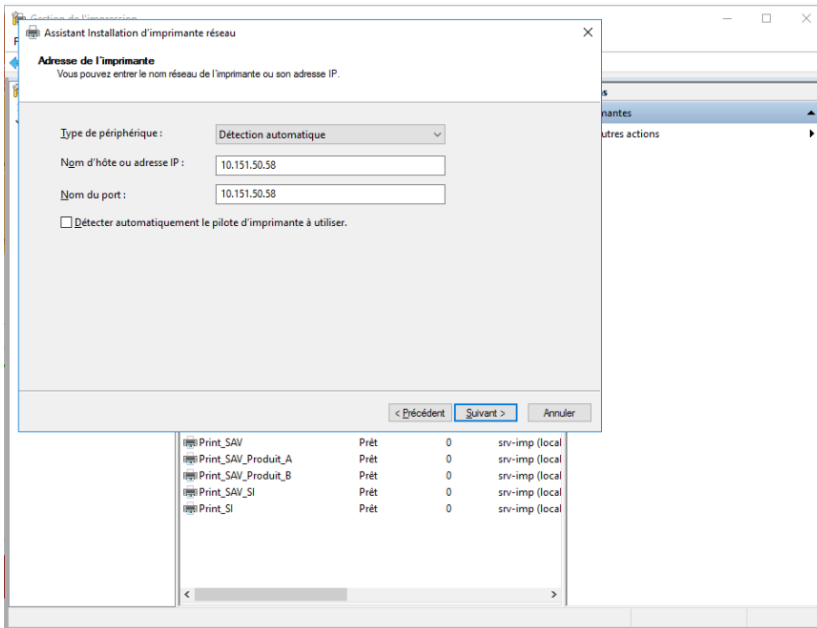


Une fois l'installation terminée, nous pouvons aller dans la gestion de l'impression pour ajouter nos imprimantes sur le réseau.

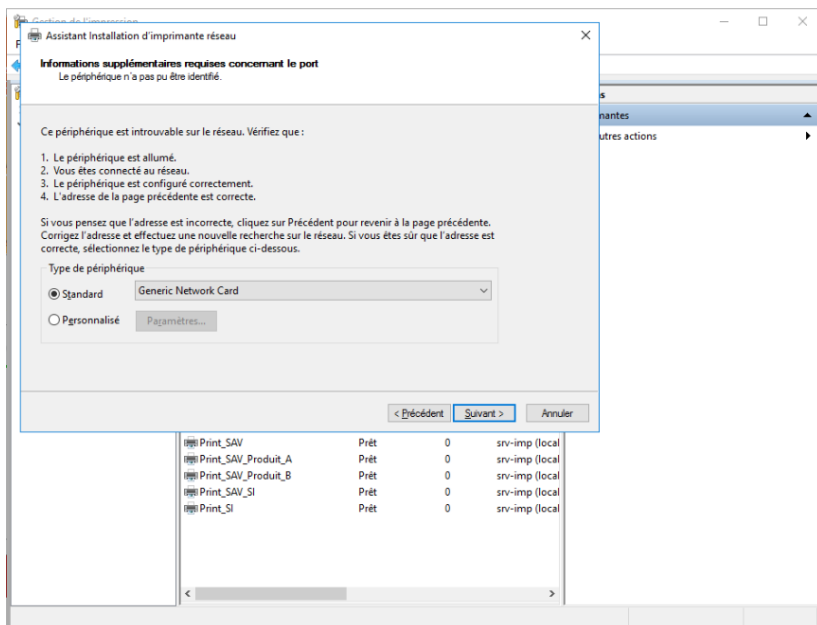


Nous pouvons ajouter une nouvelle imprimante via un port existant mais dans notre cas nous ajoutons une imprimante TCP/IP par adresse IP ou nom d'hôte.

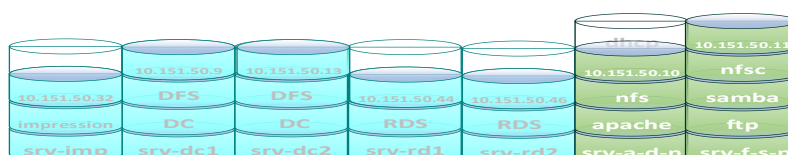


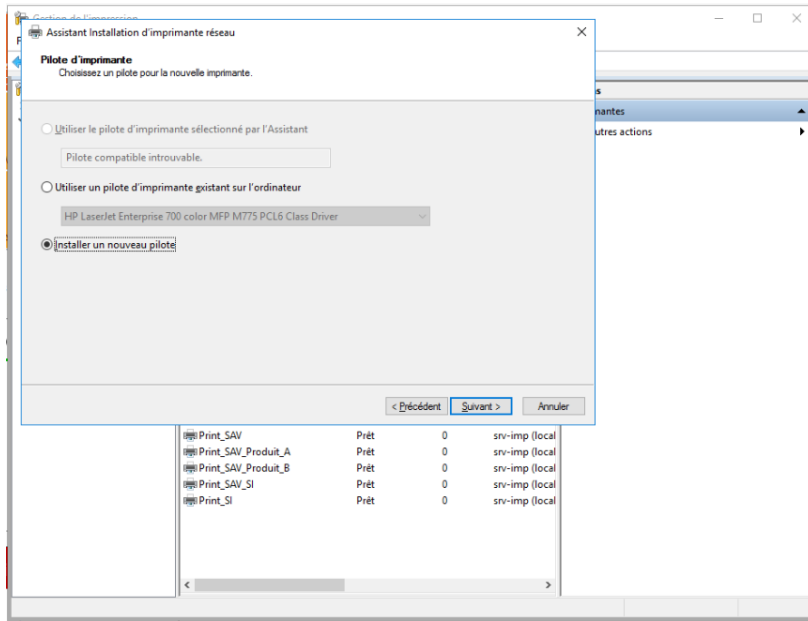


Nous indiquons le nom d'hôte ou l'adresse IP de l'imprimante.



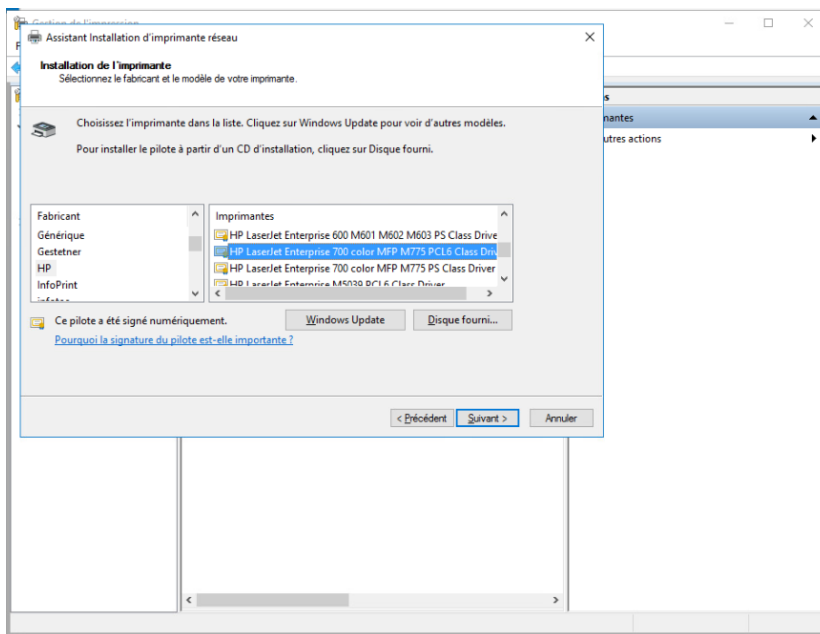
Nous sélectionnons comme type de périphérique standard « Generic Network Card »



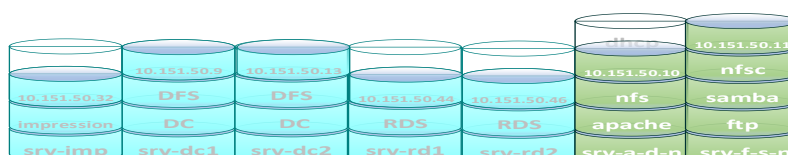


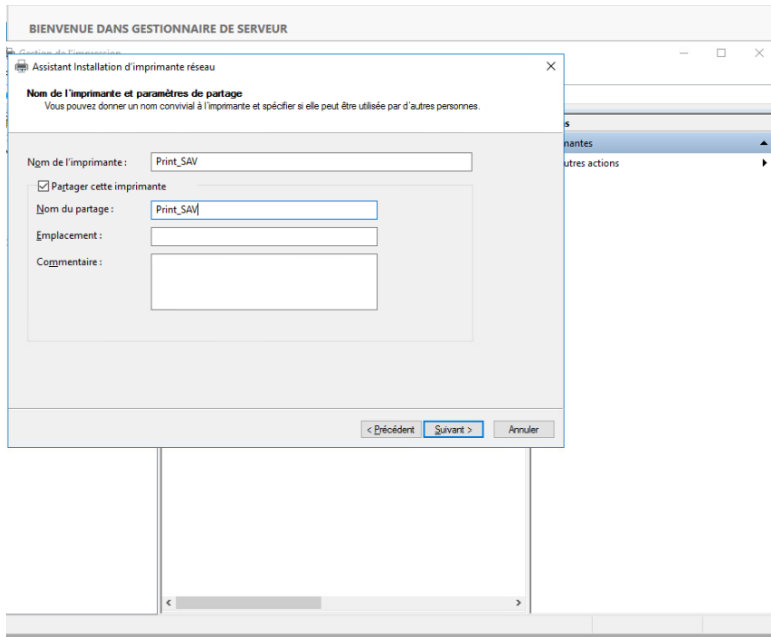
Comme nous n'avons aucun pilote d'installer, nous en ajoutons un nouveau.

Par la suite nous pourrons choisir d'utiliser le nouveau pilote installé.



Dans notre cas, nous choisissons le pilote « HP LaserJet Enterprise 700 color MFP M775 PCL6 Class Driver »



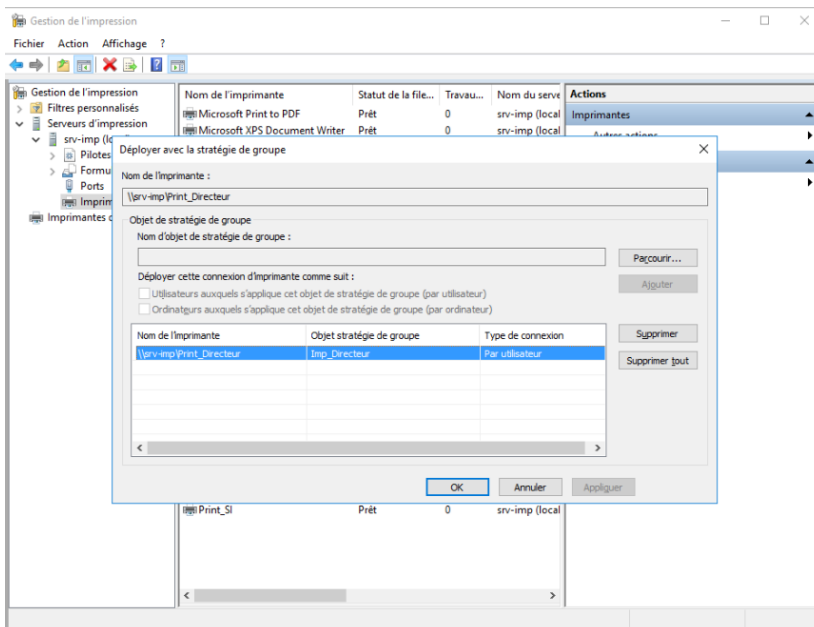


Nous choisissons le nom de l'imprimante.

Pour le service SAV, ce sera « Print_SAV »

Pour le service RH, ce sera « Print_RH »

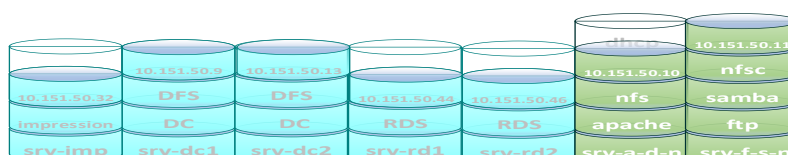
Etc...

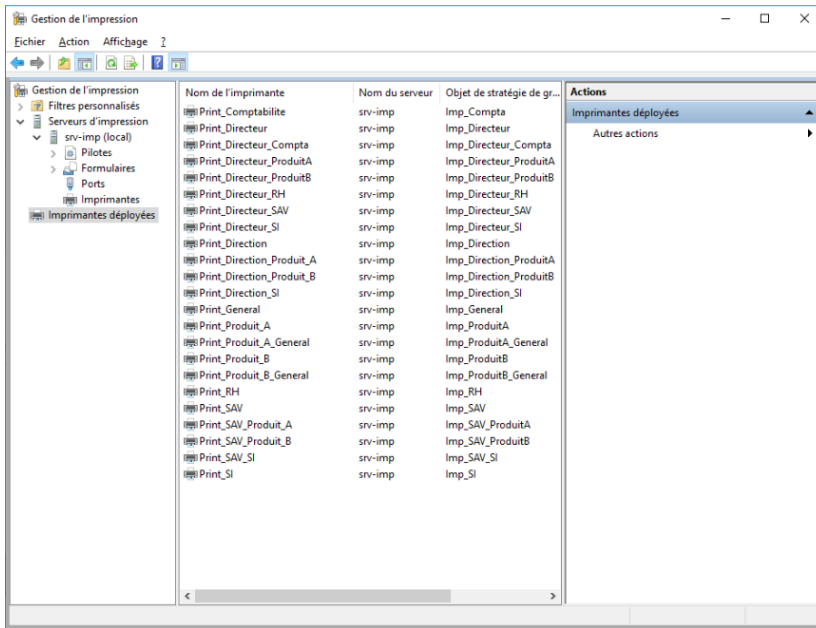


Maintenant que l'imprimante est installée, il faut la déployer.

Pour cela, nous choisissons de déployer avec une stratégie de groupe (GPO) sur l'imprimante en question.

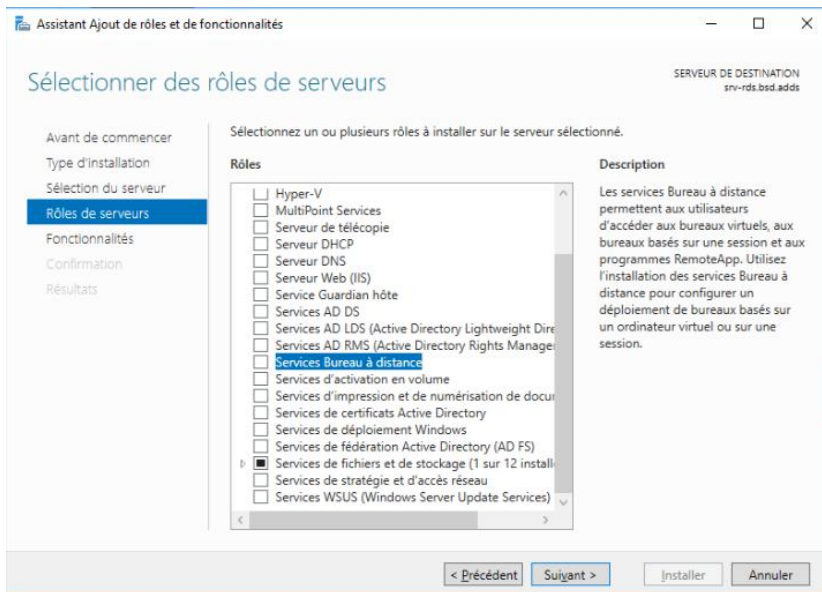
Et nous plaçons cette GPO dans l'UO correspondante.



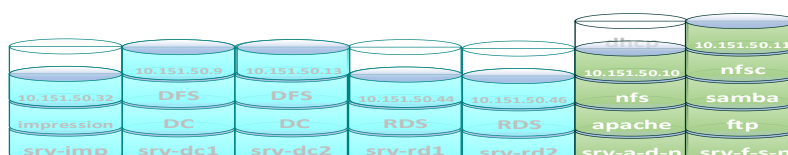


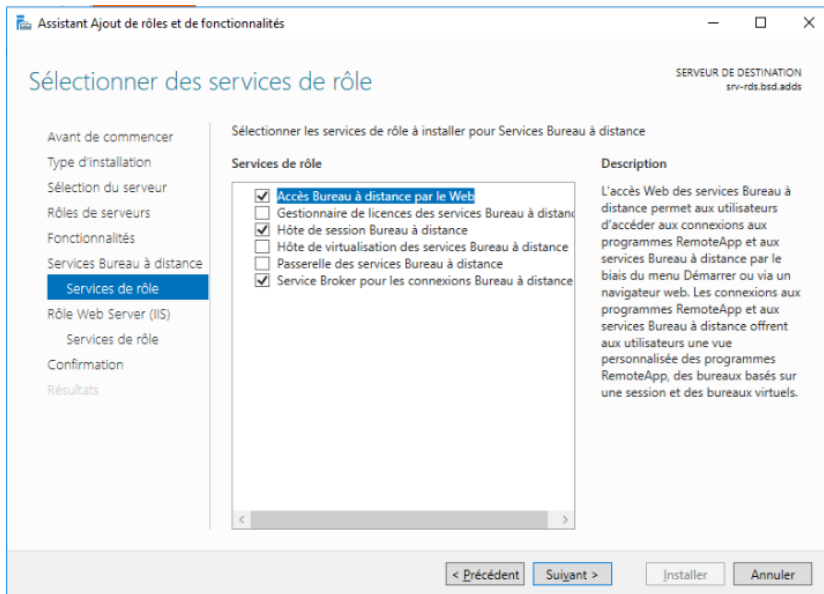
Ceci fait, les imprimantes sont déployées sur tout le réseau de l'entreprise BSD.

Passons maintenant à l'installation d'un nouveau serveur pour l'accès à distance du bureau sécurisé RDS.



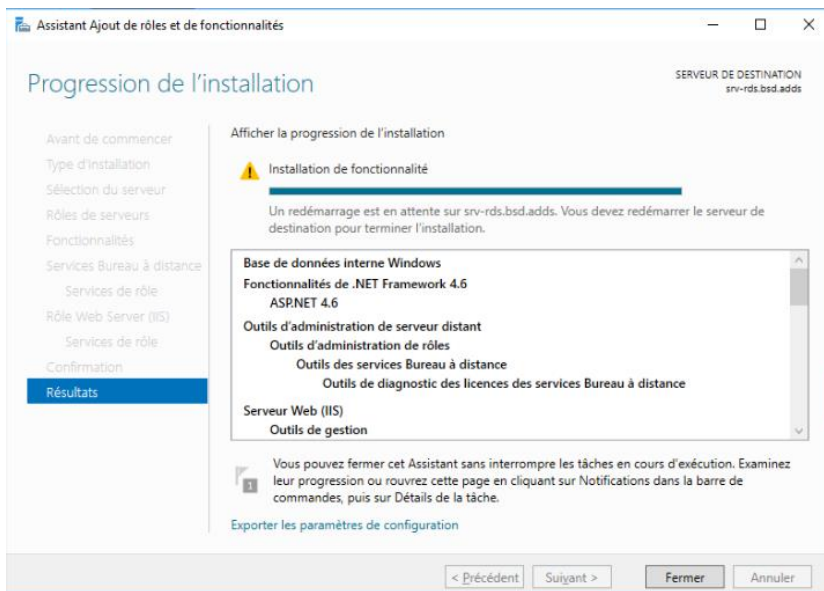
Après avoir renommé, adressé les IP et rejoint le serveur membre RDS au domaine, nous sélectionnons comme rôle « Service Bureau à distance »



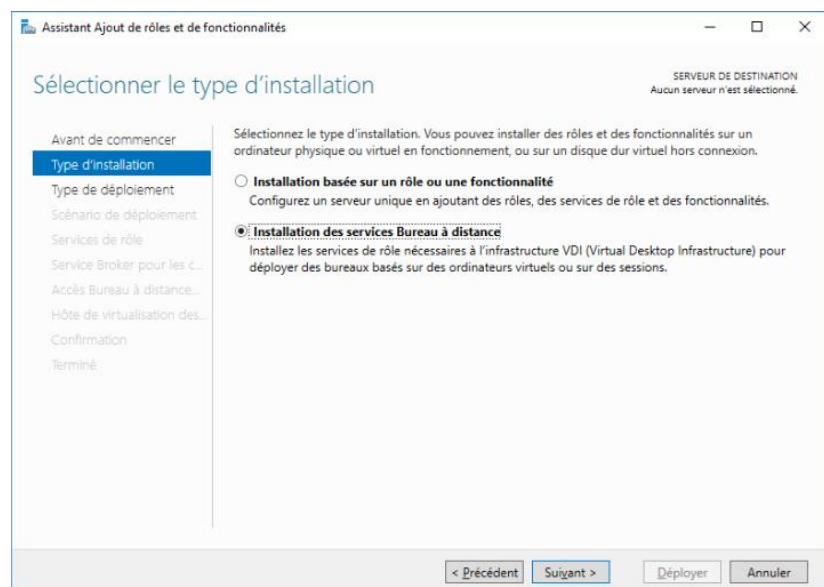


Pour les services de rôle, nous choisissons :

- * Accès Bureau à distance par le web
- * Hôte de session Bureau à distance
- * Service Broker pour les connexions Bureau à distance

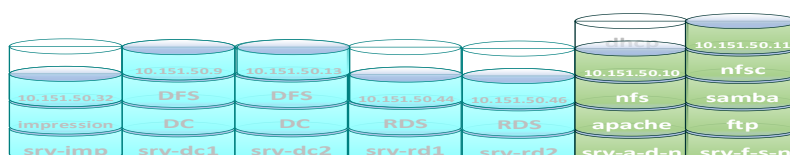


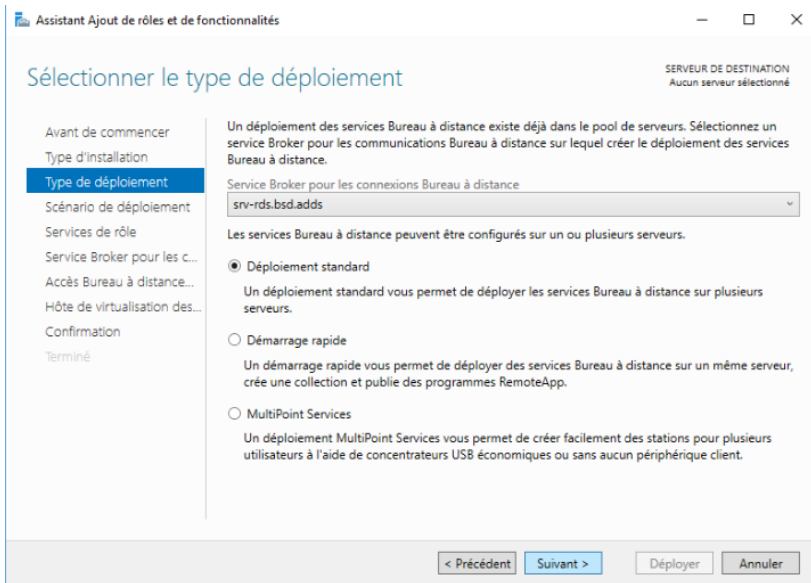
Attendre la fin de l'installation pour redémarrer le serveur.



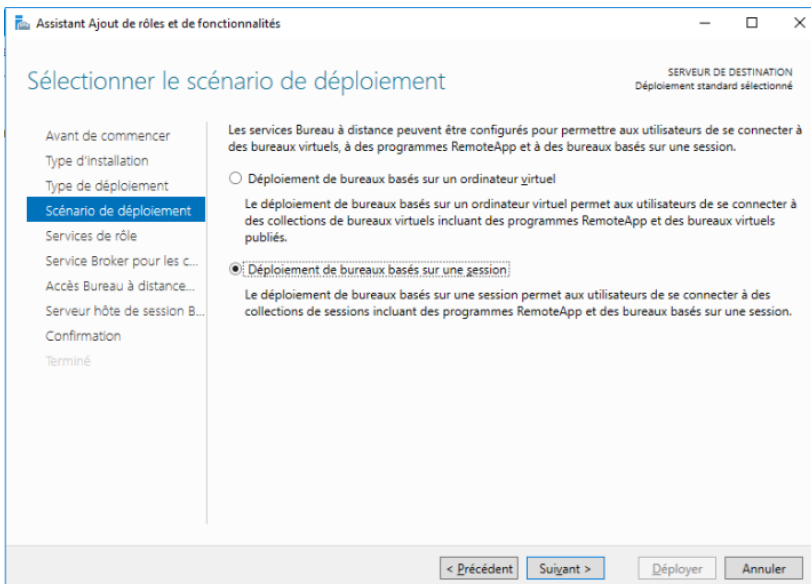
Passons au déploiement.

Dans l'ajout de rôles et de fonctionnalités, nous sélectionnons « Installation des services Bureau à distance »

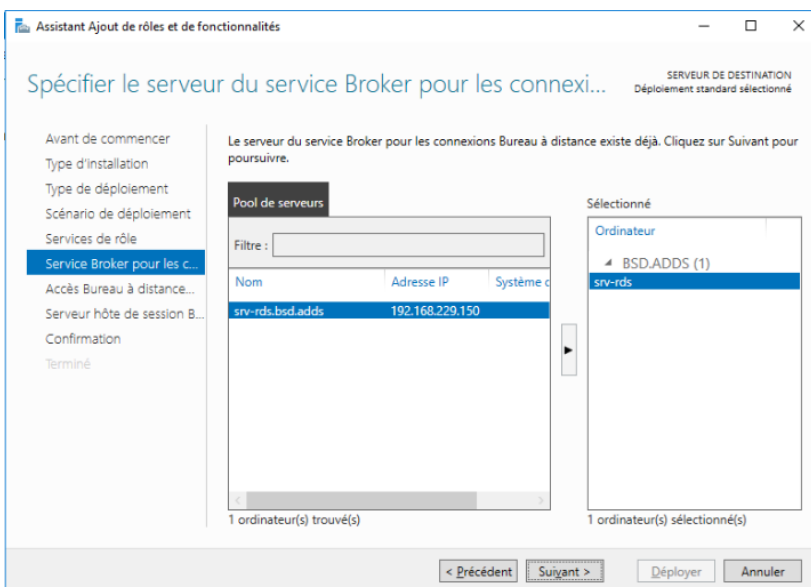




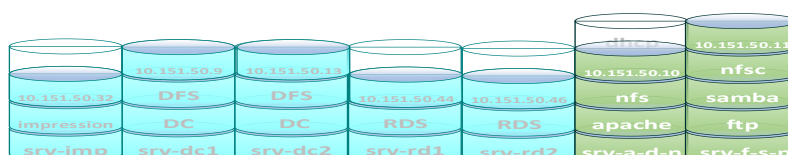
Le service Broker est un prérequis pour le bon fonctionnement d'un serveur RDS.
Nous choisissons un déploiement standard.

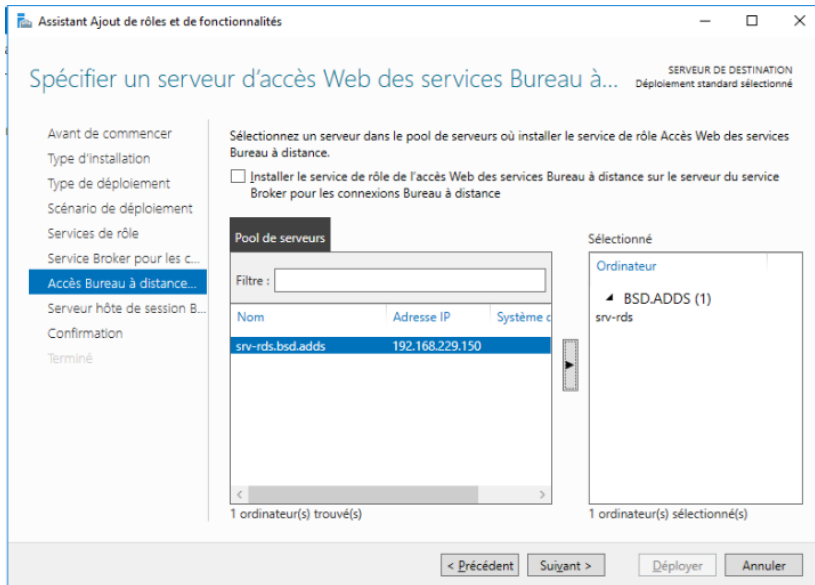


Nous choisissons ici « Déploiement de bureaux basés sur une session ».

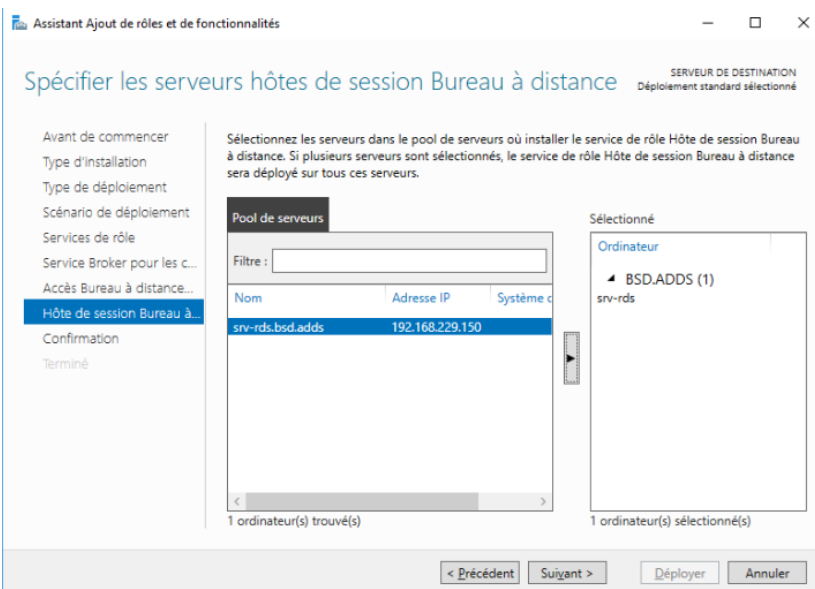


Nous sélectionnons le serveur du service Broker pour les connexions Bureau à distance.

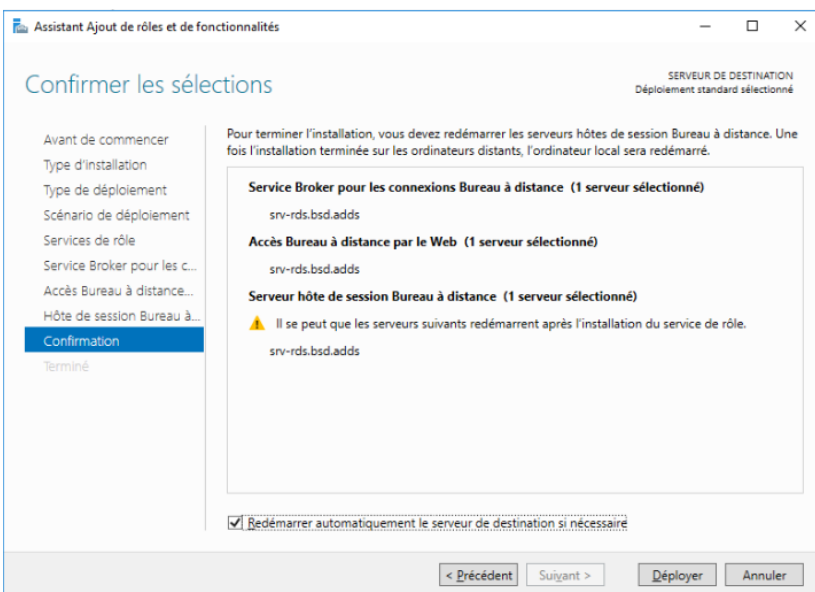




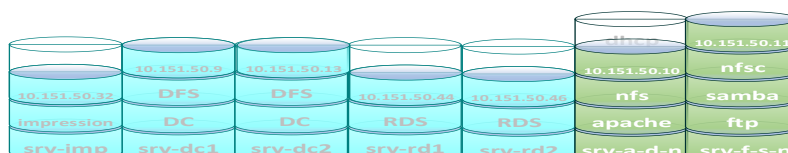
Nous sélectionnons le serveur d'accès Web pour les services Bureau à distance.



Nous sélectionnons le serveur hôte de session Bureau à distance.



Nous pouvons confirmer le déploiement et redémarrer le serveur.

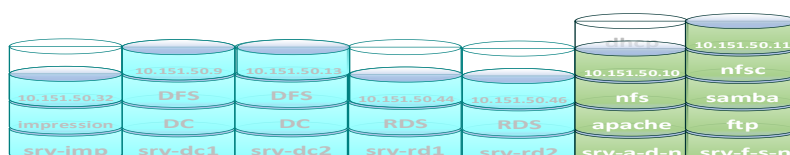


Voilà une vue d'ensemble du serveur RDS après déploiement.

The screenshot displays the 'PRISE EN MAIN DES SERVICES BUREAU À DISTANCE' (Getting Started with RemoteApp and Desktop Connections) wizard. It includes a navigation pane on the left with 'Vue d'ensemble', 'Serveurs', and 'Collections'. The main area shows a 3-step process: 1. Configurer un déploiement pour les services Bureau à distance (Configure deployment for RemoteApp and Desktop Connections), 2. Ajouter des serveurs hôtes de session Bureau à distance (Add RemoteApp and Desktop session host servers), and 3. Créer des collections de sessions (Create session collections). Below this, the 'VUE D'ENSEMBLE DU DÉPLOIEMENT' (Deployment Overview) shows a hierarchy: 'Accès Bureau à distance' (RemoteApp and Desktop Connections) at the top, connected to 'Passerelle des services' (Service Gateway) and 'Gestionnaire de licences' (License Manager), which both connect to 'Service Broker pour les connexions Bureau à distance' (RemoteApp and Desktop Connection Service Broker). This broker then connects to 'Serveur hôte de session virtuel' (Virtual session host server) and 'Serveur hôte de session' (Session host server). To the right, the 'SERVEURS DE DÉPLOIEMENT' (Deployment Servers) table lists the installed services for the server 'SRV-RDS.BSD.ADDS':

Nom de domaine complet du serveur	Service de rôle installé
SRV-RDS.BSD.ADDS	Service Broker pour les connexions Bureau à distance
SRV-RDS.BSD.ADDS	Hôte de session Bureau à distance
SRV-RDS.BSD.ADDS	Accès Web des services Bureau à distance

Figure XIII-24 vue d'ensemble RDS



Pour que les utilisateurs puissent se connecter au bureau sécurisé à distance, l'administrateur LOCAL du serveur RDS doit autoriser l'utilisation de ce service.

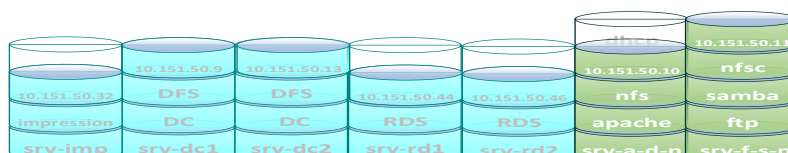
Nom	Description
Accès DCOM service de certificats	Les membres de ce groupe sont autorisés à se connecter à des autorités de certification d'entre...
Administrateurs	Les membres du groupe Administrateurs disposent d'un accès complet et illimité à l'ordinateur...
Administrateurs Hyper-V	Les membres de ce groupe disposent d'un accès complet et illimité à toutes les fonctionnalités...
Duplicateurs	Prend en charge la réplication des fichiers dans le domaine
IIS_IUSRS	Groupe intégré utilisé par les services Internet (IIS).
Invités	Les membres du groupe Invités disposent par défaut du même accès que les membres du gro...
Lecteurs des journaux d'événements	Des membres de ce groupe peuvent lire les journaux des événements à partir de l'ordinateur lo...
Opérateurs d'assistance de contrôle d'accès	Les membres de ce groupe peuvent interroger à distance les attributs d'autorisation et les auto...
Opérateurs de chiffrement	Les membres sont autorisés à effectuer des opérations de chiffrement.
Opérateurs de configuration réseau	Les membres de ce groupe peuvent disposer de certaines autorisations d'administration pour l...
Opérateurs de sauvegarde	Les membres du groupe Opérateurs de sauvegarde peuvent passer outre les restrictions de séc...
Opérateurs d'impression	Les membres peuvent administrer les imprimantes installées sur des contrôleurs de domaine
Serveurs Accès Distant RDS	Les serveurs de ce groupe permettent aux utilisateurs des programmes RemoteApp et aux bure...
Serveurs Gestion RDS	Les serveurs de ce groupe peuvent effectuer des actions administratives de routine sur les serve...
Serveurs RDS Endpoint	Les serveurs de ce groupe exécutent des ordinateurs virtuels et hébergent des sessions où les ut...
Storage Replica Administrators	Les membres de ce groupe bénéficient d'un accès total et illimité à l'ensemble des fonctionnali...
System Managed Accounts Group	Les membres de ce groupe sont gérés par le système.
Utilisateurs	Les utilisateurs ne peuvent pas effectuer de modifications accidentelles ou intentionnelles à l'é...
Utilisateurs avec pouvoir	Les utilisateurs avec pouvoir sont inclus pour des raisons de compatibilité et possèdent des dro...
Utilisateurs de gestion à distance	Les membres de ce groupe ont accès aux ressources WMI via des protocoles de gestion (tels q...
Utilisateurs de l'Analyseur de performances	Les membres de ce groupe peuvent accéder aux données de compteur de performance locale...
Utilisateurs du Bureau à distance	Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance
Utilisateurs du journal de performances	Les membres de ce groupe peuvent planifier la journalisation des compteurs de performance, ...
Utilisateurs du modèle COM distribué	Les membres sont autorisés à lancer, à activer et à utiliser sur cet ordinateur les objets COM dis...

Pour cela, l'administrateur LOCAL ajoute dans la console « mmc » les utilisateurs du Bureau à distance.

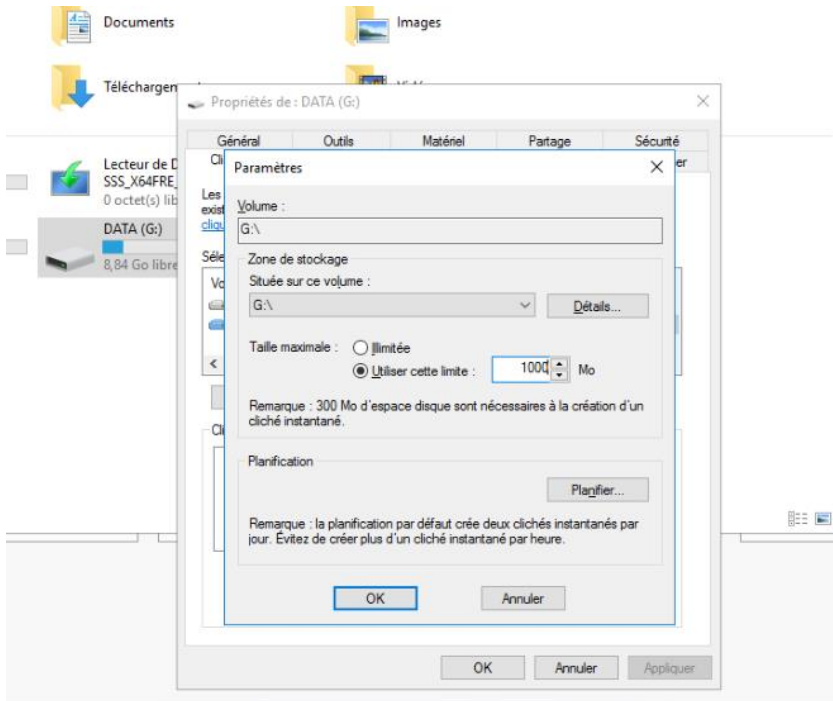
Dans notre cas, ce sera le groupe « Toutankhamon18 » dans lequel il y a les utilisateurs des services Produit A et Produit B.

Ils sont maintenant autorisés à se connecter au service Bureau à distance de l'entreprise BSD.

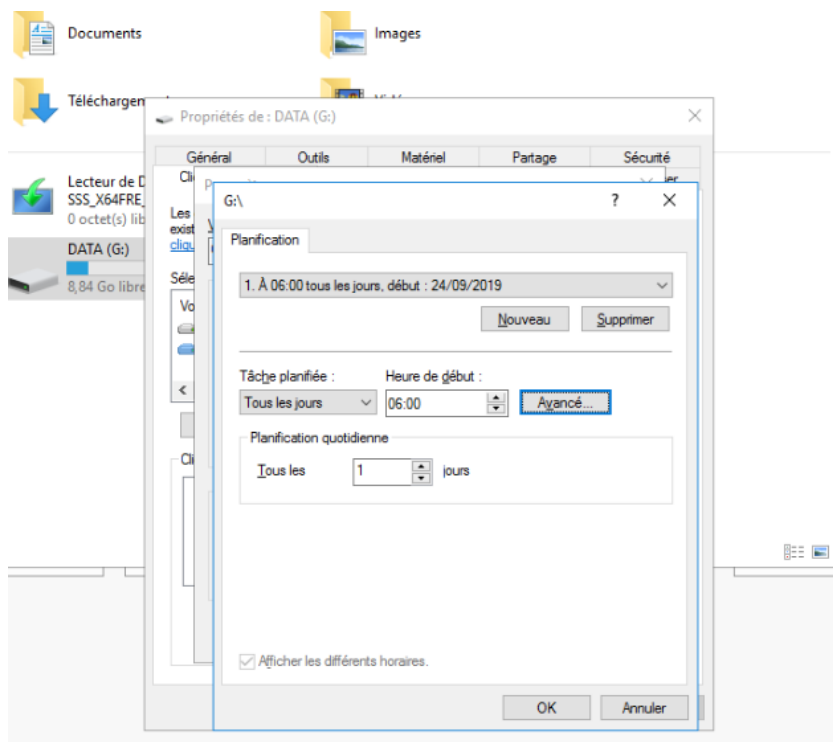
The screenshot shows the 'Propriétés de : Utilisateurs du Bureau à distance' dialog box. The 'Général' tab is active, showing the group name 'Utilisateurs du Bureau à distance' and a description: 'Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance'. The 'Membres' list contains 'BSD\Toutankhamon18'. Buttons for 'Ajouter...', 'Supprimer', 'OK', 'Annuler', 'Appliquer', and 'Aide' are visible.



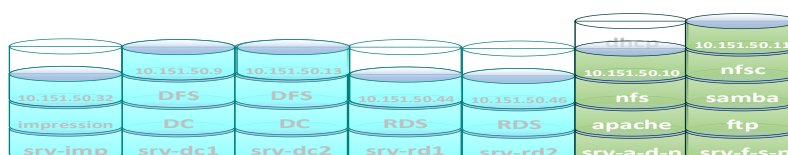
Nous allons maintenant mettre en place les clichés instantanés sur la partition DATA.



Dans les propriétés de DATA, en allant sur clichés instantanés, nous paramétrons une limite à ne pas dépasser pour ce cliché.

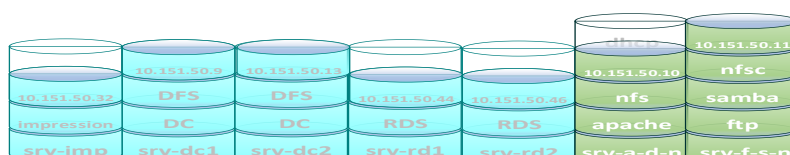
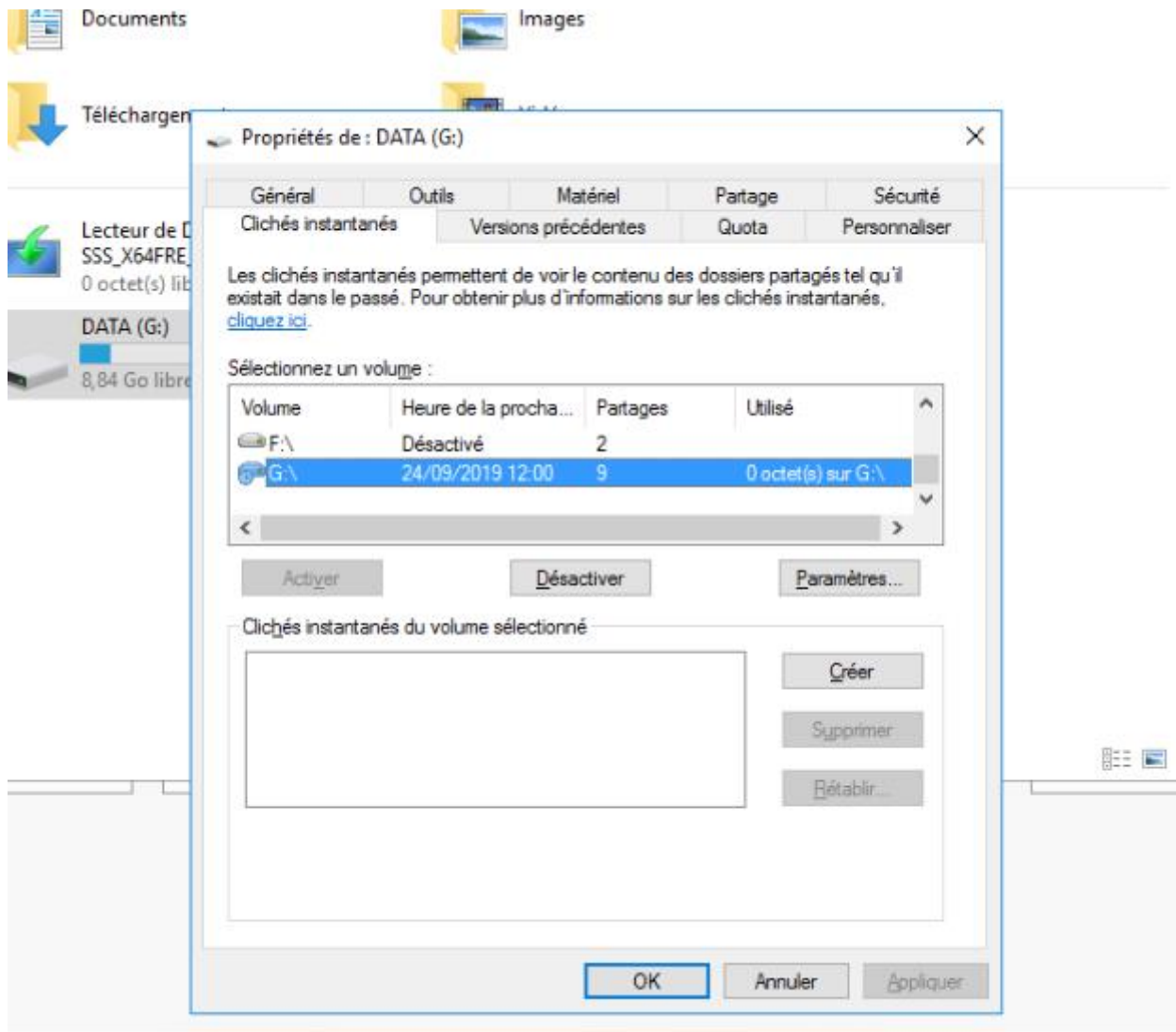


Nous planifions ensuite quand ce cliché instantané se réalisera. Dans notre cas nous choisissons tous les jours à 6h00.



À partir de maintenant, un cliché instantané se fera tous les jours à 6h00.

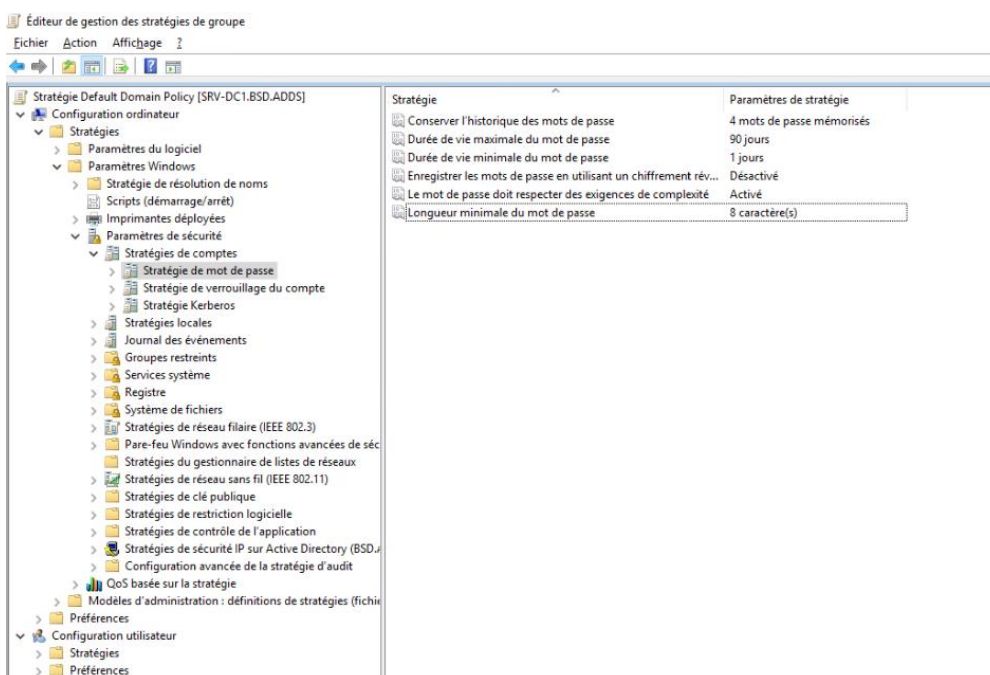
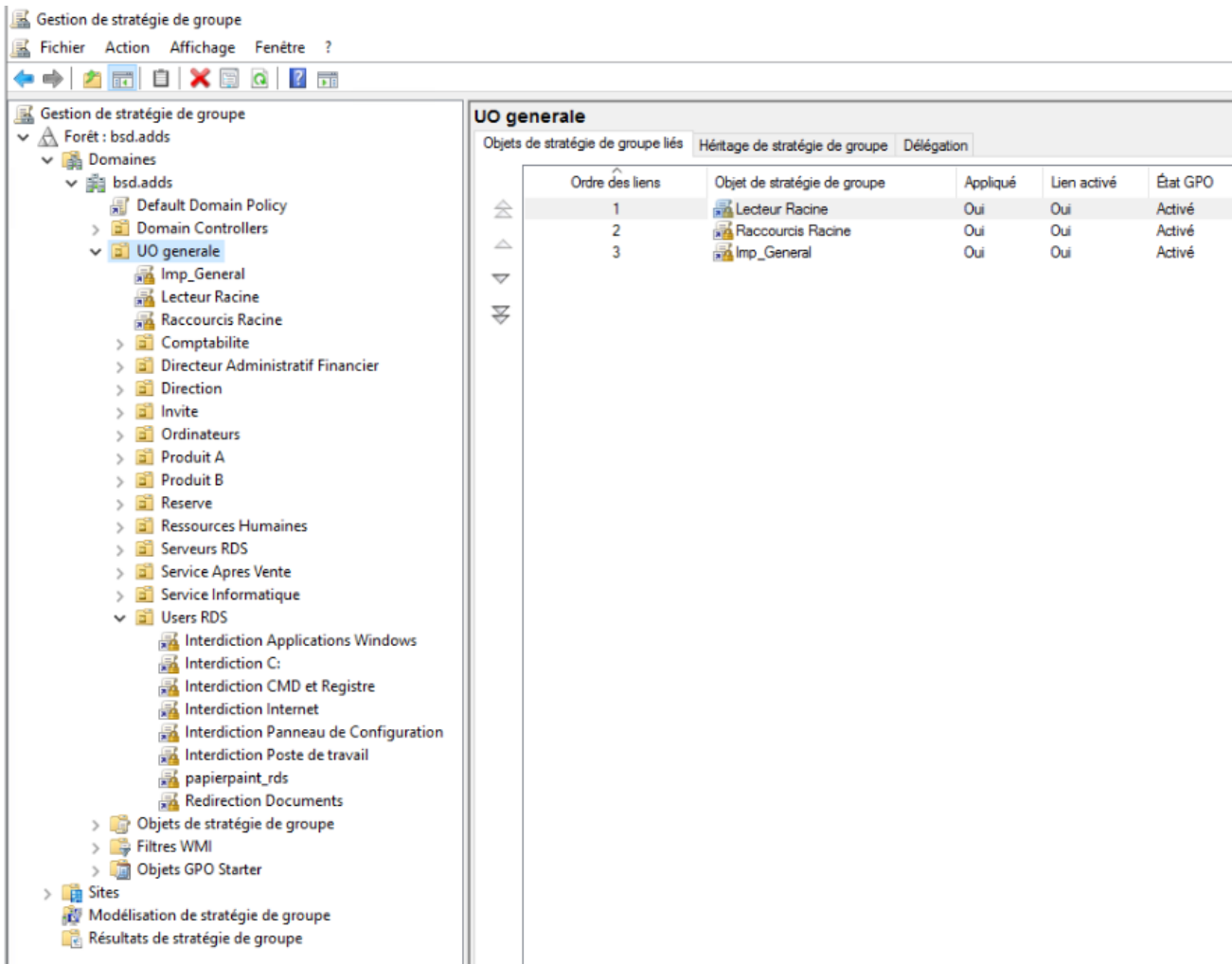
Dans le cas où un utilisateur supprime par mégarde un fichier ou un dossier quelconque, il peut restaurer ses données d'un jour antérieur.



Nous allons mettre en place les Group Policy Objects (GPO).

Ces GPO permettent la gestion des utilisateurs et des ordinateurs dans un Active Directory.

Certaines GPO sont déjà implémentées dans les UO pour les imprimantes réalisées plus haut.

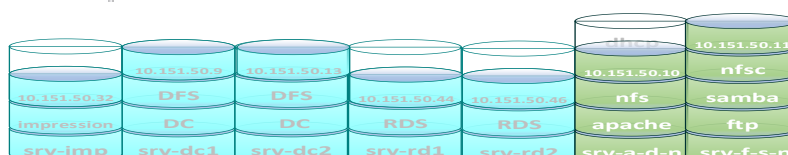


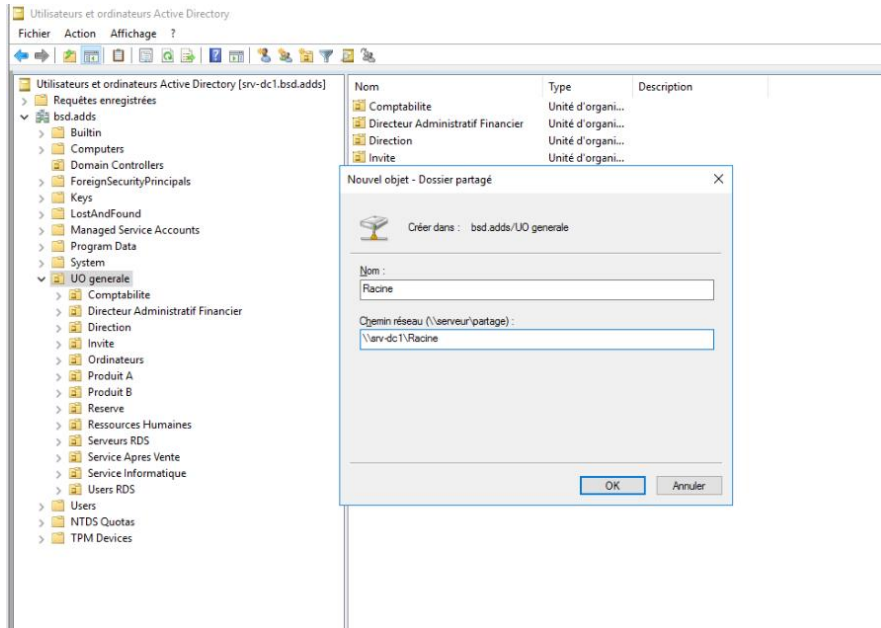
Une stratégie de mot de passe est déjà présente par défaut. Nous changeons cette stratégie pour l'entreprise.

Une conservation de 4 mots de passe mémorisés.

Une durée de vie maximale à 90 jours.

Une longueur minimale de 8 caractères.





Pour la création d'un lecteur réseau pour les utilisateurs, nous devons tout d'abord créer un objet « Dossier partagé » dans l'Active Directory.

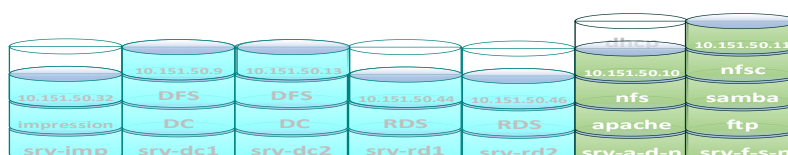
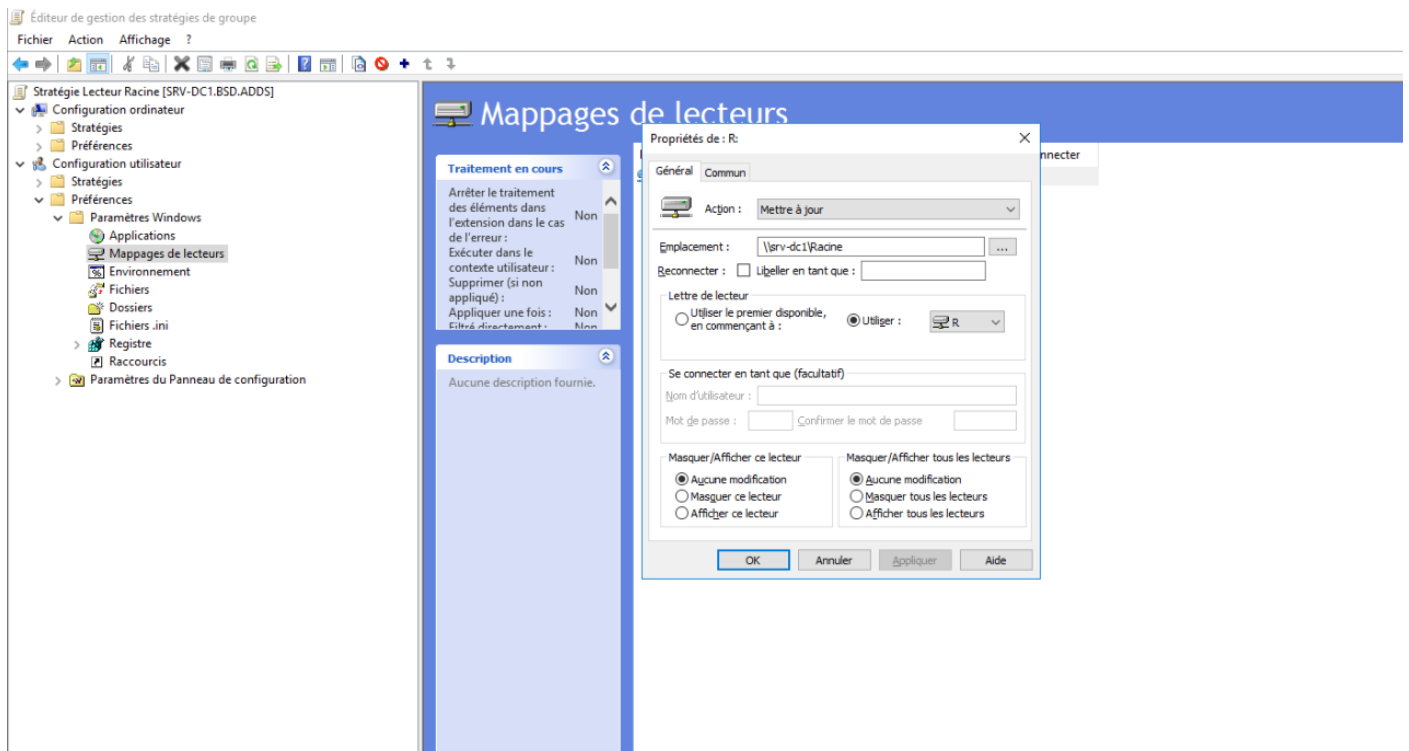
Nous lui mettons un nom, ainsi que le chemin réseau du partage.

« `\\srv-dc1\Racine` » sera le chemin réseau.

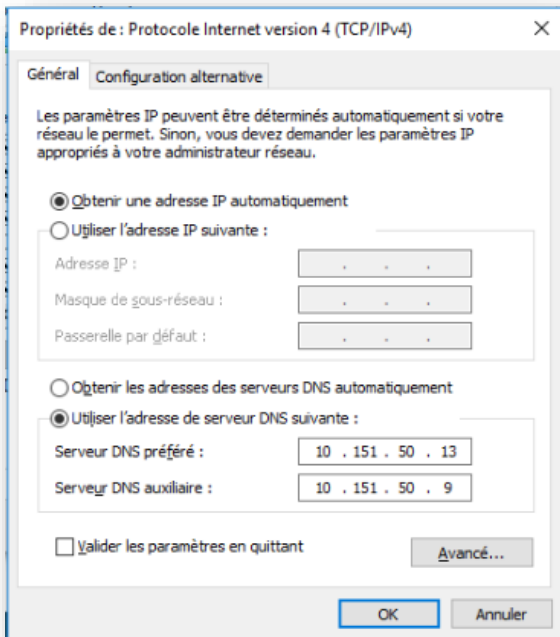
Ensuite nous ajoutons une GPO, nous lui mettons le nom « Lecteur Racine » et on clique sur « Modifier... »
 Nous sommes dans l'éditeur de gestion des GPO. Nous allons dans « Configuration utilisateur », « Préférences », « Paramètres Windows » et « Mappages de lecteurs ».

Nous mettons comme action « Mettre à jour » et comme emplacement, nous cliquons sur « ... », nous retrouvons notre objet dossier partagé « Racine ».

Pour finir, nous choisissons la lettre « R » pour ce lecteur réseau.



Une fois toutes les GPO mise en place (un listing complet est fournis plus bas en annexe), nous allons pouvoir passer aux utilisateurs.



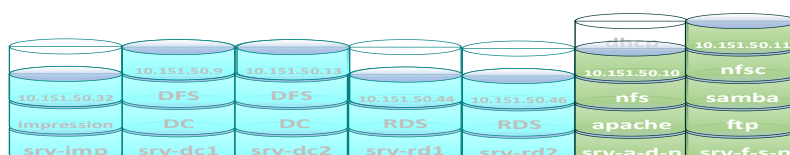
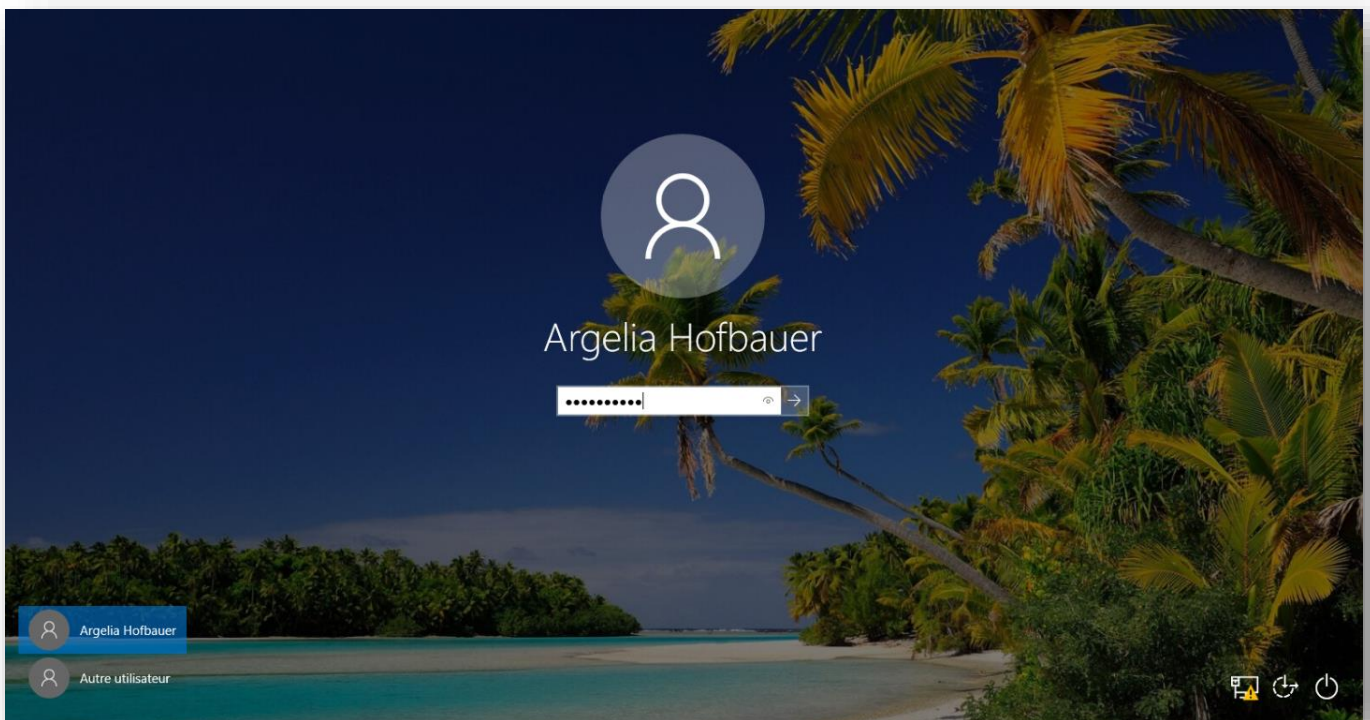
Nous laissons le serveur DHCP fournir une adresse IP automatiquement.

Pour le DNS, c'est exactement la même étape que pour les serveurs membres.

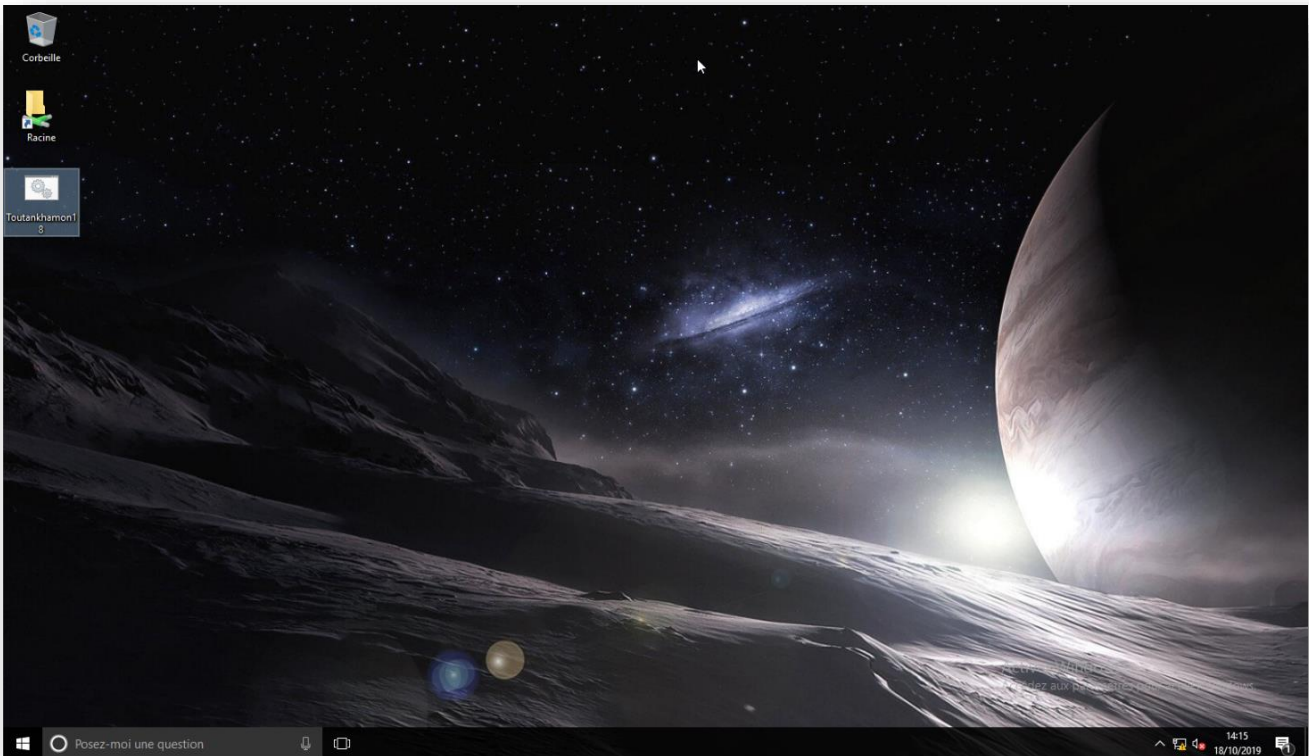
DNS préféré = adresse IP srv-dc1

DNS auxiliaire = adresse IP srv-dc2

Après l'avoir rejoint au domaine, l'utilisateur peut se connecter en tant qu'utilisateur du domaine.

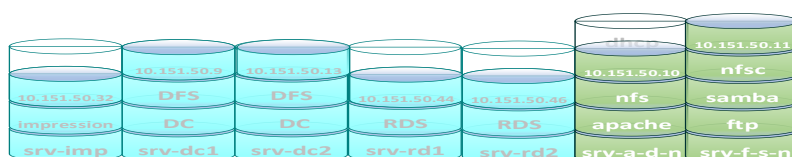
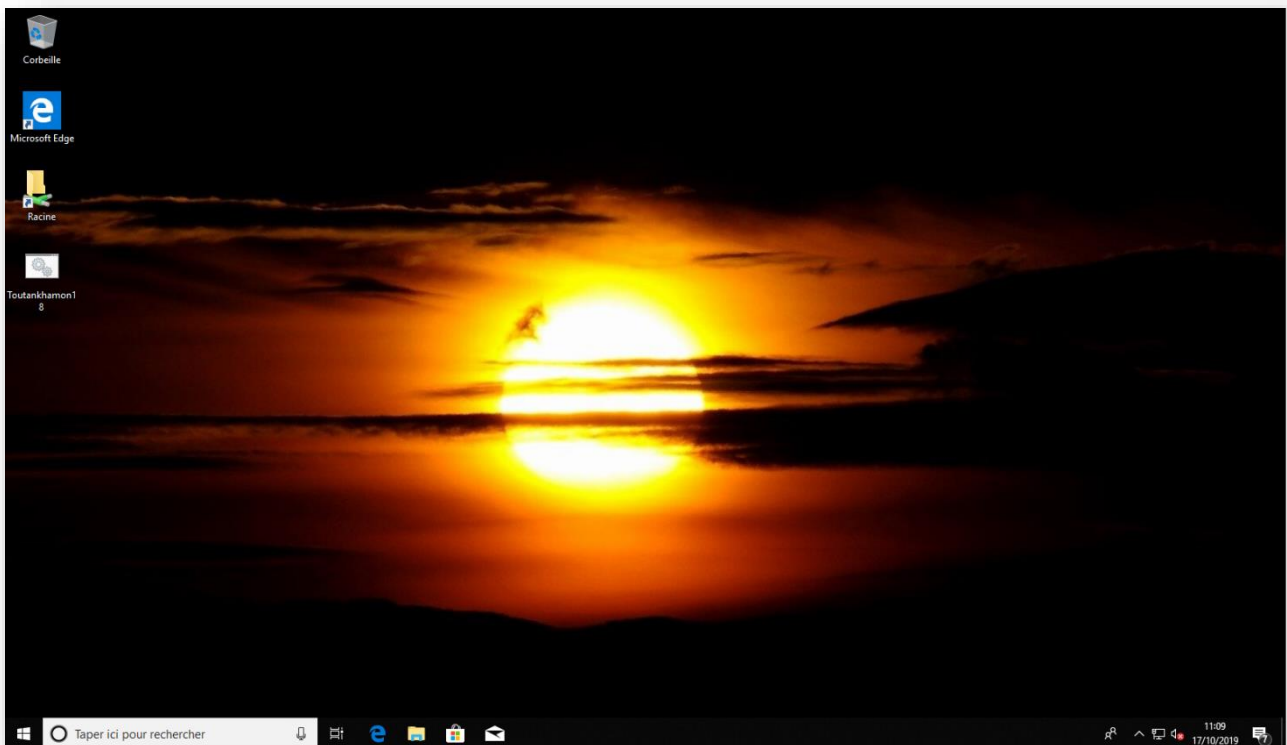


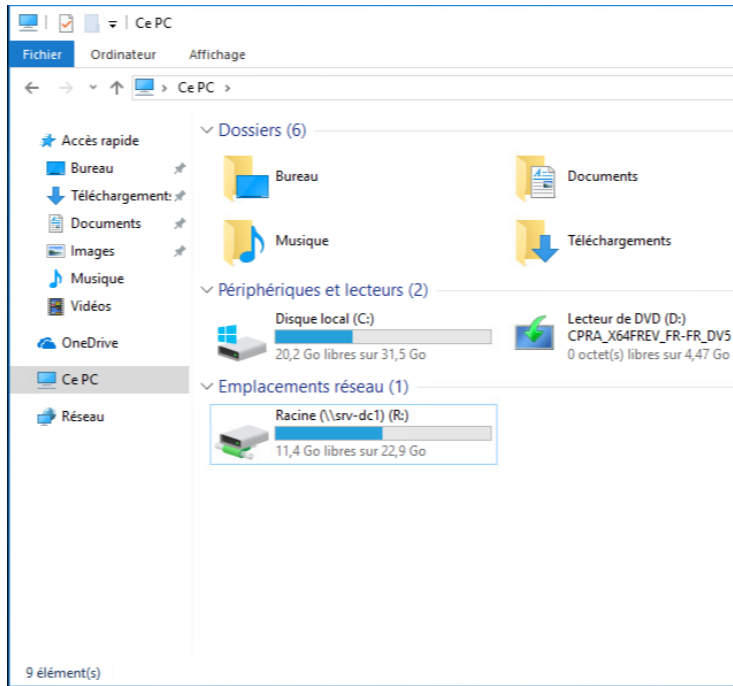
Voilà le bureau de l'utilisateur du service produit A.



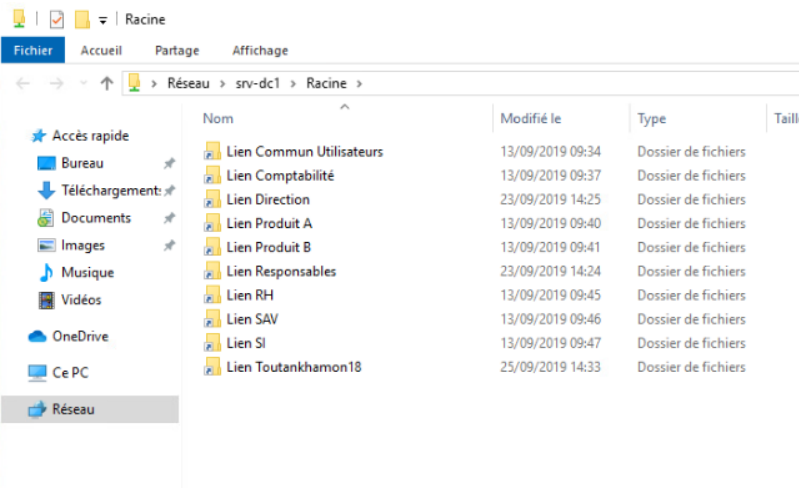
Ainsi que le bureau du service produit B.

Chaque service dispose de sa propre image en arrière-plan via une GPO.

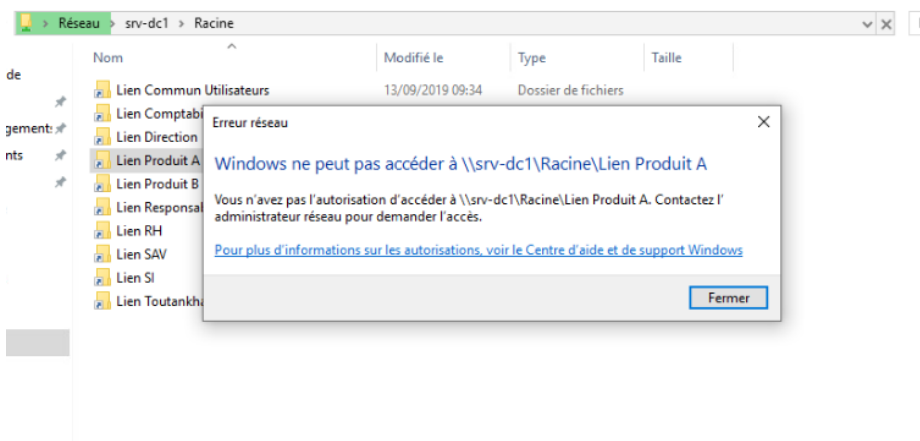




Nous pouvons voir la présence du lecteur réseau Racine.

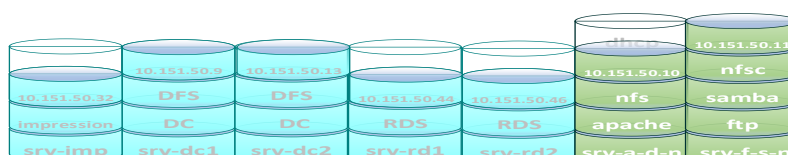


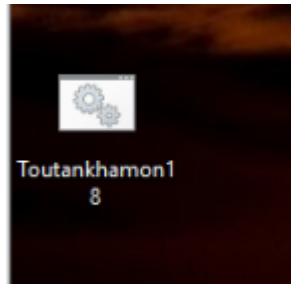
Nous retrouvons à l'intérieur du lecteur Racine, les liens créés avec DFS.



On voit ici qu'un utilisateur du produit B ne peut pas accéder au dossier « Produit A ».

Il peut accéder seulement à son dossier et au dossier « Commun Utilisateurs ».

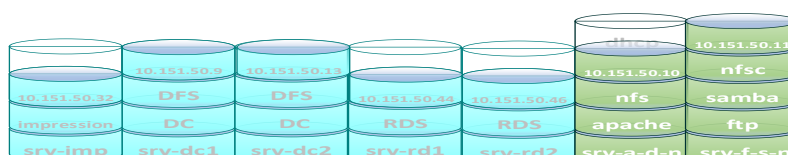


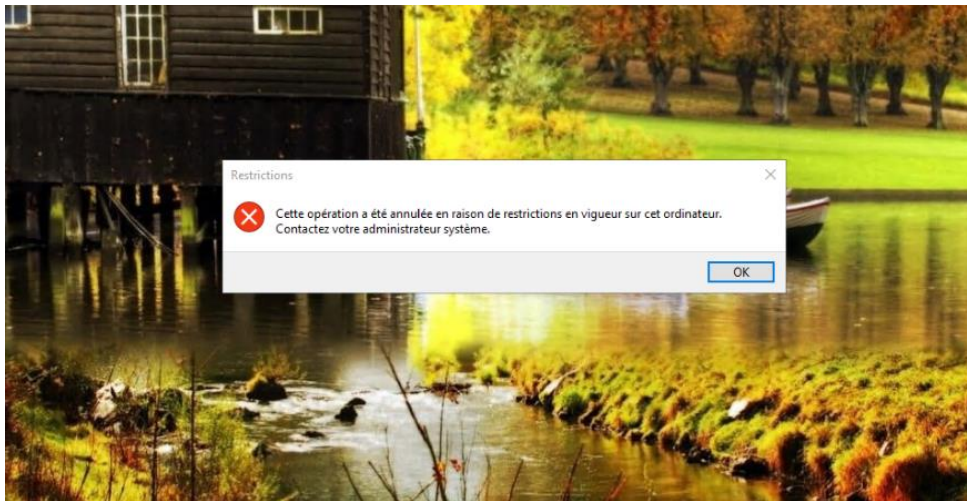


Pour se connecter au bureau sécurisé à distance, l'utilisateur doit cliquer sur cette icône sur son bureau.

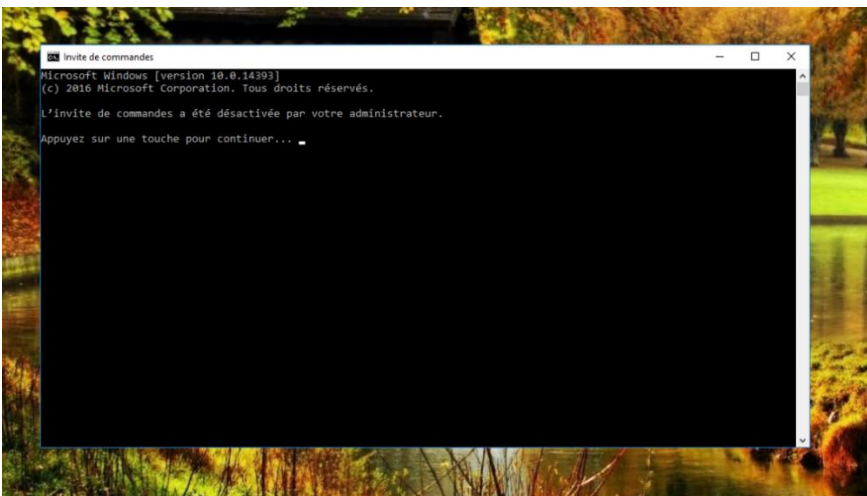
Le script se lancera automatiquement. Pour la première connexion, l'utilisateur va devoir renseigner son mot de passe pour rentrer sur le bureau sécurisé à distance.

Une fois la connexion établie, l'utilisateur aura accès à son application métier et seulement à cette application.

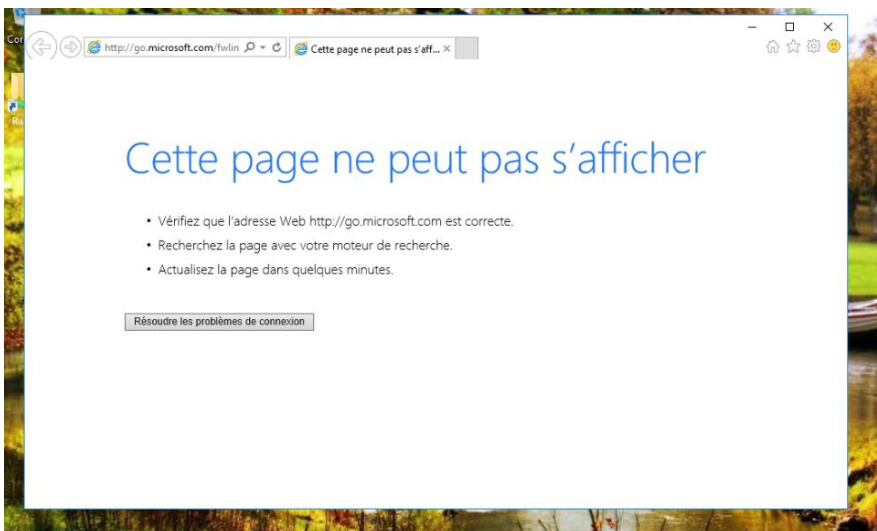




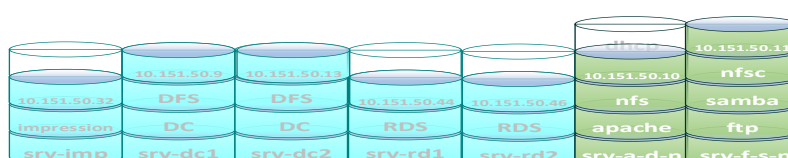
L'utilisateur aura différentes interdictions.

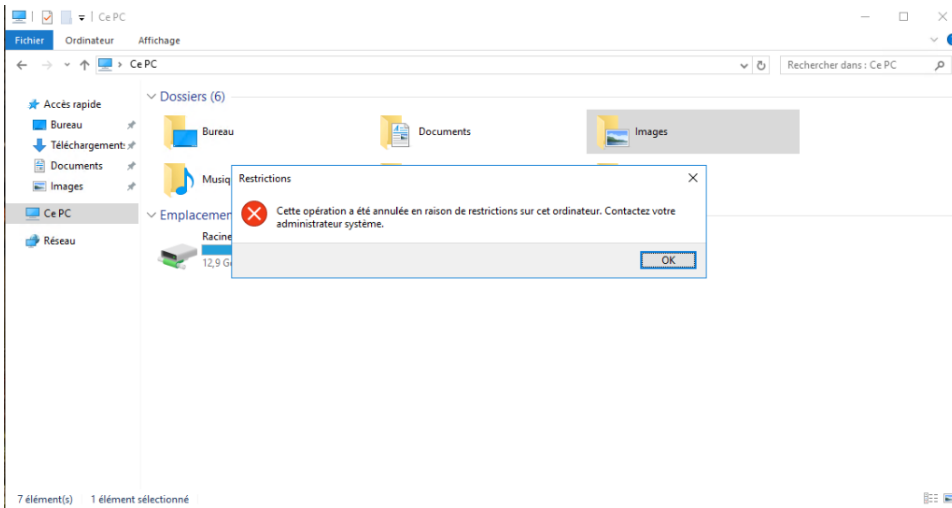


Interdiction d'exécuter des commandes via l'invite de commandes.

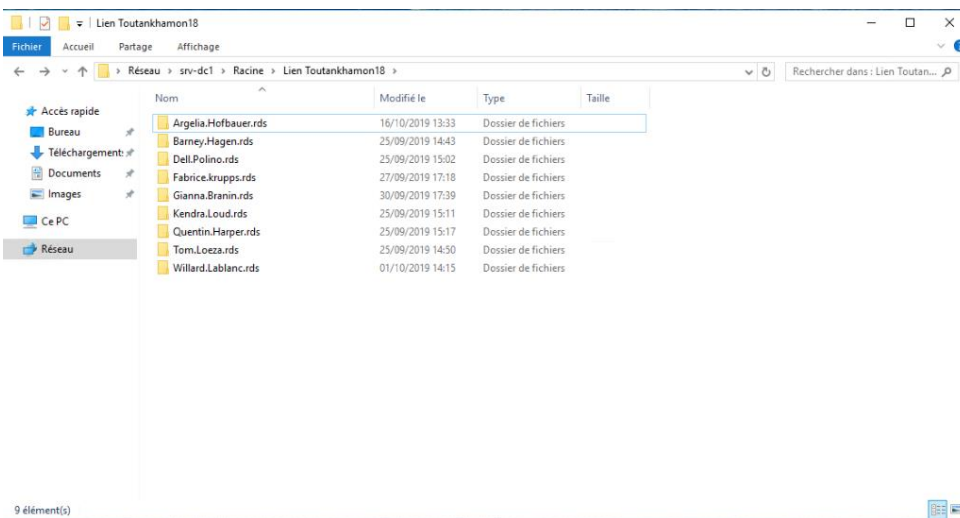


Interdiction d'aller sur internet.





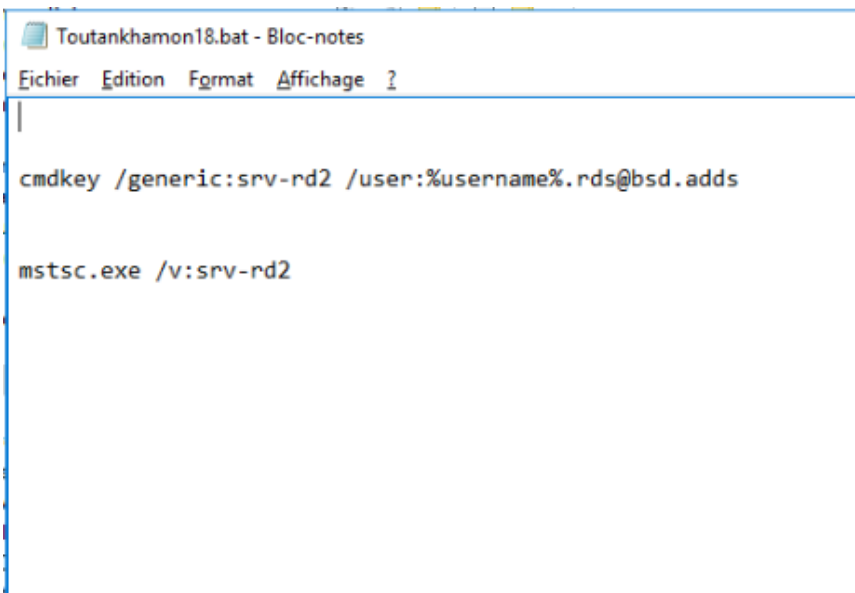
Interdiction d'écrire et d'accéder sur le lecteur C.



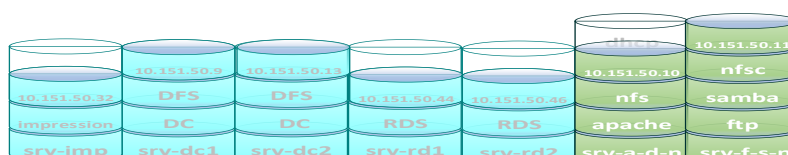
À la première connexion d'un utilisateur, un dossier est créé dans le lien correspondant via une GPO.

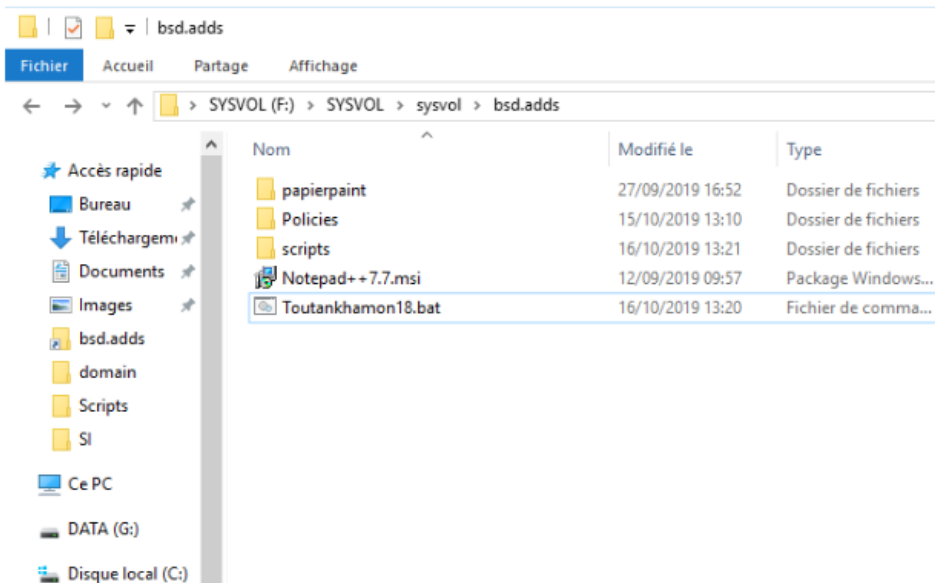
Il n'aura pas accès aux autres dossiers.

Si l'utilisateur crée un fichier dans Documents, ce fichier sera redirigé vers son dossier.



Pour information, ceci est le script de connexion pour les utilisateurs RDS.





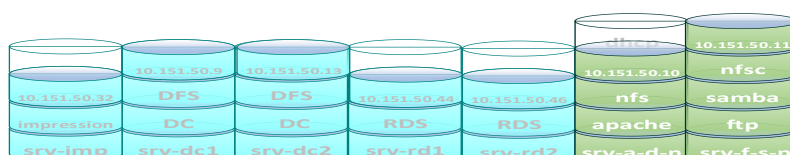
Ce script est stocké dans SYSVOL.

Aparté sur les quotas :

Dans les OS Windows, les quotas limitent la quantité de stockage d'un utilisateur. Cet outil correspond aux exigences du cahier des charges de l'entreprise BSD, à savoir un espace de 5 Go par utilisateur.

La mise en place de cette fonctionnalité peut se faire de 3 façons différentes :

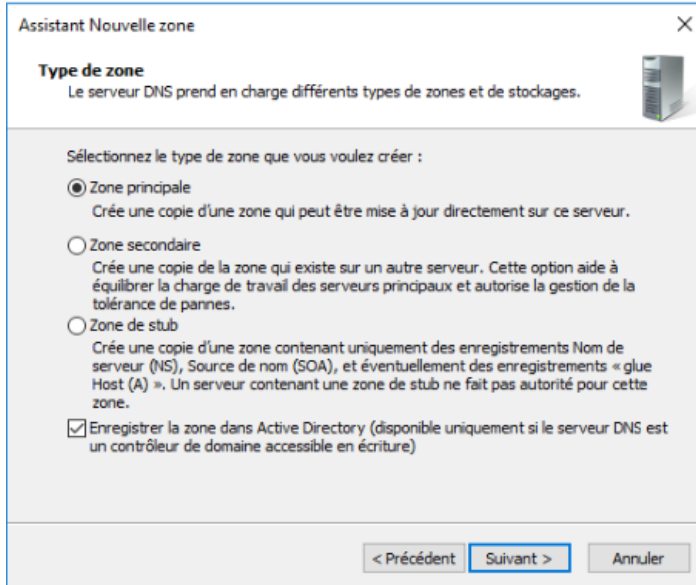
- Les propriétés d'un volume contiennent une version accessible pour un utilisateur courant. Cependant, l'application de cette version des quotas a rendu les comptes utilisateurs instables. Dès le dépassement de la limite, la session client dysfonctionne, d'où l'abandon de cette première solution.
- Le second moyen de restreindre l'espace de stockage s'effectue par GPO. Opérationnelle, elle a néanmoins l'inconvénient d'augmenter drastiquement le temps d'accès du service Bureau à Distance (10 min environ par connexion).
- Enfin, la troisième solution consiste à installer le rôle « Gestionnaire de ressources du serveur de fichiers ». Cette solution, par manque de temps, sera abordée dans une étude additionnelle.



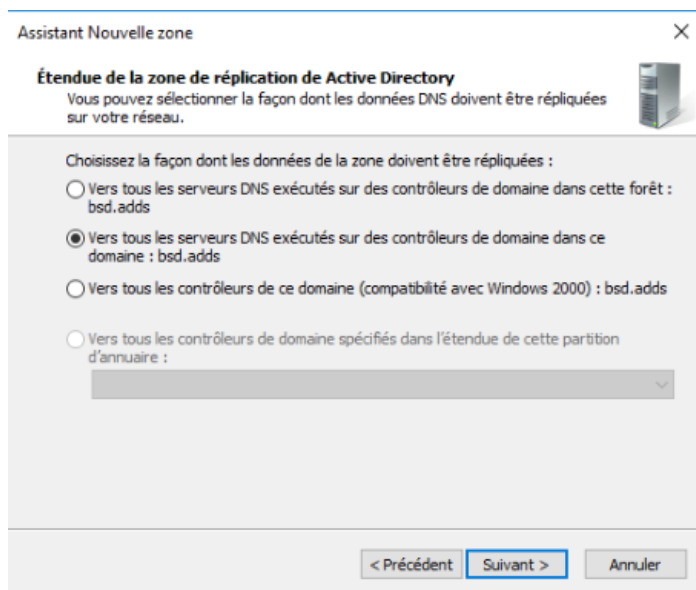
Nous allons configurer la zone de recherche indirect (zone de recherche inversée).

De base, les clients effectuent une recherche directe, ce qui veut dire une recherche basée sur le nom DNS pour connaître son adresse IP.

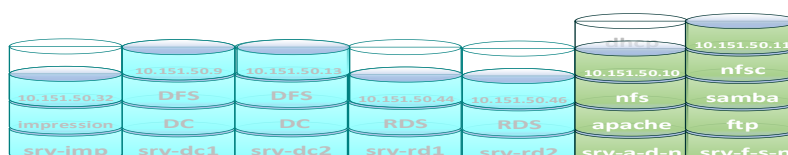
Il existe une méthode inversée. Nous pouvons effectuer une recherche en tapant l'adresse IP pour connaître le nom DNS.

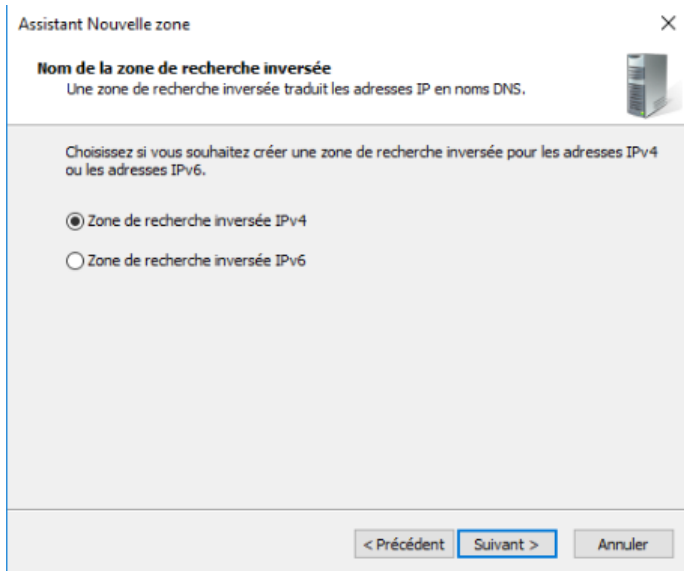


Nous créons donc une nouvelle zone principale dans la zone de recherche indirecte.

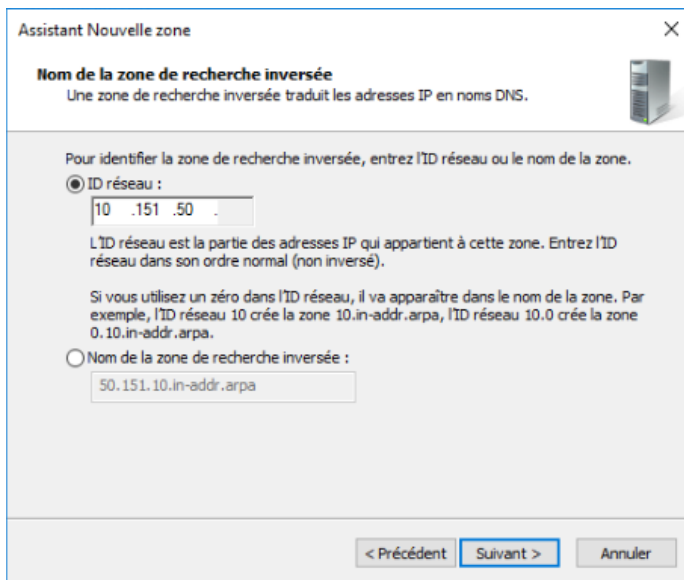


Nous choisissons d'étendre vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : bsd.adds.

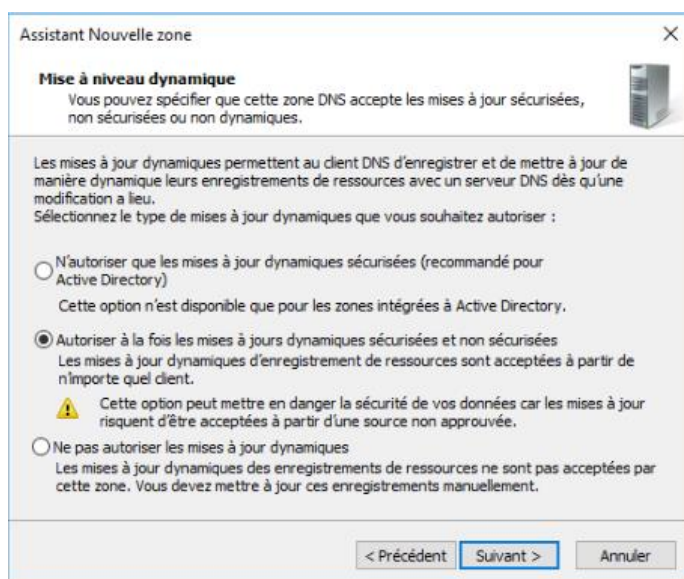




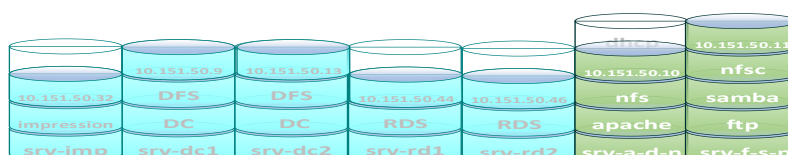
Nous sélectionnons « Zone de recherche inversée Ipv4 ».



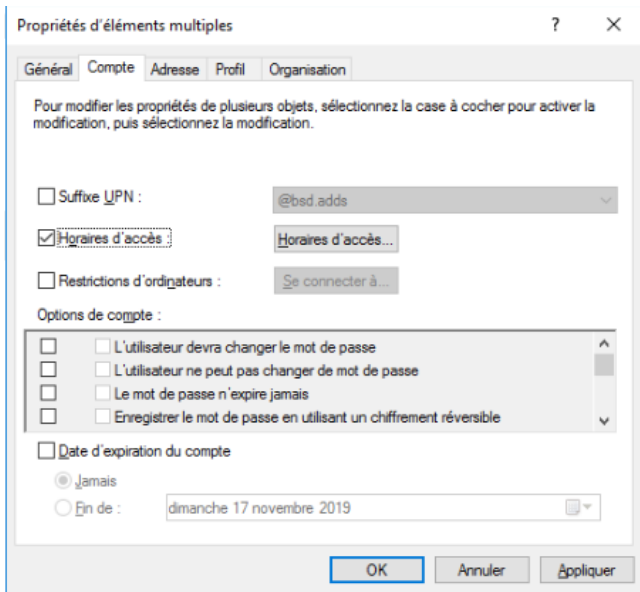
Nous indiquons l'ID réseau qui correspond aux trois premières zones de l'adresse IP de srv-dc1.



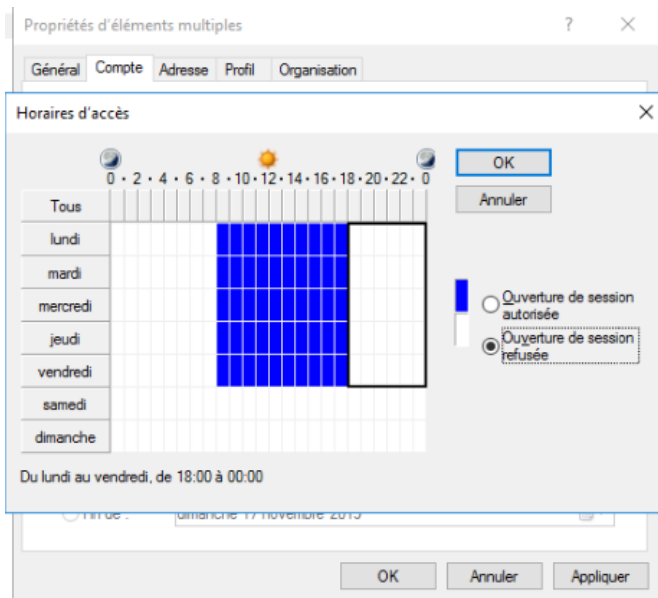
Pour finir, nous sélectionnons d'autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées.



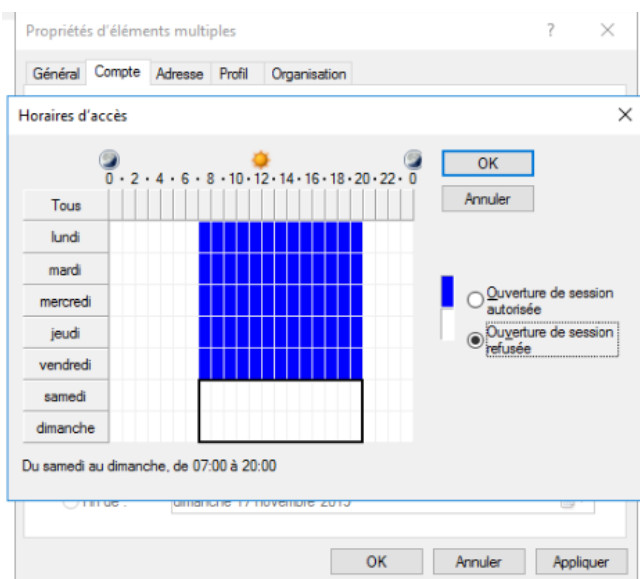
Certains utilisateurs ont des restrictions sur les horaires de connexion au sein de l'entreprise BSD.



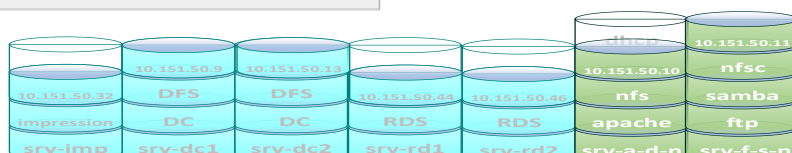
Nous sélectionnons les utilisateurs concernés dans l'Active Directory, dans les propriétés et compte, nous cochons « Horaires d'accès ».



Dans notre cas, Mme BEZIAT, ELLA, AYO et ACIEN sont autorisées à se connecter qu'entre 8h00 et 18h00, du lundi au vendredi.



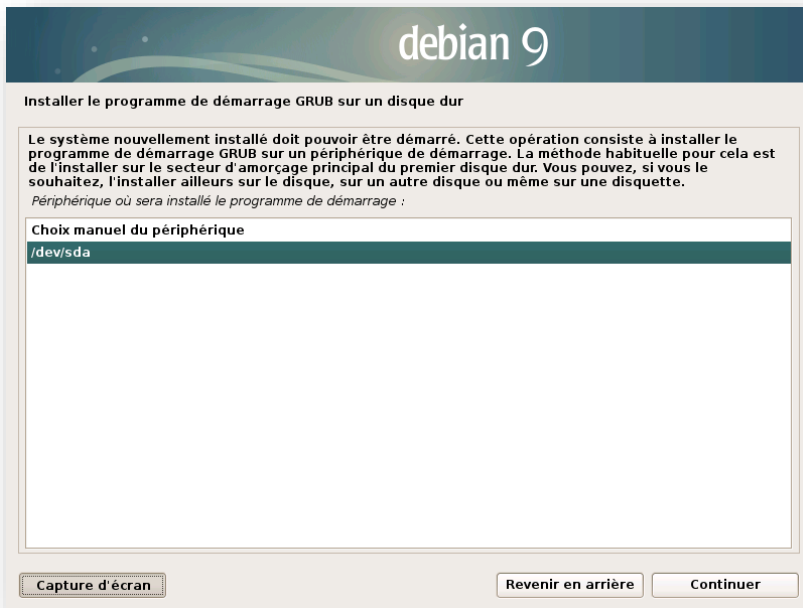
Tous les autres salariés, sauf la direction, le SAV et le service informatique, ne peuvent se connecter entre 20h00 et 7h00.



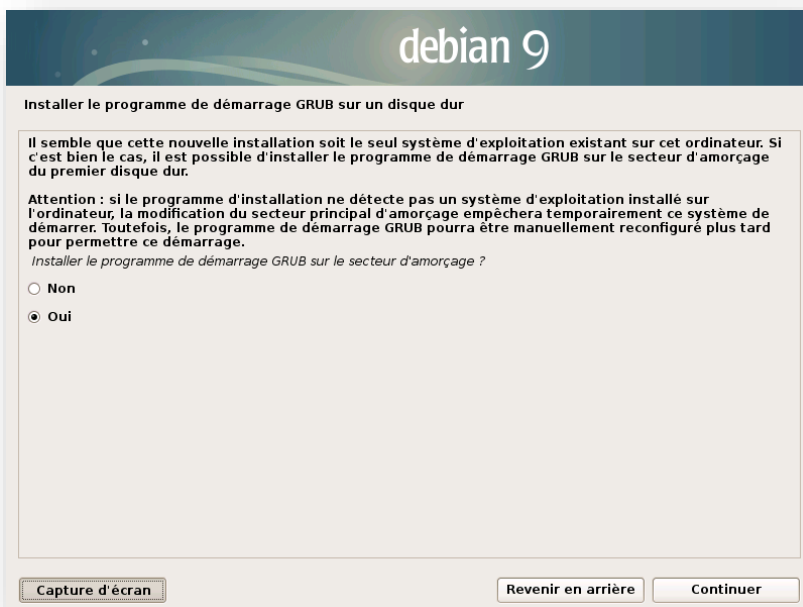
K. Procédure Linux

❖ Installation

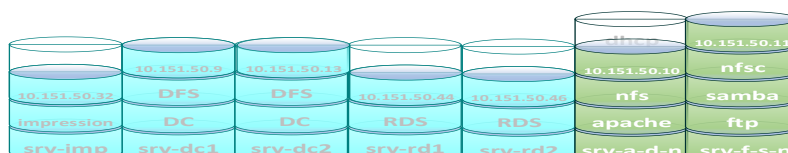
Nous allons commencer par installer le système d'exploitation DEBIAN.

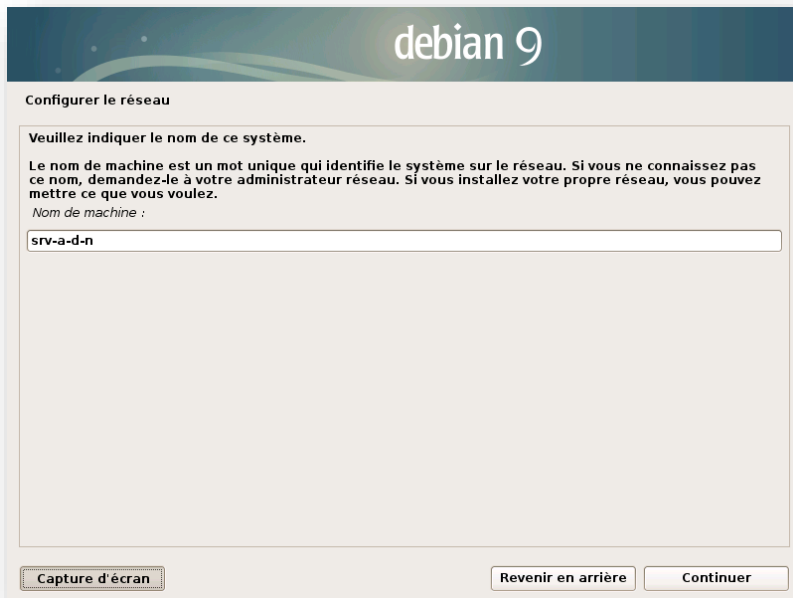


À cette étape, il faut bien choisir le bon périphérique, à savoir « /dev/sda ».



Nous choisissons d'installer le programme de démarrage GRUB sur le secteur d'amorçage.

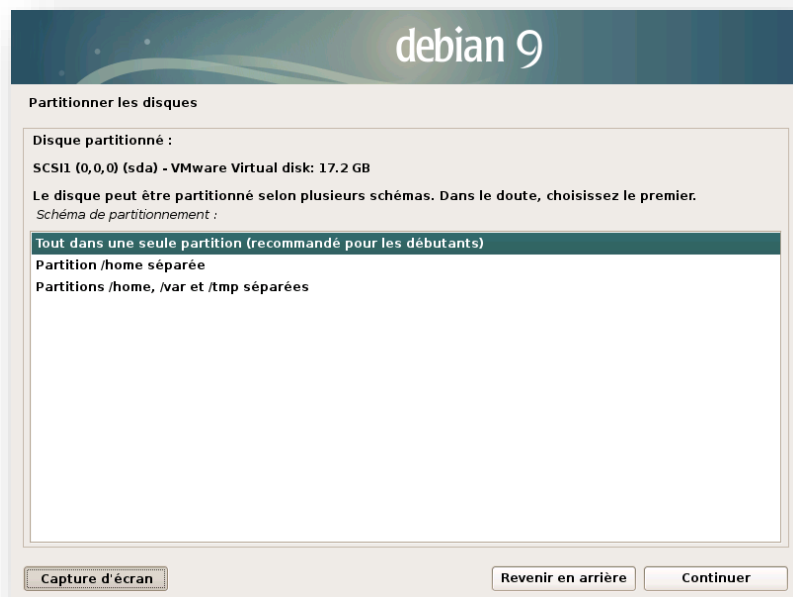




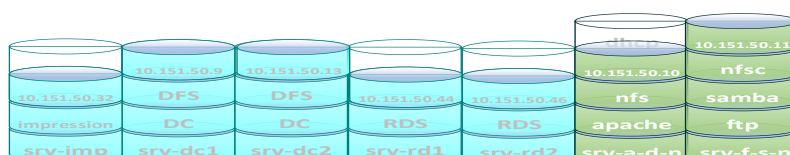
Nous choisissons un nom pour les deux serveurs DEBIAN.

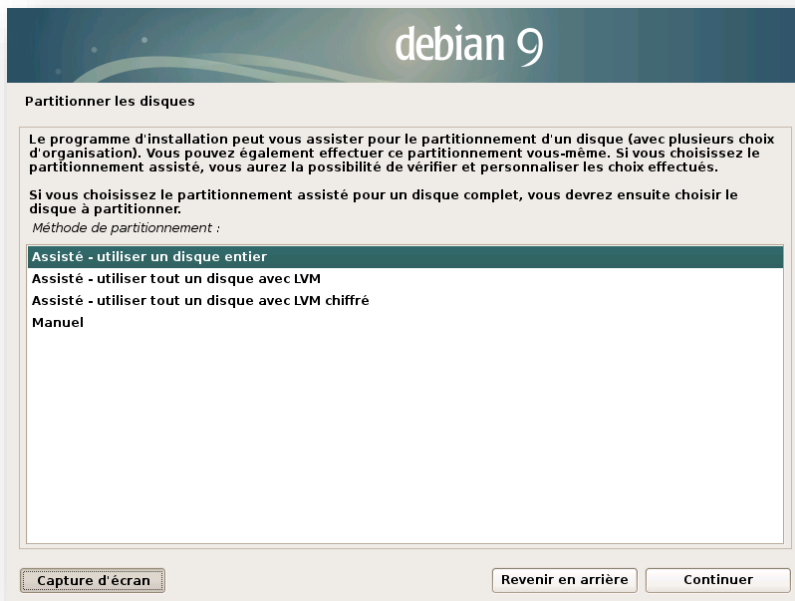
« srv-a-d-n » contiendra les rôles Apache, DHCP et NFS Serveur.

« srv-f-s-nc » contiendra les rôles ProFTP, Samba et NFS Client.



Nous choisissons d'installer le tout dans une seule partition.





Comme méthode de partitionnement, nous choisissons d'utiliser un disque entier.

Une fois l'installation terminée, nous allons lancer une console et se connecter en tant que root en tapant la commande « su », puis nous entrons le mot de passe de root.

```
GNU nano 2.7.4 Fichier : /etc/apt/sources.list
# deb cdrom:[Debian GNU/Linux 9.6.0 _Stretch_ - Official amd64 NETINST 20181110-11:34]/ stretch main
#deb cdrom:[Debian GNU/Linux 9.6.0 _Stretch_ - Official amd64 NETINST 20181110-11:34]/ stretch main
deb http://ftp.fr.debian.org/debian/ stretch main
deb-src http://ftp.fr.debian.org/debian/ stretch main
deb http://security.debian.org/debian-security stretch/updates main
deb-src http://security.debian.org/debian-security stretch/updates main
# stretch-updates, previously known as 'volatile'
deb http://ftp.fr.debian.org/debian/ stretch-updates main
deb-src http://ftp.fr.debian.org/debian/ stretch-updates main
```

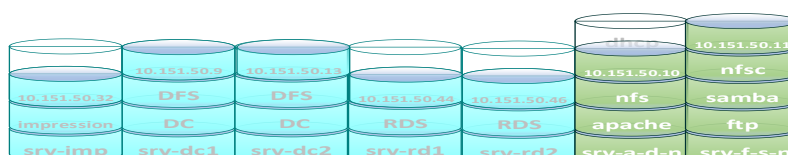
Nous allons maintenant changer le fichier « sources.list » qui est un prérequis pour le bon fonctionnement de DEBIAN en tapant la commande « nano /etc/apt/sources.list »

```
user1@srv-a-d-n:~$ su
Mot de passe :
root@srv-a-d-n:/home/user1# nano /etc/apt/sources.list
root@srv-a-d-n:/home/user1# apt-get update
```

Après avoir changé le fichier « sources.list », nous lançons la commande « apt-get update » pour la prise en compte du changement.

```
root@srv-a-d-n:/home/user1# apt-get install ssh
```

Nous pouvons installer ssh avec cette commande qui est un protocole de communication sécurisé.



❖ Webmin

Nous allons utiliser une interface web pour faciliter l'administration des deux serveurs DEBIAN à distance via n'importe quel navigateur web.

Cette interface est Webmin.



Pour commencer, nous allons télécharger webmin sur leur site internet.

Figure XIII-25 Webmin interface

```
root@srv-a-d-n:/home/user1# cd Téléchargements/
root@srv-a-d-n:/home/user1/Téléchargements# dpkg -i webmin_1.930_all.deb
```

Ensuite, nous allons dans « Téléchargements », là où est enregistré le fichier.

Puis nous lançons cette commande pour lancer l'installation.

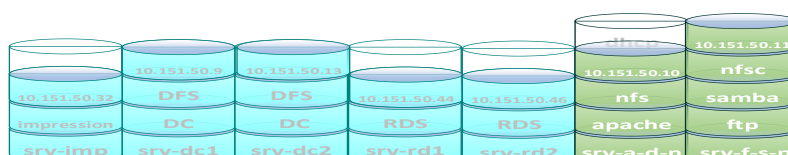
```
dpkg: erreur de traitement du paquet webmin (--install) :
problèmes de dépendances - laissé non configuré
Traitement des actions différées (« triggers ») pour systemd (232-25+deb9u12)
Des erreurs ont été rencontrées pendant l'exécution :
 webmin
root@srv-a-d-n:/home/user1/Téléchargements# apt-get install -f
```

Nous avons une erreur de dépendances.

Nous devons donc forcer l'installation avec cette commande.

Figure XIII-26 webmin dpkg

Voilà à quoi ressemble l'interface Webmin. Pour y accéder, il suffit d'aller sur un navigateur internet, taper l'adresse « [https://\(adresseIP du serveur\):10000](https://(adresseIP du serveur):10000) ». Puis se connecter en tant que root.



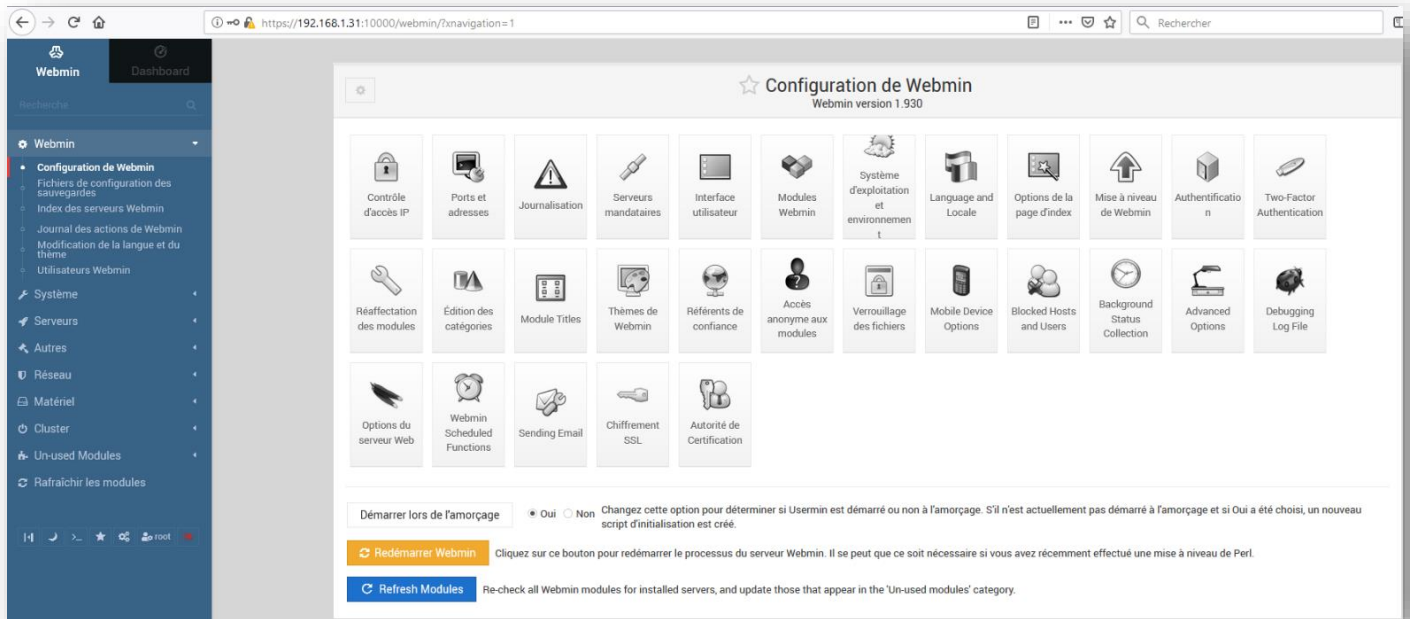
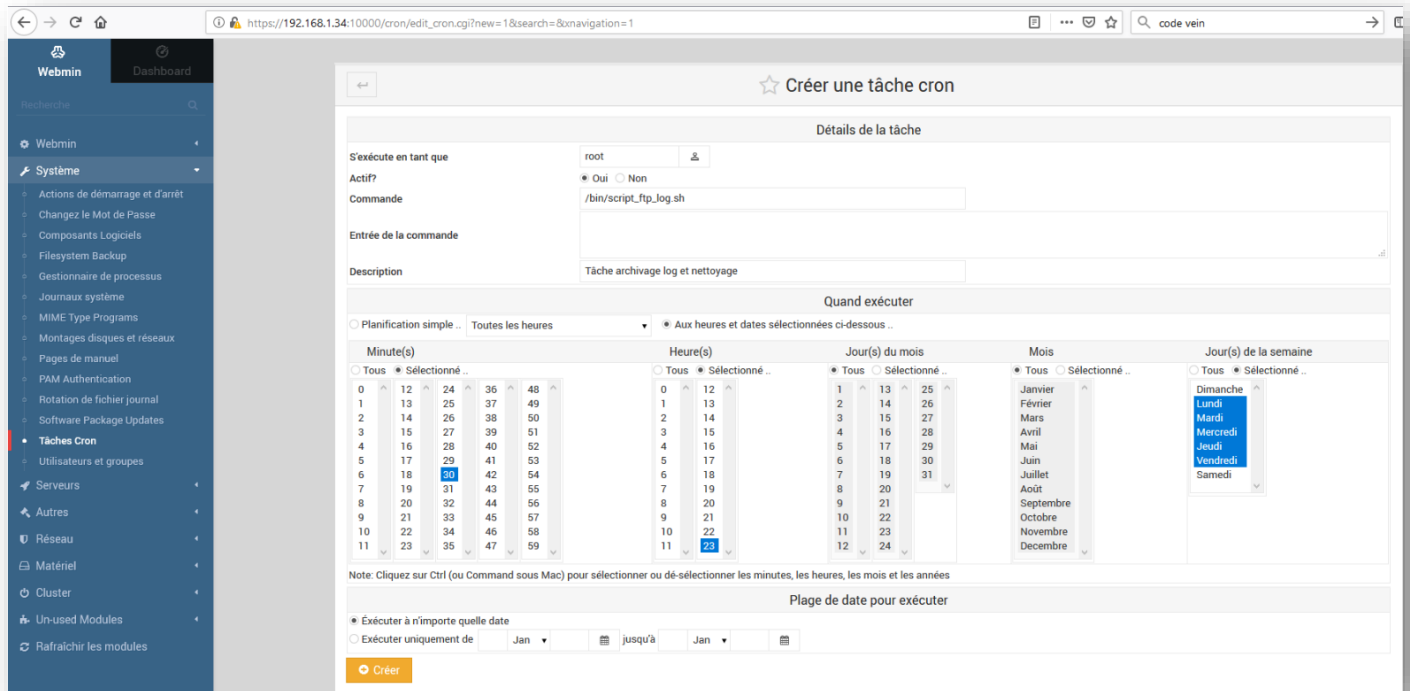


Figure XIII-27 webmin interface 2

Voilà la création d'une tâche planifiée qui lancera un script expliqué plus bas.

Figure XIII-28 webmin interface 3



❖ Nfs

```
root@srv-a-d-n:/home/user1/Téléchargements# apt-get install nfs-kernel-server
```

Commençons d'abord par installer NFS côté serveur pour srv-a-d-n.

```
root@srv-f-s-nc:/home/user2/Téléchargements# apt-get install nfs-common
```

Nous faisons de même pour srv-f-s-nc avec l'installation de NFS côté client.

```
GNU nano 2.7.4 Fichier : /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/var/log/installer 192.168.1.34(rw,root_squash)
```

Côté serveur, nous devons ajouter cette dernière ligne dans le fichier `/etc/exports` avec l'adresse IP du client.

Puis nous devons redémarrer le serveur en tapant la commande `/etc/init.d/nfs-kernel-server restart`.

Figure XIII-29 Nfs exports

```
mount -t nfs 192.168.1.31:/var/log/installer /mnt/screenshot
```

Ensuite, côté client, nous tapons cette commande avec l'adresse IP du serveur.

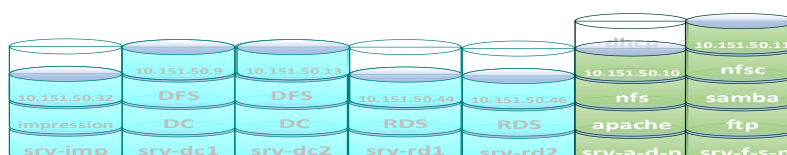
Ceci va créer un point de montage pour la récupération de fichier dans `/mnt/screenshot`.

Pour finir, pour que ce dossier soit remonter à chaque reboot, il suffit de taper cette ligne dans `/etc/fstab` « (adresse IP du serveur):/var/log/installer /mnt/screenshot nfs defaults 0 0 ».

❖ Apache

```
apt-get install apache2
```

Tout d'abord, nous installons apache avec cette commande.



```
GNU nano 2.7.4 Fichier : /etc/apache2/sites-available/internet.conf
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/internet/
```

En allant dans le fichier de conf dans `/etc/apache2/sites-available/internet.conf`, nous renseignons juste la ligne « DocumentRoot » en indiquant le chemin où sera stocké le site internet.

```
GNU nano 2.7.4 Fichier : intranet.conf
VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/intranet/
```

Même démarche pour le fichier « intranet.conf ».

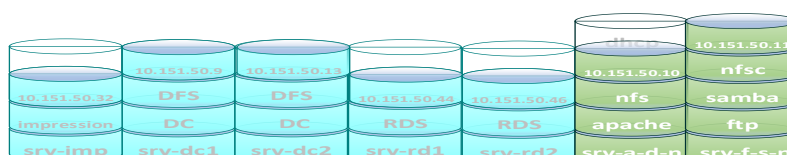
```
root@srv-a-d-n:/etc/apache2/sites-available# a2ensite internet.conf
Enabling site internet.
To activate the new configuration, you need to run:
systemctl reload apache2
root@srv-a-d-n:/etc/apache2/sites-available# a2ensite intranet.conf
Enabling site intranet.
To activate the new configuration, you need to run:
systemctl reload apache2
```

Pour activer les sites, nous tapons ces commandes. `a2ensite internet.conf` et `a2ensite intranet.conf`.

```
root@srv-a-d-n:/var/www/html# /etc/init.d/apache2 restart
[ ok ] Restarting apache2 (via systemctl): apache2.service
```

Nous devons redémarrer le service apache avec cette commande.

Nous créons un « index.html » pour le fichier « internet.conf ».

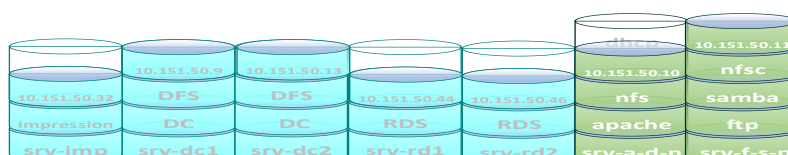


```

GNU nano 2.7.4                                Fichier : index.html
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8"/>
    <title>WWW.BSD.COM</title>
  <body style="background-color:#e2e2e2">
    <center><h1>BIENVENUE SUR BSD !</h1></br></br>
    <h1>L'ENTREPRISE DE TOUTES LES IDEES !</h1></br></br></br></br>
    <div style="border:2px solid; padding:10px; background-color:#c5ddf6">
  <p>
In his tractibus naverum nusquam visitur flumen sed in locis plurimis aquae suapte natura calentes emergunt ad usus aptae multiplicium medelarum. verum has $
Sed ut tum ad senem senex de senectute, sic hoc libro ad amicum amicissimus scripsi de amicitia. Tum est Cato locutus, quo erat nemo fere senior temporibus il$
Coactique aliquotiens nostri pedites ad eos persequendos scandere clivos sublimes etiam si lapsantibus plantis fruticeta prensando vel dumos ad vertices vener$
Et olim licet otiosae sint tribus pacataeque centuriae et nulla suffragiorum certamina set Pompiliani redierit securitas temporis, per omnes tamen quotquot su$
Raptim igitur properantes ut motus sui rumores celeritate nimia praevenirent, vigore corporum ac levitate confisi per flexuosas semitas ad summitates collium $
Tantum autem cuique tribuendum, primum quantum ipse efficere possis, deinde etiam quantum ille quem diligas atque adiuves, sustinere. Non enim neque tu possis$
Haec igitur lex in amicitia sancitur, ut neque rogemus res turpes nec faciamus rogati. Turpis enim excusatio est et minime accipienda cum in ceteris peccatis$
Apud has gentes, quarum exordiens initium ab Assyriis ad Nili cataractas porrigitur et confinia Blemmyarum, omnes pari sorte sunt bellatores seminudi coloratis$
Iamque lituis cladium concrepantibus internarum non celate ut antea turbidum saeviebat ingenium a veri consideratione detortum et nullo inpositorum vel conpos$
Ac ne quis a nobis hoc ita dici forte miretur, quod alia quaedam in hoc facultas sit ingeni, neque haec dicendi ratio aut disciplina, ne nos quidem huic uni s$

```

Figure XIII-30 code Html internet





Voilà le résultat de ce code HTML.

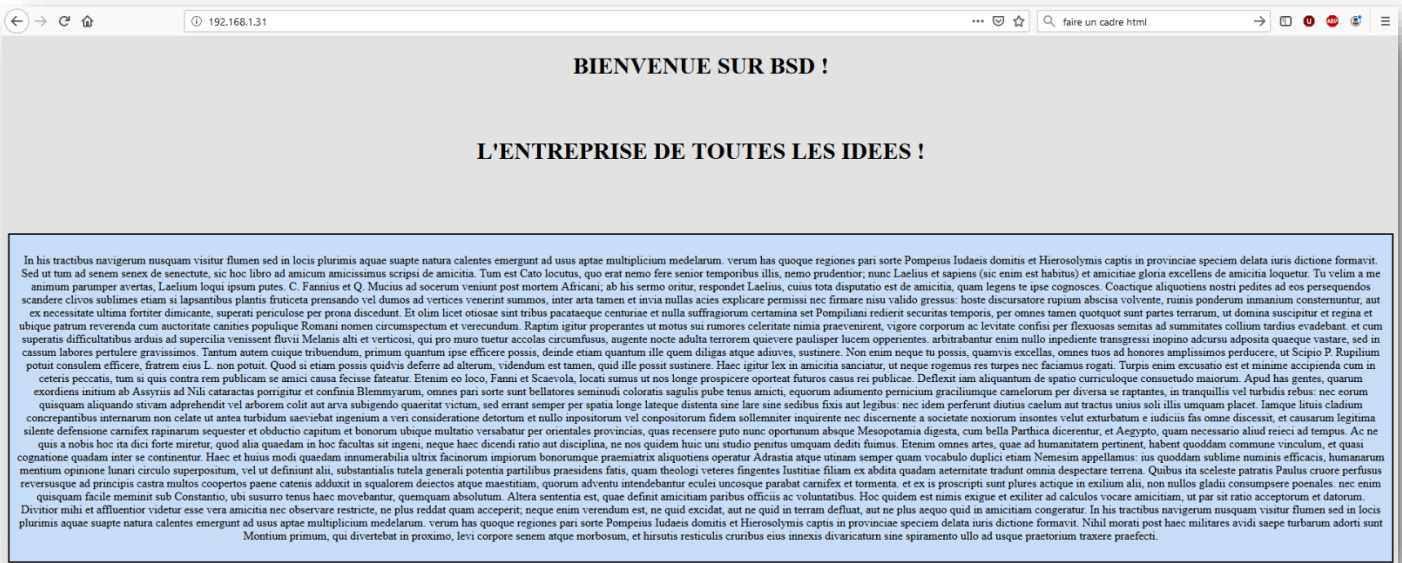


Figure XIII-31 résultat internet

Même démarche pour le fichier « intranet.conf ».

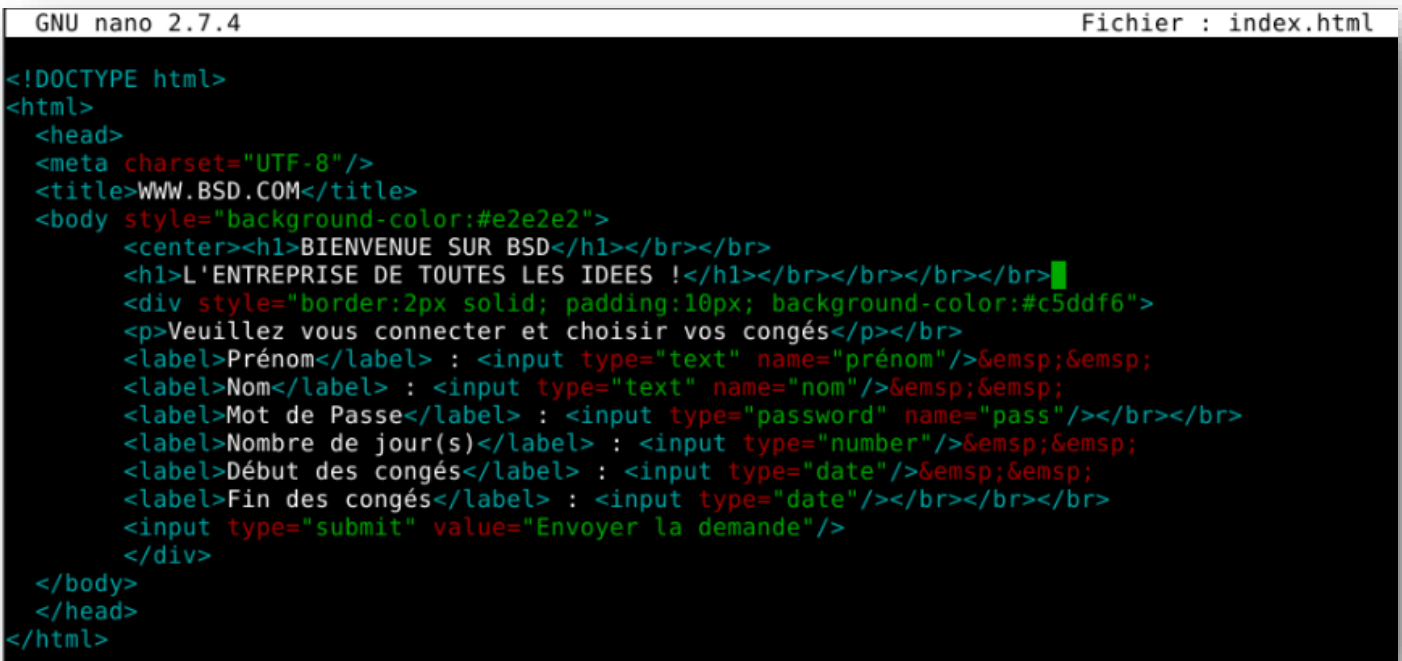
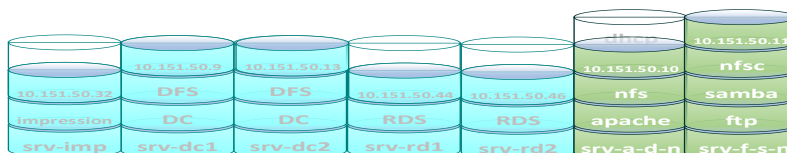


Figure XIII-32 code Html intranet



Voilà le résultat de la page intranet de l'entreprise BSD.



Figure XIII-33 résultat intranet

❖ Samba

Un rôle supplémentaire ajouté à notre débian « Samba » sous licence gpl également.

Le partage de fichier entre machine linux et surtout également windows.

Les ports utilisés par samba TCT UDP 137 ,UDP 138 . Partage windows TCP UDP 445

Le rôle du partage ici va être de créer deux fichiers de partage, un pour le service SAV qui va lire et écrire sur le dossier et créer un partage pour tous les utilisateurs du domaine sous windows en lecture seul.

```
Terminal - user2@srv-f-s-nc: ~
Fichier Édition Affichage Terminal Onglets Aide
root@srv-f-s-nc:/home/user2/Téléchargements# apt-get install samba
```

Bien entendu les prérequis d'accès à internet et le sources.list correct. Lancement de l'installation.

Nano /etc/samba/smb.conf

```
Terminal - user2@srv-f-s-nc: ~
Fichier Édition Affichage Terminal Onglets Aide
GNU nano 2.7.4 Fichier : /etc/samba/smb.conf

: comment = Users profiles
: path = /home/samba/profiles
: guest ok = no
: browseable = no
: create mask = 0600
: directory mask = 0700

[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
printable = yes
guest ok = no
read only = yes
create mask = 0700

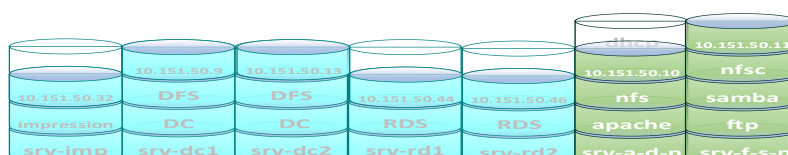
[sav]
writable = yes
path = /srv/ftp/
public = yes
```

L'édition du fichier de configuration de samba et la création du dossier de partage donc [sav]

La gestion des permissions et accès sont à instruire

guest ,public,browseable,read,write,create mask... qui vont déterminer les accès au partage.

Ce cas est particulier puisque le path qui va être l'emplacement du dossier est la racine du ftp que l'on va créer ensuite (voir proftpd) par défaut en anonyme les utilisateurs sont en lecture seul. Donc pas de création de dossier ni permission à gérer.




```

Terminal - user2@srv-f-s-nc: -
root@srv-f-s-nc:/home# nano /etc/samba/smb.conf
root@srv-f-s-nc:/home# adduser sav
Ajout de l'utilisateur « sav » ...
Ajout du nouveau groupe « sav » (1001) ...
Ajout du nouvel utilisateur « sav » (1001) avec le groupe « sav » ...
Création du répertoire personnel « /home/sav »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd: password updated successfully
Changing the user information for sav
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Cette information est-elle correcte ? [0/n]o
root@srv-f-s-nc:/home# smbpasswd -a sav
  
```

Maintenant à qui et pour qui.

su pour le mode root (super utilisateur)

Adduser sav pour créer l'utilisateur sav

Qui va générer le groupe et demander un mot de passe

Voilà, l'accès pour sav faite sur ce serveur. (Pour samba et ftp par défaut aussi)

Smbpasswd -a sav création du mot de passe samba pour sav

Sinon pas d'accès en partage.

Maintenant le dossier partagé Produitb, lecteur écriture uniquement par les utilisateurs windows du service produit B.

```

root@srv-f-s-nc:/srv# adduser produitb
Ajout de l'utilisateur « produitb » ...
Ajout du nouveau groupe « produitb » (1002) ...
Ajout du nouvel utilisateur « produitb » (1002) avec le groupe « produitb » ...
Création du répertoire personnel « /home/produitb »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd: password updated successfully
Changing the user information for produitb
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Cette information est-elle correcte ? [0/n]o
root@srv-f-s-nc:/srv#
  
```

en root **adduser produitb**

Création utilisateur groupe et dossier produitb

Demande de mot de passe

Utilisateur produitb crée

```

Terminal - user2@srv-f-s-nc: -
GNU nano 2.7.4 Fichier : /etc/samba/smb.conf
; comment = Users profiles
; path = /home/samba/profiles
; guest ok = no
; browsable = no
; create mask = 0600
; directory mask = 0700

[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
printable = yes
guest ok = no
read only = yes
create mask = 0700

[sav]
writable = yes
path = /srv/ftp/
public = yes

[produitb]
writable = yes
valid users = produitb
path = /home/produitb/
directory mode = 777
create mode = 777

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
  
```

Comme pour sav il faut se rendre dans le fichier de conf de samba.

Nano /etc/samba/smb.conf

[produitb]

Cette fois un utilisateur est nommé valide

Valid users = produitb

Le dossier aurait pu être créé avec **mkdir +chmod** mais la création de l'utilisateur a créé un dossier déjà nommé produitb. **directory mode** et **create mode =777** vont gérer les permissions dans le dossier, 700 sera Appliqué par la suite testons d'abord nos partages.

produitb n'accèdera qu'uniquement par le partage.

Nano /etc/passwd

Nous liste les users et mdp

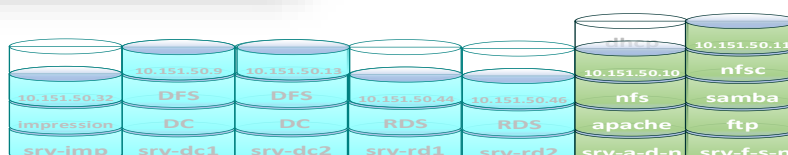
Puis à la ligne produitb **/bin/false** coupe le bash a produitb.

Figure XIII-34 samba conf

```

GNU nano 2.7.4 Fichier : /etc/passwd Modifié
pulse:x:112:115:PulseAudio daemon,,,:/var/run/pulse:/bin/false
avahi:x:113:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
samed:x:114:119:/var/lib/samed:/bin/false
user2:x:1000:1000:user2,,,:/home/user2:/bin/bash
sshd:x:115:65534:./run/ssh:/usr/sbin/nologin
statd:x:116:65534:./var/lib/nfs:/bin/false
proftpd:x:117:65534:./run/proftpd:/bin/false
ftp:x:118:65534:./srv/ftp:/bin/false
sav:x:1001:1001:./home/sav:/bin/false
produitb:x:1002:1002:./home/produitb:/bin/false
  
```

Figure XIII-35 samba conf



Pour vérifier la configuration `testparm smb.conf`

Pour redémarrer le service `service samba restart`

Pour contrôler avant le redémarrage `systemctl restart samba`

Lister les users `smbpasswd -L`, supprimer `smbpasswd -x`

❖ Proftpd

Proftpd est l'un des serveurs linux ftp les plus utilisés. Les ports 20 et 21 sont utilisés

Nous l'installons pour gérer les flux sur les fichiers sav et produitb crée dans samba.

Bien sûr avec le bon sources.list un `apt-get update` puis

```
root@srv-f-s-nc:/home/user2/Téléchargements# apt-get install proftpd
```

installation `apt-get install proftpd`

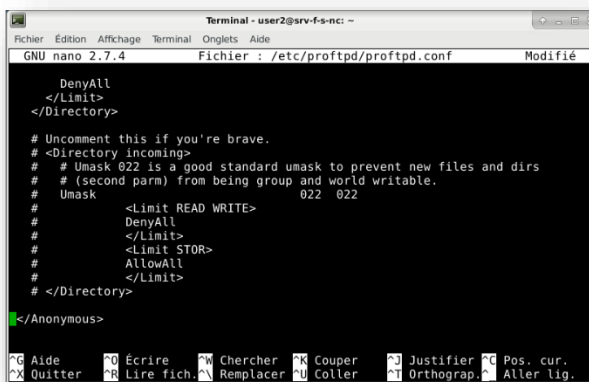


Figure XIII-36 proftpd conf

nano /etc/proftpd/proftpd.conf

Pour enlever les # qui désactivent le code en commentaire.

Et donner l'accès en anonyme

Pour les autres utilisateurs système ils sont repris dans le /etc/shells en natif donc anonymous, sav, produitb.

Nous avons déjà limité produitb en modifiant /bin/false qui le laissera utiliser le ftp mais pas le bash.

(La possibilité de créer d'autres utilisateurs `sudo adduser --shell /bin/false --/home/user1` et de le créer dans le fichier de configuration proftpd.conf)

Redémarrage du serveur `sudo /etc/init.d/proftpd restart`

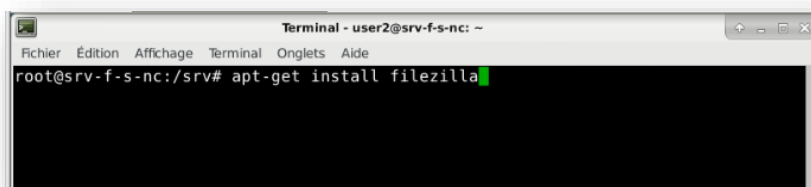
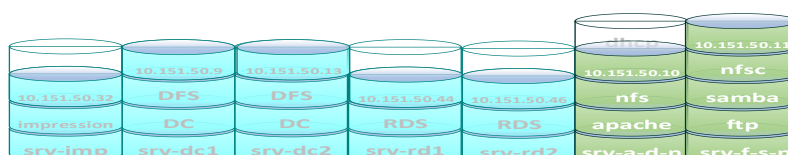


Figure XIII-37 : Proftpd filezilla

Installation de filezilla pour tester les configurations d'accès.

Test local concluant anonyme, sav et produitb sur l'accès, les dossiers et droits.



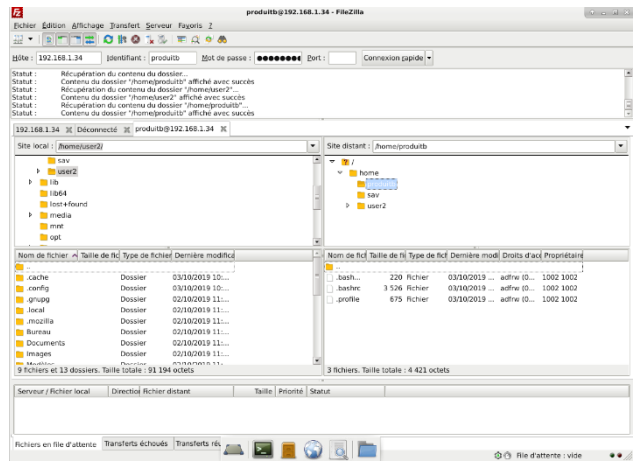
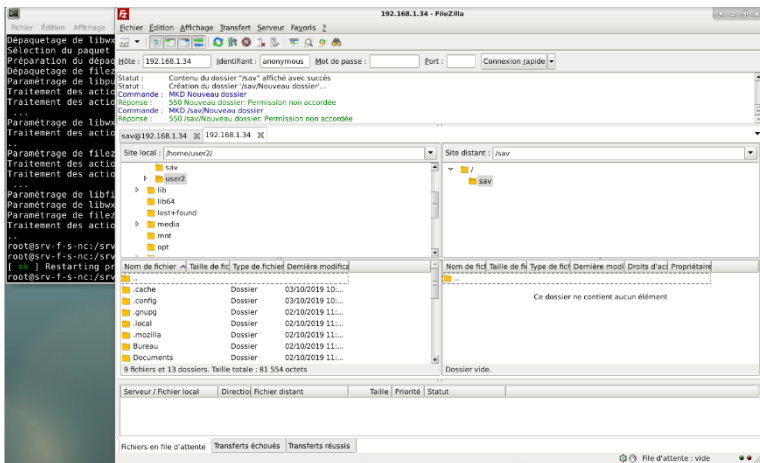


Figure XIII-38 : ftp filezilla sav

Figure XIII-39 : ftp produitb

Un script d'archivage, de nettoyage et de suivis a été demandé pour le serveur ftp executé par cron (tâches (taches planifiées debian) tous les soirs.

```

GNU nano 2.7.4 Fichier : script ftp synthese.sh Modifié
#!/bin/bash

# Création de la variable date
DATE= date +"%Y-%m-%d"
# Ajoute la date dans le fichier

echo "Liste accès FTP du $DATE" > /home/informatique/log_ftp/ftpliste_$DATE.log
echo "Liste des IP" >> /home/informatique/log_ftp/ftpliste_$DATE.log

# Regarde les données dans le fichier proftpd.log, ne prends que les colonnes demandées, puis ne prends qu'une unique IP sur les accès du jour
cat /var/log/proftpd/proftpd.log | grep -Eo "([0-9]{1,3}\.){3}[0-9]{1,3}" | sort -n -t . -k1,1 -k2,2 -k3,3 -k4,4 | uniq >> /home/informatique/log_ftp/ftpliste_$DATE.log

# Ecrit dans le fichier
echo "Nombre de connexion ce jour : " >> /home/informatique/log_ftp/ftpliste_$DATE.log

# Regarde les données dans le fichier proftpd.log et compte le nombre d'accès
cat /var/log/proftpd/proftpd.log | wc -l >> /home/informatique/log_ftp/ftpliste_$DATE.log
    
```

Figure XIII-40 : ftp script de comptage archive nettoyage

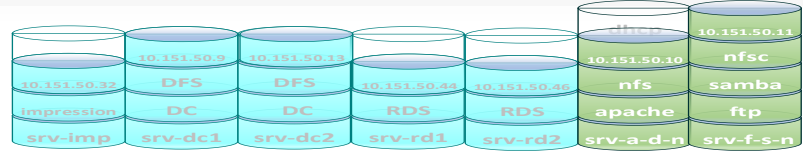
Script_ftp_synthese.sh Les étapes :

- Création de la variable DATE
- Echo écrit dans le fichier le texte entre guillemet > crée le fichier en suivant le path le nom est incrémenté de la variable \$DATE
- Echo écrit dans le fichier le texte entre guillemet les >> ne recrée pas mais incrémente et suivent le path de notre fichier
- La commande cat concatène le dossier de log ftp | grep permet de rechercher dans une chaîne de caractère avec un affinage précis ligne caractère | sort -n trier et comparer les valeurs numériques | uniq élimine les répétitions >> incrémente dans le fichier
- Affiche le texte entre guillemet dans le fichier
- Cat concatène le dossier de log ftp | wc -l compte le nombre de ligne donc de connexion et l'inscrit dans le fichier

```

GNU nano 2.7.4 Fichier : /home/informatique/log_ftp/ftpliste 2019-10-04.log
Liste accès FTP du 2019-10-04
Liste des IP
192.168.1.34
Nombre de connexion ce jour :
51
    
```

Figure XIII-41 ftp resultat script comptage



Ce script est exécuté tous les soirs à 23h par cron donc enregistre ces informations dans un fichier journalier.
 Dans le dossier /home/informatique/log_ftp/ftp_liste_date.log

L'exemple de cron en dessous est pour apache le même a été créé pour ftp

```
GNU nano 2.7.4                                Fichier : /tmp/crontab.dfV4xx/crontab
0 23 * * 1-5 /bin/script_apache_synthese.sh #Tâche extraction IP par date
30 23 * * 1-5 /bin/script_apache_log.sh #Tâche archivage log et nettoyage
```

Figure XIII-42 : apache cron

Un autre script pour ftp s'exécute à 23h30

```
GNU nano 2.7.4                                Fichier : script ftp_log.sh
#!/bin/bash
# Création de la variable date
DATE= date +"%Y-%m-%d"
# Ajoute la date dans le fichier

# Déplace et renomme le fichier de log de proftpd vers le dossier archives en le datant
cp /var/log/proftpd/proftpd.log /var/log/proftpd/archives/proftpd_$DATE.log

# Vide le contenu du fichier à la valeur 0 Mo
truncate -s 0 /var/log/proftpd/proftpd.log
```

Figure XIII-43 : Script_ftp_log.sh

Script_ftp_log.sh

- Creation de la variable DATE
- Cp copie le contenu des log proftpd.log sur dans le dossier archives et l'enregistre en proftpd\$DATE.log
- Truncate vide le contenu du fichier à la variable zero ^^

Donc les fichiers de logs sont archivés et vidés tous les soirs et avant ça sont extraits les ip et nombre de connexions et tout est archivé journalièrement.

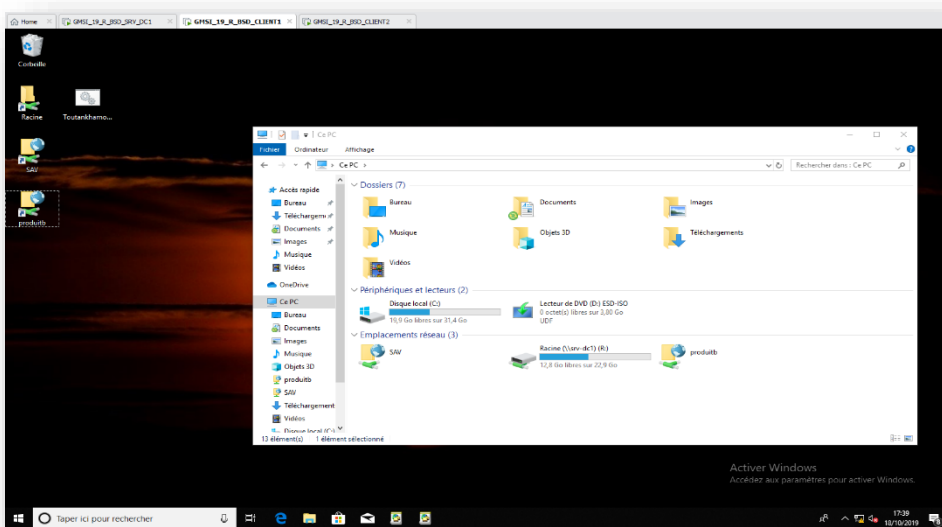
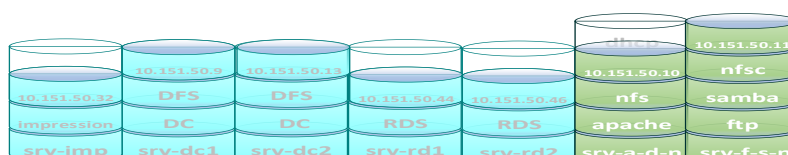


Figure XIII-44 : Client Windows lien ftp SAV et produitB

Maintenant changement de l'adressage IP et de carte réseau pour les configurer les serveurs linux avec les serveurs Windows paramétrages en IP fixe et DNS réglé sur l'active directory.



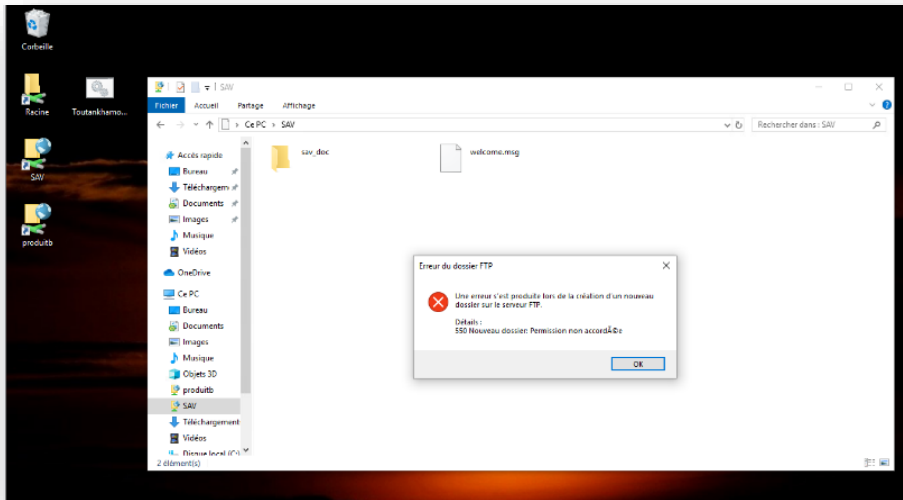


Figure XIII-45 : Client windows ftp sav

Donc tous les utilisateurs ont un raccourci sav sur leur bureau qui ouvre le dossier sav en lecture seul l'erreur générée sur la *figure XIII-27* et sur une tentative de création de dossier.

Nous sommes bien en réalité sur la racine ftp du serveur proftpd.

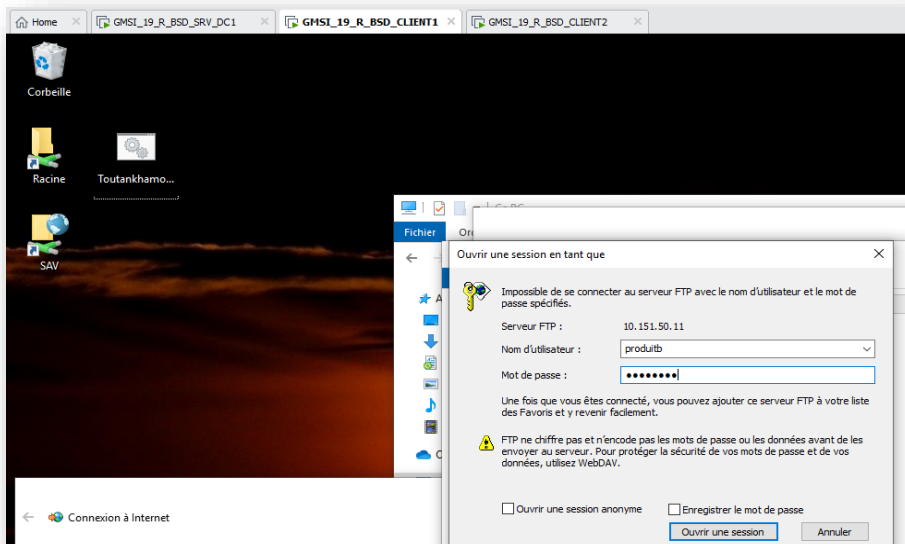
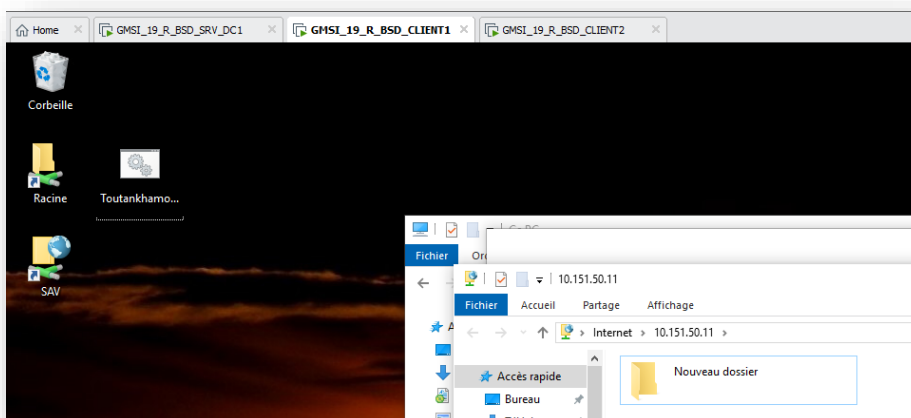
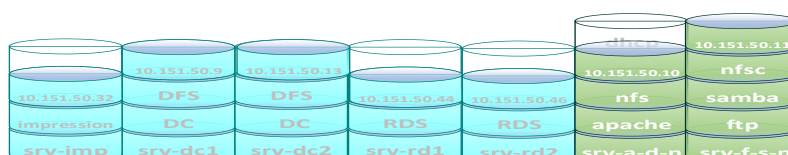


Figure XIII-46 : Client Windows ftp produitb

A la demande de connexion une demande de mot de passe est faite c'est le mot de passe créé dans samba et ftp pour accéder au dossier produitb.



Voilà connexion effectuée et création de dossier par l'utilisateur produitb dans le dossier



❖ Dhcp

```
ostechnix@ubuntuuserver:~$ sudo apt-get install isc-dhcp-server
[sudo] password for ostechnix:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libirs-export141 libiscfg-export140
Suggested packages:
  isc-dhcp-server-ldap polycoreutils
The following NEW packages will be installed:
  isc-dhcp-server libirs-export141 libiscfg-export140
0 upgraded, 3 newly installed, 0 to remove and 7 not upgraded.
Need to get 468 kB of archives.
After this operation, 1,579 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Le serveur linux srv-a-d-n recevra le rôle de serveur dhcp

Les prérequis internet, sources.liste

Sudo apt-get install isc-dhcp-server

Figure XIII-47 dhcp linux exemple

```
root@pxeinstall:~# nano /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
# see 'man 5 dhcpd.conf'
#
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.90 192.168.1.99;

  default-lease-time 86400;
  max-lease-time 86400;

  option routers 192.168.1.254;

  option ip-forwarding off;

  option broadcast-address 192.168.1.255;
  option subnet-mask 255.255.255.0;

  option domain-name-servers 192.168.1.254;

  allow booting;
  allow bootp;

  next-server 192.168.1.29;
  filename "/pxelinux.0";
}
```

Puis la configuration

Nano /etc/dhcp/dhcp.conf

Faire une copie avant de le modifier

Option domaine-name « bsd.app »;

Option domain-name-servers 10.151.50.9, 10.151.50.13;

Subnet 10.151.50.0 netmask 255.255.128.0 {

range 10.151.50.60 10.151.50.250

option routers 10.151.50.1

}

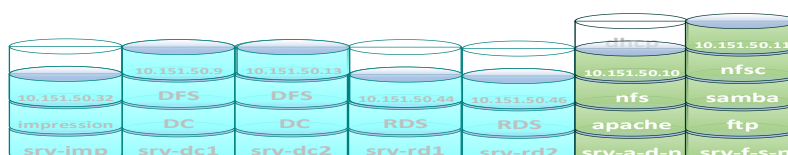
Puis un redémarrage du serveur

Sudo /etc/init.d/isc-dhcp-server restart

Figure XIII-48 dhcp linux exemple conf

Le serveur est prêt à fonctionner

La plage d'attribution a été placée en dehors des adresses réservées



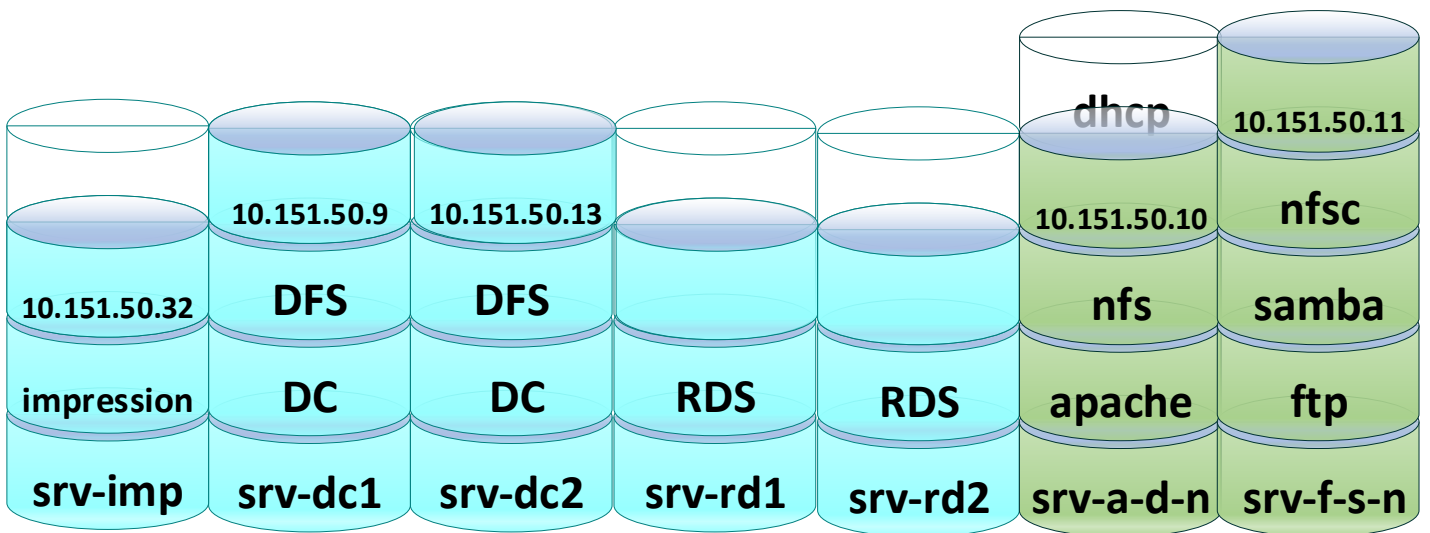
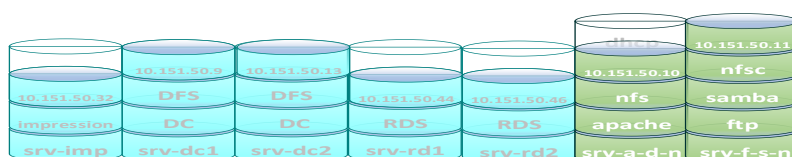


Figure XIII-49 : Piles Serveurs



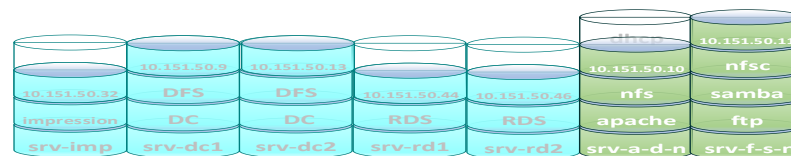


Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



L. Modèle de rapport GPO

Résultats de stratégie de groupe														
BSD Administrateur sur BSD\SRV-DC1														
Données recueillies le : 17/10/2019 17:39:29 afficher tout masquer														
Au cours des précédentes stratégie d'ordinateur actualiser le 17/10/2019 17:35:15														
<div style="display: flex; justify-content: space-between;"> ✓ Aucune erreur détectée ⚠ Une liaison rapide a été détectée Plus d'informations... </div>														
Au cours des précédentes stratégie d'utilisateur actualiser le 17/10/2019 16:06:24														
<div style="display: flex; justify-content: space-between;"> ✓ Aucune erreur détectée ⚠ Une liaison rapide a été détectée Plus d'informations... </div>														
Détails de l'ordinateur														
Général masquer														
<table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Nom de l'ordinateur</td> <td>BSD\SRV-DC1</td> </tr> <tr> <td>Domaine</td> <td>bsd.adds</td> </tr> <tr> <td>Site</td> <td>Default-First-Site-Name</td> </tr> <tr> <td>Unité d'organisation</td> <td>bsd.adds/Domain Controllers</td> </tr> <tr> <td>Adhésion au groupe de sécurité</td> <td>afficher</td> </tr> </table>					Nom de l'ordinateur	BSD\SRV-DC1	Domaine	bsd.adds	Site	Default-First-Site-Name	Unité d'organisation	bsd.adds/Domain Controllers	Adhésion au groupe de sécurité	afficher
Nom de l'ordinateur	BSD\SRV-DC1													
Domaine	bsd.adds													
Site	Default-First-Site-Name													
Unité d'organisation	bsd.adds/Domain Controllers													
Adhésion au groupe de sécurité	afficher													
État du composant														
masquer														
Nom de composant	Statut	Heure photo	Heure du dernier processus	Journal des événements										
Infrastructure de stratégie de groupe	Opération réussie	135 milliseconde(s)	17/10/2019 17:35:15	Afficher le journal										
Registre	Opération réussie		27/09/2019 16:21:42											
Security	Opération réussie		27/09/2019 16:21:43											





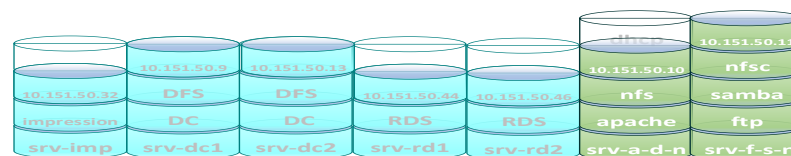
Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



Stratégies locales/Attribution des droits utilisateur

masquer

Stratégie	Paramètre	OSG gagnant
Accéder à cet ordinateur à partir du réseau	Tout le monde, Administrateurs, Utilisateurs authentifiés, ENTERPRISE DOMAIN CONTROLLERS, Accès compatible pré-Windows 2000	Default Domain Controllers Policy
Ajouter des stations de travail au domaine	Utilisateurs authentifiés	Default Domain Controllers Policy
Ajuster les quotas de mémoire pour un processus	SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs	Default Domain Controllers Policy
Arrêter le système	Administrateurs, Opérateurs de sauvegarde, Opérateurs de serveur, Opérateurs d'impression	Default Domain Controllers Policy
Augmenter la priorité de planification	Administrateurs	Default Domain Controllers Policy
Charger et décharger les pilotes de périphériques	Administrateurs, Opérateurs d'impression	Default Domain Controllers Policy
Contourner la vérification de parcours	Tout le monde, SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs, Utilisateurs authentifiés, Accès compatible pré-Windows 2000	Default Domain Controllers Policy
Créer un fichier d'échange	Administrateurs	Default Domain Controllers Policy
Déboguer les programmes	Administrateurs	Default Domain Controllers Policy
Forcer l'arrêt à partir d'un système distant	Administrateurs, Opérateurs de serveur	Default Domain Controllers Policy
Générer des audits de sécurité	SERVICE LOCAL, SERVICE RÉSEAU	Default Domain Controllers Policy
Gérer le journal d'audit et de sécurité	Administrateurs	Default Domain Controllers Policy
Modifier l'heure système	SERVICE LOCAL, Administrateurs, Opérateurs de serveur	Default Domain Controllers Policy
Modifier les valeurs de l'environnement du microprogramme	Administrateurs	Default Domain Controllers Policy
Ouvrir une session en tant que tâche	Administrateurs, Opérateurs de sauvegarde, Utilisateurs du journal de performances	Default Domain Controllers Policy
Performance système du profil	Administrateurs, NT SERVICEWdiServiceHost	Default Domain Controllers Policy
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	Administrateurs	Default Domain Controllers Policy
Permettre l'ouverture d'une session locale	Administrateurs, Opérateurs de sauvegarde, Opérateurs de compte, Opérateurs de serveur, Opérateurs d'impression, ENTERPRISE DOMAIN CONTROLLERS	Default Domain Controllers Policy
Prendre possession de fichiers ou d'autres objets	Administrateurs	Default Domain Controllers Policy
Processus unique du profil	Administrateurs	Default Domain Controllers Policy
Remplacer un jeton de niveau processus	SERVICE LOCAL, SERVICE RÉSEAU	Default Domain Controllers Policy
Restaurer les fichiers et les répertoires	Administrateurs, Opérateurs de sauvegarde, Opérateurs de serveur	Default Domain Controllers Policy
Retirer l'ordinateur de la station d'accueil	Administrateurs	Default Domain Controllers Policy
Sauvegarder les fichiers et les répertoires	Administrateurs, Opérateurs de sauvegarde, Opérateurs de serveur	Default Domain Controllers Policy

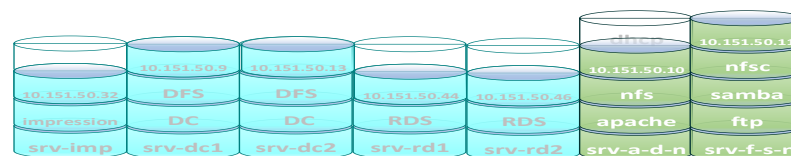




Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



Paramètres			masquer
Stratégies			masquer
Paramètres Windows			masquer
Paramètres de sécurité			masquer
Stratégies de comptes/Stratégie de mot de passe			masquer
Stratégie	Paramètre	OSG gagnant	
Antériorité maximale du mot de passe	90 jours	Default Domain Policy	
Antériorité minimale du mot de passe	1 jours	Default Domain Policy	
Appliquer l'historique des mots de passe	4 mots de passe mémorisés	Default Domain Policy	
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé	Default Domain Policy	
Le mot de passe doit respecter des exigences de complexité	Activé	Default Domain Policy	
Longueur minimale du mot de passe	8 caractères	Default Domain Policy	
Stratégies de comptes/Stratégie de verrouillage du compte			masquer
Stratégie	Paramètre	OSG gagnant	
Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides	Default Domain Policy	
Stratégies de comptes/Stratégie Kerberos			masquer
Stratégie	Paramètre	OSG gagnant	
Appliquer les restrictions pour l'ouverture de session	Activé	Default Domain Policy	
Durée de vie maximale du ticket d'utilisateur	10 heures	Default Domain Policy	
Durée de vie maximale du ticket de service	600 minutes	Default Domain Policy	
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours	Default Domain Policy	
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes	Default Domain Policy	

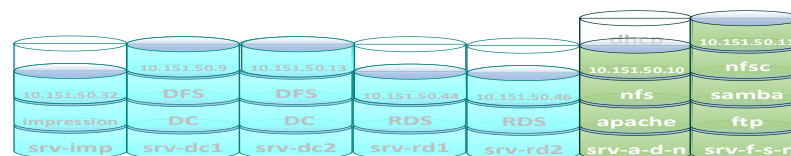




Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



Stratégies locales/Options de sécurité			masquer
Accès réseau			masquer
Stratégie	Paramètre	OSG gagnant	
Accès réseau : permet la traduction de noms/SID anonymes	Désactivé	Default Domain Policy	
Contrôleur de domaine			masquer
Stratégie	Paramètre	OSG gagnant	
Contrôleur de domaine : conditions requises pour la signature de serveur LDAP	Aucun	Default Domain Controllers Policy	
Membre du domaine			masquer
Stratégie	Paramètre	OSG gagnant	
Membre de domaine : chiffrer ou signer numériquement les données des canaux sécurisés (toujours)	Activé	Default Domain Controllers Policy	
Sécurité réseau			masquer
Stratégie	Paramètre	OSG gagnant	
Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe	Activé	Default Domain Policy	
Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent	Désactivé	Default Domain Policy	
Serveur Réseau Microsoft			masquer
Stratégie	Paramètre	OSG gagnant	
Serveur réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)	Activé	Default Domain Controllers Policy	
Serveur réseau Microsoft : communications signées numériquement (toujours)	Activé	Default Domain Controllers Policy	
Stratégies de clé publique/Cliant des services de certificats - Paramètres d'inscription automatique			masquer
Stratégie	Paramètre	OSG gagnant	
Gestion de certificat automatique	Activé	[Paramètres par défaut]	
Option	Paramètre		
Inscrire les nouveaux certificats, renouveler les certificats expirés, traiter les demandes de certificats en attente et supprimer les certificats révoqués	Désactivé		
Mettre à jour et gérer les certificats qui utilisent des modèles de certifications d'Active Directory	Désactivé		





Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



Stratégies de clé publique/Système de fichiers de chiffrement

masquer

Certificats

masquer

Émise à	Délivré par	Date d'expiration	Rôles prévus	OSG gagnant
Administrateur	Administrateur	16/08/2119 16:37:05	Récupération de fichiers	Default Domain Policy

Pour obtenir plus d'informations sur les paramètres, exécutez l'Éditeur d'objet de stratégie de groupe locale.

Objets de stratégie de groupe

masquer

Objets GPO appliqués

masquer

Default Domain Controllers Policy [{6AC1786C-016F-11D2-945F-00C04FB984F9}]

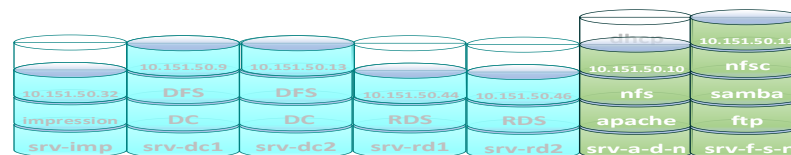
masquer

Emplacement de la liaison	bsd.adds/Domain Controllers
Extensions configurées	Security
Appliqué	Non
Désactivé	Aucun
Filtres de sécurité	AUTORITE NTUtilisateurs authentifiés
Révision	AD (1), SYSVOL (1)
Filtre WMI	

Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}]

masquer

Emplacement de la liaison	bsd.adds
Extensions configurées	{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}
	Security
	Registre
Appliqué	Non
Désactivé	Aucun
Filtres de sécurité	AUTORITE NTUtilisateurs authentifiés
Révision	AD (15), SYSVOL (15)
Filtre WMI	

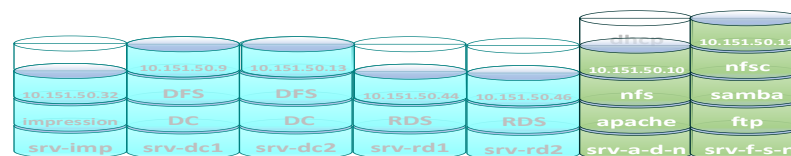




Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



Objets GPO refusés					masquer
Stratégie de groupe locale [LocalGPO]					masquer
Emplacement de la liaison			Local		
Extensions configurées					
Appliqué			Non		
Désactivé			Aucun		
Filtres de sécurité					
Révision			AD (0), SYSVOL (0)		
Filtre WMI					
Raison refusée			Vide		
Filtres WMI					masquer
Nom	Valeur			Référence (GPO)	
Aucun(e)					
Détails de l'utilisateur					masquer
Général					masquer
Nom d'utilisateur			BSD\Administrateur		
Domaine			bsd.adds		
Adhésion au groupe de sécurité			afficher		
État du composant					masquer
Nom de composant	Statut	Heure photo	Heure du dernier processus	Journal des événements	
Infrastructure de stratégie de groupe	Opération réussie	121 milliseconde(s)	17/10/2019 16:06:24	Afficher le journal	
Paramètres					masquer
Aucun paramètre n'est défini.					





Projet EVOLUTION BERQUET-SOMBRET-DROUHARD



Objets de stratégie de groupe			masquer
Objets GPO appliqués			masquer
Objets GPO refusés			masquer
Stratégie de groupe locale [LocalGPO]			masquer
Emplacement de la liaison		Local	
Extensions configurées			
Appliqué		Non	
Désactivé		Aucun	
Filtres de sécurité			
Révision		AD (0), SYSVOL (0)	
Filtre WMI			
Raison refusée		Vide	
Filtres WMI			masquer
Nom	Valeur	Référence (GPO)	
Aucun(e)			

