

BTS Services informatiques aux organisations
1^{re} année

Pacôme Massol

Support des services et des serveurs

Travaux pratiques

Directeur de publication : Serge Bergamelli

Les cours du Cned sont strictement réservés à l'usage privé de leurs destinataires et ne sont pas destinés à une utilisation collective. Les personnes qui s'en serviraient pour d'autres usages, qui en feraient une reproduction intégrale ou partielle, une traduction sans le consentement du Cned, s'exposeraient à des poursuites judiciaires et aux sanctions pénales prévues par le Code de la propriété intellectuelle. Les reproductions par reprographie de livres et de périodiques protégés contenues dans cet ouvrage sont effectuées par le Cned avec l'autorisation du Centre français d'exploitation du droit de copie (20, rue des Grands Augustins, 75006 Paris).

Sommaire

Conseils généraux	5
Atelier 1 : Anatomie d'un serveur	7
Atelier 2 : Installation de Windows 2008 R2	19
Atelier 3 : Installation d'un domaine Windows 2008 R2	27
Atelier 4 : Gestion des utilisateurs du domaine	39
Atelier 5 : Intégration d'une station au domaine	55
Atelier 6 : Administration à distance Windows	69
Atelier 7 : Serveur d'application web Windows	77
Atelier 8 : SQL Server 2008 R2	93
Atelier 9 : Initiation au PowerShell	119
Atelier 10 : Présentation de Linux Debian	131
Atelier 11 : Installation de Linux Debian	135
Atelier 12 : Linux : la ligne de commande	159
Atelier 13 : Gestion des paquets Debian	177
Atelier 14 : Généralités sur les services réseaux	183
Atelier 15 : Gestion des utilisateurs et des permissions	193
Atelier 16 : Administration à distance	201
Atelier 17 : Installation d'un serveur Web	211
Atelier 18 : Installation de Php/MySQL	225
Atelier 19 : Installation de Java/Tomcat	235
Atelier 20 : Apache et https	245
Atelier 21 : Virtualisation	255
Corrigés des ateliers	270

Conseils généraux

1. Objectifs

Nous partageons un profil d'enseignant informatique et de responsable d'un service informatique. Cet avantage nous permettra de poursuivre, dans ce cours, un double objectif :

- une approche pédagogique vous permettant d'appréhender le domaine complexe des réseaux informatiques en partant de la « base » ;
- une approche professionnelle vous présentant les connaissances, les outils et les méthodes dont vous aurez besoin sur le marché du travail. Nous partagerons avec vous, dès que cela sera possible, notre expérience du « terrain ».

Voici l'état d'esprit dans lequel vous devez étudier ce cours (vous remarquerez que ce sont les mêmes qualités qui sont appréciées dans un entretien d'embauche) :

- méthode et rigueur : la mise en oeuvre d'un nouveau service réseau ou la résolution de problèmes seront votre pain quotidien. Autant avoir les bons réflexes pour être efficace : lire les manuels de référence, exploiter les journaux, mettre en oeuvre les outils de surveillance et de débogage, etc.
- autonomie : l'informatique évolue constamment, la plupart des problèmes que nous rencontrons, nous ne les rencontrerons qu'une fois mais la plupart du temps d'autres les ont déjà rencontré : il faut savoir chercher les informations à la **bonne** source.
- lecture de l'anglais technique : la plupart des documentations sont en anglais... désolé mais c'est comme ça et ce n'est pas prêt de s'arranger. Sans se lancer dans des études approfondies de l'anglais littéraire, sachez que l'acquisition du vocabulaire se fera petit à petit au fur et à mesure de vos lectures.

Ces ateliers font partie d'un module de cours commun aux deux spécialités du BTS. Nous essayons donc de traiter ce qui sera utile aux SLAM dans leur futur emploi. En effet, développement et réseau sont intimement liés et vous devez acquérir une culture en ce domaine. Quant aux SISR, ils auront largement la possibilité d'approfondir tout ceci dans les modules de cours à venir.

2. Organisation de ce fascicule

Ces ateliers sont articulés autour des deux systèmes d'exploitation serveur que vous retrouverez en entreprise. La première partie est consacrée à Windows 2008 R2 et la deuxième à Linux. Nous aurons pu étudier les deux en parallèle et voir pour chaque sujet comment le traiter avec Windows et avec Linux. Mais, compte tenu du faible volume horaire de ce module, ce n'est pas possible. Il a donc fallu faire des choix qui se rapprochent des pratiques les plus répandues dans l'entreprise.

3. Comment compléter ces ateliers ?

Malgré tout le soin que nous apportons à la rédaction, vous aurez probablement des questions, des incompréhensions, des difficultés, etc. C'est a priori normal. Voici les références conseillées :

- Livres
 - « Technologie des ordinateurs et des réseaux » de notre collègue PA Goupille : excellent livre, bien adapté pour le BTS.
 - « Les réseaux » de Guy Pujolle : la référence mais l'approche n'est pas forcément très simple.
- Sites
 - Wikipedia : l'encyclopédie en ligne est bien fournie sur le domaine des réseaux. Par expérience, je dirai que les pages en anglais sont plus développées que les pages en français.
 - <http://www.laissus.fr/cours/cours.html>
 - <http://christian.caleca.free.fr/>
 - <http://www.linux-france.org/prj/inetdoc>
 - <http://www.debian.org> pour tous les TP sous Debian. Le site contient toutes les documentations (installation, configuration) nécessaires et en français.
 - <http://www.labo-microsoft.org> pour tous les TP sous Windows. Le site développe la plupart des aspects de l'administration.
- Forums du CNED



Si vous poursuivez dans la spécialité SISR, conservez toutes les machines virtuelles créées dans ces ateliers, vous en aurez besoin dans les prochains modules.

Nous vous souhaitons une bonne formation.

Atelier 1

Anatomie d'un serveur

► **Durée approximative de cet atelier : 1 heure**

► **Objectif**

Faire un tour d'horizon d'un « vrai » serveur.

► **Durée approximative de cet atelier**

Aucune en particulier.

► **Considérations techniques**

Aucune. Vous pouvez « observer » ce TP si vous n'avez pas de serveur sous la main. Sinon, rapprochez ce qui est exposé avec le matériel de votre entreprise, qu'il soit dans les locaux ou hébergé.

► **Contenu**

1. Introduction	8
2. Architecture	8
3. Onduleur	15
4. Stockage/sauvegarde.....	16

1. Introduction

Que nous soyons particulier ou professionnel, il faut admettre que nous sommes dépendants de la technique : les serveurs et l'accès internet. Si l'un des deux n'est pas disponible, il est très difficile de travailler. Il est donc fondamental pour l'entreprise de se doter de matériel fiable. Le serveur est au coeur de son système d'information et l'objectif est la continuité de service (même si un composant tombe en panne).

Nous présentons ici deux aspects : l'architecture matérielle courante d'un serveur puis, plus en détail, la gestion des disques.

2. Architecture

2A. Boîtier

Un serveur est généralement présenté en « rack » dans une armoire. Certes un serveur peut être au format « tour » mais c'est maintenant plus rare en raison de la place perdue et des problèmes d'organisation que cela pose lorsque plusieurs serveurs sont utilisés.

Le facteur de forme (i.e. l'épaisseur de l'appareil) va déterminer ses capacités d'extension, en particulier dans le domaine du stockage et du nombre de processeurs.

Le plus petit modèle est le « 1U ». Cet appareil peut néanmoins embarquer jusqu'à 4 disques (on observe ici les 4 tiroirs), 1 lecteur/graveur de DVD, 2 processeurs et plusieurs dizaines de Gio de RAM :

Atelier 1

Anatomie
d'un serveur

Page 8



Figure 1 : Serveur 1U

1U correspond à la place occupée dans une armoire :



Figure 2 : serveur 1U dans une armoire

Les capacités de ce genre de machine peuvent s'avérer insuffisantes dans certains cas (espace disque par exemple). On peut alors passer sur des appareils 2 U :



Figure 3 : serveur 2U

Les possibilités d'évolution sont plus importantes. Ce serveur dispose de 4x3 disques. De nombreuses cartes d'extension au format PCI-Express ou PCI-X peuvent être insérées dans l'appareil.

Le format 4U est encore plus complet :



Figure 4 : Serveur 4U

Atelier 1

Anatomie
d'un serveur

Page 9

Les hébergeurs gèrent de nombreux serveurs. Afin de gagner de la place et de faciliter la gestion, ils peuvent faire appel à des serveurs de type « lame » (blade) qui accueillent dans un seul boîtier plusieurs serveurs indépendants :

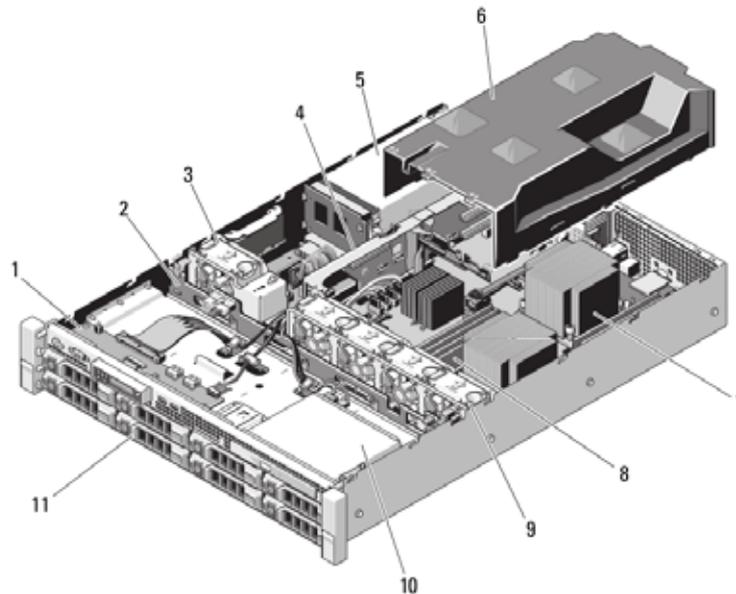


Figure 5 : serveur «lame»

Chaque carte correspond à un serveur : 1 à 2 processeurs, RAM, 2 disques.

2B. Structure interne

Observons maintenant l'intérieur d'un 2U :



1	Carte du panneau de commande	2	Fond de panier SAS
3	Ventilateur	4	Carte de montage pour carte d'extension
5	Baies de bloc d'alimentation (2)	6	Carénage de refroidissement
7	Dissipateur de chaleur/processeur (2)	8	Barrettes de mémoire (8)
9	Ventilateurs du système (4)	10	Lecteur optique (en option)
11	Disques durs (8)		

Atelier 1

Anatomie
d'un serveur

Page 10

Figure 6 : Structure d'un 2U (source : DELL)

Un élément marquant est la présence de nombreux ventilateurs qui doivent dissiper la chaleur d'une machine prévue pour tourner 24/7.

2C. Alimentation

Première chose sensible dans un serveur : l'alimentation électrique. Il est fortement conseillé de prévoir des systèmes à double alimentation afin de pallier à la défaillance de l'une :



Figure 7 : double alimentation

Chaque alimentation est indépendante. Elle peut être retirée et remplacée à chaud :



Figure 8 : alimentation hot-plug

Atelier 1

Anatomie
d'un serveur

Page 11

2D. Les disques

Les autres éléments très sensibles dans un serveur sont les disques. En effet, ils contiennent de précieuses données. Et même si celles-ci sont sauvegardées, on cherche à gérer les éventuelles pannes afin d'éviter l'arrêt des machines et de fastidieuses opérations de restauration. Les disques sont placés dans des tiroirs qui permettent de les extraire en cas de panne ou d'en ajouter en cas de saturation :



Figure 9 : tiroirs pour disques hot-plug

Différents modes de gestion (RAID) et technologies (SATA ou SAS) sont possibles. Par expérience du terrain, deux modes sont particulièrement privilégiés :

- RAID 1 SATA : pour des serveurs d'application (serveurs web par exemple)
- RAID 5 SAS : pour des serveurs de bases de données (accès intensif aux données)

Exercice 1

Rappelez les spécificités du RAID 1 et du RAID 5. Combien de disques au minimum faut-il pour chacun de ces modes ? Que signifie « spare disk » dans le mode RAID 5 ?

La configuration des disques se fait au démarrage, dans un BIOS spécifique, après le setup du BIOS du serveur et avant toute installation de système d'exploitation. Nous observons ci-après la création d'un volume logique en RAID 5 constitué de 4 disques. La notion de « volume logique » signifie que le système d'exploitation ne verra qu'un seul disque sans se douter de l'organisation matérielle sous-jacente, la gestion du RAID étant assurée par le contrôleur RAID : une carte d'extension¹ insérée dans le serveur.

2D1. Choix du niveau de RAID

Ce contrôleur propose différents modes de gestion du RAID :

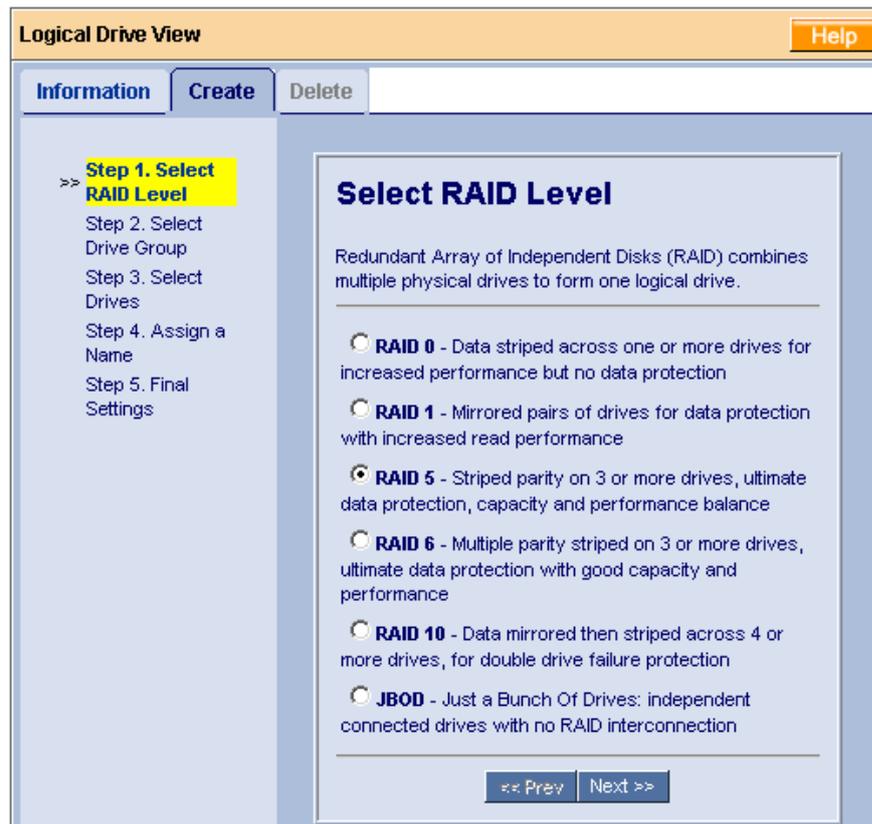


Figure 10 : choix du niveau de RAID

2D2. Choix du disque logique

Ici, l'espace libre est sélectionné puisque aucun volume n'existe. Il est en effet possible d'ajouter a posteriori des disques à un volume logique afin d'étendre sa capacité.

1. Nous ne recommandons pas le RAID logiciel, géré par le système d'exploitation coûteuse en termes de CPU.

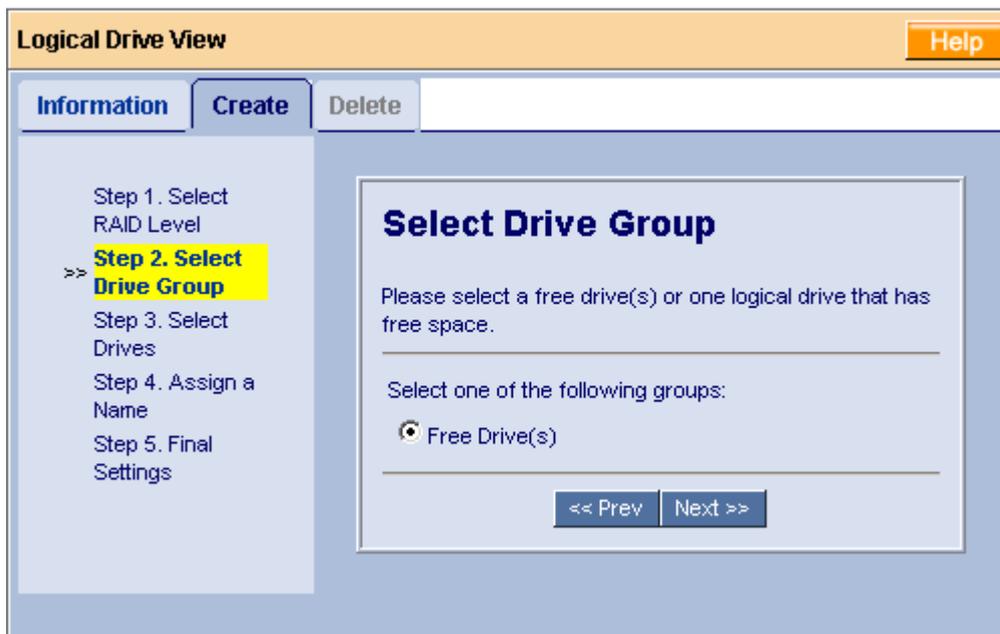


Figure 11 : choix du volume logique

2D3. Choix des disques physiques

Une fois un volume logique constitué, on y ajoute des disques durs. Un contrôleur peut gérer plusieurs volumes logiques, constitués de disques différents. Dans ce cas, 4 disques sont ajoutés au volume logique, chaque disque aura le même niveau (selected). Mais, il est également possible de définir ici un ou plusieurs disques de rechange (spare). Le contrôleur remplacera automatiquement un disque défaillant le cas échéant :

Atelier 1

Anatomie
d'un serveur

Page 13

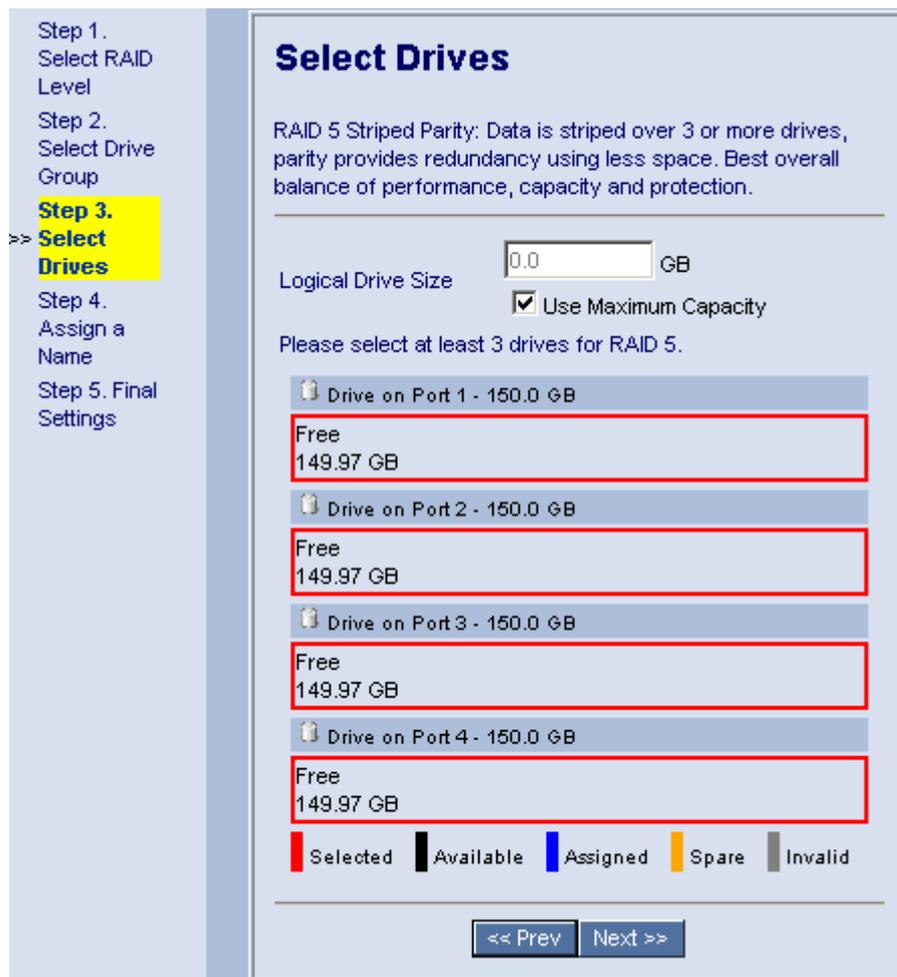


Figure 12 : choix des disques physiques

Exercice 2

Quelle est la capacité de chaque disque dur ? Quelle sera la capacité globale de stockage de ce volume logique en fonction de l'organisation proposée plus haut ?

2D4. Derniers paramétrages

Il est possible de jouer sur certains paramètres « avancés ». Mais par expérience, nous n'avons jamais modifié ces paramètres et toujours conservé les paramètres par défaut. Un point important est à souligner : le paramètre « write cache » est particulièrement redoutable en cas de panne de courant. En effet, dans le mode « write back », les données ne sont pas écrites immédiatement sur disque mais uniquement dans le cache du contrôleur RAID. Si celui-ci n'a pas de batterie, des données peuvent être perdues en cas de coupure ! Dans le doute, il est préférable de conserver le mode « write through ».

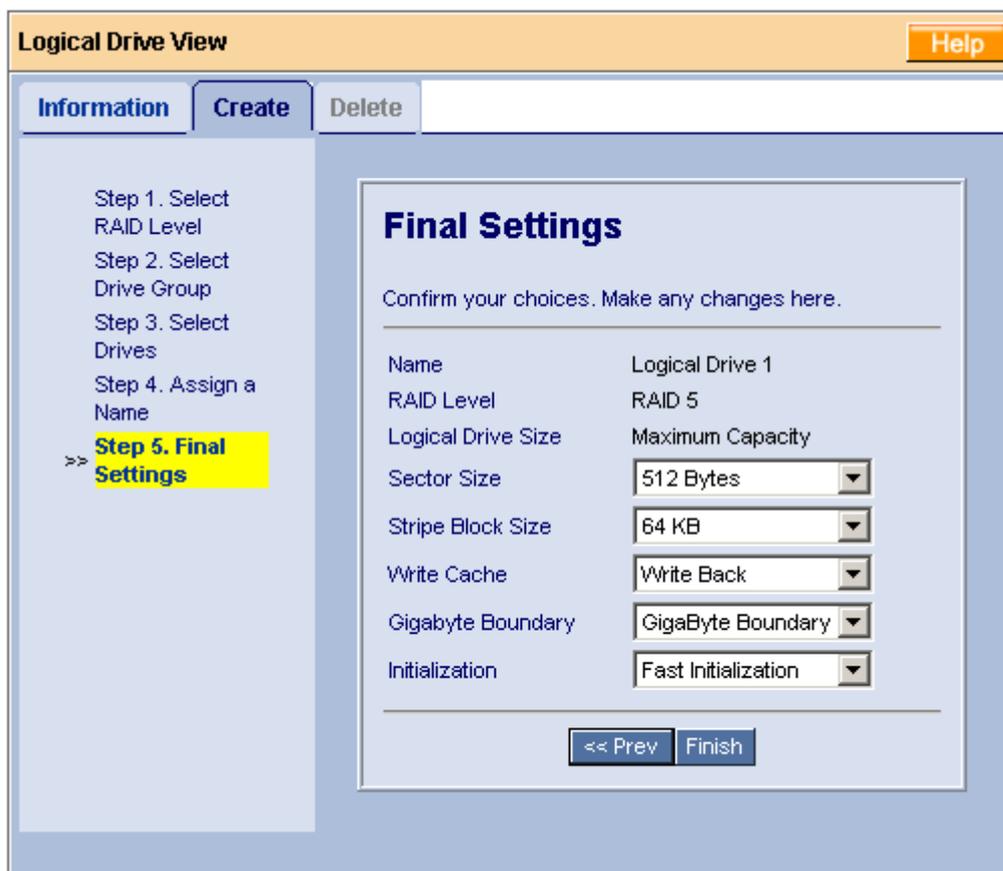


Figure 13 : Paramètres avancés

Atelier 1

Anatomie
d'un serveur

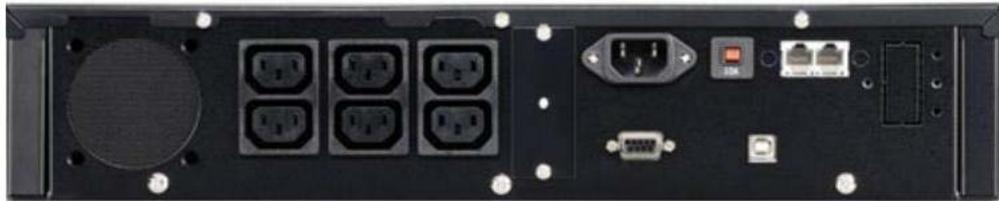
Page 15

3. Onduleur

Dans un environnement de datacenter, le courant électrique est déjà filtré et protégé. Des groupes électrogènes peuvent se déclencher si besoin. Dans un cadre d'entreprise, il faut envisager d'acquérir des onduleurs qui pourront protéger un ou plusieurs serveurs des surtensions et des coupures. Le boîtier se présente comme un serveur 2U mais il ne contient quasiment que des batteries. À l'arrière, des prises permettent de connecter les alimentations électriques des serveurs protégés :



Rear Panel - 2U



Rear Panel - 3U



Figure 14 : Divers onduleurs rackables

Atelier 1

Anatomie d'un serveur

Page 16

La durée de la protection électrique fournie par un onduleur est exprimée en **VA** (*Volt-Ampère*). On considère généralement que pour une protection électrique correspondant à une coupure électrique de 10 minutes, il est nécessaire de se doter d'un onduleur ayant une capacité égale à la puissance de l'ensemble des matériels raccordés à l'onduleur multiplié par un coefficient 1,6.

4. Stockage/sauvegarde

Lorsque de grandes quantités de données sont à gérer ou à sauvegarder, un SAN (Storage Area Network) peut être mis en oeuvre. Le ou les serveurs maîtres voient le SAN comme un ou plusieurs disques directement connectés (alors qu'ils sont utilisés à travers le réseau) :



Figure 15 : armoire SAN

À retenir

Un serveur dispose d'une architecture particulière. En fonction de l'évolutivité souhaitée, on choisira un boîtier 1U, 2U ou 4U. Lorsque de nombreux serveurs doivent être mis en service, une solution de type « lame » pourra être étudiée.

Deux éléments sont particulièrement sensibles dans un ordinateur, a fortiori dans un serveur :

- l'alimentation électrique : choisir un modèle à double alimentation, remplaçable à chaud,
- la gestion des disques : choisir un mode RAID 1 et/ou RAID 5 suivant les cas, contrôleur RAID de préférence avec mémoire cache et batterie intégrées, disques remplaçables à chaud.

Afin d'améliorer la protection électrique, un onduleur s'avère indispensable. La sauvegarde et la protection des données peut passer par un SAN dans le cadre d'une grande entreprise.

Si vous voulez approfondir

Consulter les sites de fabricants (DELL, HP, IBM). Faire des devis en ligne pour observer les différentes solutions techniques proposées et les prix.

Atelier 2

Installation de Windows 2008 R2

► Durée approximative de cet atelier : 1 heure

► Objectif

Installer un Windows 2008 server R2 en vue des prochains TP.

► Durée approximative de cet atelier

Aucune en particulier.

► Considérations techniques

Après avoir travaillé avec différents systèmes d'exploitation à destination des utilisateurs (Windows 7 pro ou Android), nous installons maintenant un système d'exploitation de type « Windows serveur » que nous utiliserons pendant toute la première partie de ce fascicule de TP.

L'image ISO du DVD de votre Windows 2008 R2 server est à récupérer sur le site MSDNAA du CNED.

Nous travaillons ici avec une machine virtuelle VirtualBox. Ce n'est bien sûr qu'à des fins de formation. En **production**, autrement dit dans la « vraie vie », vous l'installerez sur un serveur digne de ce nom, répondant aux caractéristiques évoquées précédemment (RAID, redondance, etc.).

Vous devrez faire toutes les mises à jour de Windows ce qui vous amènera à installer le Service Pack 1 (SP1) de Windows 2008 R2.

► Contenu

1. Introduction	20
2. Installation	20
3. Démarrage	22
4. Configuration réseau	25

1. Introduction

Installer un système d'exploitation dans une machine virtuelle est un vrai plaisir : aucun souci ! Les périphériques présentés au système d'exploitation par VirtualBox (ou tout autre outil de virtualisation) sont ultra-standards, donc connus et gérés par tous les OS. Mais dans la réalité, c'est généralement différent. En effet, votre serveur physique aura un certain nombre de composants « atypiques » ou plus récents que le système d'exploitation, et donc non supportés nativement. Par expérience, je pense particulièrement aux cartes contrôleur RAID que bien souvent notre Windows ne reconnaît pas. Sans reconnaissance du système RAID, pas de stockage et donc pas d'installation. Deux possibilités existent :

- télécharger le pilote sur le site Internet du constructeur sur une clé USB à présenter à Windows lors de l'installation ;
- démarrer l'installation par un CD du constructeur du serveur. C'est le cas par exemple chez DELL, où ce CD « prépare » le serveur à installer Windows ou Linux. Le DVD de Windows est introduit dans une deuxième phase.

Note : à partir de Windows 2008 R2 64 bits, tous les pilotes doivent être signés numériquement ! Donc, compatibilité du matériel à vérifier avant l'achat de la machine !

2. Installation

Atelier 2

Installation
de Windows 2008 R2

Page 20

Vous créez une machine VirtualBox adaptée, comme vu dans les précédents modules (rappel : mettre une connexion réseau en mode « pont »). Puis vous démarrez sur l'image ISO correspondante pour faire l'installation.

Le premier écran notablement intéressant est celui qui permet de choisir le type de système d'exploitation à installer :

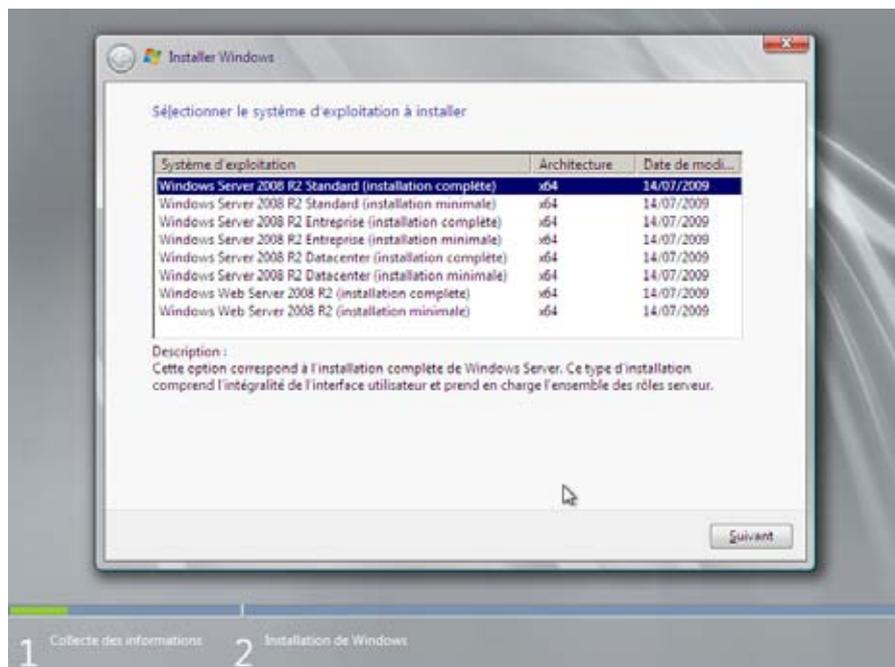


Figure 1 : choix du type d'OS

Dans un premier temps, on peut se demander la différence entre une installation « complète » et une installation « minimale ». On peut le résumer en regardant ceci (installation minimale de Windows 2008) :

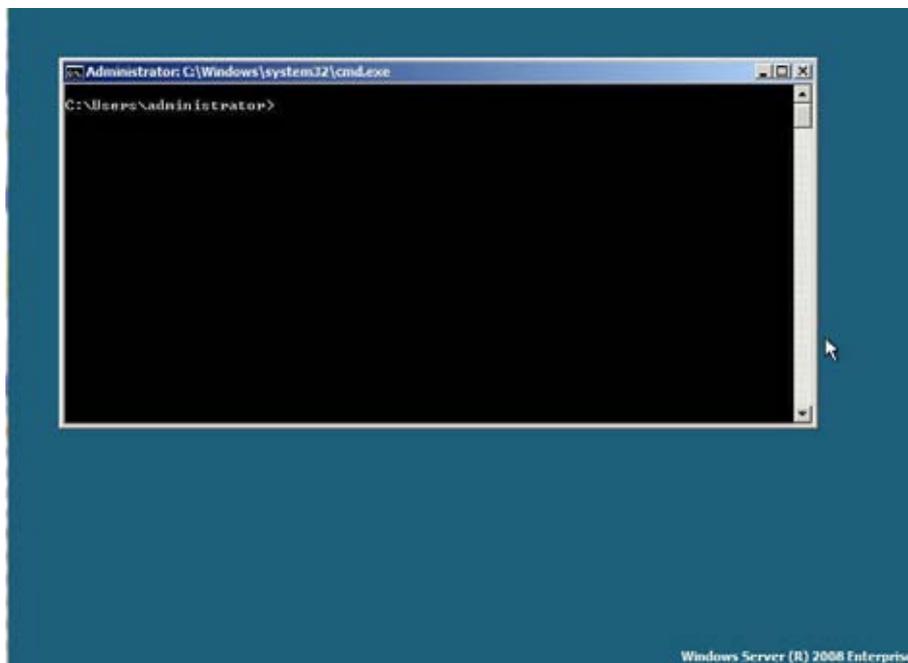


Figure 2 : Installation Windows en mode core

Ne cherchez pas les icônes ou les menus. Dans la version minimale ou « core » de Windows 2008, tout se gère en ligne de commandes.

Mais d'autres versions de Windows sont proposées (standard, datacenter, etc.) :

Exercice 1

Recherchez les caractéristiques matérielles et fonctionnalités des différentes versions (standard, entreprise, datacenter, web server). Quelle mémoire maximum pour une « standard » ? Combien de CPU pour une « Datacenter » ?

Pour les besoins des ateliers, une version « standard/complète » est suffisante. L'écran intéressant suivant, comme pour Windows 7, est celui du partitionnement. Comme indiqué en début d'atelier, le pilote de votre contrôleur RAID peut ne pas être connu de Windows et dans ce cas, aucun espace de stockage ne vous est proposé. Vous pourrez donc indiquer ici un pilote spécifique en cliquant sur « charger un pilote » :

Atelier 2

Installation
de Windows 2008 R2

Page 21

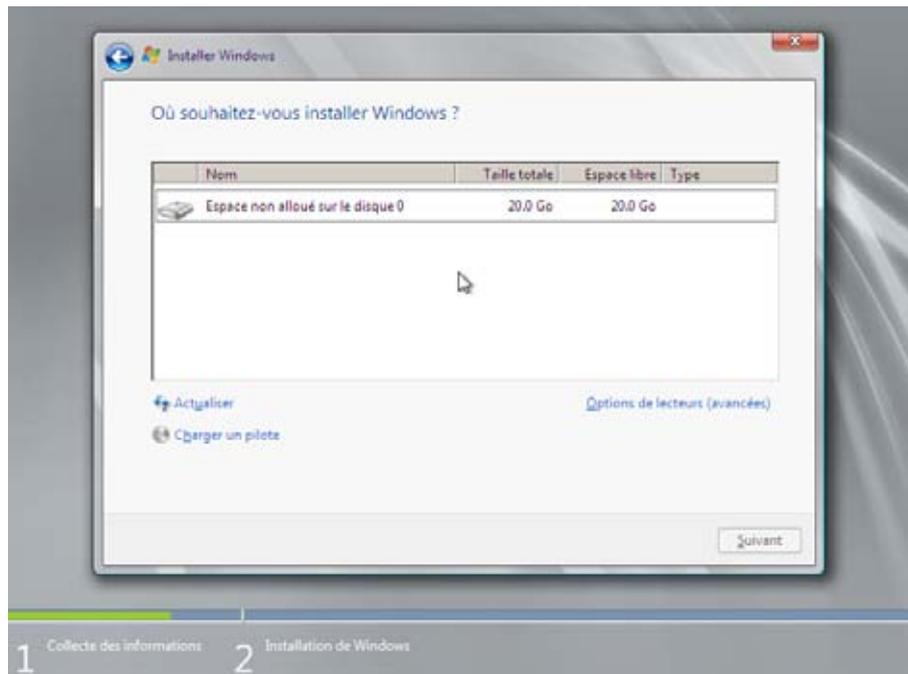


Figure 3 : partitionnement

Il est conseillé de créer au moins deux partitions et de laisser un espace non alloué qui permettra d'agrandir les partitions avec le logiciel nécessaire. À cause des nombreuses mises à jour et du mode de gestion des désinstallations de logiciels, il est conseillé de laisser un espace important sur la partition système : 50 Gio étant un strict minimum.

Atelier 2

Installation
de Windows 2008 R2

Page 22

3. Démarrage

Lors du premier démarrage de Windows 2008, vous devrez choisir un mot de passe pour l'administrateur. Celui-ci doit respecter des contraintes très précises : faire au moins 6 caractères et faire partie de 3 des 4 catégories suivantes : caractères minuscules, caractères majuscules, nombres, ponctuation.

Une fois dans le bureau Windows, il est conseillé d'installer les additions invités de VirtualBox.

Vous êtes invité à suivre l'assistant ci-dessous pour vérifier ou réaliser les configurations nécessaires :

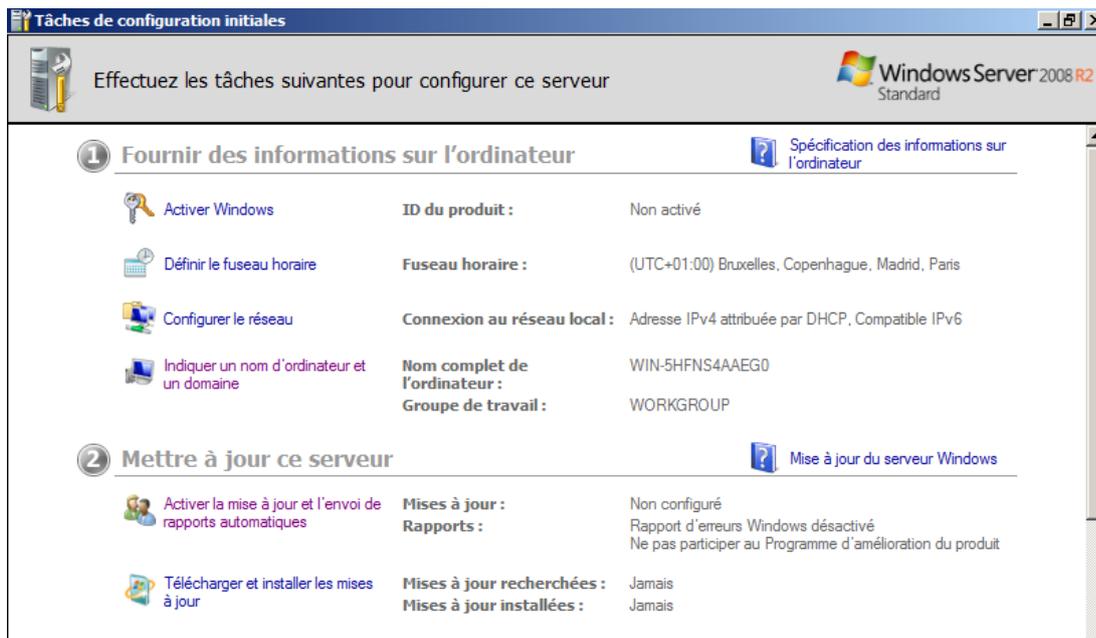


Figure 4 : assistant de configuration - partie 1

Cet écran se poursuit :

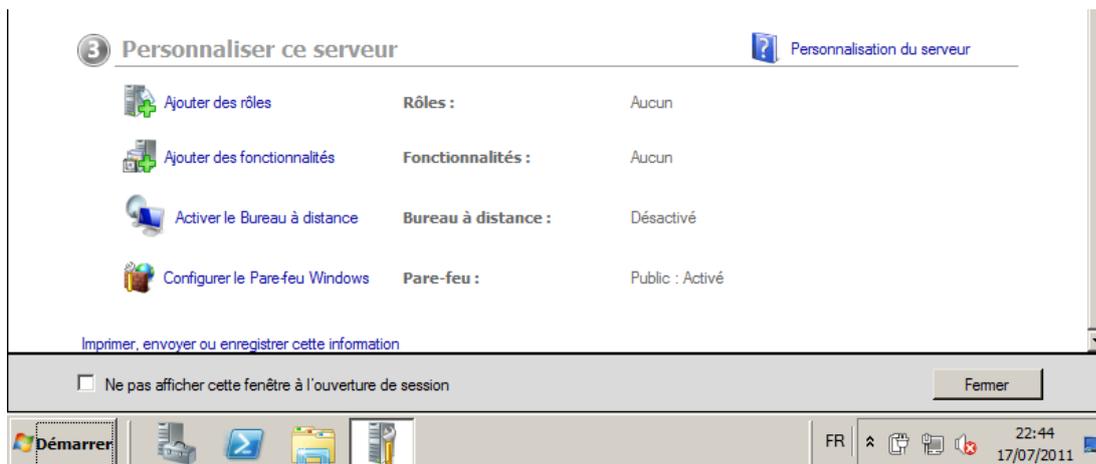


Figure 5 : assistant de configuration - partie 2

Lors de l'installation, Windows a généré un nom aléatoire mais nous allons définir un nom convenable pour notre serveur. En prévision des prochains ateliers, il est important de mettre un nom « compatible » avec Internet puisqu'il s'agit en réalité d'un nom NET-BIOS dont les règles sont différentes. En résumé, vous devez vous cantonner aux caractères alphanumériques non accentués et aux tirets, le tout sur 15 caractères au maximum commençant par une lettre :

Atelier 2

Installation
de Windows 2008 R2

Page 23

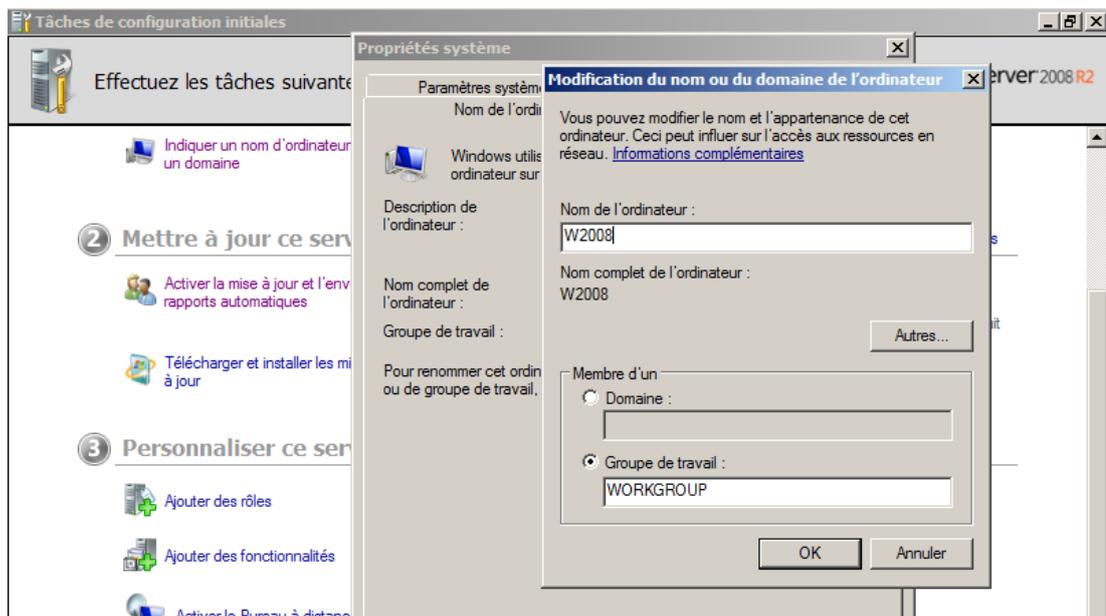


Figure 6 : Changement du nom

Il vous appartient également de vérifier l'horloge et surtout que celle-ci se met à jour automatiquement via un serveur de temps (NTP) et d'activer les mises à jour. Vous ferez aussi toutes les mises à jour avant d'aller plus loin. Ça vous rappelle de bons souvenirs n'est-ce pas :-)? Vous avez largement le temps de continuer l'étude du cours pendant ce temps-là ou d'aller vous coucher, selon l'heure...

Atelier 2

Installation
de Windows 2008 R2

Page 24

4. Configuration réseau

Nous affectons des paramètres réseau statiques pour notre serveur. Vous mettez un adressage cohérent avec votre installation :

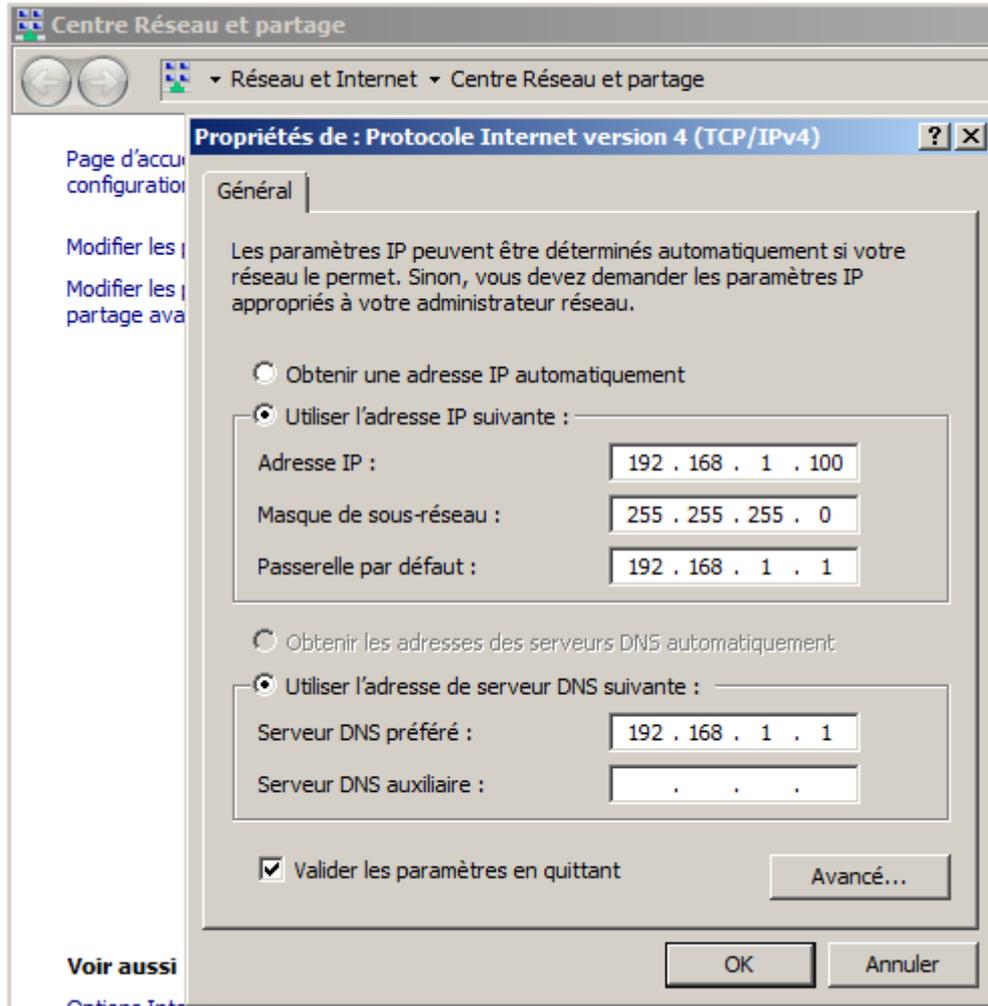


Figure 7 : Configuration IP du serveur

À retenir

Windows est proposé dans de nombreuses versions avec des capacités techniques et des fonctionnalités différentes et donc des prix différents. Chaque version peut être installée, au choix, en mode « complet » ou « minimal ». En mode « minimal », tout se fait en ligne de commandes DOS et Powershell.

Le seul écran critique de l'installation concerne la gestion du disque et le partitionnement. Créer au moins deux partitions avec une partition système suffisamment grande pour absorber les mises à jour, les installations et désinstallations de logiciels, la mémoire virtuelle, etc.

Le nom de la machine doit respecter certaines contraintes : 15 caractères alphanumériques sans les accents plus les tirets et commencer par une lettre.

Les mises à jour automatiques doivent être activées. L'horloge doit être synchronisée automatiquement via un serveur de temps.

Si vous voulez approfondir

Attendez les ateliers suivants !

Atelier 2

Installation
de Windows 2008 R2

Page 26

Atelier 3

Installation d'un domaine Windows 2008 R2

► **Durée approximative de cet atelier : 1 heure 30**

► **Objectif**

Installer les composants nécessaires et réaliser les configurations pour que notre serveur Windows 2008 R2 devienne contrôleur de domaine Windows.

► **Durée approximative de cet atelier**

Serveur Windows 2008 R2 SP1 fraîchement installé.

► **Considérations techniques**

Dans cet atelier et les suivants, nous cherchons à monter un réseau d'entreprise basé sur des règles de sécurité centralisées. C'est pourquoi nous installons un contrôleur de domaine Windows qui va jouer ce rôle.

► **Contenu**

1. Licences	28
2. Devenir « contrôleur de domaine »	28
3. Tour du propriétaire	35

1. Licences

Avant de commencer, parce que nous installons un serveur qui sera partagé par différents clients et parce que Windows n'est pas gratuit, faisons un détour par la notion de licence. Comme vous êtes en formation et dans le cadre du programme MSDNAA souscrit par le CNED, vous accédez gratuitement à un certain nombre de logiciels Microsoft dont la plupart sont payants.

Dans le monde de l'entreprise, vous devez vous acquitter de licences qui sont un droit d'utilisation du logiciel concédé par Microsoft. Dans l'univers de Windows, 3 niveaux de licences sont à posséder. Les deux premières sont évidentes, la troisième moins... :

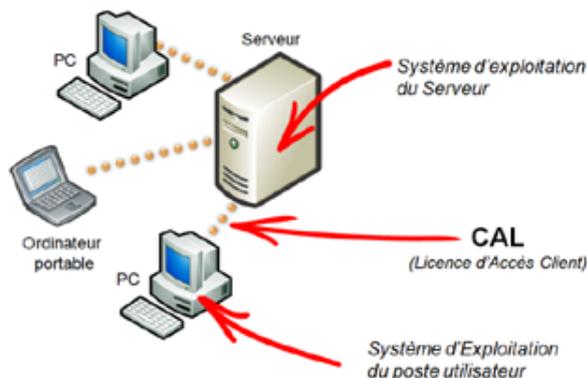


Figure 1 : licences OS (source : Microsoft)

Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 28

- les licences serveur
- les licences client
- les licences d'accès client (CAL), qui sont l'autorisation d'accès d'un client sur un serveur (il s'agit bien d'une relation de 1 à 1). Ce n'est pas un logiciel, juste un « papier ».

En résumé, la règle à connaître est que le fait de posséder un système d'exploitation Microsoft sur une station ne vous donne pas un droit d'accéder aux serveurs.

Sachant que là-dessus, viennent s'ajouter d'autres logiciels (bureautique, SGBD, etc.) qui ont eux aussi leur mode de licence, il est préférable de se rapprocher d'un revendeur de logiciel afin d'étudier avec lui le programme d'acquisition et de gestion des licences adapté à votre entreprise.

2. Devenir « contrôleur de domaine »

La gestion d'un serveur Windows est basée sur la notion de rôle et être un « contrôleur de domaine » est un rôle parmi d'autres. Un serveur Windows peut assumer plusieurs rôles.

Exercice 1

Vous recherchez dans l'aide en ligne Windows la définition du mot rôle.

Au départ, notre machine, bien que disposant d'un système d'exploitation serveur n'a aucun rôle particulier. Au fond, ce n'est qu'une machine lambda qui peut fonctionner en « poste à poste » avec les autres machines du réseau. Ceci est le mode « groupe de travail » (workgroup).

Nous allons « promouvoir » notre serveur en lui donnant ce rôle de « contrôleur de domaine », ce qui constitue la première brique d'un réseau local d'entreprise. La base de données des utilisateurs et d'autres paramètres de sécurité seront centralisés dans cette machine, contrairement au réseau basé sur les groupes de travail :

Groupe de travail



Domaine



Figure 2 : Groupe de travail / Domaine

Note importante : la notion de domaine au sens Microsoft est différente de celle de domaine au sens Internet (DNS). Néanmoins, des recoupements existent comme nous le verrons par la suite.

2A. Ajouter un rôle

Vous pouvez ajouter des rôles dans le « gestionnaire de serveur » :

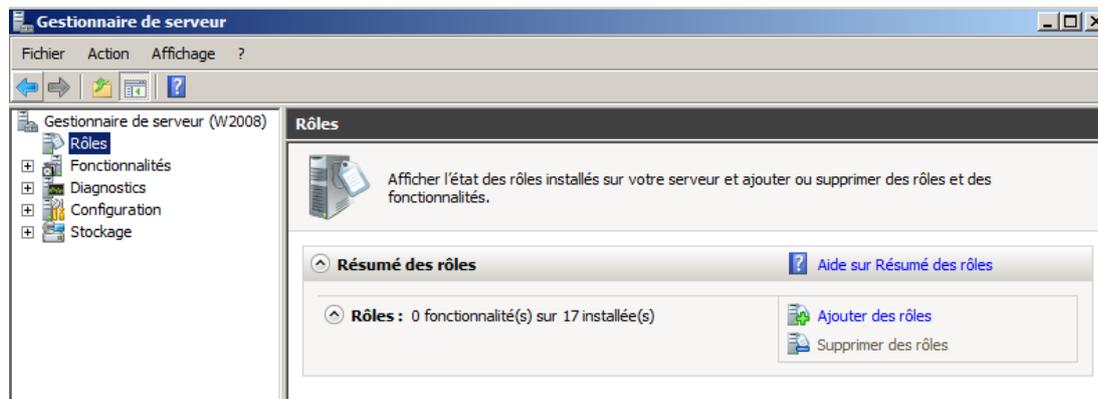
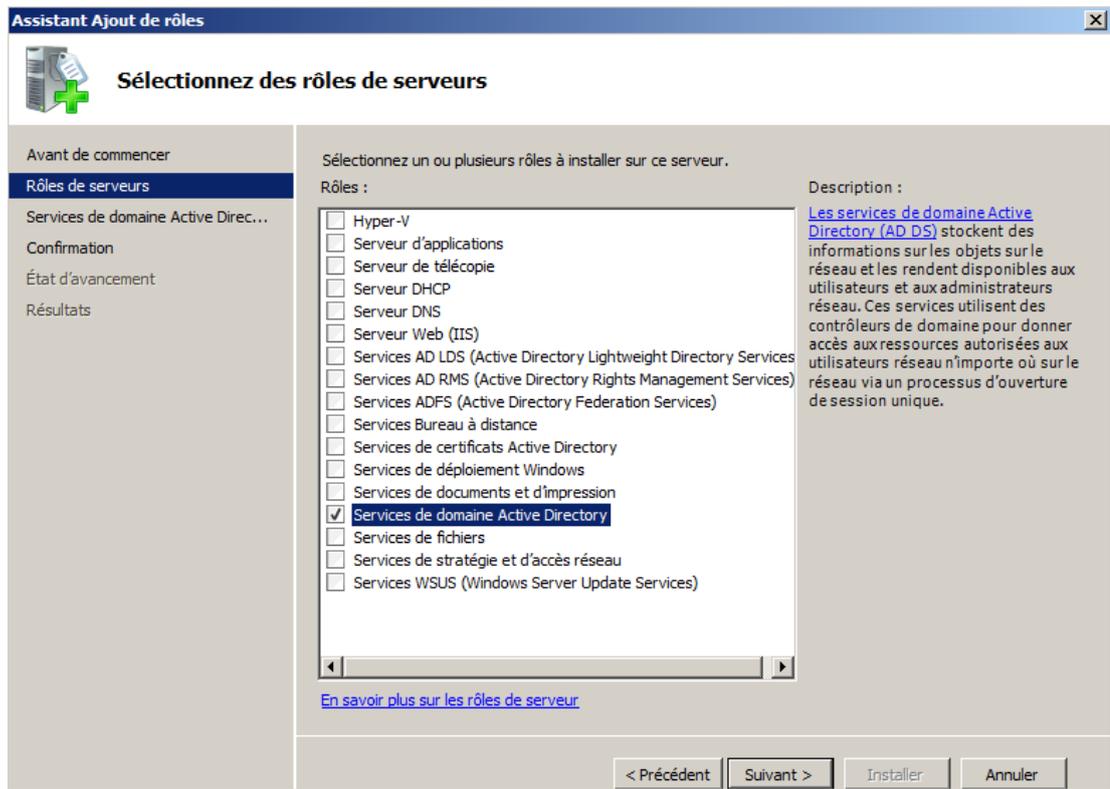


Figure 3 : Le gestionnaire de serveur

En cliquant sur « ajouter des rôles », vous pouvez observer les différents rôles (17) que peut assurer un serveur Windows 2008 :



Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 30

Figure 4 : Installation de rôles

Nous choisissons le rôle « Services de domaine Active Directory ». Ce qui entraînera l'installation du framework.NET 3.5.1.

Exercice 2

Qu'est-ce que « Active Directory » ? Quelle technologie Internet cela utilise-t-il ? qu'est-ce que le « framework.NET » ? Quel est son rôle ?

L'assistant d'installation est lancé lorsque l'on clique sur « suivant ». Lisez attentivement ce qui est indiqué sur l'écran suivant :

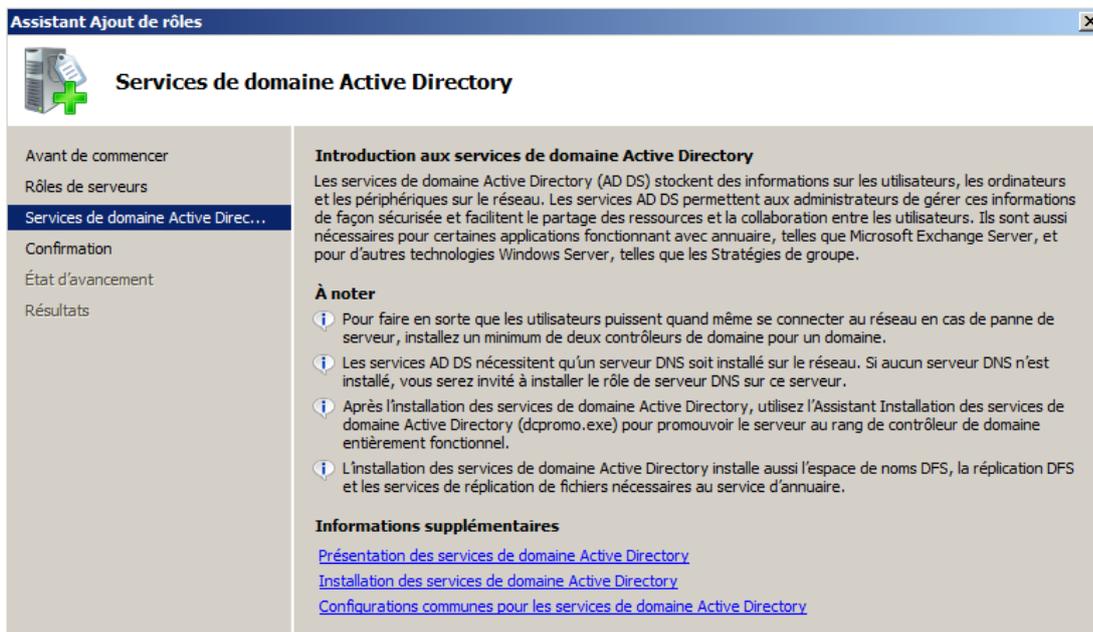


Figure 5 : Avertissements concernant AD

Les deux informations essentielles sont :

- il est conseillé d'installer deux contrôleurs de domaines afin de gérer la panne de l'un d'eux. En effet, si un contrôleur tombe en panne, les utilisateurs auront des difficultés à utiliser le réseau, se connecter à leur poste de travail, etc. Lorsque deux contrôleurs du même domaine sont installés, ceux-ci se synchronisent automatiquement de façon transparente.
- installation impérative d'un serveur DNS pour le domaine : le serveur DNS sera lié à Active Directory. En particulier, les postes clients utiliseront le serveur DNS pour retrouver le contrôleur de domaine qui leur est associé.

Lorsque Windows a installé tous les fichiers, nous revenons au gestionnaire de serveur. Nous constatons que la partie « Services de domaine Active Directory » est en erreur car le paramétrage n'a pas encore été fait :

Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 31

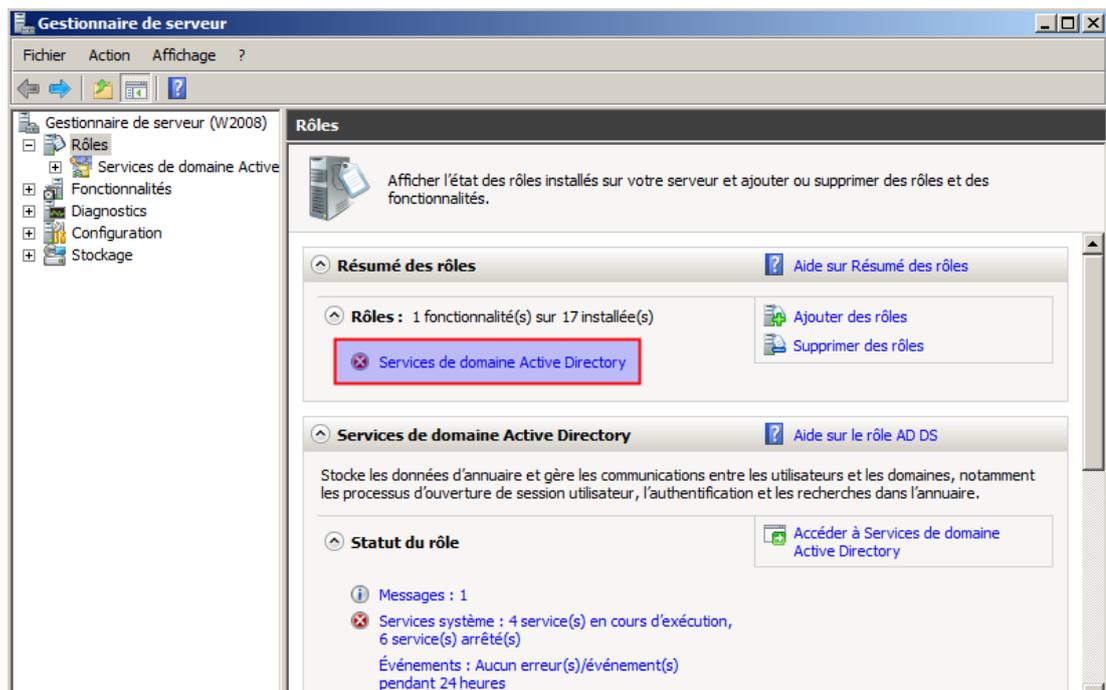


Figure 6 : AD installé mais paramétrage non réalisé

Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 32

Si on clique sur la croix, on rentre dans la gestion du domaine. Nous allons pouvoir faire la promotion du serveur (équivalent de la commande DOS `dcpromo.exe`) :

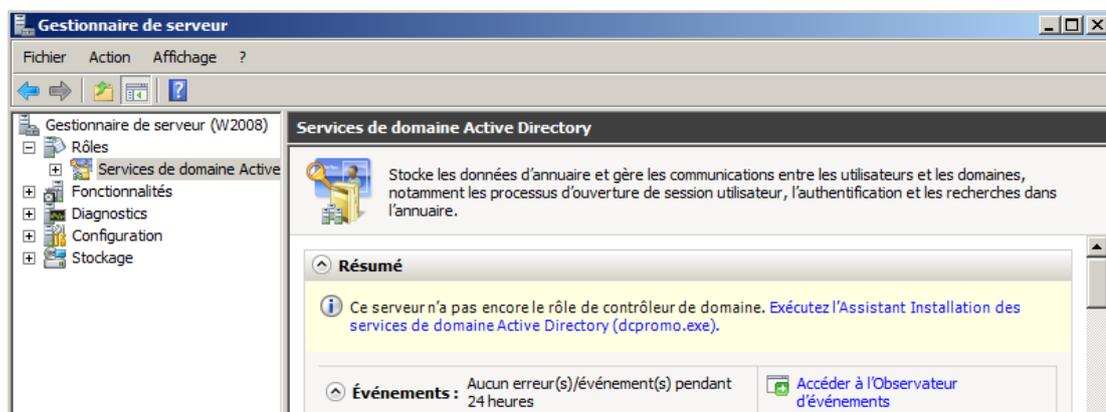


Figure 7 : Invitation à lancer l'assistant

2B. Assistant de configuration de AD

Nous ne présentons ici que les écran importants. Il est inutile d'exécuter l'assistant en mode avancé (vous pouvez néanmoins consulter l'aide sur ce sujet).

Principales étapes :

- Avertissement sur la compatibilité des algorithmes de chiffrement : peut avoir des conséquences si vous voulez intégrer au domaine des clients SAMBA ou des NAS basés sur Linux ou BSD.
- Vu que nous installons notre premier serveur, il faut « créer un domaine dans une nouvelle forêt ». Nous ne développerons pas ici, le concept de forêt au sens AD, sachez seulement qu'il s'agit d'un ensemble de domaines Windows qui se font confiance mutuellement. Ceci s'applique aux très grandes entreprises .

- Nom du domaine : important, si l'entreprise possède un nom de domaine Internet, ne pas l'utiliser ici, sinon conflit avec la résolution DNS (supposons que nous soyons présent sur Internet avec le domaine labocned.fr, nous utiliserons (par exemple) labocned.local pour le domaine Windows) :

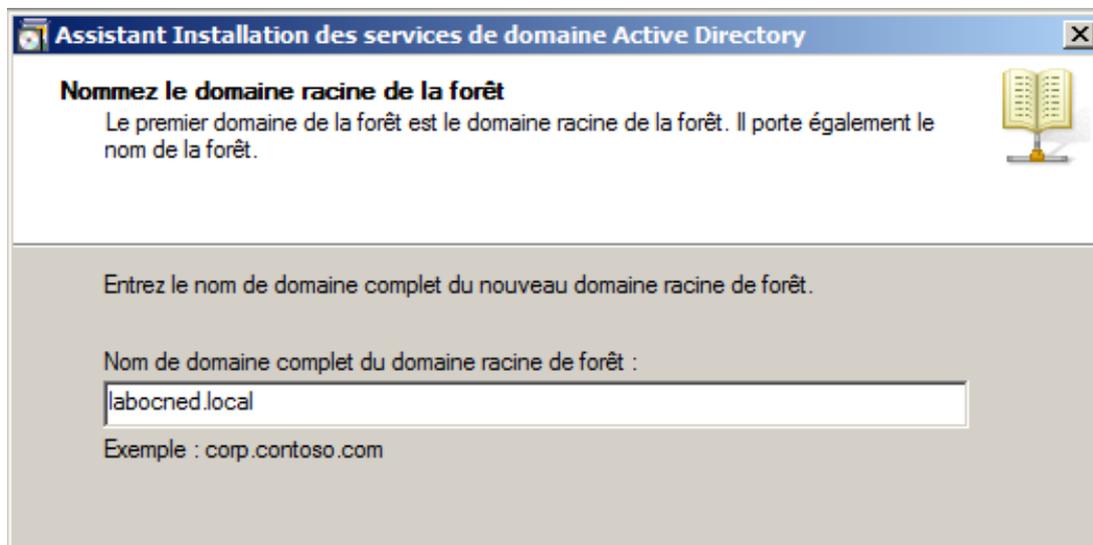


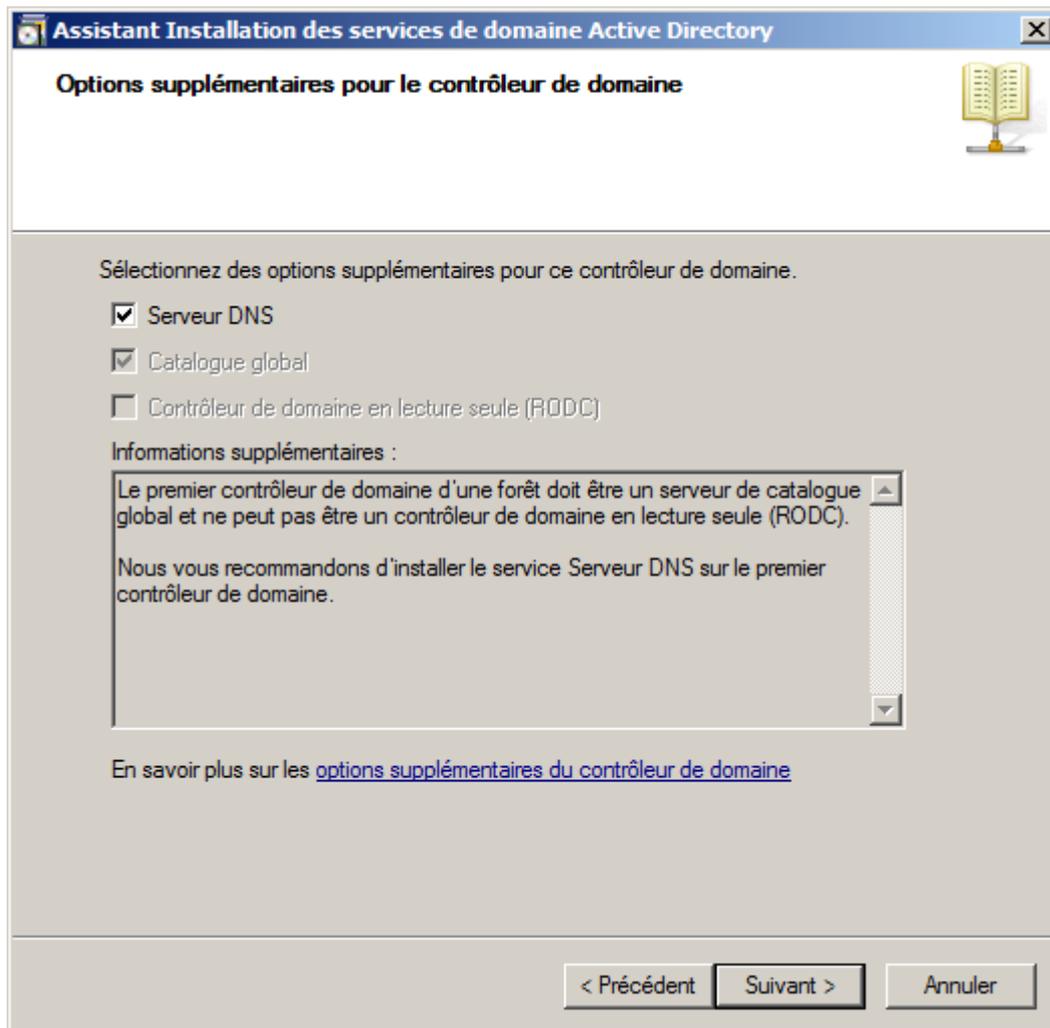
Figure 8 : Nom du domaine Windows

- Windows vérifie que le nom indiqué n'est pas déjà utilisé sur le réseau local...
- Niveau fonctionnel : chaque version de Windows apporte ses améliorations. La compatibilité est descendante (Windows 2008 est compatible avec le niveau fonctionnel Windows 2000 mais Windows 2003 n'est pas compatible avec le niveau fonctionnel Windows 2008 R2). Le choix dépend donc de l'existant sur le réseau : ici, on choisit 2008 R2 puisque le serveur est seul.
- Serveur DNS : on laisse coché, le rôle « serveur DNS » est indispensable et sera donc installé. Nous y reviendrons après :

Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 33



Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 34

Figure 9 : Installation du serveur DNS

- Ignorer l'avertissement sur la création d'une délégation DNS : ne concerne que les sous-domaines
- Chemins pour les fichiers Active Directory : éventuellement stocker sur des disques différents la base de données et les fichiers journaux
- Mot de passe pour la restauration de l'annuaire : forcément différent de celui de l'administrateur puisque les données de l'administrateur sont dans l'annuaire
- ouf :

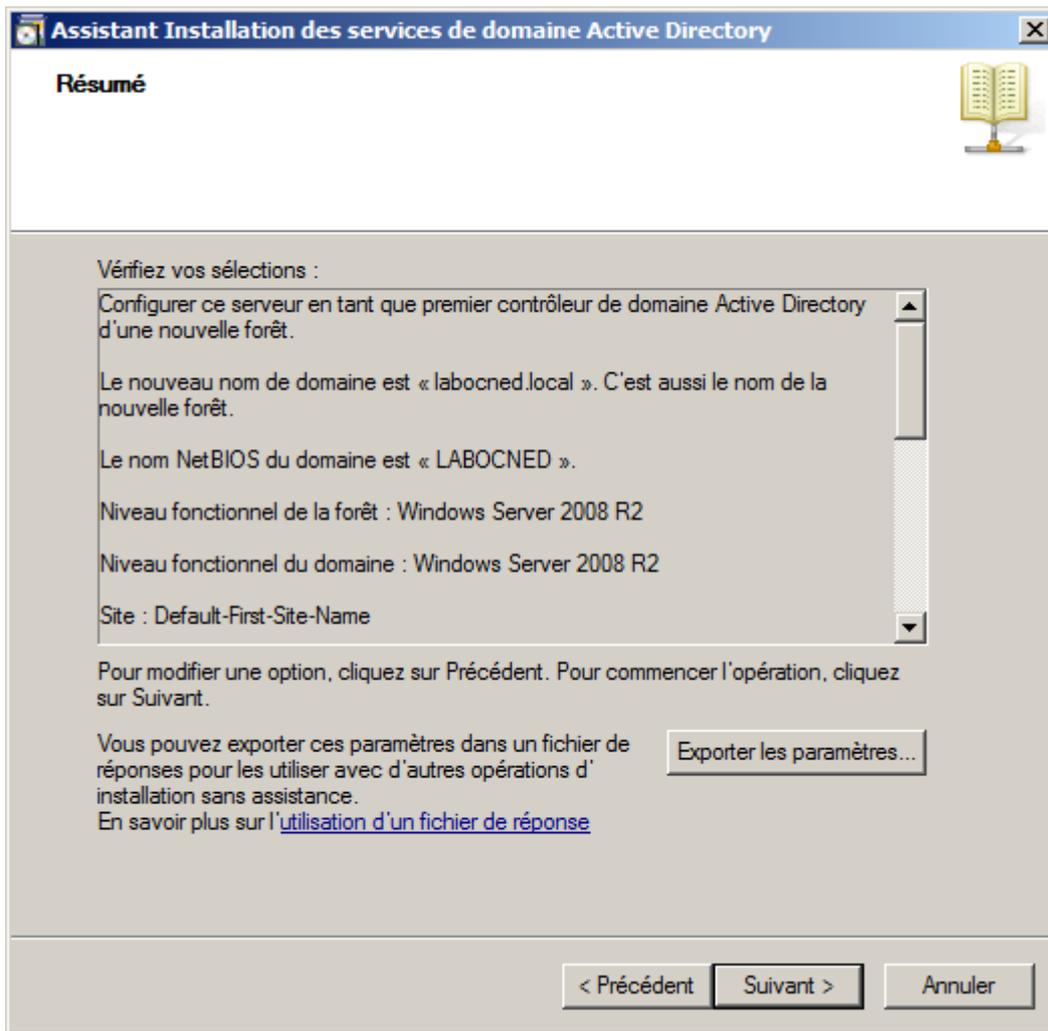


Figure 10 : Résumé avant installation

Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 35

Redémarrage nécessaire !

3. Tour du propriétaire

Nous avons maintenant un contrôleur de domaine tout beau tout propre, prêt à accueillir utilisateurs et ordinateurs. Observons les nouveaux outils à notre disposition :

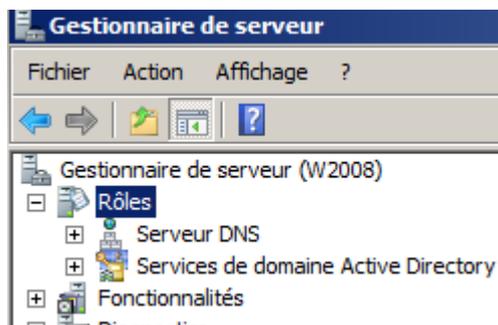


Figure 11 : Rôles

Deux nouveaux éléments sont apparus dans la partie « rôles » du « gestionnaire de serveur » :

- serveur DNS
- services de domaine Active Directory

Examinons les successivement.

3A. DNS

Dans la partie DNS, nous pouvons observer ceci :

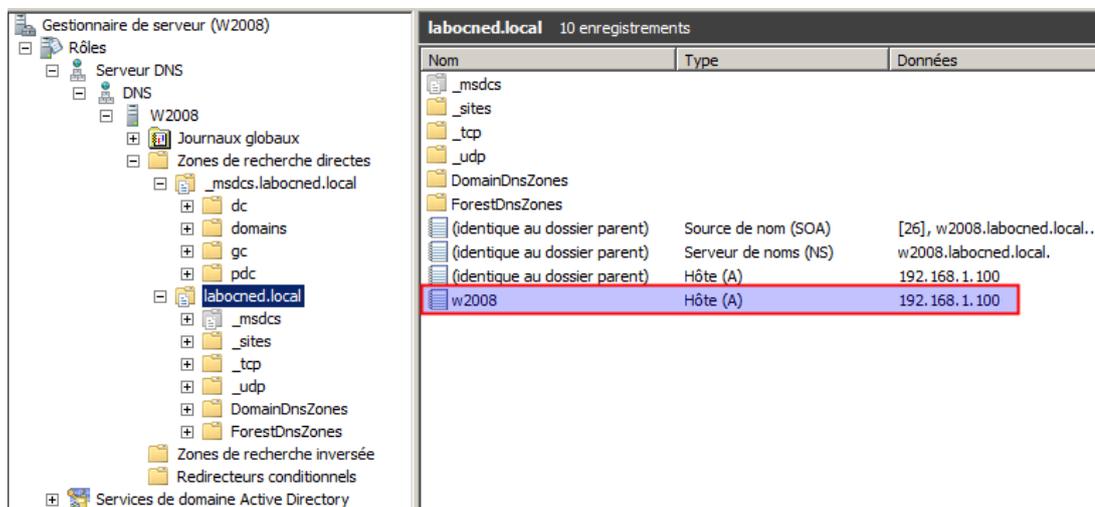


Figure 12 : DNS

Une zone labocned.local a été créée pour contenir les enregistrements correspondants aux machines du réseau (on voit ici l'IP et le nom de notre serveur). D'autres enregistrements spécifiques à AD ont aussi été créés (_msdcs, _sites, _tcp, _udp, etc.) : ceux-ci sont utilisés par les clients AD pour localiser les contrôleurs de domaines et autres services proposés. Leur étude dépasse le cadre de ce module mais **surtout, on n'y touche pas !**

Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 36

Exercice 3

Mais au fait, est-ce que mon serveur Windows utilise lui-même ce serveur DNS ? Pouvez-vous répondre à cette question ?

Exercice 4

Mais alors, est-ce que j'ai toujours accès à Internet ?

Comment est-ce possible ? Nous avons vu que Windows a modifié la configuration IP de la machine lors de l'installation de Active Directory. En fait, il a récupéré le serveur DNS qui était configuré avant pour l'intégrer dans le serveur DNS en tant que redirecteur. Allez dans les propriétés du serveur DNS :

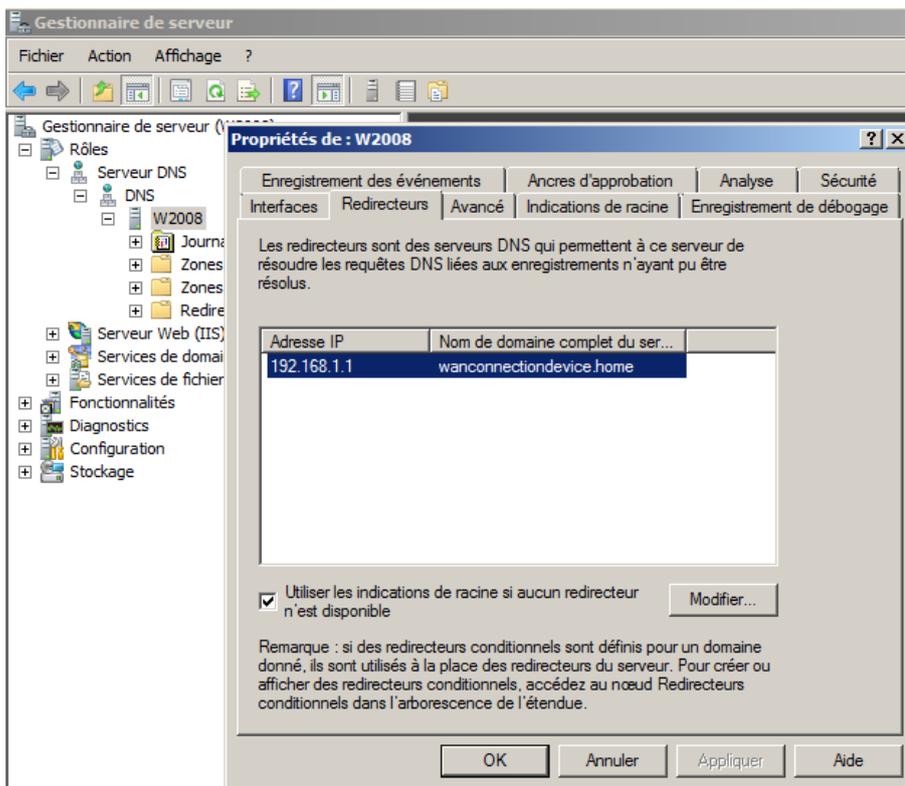


Figure 13 : Propriétés du serveur DNS

En clair, le serveur DNS de Windows reçoit toutes les requêtes. Quand il ne sait pas y répondre, il transmet, récupère la réponse et la renvoie au client. Au passage, il la met dans son cache.

Notez également qu'il connaît l'adresse des 13 serveurs DNS racine (bouton « modifier ») il peut donc résoudre les adresses Internet si aucun redirecteur n'est défini.

3B. Services AD

Cette section présente un écran très complet divisé en 3 grandes catégories :



Figure 14 : AD

- résumé : indique les éventuels message d'erreurs, les services Windows actifs, des conseils pour la gestion et la possibilité d'ajouter des services de rôle.
- outils avancés : toute la panoplie des outils Windows disponibles pour la gestion de votre contrôleur de domaine et de AD.
- ressources et support : recommandations, documentations, etc.

Si l'on développe l'arborescence, on peut consulter le contenu de notre Active Directory dont le but premier est de gérer les « objets » de notre réseau : ordinateurs et utilisateurs.

Users 18 objets [Filtre activé]		
Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'adm...
Administrateurs de l'entre...	Groupe de sécu...	Administrateurs désignés ...
Administrateurs du schéma	Groupe de sécu...	Administrateurs désignés ...
Admins du domaine	Groupe de sécu...	Administrateurs désignés ...
Contrôleurs de domaine	Groupe de sécu...	Tous les contrôleurs de do...
Contrôleurs de domaine d'...	Groupe de sécu...	Les membres de ce group...
Contrôleurs de domaine e...	Groupe de sécu...	Les membres de ce group...
DnsAdmins	Groupe de sécu...	Groupe des administrateu...
DnsUpdateProxy	Groupe de sécu...	Les clients DNS qui sont a...
Éditeurs de certificats	Groupe de sécu...	Les membres de ce group...
Groupe de réplication don...	Groupe de sécu...	Les mots de passe des me...
Invité	Utilisateur	Compte d'utilisateur invité
Invités du domaine	Groupe de sécu...	Tous les invités du domaine
Ordinateurs du domaine	Groupe de sécu...	Toutes les stations de tra...
Propriétaires créateurs de...	Groupe de sécu...	Les membres de ce group...
Serveurs RAS et IAS	Groupe de sécu...	Les serveurs de ce group...
Utilisateurs du domaine	Groupe de sécu...	Tous les utilisateurs du do...

Figure 15 : Contenu de AD

Nous allons développer ces éléments dans l'atelier suivant.

À retenir

Atelier 3

Installation
d'un domaine
Windows 2008 R2

Page 38

Un serveur doit être promu au rôle de contrôleur de domaine. Ceci a pour effet d'installer les services Active Directory ainsi que le serveur DNS. Le serveur DNS permet aux clients de retrouver le contrôleur de domaine sur le réseau.

Si vous voulez approfondir

Installer un deuxième contrôleur de domaine afin d'activer la redondance Active Directory.

Comparer les fonctionnalités entre Active Directory et l'implémentation libre des services de contrôleur de domaine Samba (samba.org)

Atelier 4

Gestion des utilisateurs du domaine

► **Durée approximative de cet atelier : 2 heures**

► **Objectif**

Comprendre et mettre en oeuvre la gestion des utilisateurs avec Active Directory.

► **Durée approximative de cet atelier**

Serveur Windows 2008 R2 SP1 fraîchement installé.

► **Considérations techniques**

Nous mettons en oeuvre l'Active Directory qui est au coeur de la gestion de domaine Windows. Sans le savoir, vous allez manipuler un annuaire LDAP.

► **Contenu**

1. Introduction	40
2. Création des unités d'organisation (UO)	41
3. Création des groupes	43
4. Création des utilisateurs	48
5. Gestion des droits d'accès.....	50

Atelier 4

Gestion des utilisateurs du domaine

Page 39

1. Introduction

Souvenez-vous des TP sur Windows 7 professionnel. Ce système d'exploitation est multi-utilisateur, il intègre donc une gestion des utilisateurs et des droits associés. Lorsqu'un utilisateur tente d'ouvrir une session, Windows 7 vérifie dans sa base locale son mot de passe et lui affecte un certain nombre de droits. Pour un Windows 2008 server « de base », c'est bien évident la même chose.

Mais une fonctionnalité proposée sur les versions serveurs et indisponible sur les versions « professionnelles » est de pouvoir assumer le rôle de contrôleur de domaine. Cela change tout, car Windows va gérer dans son Active Directory (AD) une base d'utilisateurs et de groupes partagés avec les autres machines du domaine. Lorsqu'un utilisateur tente d'ouvrir une session sur son poste de travail, si la machine est membre d'un domaine, la vérification des droits d'accès et l'attribution des droits se fait sur le contrôleur de domaine (et non plus localement). Nous verrons dans l'atelier suivant, qu'une machine doit être intégrée au domaine pour cela.

Le point central de notre travail dans ce TP consacré à la gestion des utilisateurs est la « console de gestion des groupes et utilisateurs » qui est accessible dans le gestionnaire de serveur :

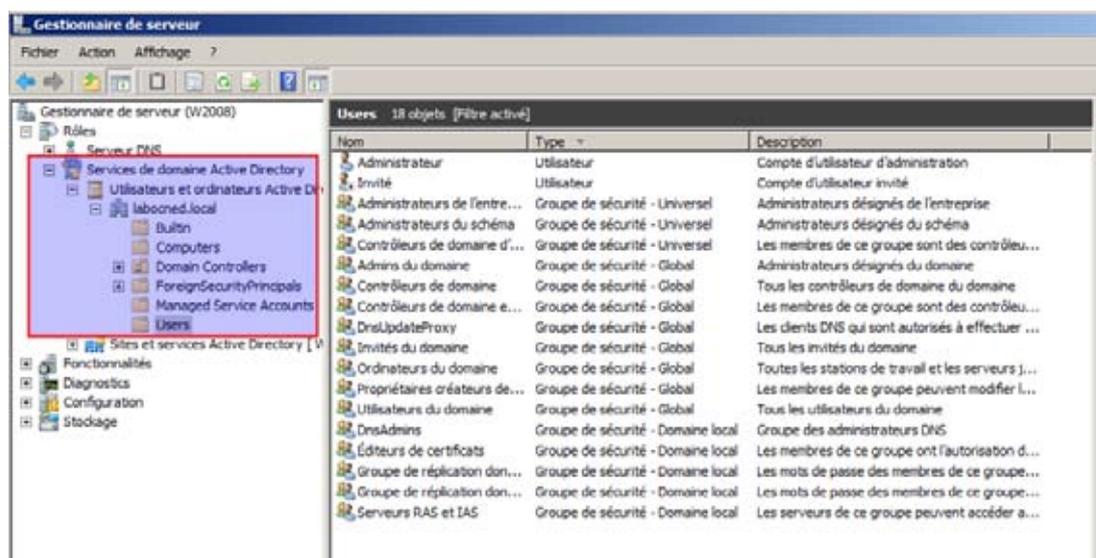


Figure 1 : Console de gestion des utilisateurs AD

En ouvrant l'item « Services de domaine Active Directory », nous retrouvons notre domaine labocned.local. C'est une vue de l'Active Directory constituée d'un certain nombre de sous-dossiers qui contiennent les objets stockés dans l'annuaire. En examinant la figure précédente, nous voyons que l'annuaire contient des éléments créés par défaut lors de la promotion de notre serveur au rang de contrôleur de domaine :

- des utilisateurs : les habituels administrateur et invité
- des groupes : ce sont des ensembles d'utilisateurs avec, dans le jargon Microsoftesque, des portées différentes. Nous développerons plus loin les notions de « Groupe de sécurité – global » et de « Groupe de sécurité – Domaine local ». Par contre, nous n'évoquerons pas les groupes « universels » qui concernent les « forêts » Active Directory.

Il faut bien voir que Windows Server est prévu pour gérer des multinationales avec de nombreux domaines reliés les uns aux autres (notion de « forêt » vue lors de l'installation). Dans ce module, nous nous cantonnons à un domaine unique, c'est pourquoi nous ne développerons pas la multitude des possibilités offertes par Active Directory. Disons que pour l'instant nous nous situons dans un contexte de PME avec un domaine unique. Néanmoins, vous devez savoir qu'un annuaire Active Directory peut contenir des objets de natures très différentes :



Figure 2 : Objets AD

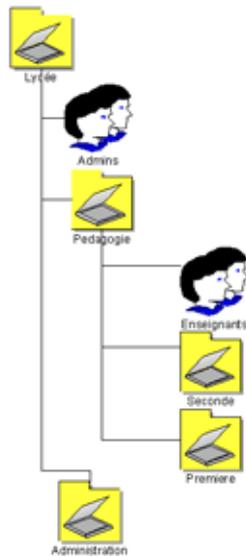
Pour ce qui nous intéresse, nous trouvons des groupes, des utilisateurs, des ordinateurs, des imprimantes, des dossiers partagés, des serveurs et des unités d'organisation (UO) qui vont nous permettre d'organiser notre annuaire.

Vous allez voir que la création des utilisateurs intervient en dernier, une fois que l'organisation de l'entreprise a été décrite et que les groupes de sécurité ont été déclarés.

2. Création des unités d'organisation (UO)

Les UO sont des conteneurs Active Directory dans lesquels vous pouvez placer des utilisateurs, des groupes, des ordinateurs et d'autres unités d'organisation. Vous pouvez créer des unités d'organisation de façon à refléter la structure hiérarchique, fonctionnelle ou commerciale de l'entreprise concernée. Vous pourrez aussi facilement déléguer une partie de l'administration (imaginons par exemple, un seul domaine Windows mais réparti sur plusieurs sites géographiques).

Examinons cet exemple issu du domaine scolaire :



C'est un extrait de l'organisation d'un lycée :

- les admins qui supervisent sont à part
- deux UO principales : pédagogie et administration
- dans la pédagogie, nous trouvons le groupe des enseignants et en dessous des UO correspondant aux niveaux.

On imagine bien qu'en dessous nous pourrions trouver la seconde 1, la seconde 2, etc. Dans l'UO correspondant à la seconde 1, nous trouverions le groupe des élèves de cette classe, le serveur et l'imprimante qu'ils utilisent habituellement par exemple.

La gestion à base d'UO nous permettrait de déléguer l'administration de chaque classe à un professeur principal par exemple.

Figure 3 : Organisation en UO

Nous allons maintenant mettre en application. En cliquant droit sur le niveau concerné de l'arborescence, vous avez un menu « nouveau » qui vous propose de créer une nouvelle UO. Le seul élément à saisir sera son nom :

Atelier 4

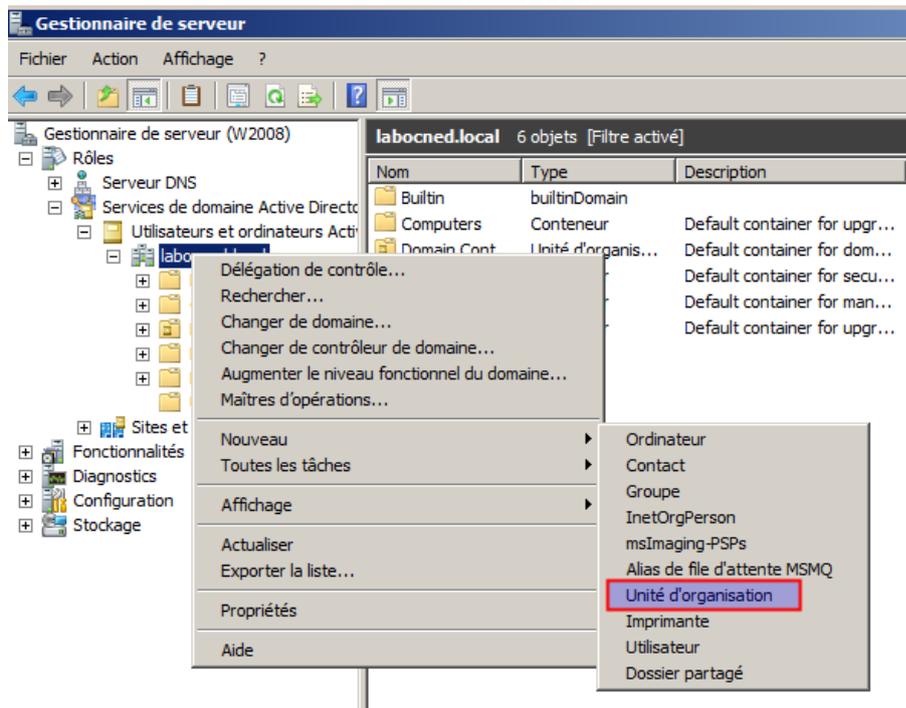
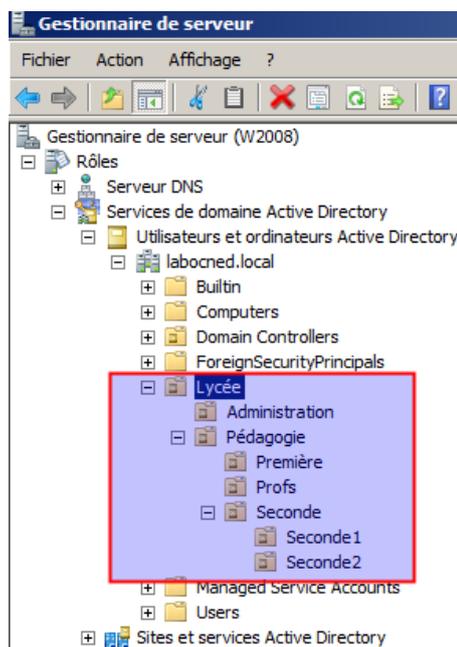


Figure 4 : Création d'une UO

Votre objectif est de créer la structure suivante :



Vous remarquerez au passage que les OU sont protégées contre la suppression accidentelle. En effet, une OU est pratique pour l'organisation mais aussi dangereuse, car comme pour un dossier dans le système de fichiers, **la suppression d'une OU entraîne la suppression de tous les objets contenus !**

Lorsque ce travail est réalisé, nous passons maintenant à la gestion des groupes d'utilisateurs.

Atelier 4

Gestion des utilisateurs du domaine

Page 43

3. Création des groupes

Bon, avec Windows nous avons deux gros morceaux à ingérer : les groupes et les droits d'accès. Comme je l'ai déjà dit, l'Active Directory a été conçue pour gérer de très grandes entreprises, d'où une complexité inévitable. Dans des cas simples comme le notre, on a souvent l'impression de devoir faire des manipulations compliquées pour obtenir un résultat en apparence élémentaire. Heu... ce n'est pas qu'une impression...

Pour vous consoler, disons qu'une fois que c'est maîtrisé, vous avez à disposition une grande puissance. Et puis qui sait, peut-être aurez vous à gérer une forêt Active Directory dans votre carrière !

3A. Typologie des groupes Windows

Dans un premier temps, observons les groupes fournis par Windows lors de l'installation de Active Directory. Ouvrez les conteneurs « Builtin » et « Users ». Regardez bien la colonne « type », ces différents groupes ont un point commun : ce sont tous des **groupes de sécurité** (nous ne présenterons pas ici l'autre type moins important qui est « distribution »). Ce qui signifie que ces groupes et ceux que nous allons créer vont jouer un rôle dans la définition des droits d'accès aux objets du système. Nous reviendrons un peu plus loin sur l'importance de définir des groupes.

Par contre, ces groupes ont des différences : leur « étendue ». Windows distingue 3 étendues :

Groupes globaux	Ces groupes peuvent être utilisés pour accorder un accès à des ressources dans n'importe quel domaine de la forêt et servent généralement à regrouper des utilisateurs ayant des besoins similaires en termes d'accès aux ressources.
Groupes locaux de domaine	Ces groupes ne peuvent être utilisés que pour un accès à des ressources du domaine local.
Groupes universels	Cette étendue concerne essentiellement les forêts, sujet que nous ne développons pas ici.

Important : ne pas confondre « groupes locaux de domaine » et « groupes locaux ». En effet, pour rajouter à cette complexité, il faut savoir que les stations Windows, même intégrées à un domaine (comme nous le ferons dans le prochain atelier), conservent leur gestion de groupes et d'utilisateurs locaux (comme nous l'avons fait dans le TP Windows 7 du premier module) indépendamment du domaine. Lors d'une ouverture de session, on peut choisir sur le domaine ou en local.

Active Directory propose de nombreuses possibilités de gestion des utilisateurs et de leurs droits, néanmoins il est plus que très vivement conseillé de suivre la démarche préconisée par nos amis de Microsoft (dans un contexte de domaine unique, sans forêt) : **AGDLP**, ce qui signifie : **A**ccount, **G**lobal group, **D**omain Local group, **P**ermission. En gros, même si c'est possible, vous ne mettez pas de droits d'accès directement sur les utilisateurs (on peut accepter une exception si l'utilisateur est vraiment unique). Vous suivez ce schéma :

Atelier 4

Gestion des utilisateurs du domaine

Page 44

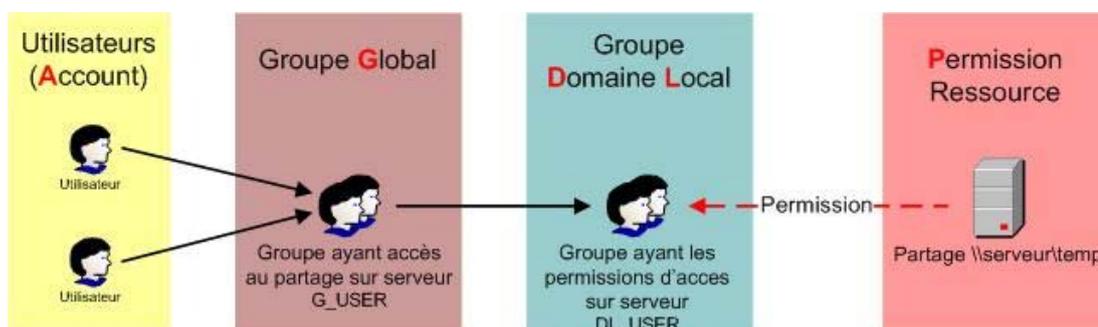


Figure 5 : AGDLP

Honnêtement, la distinction « groupe global » / « groupe domaine local » n'est pas très simple à saisir, d'autant plus que l'interface utilisateur Windows est très permissive et n'empêche donc pas de réaliser d'autres configurations.

Le principe est qu'un groupe global reflète l'organisation humaine de l'entreprise (bien souvent, un groupe global = un service). Le groupe local concerne les droits d'accès sur une ressource bien déterminée qui peuvent être communs à plusieurs groupes globaux.

Prenons un exemple simple mais typique. Nous avons deux groupes globaux correspondant à deux services d'une entreprise :

- g_compta
- g_commercial

Chacun comporte les personnels du service indiqué. Il se trouve que ces deux services sont dans le même couloir et que donc ils partagent une même imprimante. Dans ce cas, on crée un groupe local de domaine : DL Impr_Etg1 dans lequel on place les deux groupes globaux et auquel on donne le droit d'imprimer.

3B. Les groupes prédéfinis

Les groupes présents après l'installation de Active Directory sont appelés « groupes prédéfinis ». Certains peuvent être gérés par l'administrateur, présentons les plus fréquents :

Opérateurs de compte	Les membres de ce groupe peuvent administrer les comptes d'utilisateurs et les groupes (ajouter, supprimer et modifier). Ils ne peuvent cependant pas toucher au compte Administrateur ni aux autres membres du groupe Opérateurs de compte.
Opérateurs de serveur	Les membres de ce groupe peuvent partager des ressources ainsi qu'effectuer des sauvegardes et des restaurations sur des contrôleurs de domaine.
Opérateurs d'impression	Les membres de ce groupe peuvent gérer les imprimantes réseau des contrôleurs de domaine.
Opérateurs de sauvegarde	Les membres de ce groupe peuvent effectuer des sauvegardes et restaurations sur tout contrôleur de domaine.
Administrateurs	Les membres de ce groupe peuvent administrer les contrôleurs de domaine ainsi que toute station ayant intégré le domaine. Par défaut, le groupe global Administrateurs de domaine ainsi que le compte Administrateur font partie du groupe local Administrateurs.
Invité	Le groupe global Invités du domaine ainsi que le compte d'utilisateur Invité sont intégrés dans ce groupe. Les membres de ce dernier disposent de peu de droits.
Utilisateurs	Le groupe global du domaine utilisateur est intégré dans ce groupe. Ce groupe peut être utilisé pour affecter des droits et permissions à toute personne disposant d'un compte dans le domaine.

Par imbrication de groupe, l'appartenance à des groupes avec une étendue globale offre aussi des droits particuliers dans le domaine.

Invités du domaine	Le compte d'utilisateur Invité est automatiquement intégré à ce groupe. De plus, ce groupe global est lui aussi automatiquement intégré dans le groupe local du domaine Invités.
Utilisateurs du domaine	Tous les comptes d'utilisateurs que vous créez font partie de ce groupe. Ils ne peuvent effectuer que des tâches que vous avez spécifiées et n'ont accès qu'aux ressources auxquelles vous avez attribué des permissions. Ce compte est automatiquement intégré au groupe local du domaine Utilisateurs. Tout utilisateur créé dans le domaine est automatiquement inséré dans ce groupe.
Administrateurs du domaine	Le compte administrateur fait partie de ce groupe, qui est intégré au groupe local du domaine Administrateurs. En fait, le compte d'utilisateur Administrateur ne possède pas de droit particulier en tant que compte. C'est le fait de l'intégrer dans ce groupe global qui lui-même fait partie du groupe local du domaine Administrateurs qui lui donne ses droits.
Contrôleurs de domaine	Ce groupe contient les comptes d'ordinateur contrôleurs de domaine du domaine. En effet, vous constaterez dans l'atelier suivant que les ordinateurs intégrés au domaine (contrôleurs ou non) possèdent un compte qui ressemble à celui d'un utilisateur.

3C. Les groupes spéciaux

Hé hé ! Vous croyez que c'est fini ? Pas encore. Nous avons les groupes spéciaux à voir. Ces groupes ne sont pas dans la gestion des utilisateurs pour la simple et bonne raison que la qualité de membre de ces groupes ne peut pas être modifiée et **fait référence à l'état de votre système à un instant donné.**

Atelier 4

Gestion des utilisateurs du domaine

Page 45

Nous pouvons néanmoins les observer dans la gestion des droits d'accès. En faisant une recherche sur les « comptes de service » ou les « entités de sécurité intégrées » (modifier les « types d'objets ») :

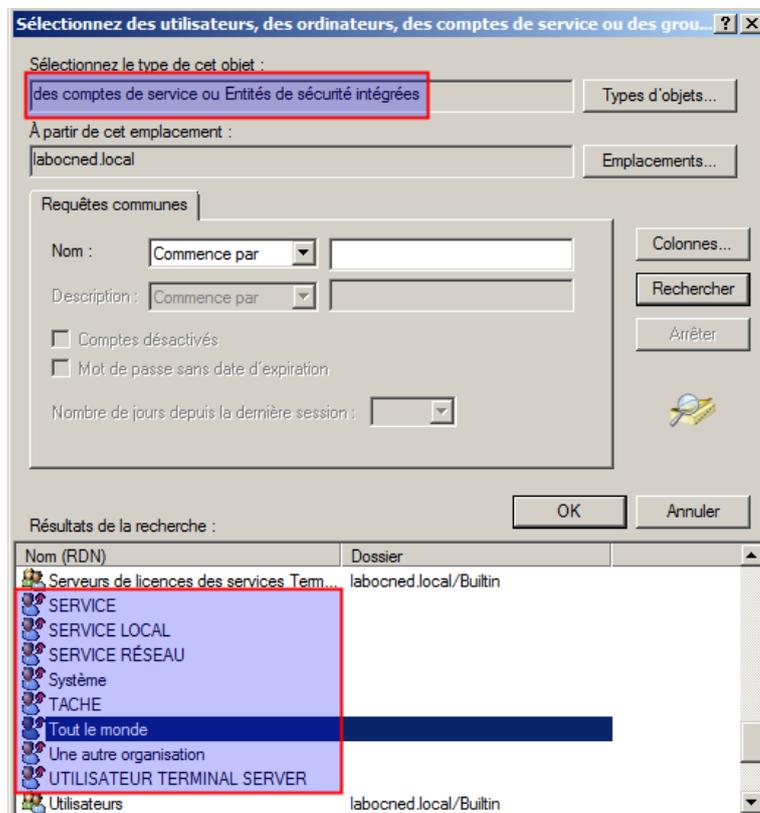


Figure 6 : Recherche des groupes spéciaux

Atelier 4

Gestion des utilisateurs du domaine

Page 46

Un exemple typique est le groupe spécial « tout le monde ». Nous voyons aussi certains comptes utilisateurs spéciaux comme « service », « service local » ou « service réseau ». Examinons les groupes spéciaux les plus utilisés dans la gestion des droits :

Tout le monde	Comprend tous les utilisateurs, ceux que vous avez créés, le compte Invité ainsi que tous les utilisateurs des autres domaines. Attention, car lorsque vous partagez une ressource, ce groupe dispose par défaut de la permission Lecture sur le partage.
Utilisateurs authentifiés	Comprend tout utilisateur possédant un compte d'utilisateur et un mot de passe pour la machine locale ou Active Directory. Affectez des permissions à ce groupe plutôt qu'au groupe Tout le monde.
Créateur propriétaire	Toute personne ayant créé ou pris possession d'une ressource, fait partie de ce groupe pour la ressource concernée. Le propriétaire d'une ressource dispose des pleins pouvoirs sur cette dernière.
Réseau	Comprend toute personne accédant via le réseau à une ressource.
Interactif	Comprend tous les utilisateurs qui ont ouvert une session localement (dans le cas où vous utilisez le « bureau à distance » ce groupe comporte tous les utilisateurs ayant ouvert une session sur le serveur de terminal).

3D. Groupes manuels

L'écran de création de groupe se présente ainsi, nous retrouvons les caractéristiques présentées juste avant :

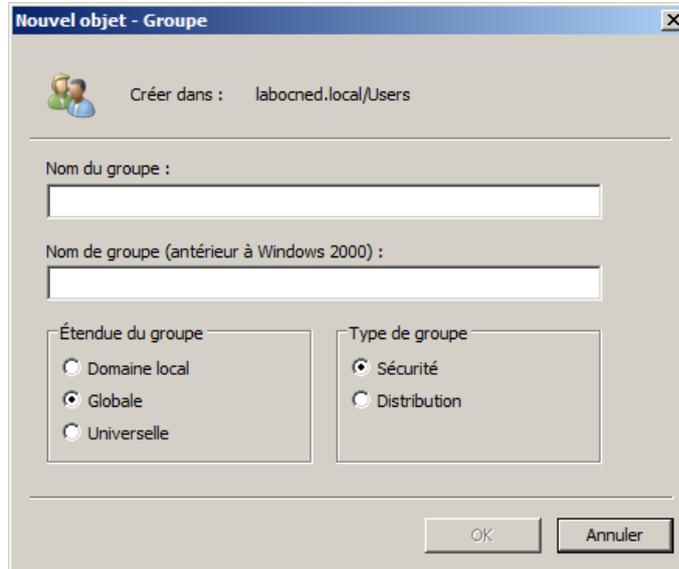


Figure 7 : Création de groupe

Nous allons maintenant créer dans chaque OU de classe un groupe g_profs_21 dans l'OU seconde1 et g_profs_22 dans l'OU seconde2 :

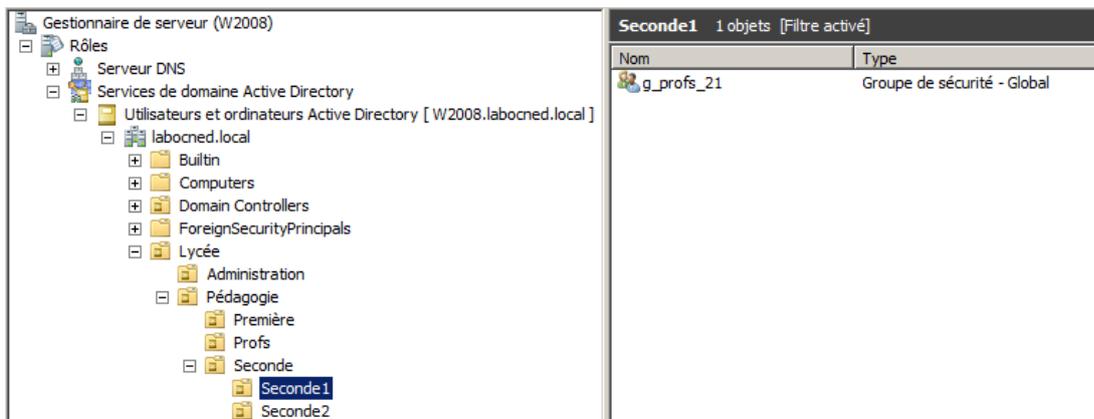
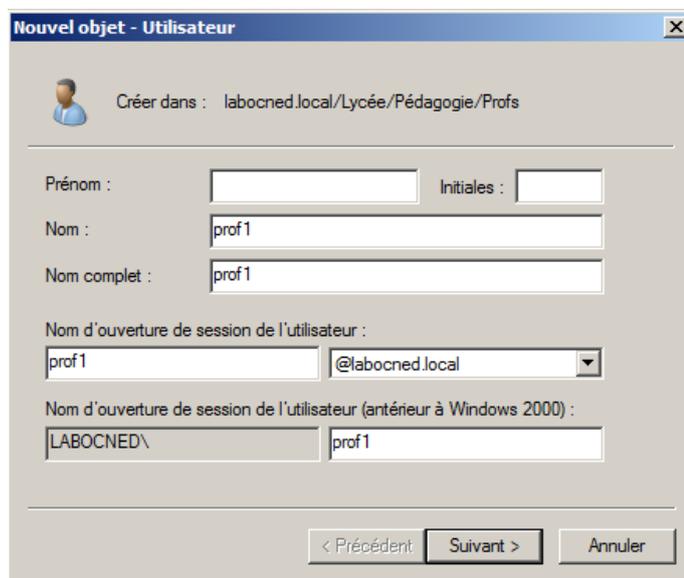


Figure 8 : Création d'un groupe dans une OU

Nous créerons toute à l'heure des groupes locaux.

4. Création des utilisateurs

Vous créez dans l'OU Profs 4 professeurs prof1, prof2, prof3, prof4. Chacun devra saisir son propre mot de passe lors de l'ouverture de session. Le principe est de créer un utilisateur comme modèle, puis de le copier pour les suivants.



Lors de la création de l'utilisateur, en sus des informations nominatives le concernant, un « login » lui est attribué (nom d'ouverture de session de l'utilisateur).

Atelier 4

Gestion
des utilisateurs
du domaine

Page 48

Figure 9 : Création d'un utilisateur - écran 1

La saisie d'un mot de passe, conforme à la stratégie du domaine (cf. installation) par l'administrateur est obligatoire mais il est fondamental que les utilisateurs disposent de leur propre mot de passe, inconnu de l'administrateur lui-même qui ne peut pas le découvrir (il est stocké chiffré dans AD). On laisse donc coché « l'utilisateur doit changer de mot de passe... » :

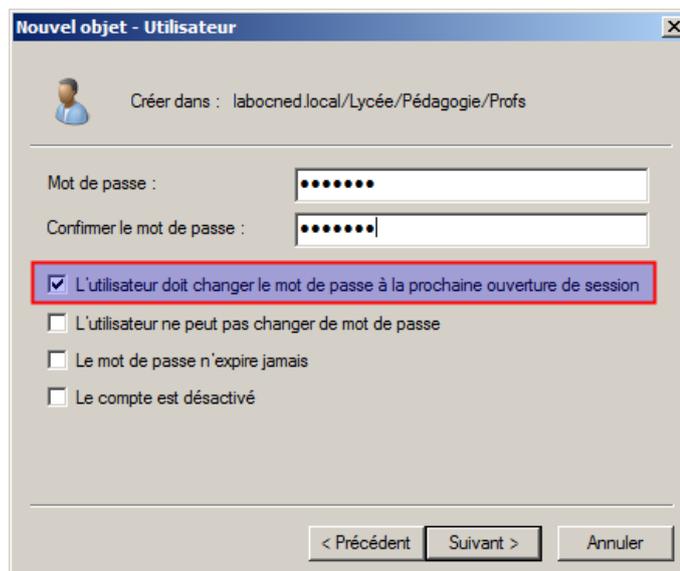


Figure 10 : Création d'un utilisateur - écran 2

Ensuite, pour les suivants :

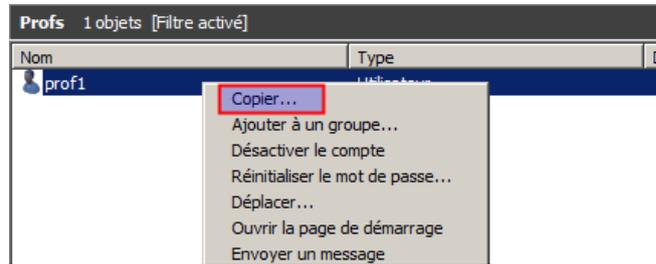


Figure 11 : Copie d'un utilisateur

Maintenant, imaginons que prof1 et prof2 interviennent en seconde1 et que prof1, prof3 et prof4 en seconde2 (donc prof1 intervient dans 2 classes). Mettez ces professeurs dans le groupe global correspondant (clic droit / ajouter à un groupe / avancé pour pouvoir rechercher le groupe). Ce qui nous donnera par exemple pour le groupe g_prof_21 :

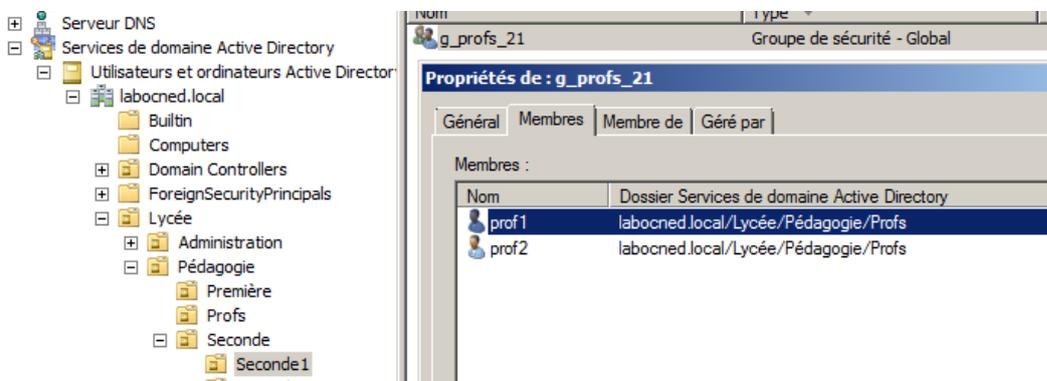


Figure 12 : Membres d'un groupe

Atelier 4

Gestion des utilisateurs du domaine

Maintenant vous faites des manipulations similaires pour les élèves. Créez deux groupes globaux (g_eleves_21 et g_eleves_22) dans l'OU de la classe correspondante. Mettez dans le groupe g_eleves_21, les élèves eleve_211, eleve_212 et dans le groupe g_eleves_22, les élèves eleve_221 et eleve_222. Les élèves seront auparavant créés dans une OU Elèves à la racine de l'OU pédagogie (idem « Profs »). Choisissez ensuite le mode « utilisateurs, contacts, groupes et ordinateurs en tant que conteneurs » dans le menu « affichage » pour obtenir l'affichage ci-dessous qui vous permettra de contrôler votre travail :

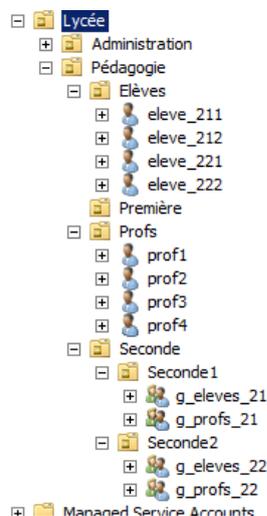


Figure 13 : Structure AD

Page 49

Vous remarquerez au passage que les groupes ne sont pas des conteneurs contrairement aux OU : les membres du groupe ne sont pas présentés dans l'arborescence.

5. Gestion des droits d'accès

Maintenant que notre mini-structure est en place (vous imaginez le travail pour un lycée important), nous allons pouvoir nous amuser un peu. Imaginons que chaque classe dispose d'un répertoire partagé sur le serveur. Le principe est que les professeurs de la classe peuvent lire et écrire, les élèves peuvent seulement lire.

Créez deux groupes de domaine local :

- dl_partage_eleves_211 contenant le groupe de domaine local des élèves de seconde1
- dl_partage_profs_211 contenant le groupe de domaine local des professeurs de seconde1

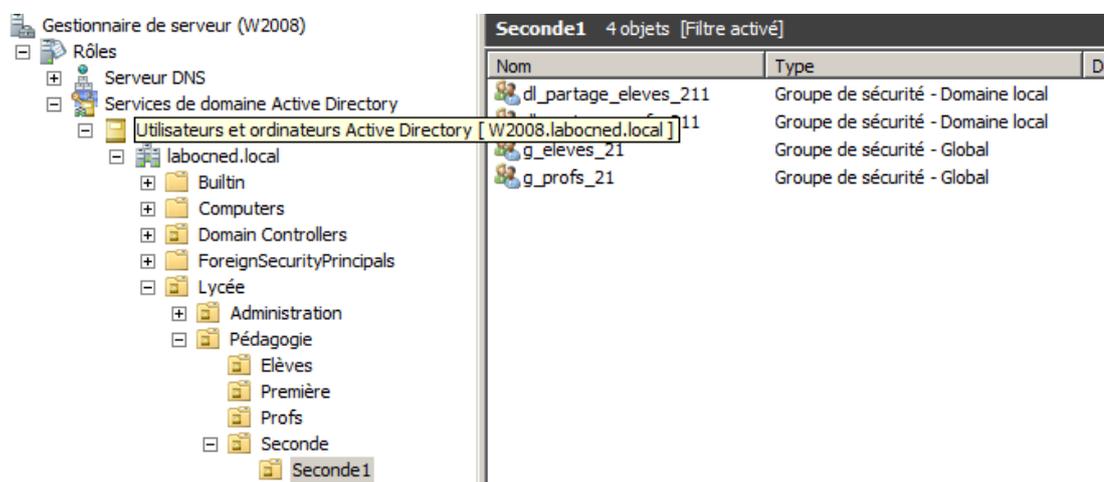


Figure 14 : Création de groupes de domaine local

Dans l'explorateur Windows, créez à la racine d'un disque un répertoire « partages ». Dedans, vous créez un répertoire « seconde1 » que vous partagez (clic droit / propriétés / partage) :

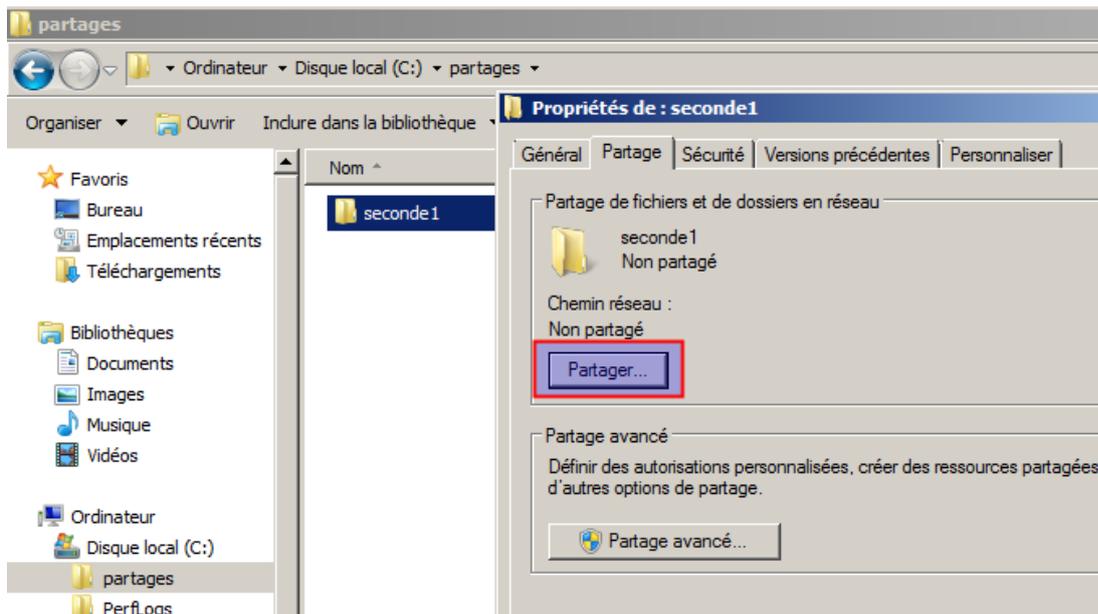


Figure 15 : Partage d'un répertoire

Ensuite, en cliquant sur le bouton « Partager... » vous attribuez les droits d'accès définis plus haut en laissant les droits par défaut de l'administrateur :

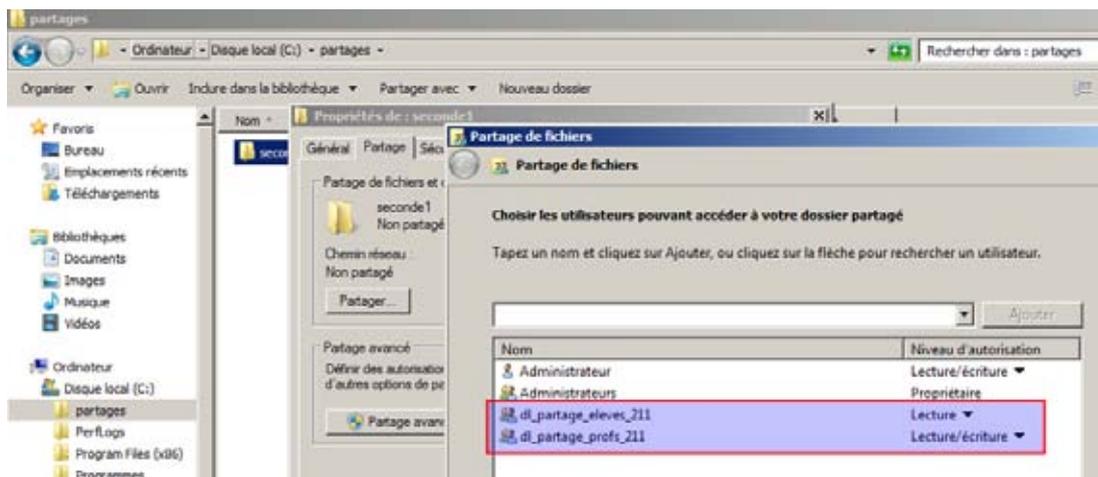


Figure 16 : Droits sur le partage

Enfin, vous ajoutez ce partage dans l'OU correspondant à cette classe. Le chemin réseau à indiquer, puisqu'il n'y a pas de sélecteur, est au format UNC \\<nom machine>\<nom partage> (vous pouvez le copier-coller dans les propriétés du partage) :

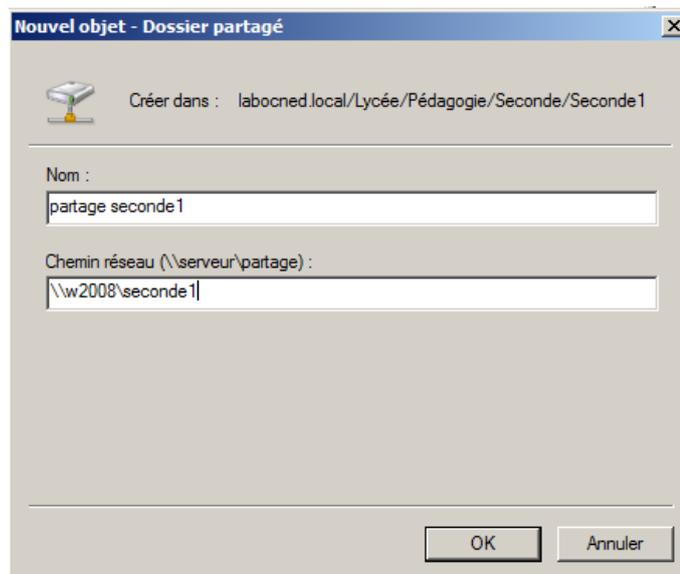


Figure 17 : Ajout du répertoire partagé à AD

Ce qui nous donne désormais dans la liste des objets de l'OU seconde1 :



Figure 18 : Objets de l'OU

Atelier 4

Gestion des utilisateurs du domaine

Page 52

Continuons dans cette logique et démontrons ici l'intérêt de l'architecture « groupe local de domaine » / « groupe global ». L'ensemble des professeurs du lycée dispose d'un répertoire partagé « commun » dans lequel ils ont un droit en lecture/écriture.

Créez dans l'OU pédagogie un groupe de domaine local dl_commun_profs dans lequel vous insérez les deux groupes de profs. Puis vous créez un répertoire « commun » dans le répertoire « partages ». Vous le partagez en mettant ce groupe en lecture/écriture.

Nous accéderons à ces différents partages dans l'atelier suivant, une fois qu'une station sera intégrée au domaine.

À retenir

Active Directory propose les outils permettant d'organiser les utilisateurs. Les unités d'organisation (OU) sont des conteneurs dans lesquels on peut placer tous types d'objets, y compris des OU. Elles permettent en particulier de déléguer l'administration à d'autres utilisateurs.

Les groupes d'utilisateurs jouent un rôle central dans la définition de la sécurité. Seuls des utilisateurs peuvent être membres d'un groupe. Lors de l'installation, Windows a créé un certain nombre de groupes prédéfinis qu'il faut évidemment conserver. Des groupes spéciaux existent également et sont très utiles dans la définition de la sécurité. Ils ne peuvent pas être gérés par l'administrateur car ils reflètent l'état du système à un instant t. Les groupes ont des portées différentes (Domaine local et global). Les groupes globaux reflètent généralement la structure de l'entreprise alors que les groupes de domaine local sont utilisés pour la définition des droits d'accès sur les objets du système. Il est conseillé de mettre en oeuvre la méthodologie AGDLP : ne pas mettre de droits directement sur les utilisateurs (sauf exception) mais placer les utilisateurs dans un groupe global, puis placer un ou plusieurs groupes globaux dans un groupe de domaine local. Enfin, attribuer les droits sur ce dernier groupe.

Concernant la gestion des utilisateurs, il est important de signaler que les utilisateurs doivent être responsables de leur mot de passe et que l'administrateur ne peut pas le découvrir (par des moyens honnêtes disons :-)

Si vous voulez approfondir

Nous n'avons vu ici que l'essentiel. Vous pouvez vous plonger dans l'abondante littérature concernant ce sujet, à commencer par la documentation en ligne de Windows. Bonne lecture.

Atelier 4

Gestion
des utilisateurs
du domaine

Page 53

Atelier 5

Intégration d'une station au domaine

► **Durée approximative de cet atelier : 1 heure 30**

► **Objectif**

Apprendre à intégrer une station Windows à un domaine Windows. Action indispensable pour profiter de toutes les possibilités offertes par Active Directory.

► **Durée approximative de cet atelier**

Notre serveur Windows 2008 R2 SP1 contrôleur de domaine installé au TP précédent et une machine sous Windows 7 pro, de préférence installée de frais.

► **Considérations techniques**

Nous intégrons une machine à un domaine et voyons l'intérêt pour l'administration.

► **Contenu**

1. Introduction	56
2. Configuration IP.....	56
3. Intégration au domaine	58
4. Validation.....	60
5. Stratégies de groupe.....	62

1. Introduction

Pour pouvoir faire pleinement partie du domaine et contrairement au modèle « groupe de travail » qu'il suffit de déclarer, notre machine doit être intégrée. Ne fait pas partie d'un domaine qui veut, c'est une configuration réalisée par l'administrateur qui va permettre à la machine de se faire connaître du contrôleur de domaine et d'expliquer à la station que son référent en matière de sécurité est le contrôleur. Nous verrons que lors de cette étape, un compte va être créé pour la machine.

Dans un premier temps, nous allons vérifier les configurations IP de nos machine : la cohérence de celles-ci est indispensable au processus d'intégration. Une fois l'intégration réalisée, nous constaterons les effets sur la station et le serveur. Puis nous vérifierons le bon fonctionnement des configurations réalisées à l'atelier précédent.

2. Configuration IP

Commençons par vérifier les paramètres réseau du serveur pour nous en inspirer car celui-ci va constituer notre « référence ». Sur le serveur Windows 2008, lançons un ipconfig /all :

```
C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : W2008
Suffixe DNS principal . . . . . : labocned.local
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS. : labocned.local

Carte Ethernet Connexion au réseau local :
Description. . . . . : Carte Intel(R) PRO/1000 MT pour station de tra
vail
Adresse physique . . . . . : 08-00-27-06-AC-E7
DHCP activé . . . . . : Non
Configuration automatique activée. . . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::f419:f79d:facf:a171%10<préféré>
Adresse IPv4. . . . . : 192.168.1.100<préféré>
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 235405351
DUID de client DHCPv6. . . . . : 00-01-00-01-15-B4-FC-A6-08-00-27-06-AC-E7
Serveurs DNS. . . . . : :1
127.0.0.1
NetBIOS sur Tcpip. . . . . : Activé
```

Figure 1 : Configuration IP du serveur

Dans la masse d'informations, c'est la configuration IP et surtout le serveur DNS qui nous intéressent. En conséquence, nous allons configurer notre station Windows 7 avec des paramètres similaires avant de nous lancer dans l'intégration au domaine.

Exercice 1

Petite colle : sur la station quelle adresse IP va-t-on mettre pour le serveur DNS ?

Passons sur la station et réalisons une configuration IP de ce type (à adapter éventuellement en fonction de votre réseau et de votre contrôleur de domaine) :

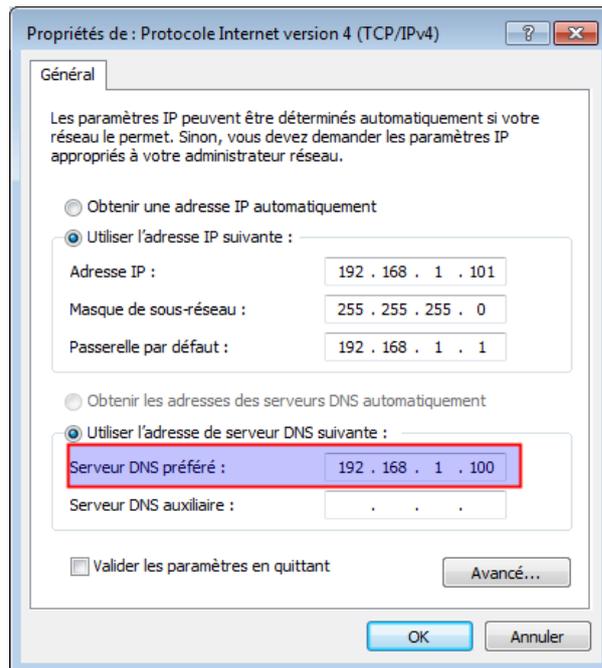


Figure 2 : Configuration IP de la station Windows 7

L'adresse IP du serveur DNS est celle de notre machine Windows 2008. Mais pour la partie DNS, ce n'est pas fini. En cliquant sur « avancé » puis sur l'onglet DNS, nous réalisons ceci :

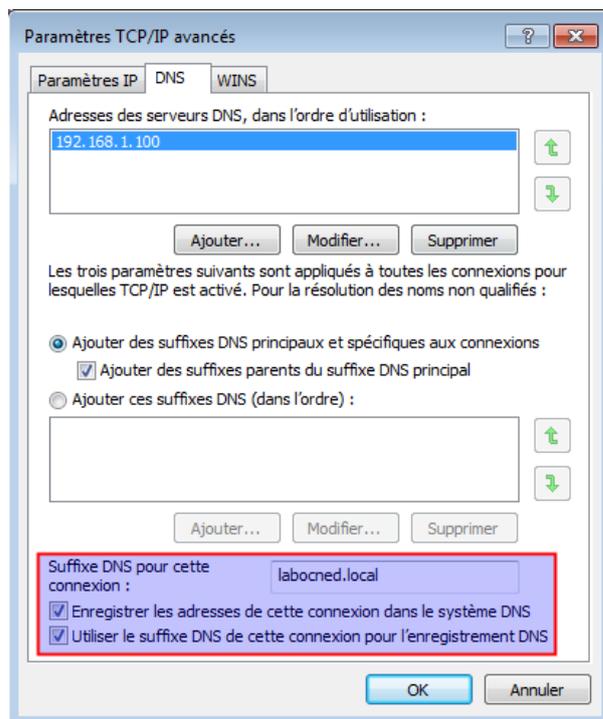


Figure 3 : Configuration DNS de la station

Atelier 5

Intégration
d'une station
au domaine

Page 57

Nous indiquons notre nouveau suffixe DNS qui est le nom du domaine. Nous cochons ensuite les deux cases en dessous qui vont nous permettre d'ajouter les machines automatiquement au serveur DNS. Enfin, réalisons un petit test de connectivité avec notre serveur w2008 afin de s'assurer que tout roule :

```
C:\Users\util1>ping w2008

Envoi d'une requête 'ping' sur w2008.labocned.local [192.168.1.100] avec 32 octets de données :
Réponse de 192.168.1.100 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.100 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.100 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.100 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Figure 4 : ping entre la station et le serveur

Ceci nous garantit que le DNS fonctionne correctement et que les noms de machines sont bien reconnus. Vous remarquez que Windows a automatiquement ajouté au nom de la machine (w2008) le nom de domaine DNS (labocned.local).

3. Intégration au domaine

Atelier 5

Intégration d'une station au domaine

Ça y est vous êtes prêt ? Les ceintures sont attachées ? Non, rassurez-vous, comme toutes les garanties ont été prises auparavant, tout doit fonctionner correctement. Le point de départ se situe dans les propriétés système puis dans « modifier les paramètres » :

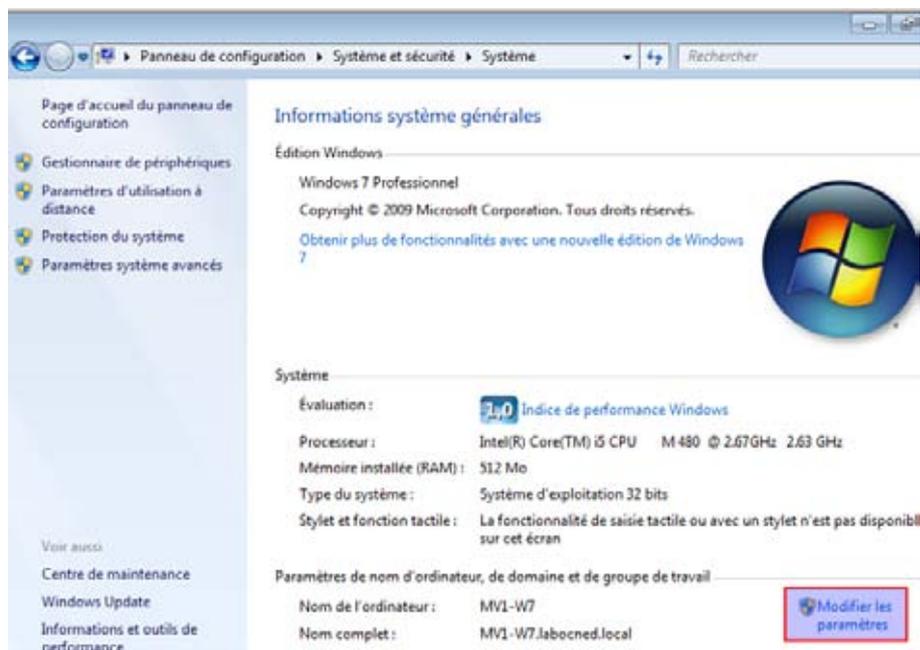


Figure 5 : paramètres de domaine

Ce qui nous amène sur l'écran ci-dessous qui est le point de départ du processus :

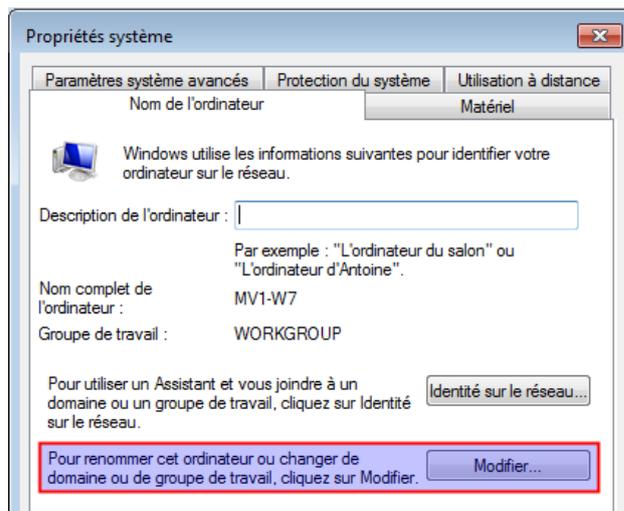


Figure 6 : Modifier l'intégration au domaine

Ensuite, nous indiquons tout simplement à quel domaine nous voulons être intégré :

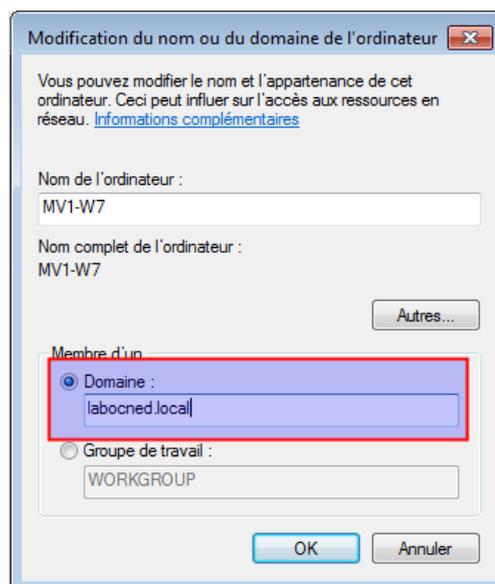


Figure 7 : Saisie du nom de domaine à joindre

Forcément, on nous demande un compte autorisé pour cette tâche (en général un administrateur, mais cela peut être quelqu'un du groupe administrateur ou un opérateur de compte) :

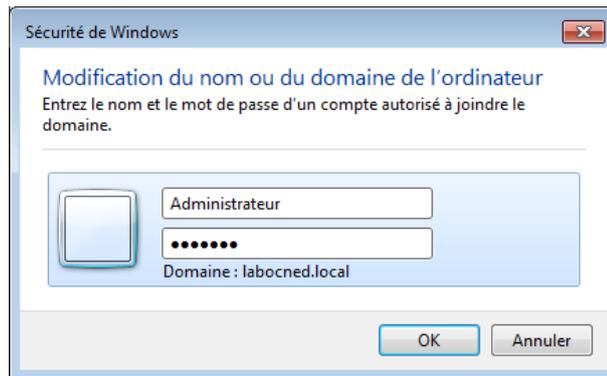


Figure 8 : identification d'un compte de domaine autorisé

Et maintenant voici !

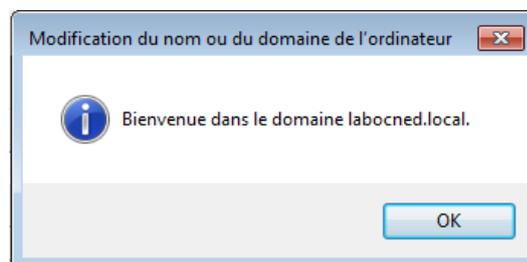


Figure 9 : on nous confirme que l'opération est réussie

Atelier 5

Intégration
d'une station
au domaine

Page 60

Bravo ! Vous avez gagné un petit redémarrage...

4. Validation

4A. Côté station

Vous redémarrez et sur l'écran de connexion, vous allez constater la différence :

Remarquez la syntaxe du nom d'utilisateur pour distinguer l'administrateur du domaine de celui de la machine local : DOMAINENom d'utilisateur.

Vous vous connecterez donc avec un compte de domaine (administrateur ou autre). Notez que vous pouvez toujours vous connecter en mode local (ou éventuellement, sur un autre domaine si des relations existent) :



Figure 10 : Écran de connexion Windows 7

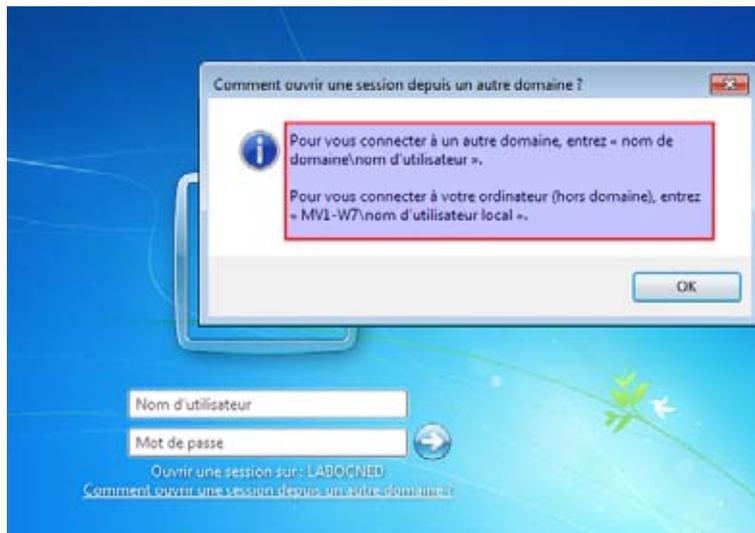


Figure 11 : Choix du mode de connexion

Une fois connecté, nous pouvons observer la configuration réseau de notre station :

```

C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : MVI-W7
Suffixe DNS principal . . . . . : labocned.local
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS : labocned.local

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion . . . : labocned.local
    Description . . . . . : Carte Intel(R) PRO/1000 MT pour station de travail
    Adresse physique . . . . . : 08-00-27-A5-A6-92
    DHCP activé . . . . . : Non
    Configuration automatique activée . . . : Oui
    Adresse IPv6 de liaison locale . . . . . : fe80::3de6:332:b2de:e6f1x11<préféré>

    Adresse IPv4 . . . . . : 192.168.1.101<préféré>
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.1.1
    IAD DHCPv6 . . . . . : 235405351
    DUID de client DHCPv6 . . . . . : 00-01-00-01-15-48-6C-00-08-00-27-A5-A6-92
    Serveurs DNS . . . . . : 192.168.1.100
    NetBIOS sur Tcpip . . . . . : Activé
  
```

Figure 12 : Configuration réseau de la station

Nous constatons que le suffixe DNS a été modifié.

4B. Côté serveur

L'intégration de notre machine a eu des impacts sur le serveur.

4B1. Côté DNS

Notre machine a été ajoutée automatiquement au serveur DNS. Son adresse et son nom pourront donc être connus des autres machines du réseau :

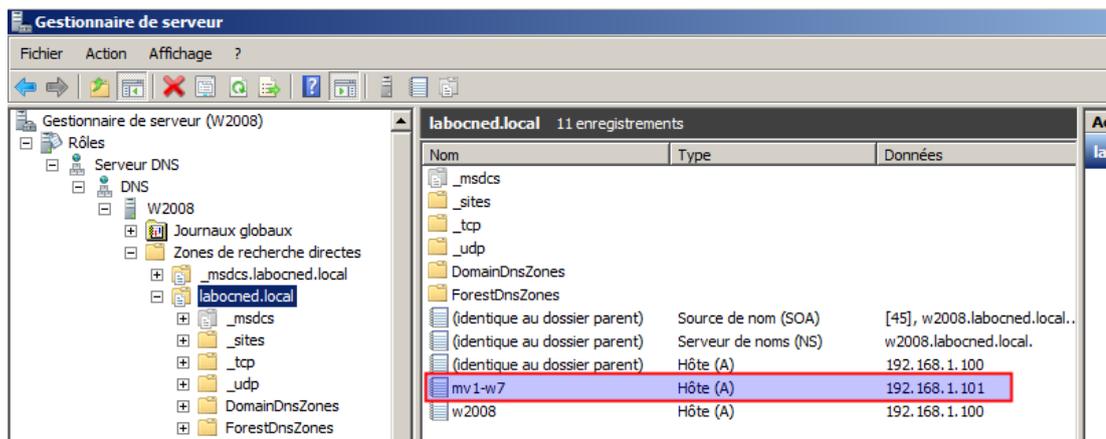


Figure 13 : enregistrement DNS

4B2. Côté Active Directory

De même dans l'interface de gestion du domaine, dans le conteneur « Computers », nous retrouvons notre machine, signe que celle-ci a bien été intégrée dans l'Active Directory.

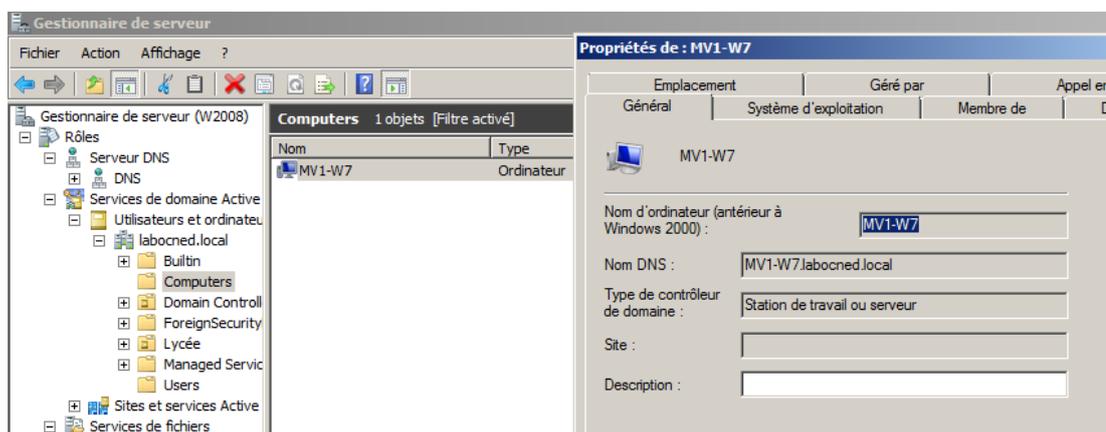


Figure 14 : Machine dans AD

Passons maintenant à ce qui fait l'intérêt d'un domaine : la gestion des droits et des stratégies.

5. Stratégies de groupe

5A. Intérêt

Connectez-vous sur votre station Windows 7 avec un compte d'élève de seconde1 (donc compte de domaine). Conformément au paramétrage de son compte, vous devrez saisir un nouveau mot de passe qui ne sera connu que de l'utilisateur.

Essayons d'accéder aux répertoires partagés sur notre serveur. Vous allez dans « ordinateur » puis dans le menu « réseau ». Vous allez alors tomber sur ceci :

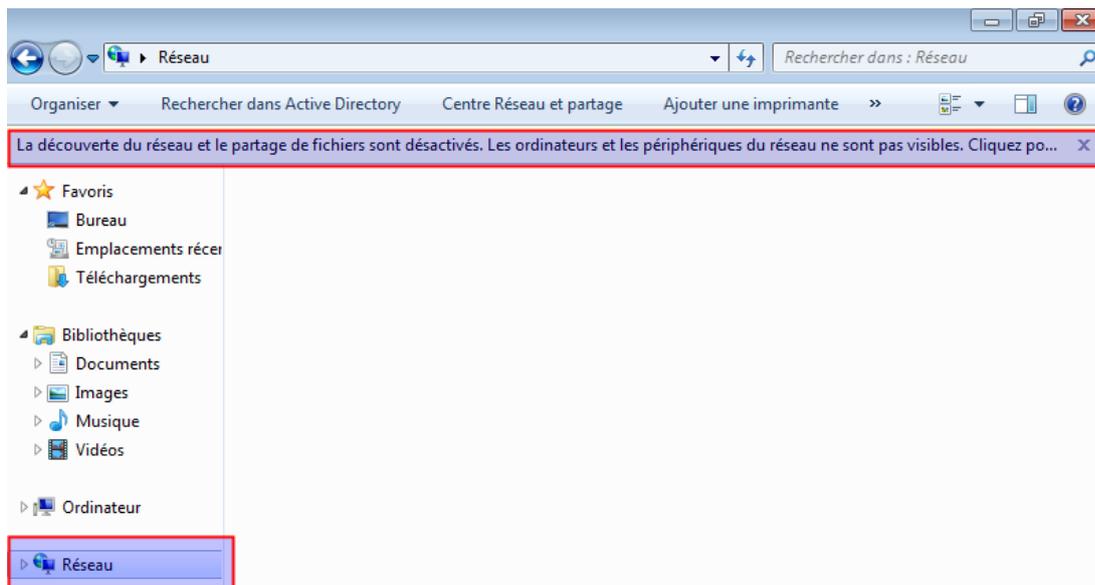


Figure 15 : Découverte du réseau désactivée

La découverte du réseau est désactivée par défaut ! Un utilisateur « lambda » comme notre élève ne peut pas l'activer et seule une personne avec des droits d'administrateur le peut... Si votre réseau comporte des dizaines de machines, vous vous voyez passer sur chacune ? Excellente transition vers les « **stratégies** » Windows (ou GPO pour *Group Policy Object*) !

5B. Notion de stratégie de groupe

Une stratégie de groupe peut être définie comme (selon Wikipedia) : « des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement *Active Directory*. »

Bien que les stratégies de groupe soient régulièrement utilisées dans les entreprises, elles sont également utilisées dans les écoles ou dans les petites organisations pour restreindre les actions et les risques potentiels comme par exemple le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, etc. »

En clair, on va pouvoir décider de façon centralisée d'un certain nombre de paramètres des stations de travail du domaine. Ces paramètres pourront être appliqués de façon différente suivant les endroits de l'arborescence Active Directory, d'où l'intérêt des OU par exemple. Ce qui permet donc d'avoir des paramétrages différents selon les profils d'utilisateurs.

5C. Stratégies locales

En premier lieu, il faut savoir que des « stratégies locales » existent sur chaque machine Windows qu'elles soient serveur ou non. Elles définissent les paramètres en vigueur. Sur la machine Seven, recherchez « stratégie » dans le menu démarrer. Bien sûr il faut être administrateur local de la machine ou du domaine pour accéder à ces informations :

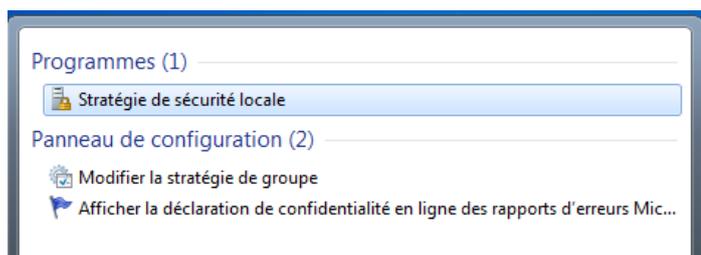


Figure 16 : stratégie locale d'une machine

Ci-dessous, nous voyons le contenu de la stratégie locale de notre machine : ensemble de paramètres par défaut que l'on peut modifier directement dans le cas d'une machine hors domaine :

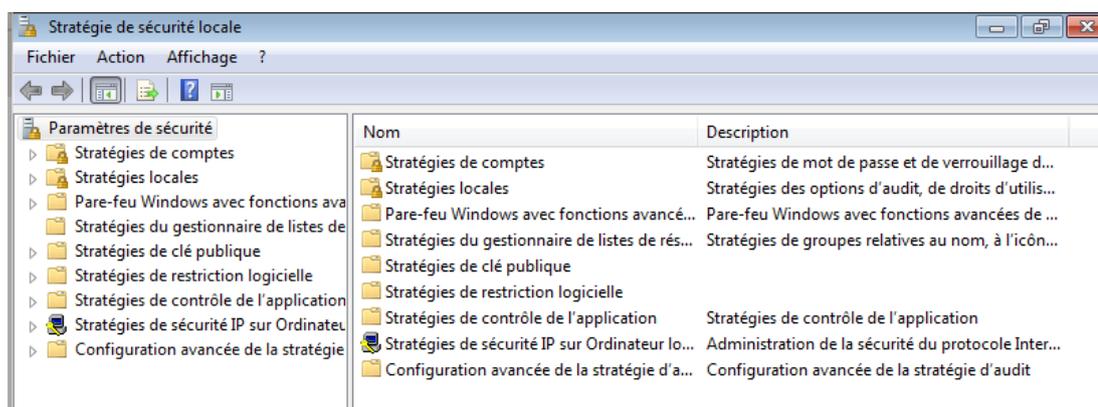


Figure 17 : Détail d'une stratégie locale

Atelier 5

Intégration
d'une station
au domaine

Page 64

Sur un contrôleur de domaine, les GPO ont à peu près le même contenu. Le principe étant qu'au démarrage d'une station, celle-ci va chercher sur le contrôleur de domaine la ou les stratégies à s'appliquer.

La figure ci-dessus résume bien l'intérêt de la chose : action unique de l'administrateur, effet multiple sur des utilisateurs et/ou des machines.

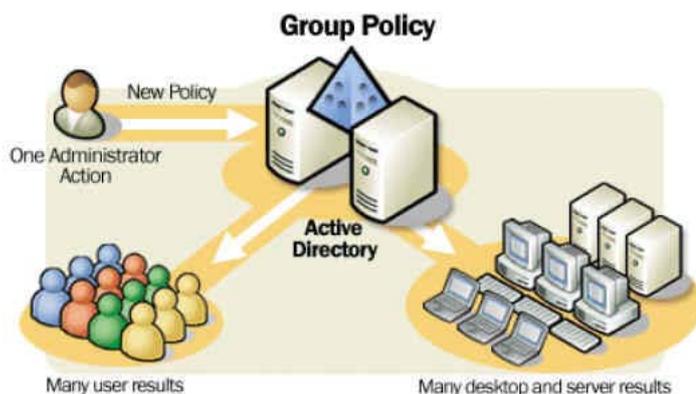


Figure 18 : Principe des stratégies de groupe

5D. Stratégies de groupe

Revenons sur notre serveur 2008 R2. Recherchez « stratégie » dans le menu démarrer et choisissez « gestion de stratégie de groupe » (n'allez pas dans « stratégie locale »!), ce qui vous amène sur cet écran :

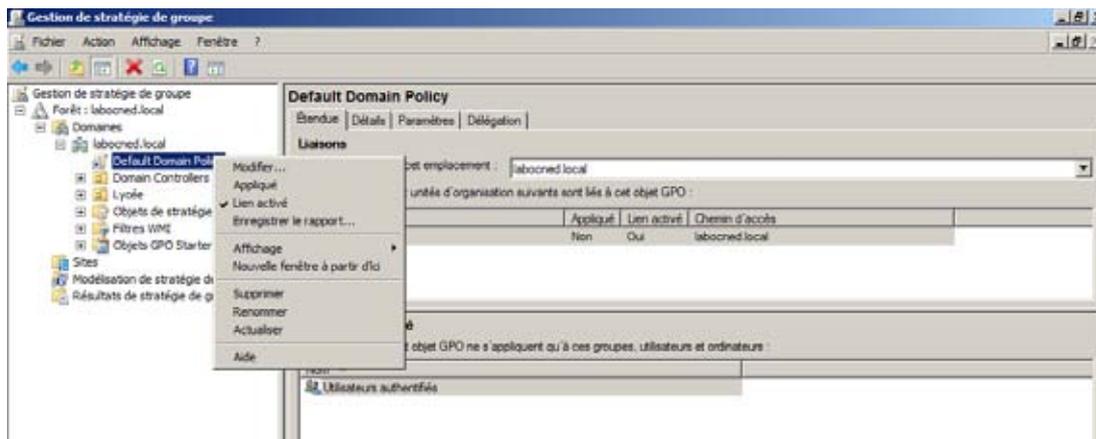


Figure 19 : Gestion de stratégie de groupe

Dans un premier temps, modifions la stratégie du domaine dans son intégralité (Default Domain Policy). Cliquons droit sur cet item puis sur « Modifier... ».

Revenons à notre sujet de départ : activer par défaut la « découverte du réseau », ce qui empêche de voir les machines et partages du domaine. Cela repose en fait sur des règles du pare-feu personnel. En effet, cette fonctionnalité a été désactivée par défaut pour des raisons de sécurité. Sur la station, lorsque l'on clique sur le bandeau « activer la découverte etc. », ce sont en fait des règles de pare-feu qui sont appliquées sur la machine. Pour activer la découverte sur tout le domaine, nous devons intervenir dans la GPO concernée. Suivez le chemin (allez jusqu'aux règles de trafic entrant du pare-feu) :

Atelier 5

Intégration d'une station au domaine

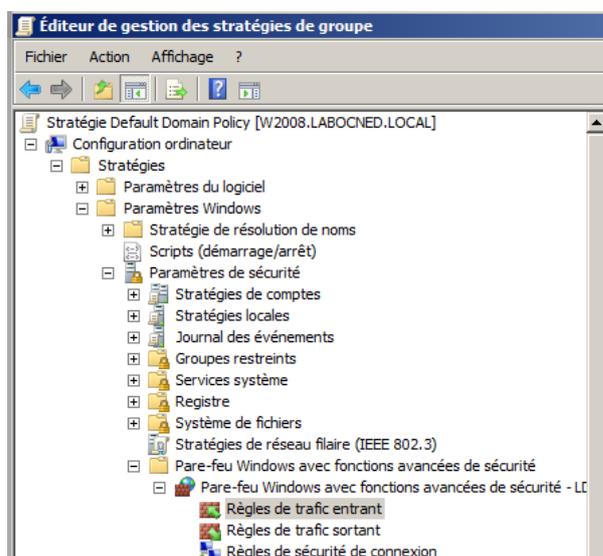


Figure 20 : Règle de pare-feu

Ajoutez une nouvelle règle de trafic entrant et choisissez « prédéfinie ». Sélectionnez « recherche du réseau » (mauvaise traduction pour découverte) :

Page 65

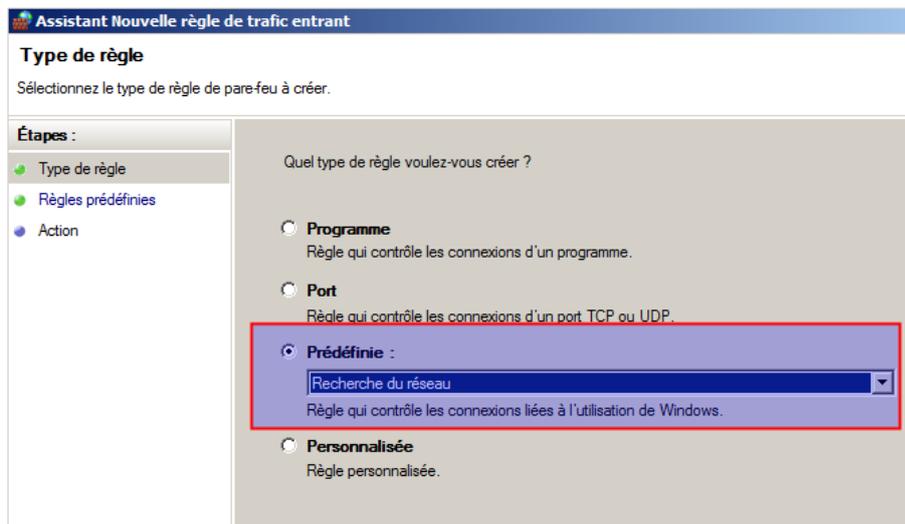


Figure 21 : choix des règles de pare-feu

Validez les différentes règles proposées. Fermez l'éditeur de stratégies. Redémarrez votre station (c'est à ce moment que les stratégies sont chargées) et reconnectez-vous. Vous avez maintenant accès à la recherche du réseau :

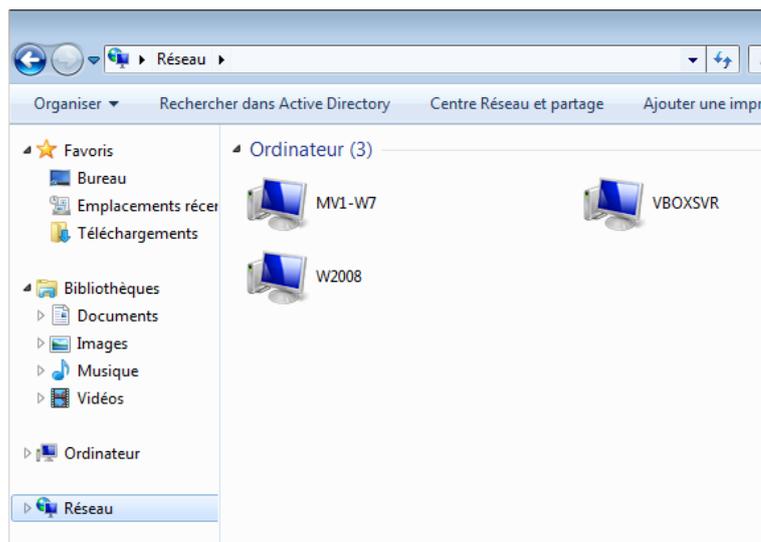


Figure 22 : Voisinage réseau

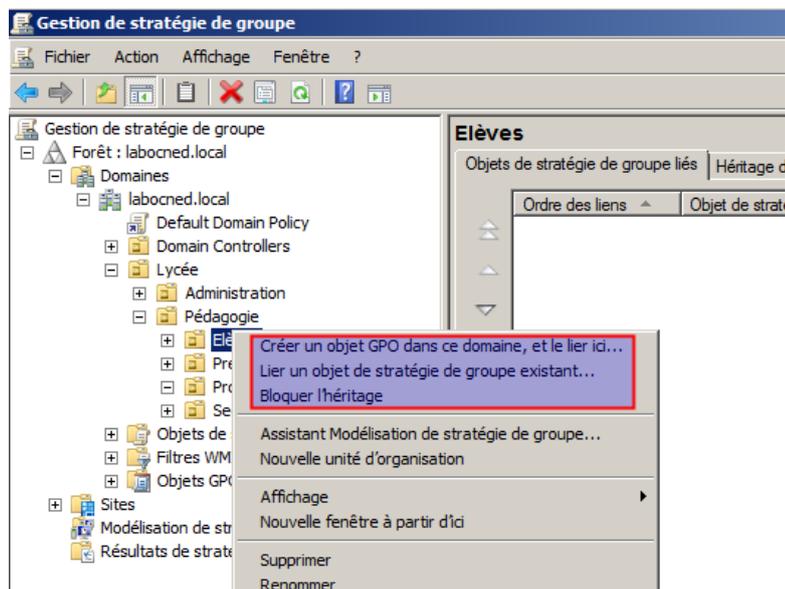
Pour finir, vous vérifiez les droits d'accès définis à l'atelier précédent. Un élève ne peut même pas rentrer dans « commun » dans W2008, alors qu'un professeur le peut. L'élève ne peut pas créer de fichier dans son dossier de classe (seconde1) par exemple, mais peut lire des données mises par l'un de ses professeurs.

Faisons une autre manipulation. Nous voulons que les élèves n'aient pas accès au panneau de configuration de leur machine (ceci ne concernera pas les professeurs). Nos élèves sont tous dans une OU, ce qui est bonne chose puisque nous allons leur définir une stratégie spécifique. En cliquant droit sur l'OU élèves, nous voyons :

Atelier 5

Intégration
d'une station
au domaine

Page 66



Dans la première partie de ce menu contextuel, nous remarquons ici plusieurs éléments très intéressants :

- les UO constituent une bonne base pour affecter les GPO, l'organisation doit donc être bien pensée
- on peut réutiliser à plusieurs endroits des GPO existantes (lier un objet ... existant)
- les GPO s'héritent : dans une arborescence d'UO, une GPO appliquée à un niveau supérieur s'applique aussi dans les niveaux inférieurs, sauf indication contraire.

Créons un nouvel objet. Le paramétrage pour désactiver le panneau de configuration se trouve dans « configuration utilisateur / Stratégies / Modèles / Panneau » :

Nous activons ce paramètre. Ensuite, il faut se connecter en tant que professeur et élève sur la station pour constater la différence. Normalement, les GPO (stockées sur le serveur) sont appliquées au démarrage de la machine mais on peut le forcer en faisant un `gpupdate /force` dans un interpréteur de commandes.

À retenir

L'intégration d'une machine à un domaine est faite par l'administrateur. Une configuration DNS cohérente entre le serveur et la station est indispensable.

Une fois la machine intégrée, il est possible de définir des « stratégies » (GPO). De très nombreux paramètres concernant les utilisateurs et les ordinateurs peuvent être fixés. Une seule action de l'administrateur sur une stratégie peut s'appliquer à de nombreux utilisateurs et de nombreuses machines. L'OU est un bon niveau pour appliquer les stratégies.

Les stratégies ne sont pas appliquées immédiatement sur les stations, on peut cependant le forcer avec la commande `gpupdate /force`

Si vous voulez approfondir

Nous n'avons vu ici que l'essentiel. Vous pouvez vous plonger dans l'abondante littérature concernant ce sujet, à commencer par la documentation en ligne de Windows. Bonne lecture.

Atelier 6

Administration à distance Windows

► **Durée approximative de cet atelier : 1 heure**

► **Objectif**

Utiliser les outils de gestion à distance d'un serveur Windows

► **Durée approximative de cet atelier**

Notre serveur Windows 2008 R2 SP1 et une machine sous Windows 7 pro.

► **Considérations techniques**

Les outils d'administration à distance de Windows reposent sur le protocole RDP et le « bureau à distance ».

► **Contenu**

1. Introduction	70
2. Configuration.....	70
3. Utilisation.....	72

Atelier 6

Administration
à distance Windows

Page 69

1. Introduction

Il faut constater deux choses :

- le nombre de serveurs à gérer peut être important
- les serveurs sont en général dans un local spécifique dédié à cet effet ou en data-center.

Il est donc indispensable de pouvoir les administrer via le réseau ou Internet sans avoir un accès physique. Tous les systèmes d'exploitation serveur disposent des outils nécessaires et Windows ne déroge pas à la règle, ils sont même installés par défaut, bien que désactivés. Côté client, divers outils existent, il suffit qu'ils soient conformes au protocole RDP utilisé par ce service : bien sûr la « connexion bureau à distance » de Windows ou rdesktop côté Unix par exemple.

Il faut aussi noter qu'il existe deux modes d'utilisation. Dans notre cas, nous utilisons la fonctionnalité d'administration : seul deux utilisateurs peuvent se connecter simultanément. Si vous voulez plus d'utilisateurs (on n'est donc plus dans un cas d'administration), il faudra installer un rôle de serveur spécifique. Notez que dans ce cas, il faudra aussi acquérir des licences d'accès... C'est néanmoins un mode assez répandu qui permet de partager des applications avec des utilisateurs en évitant les contraintes d'une installation individuelle sur chaque poste.

2. Configuration

Atelier 6

Administration
à distance Windows

Page 70

Avant toute chose, nous allons faire une manipulation absolument indispensable, à plus forte raison lorsque l'on se connecte à distance. Dans la vraie vie, nous n'utilisons jamais le compte « Administrateur » (certains le désactivent même). Pour des raisons de sécurité, il est préférable de créer un compte personnel par personne physique et de le placer dans le groupe local des administrateurs. Cela limitera les risques d'attaque réseau et d'autre part, cela permet plus facilement de savoir qui s'est connecté et les actions réalisées lorsque l'on est plusieurs administrateurs.

Faites les manipulations décrites ci-dessus et désactivez la connexion à distance pour le compte « administrateur » dans les propriétés de son compte :

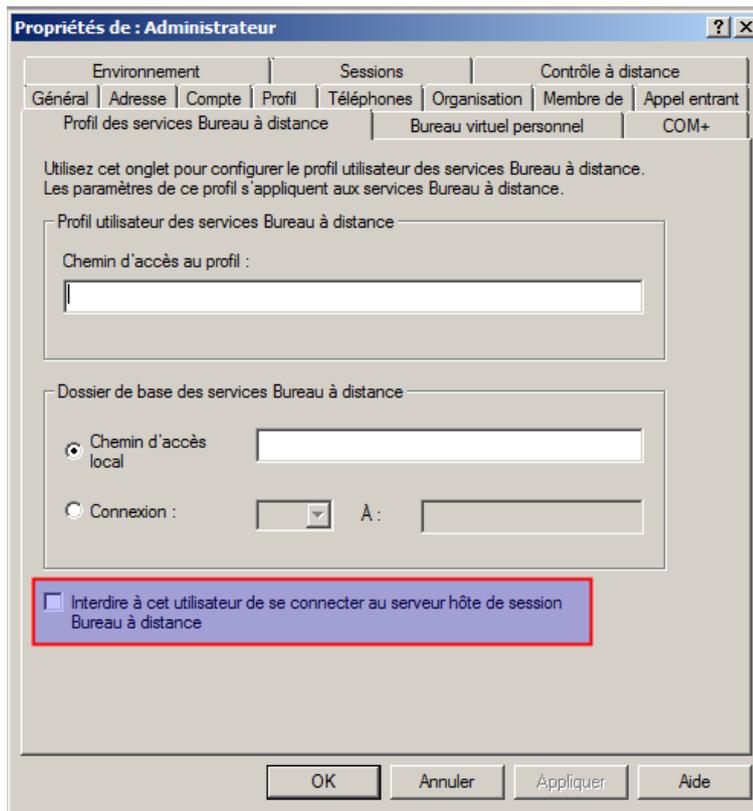


Figure 1 : Désactiver la connexion à distance

S'il tentait de se connecter avec le bureau à distance, il obtiendrait ceci :

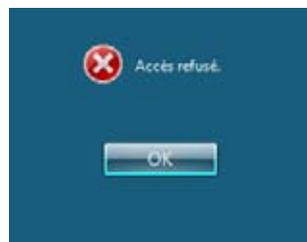


Figure 2 : accès refusé

Pour activer la connexion à distance sur le serveur, il faut se rendre dans les propriétés de l'ordinateur, rubrique « paramètres d'utilisation à distance » :

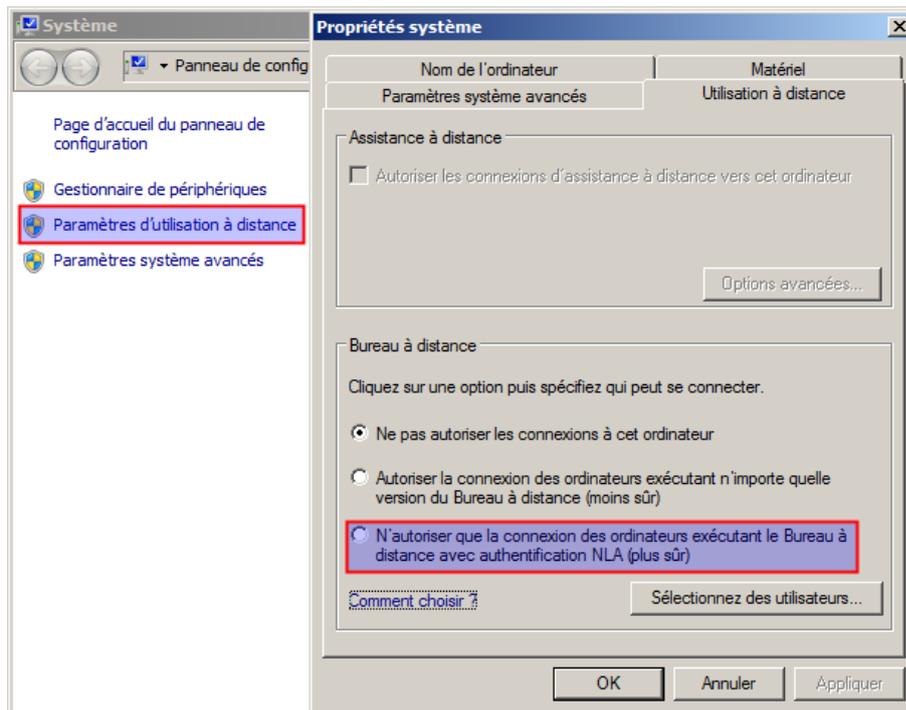


Figure 3 : Activer la connexion à distance

Atelier 6

Administration à distance Windows

Page 72

Deux modes sont disponibles, sachez que le mode avec NLA (Network Layer Authentication) est plus sécurisé mais qu'il faut des versions récentes du client de connexion à distance.

Un avertissement vous propose de configurer le pare-feu pour n'autoriser la connexion à distance que sur certaines adresses réseau. Nous ne le ferons pas ici mais cela peut être utile pour mieux sécuriser votre serveur.

Les membres du groupe des administrateurs ont d'office un accès, sinon il faut les ajouter grâce à la commande « Sélectionnez des utilisateurs... ».

3. Utilisation

3A. Utilisation basique

Pour tester le fonctionnement, nous pouvons tenter une connexion locale. Lançons la « connexion bureau à distance » directement sur le serveur. Il suffit de saisir l'adresse IP ou le nom de la machine :

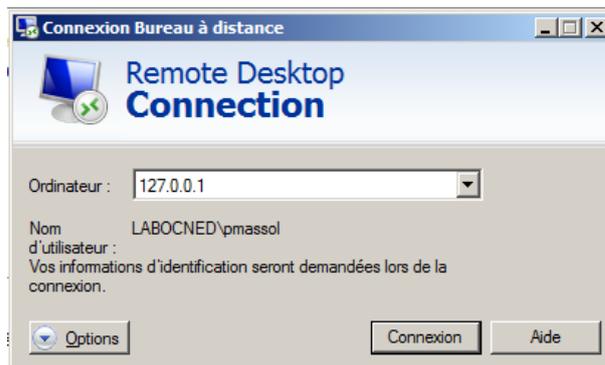


Figure 4 : ouverture d'une connexion

Vous vous authentifiez avec un compte autorisé :

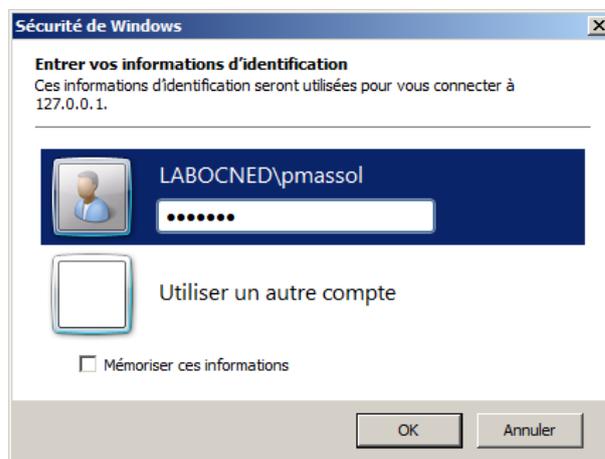


Figure 5 : identification

Vous pourrez rencontrer cet avertissement qui nous indique que nous n'avons pas de certificat de serveur généré par une autorité de certification :



Figure 6 : Erreur de certificat

Vous acceptez. Une fois connecté, on se retrouve dans un bureau tout à fait classique. On pourrait s’y tromper. Le seul élément visuel qui nous rappelle que nous sommes à distance est la barre d’outil située en haut de l’écran :



Figure 7 : barre d’outil bureau à distance

Nous pouvons suivre les connexions dans le gestionnaire de tâches, onglet « Utilisateurs » :



Figure 8 : gestionnaire des tâches

Les connexions à distance sont notées en RDP-Tcp. Le statut peut être « actif » si la session est actuellement utilisée ou « déconnecté » si l’utilisateur a fermé sa connexion à distance sans fermer la session Windows (l’avantage est que vos applications continuent à tourner dans la session Windows et que vous la retrouvez dans l’état où vous l’avez laissé lorsque vous vous reconnectez).

Atelier 6

Administration à distance Windows

Page 74

3B. Paramètres

De nombreux paramètres sont proposés pour gérer l’interaction entre votre session locale et la session distante :

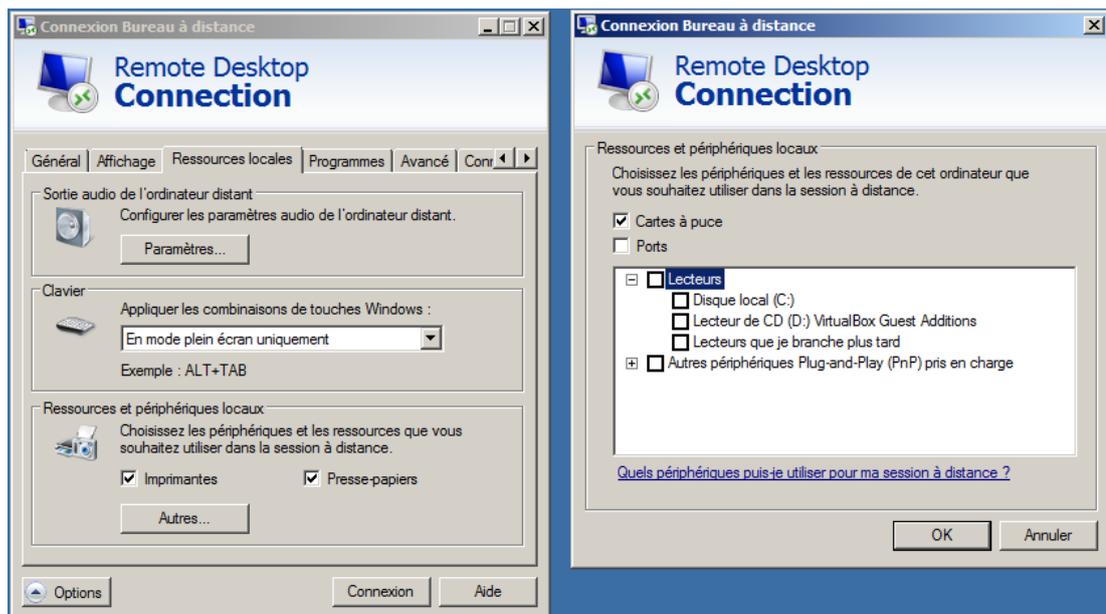


Figure 9 : paramètres RDP

Une fonctionnalité intéressante consiste à partager un disque local de façon à ce qu'il apparaisse dans le bureau distant permettant ainsi l'échange de fichiers (relativement lent) :

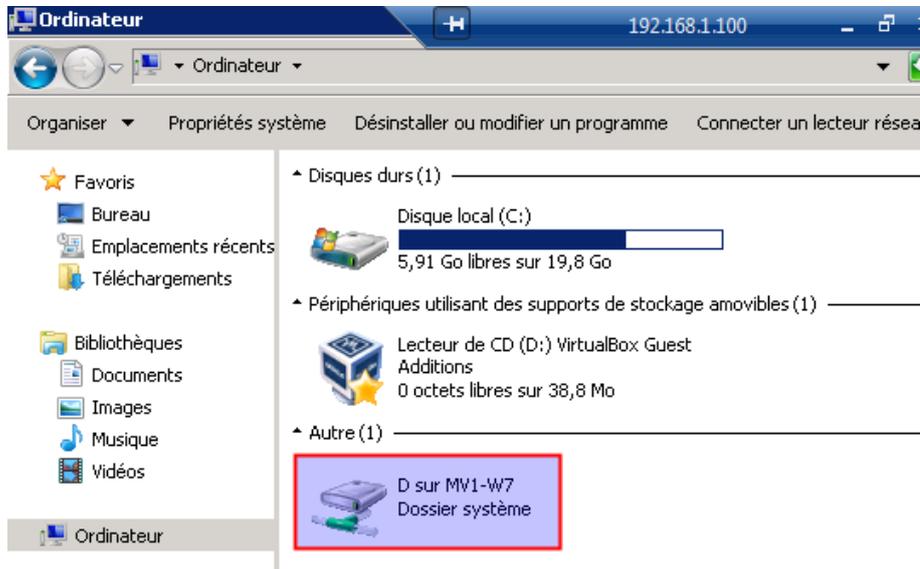


Figure 10 : accès à un lecteur local

En conclusion, rappelons que le client peut être non-Windows. Dans la figure ci-dessous, nous voyons un client Linux Ubuntu ouvrant une session avec le serveur Windows :

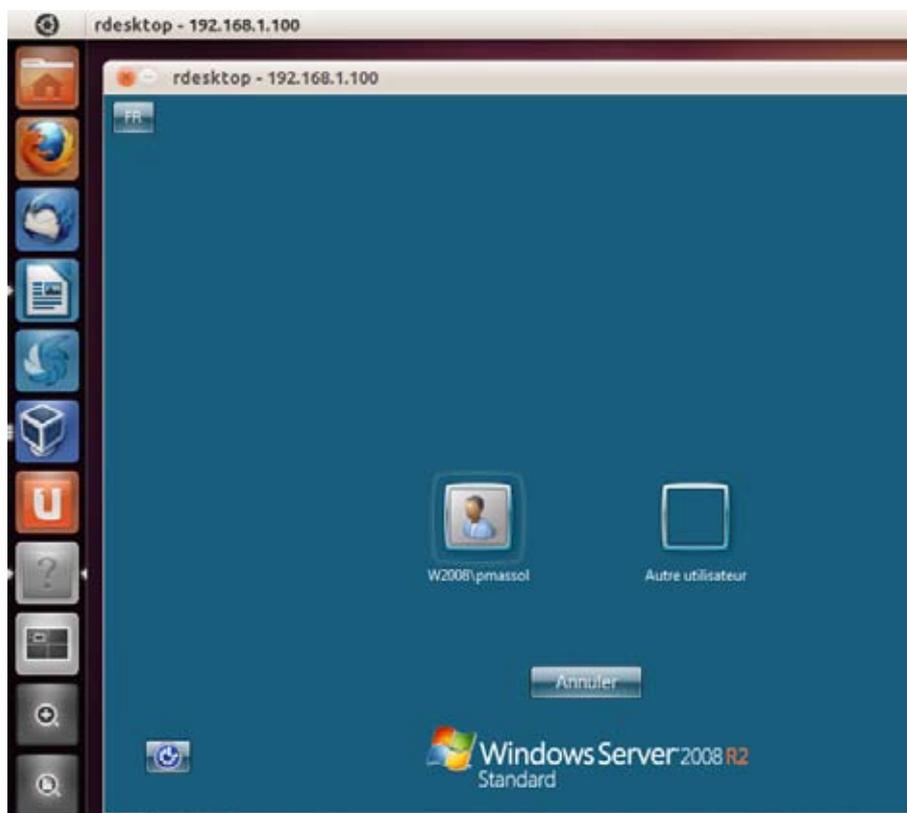


Figure 11 : Connexion à distance via Linux

À retenir

Le compte « Administrateur » ne doit pas être utilisé pour des connexions à distance. Nous créons autant de comptes personnels que d'administrateurs et plaçons ces comptes dans le groupe « Administrateurs ». L'accès au bureau à distance est désactivé pour « Administrateur ».

Le serveur de bureau à distance et le client sont intégrés à Windows. Le serveur autorise deux accès simultanés. Au-delà, il faut installer un « rôle » et acquérir des licences.

La configuration côté serveur est élémentaire et se résume à deux niveaux de sécurité. Côté client, de nombreux paramètres sont disponibles, en particulier la possibilité de partager un disque local dans une session distante.

Si vous voulez approfondir

Mettre en oeuvre des clients RDP non-Windows.

Atelier 7

Serveur d'application web Windows

► Durée approximative de cet atelier : 2 heures

► Objectif

Installer le serveur Web Microsoft IIS (Internet Information Server) et l'environnement d'exécution des applications développées pour le framework.NET.

► Durée approximative de cet atelier

Notre serveur Windows 2008 R2 SP1 et une machine sous Windows 7 pro.

► Considérations techniques

Du fait de la présence du SP1 de Windows 2008 R2, nous installerons la version 7.5 de IIS et le framework 4.0. IIS peut s'installer sur une station de travail mais cela concernera le développement. La mise en production se fera nécessairement sur un système d'exploitation de serveur.

Notez qu'il n'est pas nécessaire que ce serveur soit contrôleur de domaine ou membre d'un quelconque domaine. Une machine autonome peut tout à fait être serveur Web.

► Contenu

1. Introduction	78
2. Installation	78
3. Configuration DNS	81
4. Création d'un nouveau site	82
5. Journaux	85
6. Exécution.....	85
7. Sécurisation du site	87

1. Introduction

L'ensemble constitué par Windows server / IIS /.NET est l'un des serveurs d'application Web avec LAMP (Linux / Apache / Mysql / Php) et Tomcat (Java) le plus répandu. Nous allons présenter ici l'installation et la configuration du serveur. Pour valider tout cela, nous mettrons en place un script ASPX minimal. Nous nous arrêterons à ce niveau, le reste dépendant de vos cours de développement.

Voici comment sont architecturés les différentes composants :

Ce qui est à noter est que le framework.NET est indépendant du serveur IIS qui peut fonctionner de façon autonome pour servir des contenus statiques en css/html. Par ailleurs, le même framework est utilisé pour développer des applications Web mais aussi des applications Windows.

2. Installation

Tout commence par l'ajout d'un rôle dans le gestionnaire de serveur :

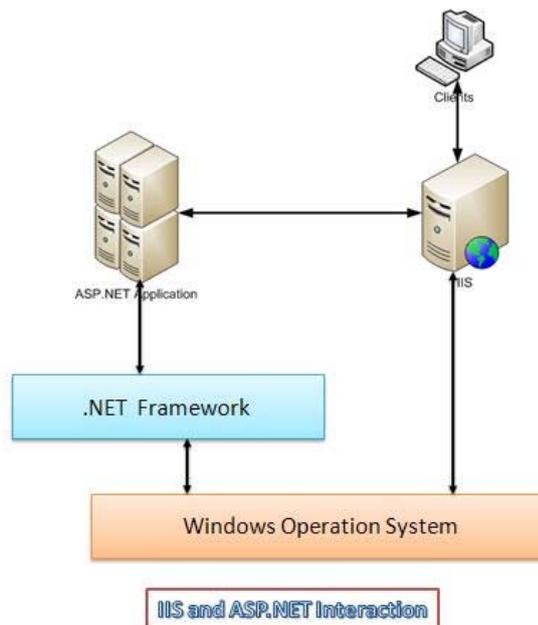


Figure 1 : articulation des composants



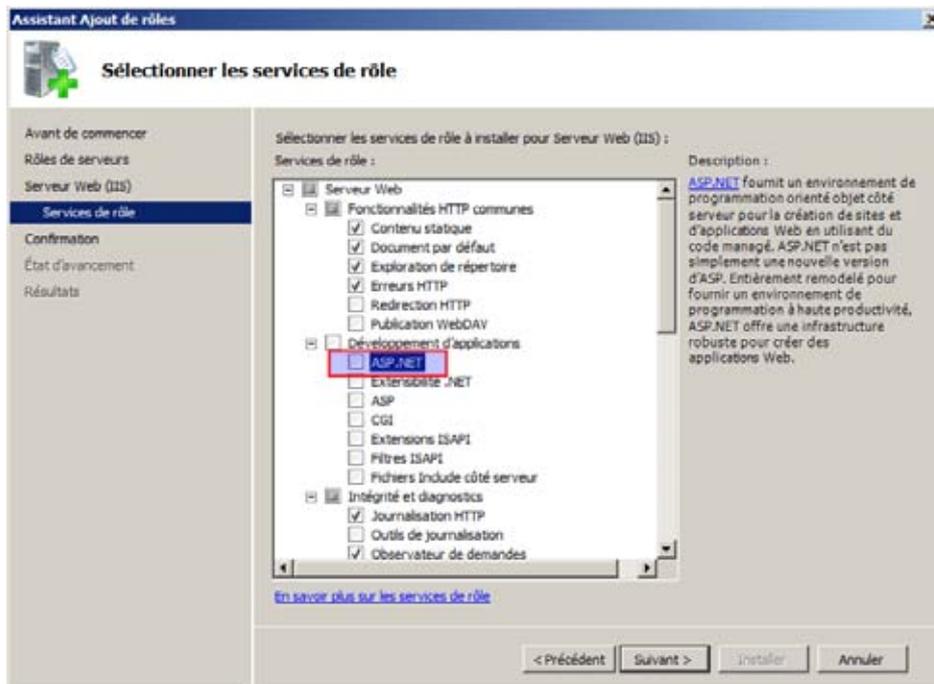
Figure 2 : ajout d'un rôle

Le rôle à choisir est bien sûr « Serveur Web (IIS) » :



Figure 3 : choix du rôle

Au fil du temps, IIS est devenu un serveur Web modulaire. Par conséquent, lors de l'installation (ou plus tard), vous pouvez choisir des fonctionnalités :



Atelier 7

Serveur d'application
web Windows

Page 79

Les choix proposés par défaut sont à mon avis correct, hormis le fait qu'il faille choisir le composant ASP.NET sans quoi IIS ne sera pas capable de traiter des applications.NET. On peut discuter de l'opportunité de conserver « Exploration de répertoire » dans la mesure où c'est généralement une erreur que le serveur affiche le contenu de l'un de ses répertoires au lieu de pages Web. À voir selon le contexte.

En cascade, des fonctionnalités supplémentaires seront installées :

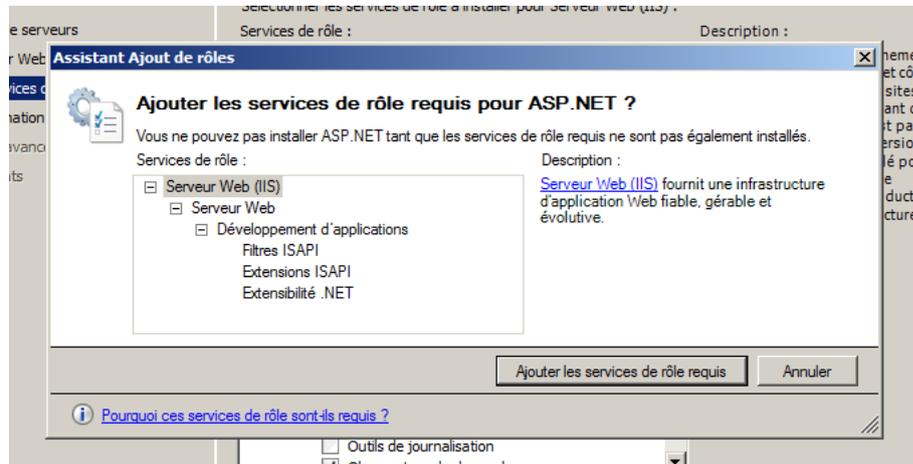


Figure 4 : fonctionnalités installées automatiquement

L'outil d'installation nous fait un petit récapitulatif de ce qui sera installé :

Atelier 7

Serveur d'application
web Windows

Page 80

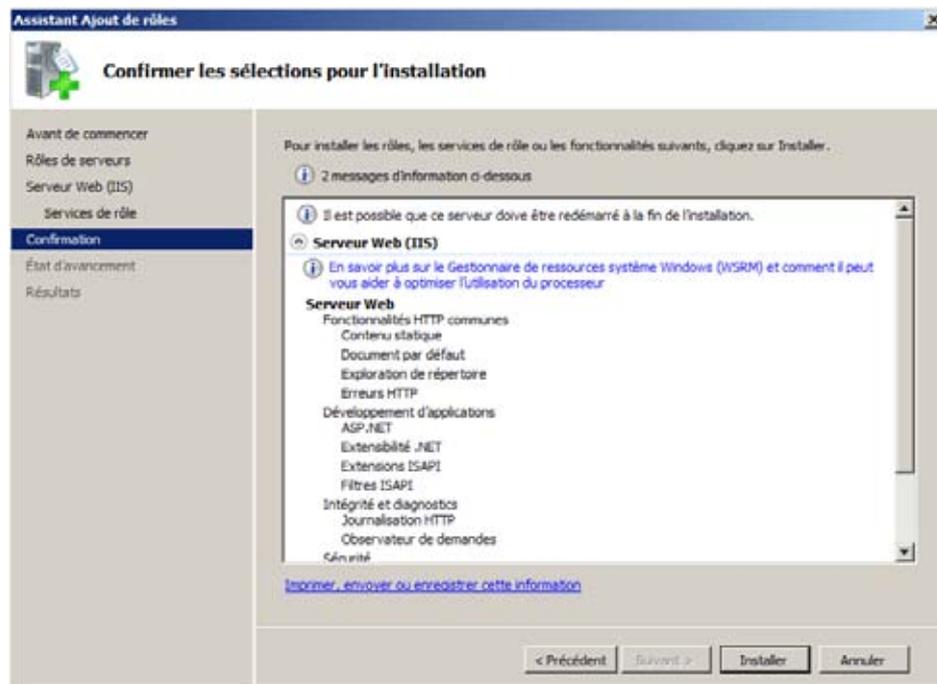


Figure 5 : récapitulatif de l'installation

Lorsque tout est terminé, vous pouvez tester localement (sur l'adresse 127.0.0.1) le bon fonctionnement de IIS avec votre navigateur préféré. Un joli écran d'accueil vous attend :



Figure 6 : accueil de IIS

3. Configuration DNS

Nous souhaitons évidemment que notre futur site web réponde à une adresse sympathique : intranet.labocned.local par exemple. Allons dans la configuration du DNS pour notre domaine labocned.local et ajoutons un alias puisque ce n'est pas une nouvelle machine sur une IP différente mais un autre nom pour la même machine :

Atelier 7

Serveur d'application web Windows

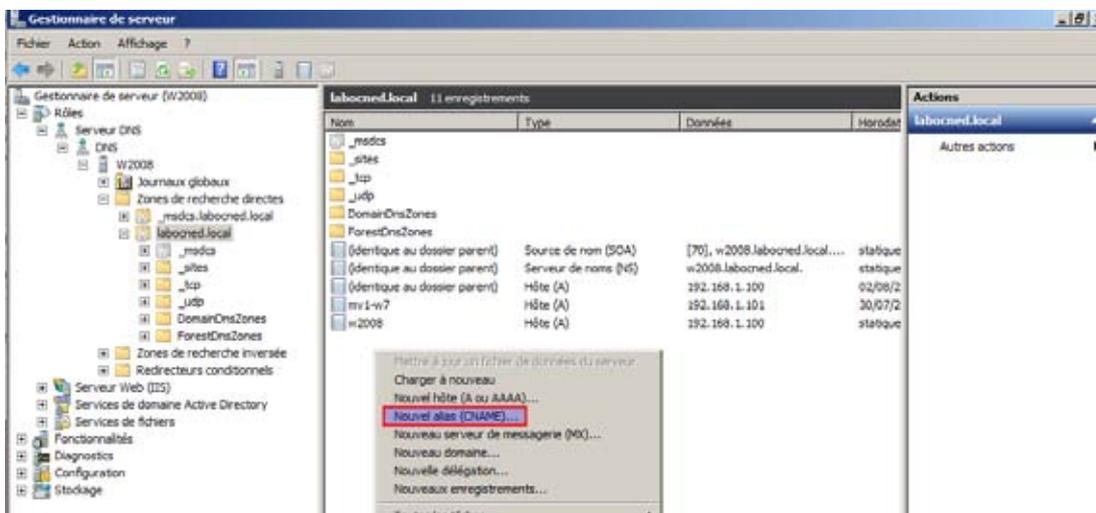


Figure 7 : déclaration d'un alias (CNAME)

Page 81

Nous saisissons le nouveau nom puis nous le faisons pointer sur la machine dont nous sommes l'alias (ici W2008, notre serveur sur l'adresse 192.168.1.100) :

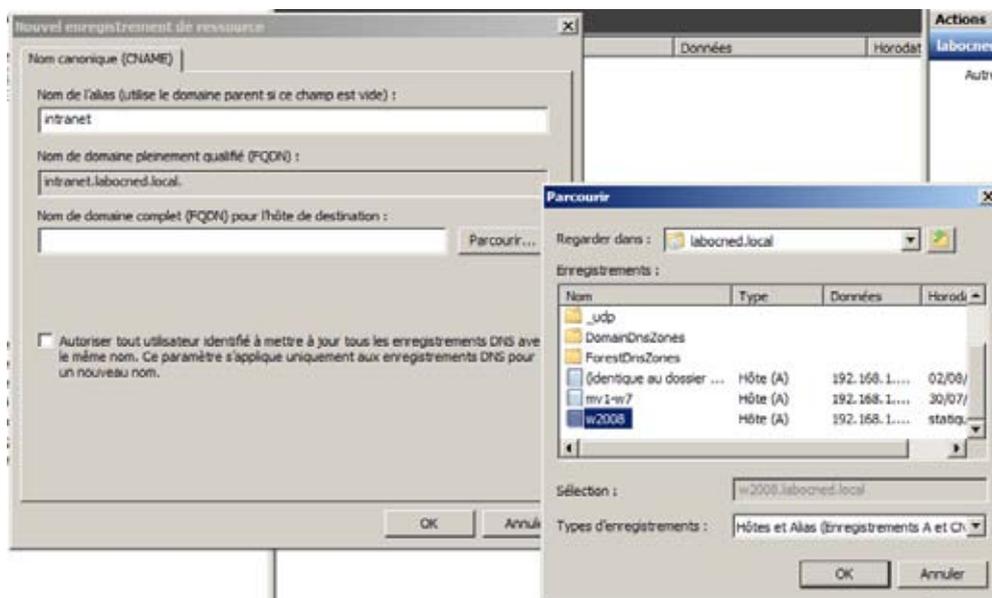


Figure 8 : définition de l'alias

Sur notre station Windows 7, nous vérifions que la résolution fonctionne à présent :

Atelier 7

Serveur d'application
web Windows

Page 82

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\eleve_211>nslookup intranet
Serveur : Unknown
Address: 192.168.1.100

Nom :      w2008.labocned.local
Address: 192.168.1.100
Aliases:  intranet.labocned.local

C:\Users\eleve_211>_
```

Figure 9 : Vérification de la résolution de nom

Parfait ! Passons à la création et à la configuration du site.

4. Création d'un nouveau site

Un nouvel élément a été ajouté à notre « gestionnaire de serveur », il s'agit du gestionnaire des services Internet (IIS). C'est ici que tout se passe concernant les sites web :

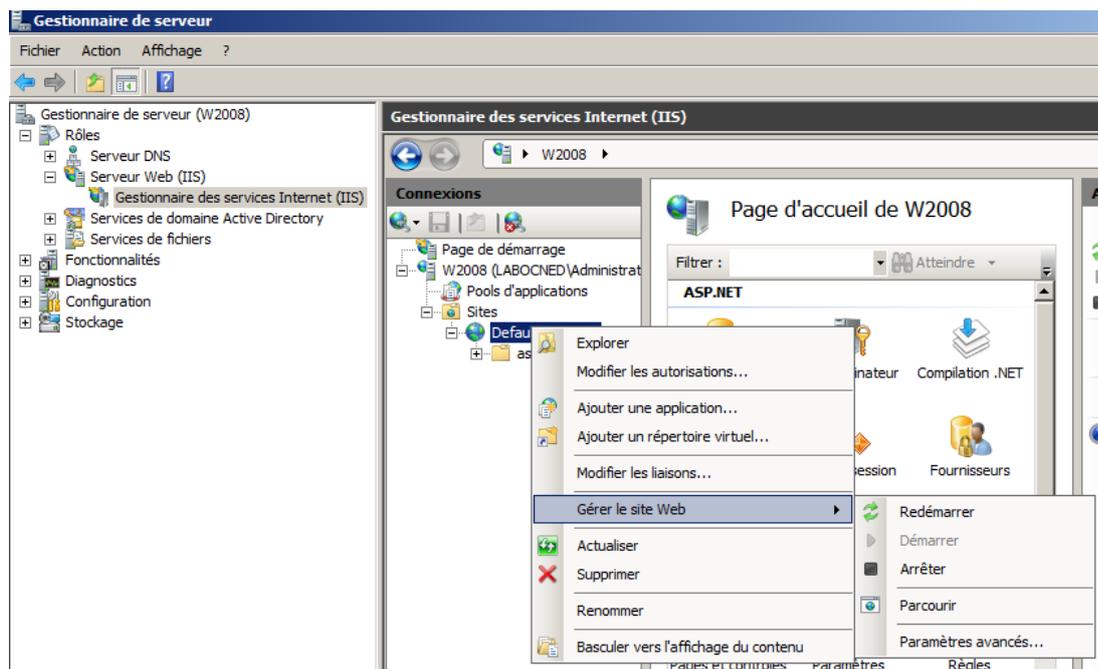


Figure 10 : gestionnaire des services Internet

Dans la partie « Sites », vous voyez le « Default Web Site » qui contient l'image d'accueil IIS que nous avons vu tout à l'heure. Ce site doit être arrêté ou tout simplement supprimé.

Créez sur disque un répertoire qui accueillera les fichiers du site Web. Il n'y a pas de recommandations particulières mais c'est préférable de le mettre dans une autre partition que le système (avec VirtualBox vous pouvez facilement ajouter des disques quand une machine virtuelle est éteinte).

Dans ce répertoire, vous saisissez le fichier hello.aspx (l'extension ASPX est très importante et indique à IIS qu'il s'agit d'une page ASP.NET) suivant :

```

<%@ Page Language="VB" %>
<%
HelloWorld.Text = "Hello World!"
%>

<html>
<head>
<title>ASP.NET Hello World</title>
</head>
<body bgcolor="#FFFFFF">
<p><asp:label id="HelloWorld" runat="server" /></p>
</body>
</html>

```

Les instructions présentées en gras ne sont pas des instructions HTML mais bien du code ASP.NET.

Revenons dans le gestionnaire IIS, puis cliquons droit sur « Sites » puis « ajouter un site Web... » :

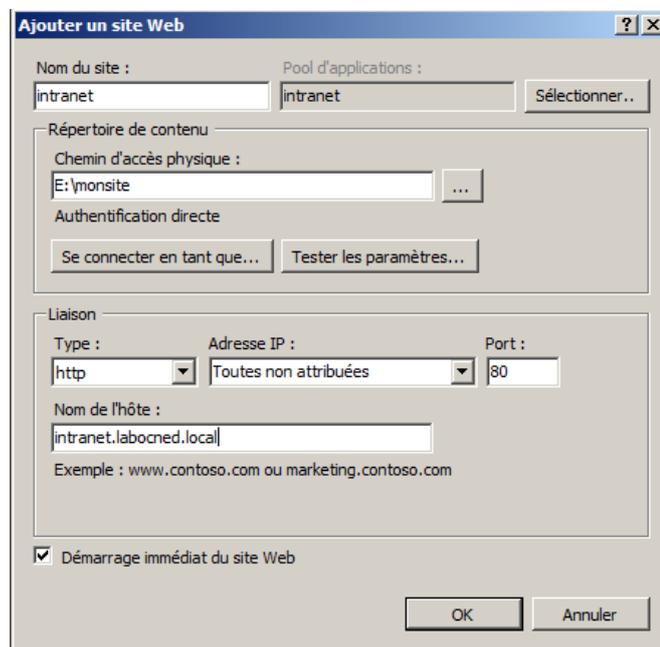


Figure 11 : Création d'un site web

Atelier 7

Les informations à saisir sont le nom du site (ce qu'on veut mais quelque chose de clair). Vous indiquez le chemin du répertoire que vous venez de créer. Dans la partie « liaison » vous laissez http et port 80. Par contre, il est indispensable de saisir le nom FQDN (donc complètement qualifié) du serveur (l'adresse qui sera tapée dans la barre d'adresse du navigateur).

Maintenant, dans notre navigateur Windows 7 :

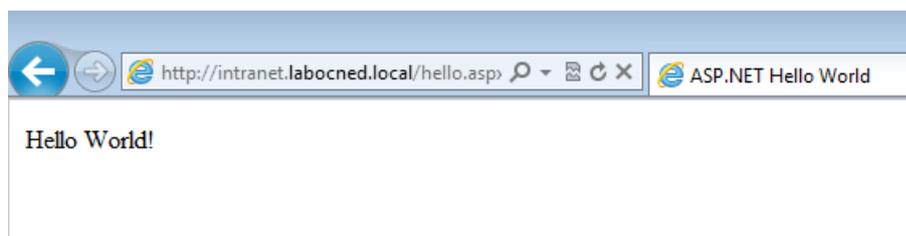


Figure 12 : Accès au site à partir d'un navigateur

Et voilà !

5. Journaux

Des informations importantes qui vous aideront à résoudre des problèmes de configuration, des erreurs d'applications ou des anomalies se trouvent dans les fichiers journaux de IIS. Ceux-ci se trouvent par défaut c:\inetpub\logs\LogFiles :

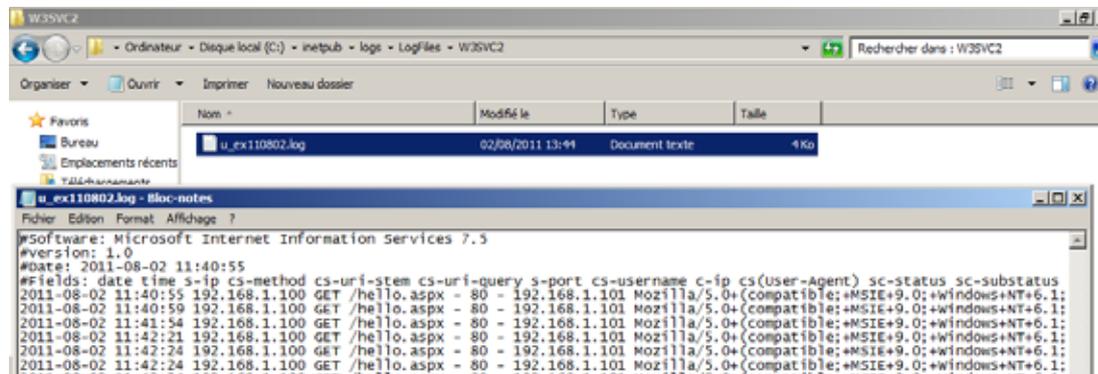


Figure 13 : Journaux IIS

Ces fichiers contiennent des informations précieuses :

- quand : date et heure de la requête HTTP
- qui : adresse IP du client
- quoi : quelle URL a été demandée
- avec quoi : référence du navigateur
- résultat : le code http résultat (200 = ok, 404 = non trouvé, 403 = interdit, etc.)

Atelier 7

Serveur d'application
web Windows

6. Exécution

Pour des raisons de sécurité et de bon fonctionnement, les sites webs sont exécutés dans des pools d'application. Ceci peut être observé dans le gestionnaire des tâches. Par exemple, nous voyons un site qui est traité par un « IIS Worker Process » (processus qui répond aux requêtes http) s'exécutant sous un compte d'utilisateur créé pour l'occasion (ici, intranet en référence au nom du site) :

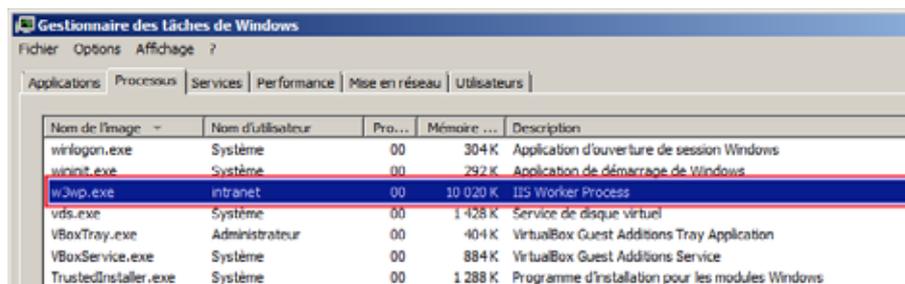


Figure 14 : gestionnaire de tâches

Ceci est configurable dans la partie « pools d'application » du gestionnaire des services IIS. Par exemple, si l'on observe les paramètres mis par défaut lors de la création du site :



Figure 15 : pool d'application

Les pools d'application sont des environnements étanches, isolés les uns des autres. Il y a autant de IIS Worker Process que de pool. Un pool peut contenir plusieurs sites ou applications :

Atelier 7

Serveur d'application web Windows

Page 86

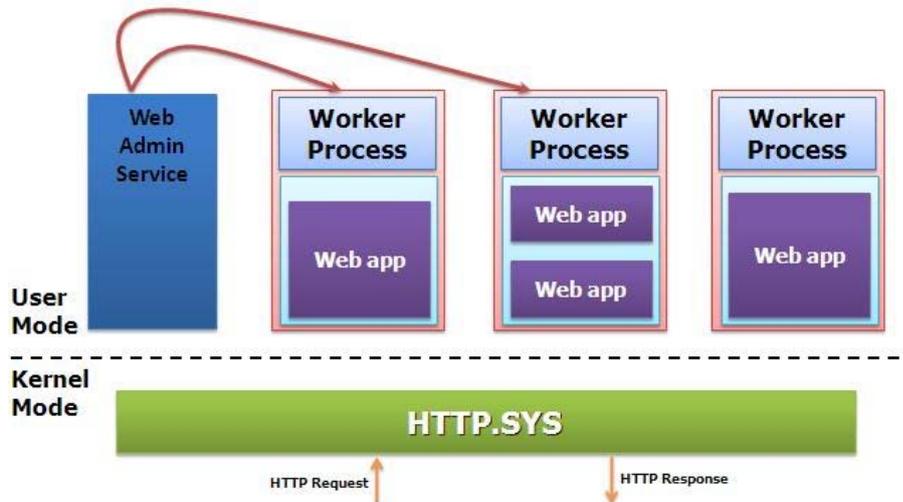


Figure 16 : architecture des pools d'application

Chaque pool vit donc sa vie sans interférer avec celle des autres. Un pool ou un processus IIS planté ou compromis n'affecte pas les autres. Des paramètres peuvent être gérés pour chaque pool, en particulier la fréquence à laquelle celui-ci redémarre (de façon à faire le ménage au bout d'un certains temps). Ceci est transparent pour l'utilisateur qui malgré un temps d'attente un peu plus important ne se rend compte de rien. Les données de sa session étant conservés.

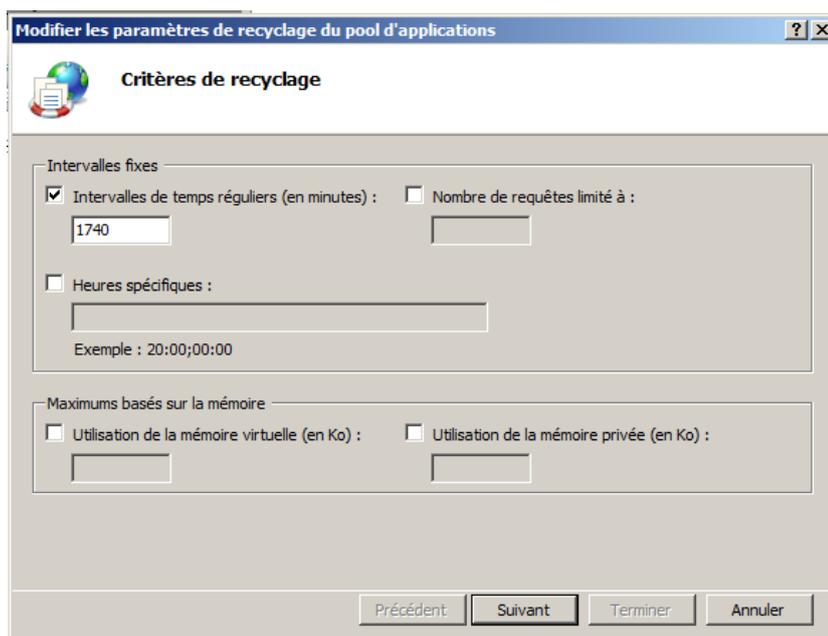


Figure 17 : recyclage des pools d'application

Les paramètres par défaut proposés par Microsoft sont corrects mais dans certains cas, il peut être important de les modifier.

7. Sécurisation du site

Comme vous le savez, par défaut les données circulent en clair sur le réseau local ou Internet. Une capture de trame avec un outil comme Wireshark peut révéler des informations confidentielles. La solution habituelle consiste à passer du http au https, ce qui va permettre de « brouiller » les communications afin que les paquets de données ne soient pas lisibles.

Le principe de chiffrement repose sur la notion de certificat SSL que doit posséder le serveur. Ce certificat contient deux clés (chiffrement asymétrique) utilisée pour chiffrer et déchiffrer les messages.

Pour mettre en oeuvre un certificat, il faut cliquer sur le serveur Web puis sur « Certificats de serveur » :

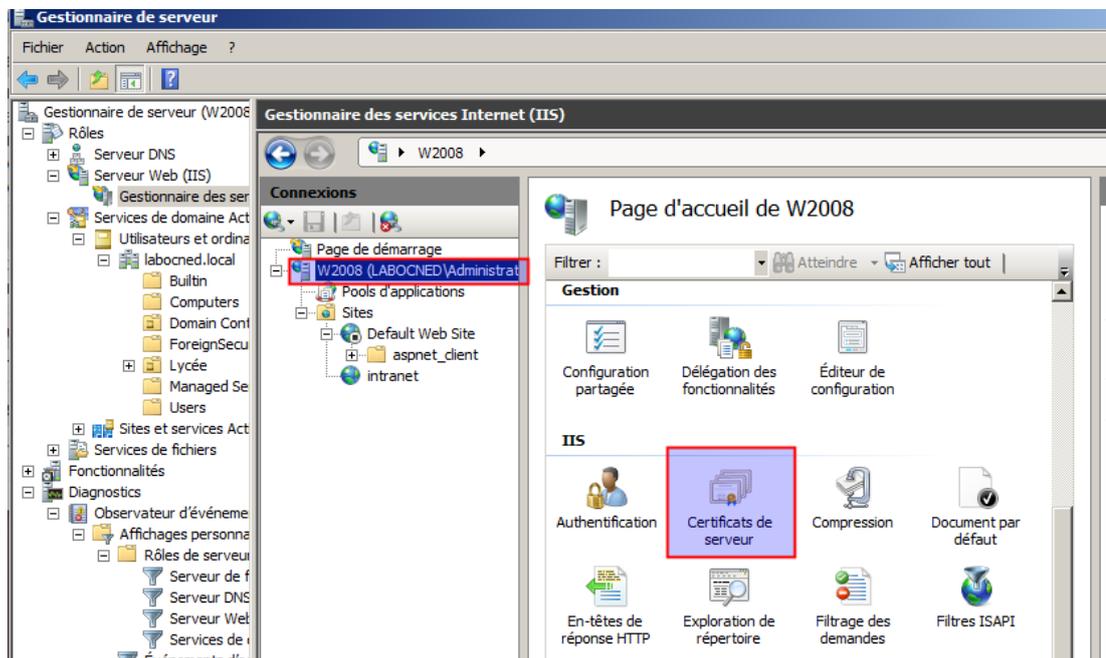


Figure 18 : création d'un certificat de serveur

Atelier 7

Serveur d'application
web Windows

Page 88

Observez l'encadré ci-dessous. Nous pouvons voir qu'il y a différentes catégories de certificats.

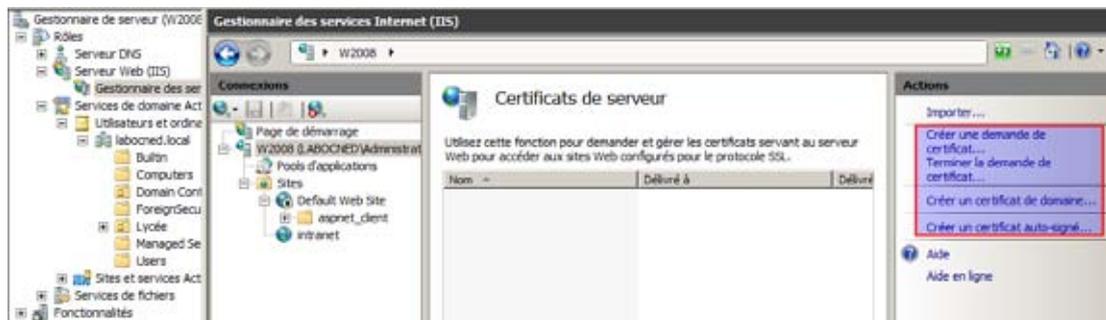


Figure 19 : Catégories de certificats

Un vrai certificat reconnu sur Internet est généré par une autorité de certification indépendante (comme Thawte) connue de votre navigateur préféré. La génération se fait en trois temps :

1. « Créer une demande de certificat » : cette demande produit un fichier qui contient toutes les informations nécessaires (en particulier la société demandeuse et le contact technique) et qui est envoyé à l'autorité de certification.
2. L'autorité reçoit la demande, effectue des vérifications (quelqu'un téléphone dans la société pour vérifier l'identité du contact technique) puis un certificat unique est généré et envoyé au demandeur.
3. « Terminer la demande de certificat » : IIS se souvient qu'une demande a été faite. Il faut indiquer le fichier du certificat qui sera alors intégré dans la base de IIS.

Nous ne pouvons pas dans le cadre de ces ateliers du CNED réaliser cette manipulation ! Mais vous la ferez très probablement en entreprise. Nous nous cantonnons au troisième

cas « Créer un certificat auto-signé ». La deuxième possibilité concerne aussi les certificats internes : il est possible avec Windows de se gérer sa propre autorité de certification mais ceci ne sera pas mis en oeuvre dans ces ateliers.

Choisissez donc « Créer un certificat auto-signé », il suffit de lui donner un nom. Celui apparaîtra ensuite dans la liste :

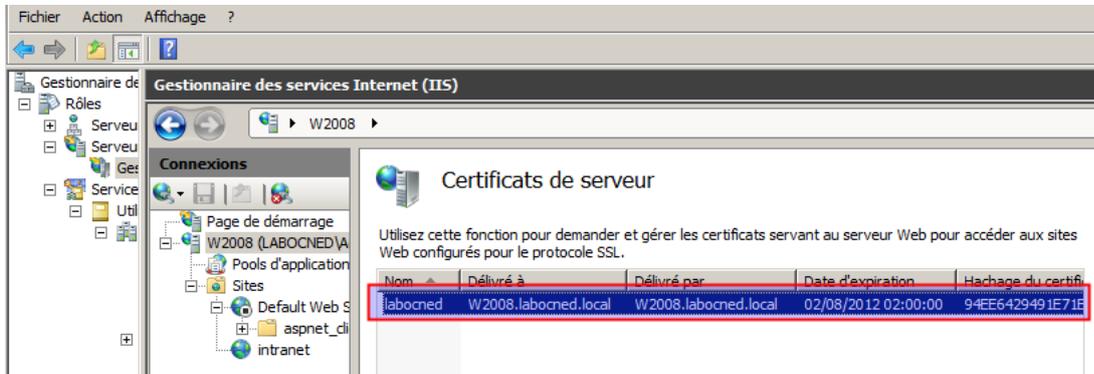


Figure 20 : certificat auto-signé généré

Notons que les certificats ont toujours une date d'expiration. Ce certificat est dans la base de données de IIS mais il n'est pas affecté au site. Cliquez sur votre site web puis sur « Liaisons » dans le menu de droite :

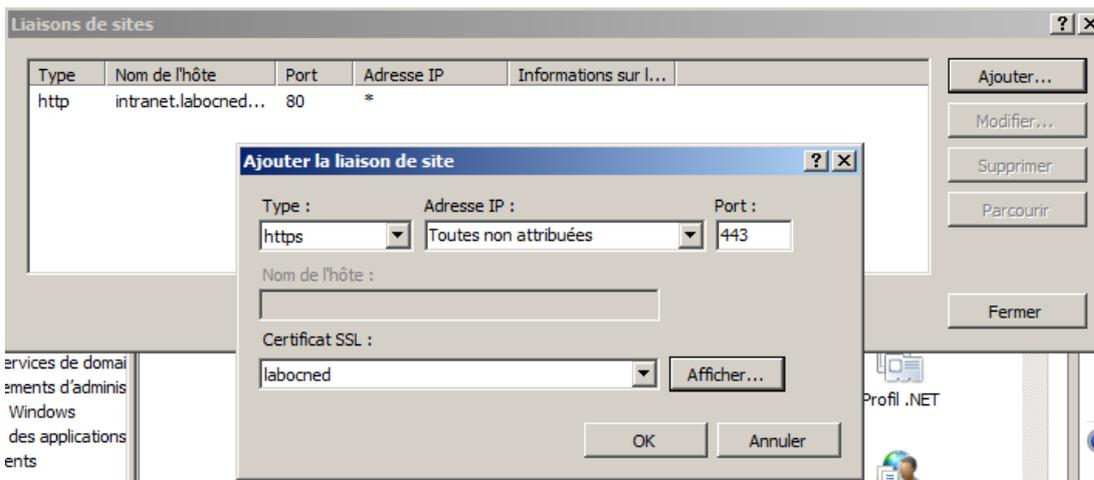


Figure 21 : liaison site/certificat

Vous indiquez https (le numéro de port passera automatiquement à 443) et vous choisissez votre certificat dans la liste.

Important : l'autre liaison (celle en http) doit être supprimée ! Sinon, vous aurez travaillé pour rien !

Maintenant, si nous essayons d'accéder à la page de toute à l'heure en utilisant le protocole https :

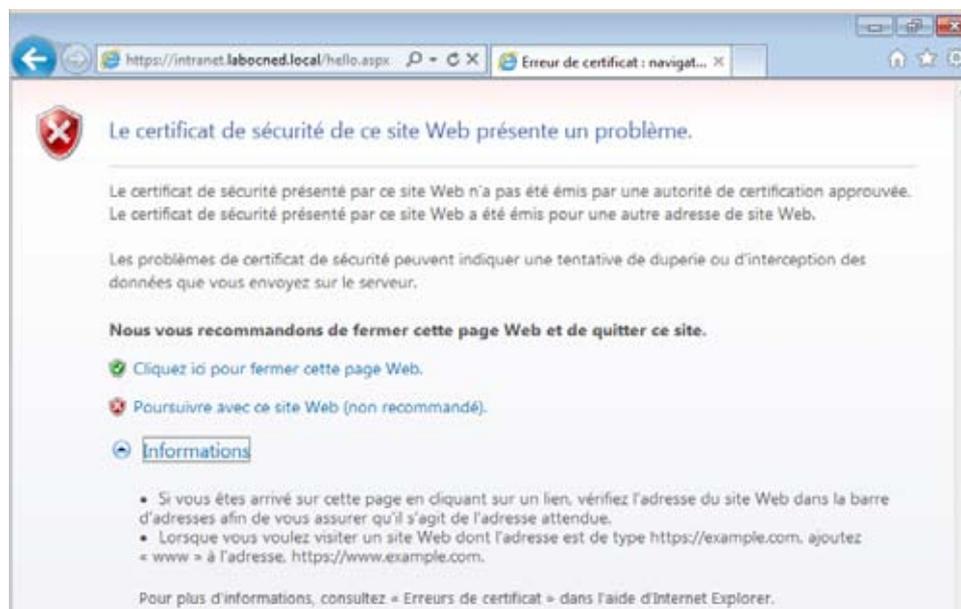


Figure 22 : Erreur d'accès

Notre certificat auto-signé n'a aucune valeur pour notre navigateur. Si chacun pouvait se générer ses certificats sur Internet, n'importe qui pourrait se faire passer pour la Banque de France ou Microsoft. Si vous ignorez le message, vous pourrez tout de même accéder au site :

Atelier 7

Serveur d'application
web Windows

Page 90

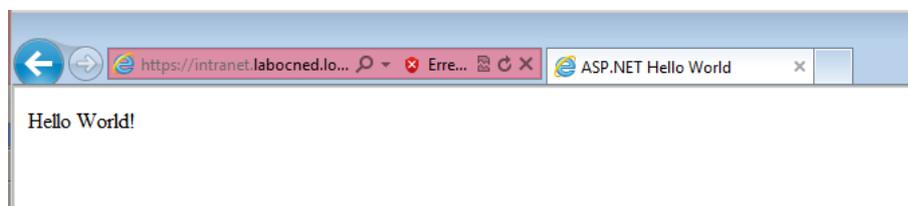


Figure 23 : accès au site malgré une erreur SSL

Dans la réalité, les certificats auto-signés sont utilisés pour effectuer du développement ou pour un accès du personnel à des sites internes. Notez bien que ce n'est pas parce qu'il y a une erreur que la communication n'est pas chiffrée. C'est juste l'identité du site qui ne peut être garantie.

À retenir

Serveur web est un rôle à installer. IIS et .NET sont deux composants indépendants qu'il faut installer tous les deux.

Un site Web possède un nom FQDN qui doit figurer dans le serveur DNS pour qu'il soit connu des clients.

Par défaut, un site s'exécute dans un pool d'application créé automatiquement. Un pool est un environnement d'exécution indépendant et représenté par un processus w3wp.exe. Un pool peut contenir plusieurs sites.

Les journaux gérés par IIS tracent toutes les requêtes HTTP reçues par le serveur et contiennent de nombreuses informations (utilisées par exemple pour les outils de statistiques d'usage des sites).

La mise en place du https nécessite de générer un certificat pour le site concerné. IIS permet de générer très facilement des certificats auto-signés pour des sites internes. Sinon, il faut générer une demande à envoyer à une autorité indépendante qui après vérification renverra un certificat reconnu sur Internet.

Si vous voulez approfondir

Capturer des trames avec Wireshark pour mettre en évidence les différences entre http et https.

Atelier 8

SQL Server 2008 R2

► Durée approximative de cet atelier : 3 heures

► Objectif

Installer, configurer, mettre à disposition et sauvegarder un serveur SQL.

► Durée approximative de cet atelier

Notre serveur Windows 2008 R2 SP1 et une machine sous Windows 7 pro.

► Considérations techniques

À l'instar de Windows Server, SQL Server 2008 R2 est proposé dans plusieurs versions avec chacune des limites matérielles (mémoire ou nombre de CPU supportés) et de fonctionnalités. Dans cet atelier, une version standard ou entreprise est suffisante.

► Contenu

1. Introduction	94
2. Architecture serveur	94
3. Installation	95
4. Configuration.....	99
5. Création d'une base de données.....	101
6. Création d'une application	105
7. Sauvegardes.....	107

Atelier 8

SQL Server 2008 R2

Page 93

1. Introduction

Le SGBD ou système de gestion de base de données est un élément clé d'une application Web. De sa robustesse et de sa gestion de la montée en charge lorsque les utilisateurs se déchaînent dépend la fiabilité du site. SQL Server avec Oracle pour la partie propriétaire ou MySQL et PostgreSQL du côté libre sont les 4 grands standards que l'on retrouve derrière la majorité des sites Web.

Dans cet atelier, nous présentons SQL Server 2008 R2 Entreprise que vous pourrez récupérer sur le site MSDNAA du CNED. Nous abordons ici la partie système et serveur. Ce qui relève de la conception et de l'exploitation des données est présenté dans d'autres modules.

Dans un premier temps, nous discuterons de l'architecture matérielle du serveur sur lequel sera installé le logiciel. Puis nous présenterons les principales options d'installation et de configuration. Nous créerons une base de données et un script ASPX de test afin de valider l'installation. Enfin, nous présenterons la sauvegarde des données.

2. Architecture serveur

Comme nous l'avons dit en introduction, la partie SGBD d'une application Web est cruciale et l'expérience montre que ce serveur est souvent plus sollicité en termes de CPU et d'accès disque que la partie applicative qui est finalement relativement statique. Nous donnons ici quelques conseils issus du terrain mais la plupart des choix d'architecture sont dictés par les prévisions de charge du ou des serveurs en prenant, bien sûr, une marge de manoeuvre.

Pour l'hébergement d'un site web, une pratique courante consiste à utiliser deux serveurs : un pour la partie applicative, l'autre pour la partie données.

Concernant l'architecture du serveur de données à proprement parler, SQL Server a été développé pour supporter une architecture multicore et multiCPU (jusqu'à 256 processeurs logiques) et plusieurs To de mémoire. Notez que certaines réserves concernent l'hyperthreading et qu'il est conseillé de le désactiver dans le BIOS du serveur.

Un SGBD étant par définition conçu pour le stockage des données, un système de disque au minimum en RAID 5 et en technologie SAS est à prévoir. Le RAID 5 est efficace pour les opérations de lecture/écriture car il travaille sur plusieurs disques physiques simultanément et intègre, bien sûr, la tolérance de panne.

L'autre élément à connaître, est qu'en fait une base de données est constituée de deux catégories de fichiers :

- les données proprement dites ;
- les journaux des transactions : ce sont des enregistrements qui permettent de garantir l'intégrité de la base en cas de coupure brutale du serveur.

Il est donc souvent préconisé de prévoir deux systèmes de disques indépendants de façon à ce que les lectures/écritures de données ou de journal puissent se faire en parallèle. Par exemple : un RAID 1 sur un contrôleur pour les journaux, un RAID 5 sur un autre contrôleur pour les données.

Attaquons l'installation !

3. Installation

Le programme d'installation vérifie la compatibilité de votre environnement :

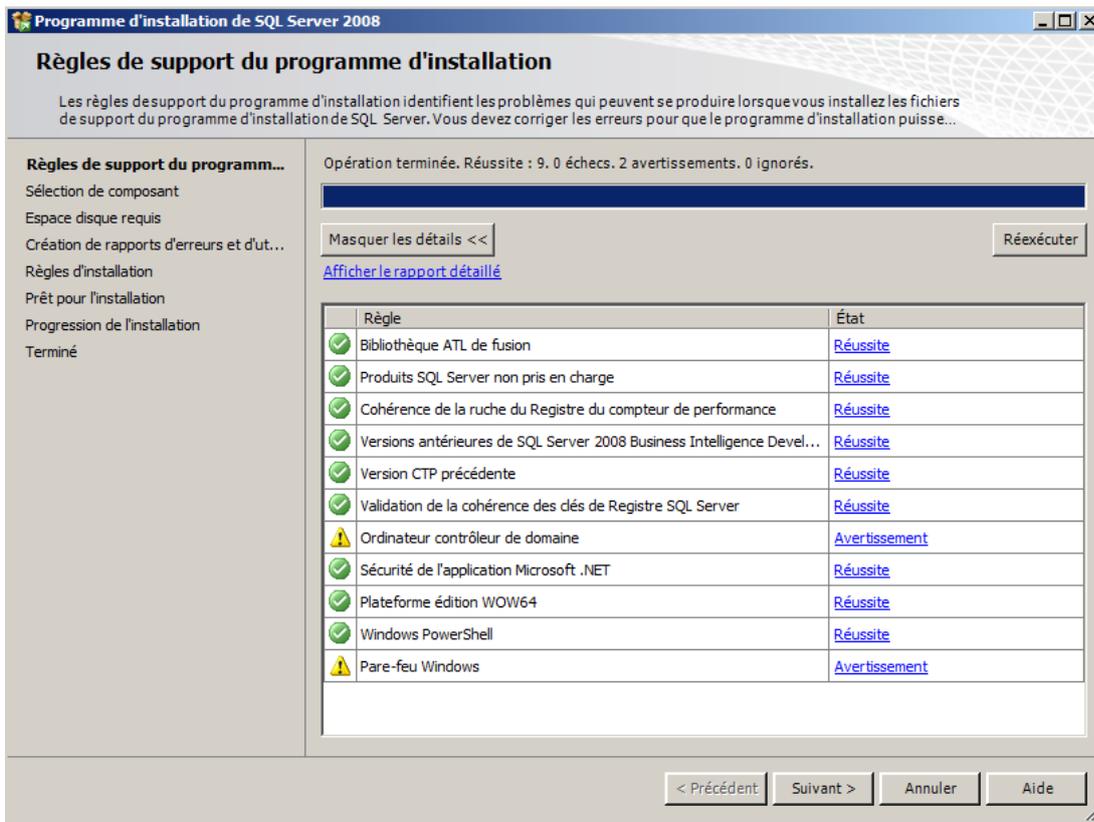


Figure 1 : vérification de la compatibilité

Atelier 8

SQL Server 2008 R2

Page 95

Pour des raisons de sécurité, il vaut mieux éviter de l'installer sur un contrôleur de domaine. Mais des fois, on n'a pas le choix ! Dans le cadre d'une application Web, l'utilisation d'un domaine est inutile, donc la question ne se posera pas. Il faudra aussi vérifier le pare-feu Windows qui dans le cas d'une utilisation en réseau pourrait bloquer les accès. Dans notre atelier, le problème ne se posera pas puisque application et données seront sur le même serveur.

L'installation propose de nombreux composants :

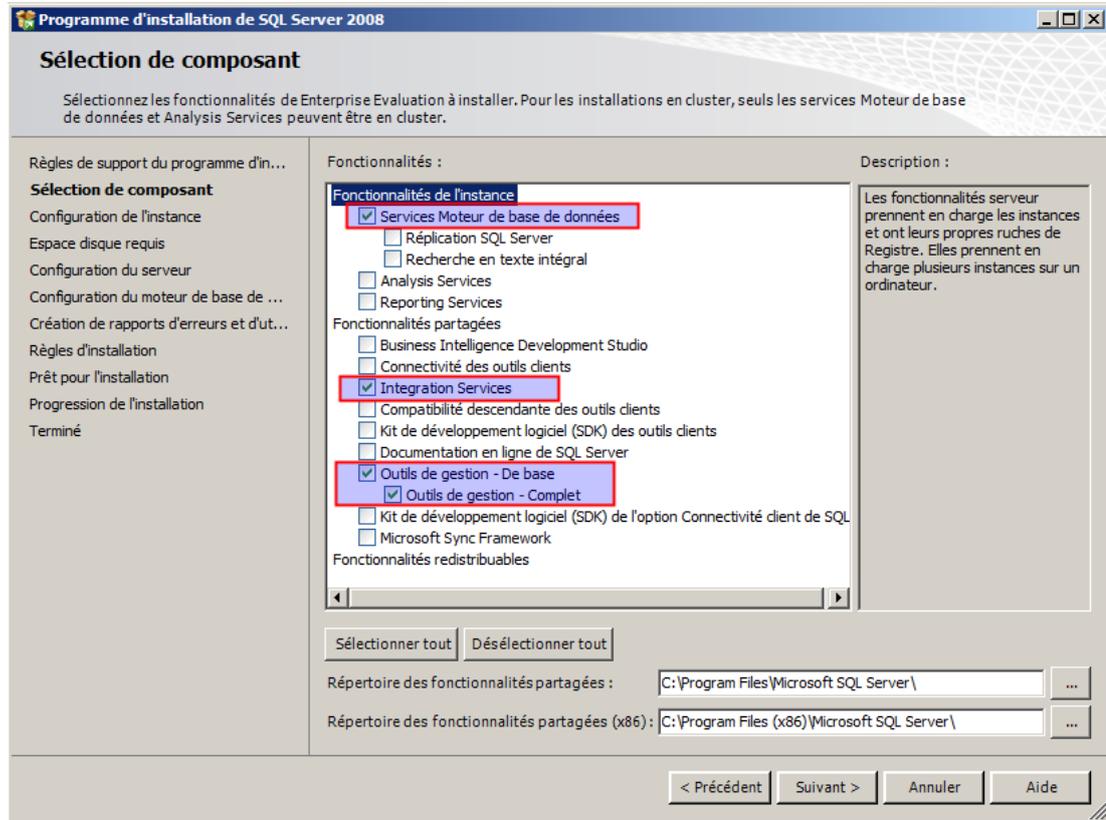


Figure 2 : choix des composants

Atelier 8

SQL Server 2008 R2

Page 96

Dans la grande majorité des situations, vous aurez besoin de 3 composants :

- le service de moteur de base de données : sans ça nous ne pourrions pas faire grand chose !
- intégration services : qui nous sera indispensable pour les sauvegardes planifiées au travers du réseau ;
- outils de gestion : en fait SQL Server Management Studio qui est l'interface graphique d'administration.

L'écran suivant vous demande de configurer l'instance. En effet, sur un même serveur physique peuvent s'exécuter plusieurs instances de SQL Server (plusieurs serveurs logiciels). C'est le cas si vous utilisez des applications différentes qui utilisent toutes SQL Server. Il est préférable de créer plusieurs instances afin de ne pas mettre tous les oeufs dans le même panier. Ici, nous conservons le choix par défaut qui est pour une instance unique.

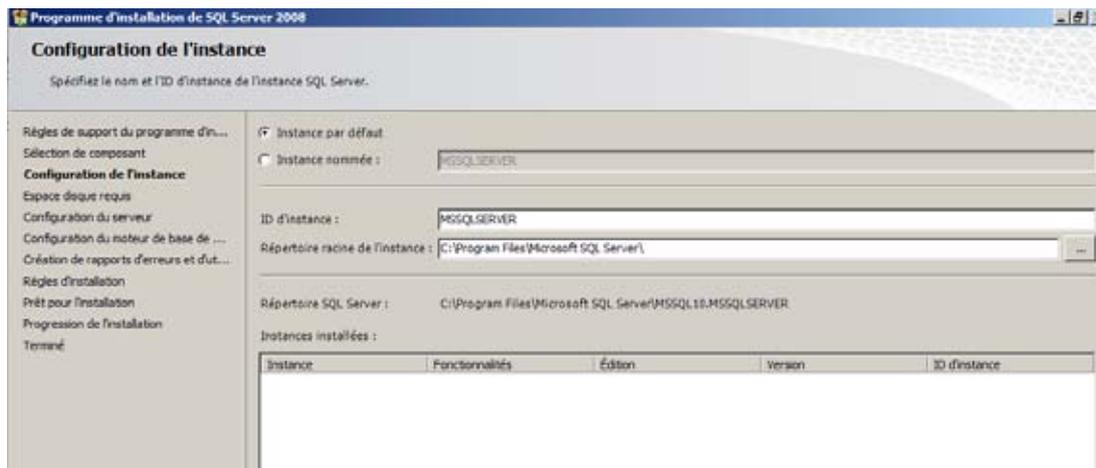


Figure 3 : Choix de l'instance

L'écran suivant est important et permet de choisir sous quels comptes vont s'exécuter les différents processus de SQL Server. Pour l'instant, nous mettons partout l'utilisateur « Système » mais nous y reviendrons lorsque nous parlerons de la sauvegarde. Veillez bien à ce que le type de démarrage soit « automatique » :

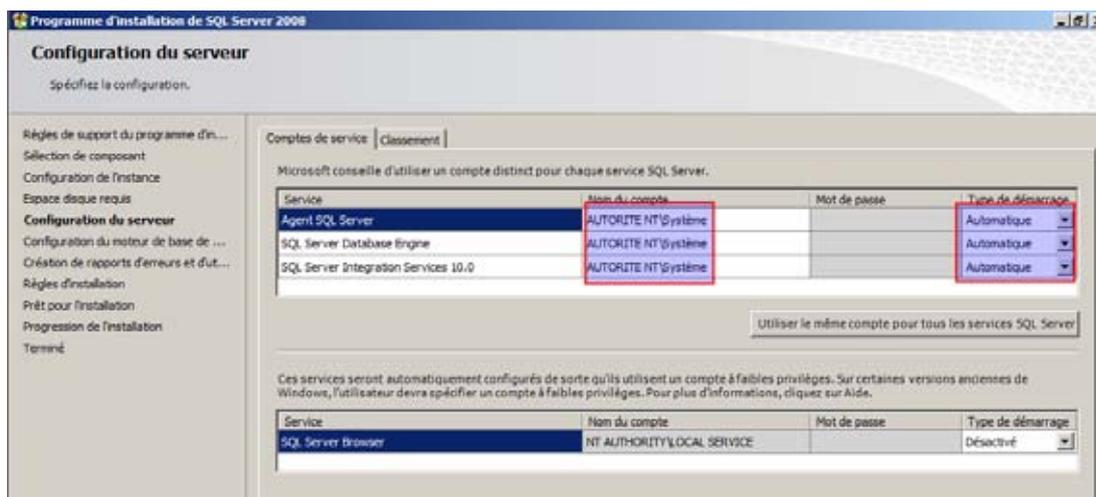


Figure 4 : Choix des utilisateurs

Ensuite, vient la problématique de la sécurité. SQL Server étant un outil Microsoft, il est logique qu'il s'intègre à Windows (Mode d'authentification Windows). Tous les administrateurs Windows sont administrateurs SQL Server. Néanmoins, nous conseillons de prendre le mode mixte qui offre plus de souplesse. Il faudra donner un mot de passe pour l'utilisateur « sa » (system administrator) qui est l'administrateur par défaut.

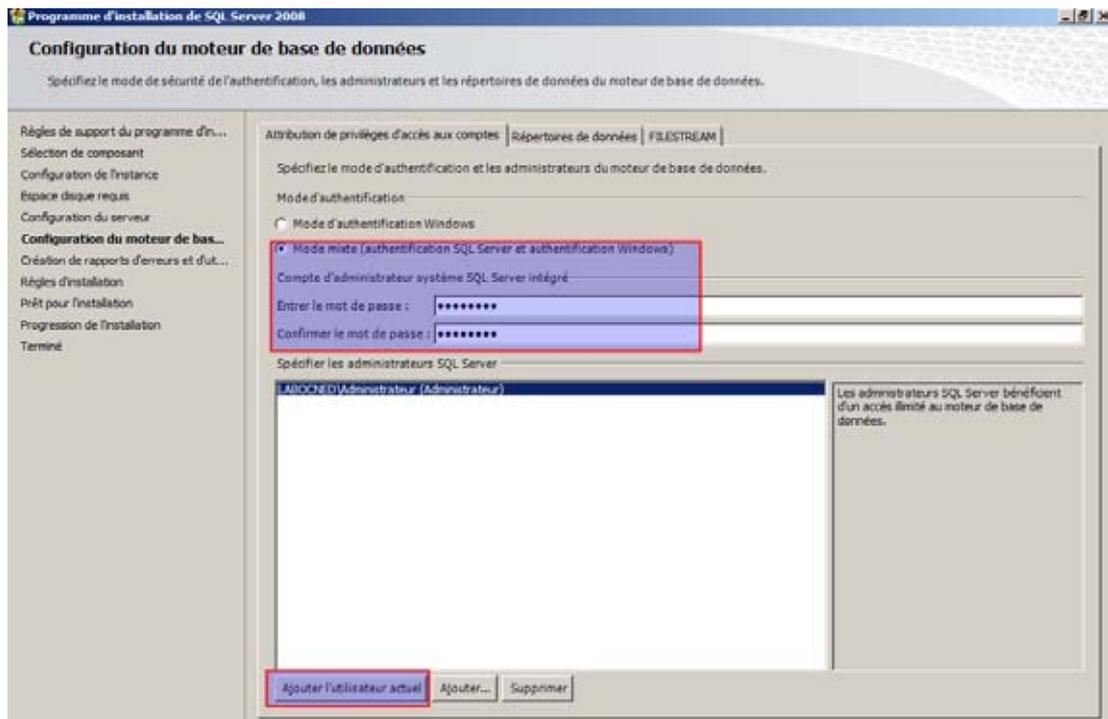


Figure 5 : Choix du mode d'authentification

Les autres écrans ne présentent que peu d'intérêt, la fin de l'installation fera le bilan suivant :

Atelier 8

SQL Server 2008 R2

Page 98

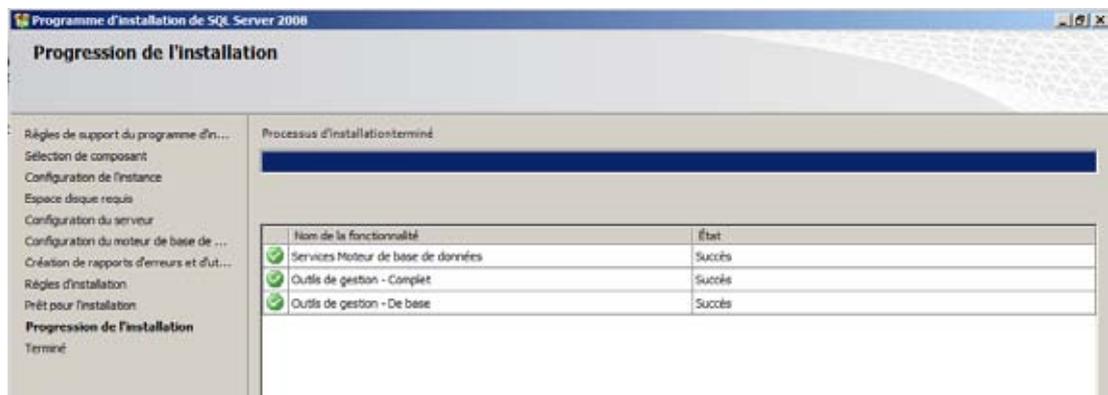


Figure 6 : Fin de l'installation

4. Configuration

Dans le menu « démarrer » puis « SQL Server », vous trouverez un outil de configuration qu'il faut connaître dans le cas d'une utilisation de SQL Server au travers du réseau. En effet, par défaut, pour des raisons de sécurité, les protocoles réseau sont désactivés :

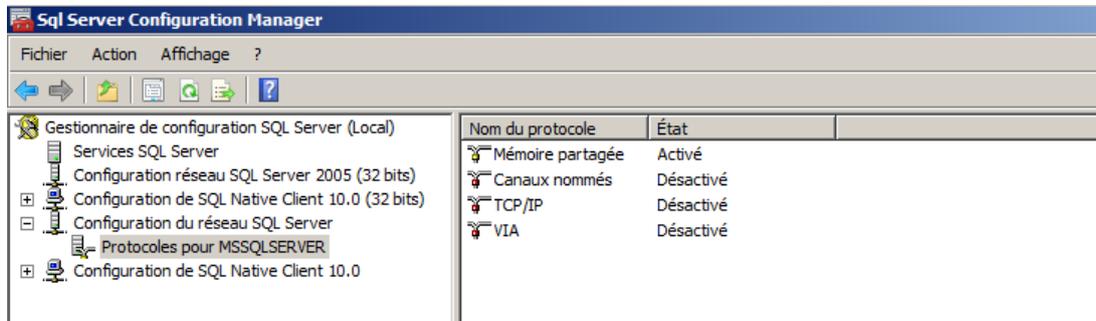


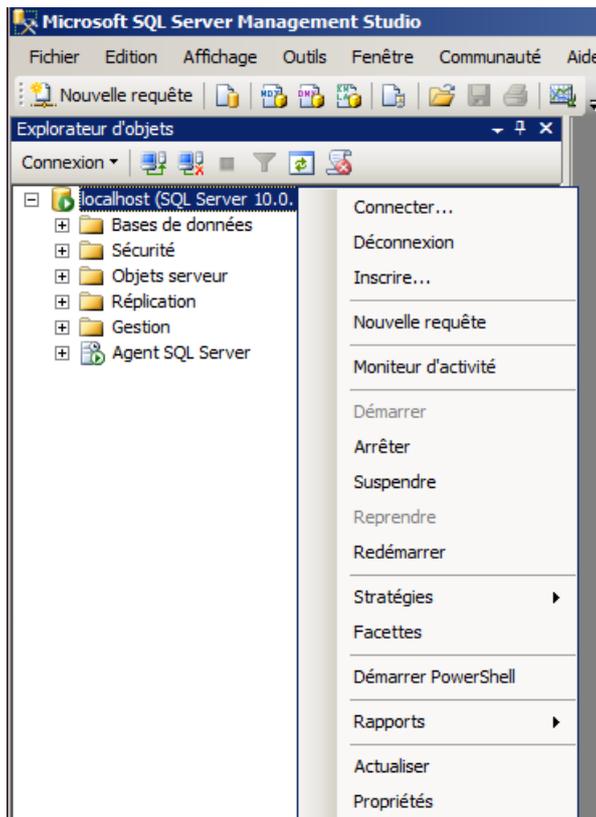
Figure 7 : Configuration réseau

Lançons maintenant le Management Studio. Pour se connecter, vous pouvez utiliser l'authentification Windows ou l'authentification SQL Server :



Figure 8 : Connexion à SQL Server

L'utilisateur à prendre pour l'authentification SQL Server est « sa » avec le mot de passe saisi lors de l'installation.



En cliquant droit sur le serveur, vous trouvez le menu de gestion du serveur. Des éléments de configuration sont disponibles dans « propriétés ». Ils apparaissent désactivés car vous ne pouvez pas les changer pendant que SQL Server fonctionne. Il faut d'abord l'arrêter.

Atelier 8

SQL Server 2008 R2

Page 100

Un élément important concerne la gestion des processeurs. Vous pouvez choisir sur quel(s) processeur(s) le logiciel s'exécutera et aussi « renforcer la priorité ». Ceci est utile sur un serveur dont le seul rôle est d'être serveur de base de données, sinon laissez décoché.

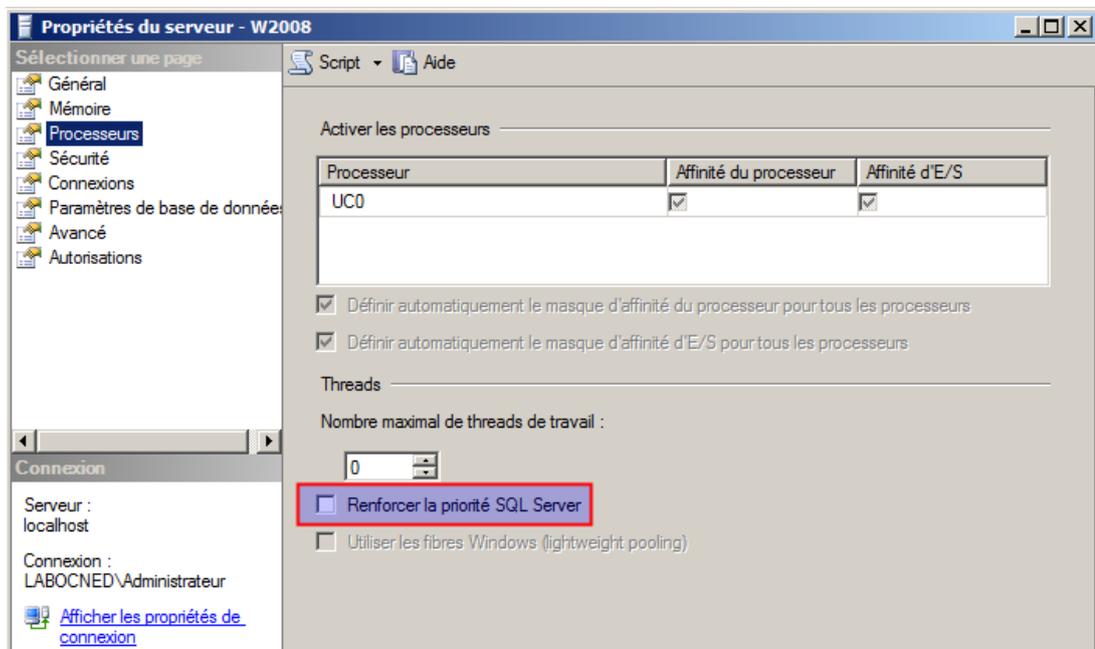


Figure 9 : Gestion du processeur

5. Création d'une base de données

Nous créons une base de données simplissime dans l'unique objectif de réaliser des tests :

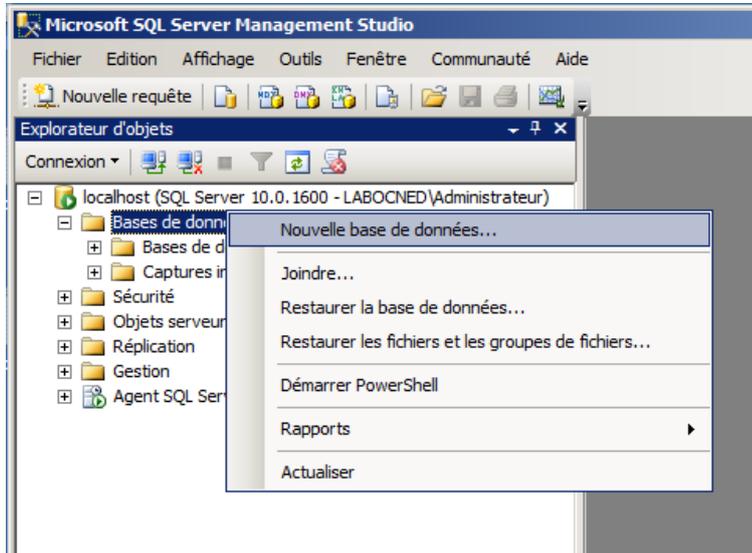


Figure 10 : Création d'une base

Il faudra lui donner un nom (cned par exemple). Puis nous créons une table dans cette base de données :

nom : matable

colonnes : id en clé primaire, identité (auto incrément) et label en nchar(100) :

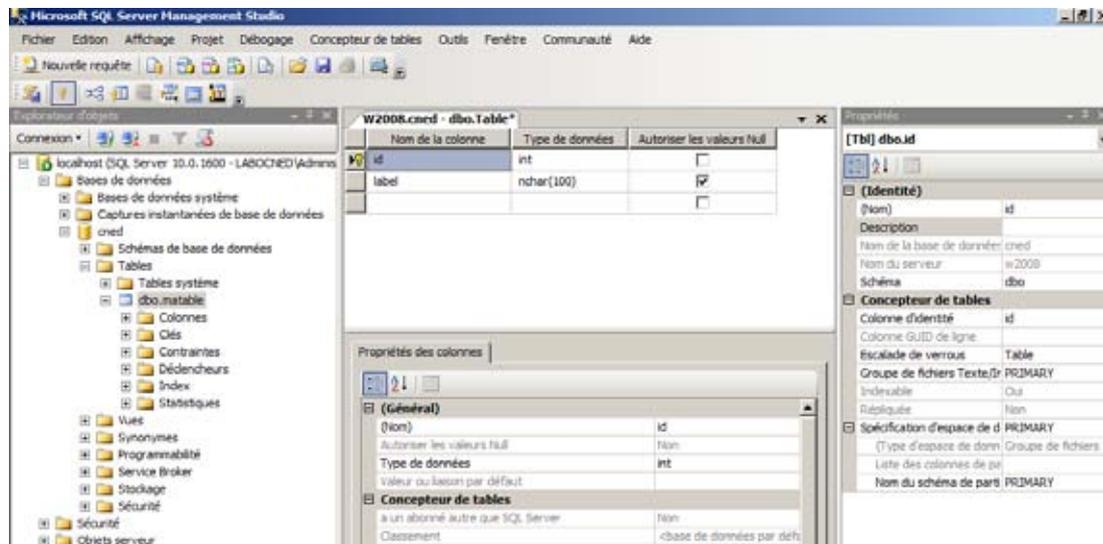


Figure 11 : création d'une table

Ensuite, vous sélectionnez « matable » et faites « modifier les 200 lignes du haut » pour saisir quelques données à l'intérieur :

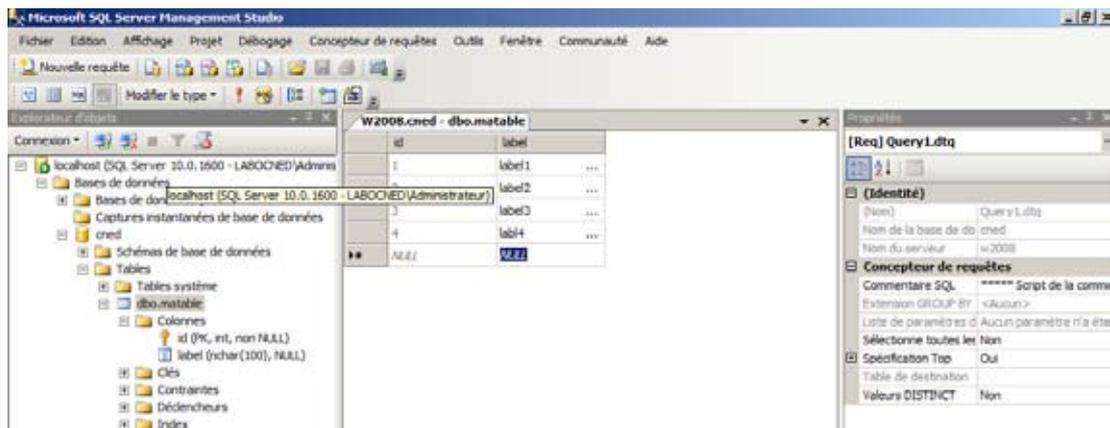


Figure 12 : Quelques données

Enfin, nous créons une connexion qui sera utilisée par l'application.NET pour se connecter à la base de données :

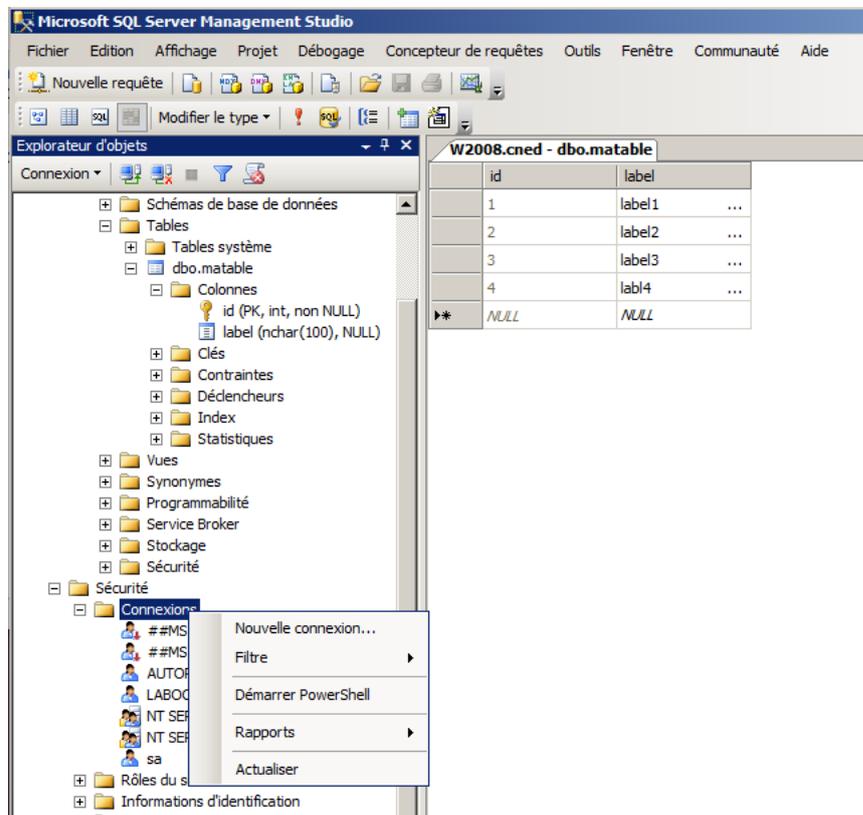


Figure 13 : Nouvelle connexion

Cette connexion aura les propriétés suivantes :

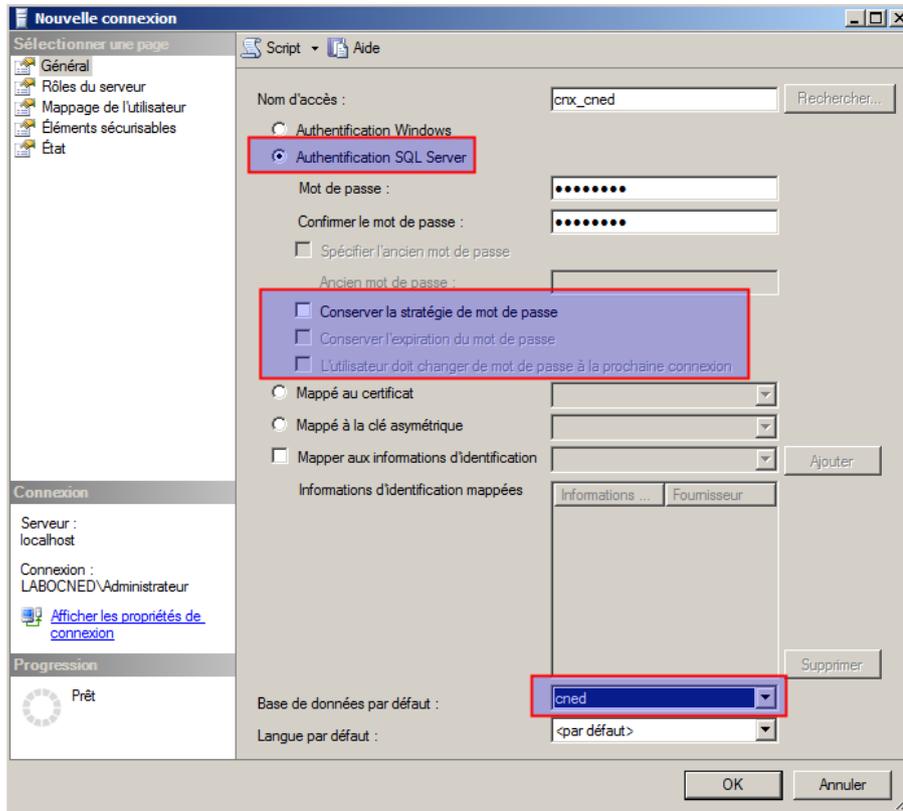


Figure 14 : création de l'utilisateur 1/2

- Authentification SQL Server (mot de passe à créer)
- Conserver la stratégie : décoché
- Base de données par défaut : cned

Observez également l'écran suivant qui permet d'indiquer sur quelle(s) base(s) de données notre utilisateur peut accéder et avec quels droits. Nous le mettons ici propriétaire (db_owner) de la base cned, ce qui signifie qu'il peut faire ce qu'il veut à l'intérieur de cette base.

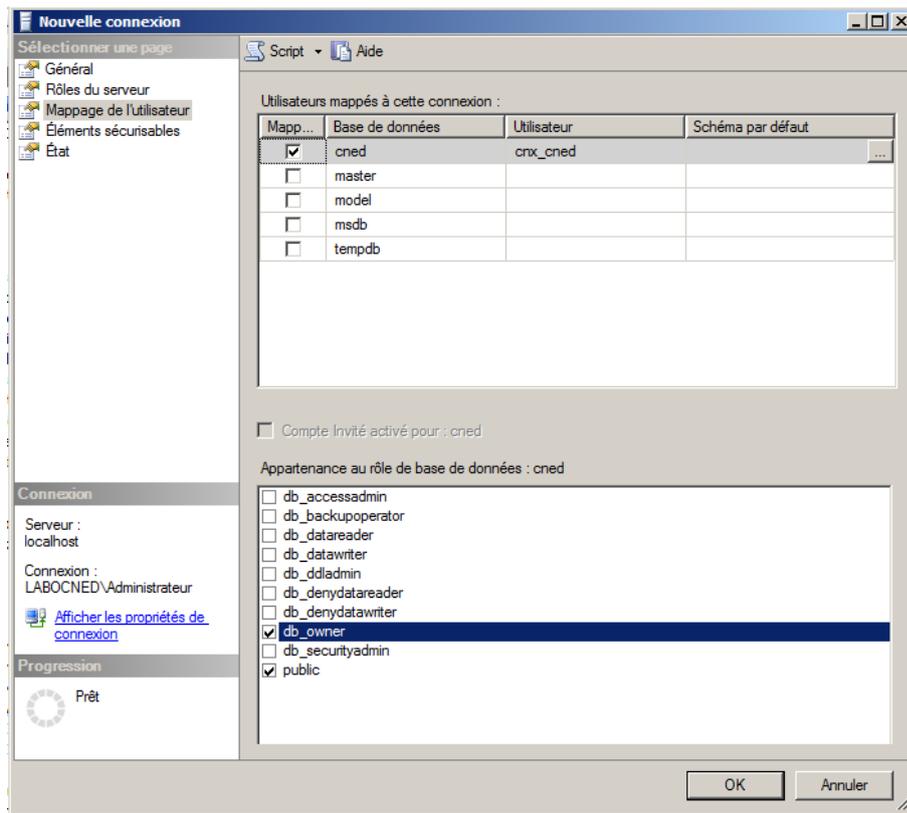


Figure 15 : création de l'utilisateur 2/2

Atelier 8

SQL Server 2008 R2

Page 104

Vous pouvez tester votre connexion en vous reconnectant à SQL Server avec le compte créé qui doit pouvoir lister le contenu de la table matable de la base CNED. Dernière chose, comme dit en introduction, la base de données est constituée de deux fichiers dans le système de fichiers :

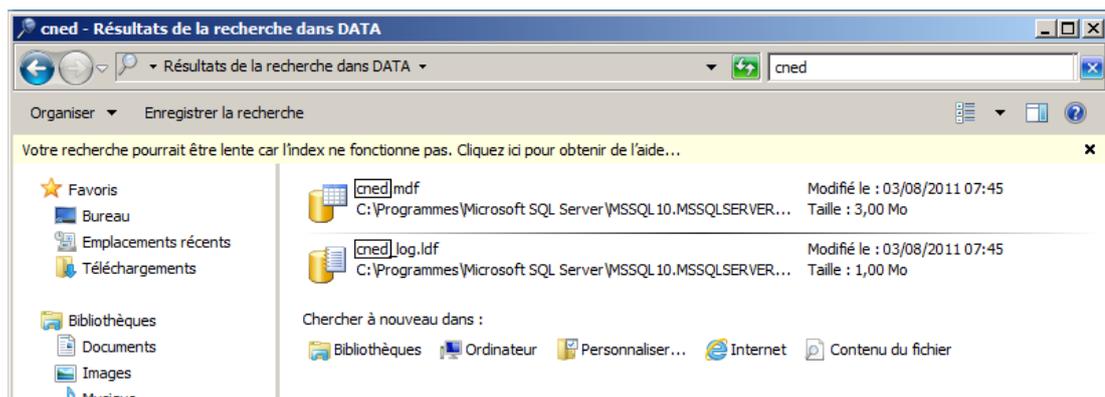


Figure 16 : fichiers de base de données

- un fichier mdf qui contient les données
- un fichier ldf qui contient les journaux

6. Création d'une application

Nous allons créer une page ASPX qui interrogera la base de données et en affichera le contenu. Dans un premier temps, il faut indiquer à notre future application comment se connecter à la base de données. Revenons dans la gestion IIS, cliquez sur le site :

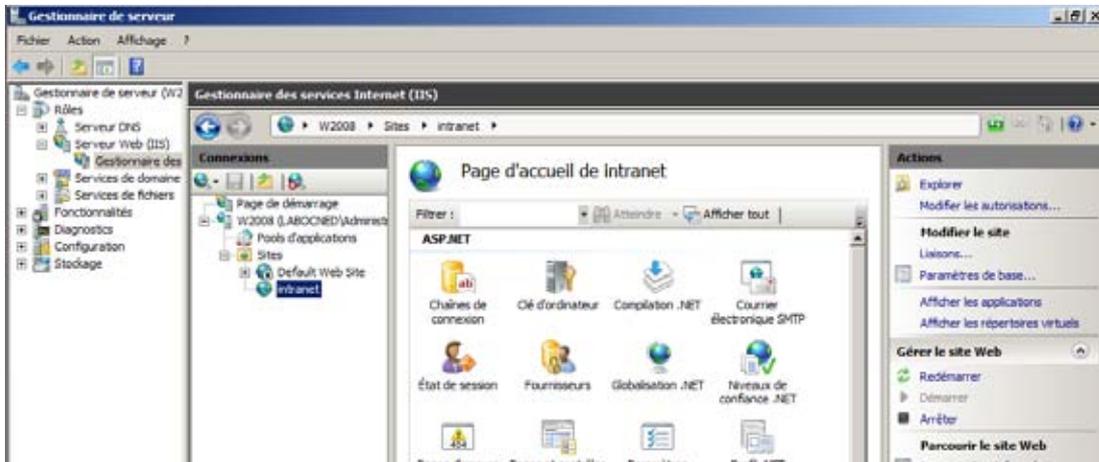


Figure 17 : Gestion IIS

Ensuite, choisissez « chaînes de connexion » dans la rubrique ASP.NET :

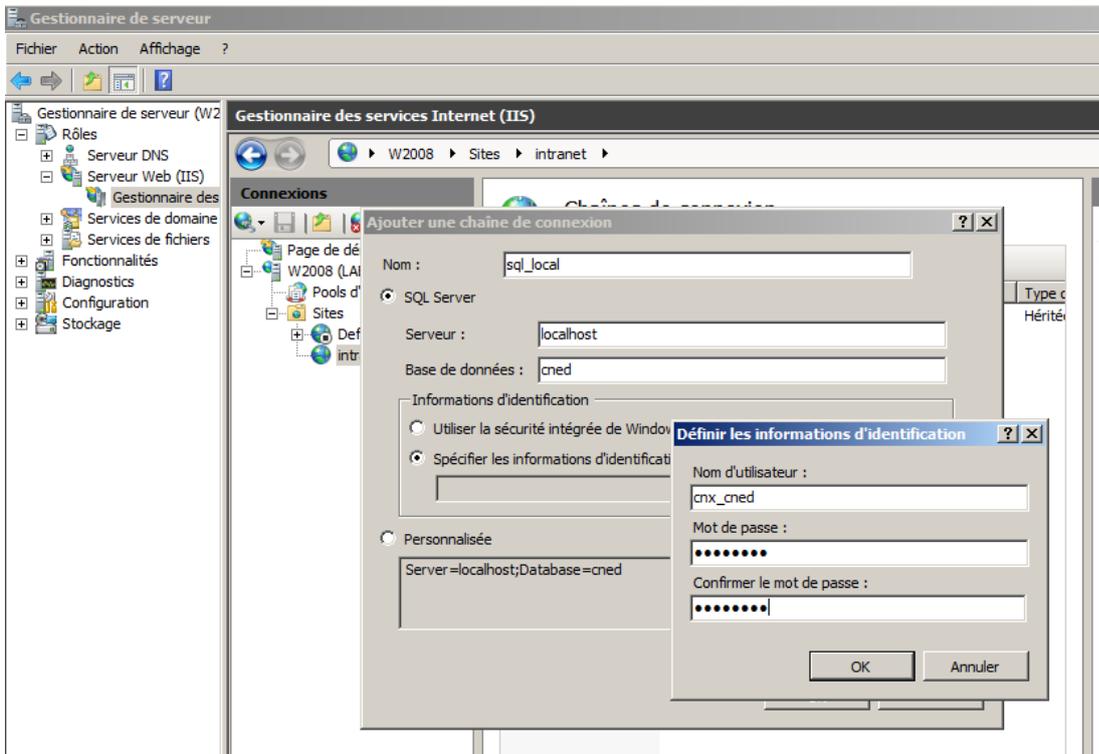


Figure 18 : Chaîne de connexion

Une fois cette manipulation réalisée, vous pourrez constater qu'un fichier a été créé dans le répertoire du site Web. Il s'agit du web.config associé à toute application.NET et qui contient tous les paramètres :

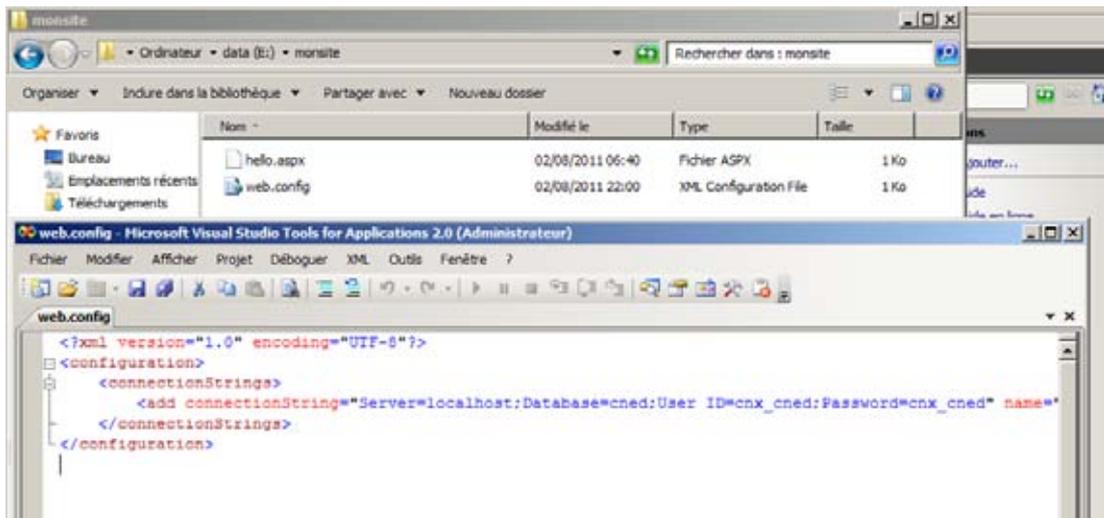


Figure 19 : web.config

Enfin, dans ce même répertoire, créez un nouveau script `sgbd.aspx` qui contiendra les éléments suivants :

```
<form id="form1" runat="server">
  <asp:SqlDataSource
    id="matable"
    runat="server"
    ConnectionString="<%$ ConnectionStrings:sql_local %>"
    SelectCommand="SELECT id,label FROM matable" />
  <asp:GridView
    id="grdListe"
    DataSourceID="matable"
    Runat="server" />
</form>
```

Atelier 8

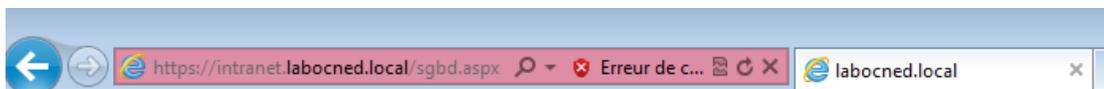
SQL Server 2008 R2

Page 106

Nous utilisons deux composants.NET :

- une datasource qui fait référence à la connexion précédemment créée et contient une requête (un simple select qui liste le contenu de matable) ;
- un gridview pour l'affichage qui génère un tableau avec les données.

Depuis un navigateur, nous obtenons la merveille ci-dessous :



id	label
1	label1
2	label2
3	label3
4	label4

Figure 20 : affichage depuis un navigateur

7. Sauvegardes

Autant SQL Server est bien outillé pour faire des sauvegardes locales sur le serveur, autant envoyer ces sauvegardes sur le réseau n'est pas simple et il n'existe toujours pas à ce jour de méthode « officielle ». Il faut quand même constater que c'est très curieux puisque le b.a.-ba d'un dispositif de sauvegarde est de ne pas conserver les sauvegardes au même endroit que les données elles-mêmes ! Donc, nous vous présenterons une méthode utilisée en production, l'idée est d'envoyer la sauvegarde sur un répertoire partagé sur une autre machine du réseau local. Ceci fonctionne bien en local mais à éviter si vous devez exporter les données en dehors du LAN, il faudra envisager d'autres méthodes (rsync par exemple), mais vous tomberez alors sur une autre problématique : les débits réseau ne sont pas toujours (et même rarement) en adéquation avec les volumes (allez exporter 100 Gio avec du 6 Mbits/s!).

Revenons à nos moutons. L'intérêt de SQL Server est que les sauvegardes peuvent être faites à chaud, donc pendant que la base de données est utilisée. Néanmoins, les sauvegardes sont généralement programmées à un horaire plus calme (dans la nuit). Mais avec Internet et la mondialisation, la nuit en France c'est le jour ailleurs dans le monde...

Dans un premier temps, il faut modifier l'utilisateur sous lequel tournent les processus SQL Server. En effet, lors de l'installation, nous avons indiqué « system », or ce pseudo-utilisateur n'a pas le droit d'utiliser le réseau.

7A. Création d'un utilisateur

Dans la console de gestion des utilisateurs Active Directory, vous créez dans l'OU Users un utilisateur que vous appelez comme vous voulez (sqlagent ou sqlserver semblent une bonne idée). Ensuite, vous l'affectez au groupe des administrateurs. En effet, les processus SQL Server ont besoin d'avoir des privilèges élevés pour fonctionner. Dans le temps (SQL 2005), un groupe avec les bons droits était créé lors de l'installation, mais ceci a disparu... Dommage.

Lorsque c'est fait, vous retournez dans l'outil de configuration de SQL Server, rubrique « services » :



Figure 21 : gestion des services

Vous remplacez le compte intégré « AUTORITE NTSERVICE LOCAL » pour les services SQL Server et Agent SQL Server par votre nouveau compte. Vérifiez que les deux services ont bien redémarré tous les deux !

7B. Création d'un partage

Le principe étant d'évacuer les données sauvegardées vers une autre machine, nous profitons du fait que nous avons un domaine pour créer un répertoire partagé sur la station Seven accessible **uniquement à notre nouvel utilisateur**. Question de sécurité absolument indispensable !

Vous créez quelque part un dossier que vous partagez et affectez votre utilisateur avec des droits en lecture/écriture. Vous remarquez que localement sur notre station, nous pouvons utiliser des utilisateurs définis au niveau du domaine :

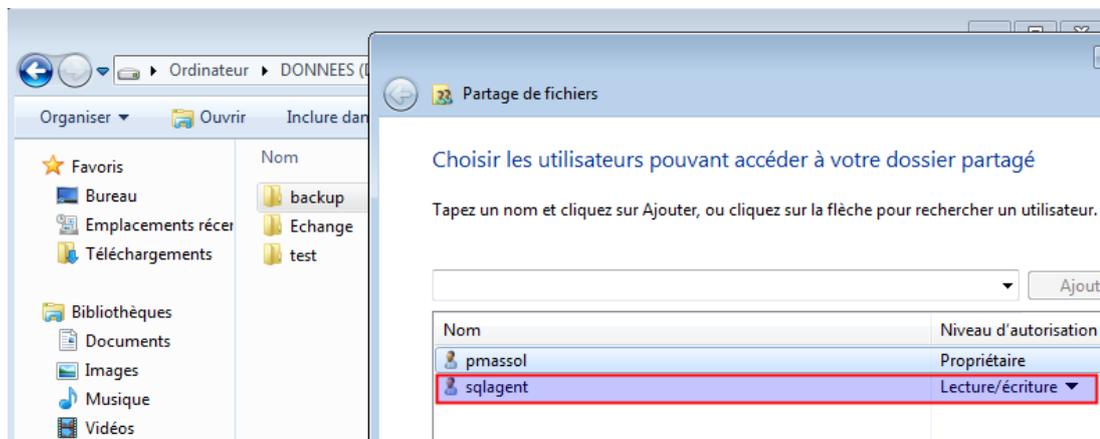


Figure 22 : déclaration du partage

Le principe est que l'agent SQL Server va se connecter à ce partage en se présentant comme « sqlagent » ce qui lui donnera le droit de déposer des fichiers.

Notez à cette étape le nom UNC (Uniform Naming Convention) de ce partage. Ce nom correspond (pour aller très vite) à une URL dans le monde Windows/Netbios/SMB (mais ne dites jamais ça à un examinateur ;-). Ces noms UNC ont toujours la forme : \\<nom de la machine>\<nom du partage>. Dans mon cas, il s'agit de \\MV1-W7\backup :

Atelier 8

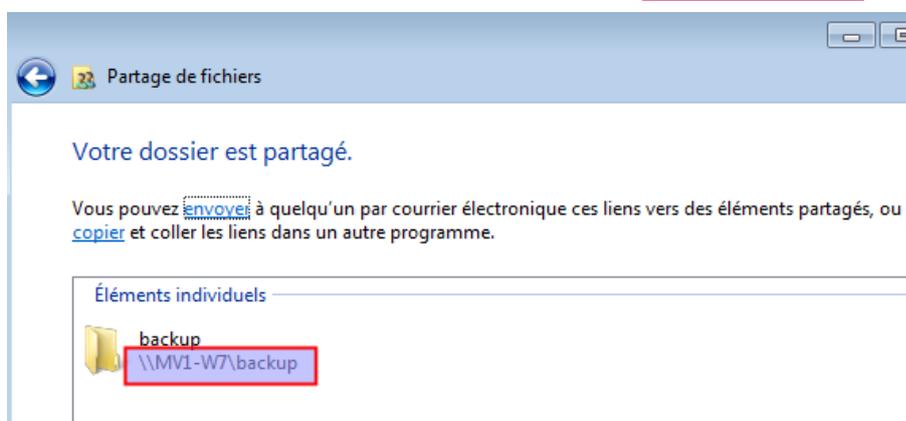


Figure 23 : nom UNC du partage

7C. Définition du plan de sauvegarde

Nous détaillons ici des principes généraux à adapter au cas par cas selon les besoins de l'entreprise, la valeur des données, les volumétries, etc.

Avertissement : la sauvegarde SQL Server réserve quelques petits pièges :-)))

7C1. Principes

Avec SQL Server, la sauvegarde se définit dans un ensemble plus vaste appelé « plans de maintenance ». Avec cet outil, vous pouvez lancer tout un tas de tâches orientées SGBD (réindexer, compacter, sauvegarder, etc.) que l'on peut ensuite planifier.

Évoquons un sujet en relation avec la sauvegarde : le mode de récupération d'une base de données :

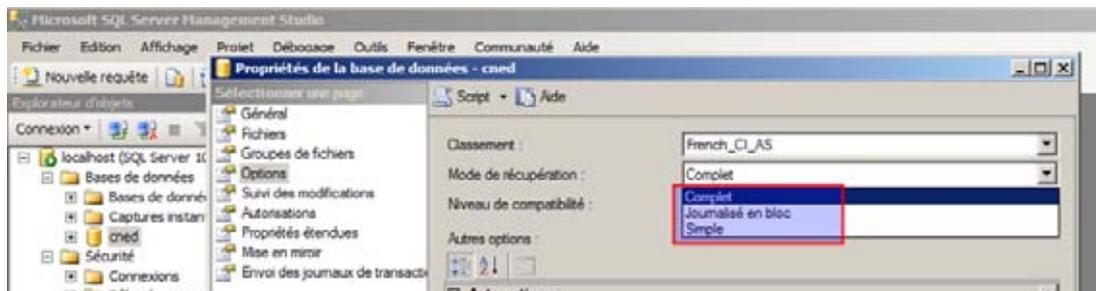


Figure 24 : mode de récupération

Il existe 3 modes, du plus au moins sécurisé, du moins au plus performant :

- complet
- journalisé en bloc
- simple

Je vous renvoie vers la documentation pour le détail. Je préconise « complet » qui assure le meilleur niveau de récupération en cas de problème. Ce mode peut éviter de faire une restauration car au redémarrage après un incident, SQL Server va se débrouiller pour présenter les bases de données dans un état cohérent. Le mode « simple » ne dispose pas du tout de journaux et donc il faudra probablement restaurer, tâche que l'on préfère éviter car :

1. ça bloque les utilisateurs ;
2. vous perdez du travail : exemple : votre sauvegarde est faite à 2h du matin tous les jours mais une panne se produit à 16h.

Quelques éléments que vous devez connaître avant de commencer car rien n'est fait « tout seul » :

- il faut sauvegarder les fichiers de données : hé hé
- il faut sauvegarder les journaux de transactions (à cause du mode « complet ») : ceci est ultra important et si on n'a pas lu la documentation, on tombe dans le panneau : **les journaux de transactions ne sont purgés que lors d'une sauvegarde**. Ces fichiers grossissent très vite et ça vous tombe dessus tôt ou tard : disque saturé !
- au bout de quelques temps, il faut supprimer les sauvegardes anciennes

7C2. Saisie du plan de maintenance

Allez dans le management studio ouvrez l'arborescence du serveur, allez dans « Gestion » puis clic droit sur « Plans de maintenance ». Donnez un nom au plan.

La structure générale du plan se définit par glisser-déplacer : vous prenez les tâches en bas à gauche et vous les placez dans l'espace de travail.

Commençons par une tâche « sauvegarder la base de données », puis double-cliquez dessus pour définir les propriétés :

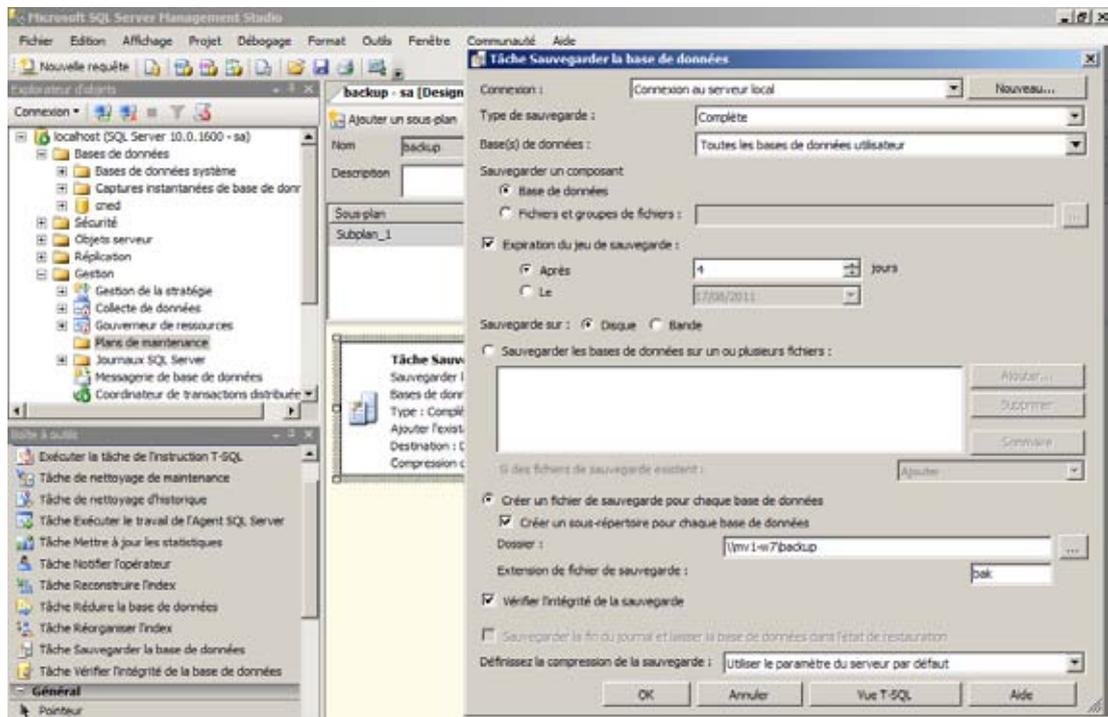


Figure 25 : propriétés de la tâche «sauvegarder»

Atelier 8

SQL Server 2008 R2

Page 110

- type de sauvegarde : laisser « complète » (éventuellement « différentielle » sur de très grosses bases)
- bases de données : vous pouvez en choisir individuellement ou dire « toutes les bases utilisateurs ». N'oubliez pas de sauvegarder les bases système (surtout master)
- expiration : à voir selon les besoins : **cela ne supprime pas les fichiers expirés sur disque !!!**
- créer un fichier et des sous-répertoires (pratique si beaucoup de BD). Dans « dossier », on indique le nom UNC du partage.
- vérifier l'intégrité : vous imaginez une sauvegarde corrompue ?

Maintenant, vous faites de même avec une nouvelle tâche « sauvegarder », dans « type de sauvegarde », vous mettez « journal des transactions ».

Ensuite, nous ajoutons deux nouvelles tâches « de nettoyage de maintenance » pour effacer les fichiers périmés (sinon, **nouveau risque de saturation de disque et donc de sauvegardes qui ne se font plus...**).

Il faudra indiquer des données cohérentes avec les plans de sauvegarde. Par exemple, pour les données :

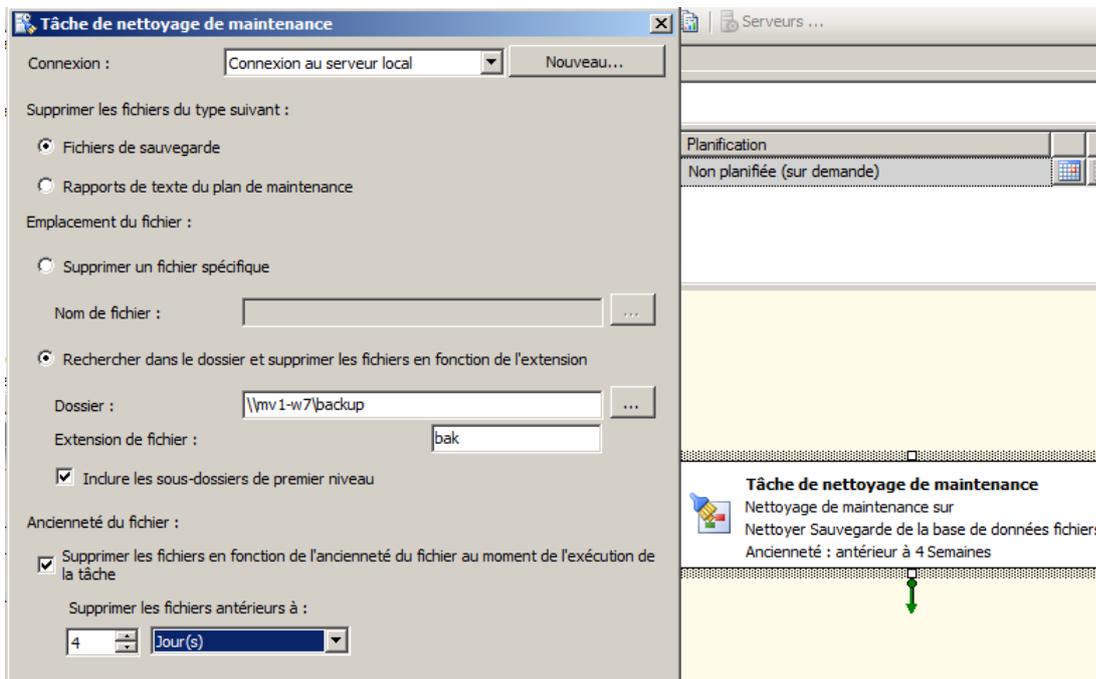


Figure 26 : propriétés de la tâche de maintenance

Vous faites de même pour les journaux (extension.trn).

Au total, vous devez obtenir quelque chose qui ressemble à ceci. Vous pouvez « lier » les tâches de façon à ce qu'elles s'exécutent dans un ordre défini (pas très important ici) :

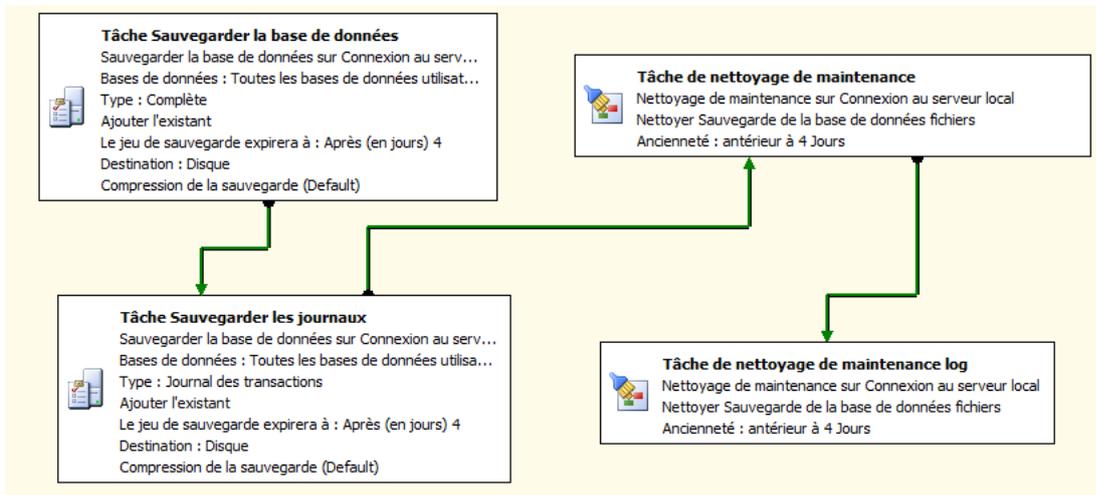


Figure 27 : plan de maintenance

Ouf ! Heureusement que l'on ne fait pas ces tâches tous les jours. On va essayer de l'exécuter pour voir ce qu'il se passe.

Vous enregistrez le plan, vous cliquez droit sur le plan et vous choisissez « exécuter » :

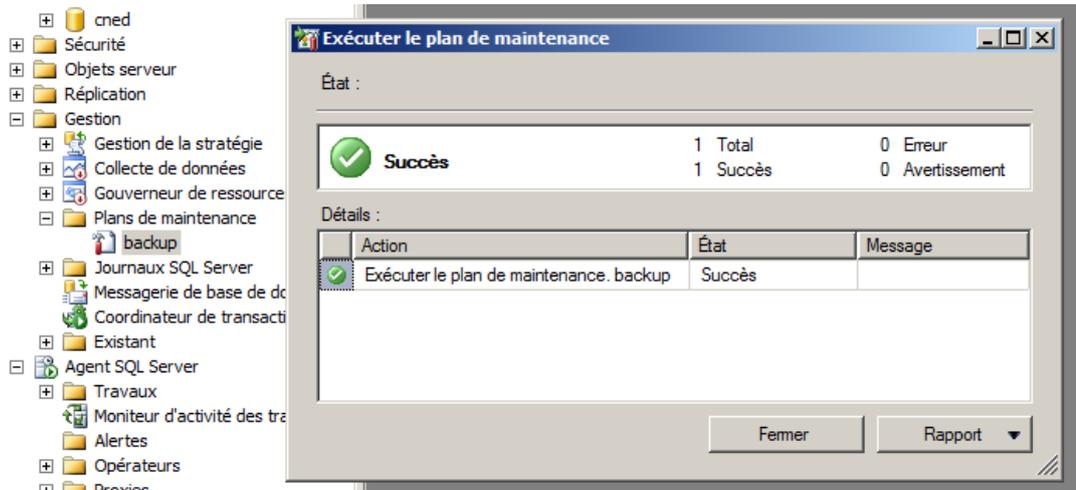


Figure 28 : exécution du plan de maintenance

Le plan a bien fonctionné. En cas de problème, vous avez un journal d'erreur qui vous aidera à les résoudre. En cliquant droit sur le plan de maintenance, choisissez « historique » :

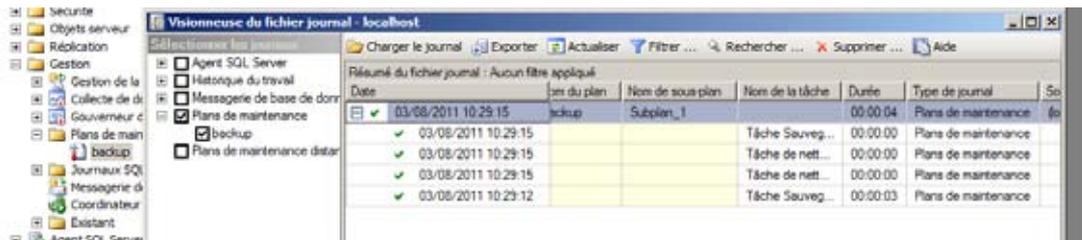


Figure 29 : journal Agent SQL

Atelier 8

SQL Server 2008 R2

Page 112

Voyons maintenant le résultat dans le répertoire partagé :

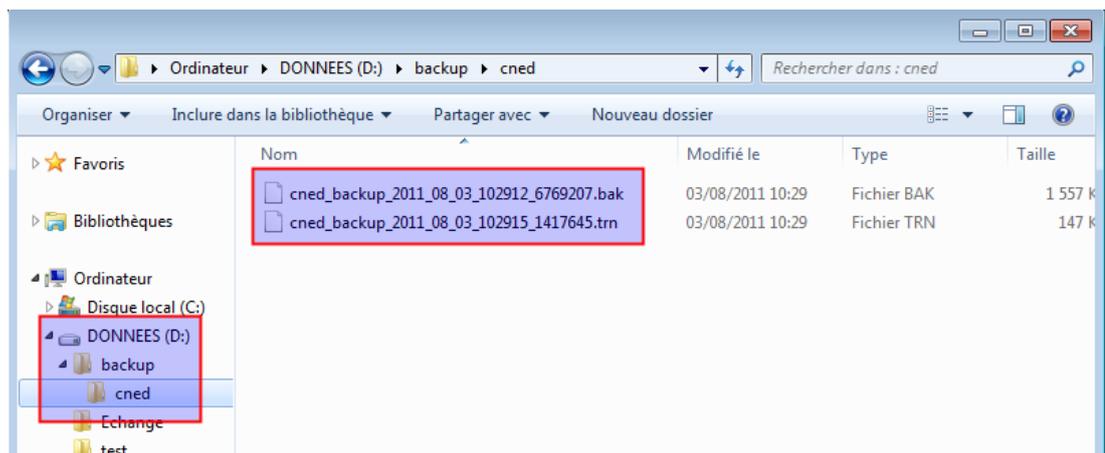


Figure 30 : Sauvegarde dans le répertoire partagé

Comme configuré, la sauvegarde a bien créé un sous-répertoire « cned » avec dedans les deux fichiers. Les fichiers viendront s'ajouter pendant 4 jours. Au-delà, les tâches de nettoyage supprimeront les fichiers les plus anciens.

7D. Planification

Vous n'allez pas passer votre temps à lancer des sauvegardes à la main ? L'agent SQL Server est là pour assurer le déclenchement de tâches planifiées. Le cas standard est qu'un plan de sauvegarde s'exécute régulièrement (une fois par jour en général). Nous allons réaliser ceci dans la configuration du plan de maintenance :

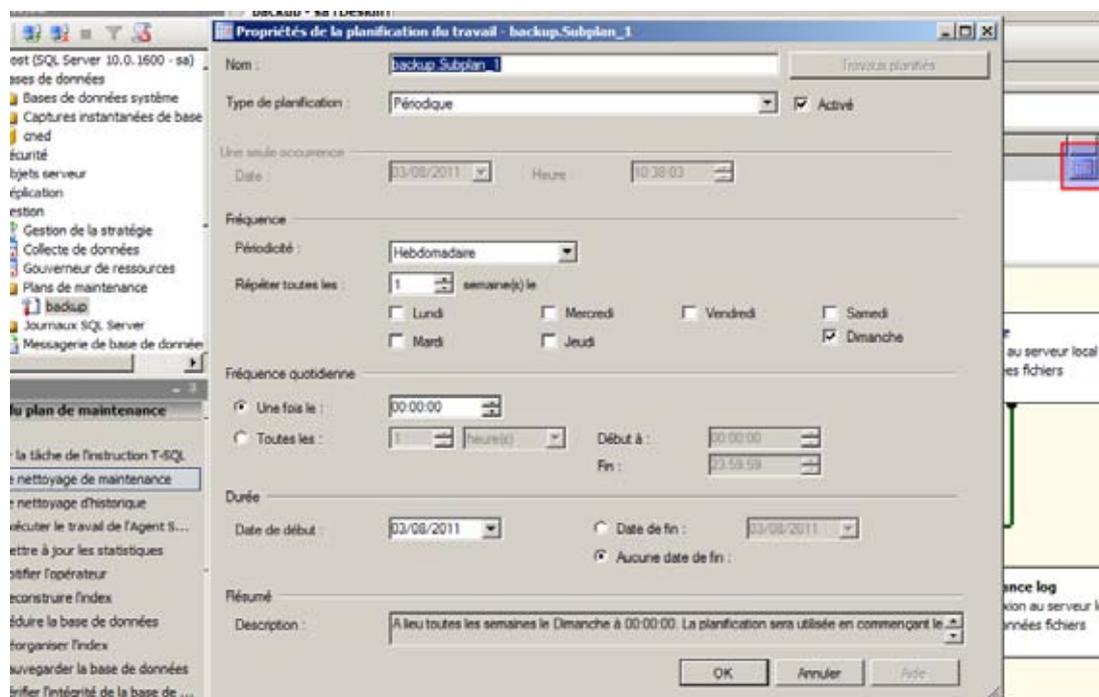


Figure 31 : planification des sauvegardes

Il faut cliquer sur le bouton qui représente un calendrier à droite du sous-plan contenu dans le plan de maintenance. La planification concernera alors les 4 tâches. Pour les paramètres, vous pouvez vous inspirer de la figure ci-dessus.

7E. Suivi des sauvegardes

Le « tout automatique » c'est bien, mais que se passe-t-il si le serveur a un problème ? Le cas le plus fréquent est la partition saturée : les plans de maintenance s'exécutent mais échouent. Et le jour où vous avez besoin de restaurer alors que cela ne marche plus depuis deux semaines, vous êtes très très mal...

Donc, l'idée est de se faire envoyer un email après chaque backup afin de suivre l'activité et d'intervenir rapidement en cas de problème. La configuration de la messagerie n'est pas des plus simples avec SQL Server... D'autant plus que cohabitent deux systèmes :

- le système dit « SQL Mail » organisé autour d'un client de messagerie type « Outlook express » ou « Microsoft mail » : vous vous doutez bien que je bannis ce mode de fonctionnement et refuse d'installer sur mes serveurs un client de messagerie quelconque (MS ou autre)
- Database Mail : le système préférable à mon sens, mais il faut disposer quelque part d'un serveur relais SMTP, ce qui n'est pas toujours le cas (même si c'est rare)...

Donc, dans l'arborescence SQL Server, nous cliquons sur « Gestion » puis sur « Messagerie de la base de données » afin de définir, pour résumer, le serveur SMTP disponible :

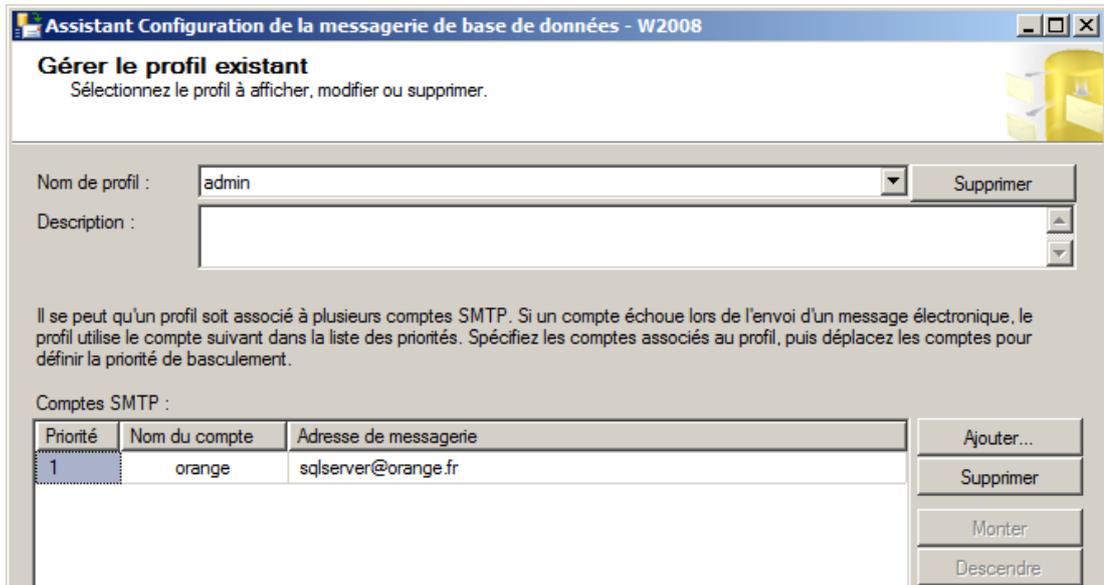


Figure 32 : profil SMTP

Il faut donner un nom à ce profil puis « ajouter » un compte SMTP. On constate sur la figure ci-dessus que plusieurs serveurs SMTP peuvent être définis pour un même profil, au cas où un ou plusieurs seraient inaccessibles.

Derrière le bouton « Ajouter » se trouve un écran dans lequel certains champs impératifs doivent être définis :

Atelier 8

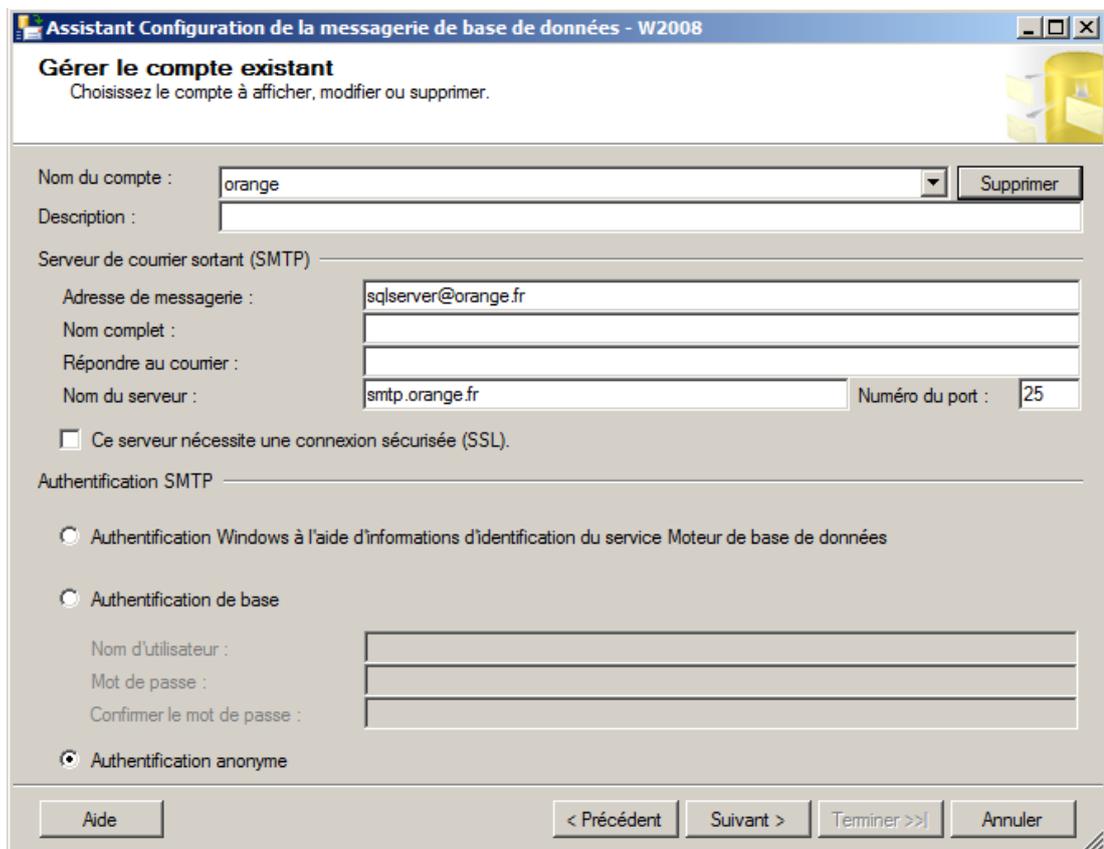


Figure 33 : compte SMTP

Au minimum, vous devez définir le nom, l'adresse email de l'expéditeur (qui doit être cohérente) et le nom (ou l'IP) du serveur SMTP à votre disposition. Chez moi, c'est mon FAI mais à vous de voir (si vous n'êtes pas chez Orange, ne mettez pas Orange !). Adaptez selon votre configuration.

Dernier élément à configurer ici : la « sécurité des profils ». Dans un cas « standard » comme le notre, il s'agit de définir le profil par défaut. Comme il n'y en a qu'un, cela sera vite fait :

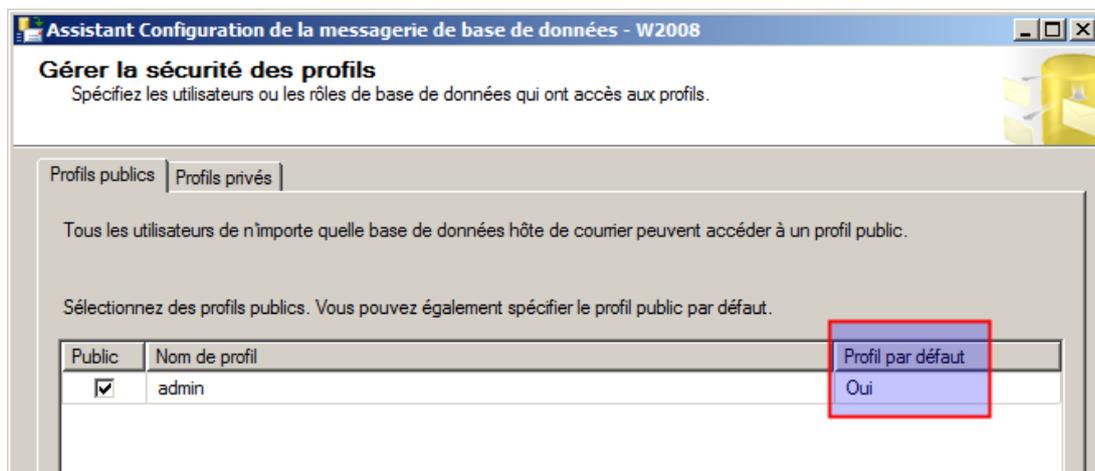


Figure 34 : sécurité des profils

Il faut cocher notre profil et **surtout, le définir comme profil par défaut**. Enregistrez le tout. Si maintenant vous cliquez droit sur « Messagerie de base de données », vous avez « envoyer un message électronique de test » : un détour indispensable !

Passons à la partie « Agent SQL ». Allons dans les propriétés de l'agent pour lui indiquer quel profil SMTP il doit utiliser :

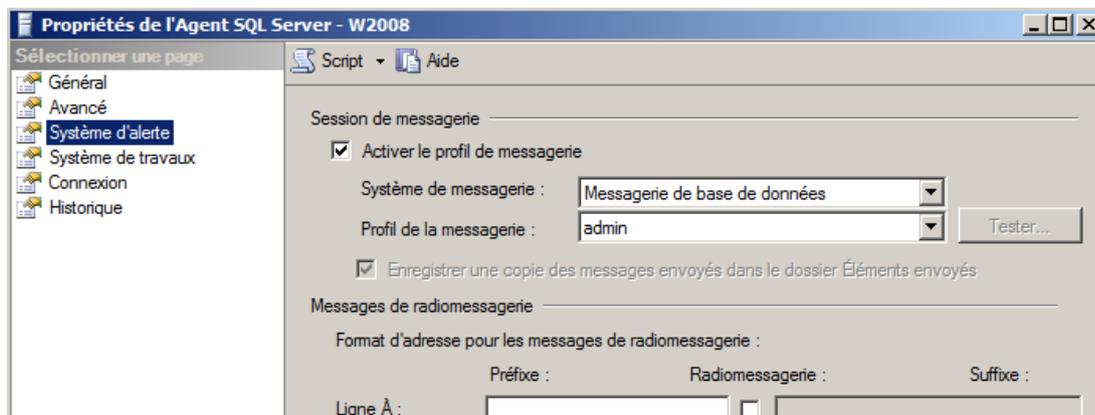


Figure 35 : Profil SMTP

Ensuite, il faut définir un ou des « opérateurs » : dans notre cas, ce sont les destinataires des emails émis par SQL Server. Cliquez sur « Agent SQL Server » puis sur « Opérateurs » puis sur « Nouvel opérateur ».

Cela consiste à donner un nom et une adresse email valide :

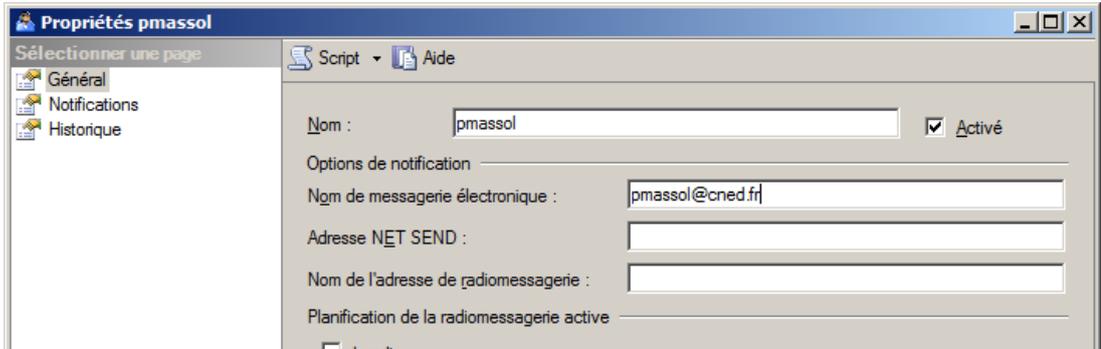


Figure 36 : nouvel opérateur

Ceci étant fait, toujours dans l'agent SQL, nous allons maintenant sur notre plan de maintenance afin de paramétrer la partie « notifications ». Vous cliquez droit sur le travail puis vous allez dans la rubrique « Notifications » :

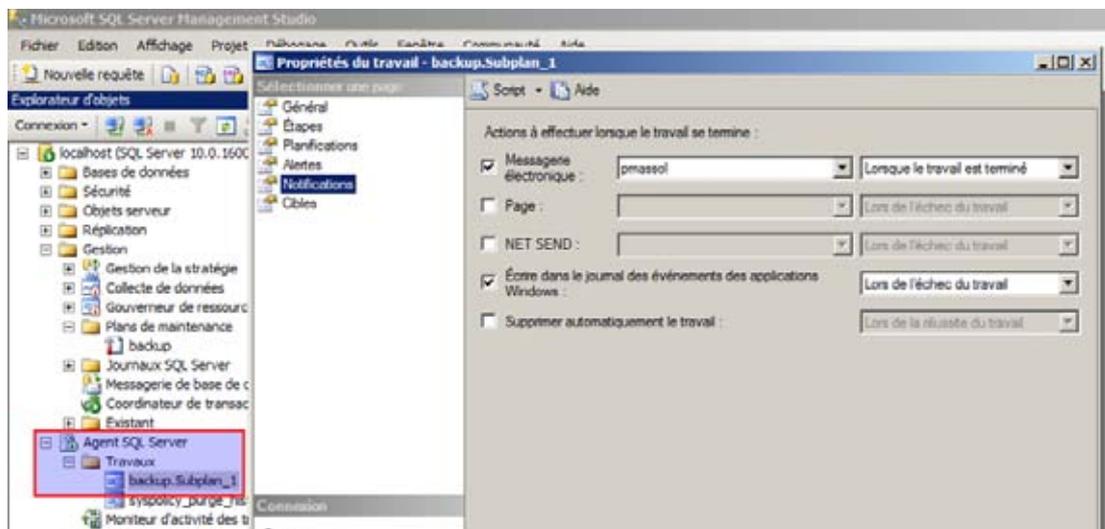


Figure 37 : paramétrer les notifications

Cela consiste à désigner un « opérateur » et les conditions d'envoi du mail. Étant un peu parano, j'aime bien recevoir un email que cela ait fonctionné ou non... Dans le domaine informatique, la paranoïa est généralement une qualité :-)

Avant d'aller plus loin, il semble nécessaire d'arrêter puis de démarrer l'agent (je n'ai pas dit « redémarrer »!).

Exécutez à nouveau votre plan de sauvegarde, vous devrez recevoir ce type de mail :

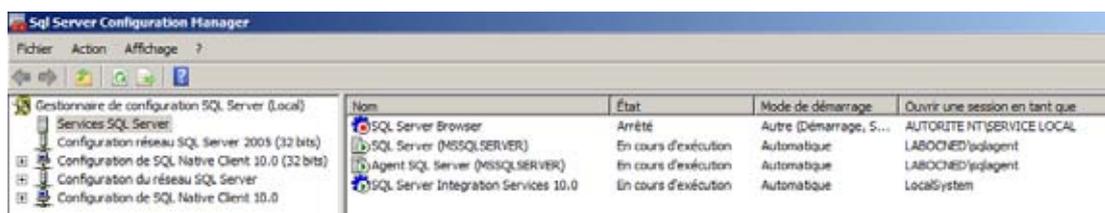


Figure 38 : gestion des services

À retenir

Un serveur SQL est un élément important dans un site Internet. Son architecture matérielle doit être correctement dimensionnée et sécurisée.

Chaque base données a un mode de récupération déterminé. Il est conseillé d'utiliser le mode « complet » qui permet la meilleure sécurité lors d'un plantage de serveur. En effet, pour optimiser son fonctionnement, le SGBD gère une mémoire cache avec des écritures différées. Les bases de données peuvent donc se retrouver dans un instable état lors d'un arrêt brutal du fonctionnement.

Les sauvegardes font l'objet d'un plan de maintenance en 4 étapes : sauvegarde des données, des journaux, purge des sauvegardes de données, purge des sauvegardes des journaux. Les plans peuvent être planifiés grâce à l'Agent. Si les sauvegardes doivent être envoyées sur le réseau, il faut que les processus SQL Server et Agent SQL Server tournent sous des utilisateurs adaptés.

Il est fortement conseillé de configurer la messagerie de base de données afin de recevoir des notifications sur le déroulement des plans de sauvegarde.

Si vous voulez approfondir

Simuler un plantage de serveur : remonter un nouveau serveur et restaurer les sauvegardes (système et données)

Faire un plan de maintenance pour réindexer et compacter les bases de données avec une planification mensuelle.

Atelier 9

Initiation au PowerShell

► Durée approximative de cet atelier : 1 heure 30

► Objectif

S'initier au PowerShell, l'interpréteur de commandes survitaminé de Windows.

► Durée approximative de cet atelier

Notre serveur Windows 2008 R2 SP1.

► Considérations techniques

Nous présentons les principes du PowerShell 2.0 fournis en standard avec 2008 et Seven. Il permet de gérer intégralement son serveur en mode « core » en ligne de commandes. Ça vous rappelle quelque chose :-)? Si vraiment cela ne vous dit rien, voyez les prochains ateliers :-)))

► Contenu

1. Introduction	120
2. Principes	120
3. Quelques commandes utiles.....	122
4. Active Directory	124
5. SQL Server.....	125
6. DNS.....	127
7. PowerShell, domaine et scripts d'ouverture de session.....	128

1. Introduction

Le PowerShell est une version moderne des interpréteurs de commandes classiques du type shell Unix. Ses principales caractéristiques sont :

- Langage orienté objet : ainsi lorsque l'on récupère une liste à la suite d'une commande, il ne s'agit pas d'une simple liste mais bien d'objets avec leurs propriétés et leurs méthodes. Donc, totalement orienté « développeur » !
- Accès complet aux assemblies (bibliothèques si vous voulez) du framework.NET : tous les objets du framework peuvent être instanciés dans PowerShell donnant accès à un nombre très importants de fonctions.
- Extensibilité : vous pouvez créer vos propres cmdlets (nom d'une commande PowerShell aussi appelées « applet de commande ») afin de rendre scriptable vos applications.
- XML : Intégration poussée avec le XML.

2. Principes

Quelques conseils élémentaires pour faciliter l'usage. Le PowerShell est disponible dans le menu démarrer, sous différentes versions, nous en reparlerons plus loin. Son interface se présente ainsi :

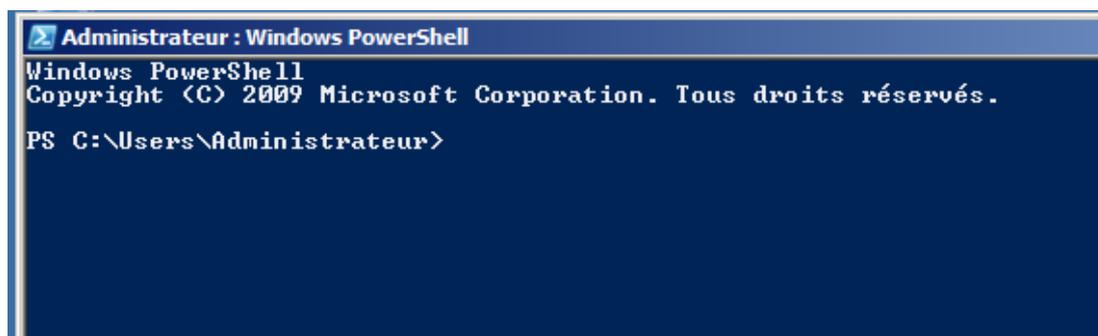


Figure 1 : Prompt PowerShell

Nos amis de Microsoft nous ont gentiment mis un fond bleu et un prompt « PS » pour éviter de le confondre avec l'interpréteur de commandes MS-DOS classique.

Vous êtes encouragé à utiliser le plus souvent la touche « tabulation » qui permet de compléter les commandes dont vous tapez le début. Les flèches haut et bas permettent de parcourir l'historique des commandes et d'en rejouer certaines.

La convention de nom des cmdlets est composée de deux parties :

- le verbe qui indique l'action à réaliser (new, set, get, enable, disable, remove, ...)
- le nom de l'objet sur lequel la cmdlet va s'appliquer (Service, Mailbox, MailBoxDatabase,...).

Un système d'aide en ligne est disponible à tout moment grâce à la commande Get-Help suivi du nom de la commande :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> Get-Help Get-Command

NOM
Get-Command

RÉSUMÉ
Obtient des informations de base sur les applets de commande et d'autres éléments des commandes Windows PowerShell.

SYNTAXE
Get-Command [-Name] <string[]> [-CommandType <Alias | Function | Filter | Cmdlet | ExternalScript | Application | Script | All>] [-ArgumentList <Object[]>] [-Module <string[]>] [-Syntax] [-TotalCount <int>] [<CommonParameters>]
Get-Command [-Noun <string[]>] [-Verb <string[]>] [-ArgumentList <Object[]>] [-Module <string[]>] [-Syntax] [-TotalCount <int>] [<CommonParameters>]

DESCRIPTION
L'applet de commande Get-Command obtient des informations de base sur les applets de commande et d'autres éléments des commandes Windows PowerShell de la session, tels qu'alias, fonctions, filtres, scripts et applications.
Get-Command obtient directement ses données du code d'une applet de commande, d'une fonction, d'un script ou d'un alias, contrairement à Get-Help, qui les obtient des fichiers de rubrique d'aide.
Sans paramètres, « Get-Command » obtient toutes les applets de commande et fonctions de la session active. « Get-Command * » obtient tous les éléments Windows PowerShell et tous les fichiers autres que Windows PowerShell dans la variable d'environnement Path ($env:path). Elle regroupe les fichiers dans le type de commande « Application ».
Vous pouvez utiliser le paramètre Module de Get-Command pour rechercher les commandes qui ont été ajoutées à la session en ajoutant un composant logiciel enfichable Windows PowerShell ou en important un module.

LIENS CONNEXES
Online version: http://go.microsoft.com/fwlink/?LinkID=113389
about_Command_Precedence
Get-Help
Get-PSDrive
Get-Member
Import-PSession
Export-PSession

REMARQUES
Pour consulter les exemples, tapez : "get-help Get-Command -examples".
Pour plus d'informations, tapez : "get-help Get-Command -detailed".
Pour obtenir des informations techniques, tapez : "get-help Get-Command -full".

PS C:\Users\Administrateur>

```

Figure 2 : Aide en ligne du PowerShell

Une aide encore plus développée peut être affichée avec ces éléments :

- Pour consulter les exemples, tapez : «get-help Get-Command -examples».
- Pour plus d'informations, tapez : «get-help Get-Command -detailed».
- Pour obtenir des informations techniques, tapez : «get-help Get-Command -full».

De plus, il est possible d'avoir le détail sur un paramètre particulier :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> Get-Help Get-Command -Parameter CommandType

-CommandType <CommandTypes>
Obtient uniquement les types de commandes spécifiés. Utilisez « CommandType » ou son alias, « Type ». Par défaut, Get-Command obtient des applets de commande et des fonctions.

Les valeurs valides sont :
-- Alias : tous les alias Windows PowerShell dans la session active.
-- All : tous les types de commandes. Il s'agit de l'équivalent de « get-command * ».
-- Application : tous les fichiers autres que Windows PowerShell figurant dans les chemins d'accès répertoriés dans la variable d'environnement Path ($env:path), notamment les fichiers .txt, .exe, et .dll.
-- Cmdlet : applets de commande dans la session active. « Cmdlet » est la valeur par défaut.
-- ExternalScript : tous les fichiers .ps1 dans les chemins d'accès répertoriés dans la variable d'environnement Path ($env:path).
-- Filter et Function : toutes les fonctions Windows PowerShell.
-- Script : blocs de script dans la session active.

Obligatoire ?           False
Position ?             named
Valeur par défaut
Accepter l'entrée de pipeline ? true (ByPropertyName)
Accepter les caractères génériques ? false

```

Figure 3 : Détail d'un paramètre

La liste complète des commandes peut être affichée ainsi :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> Get-Command | more

```

CommandType	Name	Definition
Alias	?	ForEach-Object
Alias	?	Where-Object
Function	?	Set-Location #:
Alias	ac	Add-Content
Cmdlet	Add-Computer	Add-Computer [-DomainName] <String> [-Credential...
Cmdlet	Add-Content	Add-Content [-Path] <String[]> [-Value] <Object>...
Cmdlet	Add-History	Add-History [-InputObject] <PSObject[]> [-Pass...
Cmdlet	Add-Member	Add-Member [-MemberType] <PSMemberTypes> [-Name]...
Cmdlet	Add-PSSnapin	Add-PSSnapin [-Name] <String[]> [-PassThru] [-Ve...
Cmdlet	Add-Type	Add-Type [-TypeDefinition] <String> [-Language <...>

Figure 4 : liste des commandes

Vous notez sur ce dernier écran que vous pouvez, comme dans n'importe quel shell, lier les commandes par le pipe (|).

3. Quelques commandes utiles

Commençons notre exploration du PowerShell par quelques commandes utiles :

- Lister les services activés sur la machine et leur état (en fonctionnement ou arrêté) :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> get-service

```

Status	Name	DisplayName
Running	ADWS	Services Web Active Directory
Stopped	AeLookupSvc	Expérience d'application
Stopped	ALG	Service de la passerelle de la couc...
Running	AppHostSvc	Application Host Helper Service
Stopped	AppIDSvc	Identité de l'application
Stopped	Appinfo	Informations d'application
Stopped	AppMgmt	Gestion d'applications
Stopped	asnet_state	Service d'état ASP.NET

Figure 5 : liste des services

- Formater les affichages :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> get-service adws | Format-List -Property *

```

```

Name                : adws
RequiredServices    : {}
CanPauseAndContinue : False
CanShutdown         : True
CanStop             : True
DisplayName          : Services Web Active Directory
DependentServices   : {}
MachineName         : .
ServiceName         : adws
ServicesDependedOn  : {}
ServiceHandle       : SafeServiceHandle
Status              : Running
ServiceType         : Win32OwnProcess
Site                 :
Container            :

```

Figure 6 : format d'affichage

Voici quelques autres formats de sorties utilisables :

- get-service | Format-List
- get-service | Format-Custom
- get-service | Format-Table
- get-service | Format-Wide
- get-service | Format-Table name, Servicetype, Canshutdown

- Obtenir les éléments membres d'un service (propriétés, méthodes et événements).
Oui, nous sommes bien dans un environnement orienté objet issu de.NET :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> get-service | get-member

TypeName: System.ServiceProcess.ServiceController
Name      MemberType Definition
-----
Name      AliasProperty Name = ServiceName
RequiredServices AliasProperty RequiredServices = ServicesDependedOn
Disposed  Event        System.EventHandler Disposed(System.Object, System.EventArgs)
Close     Method       System.Void Close()
Continue  Method       System.Void Continue()
CreateObjRef Method       System.Runtime.Remoting.ObjRef CreateObjRef(type requestedType)
Dispose   Method       System.Void Dispose()
Equals    Method       bool Equals(System.Object obj)
ExecuteCommand Method       System.Void ExecuteCommand(int command)
GetHashCode Method       int GetHashCode()
GetLifetimeService Method       System.Object GetLifetimeService()
GetType   Method       type GetType()
InitializeLifetimeService Method       System.Object InitializeLifetimeService()

```

Figure 7 : membres d'un objet

- Filtrer le résultat d'une commande sur une chaîne de caractères (vous notez au passage que toutes les commandes « DOS » comme ipconfig sont bien sûr disponibles et peuvent être intégrées avec du PowerShell) :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> ipconfig | findstr "Adresse"
Adresse IPv6 de liaison locale. . . . . : fe80::f419:f79d:facf:a171%10
Adresse IPv4. . . . . : 192.168.1.100
PS C:\Users\Administrateur>

```

Figure 8 : filtrer le résultat d'une commande

- Lister les processus actifs :

```

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> Get-Process

Handles  NPM(K)  PM(K)  WS(K)  UM(M)  CPU(s)  Id ProcessName
-----
39       5       1804   4432   43     3,30    3516 conhost
33       5       860    2436   22     0,03    3568 conhost
714     12     2044   1792   45     1,69    308  csrss
257     10     1944   2884   43     25,75   348  csrss
318     30     14864  7768   348   10,78   1320 dfsrs
121     13     2264   2596   34     0,34    1544 dfssvc
5161    7295   85380  4532   118    2,19    1372 dns
66       7       1320   348    49     0,03    2504 dwm
665     41     29544  27468  229    16,86   2520 explorer
0       0       0      24     0      0       0  Idle

```

Figure 9 : liste des processus actifs

- Arrêter des processus :
 - sur le PID : Stop-Process 3512
 - sur le nom : Stop-Process -processname notepad
 - sur le nom avec joker : Stop-Process -processname note*

- consultation des journaux :

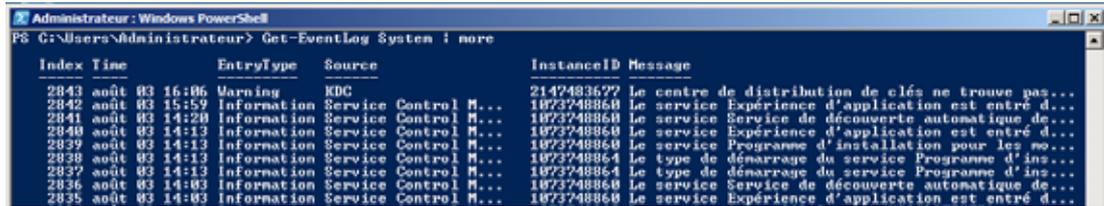


Figure 10 : Consultation des journaux

- filtrer les journaux :
 - Pour obtenir les 10 dernières erreurs dans le journal « système » :

```
Get-EventLog system -newest 10 | where {$_.entryType -match "Error"}
```

- Pour obtenir le détail des 3 derniers enregistrements du journal « système » :

```
Get-EventLog system -newest 3 | Format-List
```

- garder une trace d'une session PowerShell :

```
Start-Transcript
```

```
Stop-Transcript
```

4. Active Directory

Le contenu complet de l'Active Directory peut être affiché :

```
$Search = New-Object DirectoryServices.DirectorySearcher ([ADSI] "")
$Search.FindAll ()
```

Une seule partie peut être listée en donnant le point de départ (ici, l'adresse du conteneur « Users » exprimé dans la notation LDAP) :

```
$Search = New-Object DirectoryServices.DirectorySearcher
([ADSI] "LDAP://CN=Users,DC=labocned,DC=local")
$Search.FindAll ()
```

Un PowerShell intégrant des modules de gestion spécifiques à Active Directory est disponible dans le menu « démarrer » :

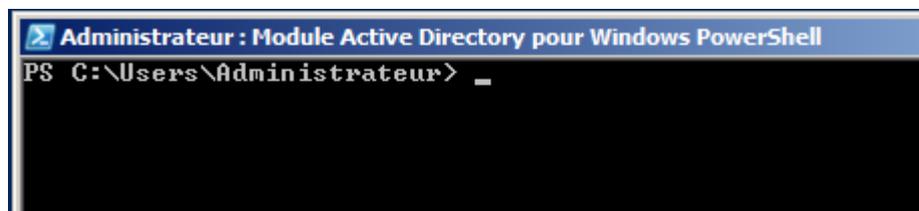


Figure 11 : PowerShell spécial AD

Get-ADuser <nom de l'utilisateur> permet d'afficher les détails sur l'utilisateur :

```
Administrateur : Module Active Directory pour Windows PowerShell
PS C:\Users\Administrateur> Get-ADuser pmassol

DistinguishedName : CN=admin,OU=Lycée,DC=labocned,DC=local
Enabled            : True
GivenName         :
Name              : admin
ObjectClass       : user
ObjectGUID        : c77e1b1a-bf4e-4460-8079-50f1ffedcd15
SamAccountName    : pmassol
SID               : S-1-5-21-1758528185-2310414739-64310122-1128
Surname           : pmassol
UserPrincipalName : pmassol@labocned.local
```

Figure 12 : Détails d'un utilisateur

En ajoutant -Properties * vous verrez toutes les données concernant l'utilisateur.

New-ADuser et Remove-ADuser permettent d'ajouter ou supprimer un utilisateur dans Active Directory :

```
Administrateur : Module Active Directory pour Windows PowerShell
PS C:\Users\Administrateur> new-aduser toto -path "OU=Lycée,DC=labocned,DC=local"
-UserPrincipalName "toto@labocned.local" -AccountPassword (Read-Host -AsSecure
String "AccountPassword")
AccountPassword: *****
PS C:\Users\Administrateur>
```

Figure 13 : ajout d'un utilisateur à AD

Vérifiez dans Active Directory que l'utilisateur figure bien.

5. SQL Server

Un autre (encore) PowerShell intègre les modules disponibles pour SQL Server. Exécutez la commande sqlps à partir du menu démarrer :

```
Administrateur : C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\SQLPS.exe
Microsoft SQL Server PowerShell
Version 10.0.1600.22
Microsoft Corp. All rights reserved.
PS SQLSERVER:\>
```

Figure 14 : Sqlps ou le PowerShell spécial SQL Server

On peut ensuite se promener dans l'arborescence SQL Server avec les bonnes vieilles commandes DOS de gestion de fichiers (cd, dir, etc.) :

```

Administrateur : C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\SQLPS.exe
Microsoft SQL Server PowerShell
Version 10.0.1600.22
Microsoft Corp. All rights reserved.

PS SQLSERVER:\> dir

Name                Root                Description
----                -
SQL                 SQLSERVER:\SQL      Moteur de base de données SQL Server
SQLPolicy           SQLSERVER:\SQLPolicy  Gestion de la stratégie SQL Server
SQLRegistration     SQLSERVER:\SQLRegistration  Inscriptions SQL Server
DataCollection     SQLSERVER:\DataCollection  Collecte de données de SQL Server

PS SQLSERVER:\> cd SQL
PS SQLSERVER:\SQL> dir

MachineName
-----
W2008

PS SQLSERVER:\SQL> cd W2008
PS SQLSERVER:\SQL\W2008> dir

Instance Name
-----
DEFAULT

PS SQLSERVER:\SQL\W2008> cd DEFAULT
PS SQLSERVER:\SQL\W2008\DEFAULT>

```

Figure 15 : parcours de l'arborescence SQL Server

Atelier 9

À partir de ce point, nous retrouvons tous les objets visibles dans le Management Studio de SQL Server :

Initiation
au PowerShell

Page 126

```

Administrateur : C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\SQLPS.exe
PS SQLSERVER:\SQL\W2008> cd DEFAULT
PS SQLSERVER:\SQL\W2008\DEFAULT> dir
Audits
BackupDevices
Credentials
CryptographicProviders
Databases
Endpoints
JobServer
Languages
LinkedServers
Logins
Mail
ResourceGovernor
Roles
ServerAuditSpecifications
SystemDataTypes
SystemMessages
Triggers
UserDefinedMessages
PS SQLSERVER:\SQL\W2008\DEFAULT> cd databases
PS SQLSERVER:\SQL\W2008\DEFAULT\databases> dir

AUVERTISSEMENT : la colonne « Owner » ne tient pas à l'écran et a été supprimée.

Name                Status                Recovery Model  CompatLvl  Collation
----                -
cned                 Normal                Full            100        French_CI_AS

PS SQLSERVER:\SQL\W2008\DEFAULT\databases> cd cned
PS SQLSERVER:\SQL\W2008\DEFAULT\databases\cned> dir
ApplicationRoles
Assemblies
AsymmetricKeys
Certificates
DatabaseAuditSpecifications
Defaults
ExtendedProperties
ExtendedStoredProcedures
FileGroups
FullTextCatalogs
FullTextStopLists
LogFiles

```

Figure 16 : objets de SQL Server

Une fois dans la base de données, on peut exécuter toute sorte de requêtes SQL :

```
Invoke-Sqlcmd -Query "select * from matable"
```

Ce qui donne :

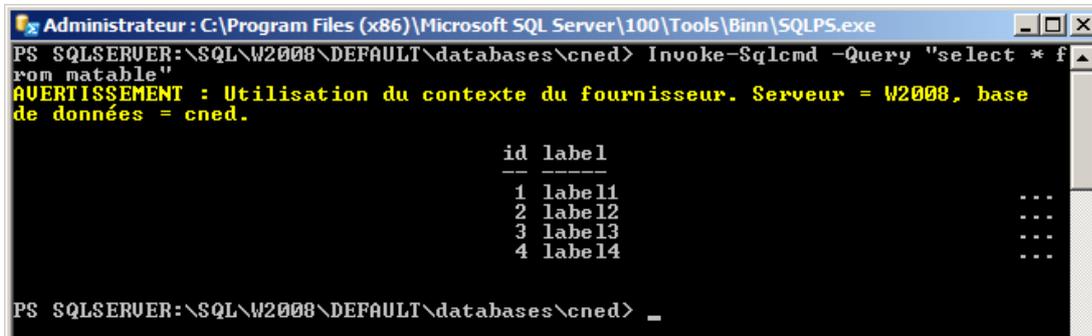


Figure 17 : exécution d'une requête SQL

6. DNS

Pour terminer, revenons au PowerShell « normal » pour faire un tour du côté du DNS et en profiter pour voir succinctement les boucles :

Lister les domaines gérés sur la machine locale :

```
Get-WmiObject -Namespace 'root\MicrosoftDNS' -Class MicrosoftDNS_Zone | select name
```

Lister toutes les adresses (enregistrements DNS de type A) :

```
$dns_entries = Get-WmiObject -namespace "root\MicrosoftDNS" -class MicrosoftDNS_Atype -Filter "DomainName = 'labocned.local'"
```

Cet objet contient maintenant tous les enregistrements :

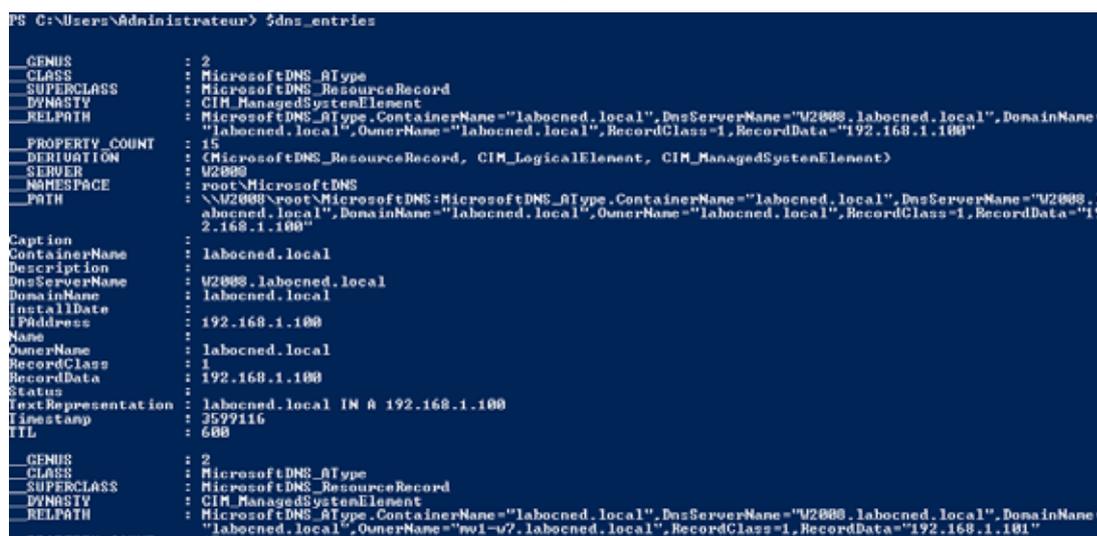
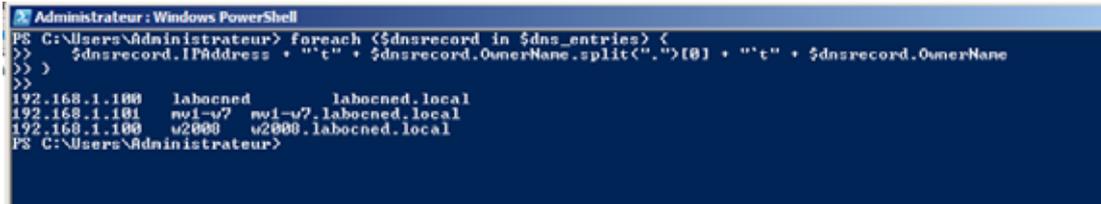


Figure 18 : résultat du parcours de l'arborescence DNS

Pour les afficher de façon structurée, nous pouvons écrire une boucle qui parcourt la collection `dns_entries` et en extrait les données intéressantes :

```
foreach ($dnsrecord in $dns_entries) {  
    $dnsrecord.IPAddress + "`t" + $dnsrecord.OwnerName.split(".") [0]  
+ "`t" + $dnsrecord.OwnerName  
}
```

Ce qui donne :



```
Administrateur : Windows PowerShell  
PS C:\Users\Administrateur> foreach ($dnsrecord in $dns_entries) {  
>> $dnsrecord.IPAddress + "`t" + $dnsrecord.OwnerName.split(".") [0]  
>> }  
>>  
192.168.1.100 labocned labocned.local  
192.168.1.101 nw1-u7 nw1-u7.labocned.local  
192.168.1.100 u2008 u2008.labocned.local  
PS C:\Users\Administrateur>
```

Figure 19 : Résultat de la boucle

7. PowerShell, domaine et scripts d'ouverture de session

Nous pouvons paramétrer notre domaine pour que lorsqu'un utilisateur ouvre une session sur une station, un script soit exécuté. Ceci est très utile dans bien des cas pour personnaliser l'environnement de l'utilisateur ou pour l'administrateur, pour faire exécuter des tâches sur les machines (déployer un logiciel, reconfigurer une imprimante, etc.).

Vous enregistrez quelque part sur votre serveur un fichier texte avec le script ci-dessous avec impérativement l'extension `ps1` :

```
$obj = New-Object -com Wscript.Network  
$obj.MapNetworkDrive("x:", "\\w2008\commun")
```

Important pour la suite (vous allez voir la bidouille pour mettre ce fichier au bon endroit). Vous copiez le fichier (clic droit sur l'icône du fichier puis « copier »).

Ensuite, vous retournez dans la gestion des stratégies. Vous créez une nouvelle GPO sur l'OU des professeurs. Ensuite, vous allez dans l'élément ci-dessous (Configuration utilisateur / Paramètres Windows / Scripts / Ouverture de session) :

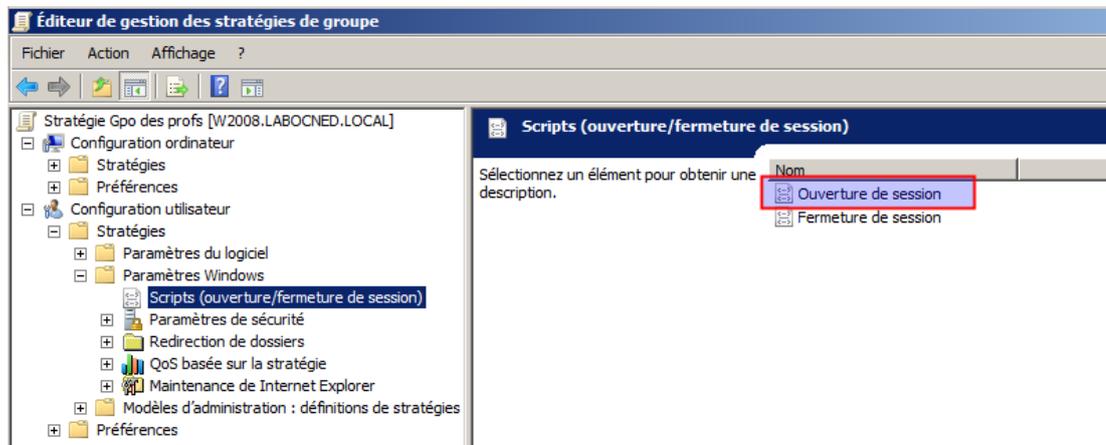


Figure 20 : Paramètre GPO

Ensuite, vous cliquez sur l'onglet « Scripts PowerShell » (l'onglet « Scripts » permet de définir des scripts pour les machines antérieures à Windows 7) puis vous cliquez sur le bouton « Afficher les fichiers... ». Celui-ci vous indique à quel endroit du système de fichiers il faut placer les scripts. Vous collez le fichier correspondant à votre script (non, vous ne rêvez pas).

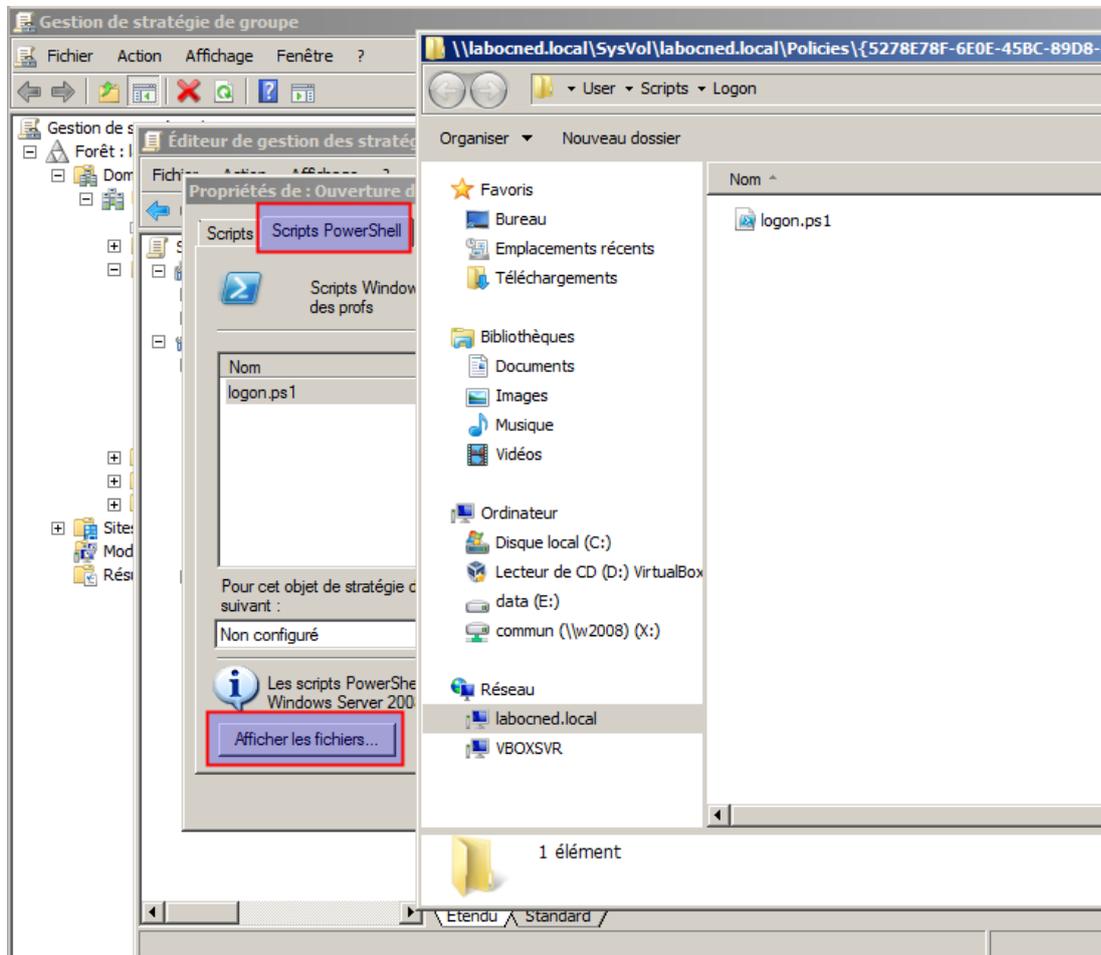
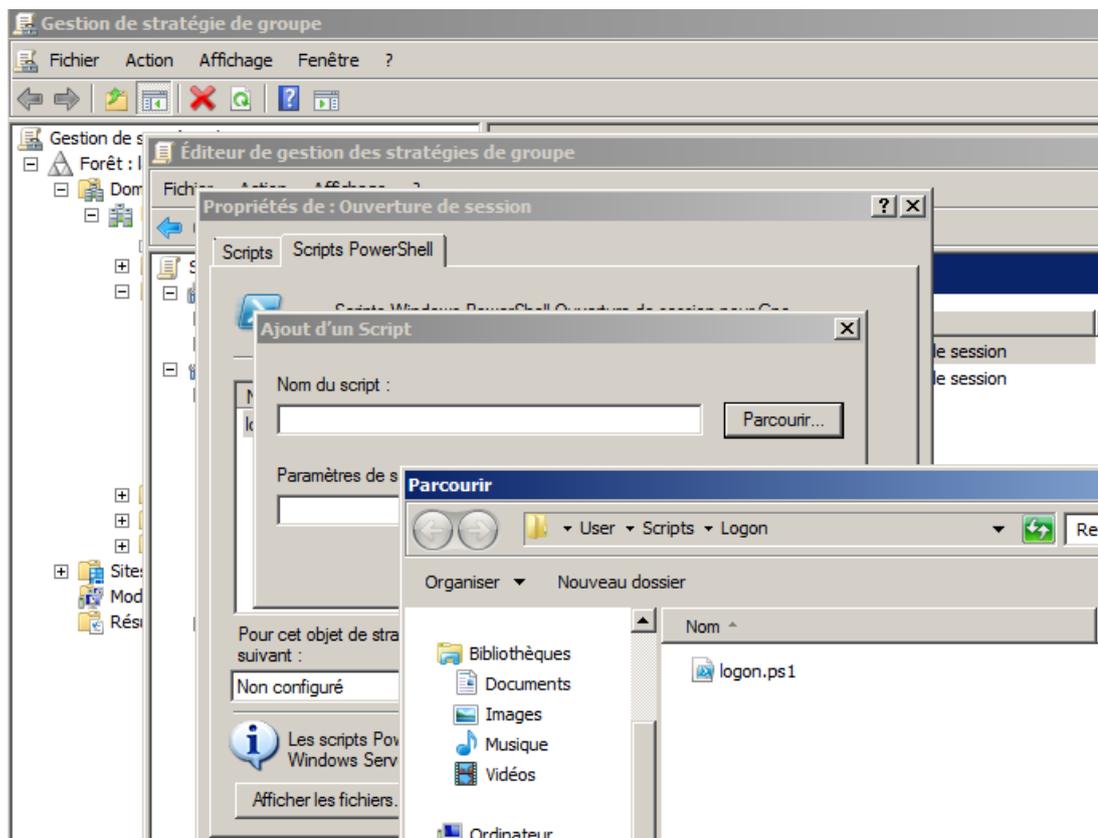


Figure 21 : copie du fichier au bon endroit

Maintenant, fermez cette fenêtre d'explorateur.

En cliquant sur « ajouter » puis « parcourir », vous pouvez récupérer votre fichier :



Atelier 9

Initiation
au PowerShell

Page 130

Celui-ci est placé dans un répertoire du style « \\labocned.local\SysVol\labocned.local\Policies\{5278E78F-6E0E-45BC-89D8-8DDC91CC8AF1}\UserScripts\Logon » qui est partagé, en vue justement de l'exécution de scripts dans le cadre des GPO.

Voilà ! Vous testez en vous connectant comme professeur. Vous devez avoir un lecteur réseau X : qui est monté (il faudra redémarrer ou faire un gpupdate /force pour que cette nouvelle stratégie s'applique).

À retenir

Le PowerShell V2 permet d'administrer intégralement Windows ainsi que tous les services installés. Son usage est indispensable lors d'installations de Windows Server en mode « core » où aucune interface graphique n'est disponible... seul un PowerShell.

Si vous voulez approfondir

Nous n'avons abordé que le dessus de l'iceberg. Consultez les nombreux sites qui parlent du sujet.

Atelier 10

Présentation de Linux Debian

▶ **Durée approximative de cet atelier : 30 minutes**

▶ **Objectif**

Pour ce module, nous tournons la page Windows pour passer à Linux, l'autre système d'exploitation serveur à connaître puisque très répandu en entreprise. Cet atelier est juste une introduction pour vous présenter un univers que vous connaissez probablement moins.

▶ **Durée approximative de cet atelier**

Aucune.

▶ **Mise en place de l'atelier**

Confortablement installé devant une machine connectée à Internet.

▶ **Matériel nécessaire**

Des gâteaux ?

Vous êtes prêt ? Allez, on y va...

▶ **Contenu**

1. **Rapide historique 132**
2. **La distribution Debian..... 133**

Atelier 10

Présentation
de Linux Debian

Page 131

1. Rapide historique

Je ne vais pas faire un historique très détaillé. Juste quelques dates et quelques noms qui me semblent importants pour votre culture.

Avant de parler de Linux, il faut parler d'Unix. La toute première version date de 1970 et s'appuie sur des travaux issus des universités américaines de Berkeley, Cambridge et Harvard (la totale quoi !). Les personnes à l'origine de ce système sont MM. Thompson, Ritchie et Kernighan¹ chercheurs des laboratoires BELL aux USA. 1972 voit la création du langage C par à peu près la même équipe. Ce langage de programmation est intimement lié à Unix car, depuis 1973, Unix est écrit en grande majorité en langage C. Tout système Unix qui se respecte intègre un compilateur C.

À l'origine, Unix n'était pas vraiment un produit commercial. Il était essentiellement diffusé auprès des universités et c'est pourquoi il était fourni avec son code source². Cela ne dura pas puisque la première version commerciale date de 1975. À partir de ce moment, des versions concurrentes d'Unix vont se développer. Chaque constructeur propose sa propre version (AIX pour IBM, HP/UX pour Hewlett Packard, Solaris pour SUN, etc.).

Au début des années 80, la plupart des ordinateurs des centres de calcul militaires et universitaires fonctionnent sous Unix. Le gouvernement américain décide de créer un réseau qui permettra d'interconnecter ces différents sites (ce qui deviendra par la suite Internet). Les recherches aboutissent au protocole TCP/IP. Le gouvernement subventionne les principaux initiateurs d'Unix pour qu'ils intègrent ce protocole à leur système d'exploitation ce qui sera fait très rapidement. C'est pourquoi, Unix, Internet et TCP/IP sont fortement liés. Cela explique également que TCP/IP est devenu un standard de fait dans le domaine des protocoles de communication.

Vers la fin des années 80, la fronde s'organise pour revenir aux sources³ d'Unix. Le projet GNU (**G**NU is **N**ot **U**nix) a pour objectif (entre autres) de remettre Unix dans le domaine public. Sur une base de volontariat, les participants au projet GNU conçoivent un Unix disponible gratuitement accompagné de ses sources.

Au cours de l'année 1991, un étudiant finlandais, nommé Linus Torvalds, a acheté un micro-ordinateur de type PC, afin d'étudier la programmation du microprocesseur i386. Ne voulant pas être limité par MS/DOS, il a tout d'abord utilisé un clone d'Unix, peu cher, appelé Minix. Minix possède lui-même certaines limitations qui, bien que moins importantes que celles de MS/DOS, sont assez gênantes (limitation de la taille des exécutables à 64 kilo-octets, limitation des systèmes de fichiers à 64 méga-octets, temps de réponse trop longs, etc.). Aussi, Linus Torvalds a commencé à réécrire certaines parties du système afin de lui ajouter des fonctionnalités et de le rendre plus efficace. Il diffuse le code source de son travail via Internet. La première version de Linux (version 0.1 en août 1991) était née.

Cette version, ses sources sont encore aujourd'hui disponibles à télécharger sur Internet. Et vous pouvez donc regarder le code de programmation dans un éditeur !

Cette base très rudimentaire à l'époque sera reprise par une flopée de développeurs de toutes nationalités. Après des années de travail intensif et reliés par Internet, ils ont pro-

1. Personnages célèbrissimes du monde informatique. Il faut savoir que le langage C est le père de nombreux autres langages (C++, C#, Java, php, etc.)
2. Le code source est un peu la recette de fabrication du logiciel. Un informaticien peut la lire et éventuellement la modifier pour ses propres besoins. La plupart des éditeurs refusent farouchement de fournir les codes sources car, d'une certaine manière, ils contiennent des « secrets de fabrication ».
3. Hé !Hé ! c'est le cas de le dire...

duit un véritable système d'exploitation, réputé pour être stable et fiable. Il se répand dans les entreprises à tel point que les majors de l'informatique (IBM, Compaq, Oracle, SUN, etc.) intègrent cet OS pour leurs ordinateurs ou adaptent leurs logiciels phares pour ce système.

Linux est associé à des concepts originaux. C'est un logiciel libre :

- liberté d'étudier comment le programme fonctionne et de l'adapter à ses besoins : accès au code source ;
- liberté de redistribuer des copies ;
- liberté d'améliorer et de diffuser ses améliorations de sorte que toute la communauté en profite.

Vous notez que le terme « gratuit » ne figure pas. En effet, il est laissé la liberté de donner ou de vendre un logiciel libre.

Le projet GNU initié par la FSF (Free Software Foundation – www.gnu.org) de Richard Stallman englobe un éventail très large de logiciels développés dans l'esprit du copyleft. Ce concept est l'opposé du copyright, puisqu'il oblige toute personne qui développe ou modifie un logiciel sous cette licence à transmettre son droit de copie et de modification. Vous verrez souvent dans l'univers Linux des logiciels sous licence GPL (Gnu Public License).

2. La distribution Debian

2A. Qu'est-ce qu'une distribution ?

Commençons par une petite recherche Wikipedia : http://fr.wikipedia.org/wiki/Distribution_Linux

Une distribution Linux (ou distribution GNU/Linux) est un ensemble cohérent de logiciels rassemblant un système d'exploitation composé d'un noyau Linux et de logiciels issus du projet GNU et des logiciels supplémentaires - le plus souvent Libres.

Consultez le lien pour plus d'informations.

2B. Quelles sont les principales distributions ?

Certains d'entre vous ne connaissent pas Linux, d'autres ont déjà en tête des noms, d'autres encore sont peut-être des partisans de telle ou telle distribution...

Eh oui l'esprit de liberté qui anime les linuxiens a engendré des familles de produits appelées distributions. Certaines ont pris des allures commerciales comme Red Hat, Mandriva ou Suse (nous avons souligné plus haut que le mot libre ne signifie pas forcément gratuit...).

D'autres ont tenu à respecter l'état d'esprit Linux à la lettre : Slackware, Debian (Ubuntu est une dérivée de Debian).

2C. Pourquoi avoir choisi Debian ?

La structure dans laquelle je travaille héberge sur différents serveurs de nombreux sites ou applications webs de toutes natures (Sip, Joomla, Apache, Tomcat, Java, Php, Perl, Python, etc.). Le point commun entre tous ces serveurs est le système d'exploitation : Debian Linux depuis au moins la Sarge (avant je n'étais pas là !).

Après 5 ans d'expérience avec ce système, je peux témoigner de sa très grande fiabilité et des conditions agréables d'administration. C'est vrai : un système Debian Linux peut fonctionner plusieurs mois sans redémarrage en absorbant régulièrement toutes les mises à jours envoyées par l'éditeur. Néanmoins, le tableau n'est pas totalement rose : les mises à jour majeures sont difficiles à mener et nécessitent de faire un gros travail de qualification auparavant sur une maquette. À moins d'être une tête brûlée :-)

Atelier 10

Présentation
de Linux Debian

Page 134

Atelier 11

Installation de Linux Debian

► Durée approximative de cet atelier : 2 heures

► Objectif

À la fin de cet atelier, vous saurez installer un système Linux opérationnel. Nous vous proposons ici un schéma d'installation directement issu de nos serveurs d'entreprise actuellement en production.

► Conditions préalables

Aucune, ce n'est pas une application directe du cours et nous développons ici ce qui peut être nouveau pour vous.

► Considérations techniques

Cet atelier (et donc les suivants) ont été réalisés avec la dernière version stable de Debian à ce jour (08/2011) : Debian Squeeze 6.0.2. Nous travaillerons avec la version « netinst » (version minimale qui récupère ensuite les logiciels nécessaires par Internet). Vous trouverez toutes les images ISO des cédéroms ici :

<http://www.debian.org/CD/netinst/>

Vous choisissez l'image adaptée à votre machine physique ou à votre machine virtuelle (en général i386 ou amd64).

Nous passerons le temps nécessaire sur la partie formatage et partitionnement et je vous donnerais une configuration type, telle que celle que nous utilisons en entreprise (LVM et XFS).

► Que faire si je bloque ?

La documentation complète : <http://www.debian.org/releases/stable/i386/>

La documentation « rapide » sur l'installation : <http://www.debian.org/releases/stable/i386/apa.html.fr>

► Contenu

1. Virtualisation	136
2. Installation	136

1. Virtualisation

Vous créez une machine virtuelle en choisissant le type de système d'exploitation adapté. Nous n'utiliserons pas l'interface graphique, 512Mio de mémoire seront suffisants.

Pourquoi pas d'interface graphique ? Pour des raisons de sécurité, de souplesse d'administration et de surcharge inutile de la machine, nous faisons toute notre administration serveur en ligne de commande. J'en profite pour vous rappeler que nos amis de Microsoft s'y sont mis aussi (recherchez Windows 2008 server **core** sur le net)... avec seulement 25 ans de retard. Mais, allez nous ne sommes pas là pour troller ;-)

Si vous voulez tester les interfaces graphiques de Linux (Kde, Gnome, etc.), créez-vous une autre machine virtuelle !

Pour les besoins de l'atelier, nous lui affecterons 2 disques virtuels de 8Gio chacun. Vous créez le premier pendant la création de la machine virtuelle. Pour le deuxième, il faudra aller dans la partie « Stockage » de la machine et cliquer sur l'icône « Ajouter disque dur » à côté du contrôleur de disque (SATA chez moi). Enfin, pensez à passer le réseau en mode « pont » et non « NAT ».

2. Installation

Nous ne détaillerons pas tous les écrans mais nous nous concentrerons sur ceux qui présentent un intérêt ou une difficulté. Nous passons donc sur les premiers écrans et nous allons nous arrêter sur la partie la plus délicate : le partitionnement et le formatage.

Dans les premiers écrans, la seule chose importante, pour être cohérent avec la configuration de la machine Windows, c'est d'indiquer :

- nom de machine : mv2-linux
- domaine : labocned.local

Linux vous demande le mot de passe pour l'administrateur root. Puis vous oblige à créer un utilisateur « normal » : vous l'appellez usercned.

2A. Partitionnement et formatage

2A1. Introduction

Voici un des pires cauchemars de l'administrateur réseau : **mon serveur de gestion commerciale est complètement planté car la partition est pleine !!! Il n'est plus possible de faire des factures ou des tickets de caisse !!! Comment faire, alors que mon patron passe régulièrement dans mon bureau pour me passer un savon !!!**

Linux nous propose tous les outils pour éviter que ce scénario catastrophe ne se produise (ou au moins pour apporter rapidement et tranquillement une réponse). Mais il faut impérativement faire les bons choix lors de l'installation, sinon c'est irréversible.

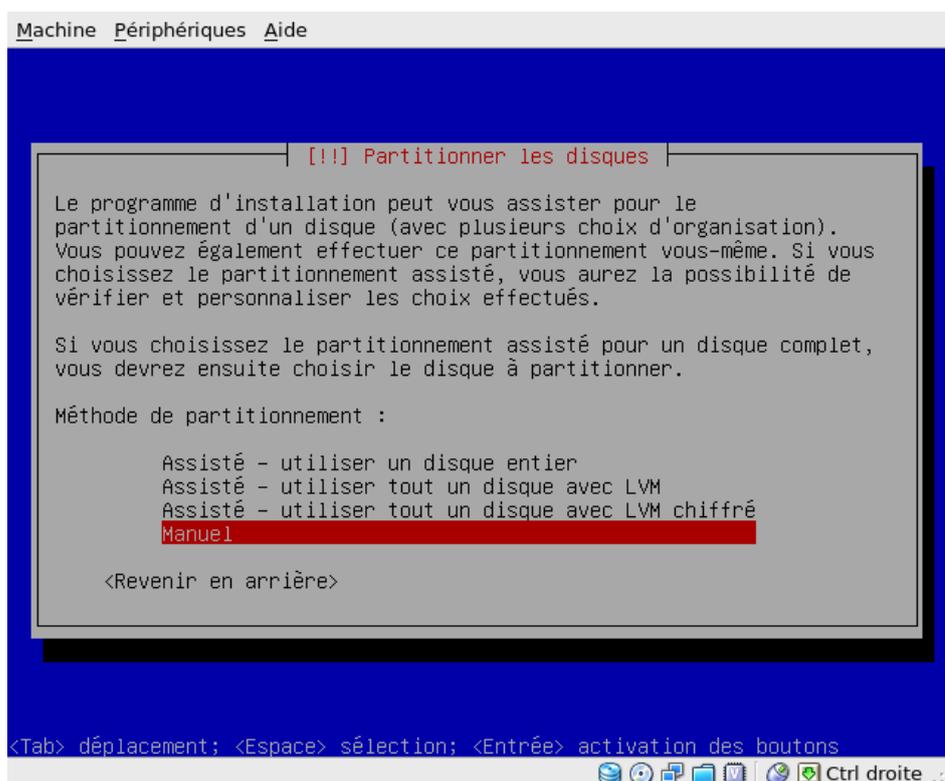
Quelles sont les idées à retenir ?

1. Jamais une seule partition avec tout dedans mais plusieurs partitions suivant l'usage (nous verrons cela en détail ensuite) : « ne pas mettre tous ses oeufs dans le même panier ».
2. Vous ne connaissez pas à l'avance l'espace disque nécessaire : pour éviter les mauvaises surprises, on se garde de l'espace libre sous la main afin de l'utiliser où et quand cela sera nécessaire.

3. Vous aviez prévu large mais votre disque physique est quand même saturé : on ajoute un deuxième disque mais celui-ci viendra en addition du premier. Le système ne verra toujours qu'un seul disque mais plus grand !

Je vous préviens à l'avance : cette séquence est relativement longue, voire pénible. Néanmoins, elle est indispensable : c'est un investissement que vous apprécierez par la suite ! Donc, courage...

Le premier écran traitant de ce sujet est le suivant :



Atelier 11

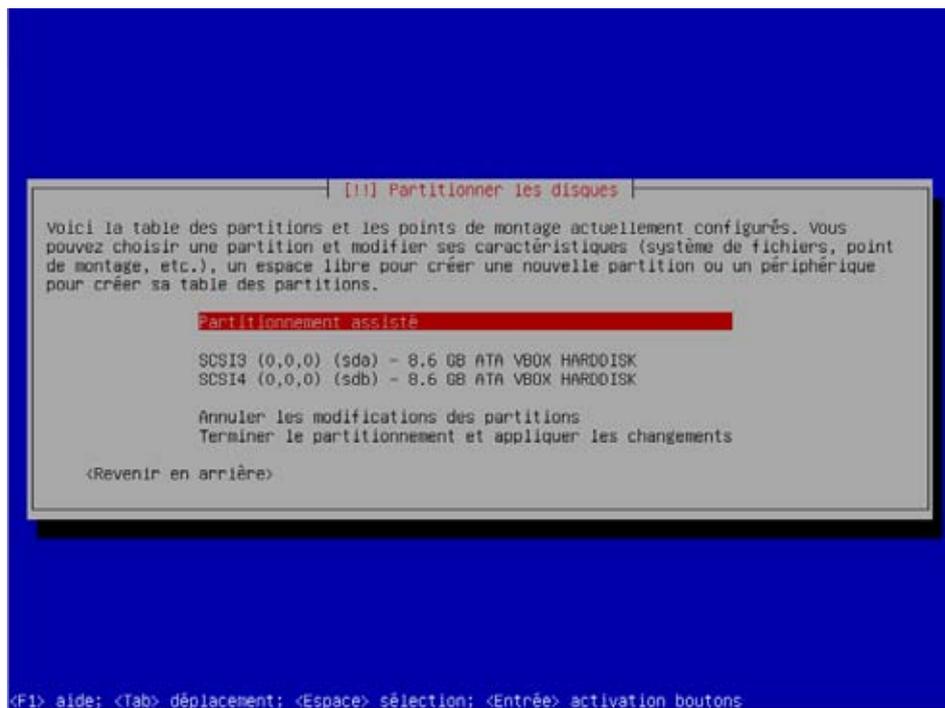
Installation de Linux Debian

Page 137

Avant d'aller plus loin, comme cette séquence est relativement longue et dense, je vous donne immédiatement notre objectif d'organisation de nos disques :

Disques physiques	Découpage logique		Système de fichiers	Point de montage	Espace	
Disque 1 8,6Gio	Partition 1	sda1	ext3	/boot	250Mio	
	Groupe de volumes LVM vg0		Volume logique 0	xfs	/home	1.3GiO
Disque 2 8,6Gio			Volume logique 1	xfs	/	250MiO
			Volume logique 2	swap	swap	512MiO
			Volume logique 3	xfs	/tmp	100MiO
			Volume logique 4	xfs	/usr	1,4GiO
			Volume logique 5	xfs	/var	600MiO
		Espace libre				

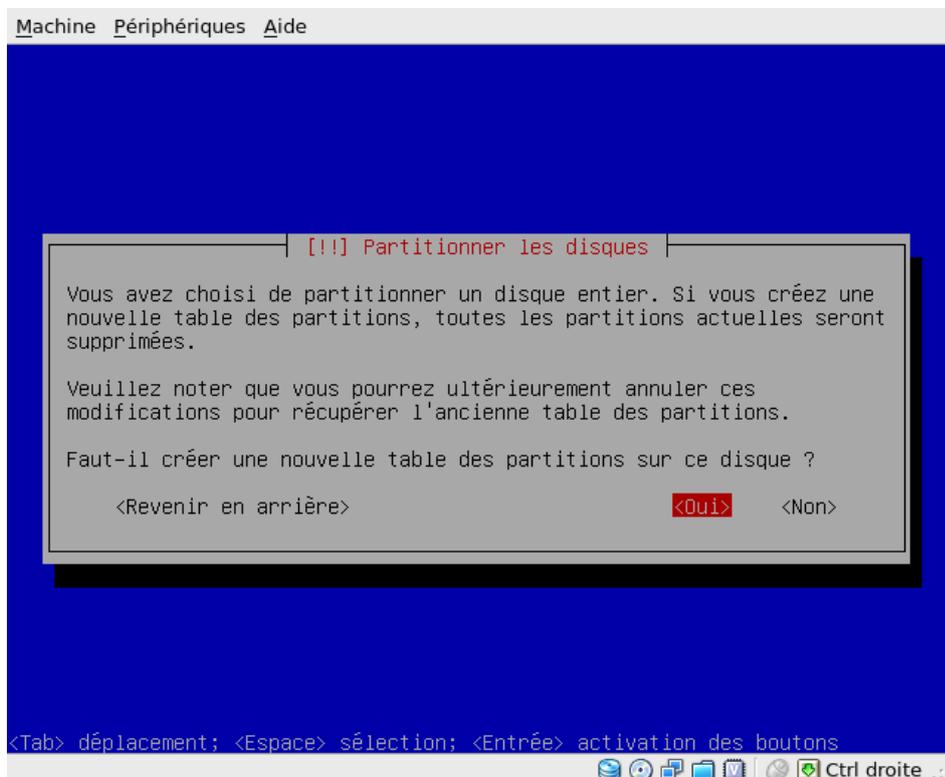
Nous choisissons « manuel » afin de plier notre machine à nos besoins !



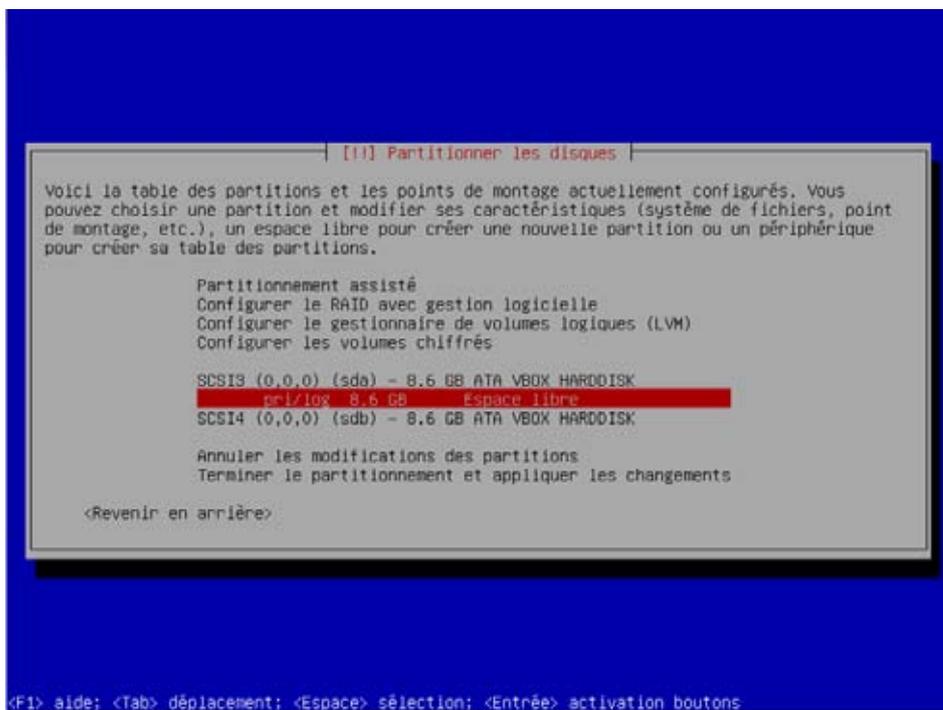
Nous retrouvons ici nos deux disques durs. Dans un premier temps, nous allons créer une partition « classique » pour le démarrage du système sur le premier disque dur.

Vous déplacez le curseur rouge sur le premier disque dur puis vous appuyez sur « Entrée ».

Atelier 11



« OUI » ! Comme ces disques sont totalement vierges, il n'existe pour le moment aucune partition.



Maintenant vous sélectionnez l'espace libre du premier disque.

Comment s'appellent les unités de disque sous Linux ? Vous avez très certainement l'habitude de voir sous Windows vos unités de disque s'appeler A:, C:, D:, etc. Sous Linux, c'est totalement différent. Les conventions suivantes ont été prises :

- Pour les unités de disquette : on aura « fd » (fd pour floppy disk) suivi d'un numéro identifiant le lecteur.
- Pour les unités de disque dur ou les lecteurs du type cédérom, dévédérom,... on aura :
 - deux lettres indiquant la norme (hd pour la norme IDE ou sd pour les normes SCSI/SAS/SATA/RAID) ;
 - une lettre identifiant l'unité physique (a pour la première, b pour la deuxième, etc.) ;
 - un numéro identifiant la partition sur l'unité physique (1 pour la première, 2 pour la deuxième, etc.)

Ces dénominations peuvent sembler complexes mais elles ont l'avantage, lorsqu'on les manipule, d'indiquer avec précision l'organisation des disques et des partitions sur l'appareil (lorsque l'on utilise D: comment savoir sur quel disque physique il se trouve et de quelle partition il s'agit ?)

Exemple :

Imaginons un ordinateur avec :	On aura les noms d'unités suivants :
un lecteur de disquette 3"1/2	fd0
un premier disque dur IDE composé de 3 partitions	hda1, hda2, hda3
un deuxième disque dur IDE composé d'une seule partition	hdb1
un lecteur IDE de DVD	hdc1

Normalement, vous avez compris la logique. Hum, voyons cela avec un petit exercice :

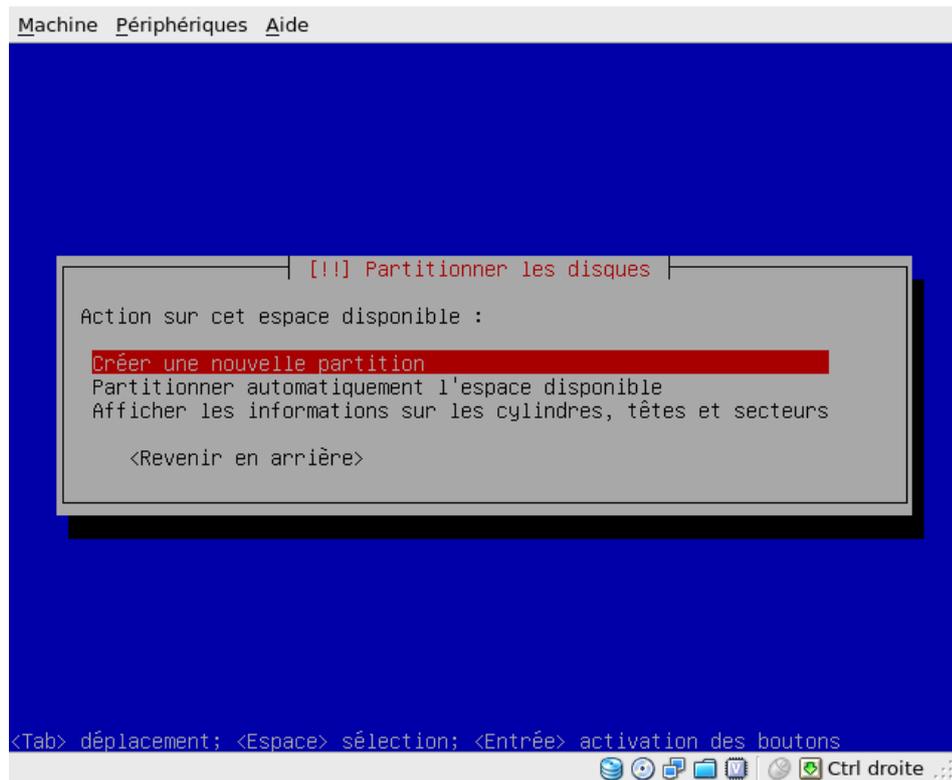
Exercice 1

Imaginons un ordinateur avec :

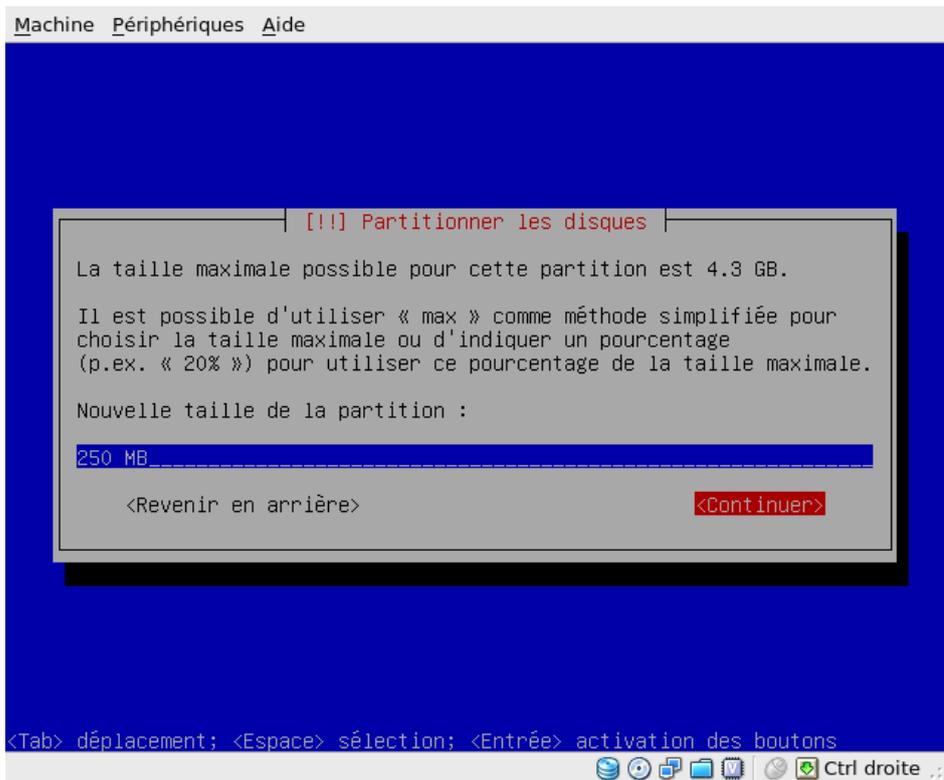
- un lecteur de disquette 3»1/2 ;
- un disque dur SCSI composé de 2 partitions ;
- un disque dur maître sur le premier canal IDE et composé d'une seule partition.

Donnez-moi les noms d'unités (sans regarder la réponse !), vous avez 10 secondes.

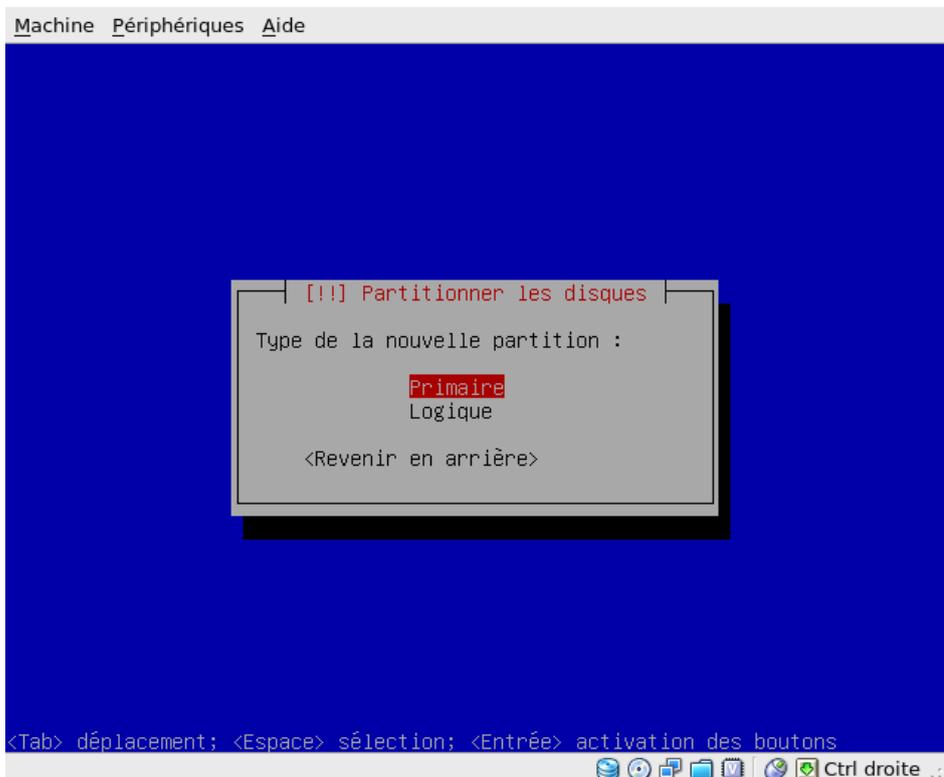
Continuons les manipulations.



Vous choisissez « Créer une nouvelle partition ».



250 Mio seront suffisants pour cette partition qui ne contient que le noyau Linux.



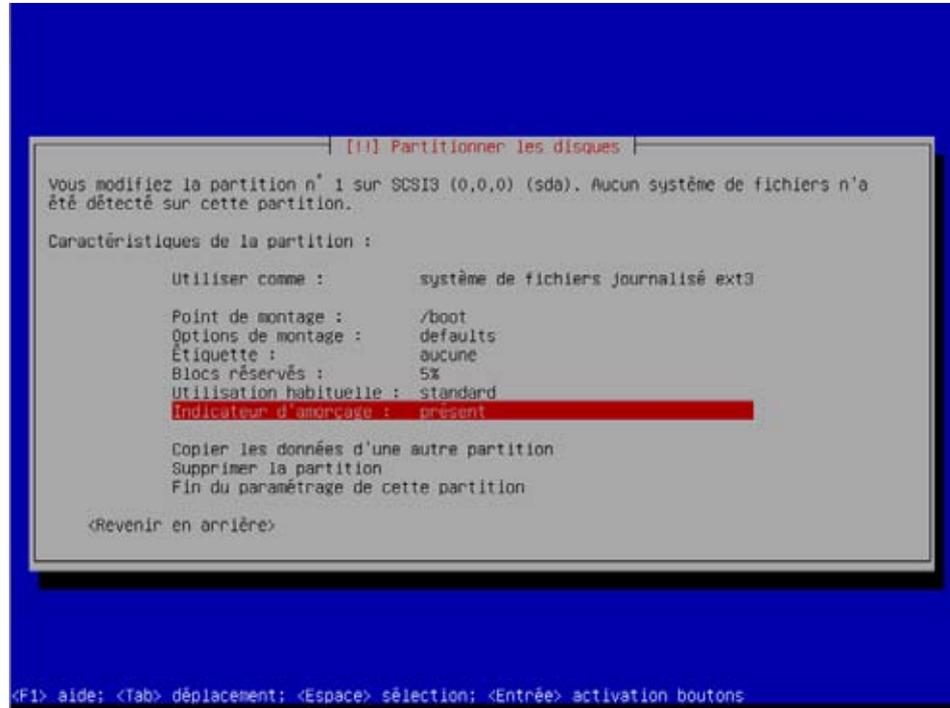
Atelier 11

Installation
de Linux Debian

Page 141

Vous choisissez « Primaire ». Pour la distinction « Primaire » / « Logique », je vous renvoie vers votre premier module de cours ou à http://fr.wikipedia.org/wiki/Partition_de_disque_dur.

Vous la positionnez ensuite au début du disque.



Atelier 11

Installation
de Linux Debian

Page 142

Les trois informations à renseigner ici sont le système de fichiers, le point de montage et l'indicateur d'amorçage présente (donc, partition de démarrage). Je serai bref concernant le système de fichiers. Retenez que ext3 est à Linux ce que NTFS est à Windows. Il est donc sécurisé (droits d'accès utilisateurs) et journalisé (même idée que pour les bases de données : récupération des données en cas d'arrêt brutal du serveur).

Qu'est-ce que le point de montage ?

Vous voyez sur cet écran « Point de montage : /boot ». La notion de « montage » est une spécificité des systèmes d'exploitation comme Unix (n'oubliez pas que ces systèmes robustes datent des années 60-70 dans leur conception initiale). Vous avez peut-être vu des images des salles informatiques de cette époque. On y voit de grandes armoires dans lesquelles tournent des bandes, un peu comme des pellicules de cinéma. À l'époque, ces bandes étaient utilisées pour y stocker des fichiers, si bien que lorsque l'ordinateur avait besoin d'utiliser des données stockées sur une certaine bande, une personne du service informatique (un pupitreur) devait :

- taper une commande sur le clavier pour informer l'ordinateur qu'il allait retirer une bande ;
- se déplacer pour enlever (démonter) la bande présente dans le lecteur ;
- mettre (monter) l'autre bande ;
- taper une commande sur le clavier pour informer l'ordinateur que la nouvelle bande était en place.

Ce mécanisme est toujours en vigueur sous Linux et a été généralisé à l'ensemble des mémoires de masse (disquettes, disques durs, cédéroms, etc.) ! Il y a certes un mécanisme d'automatisation de cette manipulation, mais vous aurez peut-être parfois à « démon-

ter » le lecteur de CD-Rom pour pouvoir récupérer votre CD (n'allez pas alors me chercher un tournevis ! Pensez à cette notion de « point de montage » : emplacement de l'arborescence logique avec laquelle Linux gère les ressources...).

Car une autre spécificité d'Unix est que toutes les unités de disques (qu'elles soient physiquement connectées à votre ordinateur ou accessibles au travers d'un réseau) constituent, dès lors qu'elles sont dites « montées », une seule et même arborescence. Le point de départ de ce système de fichiers s'appelle root¹. Il est symbolisé par la barre de division / (le slash).

Exemple :

Supposons que l'on ait l'organisation suivante :

Sur disque dur (hda1 par exemple) :	Sur disquette (fd0) :
/	/
/bin	/textes
/etc	/feuilles
/mnt	/bd
/mnt/floppy	

Si l'on monte la disquette dans le répertoire /mnt/floppy, on obtient la nouvelle arborescence :

```
/
/bin
/etc
/mnt
/mnt/floppy
/mnt/floppy/textes
/mnt/floppy/feuilles
/mnt/floppy/bd
```

D'un point de vue « logique », c'est à dire fonctionnel, il n'y a qu'une seule arborescence, les unités physiques viennent s'y greffer, on dit « monter » !

¹ Attention, sous Unix beaucoup de choses s'appellent root (en particulier, c'est le nom de connexion de l'administrateur).

Dernier point, arborescence type d'un système Linux (*nix) :

/	la racine, ne contient généralement pas de fichier, mais c'est le point de départ de l'arborescence.
/boot	fichiers nécessaires au démarrage
/dev	contient les points d'entrée des périphériques.
/etc	très important, contient tous les fichiers de configuration : autant dire que nous allons passer pas mal de temps dans ce répertoire.
/home	comptes utilisateurs
/bin	commandes « de base » du système accessibles à tous
/sbin	commandes « de base » du système accessibles uniquement aux administrateurs
/root	répertoire personnel de root, l'administrateur
/lib	librairies
/var	contient les données du système (sites webs, bases de données, etc.)
/var/log	contient tous les journaux du système. C'est ici que commence la surveillance et le dépannage d'un système Unix.
/usr	commandes complémentaires du système et applications installées.
/tmp	fichiers temporaires

Atelier 11

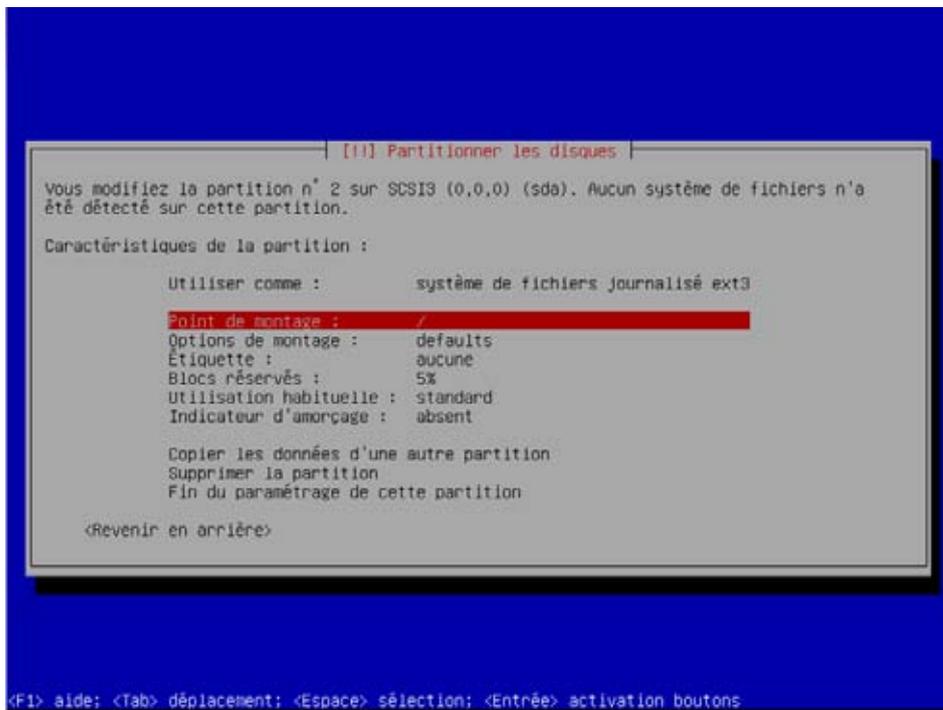
Le point de montage / sera créé un peu plus tard.

Pensez à mettre « indicateur d'amorçage » présent et choisissez « Fin du paramétrage de cette partition ».

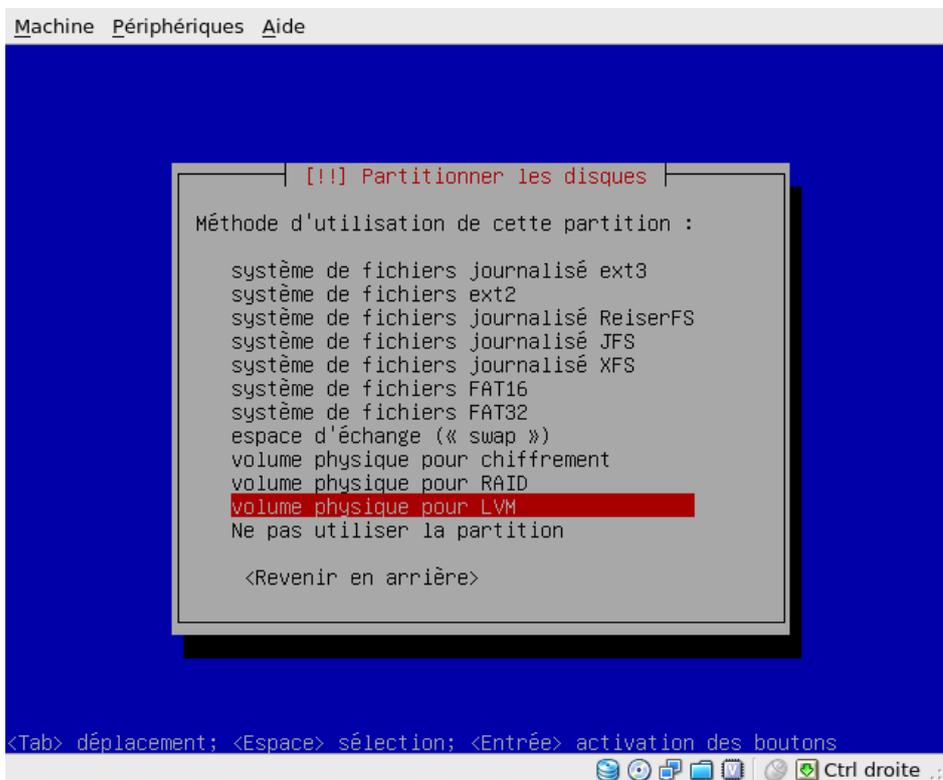
Nous poursuivons sur la partie LVM (ou Logical Volume Management) qui permet de gérer, sécuriser et optimiser de manière souple les espaces de stockage en ligne dans les systèmes d'exploitation de type UNIX/Linux (pour plus de détails, voir Wikipedia).

Lorsque vous êtes revenu à l'écran de partitionnement des disques, vous prenez l'espace libre restant sur le premier disque.

Vous créez une nouvelle partition primaire de tout l'espace restant, ce qui nous amène à cet écran déjà familier :



Dans « utiliser comme », vous allez indiquer « Volume physique pour LVM » :

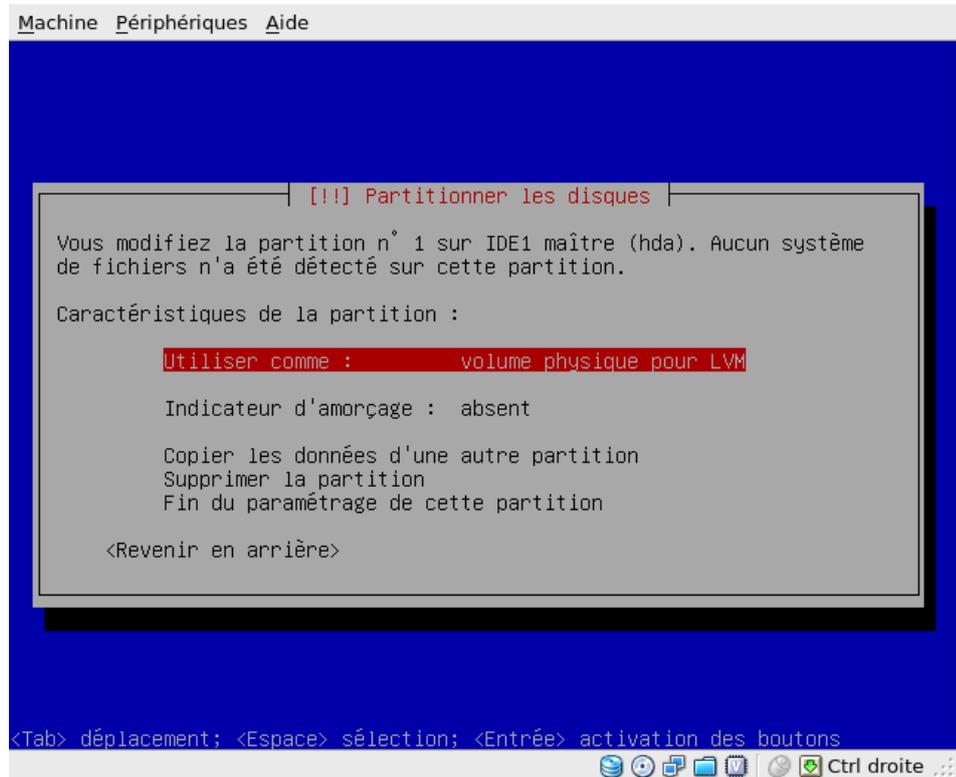


Atelier 11

Installation
de Linux Debian

Page 145

Aucun autre paramétrage n'est nécessaire à cette étape :



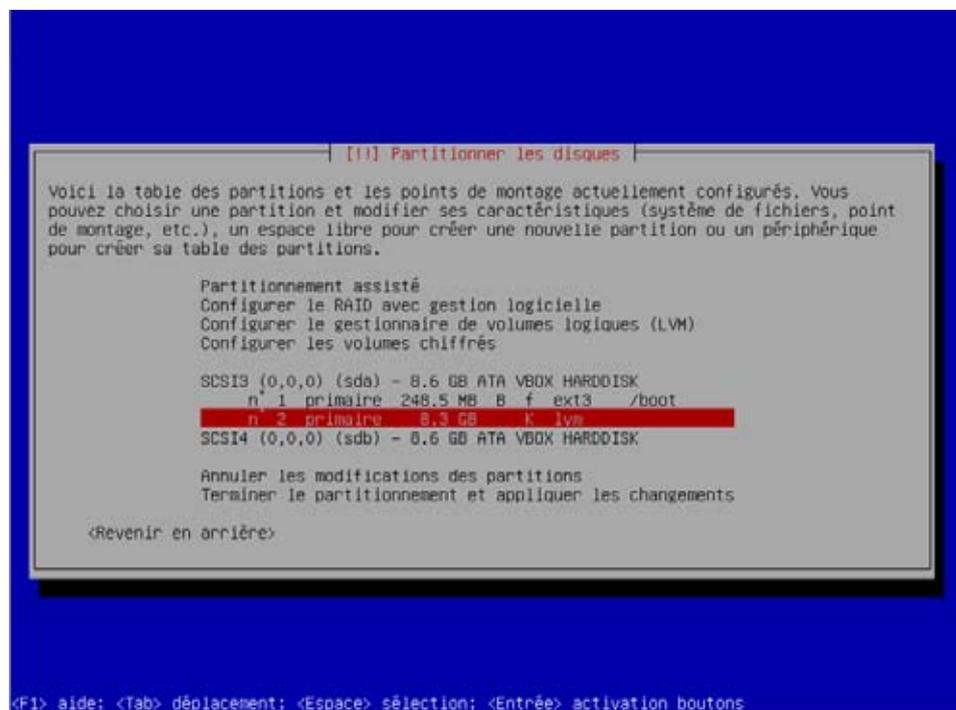
Atelier 11

Installation
de Linux Debian

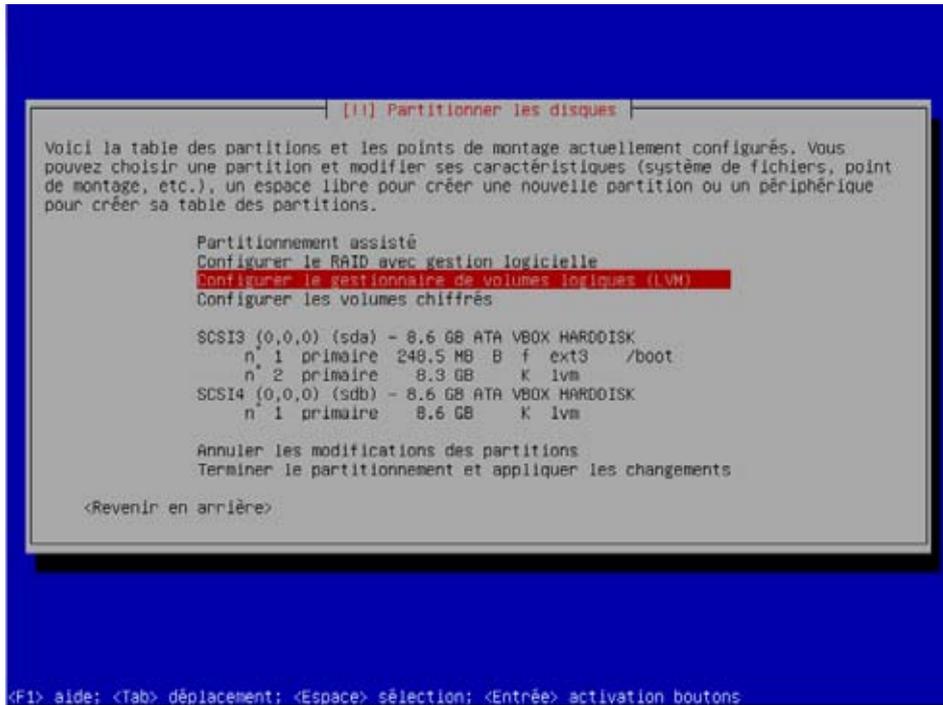
Page 146

Vous faites « Fin du paramétrage ».

Voici donc le résultat à cette étape :

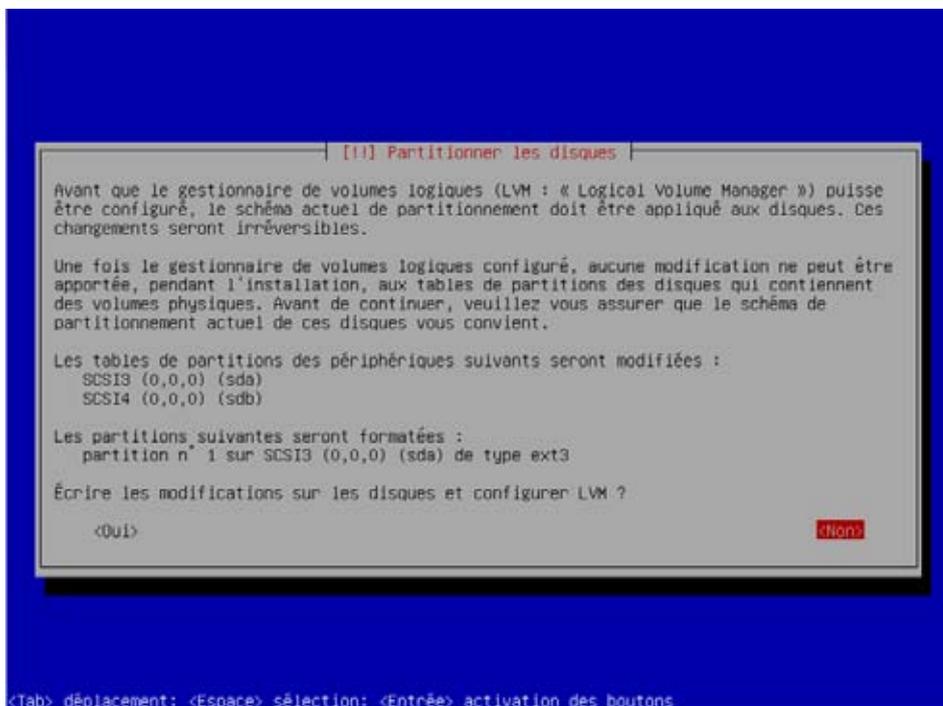


Vous recommencez la même manipulation pour le deuxième disque. Ce qui nous donne :

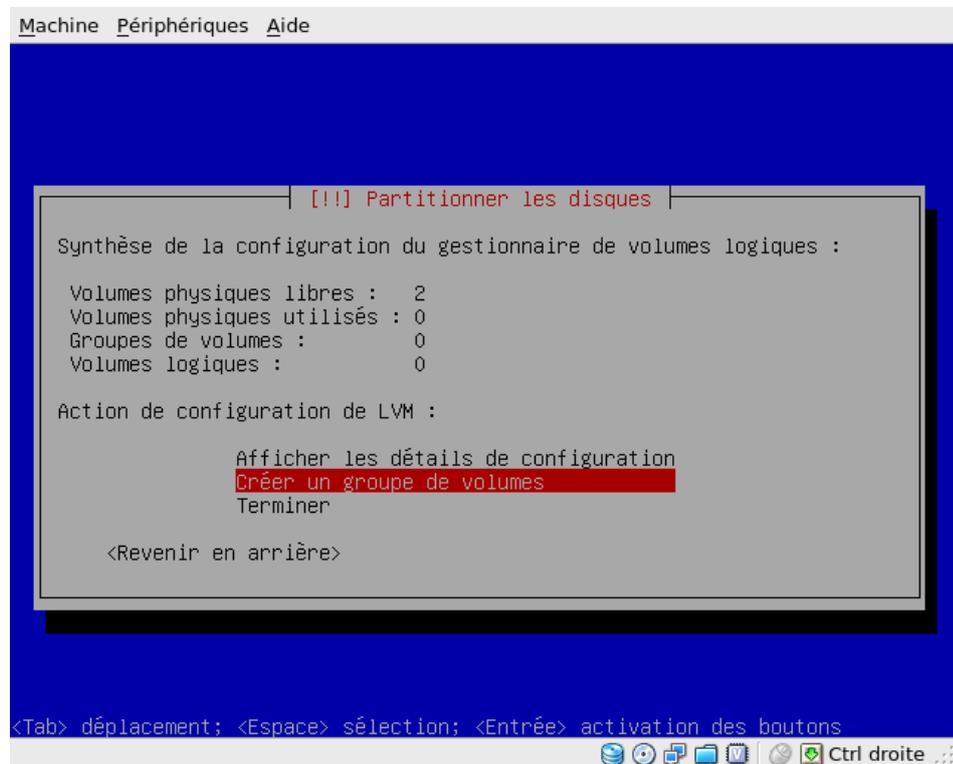


Choisissez maintenant « Configurer le gestionnaire de volumes logiques LVM ». Nous allons créer un groupe de volumes constitué des espaces LVM de chacun des disques. Notre Linux ne verra plus alors qu'un seul « disque » de 16Gio constitué par les 2 unités physiques.

Un petit écran de confirmation :



Cet écran nous indique que nous avons deux volumes physiques libres, ce qui est conforme aux manipulations précédentes.

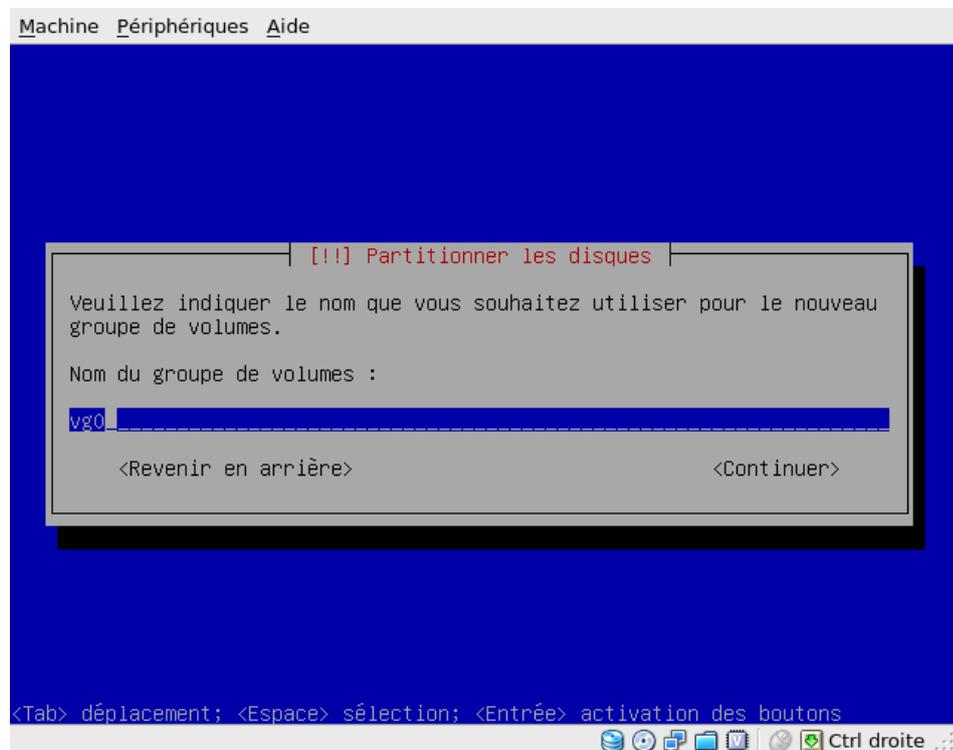


Atelier 11

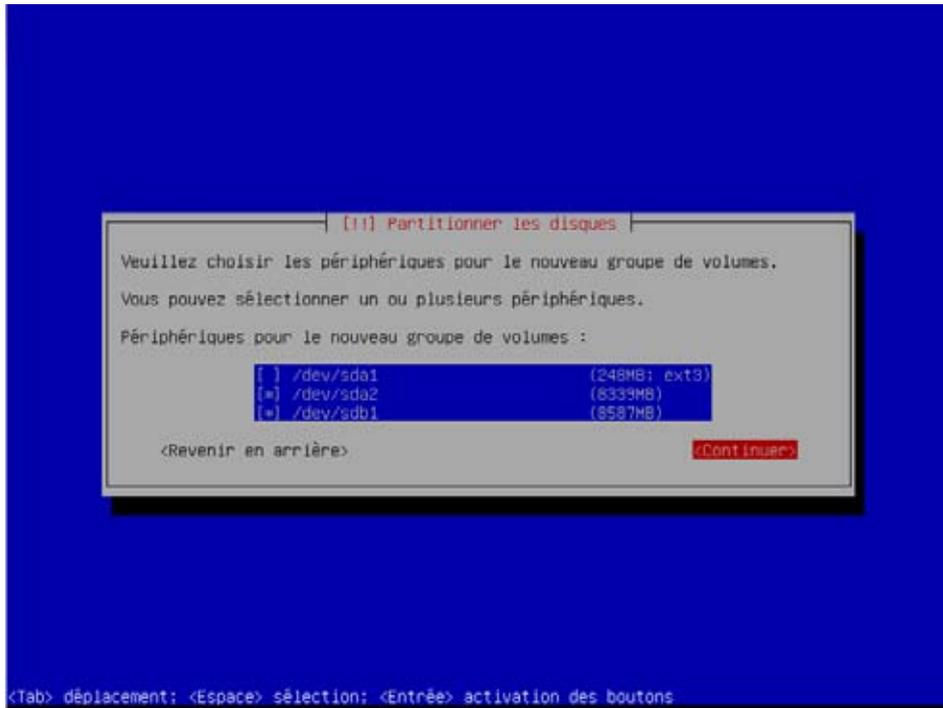
Installation
de Linux Debian

Page 148

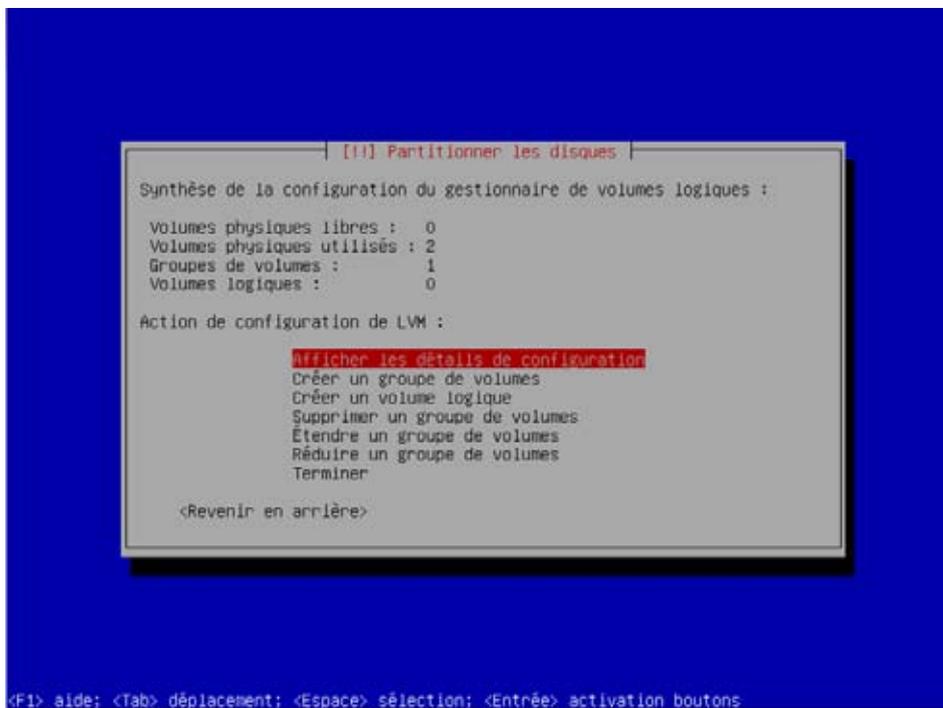
Nous choisissons de « Créer un groupe de volumes ».
Étant totalement à court d'imagination, je l'appelle vg0 :



Nous choisissons les deux volumes physiques (nous ne prenons pas la partition de boot) :



Nous allons maintenant créer la série de volumes logiques dont nous avons besoin. Pour simplifier, disons qu'un volume logique est à peu près équivalent à une partition (sauf qu'il peut être réparti sur plusieurs disques physiques).

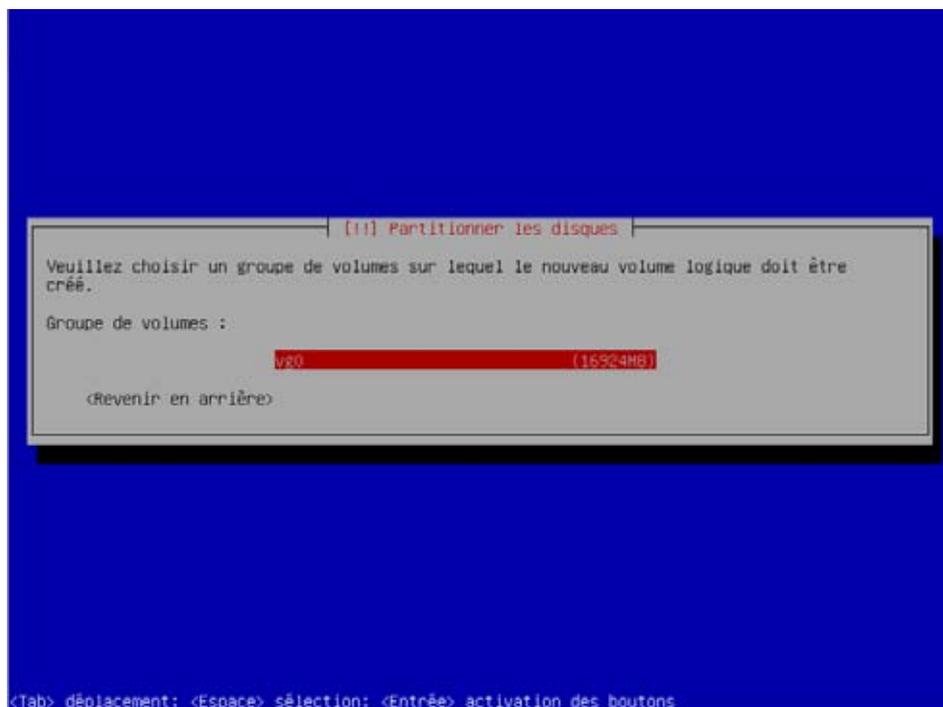


Atelier 11

Installation
de Linux Debian

Page 149

Nous allons maintenant créer un nouveau volume (vous remarquerez au passage qu'il est possible de configurer plusieurs groupes de volume) :



Atelier 11

Voici le schéma que je vous propose :

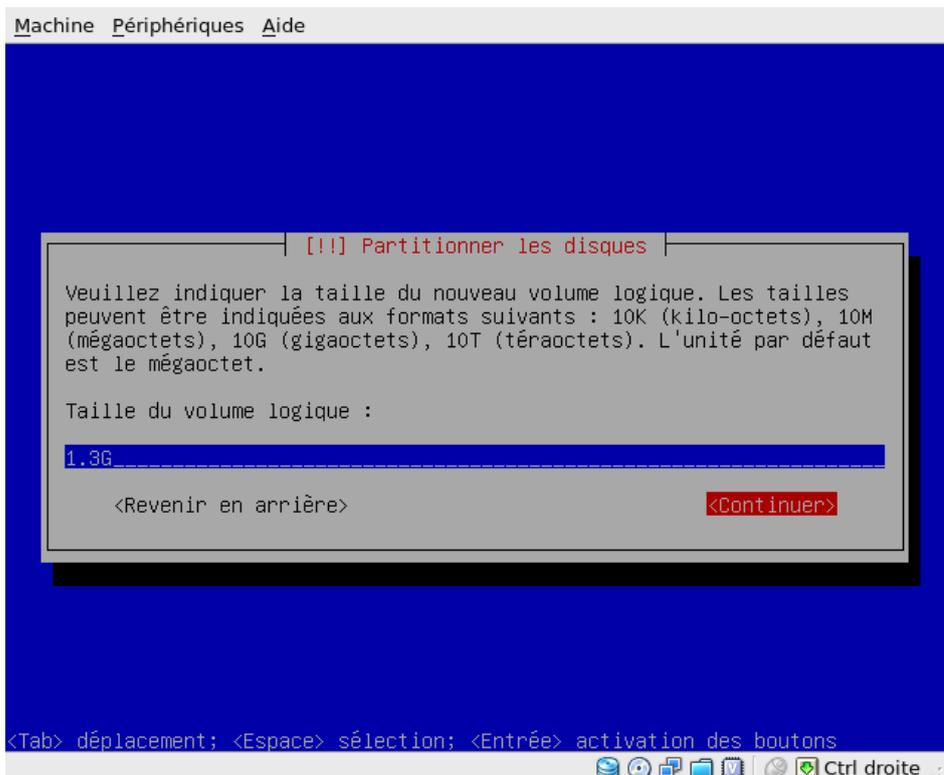
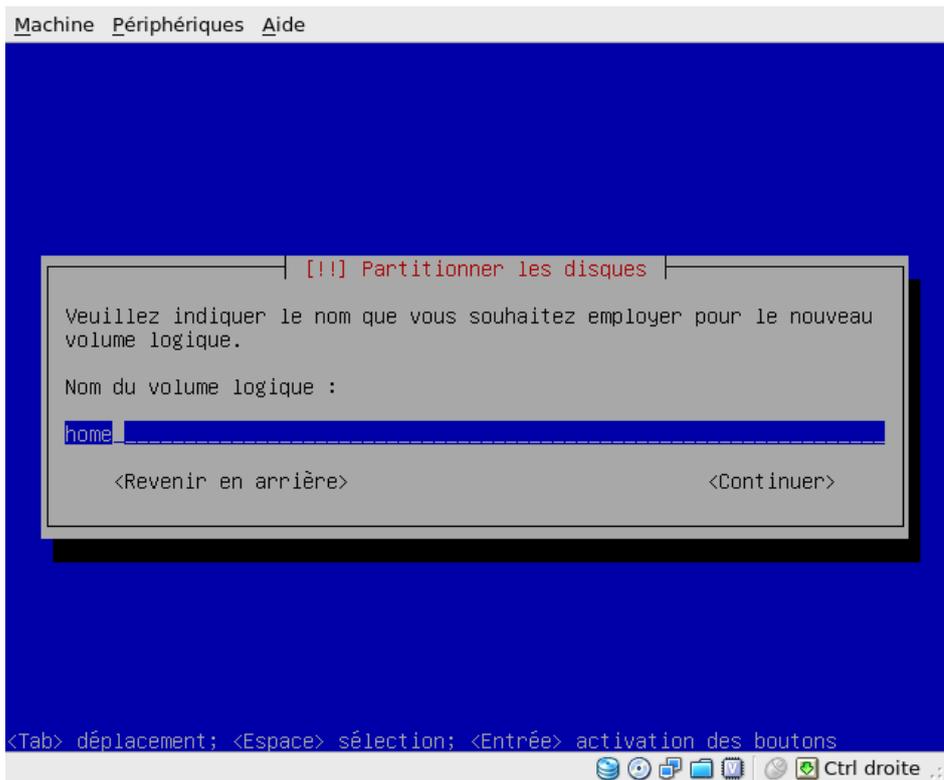
Nom du volume logique	Taille
home	1.3 GiO
root	250 MiO
swap	512 MiO
tmp	100 MiO
usr	1,4 GiO
var	600 MiO

Deux remarques :

- les noms des volumes n'ont pas d'importance. Néanmoins, il est préférable de prendre un nom en fonction des points de montage que nous ajouterons ensuite ;
- la taille du volume swap est fonction de la mémoire vive de votre machine. En général, on prend autant que de mémoire vive dans la limite de 2GiO.

La partition de swap est l'équivalent du fichier pagefile.sys sous Windows.

À vous de jouer maintenant ! Vous indiquez pour chaque volume logique un nom et une taille.

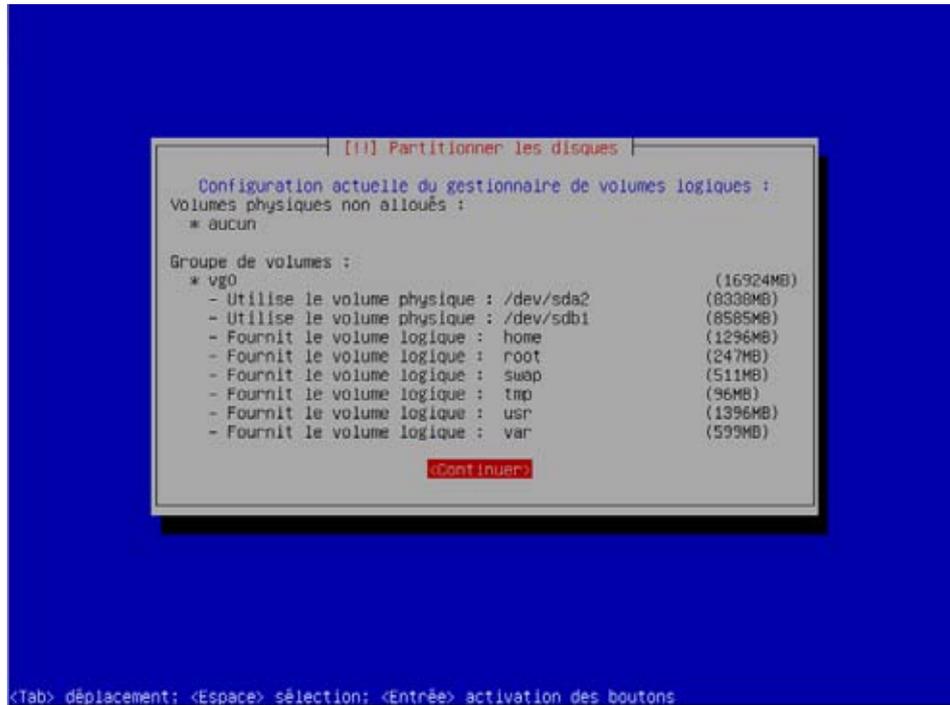


Atelier 11

Installation
de Linux Debian

Page 151

En résumé, lorsque vous faites « Détail de la configuration », vous obtenez ceci :



```
[!!] Partitionner les disques

Configuration actuelle du gestionnaire de volumes logiques :
Volumes physiques non alloués :
* aucun

Groupe de volumes :
* vg0 (16924MB)
- Utilise le volume physique : /dev/sda2 (8330MB)
- Utilise le volume physique : /dev/sdb1 (8585MB)
- Fournit le volume logique : home (1296MB)
- Fournit le volume logique : root (247MB)
- Fournit le volume logique : swap (511MB)
- Fournit le volume logique : tmp (96MB)
- Fournit le volume logique : usr (1396MB)
- Fournit le volume logique : var (599MB)

[Continuer]
```

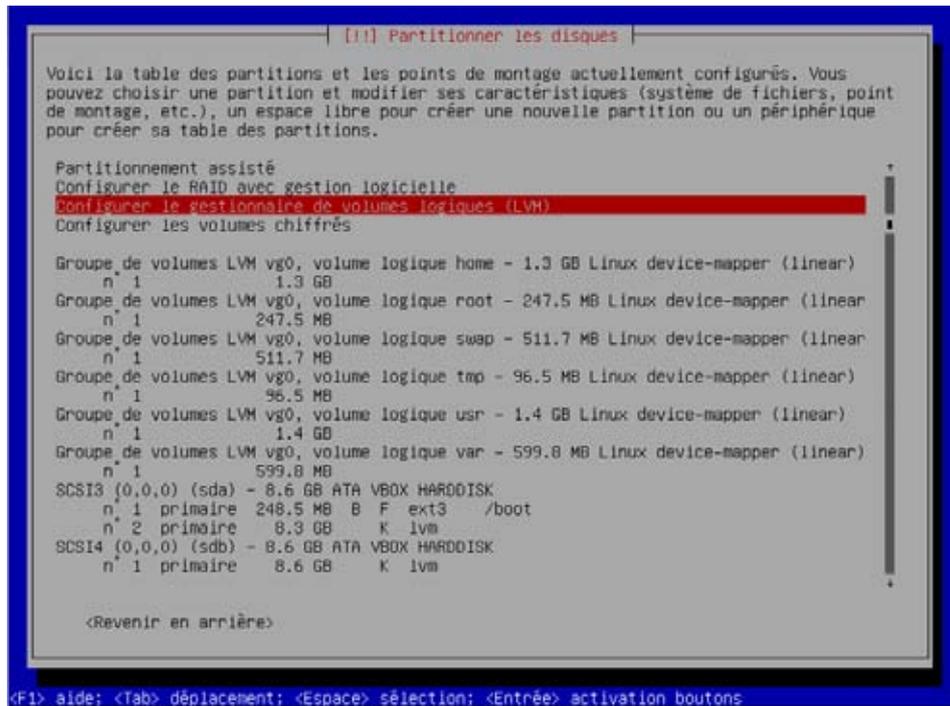
<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Atelier 11

Les tailles des volumes prises en compte par Debian sont légèrement différentes de celles saisies en raison de la géométrie des disques (rappel du premier module de cours !).

Faites « Terminer » pour quitter le gestionnaire LVM et revenir au gestionnaire de partitions proprement dit car nous avons encore du travail !

En effet, nous allons devoir indiquer tous les points de montage et le système de fichiers à utiliser (comme nous l'avons fait tout à l'heure pour /boot) :



```
[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés

Groupe de volumes LVM vg0, volume logique home - 1.3 GB Linux device-mapper (linear)
n 1 1.3 GB
Groupe de volumes LVM vg0, volume logique root - 247.5 MB Linux device-mapper (linear)
n 1 247.5 MB
Groupe de volumes LVM vg0, volume logique swap - 511.7 MB Linux device-mapper (linear)
n 1 511.7 MB
Groupe de volumes LVM vg0, volume logique tmp - 96.5 MB Linux device-mapper (linear)
n 1 96.5 MB
Groupe de volumes LVM vg0, volume logique usr - 1.4 GB Linux device-mapper (linear)
n 1 1.4 GB
Groupe de volumes LVM vg0, volume logique var - 599.8 MB Linux device-mapper (linear)
n 1 599.8 MB
SCSI3 {0,0,0} (sda) - 8.6 GB ATA VBOX HARDDISK
n 1 primaire 248.5 MB B F ext3 /boot
n 2 primaire 8.3 GB K lvm
SCSI4 {0,0,0} (sdb) - 8.6 GB ATA VBOX HARDDISK
n 1 primaire 8.6 GB K lvm

<Revenir en arrière>
```

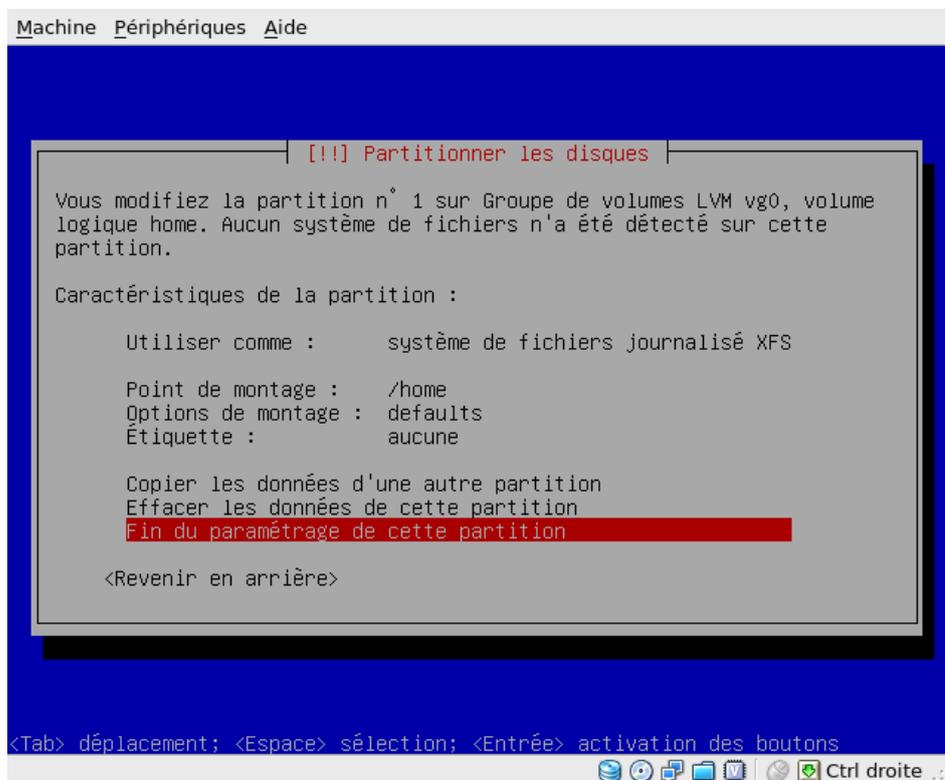
<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

Voici vos tâches maintenant :

Nom du volume logique	Taille	Point de montage	Système de fichiers
home	1.3 GiO	/home	xfs
root	250 MiO	/	xfs
swap	512 MiO	swap	swap
tmp	100 MiO	/tmp	xfs
usr	1,4 GiO	/usr	xfs
var	600 MiO	/var	xfs

Nous ne pouvons pas utiliser le classique système de fichiers ext3 de Linux car celui n'est pas extensible à chaud contrairement à xfs. Avec ext3, cela ne peut se faire qu'avec un disque démonté.

Vous validez sur chaque volume logique pour retrouver cet écran désormais familier :

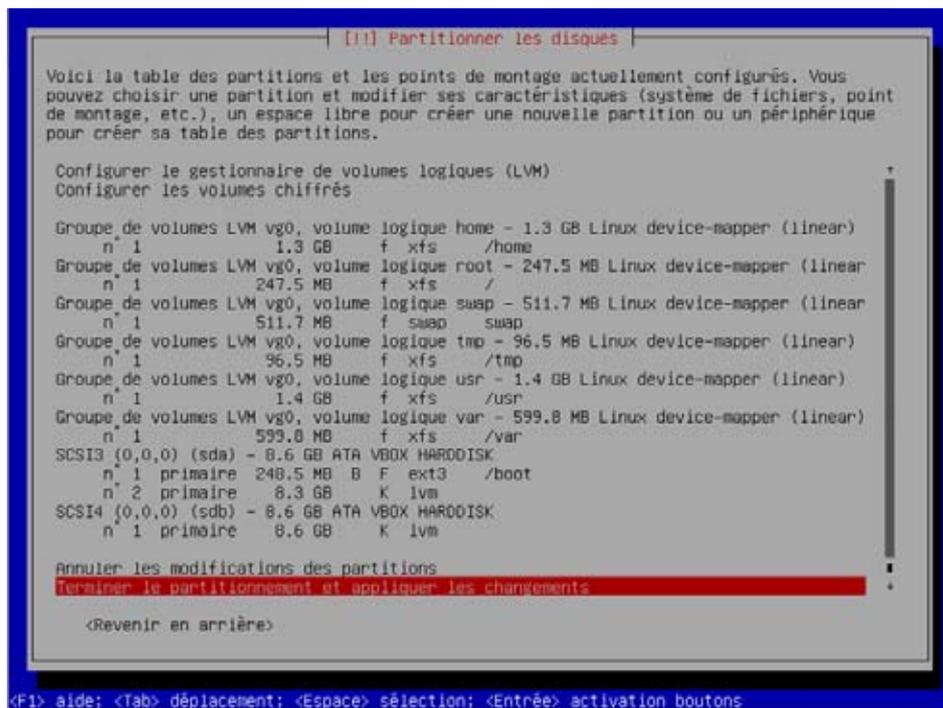


Ouf ! Ça y est ! Quel travail !

Atelier 11

Installation
de Linux Debian

Page 153

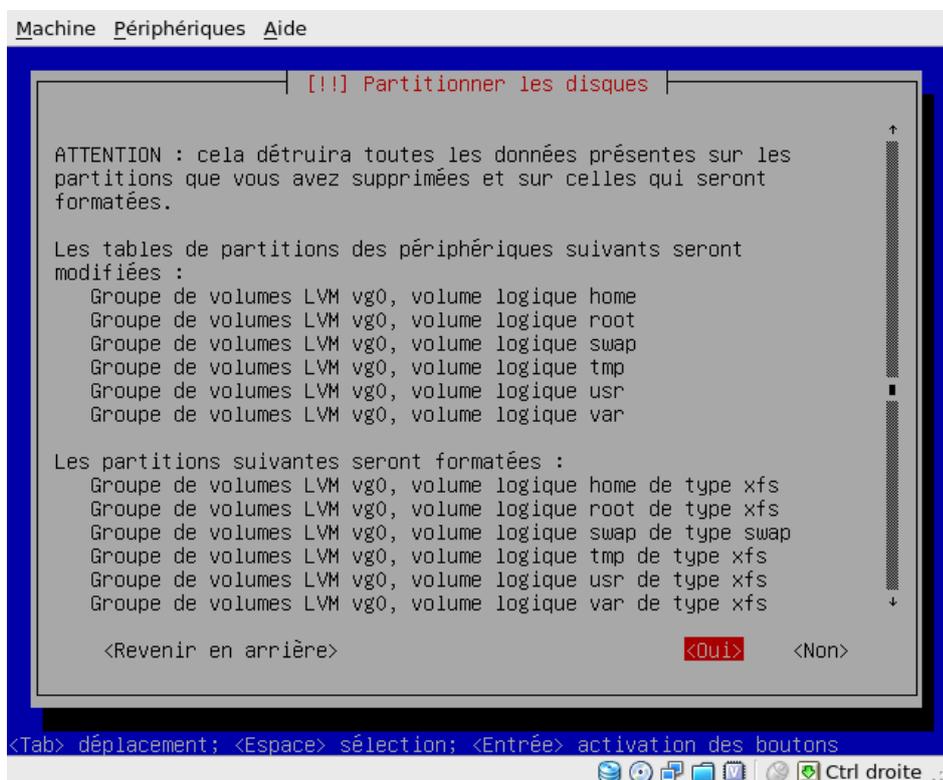


Lorsque vous faites « Terminer le partitionnement et appliquer les changements », l'installateur de Debian vous résume les actions qu'il va réaliser car pour l'instant tout est virtuel et rien n'est réalisé sur disque :

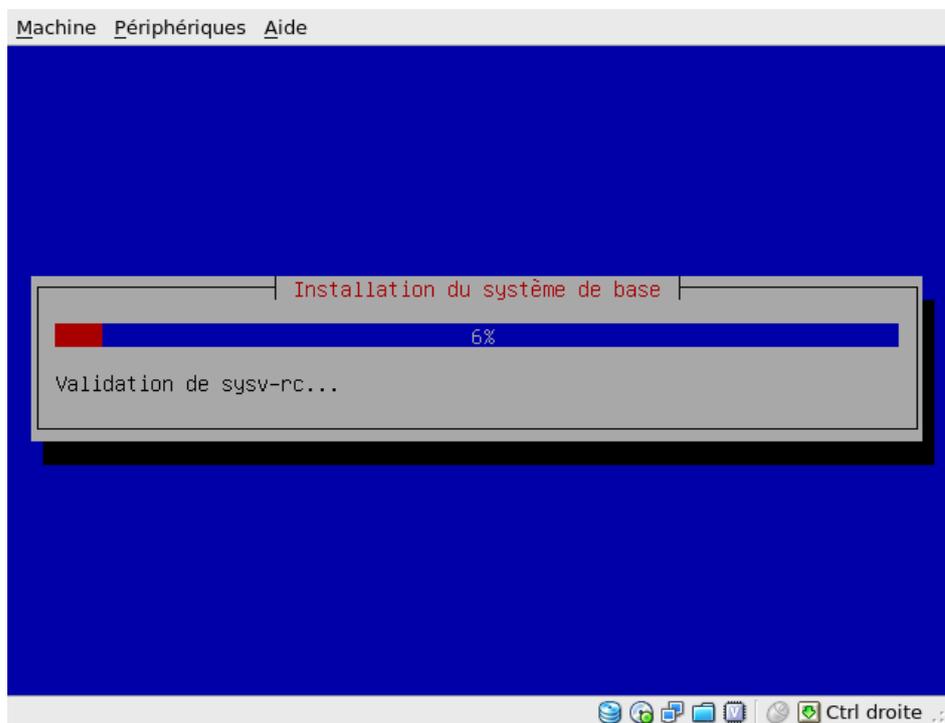
Atelier 11

Installation
de Linux Debian

Page 154



Le travail de l'administrateur est quasiment fini et nous laissons l'installateur Debian poursuivre :

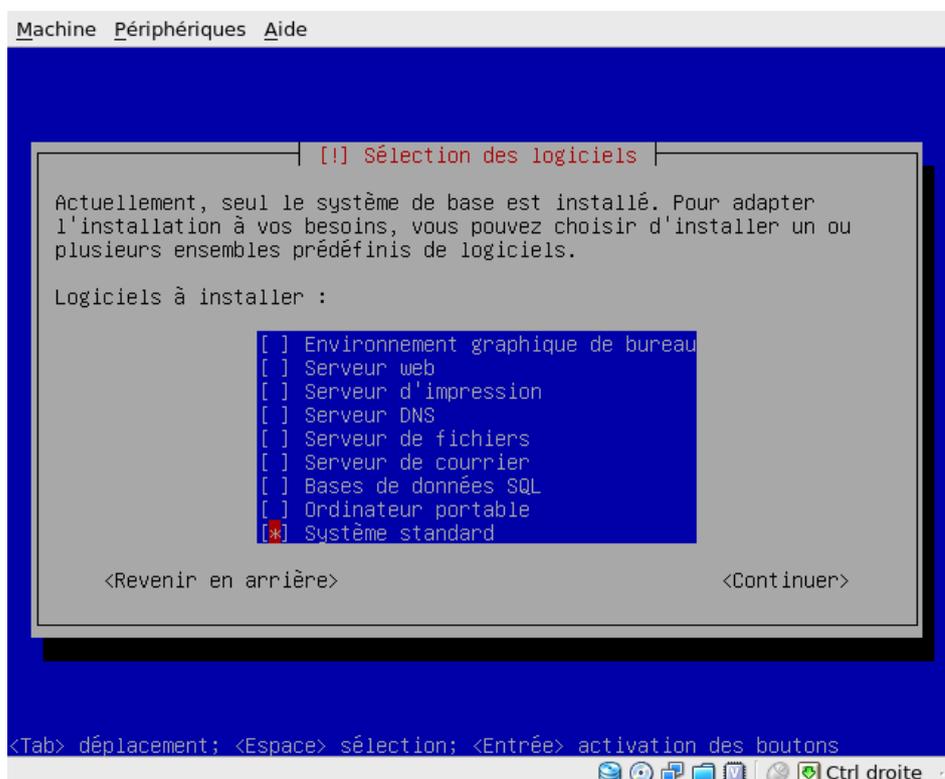


Il faudra choisir un miroir Debian pour qu'il puisse télécharger les paquets nécessaires. Ne sélectionnez que « système standard ». Le reste, nous l'installerons dans la suite de ces ateliers :

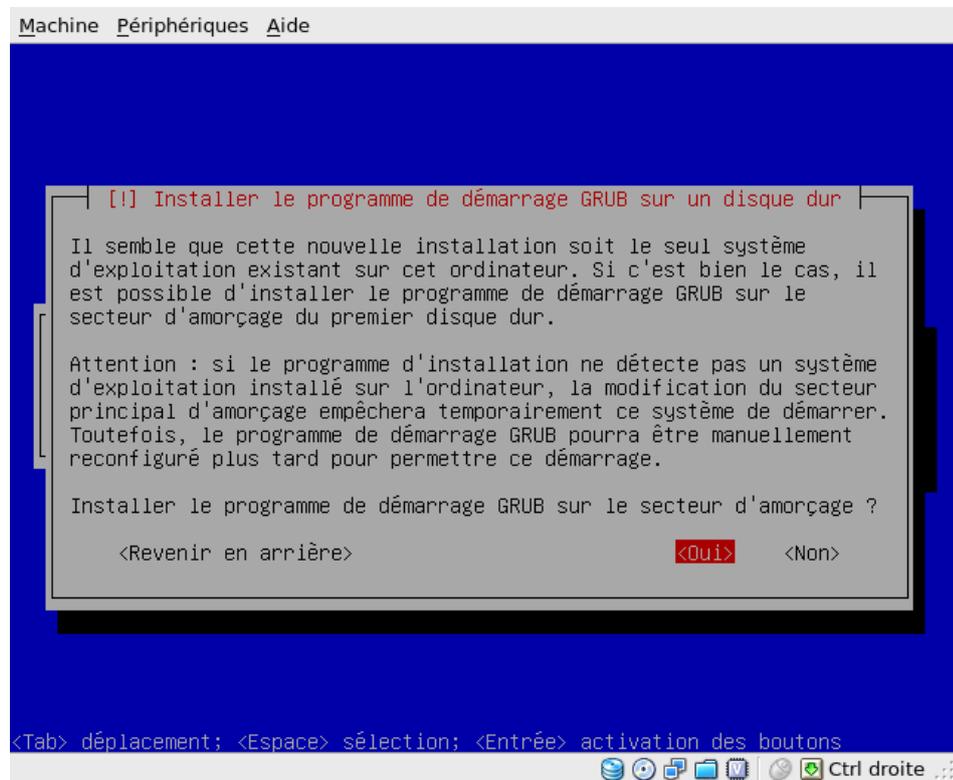
Atelier 11

Installation
de Linux Debian

Page 155



Notre machine virtuelle ne comporte que le système d'exploitation Debian Linux, nous pouvons donc sélectionner « Oui » en toute tranquillité :



Atelier 11

Installation
de Linux Debian

Page 156

L'installation se termine et l'on vous propose de redémarrer le système. Vous devez arriver sur cet écran qui attend patiemment votre connexion :

```
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting NFS common utilities: statd.
Starting portmap daemon...Already running..
Starting enhanced syslogd: rsyslogd.
Checking battery state...done.
Starting VirtualBox AdditionsVBoxService: 3.2.10_OSE r66523 started. Verbose level = 0
.
Starting ACPI services...
Starting anac(h)ronistic cron: anacron.
Starting deferred execution scheduler: atd.
Starting acpi_fakekey daemon...done.
Starting system message bus: dbus.
Starting periodic command scheduler: cron.
Starting Common Unix Printing System: cupsd.
Starting MTA: exim4.
Starting bluetooth: bluetoothd.
Loading cpufreq kernel modules...done (none).
CPUFreq Utilities: Setting ondemand CPUFreq governor...disabled, governor not available...done.

Debian GNU/Linux 6.0 mv2-linux tty1
mv2-linux login: _
```

À retenir

L'installation de Debian Linux ne pose pas de problème en soi. La seule chose délicate concerne l'organisation des disques si l'on veut un système qui offre la souplesse de pouvoir étendre à chaud la taille d'une partition.

Nous choisissons donc d'utiliser LVM (Logical Volume Manager) et XFS (ext3 ne permet pas l'extension à chaud). Une partition est créée pour chaque répertoire important du système de fichiers de Linux.

Si vous voulez approfondir

Vous pouvez refaire l'installation en mode expert (choix possible lors du premier menu après démarrage sur le cédérom).

Atelier 12

Linux : la ligne de commande

► Objectif

À la fin de cet atelier, vous saurez vous débrouiller avec les commandes de base de Linux. Ce n'est pas une séquence de cours exhaustive sur l'interpréteur de commandes du système d'exploitation, mais une présentation des commandes les plus courantes.

► Durée approximative de cet atelier : 1 heure

► Durée approximative de cet atelier

Aucune a priori. Cet atelier n'est pas une application directe du cours mais plutôt une étape nécessaire pour vous familiariser aux commandes de Linux.

► Mise en place de l'atelier

La machine virtuelle avec Debian Linux installée.

► Matériel et logiciel nécessaires

Rien de plus n'est requis.

► Que faire si je bloque ?

Reportez-vous aux sources déjà citées.

► Contenu

1. Introduction	160
2. Comment passer des ordres à Linux ?	160
3. Comment me dépatouiller avec les commandes Linux ?.....	164
4. Ouverture et fermeture de session	166
5. Gestion des fichiers	166
6. Personnalisation du shell	174
7. Arrêt du système	175

1. Introduction

Nous avons choisi de vous faire travailler en ligne de commande. Pourquoi ? Pour une simple et bonne raison : personne n'administre un serveur Linux en interface graphique !

On développe cette idée ? Voici quelques bonnes raisons :

- je me concentre sur la configuration ou le travail à réaliser. Avec un logiciel graphique, je dois d'abord apprendre à me servir du logiciel. L'ergonomie pensée par le développeur ne correspondra peut-être pas à ma façon de penser.
- je maîtrise ce que je fais. Si je modifie un fichier de configuration en mode texte, je sais que la configuration est prise en compte, je ne suis pas dépendant d'éventuels bugs de l'interface graphique.
- je réduis la « surface d'exposition » de mon serveur. Plus mon serveur est « allégé » moins j'ai de risques de plantages, de failles de sécurité, etc.

Bref, on applique un des principes fondamentaux d'Unix : KISS (*Keep It Simple, Stupid*). Plus le système à gérer est simple, plus vous gagnez en efficacité.

2. Comment passer des ordres à Linux ?

Démarrez la machine virtuelle sous Linux, vous arrivez inévitablement sur ceci :

```
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting NFS common utilities: statd.
Starting portmap daemon...Already running..
Starting enhanced syslogd: rsyslogd.
Checking battery state...done.
Starting VirtualBox AdditionsVBoxService: 3.2.10_OSE r66523 started. Verbose level = 0
.
Starting ACPI services...
Starting anac(h)ronistic cron: anacron.
Starting deferred execution scheduler: atd.
Starting acpi_fakekey daemon...done.
Starting system message bus: dbus.
Starting periodic command scheduler: cron.
Starting Common Unix Printing System: cupsd.
Starting MTA: exim4.
Starting bluetooth: bluetoothd.
Loading cpufreq kernel modules...done (none).
CPUFreq Utilities: Setting ondemand CPUFreq governor...disabled, governor not available...done.

Debian GNU/Linux 6.0 mv2-linux tty1
mv2-linux login: _
```

Tout en bas de cet écran vous voyez :

```
mv2-linux login: _
```

Comme sous Windows, vous devrez vous « logger » (se connecter au système en s'authentifiant).

Pour vous connecter comme administrateur tapez `root` puis votre mot de passe. Maintenant vous êtes « loggé », l'invite (l'interface vous invite à entrer des commandes) est :

```
mv2-linux :~#
```

C'est probablement l'occasion de mieux comprendre le fonctionnement d'un shell quelque soit le système d'exploitation. Les commandes ne sont interprétées (analysées) puis exécutées que lorsque vous appuyez sur la touche de retour chariot (**ENTREE**).

Le processus peut être découpé en différentes étapes :

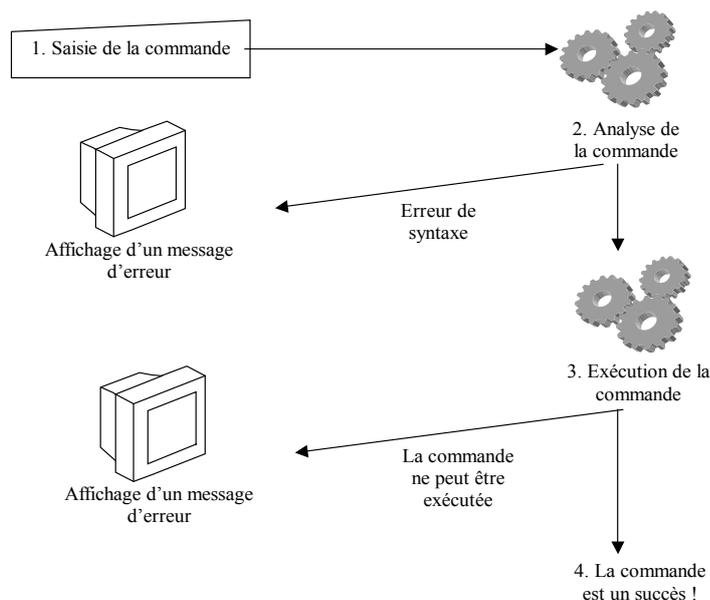


Figure 1 : traitement d'une commande par le système d'exploitation

2A. Saisie de la commande par l'utilisateur

Une commande correspond à un ordre que l'utilisateur soumet à la machine. Donc, la commande minimale est du type :

```
# ordre ENTREE
```

Commençons par analyser la ligne ci-dessus :

- le # correspond à l'invite (prompt). Il nous informe que le système attend une commande. Il nous indique aussi que nous sommes connectés en `root`¹ ;
- l'ordre est une commande que le système d'exploitation doit connaître ;
- **ENTREE** indique qu'il faut appuyer sur cette touche pour que la commande soit exécutée par Linux. Étant donné que c'est obligatoire, par la suite, j'omettrai volontairement de l'indiquer.

Par exemple, la commande pour redémarrer l'ordinateur est :

```
# reboot ENTREE
```

1. Lorsqu'il s'agit d'un utilisateur « normal », l'invite est un \$.

Mais une commande peut s'appliquer à un objet particulier. Dans ce cas, il faut indiquer le nom de cet objet. Par exemple, pour supprimer un fichier :

```
# rm nom_du_fichier ENTREE
```

Une commande peut s'appliquer sur plusieurs objets en même temps. Dans ce cas, on indique :

```
# rm nom_du_fichier1 nom_du_fichier2 ENTREE
```

Une commande peut proposer divers services. Dans ce cas, il faut indiquer un ou plusieurs commutateurs qui permettent de sélectionner le ou les services que l'on souhaite :

```
# ordre nom_des_objets -commutateurs ENTREE
```

Par exemple, si je veux supprimer le fichier fictest avec une confirmation de l'utilisateur :

```
# rm fictest -i ENTREE
```

Les commutateurs sont précédés par le symbole -.

2B. Analyse de la commande par Linux : les erreurs fréquentes

Souvent, lorsque l'on débute avec l'interpréteur de commandes, on ne comprend pas pourquoi l'ordinateur refuse certaines commandes que l'on tape. Je vous donne ici quelques règles utilisées par l'interpréteur de commande de Linux. Elles vous aideront à comprendre comment il travaille, et donc comment formuler des commandes qui marchent :

1. Linux différencie les majuscules et les minuscules.

Exemples :

La commande :

```
# RM nom_du_fichier ENTREE
```

sera refusée.

Utilisez essentiellement des minuscules.

La commande :

```
# rm nom_du_fichier ENTREE
```

sera acceptée.

2. Linux utilise le caractère espace pour reconnaître les différents éléments composant la commande.

Exemples :

Les commandes :

```
# rmnom_du_fichier ENTREE  
# rm nom_du_fichier-y ENTREE  
# rmnom_du_fichier-y ENTREE
```

seront refusées.

Respectez bien les espaces !

Les commandes :

```
# rm nom_du_fichier ENTREE  
# rm nom_du_fichier ENTREE  
# rm nom_du_fichier -y ENTREE
```

seront acceptées.

3. Linux vérifie la cohérence des paramètres

Pour certaines commandes, il faut nécessairement spécifier le nom d'un objet. Par exemple, utiliser la commande rm (suppression de fichier) sans indiquer de nom de fichier

n'a pas de sens. Utiliser la commande `mv` pour renommer un fichier sans indiquer deux noms de fichiers (l'ancien et le nouveau) n'a pas de sens non plus.

Linux vérifie le type de l'objet indiqué. Par exemple, pour certaines commandes, il faut indiquer un nom de fichier et non pas un nom de répertoire.

Enfin, il faut indiquer un ou des commutateurs qui soient pris en charge par la commande.

Si ces contraintes ne sont pas respectées, Linux affiche des messages d'erreurs :

<pre># rm rm: Trop peu de paramètres. Pour en savoir davantage, faites: `rm --help`.</pre>	Ben oui ! je veux supprimer un fichier (rm) mais je ne dis pas lequel !
<pre># rm fictest -e rm: option invalide -- e Pour en savoir davantage, faites: `rm --help`.</pre>	Bon, heu là, faut vraiment que je consulte la documentation (voir la partie suivante).
<pre># rmfictest bash: rmfictest: command not found</pre>	Avec un espace entre rm et fictest, ça serait mieux.

2C. Exécution de la commande par Linux

Si la commande est correcte au niveau syntaxique, Linux obéit bien gentiment et tente de faire le travail demandé. Mais vous savez bien que ce n'est pas une condition suffisante pour que la tâche soit réalisable (c'est la même chose quand vous programmez : la compilation peut passer bien que le programme soit bogué).

Si la commande n'est pas réalisable, Linux nous en informe. Par exemple :

<pre># rm fictoto rm: cannot remove `fictoto`: Aucun fichier ou répertoire de ce type</pre>	Je veux supprimer un fichier qui n'existe pas, c'est malin !*
---	---

* Notez au passage le délicieux mélange anglais/français du message d'erreur ! c'est ça être bilingue !

2D. La commande est un succès

Très souvent, Linux vous criera dessus si vous vous trompez mais ne vous dira rien si la commande a pu être exécutée. Dans tous les cas, une lecture attentive des messages sur l'écran est absolument impérative !

3. Comment me dépatouiller avec les commandes Linux ?

Il existe différentes façons de connaître le fonctionnement d'une commande.

3A. L'aide affichée par la commande elle-même

Si vous avez bien lu sur la page précédente, lorsque je me trompais dans la commande `rm`, Linux me conseillait gentiment de taper :

```
rm --help
```

Voyons ce que cela donne :

```
# rm --help
Usage: rm [OPTION]... FICHIER...
Remove (unlink) the FILE(s).
  -f, --force ignore nonexistent files, never prompt
  -i          prompt before every removal
  -I          prompt once before removing more than three files, or
             when removing recursively. Less intrusive than -i,
             while still giving protection against most mistakes
  --interactive[=WHEN] prompt according to WHEN: never, once
  (-I), or
             always (-i). Without WHEN, prompt always
  --one-file-system when removing a hierarchy recursively, skip
  any
             directory that is on a file system different from
             that of the corresponding command line argument
  --no-preserve-root do not treat '/' specially
  --preserve-root do not remove '/' (default)
  -r, -R, --recursive remove directories and their contents
  recursively
  -v, --verbose explain what is being done
  --help afficher l'aide-mémoire
  --version afficher le nom et la version du logiciel
```

Par défaut, `rm` n'enlève pas les répertoires. Utilisez l'option `--recursive` (`-r` ou `-R`) pour enlever les répertoires, ainsi que tout leur contenu.

Pour enlever un fichier dont le nom début par « - », par exemple « -foo »,

utiliser une de ces commandes:

```
rm -- -foo
rm ./-foo
```

Noter que si vous utilisez « `rm` » pour détruire un fichier, il est habituellement possible de récupérer le contenu de ce fichier. Si vous désirez plus d'assurance à l'effet de ne pas pouvoir récupérer le contenu, considérez `shred`.

Rapporter toutes anomalies à bug-coreutils@gnu.org.

Bon, on a déjà pas mal d'informations sur le fonctionnement de la commande. Considérez que le paramètre `--help` est valable pour la plupart des commandes.

3B. L'aide en ligne

Une commande toute simple vous rappelle en une phrase le rôle d'une commande : `whatis`

```
# whatis rm
rm (1) - remove files or directories
```

Des pages de la documentation de Linux sont accessibles via la commande `man`. Le format général de la commande est :

```
# man nom_de_la_commande
```

Par exemple, avec la commande `man rm`, on obtient :

```
# man rm
RM(1)
NOM
    rm - Effacer des fichiers et des répertoires
SYNOPSIS
    rm [OPTION]... FICHIER...
DESCRIPTION
    Cette page de manuel documente la version GNU de rm. Le
    programme rm efface chaque fichier listé. Par défaut, il n'efface
    pas les répertoires.
    Si l'option -I ou --interactive=once est fournie, et qu'il y a
    plus de trois fichiers ou qu'une des options -r, -R ou --recursive
    est utilisée, alors rm demande à l'utilisateur s'il faut effectuer
    l'opération. Si la réponse n'est pas affirmative, la commande est
    interrompue.
    [...]

```

Je ne vous présente ici qu'un extrait, car en général, le texte est très détaillé.

Tapez sur `q` pour quitter. Vous pouvez faire une recherche en tapant un slash (`/`) puis le texte à chercher. Ensuite, appuyez sur `n` pour trouver la prochaine occurrence. Tapez sur `H` pour obtenir l'aide complète.

Atelier 12

Linux : la ligne
de commande

Page 165

4. Ouverture et fermeture de session

Bien. Maintenant vous avez tous les outils pour vous jeter à corps perdu dans Linux.

4A. Ouverture de session

Avant de pouvoir travailler, vous devez vous identifier. Votre premier contact avec Linux a été de vous logger avec root. Nous allons maintenant nous déconnecter et nous logger en usercnd :

```
mv2-linux:~# logout
ENTREE
mv2-linux login: usercnd
Password: votre mot de passe
Vous obtenez l'invite :
usercnd@mv2-linux:~$
```

Nous allons ensuite faire quelques manipulations qui nous permettront de découvrir le système. Comme vous ne serez pas administrateur, vous n'aurez aucun risque de faire une bêtise.

4B. Les différents terminaux

Par défaut, Linux propose six terminaux qui donnent accès à six *shells*. Ils sont accessibles via les touches ALT+ <touche de fonction correspondant au numéro>

Exercice 1

Positionnez-vous sur le terminal numéro 2 puis connectez-vous.

Atelier 12

Linux : la ligne
de commande

Page 166

4C. Fermeture de session

Elle se fait par la commande :

```
$ exit
```

Tapez cette commande, mais attention vous êtes sur un système d'exploitation multi-tâche, multiutilisateur. Lorsque vous vous déconnectez cela ne veut pas dire que le système est arrêté. Il y a toute une série de tâches qui s'exécutent de façon invisible pour l'utilisateur et il peut y avoir aussi d'autres utilisateurs connectés au travers du réseau.

Exercice 2

Revenez sur le terminal numéro 1.

5. Gestion des fichiers

Une part importante des commandes d'un système d'exploitation concerne la gestion des fichiers stockés sur disque. Il existe essentiellement deux grands types d'objet :

- le fichier : contient des données ;
- le répertoire : contient des fichiers ou d'autres répertoires.

5A. Manipulations de répertoires

Lorsque l'on ouvre une session, on est immédiatement positionné dans un répertoire de l'arborescence de Linux. Mais avant d'aller plus loin, j'aimerais que nous fassions quelques rappels sur du vocabulaire que vous devez en principe connaître :

Exercice 3

1. Définissez le terme d'arborescence.
2. Définissez le terme de racine.
3. Soit l'arborescence suivante :

```
/  +-- bin           Sachant que le / représente la racine et que vous vous
  +-- etc           trouvez dans le répertoire /home/util2, donnez :
  +-- home +-- util1 le nom du répertoire courant
    | +-- util2 +-- rep le nom du répertoire parent
    +-- tmp         le nom du répertoire enfant
                   le chemin complet de « rep »
```

Le groupe de commandes ci-dessous permet de se balader dans l'arborescence :

Commande	Rôle
cd nom_du_répertoire	Positionne dans le répertoire enfant
cd	Positionne dans votre répertoire personnel
pwd	Donne le chemin correspondant à l'endroit où vous êtes

Atelier 12

Le groupe de commandes ci-dessous permet de modifier l'arborescence :

Commande	Rôle
mkdir nom_du_répertoire	Crée un répertoire dans le répertoire courant
rmdir nom_du_répertoire	Supprime un répertoire dans le répertoire courant
mv nom_ancien nom_nouveau	Renomme un répertoire dans le répertoire courant

Linux : la ligne de commande

Page 167

Remarque : on peut remplacer le nom d'un répertoire par un chemin.

Exercice 4

Passons à quelques exercices. Vous pouvez bien sûr les réaliser devant votre écran et vous aider de l'aide en ligne si vous coincez. Pour les faire, vous devez avoir ouvert une session en tant qu'utilisateur standard (pas en root si vous préférez).

Par exemple, si on vous demande de créer un répertoire puis d'afficher le répertoire courant :

```
usercned@mv2-linux:~$ mkdir reptest
usercned@mv2-linux:~$ pwd
/home/usercned
usercned@mv2-linux:~$ ls
reptest
usercned@mv2-linux:~$
```

Maintenant à vous de jouer :

- affichez le nom complet du répertoire où vous êtes
- créez le répertoire « repertoire_test »
- placez-vous dans ce répertoire
- placez-vous à la racine du disque
- revenez dans votre répertoire personnel
- renommez le répertoire « repertoire_test » en « ajeter »
- supprimez le répertoire « ajeter »

5B. Manipulation de fichiers

Vous allez utiliser les commandes suivantes :

Commande	Effet
<code>vi nom_de_fichier</code>	Crée un fichier texte.
<code>ls</code>	Affiche la liste des fichiers du répertoire courant
<code>ls a*</code>	Idem ci-dessus mais dont le nom commence par a
<code>ls nom_de_fichier</code>	Affiche le nom du fichier s'il existe
<code>cat nom_de_fichier</code>	Affiche le contenu d'un fichier
<code>cp original copie</code>	Duplique un fichier
<code>mv nom_ancien nom_nouveau</code>	Renomme un fichier situé dans le répertoire courant
<code>diff nom_fic1 nom_fic2</code>	Compare le contenu des deux fichiers

Atelier 12

Linux : la ligne
de commande

Page 168

Remarque : pour toutes ces commandes, le nom du fichier peut être remplacé par un chemin suivi d'un nom de fichier.

5B1. Edition de texte

vi² est un éditeur de texte. Il dispose d'une multitude de commandes permettant la manipulation des fichiers. Il présente deux caractéristiques universellement reconnues :

- tous les systèmes Unix le possèdent. Vous pourrez toujours vous en servir ;
- il est affreusement peu convivial et rustre. Bien sûr, d'autres éditeurs existent sous Linux mais ils sont beaucoup moins universels.

Tapez `vi monfic`, vous obtenez :

```
~
~
~
...
~
~
~
"monfic" [New File]
```

Le fichier n'existant pas, vi affiche un écran vierge, où clignote un curseur. vi dispose de deux modes :

- un mode commande ;
- un mode saisie.

2. Prononcez à l'anglaise : vi aïe

Le mode commande permet notamment de basculer en mode saisie, de se déplacer dans le texte et de modifier le texte. Pour commuter du mode saisie au mode commande on tape sur la touche Echap.

a. Saisie

Résumé des principales commandes de vi :

Commande	Effet
a	ajout derrière le caractère courant
i	insertion devant le caractère courant
dw	supprime le mot courant
d\$ (ou D)	supprime tous les caractères jusqu'à la fin de ligne
dd	supprime la ligne courante
u	annule la dernière suppression
nG	sauter à la ligne n (exemple 10G)
:w	enregistre le fichier
:wq	enregistre le fichier et quitte
:q!	quitte sans enregistrer

Pour saisir du texte, vous devez passer en mode insertion :

Tapez sur la touche « i » du clavier (vous êtes maintenant en mode saisie).

Tapez le texte suivant (les fautes sont volontaires) :

```
je sui un étudiant en BTS
J'ai choisi réso pour mon maleur
Saurai-je déjouer les pièges de TPCIP
mes messages franchiront ils les féroces routeurs
```

Pour enregistrer les modifications en cours de travail, vous devez passer en mode commande :

Tapez sur la touche **ECHAP**, puis tapez :w puis sur **ENTREE**. vi vous informe que le fichier a été enregistré.

Puis quittez :q et **ENTREE**

Vérifiez la présence de monfic

Corrigez le texte précédent ainsi :

```
Je suis un étudiant en BTS
J'ai choisi réseau pour mon malheur
Saurai-je déjouer les pièges de TCP-IP ?
Mes messages franchiront-ils les féroces routeurs ?
```

b. Recherche de texte

Passez en mode commande en tapant sur **ECHAP**, puis tapez /mot_recherché.

c. Remplacement de texte

En se plaçant sur le mot à remplacer, on dispose des commandes suivantes, lorsque le remplacement est effectué on appuie sur la touche entrée pour terminer la commande :

Commandes	Effet
<code>cw</code>	Remplacement du mot courant

d. Copier et déplacer du texte

Commandes	Effet
<code>yy</code> ou <code>nyy</code>	Copie 1 à n lignes dans un buffer
<code>p</code>	Insertion au dessous du curseur des lignes conservées dans le buffer
<code>P</code>	Insertion au dessus

e. Rechercher et remplacer du texte

Commandes	Effet
<code>:s/machin/truc/</code>	Remplace machin par truc sur la ligne courante
<code>:1,10s/DOS/LINUX/g</code>	Remplace le mot DOS par LINUX de la première à la dixième ligne. Si le mot apparaît plusieurs fois sur la ligne, il faut tous les remplacer (/g).
<code>:1,\$s/DOS/LINUX/</code>	Remplacement dans tout le texte (\$s) la première occurrence de chaque ligne.

Atelier 12

Linux : la ligne
de commande

Page 170

f. Une option intéressante de vi

L'option la plus utilisée est celle qui permet d'afficher le numéro des lignes (cela ne modifie pas le texte) :

Commandes	Effet
<code>:set number</code>	Activer la numérotation
<code>:set nonumber</code>	Désactiver la numérotation

Exercice 5

- Affichez les numéros de lignes
- Modifiez le texte précédent :
 - Remplacer malheur par bonheur
 - Remplacer les pièges par les charmes
 - Remplacer bonheur par grand bonheur
 - Remplacer tous les a par des A
 - Mettez un point à la fin des deux premières lignes
 - Recherchez toutes les lignes contenant un I (i majuscule)
 - Copiez la première ligne dans un autre fichier

5B2. Manipulation de fichiers

Exercice 6

Encore quelques exercices. Revenez à l'interpréteur de commande, puis :

- créez le fichier test1.txt avec vi, contenu :

```
j'aime bien
linux
```

- créez le fichier test2.txt avec vi, contenu :

```
j'aime BIEN
linux
```

Revenez à l'interpréteur de commandes :

- recherchez les différences entre les 2 fichiers
- rentrez dans le répertoire /bin
- listez tous les fichiers du répertoire /bin
- listez tous les fichiers de /bin qui commencent par ls
- revenez dans votre répertoire personnel
- affichez le contenu du fichier test1.txt
- copiez le fichier test1.txt en test3.txt
- listez les fichiers (vous devez donc avoir trois fichiers : test1.txt, test2.txt, test3.txt)
- affichez le contenu du fichier test2.txt
- supprimez le fichier test1.txt
- renommez le fichier test3.txt en test4.txt
- listez les fichiers (vous devez donc avoir deux fichiers : test2.txt et test4.txt)

Atelier 12

Linux : la ligne
de commande

Page 171

5B3. Informations sur les fichiers

Au début de l'atelier, nous avons dit que l'on pouvait associer des commutateurs aux commandes afin de modifier leur comportement. La commande ls comporte de nombreux commutateurs. Parmi les principaux, nous avons :

Commandes	Effet
ls -a	Affiche aussi les fichiers cachés
ls -l	Affiche les détails (voir ci-dessous)
ls -la	On peut cumuler les opérateurs

Dans les exercices précédents, vous avez du utiliser la commande ls sans commutateur. Par exemple, dans mon répertoire, j'obtiendrais :

```
usercnd@mv2-linux:~$ ls
reptest test2.txt test4.txt
```

On me dit que je n'ai que trois fichiers. Bien. Essayons avec les commutateurs que nous venons d'étudier :

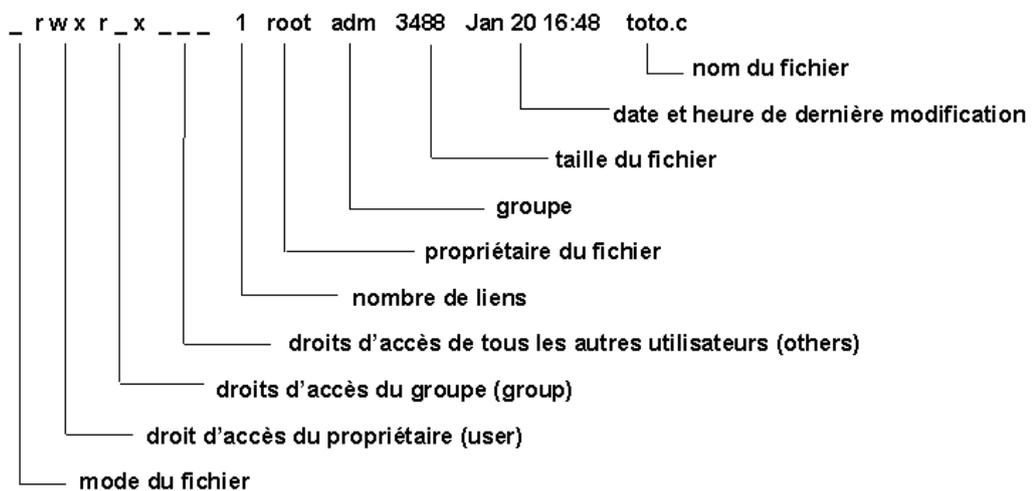
```

usercncd@mv2-linux:~$ ls -la
total 16
drwxr-xr-x 3 usercncd usercncd 120 fév 19 12:31.
drwxr-xr-x 4 root root 33 fév 3 23:54..
-rw----- 1 usercncd usercncd 141 fév 19 12:16.bash_history
-rw-r--r-- 1 usercncd usercncd 220 mai 12 2008.bash_logout
-rw-r--r-- 1 usercncd usercncd 3116 mai 12 2008.bashrc
-rw-r--r-- 1 usercncd usercncd 675 mai 12 2008.profile
drwxr-xr-x 2 usercncd usercncd 6 fév 19 12:29 reptest
-rw-r--r-- 1 usercncd usercncd 0 fév 19 12:31 test2.txt
-rw-r--r-- 1 usercncd usercncd 0 fév 19 12:31 test4.txt

```

On me cachait des choses ! En fait, tous les fichiers commençant par un . sont des fichiers de configuration propres à mon compte d'utilisateur mais gérés en partie par Linux. Ils sont « cachés » par le système.

Mais voyons le sens des informations affichées :



- Le mode (ou type) de fichier :
 - - ordinaire
 - d répertoire
- Droits d'accès : il y a trois paquets de trois lettres. Pour chaque fichier et répertoire, on peut contrôler l'accès en identifiant trois catégories :
 - du propriétaire (dont le nom est indiqué plus loin sur la ligne)
 - du groupe (dont le nom est indiqué plus loin sur la ligne)
 - de tous les autres utilisateurs

Chaque catégorie possède 3 types de permission

- r lire
- w écrire
- x exécuter
- - le droit n'est attribué

Pour l'instant, je ne vous en dit pas plus car nous reviendrons sur le sujet dans un prochain atelier.

- Nombre de liens

- Nom du propriétaire
- Nom d'un groupe
- Taille en octets
- Date de dernière modification
- Nom du fichier ou répertoire

Exercice 7

On passe à la pratique. Vous avez toute une série de commandes à réaliser ci-dessous.

- Placez-vous dans votre répertoire personnel.
- Listez tous les fichiers y compris les fichiers cachés.
- Que représentent les fichiers « . » et « .. » ?
- Listez tous les fichiers en affichant (au moins) la date et la taille.
- Affichez le contenu du fichier `bash_history`. Que remarquez-vous ?
- Affichez tous les fichiers dont le nom commence par test.

5B4. Recherche de fichiers

La commande `find` permet de parcourir l'arborescence des répertoires à la recherche d'un fichier. Son format général est : `find nom_de_répertoire(s) critère_de_selection -commutateur(s)`

Commandes	Effet
<code>find</code>	Affiche tous les fichiers à partir du répertoire courant
<code>find / -name nom_fichier</code>	Recherche à partir de la racine (/) tous les fichiers s'appelant <code>nom_fichier</code> .
<code>Whereis</code> <code>which</code>	Recherche une commande. Les deux commandes ont un fonctionnement relativement proche.

Atelier 12

Linux : la ligne de commande

Page 173

Exercice 8

Placez-vous dans le répertoire `/home`

Listez le contenu du répertoire

Recherchez les fichiers dont le nom commence par test

Recherchez dans `man` comment retrouver des fichiers qui ont été modifiés depuis 2 jours

Essayez cette recherche (les fichiers que nous avons créés aujourd'hui doivent sortir).

6. Personnalisation du shell

6A. Variables d'environnement

Un certain nombre de variables sont disponibles par défaut. Vous pouvez également en créer et elles peuvent être utilisées dans vos scripts.

Pour afficher les variables en cours :

```
# env
TERM=xterm
SHELL=/bin/bash
LC_ALL=fr_FR.UTF-8
USER=root
MAIL=/var/mail/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/root
LANG=fr_FR.UTF-8
PS1=\h:\w\$
SHLVL=1
HOME=/root
LOGNAME=root
_=/usr/bin/env
```

Atelier 12

Linux : la ligne
de commande

Page 174

Notez une variable fondamentale (PATH) qui comme dans les systèmes DOS/WINDOWS indique dans quels chemins chercher les commandes exécutables.

Pour définir une variable :

```
# export MAVAR=test
# env
TERM=xterm
SHELL=/bin/bash
LC_ALL=fr_FR.UTF-8
USER=root
MAVAR=test
MAIL=/var/mail/root
```

6B. historique

La commande history vous affiche toutes les dernières commandes tapées. Celles-ci sont conservées même après la fermeture de votre session. **Donc attention à la confidentialité et à la sécurité...**

Vous pouvez rappeler rapidement un commande en tapant un ! Suivi du début de la commande. Par exemple, je me rappelle que j'ai fait il n'y a pas longtemps une commande ls assez complexe. Si je fais :

```
# !ls
```

Le shell exécutera la dernière commande ls dans l'historique.

6C. alias

Il y a certaines commandes que vous exécutez très régulièrement. Par exemple, `ls -la`. Vous pouvez créer un alias pour la rappeler rapidement. Par exemple :

```
# alias ll='ls -la'
```

Maintenant, vous pouvez taper `ll` pour faire un `ls -la`.

Cet alias sera perdu si vous fermez votre session. Comment faire pour le rendre permanent ?

6D. Fichier de profil

Vous pouvez rendre permanent des variables d'environnement, des alias, etc. grâce aux fichiers de profil. Dans un système Unix, il en existe plusieurs et il n'est pas toujours très simple de s'y repérer. Je vous en donne deux :

- au niveau système (s'appliquera donc à tous les utilisateurs et également aux services réseau qui se lancent tout seuls) : `/etc/profile`
- au niveau utilisateur : fichier `.bashrc` situé dans le répertoire personnel.

À l'intérieur de ces fichiers, vous pouvez mettre n'importe quelle commande shell. Le premier fichier est exécuté au démarrage de la machine, le deuxième à chaque lancement d'un shell par l'utilisateur concerné.

7. Arrêt du système

Lorsque vous fermez votre session, cela n'arrête pas le système qui continue à être disponible pour d'autres utilisateurs.

Pour pouvoir l'arrêter, vous devez être connecté en tant qu'administrateur et utiliser la commande suivante :

Commandes	Effet
<code>shutdown now -h</code>	Arrête le système immédiatement
<code>shutdown now -r</code>	Arrête et redémarre le système immédiatement
<code>shutdown +5</code>	Arrêt du système dans 5 mn
<code>shutdown +5 «Vous devez vous déconnecter»</code>	Arrêt du système dans 5 mn et affiche un message supplémentaire aux utilisateurs.
<code>shutdown -c</code>	Bien pratique : annule un shutdown en cours.

À retenir

L'interpréteur de commande de Linux sert à donner des ordres au système. Il faut ouvrir une session puis saisir les commandes. Linux vérifie la syntaxe de la commande puis tente de l'exécuter. Une absence de message de la part de Linux, signifie généralement que la commande a fonctionné.

De nombreuses commandes sont disponibles, elles comportent souvent de multiples options. Le manuel en ligne donne toutes les informations à ce sujet.

Certaines commandes ne sont accessibles qu'à l'administrateur, comme par exemple la commande pour arrêter le système.

Si vous voulez approfondir

Comme pour l'atelier précédent, participer à un LUG peut être une bonne étape pour commencer.

Vous pouvez également vous procurer un mémento des commandes UNIX.

Atelier 13

Gestion des paquets Debian

► Objectif

Savoir utiliser les différents outils de gestion des paquets inclus dans votre Debian.

► Durée approximative de cet atelier : 1 heure

► Durée approximative de cet atelier

Aucune

► Considérations techniques

Debian est livré avec un outil très puissant permettant d'avoir accès « en-ligne » à plus d'une dizaine de milliers de logiciels et utilitaires. Il s'agit de la série de commandes apt qui permet de rechercher dans les paquets disponibles, de les installer, de les désinstaller, de les configurer, de connaître la liste des fichiers contenus, ...

► Contenu

1. Introduction	178
2. Quels paquets indispensables installer ?	181

Atelier 13

Gestion des paquets
Debian

Page 177

1. Introduction

Dans le monde Linux, il existe deux grandes catégories de gestionnaire de paquets (de logiciels si vous voulez). Dans le monde RedHat, Fedora, Mandriva, Suse, il s'agit de rpm. Pour Debian, Ubuntu et les autres dérivés, il s'agit de apt.

Apt est en réalité une interface à un outil de plus bas niveau appelé dpkg. Quelles différences ? Dpkg est capable d'installer un fichier de paquet (extension.deb) mais il n'est pas capable de :

- **gérer les dépendances** : il s'agit de pouvoir installer en cascade des paquets car ils sont interdépendants. Par exemple, on peut imaginer que le paquet apache-utils est dépendant du paquet apache-common. Cela signifie que apache-utils ne peut s'installer si apache-common n'est pas déjà installé. Dans ce cas, apt installe les paquets dans le bon ordre ;
- **chercher les paquets dans un dépôt**. Les dépôts sont des espaces de stockages (dvd, sites ftp ou http) qui contiennent une copie (un miroir) des dépôts officiels de Debian.

La suite de cet atelier vous est présentée comme une FAQ.

1A. Où ma Debian va-t-elle chercher les paquets ?

Cela revient à se poser la question : qu'est-ce qu'une source ? Il s'agit tout simplement d'une adresse où apt peut aller chercher des paquets. On peut consulter la liste des sources connues par notre machine :

```
mv2-linux:~# cat /etc/apt/sources.list
#
# deb cdrom:[Debian GNU/Linux 6.0.2.1 _Squeeze_ - Official amd64
NETINST Binary-1 20110628-12:58]/ squeeze main
#deb cdrom:[Debian GNU/Linux 6.0.2.1 _Squeeze_ - Official amd64
NETINST Binary-1 20110628-12:58]/ squeeze main
deb http://ftp.fr.debian.org/debian/ squeeze main
deb-src http://ftp.fr.debian.org/debian/ squeeze main
deb http://security.debian.org/ squeeze/updates main
deb-src http://security.debian.org/ squeeze/updates main
# squeeze-updates, previously known as 'volatile'
deb http://ftp.fr.debian.org/debian/ squeeze-updates main
deb-src http://ftp.fr.debian.org/debian/ squeeze-updates main
```

Dans cet exemple, la Debian Squeeze a été installée à partir d'une image iso d'un cédérom (netinst). Les dernières lignes correspondent à l'adresse d'un site de mise à jour.

Je vous laisse le soin de consulter le man sources.list qui est très bien fait. Vous apprendrez qu'une ligne de ce fichier peut avoir le format suivant :

```
deb uri distribution [composant1] [composant2] [...]
```

- uri peut être indifféremment cdrom, file, http ou ftp.
- distribution peut prendre l'une des valeurs suivantes : *stable*, *testing* ou *unstable* ou *testing*. À l'heure où j'écris ces lignes, la Debian « *stable* » est la *squeeze*, la Debian *testing* (donc la prochaine stable) est la *wheezy*. *Unstable* étant la prochaine prochaine distribution (donc, celle après la *testing*).
- composant peut être *main*, *contrib*, *non-free* ou *non-us*.

Un exemple de ligne dans le fichier pourrait être le suivant :

```
deb ftp://ftp.debian.org/debian stable main
```

En général, les paquets sont stockés dans les dépôts (ou des miroirs) Debian sur Internet. Ils changent en permanence du fait des mises à jour de la distribution. Il est donc indispensable de mettre à jour votre base de données locale avec un `apt-get update` **avant toute installation**.

1B. Comment savoir si un paquet est installé ?

Vous pouvez lister l'ensemble des paquets installés ou désinstallés avec la commande `dpkg -l`. Par exemple, pour lister les paquets en rapport avec Apache :

```
mv2-linux:~# dpkg -l bash*
Souhait=inconnU/Installé/suppRimé/Purgé/H=à garder
| État=Non/Installé/fichier-Config/dépaqUeté/échec-conFig/H=semi-
installé/W=attend-traitement-déclenchements
|/ Err?=(aucune)/H=à garder/besoin Réinstallation/X=les deux
(État,Err: majuscule=mauvais)
||/ Nom Version Description
+ + + - = = = = = = = = = = = = = = = = = = = = = = = = = = = -
=====
ii bash 4.1-3 The GNU Bourne Again SHell
```

Atelier 13

Gestion des paquets
Debian

Page 179

L'état d'un paquet est déterminé par les deux premiers caractères. Par exemple, un paquet noté « `ii` » est correctement installé et configuré.

1C. Comment trouver un paquet ?

Utilisez la commande `apt-cache search`. Par exemple, pour lister les paquets en rapport avec Samba :

```
mv2-linux:~# apt-get update
mv2-linux:~# apt-cache search samba
libsmbclient - shared library that allows applications to talk to
SMB/CIFS servers
samba - a LanManager-like file and printer server for Unix
samba-common - Samba common files used by both the server and the
client
samba-doc - Samba documentation
smbclient - a LanManager-like simple client for Unix
[...]
```

Vous pouvez également faire des recherches sur les paquets sur le site <http://packages.debian.org>.

1D. Comment installer/désinstaller un paquet ?

Pour installer :

```
mv2-linux:~# apt-get update
mv2-linux:~# apt-get install <nom_du_paquet>
```

Pour désinstaller :

```
mv2-linux:~# apt-get remove <nom_du_paquet>
```

Pour désinstaller et supprimer toute trace de l'installation, ajoutez `--purge` à la commande sinon apt conservera les fichiers contenus dans le paquet mais modifiés depuis l'installation (fichiers de configuration par exemple).

1E. Comment (re)configurer un paquet ?

Parfois, lors de l'installation d'un paquet, un outil de configuration est exécuté. Vous pouvez à tout moment exécuter cet utilitaire. Par exemple, pour reconfigurer le paquet locales :

```
mv2-linux:~# dpkg-reconfigure locales
```

1F. Comment lister les fichiers contenus dans un paquet ?

```
mv2-linux:~# # dpkg -L bash
/.
/etc
/etc/bash.bashrc
/etc/skel
/etc/skel/.profile
/etc/skel/.bashrc
/etc/skel/.bash_logout
/bin
/bin/bash
[...]
```

Atelier 13

Gestion des paquets
Debian

Page 180

1G. Comment tenir mon système à jour ?

Pour mettre à jour votre système Debian :

```
mv2-linux:~# apt-get update
mv2-linux:~# apt-get upgrade
```

Lorsque la mise à jour touche des paquets importants comme le noyau, il est nécessaire de passer par la commande suivante :

```
mv2-linux:~# apt-get dist-upgrade
```

Il va sans dire que la mise à jour de votre système doit se faire régulièrement afin de parer aux (fréquentes) failles de sécurité. Pour vous aider, il est plus que très fortement conseillé¹ de vous abonner à la liste de diffusion des correctifs de sécurité de Debian : <http://lists.debian.org/debian-security-announce>.

1. Ai-je été assez clair ;-) ?

2. Quels paquets indispensables installer ?

Vim	Par défaut, Debian installe un vi limité. Je vous conseille d'installer ce paquet qui rend vi un peu plus « humain » et efficace
Locate	Contient deux commandes : - updatedb : indexe dans une base de données, tous les noms de fichiers présents sur le système. N'hésitez pas à la lancer de temps en temps - locate : permet d'interroger cette base et donc de savoir où se trouve exactement un fichier.
Tree	Permet d'afficher la totalité d'une arborescence

À retenir

Les deux commandes permettant de gérer les paquets sous Debian sont :

- dpkg : outil de bas niveau
- apt : outil de plus haut niveau capable de chercher des paquets dans des dépôts et de gérer les dépendances.

Vous avez ainsi accès en une seule commande à la grande majorité des logiciels libres utilisés en entreprise.

Si vous voulez approfondir

Il existe des interfaces graphiques à apt qui permettent peut-être de faciliter la gestion des paquets. Par exemple : aptitude ou synaptic.

Atelier 13

Gestion des paquets
Debian

Page 181

Atelier 14

Généralités sur les services réseaux

► **Durée approximative de cet atelier : 1 heure**

► **Objectif**

À la fin de cet atelier, vous connaîtrez les caractéristiques communes à tous les services réseaux de Linux. Vous saurez déterminer les ports ouverts sur une machine, vous saurez où se trouvent les fichiers de configuration des services, comment lancer ou arrêter un service. Enfin, vous saurez suivre le fonctionnement des services grâce aux journaux systèmes.

► **Durée approximative de cet atelier**

Serveur Debian Linux installé.

► **Considérations techniques**

C'est un TP fondamental car il est préparatoire à tous les ateliers qui suivent dans ce fascicule.

► **Contenu**

1. Introduction	184
2. Configuration réseau	184
3. La notion de port.....	186
4. Les fichiers de configuration des services réseaux	189
5. Les journaux	191

1. Introduction

Dans le cours, nous vous présentons, étage par étage, le modèle OSI. Il va sans dire que vous devez impérativement maîtriser ces connaissances. Le modèle OSI est un outil de compréhension des réseaux absolument fondamental.

Dans les ateliers, nous allons intervenir essentiellement sur les aspects logiciels (couches OSI 3 à 7). Les TP « matériels » (couches OSI 1 et 2) ont été réalisés dans les modules de cours précédents. Vous avez sans doute remarqué dans les objectifs de cet atelier que le mot « service » est employé de multiples fois. En effet, c'est le propre d'un ordinateur dénommé « serveur » que de proposer des « services ».

Tous les services réseau (Web, DNS, DHCP, etc.) ont des caractéristiques et un mode de fonctionnement communs. Le but de cet atelier est de vous les présenter une fois pour toutes afin que vous les mettiez en œuvre à chaque atelier. Nous ne reviendrons donc plus dessus mais ce n'est pas pour cela que vous ne devrez pas par la suite utiliser les outils que nous allons vous présenter !

2. Configuration réseau

Avant d'aller plus loin, nous allons modifier la configuration réseau de notre machine pour passer en adressage IP statique. En principe, lors de l'installation, Debian a trouvé un serveur DHCP sur votre réseau (votre box si vous êtes chez vous) et n'a donc pas eu besoin de vous demander une adresse.

Connectez-vous sous Linux en tant que root. Ensuite, tapez la commande `ifconfig` qui donne la configuration des cartes réseau :

```
root@mv2-linux:~# ifconfig

eth0  Link encap:Ethernet HWaddr 08:00:27:9b:49:90
      inet adr:192.168.1.12 Bcast:192.168.1.255 Masque:255.255.255.0
      adr inet6: fe80::a00:27ff:fe9b:4990/64 Scope:Lien
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:6629 errors:0 dropped:0 overruns:0 frame:0
      TX packets:4613 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:1000
      RX bytes:8246520 (7.8 MiB) TX bytes:411816 (402.1 KiB)

lo    Link encap:Boucle locale
      inet adr:127.0.0.1 Masque:255.0.0.0
      adr inet6: ::1/128 Scope:Hôte
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:8 errors:0 dropped:0 overruns:0 frame:0
      TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:0
      RX bytes:560 (560.0 B) TX bytes:560 (560.0 B)
```

Notre machine Linux possède donc deux interfaces réseau :

- lo : interface réseau virtuelle qui représente la machine elle-même (lo = localhost ou hôte local). Son adresse IP est toujours 127.0.0.1
- eth0 : qui représente l'interface réseau Ethernet. Comme sous Windows, en l'absence de configuration particulière, elle récupère une adresse dynamique attribuée par le routeur via le protocole dhcp.

Afin d'être cohérent avec les machines Windows et en prévision des ateliers à venir, nous allons faire une configuration statique. Pour éditer le fichier de configuration, tapez la commande suivante :

```
# vi /etc/network/interfaces
```

Vous modifiez la ligne :

```
iface eth0 inet dhcp
```

par

```
iface eth0 inet static
```

Mettez avant cette ligne :

```
auto eth0
```

Puis après la ligne iface, ajoutez les lignes suivantes (à adapter éventuellement selon votre cas) :

```
address 192.168.1.102
netmask 255.255.255.0
gateway 192.168.1.1
```

Au final, vous devez donc obtenir ceci :

```
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
auto eth0
iface eth0 inet static
address 192.168.1.102
netmask 255.255.255.0
gateway 192.168.1.1
```

Ensuite, pour recharger les paramètres réseau de cette carte :

```
# ifdown eth0 && ifup eth0
```

Si l'on affiche maintenant les paramètres réseau :

```
# ifconfig

eth0  Link encap:Ethernet HWaddr 08:00:27:9b:49:90
      inet adr:192.168.1.102 Bcast:192.168.1.255 Masque:255.255.255.0
      adr inet6: fe80::a00:27ff:fe9b:4990/64 Scope:Lien
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:9646 errors:0 dropped:0 overruns:0 frame:0
      TX packets:5601 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:1000
      RX bytes:8579439 (8.1 MiB) TX bytes:527109 (514.7 KiB)

lo    Link encap:Boucle locale
      inet adr:127.0.0.1 Masque:255.0.0.0
      adr inet6: ::1/128 Scope:Hôte
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:8 errors:0 dropped:0 overruns:0 frame:0
      TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:0
      RX bytes:560 (560.0 B) TX bytes:560 (560.0 B)
```

Atelier 14

Généralités
sur les services
réseaux

Page 186

La connexion avec l'Internet doit fonctionner :

```
# nslookup www.cned.fr
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name: www.cned.fr
Address: 194.214.70.2
```

3. La notion de port

Nous ne rappelons pas le concept théorique de port de communication : revoyez le cours si vous avez un doute ou des difficultés ! Vous devez savoir que chaque service réseau ouvre un ou plusieurs ports sur la machine. Un certain nombre de ports (numéro inférieur à 1024) sont dits « well-known ports », c'est-à-dire « bien connus » : ils sont réservés à des services standards de l'Internet. En voici quelques uns :

Port	Type	Affectation
20	TCP	FTP Données
21	TCP	FTP Contrôle
22	TCP/UDP	SSH
25	TCP	SMTP
53	TCP/UDP	DNS
80	TCP/UDP	HTTP

Port	Type	Affectation
110	TCP/UDP	POP3
123	TCP/UDP	NTP
138	TCP/UDP	NETBIOS
139	TCP/UDP	NETBIOS
143	TCP/UDP	IMAP
161	TCP/UDP	SNMP
443	TCP/UDP	HTTPS
445	TCP/UDP	NETBIOS

Note : la plupart des services ont des numéros de port réservés pour TCP et UDP mais en général, c'est le port TCP qui est utilisé (en raison de la fiabilité de ce protocole).

Ils sont définis dans la RFC 1700 : <http://www.ietf.org/rfc/rfc1700.txt>. Votre machine les connaît aussi. Un fichier texte issu de la RFC 1700, liste tous ces ports bien connus. Sous Unix, ce fichier s'appelle /etc/services (extrait), consultez son contenu :

```
# cat /etc/services

# Network services, Internet style

[...]
tcpmux      1/tcp      # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp      sink null
discard     9/udp      sink null
sysstat     11/tcp     users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
gotd        17/tcp     quote
msp         18/tcp     # message send protocol
msp         18/udp
chargen     19/tcp     ttytst source
chargen     19/udp     ttytst source
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp     fspd
ssh         22/tcp     # SSH Remote Login Protocol
ssh         22/udp
telnet      23/tcp
[...]

```

Atelier 14

Généralités
sur les services
réseaux

Page 187

Vous pouvez également savoir quels ports sont réellement ouverts sur votre machine (autrement dit, quels services réseaux sont réellement actifs, ils sont dits « à l'écoute » : LISTEN).

Par exemple, avec la commande netstat -lt, je peux connaître les ports TCP ouverts sur ma machine :

```
# netstat -lt
Connexions      Internet  actives  (seulement serveurs)
Proto Recv-Q  Send-Q   Adresse locale   Adresse distante  Etat
tcp        0        0  *:sunrpc         *:                LISTEN
tcp        0        0  localhost:ipp    *:                LISTEN
tcp        0        0  localhost:smtp   *:                LISTEN
tcp        0        0  *:33349          *:                LISTEN
tcp6       0        0  [::]:ssh        [::]:*           LISTEN
tcp6       0        0  ip6-localhost:ipp [::]:*           LISTEN
tcp6       0        0  ip6-localhost:smtp [::]:*           LISTEN
```

On peut afficher la même information sous un format numérique et ainsi retrouver les numéros de ports :

```
# netstat -ltn
Connexions      Internet  actives  (seulement serveurs)
Proto Recv-Q  Send-Q   Adresse locale   Adresse distante  Etat
tcp        0        0  0.0.0.0:111      0.0.0.0:*         LISTEN
tcp        0        0  127.0.0.1:631    0.0.0.0:*         LISTEN
tcp        0        0  127.0.0.1:25     0.0.0.0:*         LISTEN
tcp        0        0  0.0.0.0:33349    0.0.0.0:*         LISTEN
tcp6       0        0  :::22            :::*               LISTEN
tcp6       0        0  :::1:631         :::*               LISTEN
tcp6       0        0  :::1:25          :::*               LISTEN
```

Atelier 14

Généralités
sur les services
réseaux

Page 188

Avec ces informations, je sais que le service smtp tourne sur ma machine et qu'il écoute (LISTEN) sur le port TCP 25. Celui-ci a été mis lors de l'installation. Le port 111 concerne NFS dont nous ne nous servirons pas (nous le supprimerons après). Mais qu'est-ce donc que le port 33349 ??? Ce numéro est supérieur à 1024, ce n'est donc pas un service standard TCP/IP ? Mais qu'est-ce ? Un virus ? Un cheval de Troie ???

Nous pouvons passer un paramètre supplémentaire à la commande netstat afin de savoir quel processus utilise ce port :

```
# netstat -plt
Connexions      Internet  actives  (seulement serveurs)
Proto Recv-Q  Send-Q   Adresse locale   Adresse distante  Etat  PID / Program name
tcp        0        0  *:33349         *:                LISTEN 3242/rpc.statd
```

Ouf. Il ne s'agit que d'un processus lié à NFS (rpc.statd). Nous allons le supprimer tout à l'heure.

Exercice 1

1. Faites afficher page par page le contenu de /etc/services.
2. Affichez la liste des ports TCP ouverts sur votre machine.
3. Trouvez le moyen d'afficher la liste des ports UDP ouverts sur votre machine.

Quelques remarques importantes :

- Les numéros de ports bien connus sont ceux généralement utilisés, ceci dit, on peut monter un serveur web qui écoute sur un autre port que le 80 par exemple.

- Ainsi, un autre serveur qu'un serveur web peut donc écouter sur le port 80. Cette technique est bien souvent employée par les chevaux de Troie pour franchir les pare-feux.
- Un serveur ne doit pas laisser de ports inutilisés ouverts car l'on multiplie le risque de piratage. En effet, un pirate peut connaître les ports ouverts sur une machine distante et parfois en déduire un moyen d'entrer dans le système. Vous ne devez laisser que les ports ouverts dont vous avez effectivement besoin ! Nous verrons plus loin comment désactiver les services inutilisés.

4. Les fichiers de configuration des services réseaux

Tous les fichiers de configuration des services réseaux sont stockés dans un endroit unique.

4A. Localisation

Sous Linux, tous les fichiers de configuration sont stockés dans le répertoire /etc. Soit il s'agit d'un fichier unique et dans ce cas, celui-ci est directement placé dans ce répertoire. Soit le service utilise plusieurs fichiers et dans ce cas, ils sont en général regroupés dans un sous-répertoire qui porte le nom du service. La plupart des noms de fichiers de configuration ont la forme : nom_du_service.conf.

Un simple éditeur de texte¹ suffit pour modifier une configuration. Par contre, il est nécessaire de relancer le service ou de lui indiquer de recharger sa configuration. **Ce n'est jamais fait à chaud.**

4B. Lancement des services réseaux

Comment démarrer un service réseau ou l'obliger à recharger sa configuration ?

4B1. À chaud

À tout moment, vous pouvez démarrer, arrêter et redémarrer des services² même si ceux-ci sont en cours d'utilisation par des utilisateurs ! Pour connaître les noms des services, listez le contenu du répertoire /etc/init.d.

Un service s'appelle aussi un démon (daemon en anglais). C'est pourquoi, beaucoup de noms de services se terminent par un d. D'autres fichiers se terminent par.sh c'est l'extension pour shell, ce sont des scripts. Lorsque le service a été installé, un script de démarrage a été copié dans /etc/init.d.

Souvenez-vous que suite à n'importe quelle modification d'un fichier de configuration, vous devez redémarrer le service ! Pour ce faire il suffit de nommer le service et de donner une instruction. Parmi les plus fréquentes :

- start : démarre le service ;
- stop : arrête le service ;
- reload : demande au service de recharger les fichiers de configuration sans redémarrer. Mais attention, tous les services ne savent pas le faire...
- restart : arrête le service puis le redémarre.

1. D'une part, vos services réseau ne pourront rien vous cacher dans des fichiers binaires incompréhensibles. Ensuite, vous pourrez faire toute la configuration en ligne de commandes et ainsi avoir des serveurs qui ne perdent pas bêtement leur puissance de calcul dans des interfaces graphiques ultra gourmandes de ressources mémoire, processeur et disques !

2. Eh oui, jamais besoin de redémarrer l'ordinateur !

Pour chaque service, vous pouvez savoir quels paramètres sont acceptés. Par exemple, pour Samba :

```
# /etc/init.d/samba
Usage: /etc/init.d/samba {start|stop|reload|restart|force-reload}
```

4B2. À froid

C'est-à-dire au démarrage de la machine. À un instant donné toute machine Linux est dans un mode de fonctionnement : on dit runlevel.

Il existe 6 runlevels sous Linux :

- Le runlevel 0 correspond à l'arrêt du système.
- Le runlevel 1 correspond au démarrage single-user.
- Le runlevel 2 correspond mode de démarrage normal (sous Debian).
- Les runlevels 3-5 correspondent à des modes de démarrage variables selon les distributions et a priori non utilisé sous Debian.
- Le runlevel 6 correspond au redémarrage.

Donc, votre Debian a démarré en runlevel 2 :

```
# runlevel
N 2
```

Le N correspond au mode de démarrage précédent (aucun en fait).

Le runlevel de démarrage est configuré dans le fichier `/etc/inittab` sur la directive `initdefault`. Je vous laisse le soin de vérifier mes dires.

Dans tous les cas, cela signifie que notre Debian a exécuté lors de son démarrage les scripts situés dans le répertoire `/etc/rc<runlevel par défaut>.d`. Listons le contenu de ce répertoire :

```
# ls /etc/rc2.d
README S18acpi-fakekey S18virtualbox-ose-guest-utils
S19anacron S19cron S19exim4 S20bluetooth S22rc.local
S15portmap S18fancontrol S19acpid S19apmd S 1 9 c u p s
S19loadcpufreq S20cpufrequtils S22rmnologin
S16nfs-common S18rsyslog S19acpi-support S19atd S19dbus
S21bootlogs S22stop-bootlogd
```

Ceci est la liste des services qui sont lancés au démarrage. Vous remarquez un S majuscule devant chaque script qui signifie Start suivi d'un numéro qui définit la priorité (les plus petits sont lancés en premier).

La commande `telinit` permet de changer de runlevel. Tapez `telinit 6` en tant que `root` ;-)

4C. Désactiver les services

Vous avez deux solutions : désactiver temporairement ou désinstaller définitivement le service.

- Désactiver temporairement.

La commande `update-rc.d` permet de gérer les services lancés dans les différents runlevel. Par exemple, pour ajouter le script `mon_script` dans tous les runlevel :

```
# update-rc.d mon_script defaults
```

Pour retirer le script `mon_script` de tous les runlevel :

```
# update-rc.d -f mon_script remove
```

Remarque : cela n'arrête pas le service en cours d'exécution.

Pour régler avec précision un script dans un runlevel (celui-ci ne doit pas du tout être présent dans les runlevel) :

```
# update-rc.d mon_script start 42 2 3 5. stop 31 0 6.
```

Ce qui démarre `mon_script` dans les runlevel 2, 3 ou 5 avec une priorité 42 et arrête `mon_script` avec une priorité 31 dans les runlevel 0 et 6 (ceci est un exemple).

- Désinstaller : il suffit de lancer la commande `apt-get remove <paquet>`. Le service sera arrêté proprement puis désinstallé. Vous serez tranquille !

Exercice 2

1. Faites le ménage dans les services actifs sur votre serveur. Ne conservez que ce dont vous avez réellement besoin. Ce n'est pas un exercice facile mais pourtant, il est très important.
2. Utilisez la commande `man` et Internet afin de connaître le rôle de chaque service et donc de déduire son utilité dans votre configuration.

5. Les journaux

Les journaux sont des fichiers dans lesquels sont enregistrés des événements rencontrés par le système afin d'en garder une trace pour l'administrateur.

5A. Localisation

Les fichiers sont stockés dans `/var/log`. Concernant les services réseaux, sous Linux, le fichier le plus intéressant est de loin `/var/log/syslog`. Celui-ci vous livrera une masse d'informations qui pourra vous aider à dépanner vos configurations ou surveiller l'activité de vos services. Cependant, ne négligez pas les journaux générés directement par le service. Ils portent généralement le nom du service.

5B. Consultation

Plusieurs solutions existent. Pour ne consulter que les lignes du fichier les plus récentes, la commande `tail` est une bonne solution. Pour rechercher les événements liés à un service donné, la commande `grep` est bien utile. Par exemple, je cherche les événements liés à `apt` :

- Allez dans `/var/log`
- Listez le contenu
- Vous voyez un répertoire `apt`. Vous entrez dans ce répertoire et listez le contenu :

```
# ls -la
total 32
drwxr-xr-x 2 root root 39 4 août 07:41.
drwxr-xr-x 8 root root 4096 4 août 15:07..
-rw-r--r-- 1 root root 17477 4 août 15:50 history.log
-rw----- 1 root root 6772 4 août 15:50 term.log
```

Vous pourrez retrouver par exemple l'historique des paquets installés ou désinstallés. Même si le listing obtenu vous semble pour le moment confus, ce que nous voulons ici c'est vous signaler toute l'information disponible sur un service donné ; ainsi, le jour où, devenu spécialiste de tel service, vous désirez suivre de très près le fonctionnement et l'utilisation du service, avec Debian vous savez que tout vous est possible...

Si vous voulez avoir un regard permanent sur le fichier journal, utilisez la commande `tail -f /var/log/messages` dans un terminal. La mise à jour sera automatique.

À retenir

Un service réseau correspond à au moins un port TCP ou UDP.

Tous les fichiers de configuration sont stockés dans le répertoire `/etc`, soit dans un fichier dont le nom est généralement le nom du service suivi de `.conf`, soit dans un sous-répertoire portant le nom du service, éventuellement suivi d'un `.d`.

Les fichiers journaux contiennent une trace de l'activité du système et des services réseaux. Le principal fichier s'appelle `/var/log/syslog` mais bien souvent, chaque démon gère un ou plusieurs fichiers journaux stockés dans `/var/log` ou dans un sous-répertoire.

Si vous voulez approfondir

Vous pouvez regarder du côté d'utilitaires comme `nmap` qui permettent de connaître à distance les ports ouverts sur une machine distante.

Étudiez également les techniques employées par les virus comme les « chevaux de Troie » ou (trojans), qui exploitent les ports TCP/UDP.

Atelier 14

Généralités
sur les services
réseaux

Atelier 15

Gestion des utilisateurs et des permissions

► Objectif

À la fin de cet atelier, vous saurez faire une gestion basique des utilisateurs d'un système informatique. Vous saurez créer des utilisateurs, les affecter à des groupes, leur donner accès à un répertoire personnel et, enfin, leur attribuer des permissions sur des fichiers et des répertoires.

► Durée approximative de cet atelier : 1 heure 30

► Durée approximative de cet atelier

Serveur Linux Debian

► Mise en place de l'atelier

La gestion des utilisateurs est la brique fondamentale d'un système informatique sécurisé. Lorsqu'un utilisateur souhaite utiliser le système, il doit s'identifier en fournissant un nom d'utilisateur (*login*) et un mot de passe (*password*). Si l'identification est acceptée, l'utilisateur est autorisé à accéder au système. Mais il ne sera pas libre de faire n'importe quoi, il évoluera dans le « terrain de jeu » que vous (l'administrateur) aurez soigneusement délimité.

► Matériel et logiciel nécessaires

Aucun en particulier, vous n'avez besoin que de votre réseau.

► Contenu

1. Gestion des groupes d'utilisateurs.....	194
2. Gestion des utilisateurs.....	195
3. Gestion des permissions	196

1. Gestion des groupes d'utilisateurs

Les utilisateurs d'un système informatique font toujours partie d'au moins un groupe d'utilisateurs. Les groupes facilitent le travail de l'administrateur et permettent d'attribuer en une seule étape des permissions à un ensemble d'utilisateurs. Généralement, les groupes d'utilisateurs correspondent à des services de l'entreprise. En effet, les utilisateurs d'un même service ont souvent besoin d'accéder aux mêmes fichiers, aux mêmes applications, aux mêmes imprimantes, etc. Ils ont beaucoup de permissions en commun.

1A. Le fichier /etc/group

Les caractéristiques des groupes sont contenues dans le fichier /etc/group. Listez le contenu de ce fichier :

Exemple de contenu :

```
ident:x:98:  
rpc:x:32:  
rpcuser:x:29:  
xfs:x:43:  
apache:x:48:
```

Exercice 1

Recherchez la signification des champs du fichier en tapant la commande : `man group`

1B. Principales commandes de gestion des groupes

Exercice 2

Indiquez le rôle de chacune des commandes suivantes en consultant l'aide en ligne :

```
groupadd <nom_de_groupe>  
groupdel <nom_de_groupe>  
groupmod <nom_de_groupe>  
groups <nom_utilisateur>
```

Exercice 3

- Créez un groupe d'utilisateurs appelé `bts`
- Affichez à nouveau le contenu du fichier /etc/group

2. Gestion des utilisateurs

Le fichier `/etc/passwd` contient l'ensemble des utilisateurs du système Linux.

2A. Principales commandes

Exercice 4

Listez le contenu du fichier `/etc/passwd`

Recherchez la signification des champs du fichier en tapant la commande : `man 5 passwd`

Exercice 5

Indiquez le rôle de chacune des commandes suivantes en consultant l'aide en ligne :

```
useradd <nom_utilisateur>
userdel <nom_utilisateur>
usermod <nom_utilisateur>
passwd <nom_utilisateur>
```

Exercice 6

- Créez deux utilisateurs `util1` et `util2` (recherchez dans l'aide le paramètre à indiquer pour affecter l'utilisateur au groupe `bts`)
- Visionnez le contenu du fichier `/etc/passwd` pour contrôler la création de ces deux comptes
- Vérifiez que `util1` fait bien partie du groupe `bts` (utilisez la commande `groups`)
- Attribuez aux deux utilisateurs un mot de passe.

Au sujet des mots de passe, retenez bien ceci : le mot de passe est la brique de base d'une politique de sécurité dans un réseau. Une politique de sécurité, c'est comme une chaîne : elle ne vaut que par son maillon le plus faible. Si vos utilisateurs ont des mots de passe trop faciles à trouver, ils compromettent la sécurité du système informatique dans son ensemble !

Qu'est-ce qu'un bon mot de passe ? C'est une suite de lettres majuscules et minuscules, de chiffres et de caractères variés d'au moins 6 caractères de long. Par exemple : `yaKA12#`

2B. Mais qui est connecté sur ma machine ?

La commande `who` permet de savoir qui est connecté.

Exercice 7

- Faites un `who`.
- Quel est le sens des 4 colonnes qui apparaissent (`man who` si besoin) ?

Pour savoir à tout instant "quel utilisateur vous êtes", faites un `who am i` (`who suis je marche aussi !`). Mais ne comptez pas sur cette commande pour répondre à des questions existentielles !

Atelier 15

Gestion
des utilisateurs
et des permissions

Page 195

Enfin, dernier point, la commande `w` vous donnera des informations plus détaillées :

```
# w
13:58:32 up 1:29, 3 users, load average: 0,00, 0,00, 0,00
USER      TTY          FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
root     tty1                13:24  7:33   0.45s  0.31s -bash
```

3. Gestion des permissions

3A. Les permissions sur les fichiers

Elles vont servir à définir ce que les utilisateurs peuvent et ne peuvent pas faire au niveau du système de fichiers.

Exercice 8

Indiquez le rôle de chacune des commandes suivantes en consultant l'aide en ligne :

```
chown <nouveau_propriétaire> <nom_du_fichier>
chgrp <nouveau_groupe> <nom_du_fichier>
chmod <permissions> <nom_du_fichier>
```

En tant que `root`, créez un répertoire `/travail`. Faites ensuite un `ls -la` à la racine du système de fichiers, vous devez obtenir (extrait) :

```
...
drwxrwxrwt 6 root root 4096 mar 5 23:38 tmp
drwxr-xr-x 2 root root 4096 mar 6 00:18 travail
...
```

Atelier 15

Gestion
des utilisateurs
et des permissions

Page 196

Pas évident à déchiffrer en première approche. Reprenons une figure que je vous ai déjà présenté lors de l'atelier sur la ligne de commandes Linux :

```
_ r w x r _ x _ _ _ 1 root adm 3488 Jan 20 16:48 toto.c
```

nom du fichier
date et heure de dernière modification
taille du fichier
groupe
propriétaire du fichier
nombre de liens
droits d'accès de tous les autres utilisateurs (others)
droits d'accès du groupe (group)
droit d'accès du propriétaire (user)
mode du fichier

Les permissions peuvent être :

- `r` : permission en lecture
- `w` : permission en écriture
- `x` : permission d'exécution pour un fichier, permission d'entrer dans un répertoire

Exercice 9

À partir de la figure précédente, répondez aux questions concernant la ligne ci-dessous :

```
drwxr-xr-x 2 root root 4096 mar 6 00:18 travail
```

- Ici, quel est le « mode » ? Que cela signifie-t-il ?
- Qui est le propriétaire du répertoire /travail ?
- Quelles sont les permissions de l'utilisateur root sur /travail ? Que cela signifie-t-il ?
- Quelles sont les permissions des membres du groupe root sur ce répertoire ? Que cela signifie-t-il ?
- Quelles sont les permissions des autres utilisateurs (ni l'utilisateur root, ni les membres du groupe root) sur ce répertoire ? Que cela signifie-t-il ?

À la racine, tapez la commande :

```
# chmod o-rx /travail
```

Cette commande (chmod) retire (-) les permissions r (lecture) et x (exécution) à tous les utilisateurs (o = others, donc tous sauf le propriétaire et le groupe du propriétaire). Faites un `ls -la` pour voir le changement :

```
# ls -la
...
drwxr-x--- 2 root root 1024 mar 2 04:21 travail
...
```

Essayez, en étant `util1`, de rentrer dans ce répertoire :

```
$ cd /travail
bash: cd: /travail: Permission denied
```

Exercice 10

Impossible ! À vous de jouer pour lui permettre de rentrer à nouveau (mais uniquement rentrer, donc impossibilité de créer un fichier) dans le répertoire.

Exercice 11

- En tant que root, créez dans /travail un répertoire que vous appellerez /travail/tplinux.
- Faites en sorte que seuls l'utilisateur root et les membres du groupe bts (et uniquement eux) puissent écrire à l'intérieur de tplinux. Je vous donne le résultat à obtenir :

```
# ls -la
total 3
drwxr-xr-x 3 root root 1024 mar 2 05:23.
drwxr-xr-x 20 root root 1024 mar 2 05:22..
drwxrwxr-x 2 root bts 1024 mar 2 05:25 tplinux
```

1. Si vous ne savez pas répondre à ces questions, faites un `man chmod`

Faites en sorte que util1 soit le propriétaire du répertoire. Je vous donne le résultat à obtenir :

```
# ls -la
total 3
drwxr-xr-x 3 root root 1024 mar 2 05:23.
drwxr-xr-x 20 root root 1024 mar 2 05:22..
drwxrwxr-x 2 util1 bts 1024 mar 2 05:25 tplinux
```

Revenez à la racine et rétablissez la permission r à tous les utilisateurs sur le répertoire / travail :

```
# chmod o+r /travail/
```

Exercice 12

Util1 est propriétaire du répertoire tplinux et il possède la permission d'écriture (w).

```
drwxrwxr-x 2 util1 bts 4096 fév 14 04:44 tplinux
```

Pourtant, s'il essaie de supprimer ce répertoire, il obtient :

```
rmdir: `tplinux': Permission non accordée
```

Savez-vous pourquoi ? Proposez une solution pour que util1 puisse supprimer ce répertoire (aide : il faut être root pour résoudre le problème).

Atelier 15

Gestion
des utilisateurs
et des permissions

Page 198

3B. Les permissions sur une application

Vous voulez que root puisse compiler des programmes développés en langage C mais que vos utilisateurs ne puissent pas le faire.

Tout système Unix qui se respecte est livré avec tout le kit de développement en langage C/C++.

3B1. Installation des paquetages

Il faut installer le paquet gcc si celui-ci n'est pas disponible.

3B2. Vérification de l'installation

Connectez-vous en util1, éditez avec vi le fichier hello.c ci-dessous en respectant scrupuleusement la syntaxe :

```
#include <stdio.h>
main()
{
printf("hello, world\n");
}
```

Ensuite, quittez vi puis compilez :

```
$ gcc hello.c
$
```

Il ne doit y avoir aucune erreur. Enfin, exécutez votre programme :

```
$/a.out
hello, world
$
```

Parfait! Le kit de développement est installé.

Si cela ne marche pas, analysez les erreurs :

```
# gcc hello.c
bash: gcc: command not found
# gcc hello.c
gcc: hello.c: Aucun fichier ou
répertoire de ce type
gcc: No input files
# gcc hello.c
hello.c: In function `main':
hello.c:6: parse error before
`}'
```

Le kit de développement est mal installé. Vérifiez bien que l'ensemble des paquetages a été installé et qu'il n'y a pas eu d'erreur lors du apt-get.

Vous vous trompez sur le nom du fichier source ou bien vous n'êtes pas au bon endroit. Placez-vous dans le répertoire qui contient le fichier hello.c. Vérifiez le nom du fichier.

Il s'agit d'une erreur de compilation. J'ai oublié quelque chose à la ligne 6. Je dois contrôler mon programme avec celui fournit par mon professeur.

3B3. Retrait des permissions

Je veux empêcher mes utilisateurs d'utiliser gcc. Pour ce faire, je vais leur interdire l'utilisation de la commande gcc. Mais où est cette commande ?

Connectons-nous en root, puis cherchons la commande gcc :

```
# which gcc
/usr/bin/gcc
```

Allons dans /usr/bin puis listons les droits de gcc :

```
# cd /usr/bin
# ls -la gcc
lrwxrwxrwx 1 root root 7 fév 19 13:15 gcc -> gcc-4.4
```

gcc est en fait un lien symbolique qui pointe vers gcc-4.3. Listons les droits :

```
-rwxr-xr-x 1 root root 207648 déc 31 2008 gcc-4.4
```

Tout le monde peut l'exécuter. Retirons ce droit :

```
# chmod o-x gcc-4.4
```

Redevenons util1 et retenons une compilation :

```
$ gcc hello.c
bash: /usr/bin/gcc: Permission denied
```

Ben non, ça ne marche plus. C'est ce qu'on voulait. Travail accompli !

À retenir

Linux possède une gestion des groupes et des utilisateurs autorisés à utiliser le système. On dispose de toutes les commandes pour les créer, les modifier et les supprimer. Linux est un système sécurisé. Il est possible d'attribuer ou de retirer des permissions à ces utilisateurs. Les permissions habituelles sont : le droit de lecture (r), le droit d'écriture (w) et le droit d'exécuter (x). Ces permissions peuvent être attribuées sur un fichier ou un répertoire. Le système de fichier différencie les permissions affectées à l'utilisateur propriétaire du fichier, au groupe propriétaire et à tous les autres utilisateurs.

Atelier 15

Gestion
des utilisateurs
et des permissions

Page 200

Atelier 16

Administration à distance

► Objectif

À la fin de cet atelier, vous aurez installé les outils permettant une administration à distance sécurisée de votre serveur.

► Durée approximative de cet atelier : 1 heure 30

► Condition préalables

La réalisation de l'atelier sur Linux : interface en ligne de commande est absolument indispensable.

► Mise en place de l'atelier

Comme déjà évoqué avec Windows, administrer à distance une machine est une pratique courante dans l'entreprise. En général, les serveurs sont dans une pièce à part, climatisée et sécurisée ou hébergés dans un datacenter. Cette administration à distance doit pouvoir se faire de façon simple mais complètement sécurisée puisque par définition, vous connecterez en tant qu'administrateur et qu'il ne faut donc pas que de petits curieux scrutent ce que vous faites. Personnellement, je crois que ssh est l'outil que j'utilise le plus dans mon travail...

Atelier 16

Administration
à distance

Page 201

► Matériel et logiciel nécessaires

Côté serveur : nous travaillerons avec le logiciel serveur Openssh 5.5 (paquet Debian)

Côté client : nous utiliserons le logiciel putty 0.61 (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>)

► Que faire si je bloque ?

Cet atelier ne doit pas poser de problème particulier. Si c'est le cas, utilisez la procédure classique : ping, netstat, analyse des journaux (/var/log/syslog et /var/log/auth.log en particulier.)

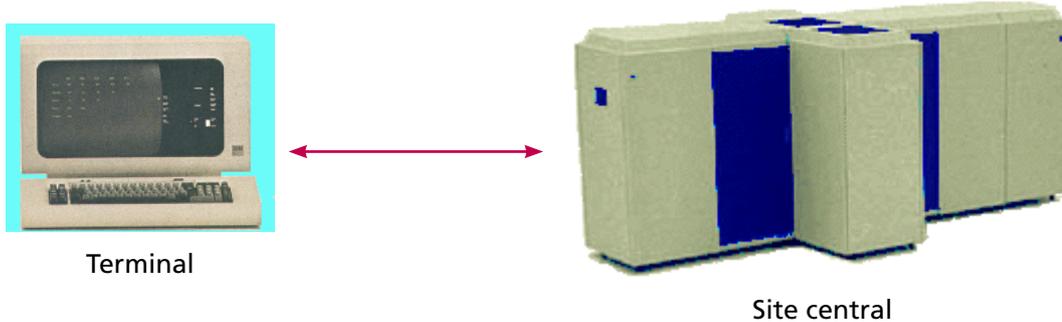
► Contenu

1. Connexion par terminal	202
2. Le chiffrement à clés asymétriques	204
3. Installation côté serveur	205
4. Installation côté client.....	206

1. Connexion par terminal

1A. Pourquoi se connecter avec un terminal ?

Comme je vous l'ai dit lors de l'installation, Linux c'est un Unix. Unix date des années 60-70. A cette époque, le micro-ordinateur n'existait pas. Sur les bureaux, on trouvait des terminaux reliés à d'énormes machines occupant des salles entières :



Le principe du terminal reste toujours d'actualité pour se connecter à une machine Linux. Seulement aujourd'hui, sur nos bureaux, on ne trouve plus de terminaux mais des micros. Alors, on a imaginé des terminaux virtuels (ou émulateurs de terminaux) qui, dans une fenêtre, font « comme si ».

Le roi des terminaux virtuels s'appelle **telnet**. C'est un moyen pratique et efficace de prendre le contrôle à distance d'un appareil et de faire comme si on était connecté directement dessus. Beaucoup d'appareils réseau (comme des commutateurs, des routeurs...) proposent un service telnet pour les configurer.

Néanmoins, **telnet est délaissé car il n'est pas sécurisé**. En effet, tout ce que vous tapez dans le terminal circule en clair sur le réseau. Il est alors possible de capturer les paquets et de les analyser (ainsi que vous apprendrez à le faire dans un prochain TP). C'est pourquoi, nous allons installer et utiliser ssh (Secure Shell) qui nous permet de faire l'équivalent de Telnet mais de façon sécurisée.

Enfin, prendre le contrôle à distance de vos serveurs reste indispensable puisque bien souvent, les serveurs ne sont pas dans l'entreprise mais hébergés dans un datacenter. Ici, pas de chaise, pas bureau mais des alignements d'armoires remplies de serveurs, routeurs, commutateurs, etc.



Figure 1 : Armoires de serveurs dans un datacenter

Commençons par définir quelques termes de vocabulaire.

1B. Qu'est-ce que chiffrer ?

C'est tout simplement l'opération par laquelle un message en clair est transformé en un message inintelligible pour tout intercepteur qui ne dispose pas de la **clé**.

La **clé** représente la méthode et/ou l'information nécessaire au déchiffrement.

Enfin, petite précision de vocabulaire : on devrait dire **chiffrement** et non pas cryptage, ainsi que **déchiffrement** et non pas décryptage. Le terme de décryptage consiste à tenter de découvrir le sens d'une information chiffrée sans y être autorisé.

Exercice 1

Vous êtes un chef gaulois et vous voulez envoyer un message stratégique à l'un de vos alliés, mais vous craignez que les romains n'interceptent ce message. Dans ce cas, votre plan serait anéanti. Vous voulez donc que votre message, dans l'éventualité où il serait récupéré par un romain soit incompréhensible.

- Proposez une solution.
- Donnez un exemple.

Vous avez compris que le but recherché en informatique est de rendre illisible les données stockées ou échangées au travers des réseaux. Après les différents TP que nous avons réalisés, je pense que vous avez maintenant conscience que les réseaux ne sont pas sûrs car la plupart des informations circulent en « clair » (elles sont donc non chiffrées).

1C. A propos de la clé

Si vous voulez que le ou les destinataires de votre message soient en mesure de le déchiffrer, il faut qu'ils connaissent la clé.

Exercice 2

Imaginez plusieurs solutions pour fournir à vos interlocuteurs la clé pour déchiffrer vos messages. Réfléchissez aux risques et contraintes que cela suppose. Imaginez en particulier que vous n'avez pas un seul interlocuteur mais des dizaines (voire beaucoup plus !).

Vous comprenez où je veux en venir ? Rendre les messages illisibles est une première problématique. Mais transmettre et protéger la clé est sans doute une problématique encore plus complexe. Ça serait tellement plus simple si on pouvait chiffrer et déchiffrer, non pas avec la même clé, mais avec deux clés différentes. Avec une clé, connue de tous, je chiffrais mon message. Dans ce cas, la diffusion de la clé ne poserait pas de problème. Ensuite, seule, la personne titulaire de la clé de déchiffrement pourrait découvrir le contenu du message. Ça serait tellement bien...

Vous savez quoi ? Ça existe ! Ça s'appelle le **chiffrement à clés asymétriques** et c'est même la base de toutes les méthodes de chiffrement utilisées dans les réseaux informatiques. Tout d'abord, nous allons expliquer le principe puis nous mettrons en œuvre dans deux situations.

2. Le chiffrement à clés asymétriques

Partons d'un petit exemple.

Supposons qu'une personne A (appelons-la Alice) désire transmettre des données chiffrées à une personne B (appelons-la Bernard). Bernard doit posséder un couple de clés :

- une clé privée **que lui seul possède et qui n'est jamais transmise** ;
- une clé publique que Alice doit aussi posséder. La clé doit lui être transmise ou bien elle peut se la procurer dans un annuaire.

Le processus de chiffrement sera le suivant :

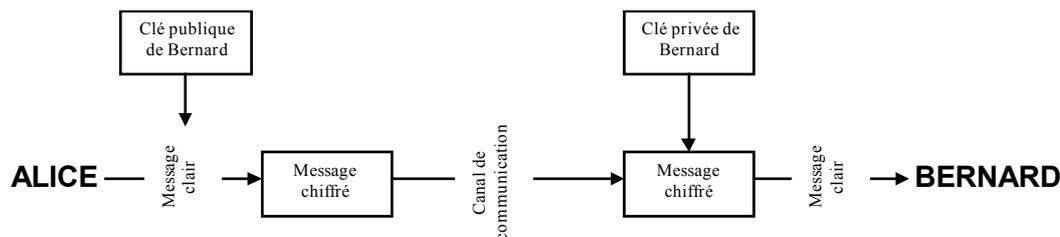


Figure 1 : exemple de chiffrement à clés asymétriques

Exercice 3

Je sais que ce schéma, qui paraît simple au premier abord, pose toujours des problèmes lorsque l'on interroge ensuite les étudiants. Voici quelques questions de « lecture » afin d'attirer votre attention sur les points importants :

- Qui est l'émetteur ? Qui est le destinataire ?
- Qui chiffre ? Avec quelle clé ? A qui appartient cette clé ?
- Qui déchiffre ? Avec quelle clé ? A qui appartient cette clé ?

Exercice 4

Alice souhaite maintenant envoyer un message chiffré à Charlotte. Comment doit-elle s'y prendre ?

Exercice 5

Sous quelle(s) condition(s), Bernard peut envoyer un message chiffré à Alice.

En supposant que cette condition soit remplie et en vous inspirant de la figure 1, représentez l'échange d'un message chiffré de Bernard vers Alice.

3. Installation côté serveur

En premier lieu, vérifions ce qui est déjà installé :

```
# dpkg -l | grep ssh
ii openssh-blacklist          0.4.1          list of default blacklisted
OpenSSH RSA and DSA keys
ii openssh-blacklist-extra 0.4.1          list of non-default
blacklisted OpenSSH RSA and DSA keys
ii openssh-client             1:5.5p1-6     secure shell (SSH) client,
for secure access to remote machines
```

En général, le client ssh est installé par défaut mais il n'est pas nécessaire pour le serveur. Pur ce qui concerne les paquets « blacklist », jetez un coup d'oeil à ceci : <http://wiki.debian.org/SSLkeys>. Vous verrez que nos amis de Debian ont fait très très fort !!!

Installons la partie serveur puisque nous voulons utiliser ssh pour administrer notre serveur Linux à distance :

```
# apt-get update
# apt-get install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Paquets suggérés :
  ssh-askpass rssh molly-guard ufw
Les NOUVEAUX paquets suivants seront installés :
  openssh-server
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis
à jour.
Il est nécessaire de prendre 318ko dans les archives.
Après cette opération, 823Ko d'espace disque supplémentaires
seront utilisés.
Réception de : 1 http://ftp.fr.debian.org/debian/ squeeze/main
openssh-server...
...
Paramétrage de openssh-server (1:5.5p1-6)...
Creating SSH2 RSA key; this may take some time...
Creating SSH2 DSA key; this may take some time...
Restarting OpenBSD Secure Shell server: sshd.
```

La fin est particulièrement intéressante. L'installation a créé deux couples de clés publique/privée, à la fois avec l'algorithme RSA et l'algorithme DSA. Ces clés sont propres à la machine, la clé privée ne doit jamais être compromise.

Exercice 6

Vous recherchez l'endroit où sont stockés les fichiers de clés du serveur openssh et vous listez les droits d'accès. Qu'en pensez-vous ?

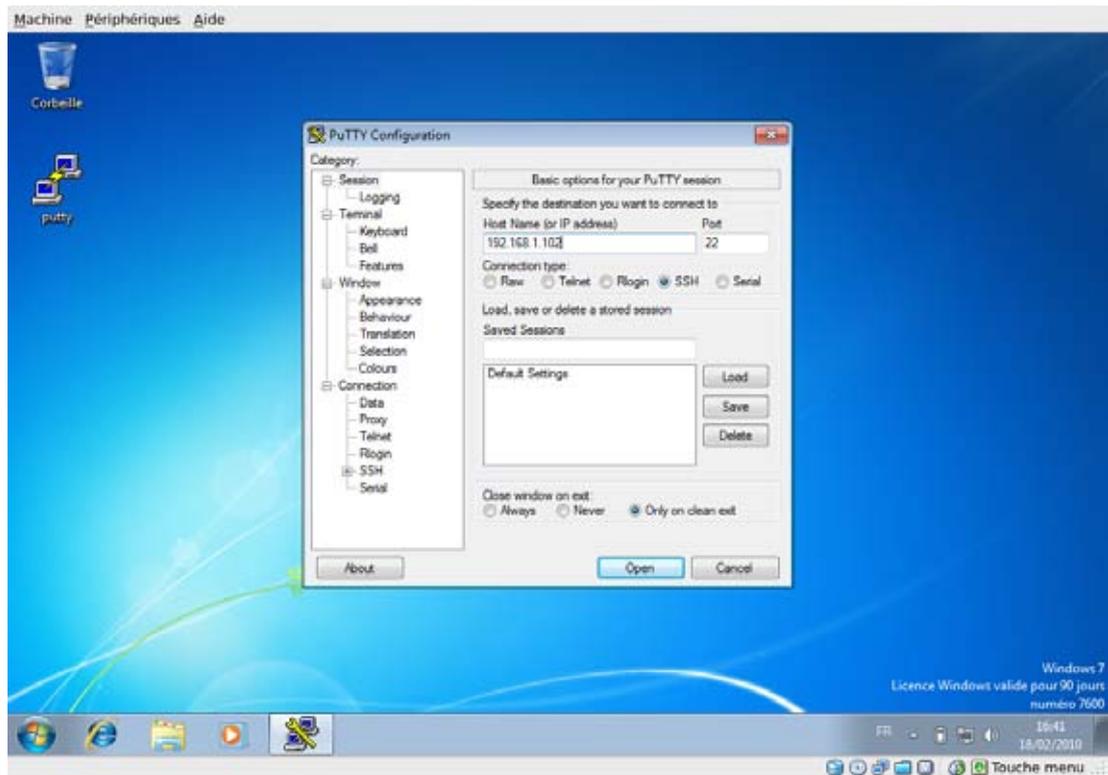
Je répète : la clé privée ne doit jamais quitter la machine et ne doit être accessible par personne (sauf à root bien entendu). Si tel était le cas, il serait possible pour une personne malintentionnée de « bluffer » vos utilisateurs et de les diriger vers un faux serveur, sans qu'ils s'en rendent compte.

4. Installation côté client

Sous Windows, il n'existe pas de client ssh intégré et vous n'avez pas beaucoup de choix dans les outils gratuits. Dans mon entreprise, nous utilisons les excellents putty et winscp :

4A. Connexion en mode terminal : putty

Téléchargez putty et exécutez-le. Vous obtenez la fenêtre ci-après. Indiquez simplement l'adresse IP puis cliquez sur « Open » :



Atelier 16

Administration
à distance

Page 206

Figure 2 : Écran de connexion de putty

Lors de votre première connexion, le client ssh (putty ou autre) va garder un certain nombre de données identifiant le serveur. Cela permettra par la suite de vous assurer que vous vous connectez sur la bonne machine.

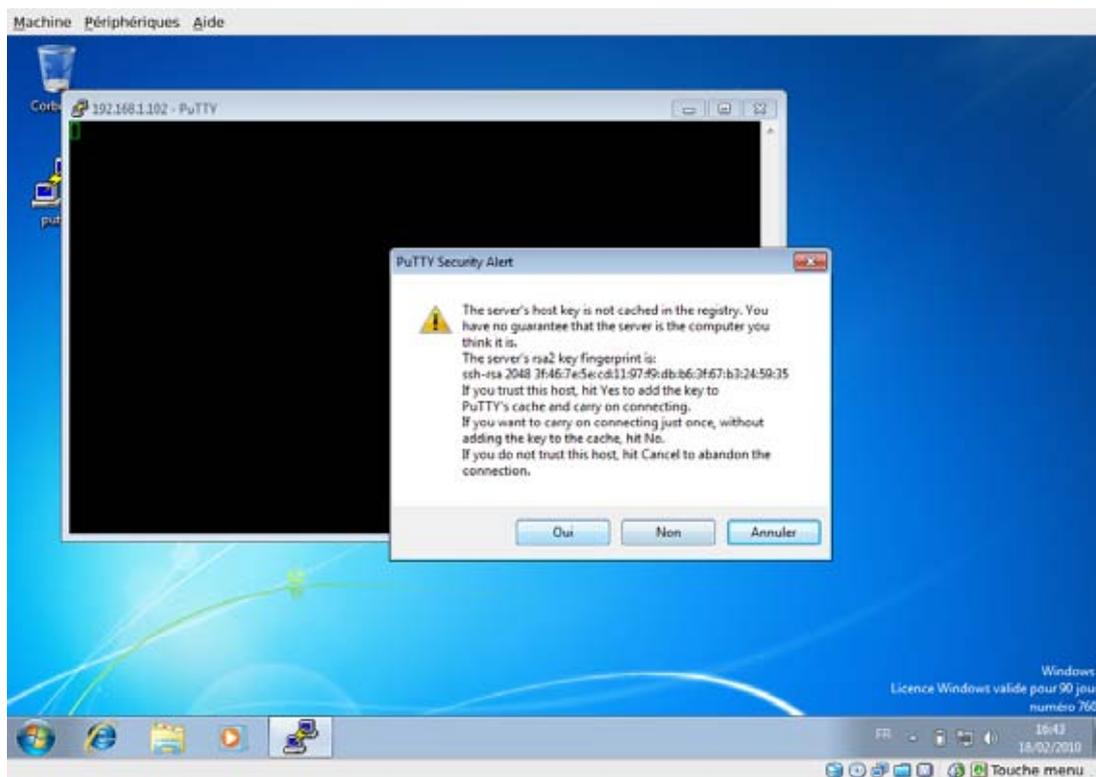


Figure 3 : putty conserve des informations sur le serveur

Enfin, vous vous retrouvez dans une interface type « ligne de commande » (un shell tout ce qu'il y a de plus standard) sauf que vous êtes à distance et que les communications sont sécurisées.

4B. Transfert de fichiers : winscp

La force de ssh est de proposer, outre une connexion de type shell, des outils de type ftp mais sécurisés. Le logiciel sous Windows le plus répandu permettant de faire du transfert de fichier sécurisé (SFTP) avec un serveur ssh est winscp.

Vous le téléchargez et l'exécutez :

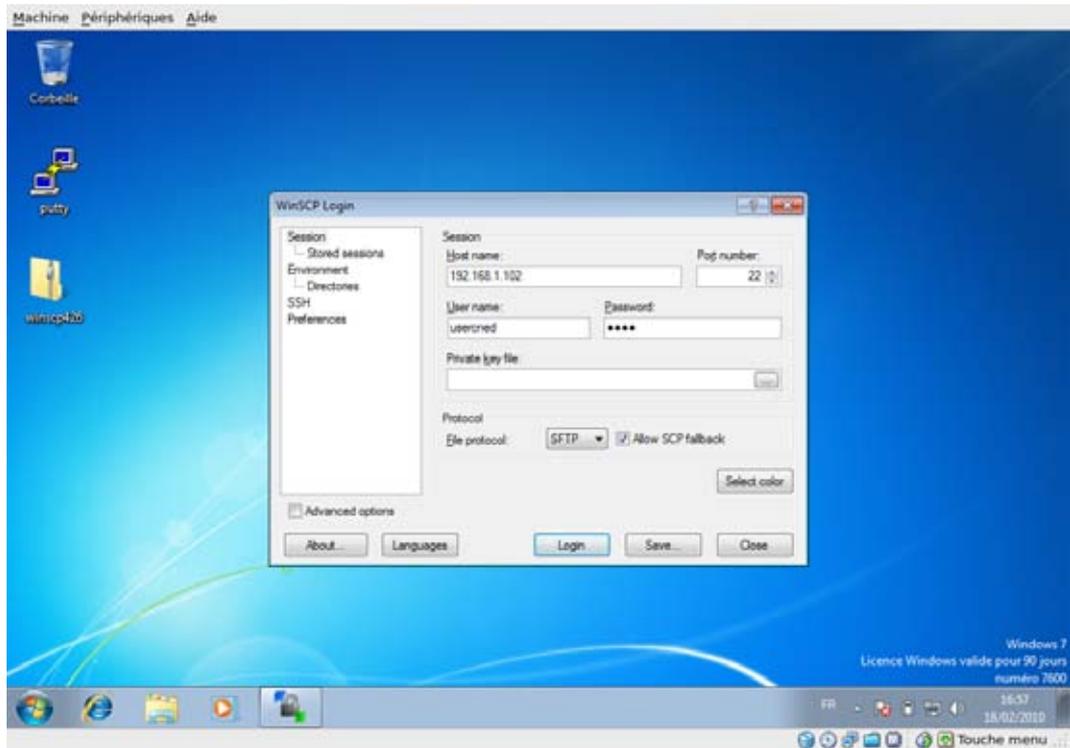


Figure 4 : Écran de connexion de winscp

Atelier 16

Administration
à distance

De la même manière que putty, winscp garde une trace des informations identifiant le serveur :

Page 208

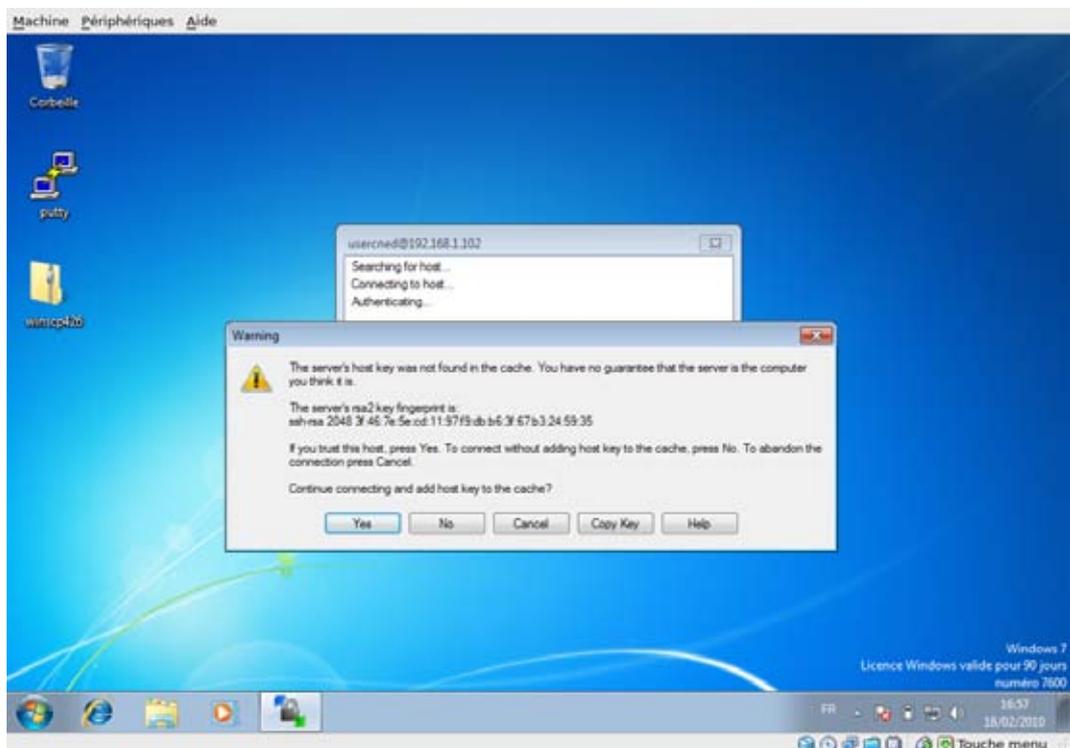
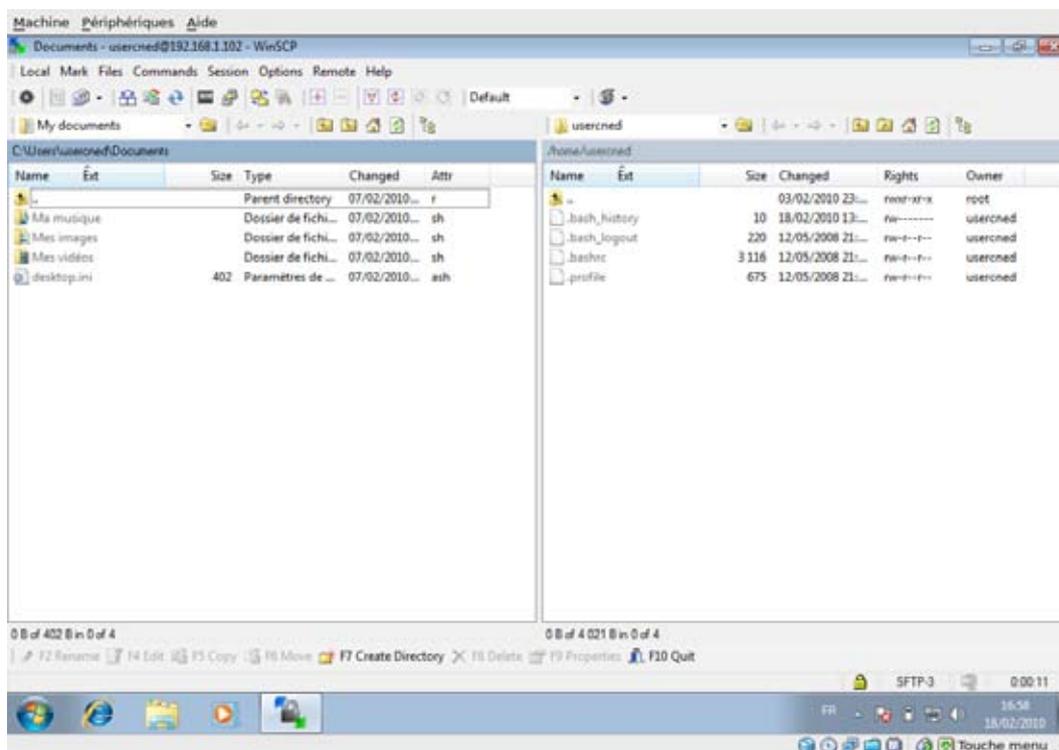


Figure 5 : winscp conserve des informations sur le serveur

Lorsque l'on est connecté, on se retrouve dans l'interface classique d'un logiciel de transfert de fichiers :



À retenir

SSH est un terminal virtuel (ce n'est pas un appareil connecté physiquement au serveur) permettant de se connecter à distance sur une machine, de façon sécurisée. Les échanges sont chiffrés, si quelqu'un tente de capturer les échanges, il ne peut en comprendre le contenu.

Le principe repose sur un couple de clés (clé privée/clé publique) propre à la machine. Lors de la connexion, une négociation se déroule et le serveur envoie sa clé publique au client. Le client utilise la clé publique du serveur pour chiffrer. Lorsque le serveur reçoit les données, il les déchiffre avec sa clé privée.

Si vous avez consulté le lien sur les mésaventures de Debian et de SSH, vous conviendrez qu'il est absolument nécessaire pour vous de suivre les alertes de sécurité pour mettre à jour vos machines. Suivez les conseils et abonnez-vous à la liste de diffusion : <http://www.debian.org/security>. Ceci est un rappel !

Si vous voulez approfondir

Une utilisation approfondie, et contrairement à ce que l'on pourrait penser, plus sécurisée que la saisie d'un mot de passe, consiste à utiliser ssh pour se connecter à distance sans taper de mot de passe mais avec un couple de clés propres à l'utilisateur.

Consulter la référence et faire les configurations indiquées : <http://www.debian.org/doc/manuals/securing-debian-howto/ch-sec-services.fr.html#s.1>

Atelier 16

Administration
à distance

Page 209

Atelier 17

Installation d'un serveur Web

► Objectif

À la fin de cet atelier, vous saurez configurer le serveur Web Apache dans ces principales options afin de diffuser des pages html.

► Durée approximative de cet atelier : 2 heures

► Durée approximative de cet atelier

Serveurs Linux Debian 6 et Windows 2008 R2 (DNS).

► Considérations techniques

Nous installerons Apache 2.2. Le serveur Web est, après la messagerie peut-être, le service le plus utilisé dans un Intranet ou sur Internet. Dans cet atelier, nous configurons le serveur pour diffuser des pages html statiques. Dans un prochain atelier, nous installerons le langage PHP et le système de gestion de bases de données MySQL. Associés à Apache, ils forment un serveur d'applications très répandu sur le Web. Enfin, dans un autre atelier nous installerons le couple Tomcat/Java, l'autre environnement de développement web.

Atelier 17

Installation
d'un serveur Web

Page 211

► Que faire si je bloque ?

La référence absolue : <http://httpd.apache.org/docs/2.2/>

Lorsque les paquetages seront installés, le manuel sera accessible dans `/var/www/html/manual` et par <http://apache.labocned.local/manual>.

Consultez la page de *man* sur httpd.

► Contenu

1. Introduction	212
2. Installation	212
3. Configuration du serveur.....	214
4. Principales directives	218
5. Étalonnage.....	222
6. Dépannage.....	224

1. Introduction

Pourquoi Apache ? C'est le serveur web le plus utilisé sur Internet (http://news.netcraft.com/archives/web_server_survey.html). De plus, il est :

- Portable : *nix (Unix, Linux, BSD, MacOS X...), Windows...
- Flexible : modulaire et extensible
- Libre et Open Source

Conforme au protocole HTTP (*Hyper Text Transfer Protocol*), il écoute, par défaut, sur le port TCP 80. Il supporte également le protocole SSL (*Secure Socket Layer*). Dans cet atelier, nous nous contenterons du serveur Web non chiffré.

2. Installation

2A. DNS

Un site web est accessible via une URL de la forme : <http://apache.labocned.local>. Or, ce nom d'hôte n'a pas été déclaré et, en fait, notre machine Linux n'utilise même pas le serveur DNS qui sera capable de lui donner l'adresse IP en fonction de son nom : notre Windows 2008 server, responsable du nom de domaine labocned.local

Vérifions en premier lieu la connectivité entre nos deux machines :

Atelier 17

Installation
d'un serveur Web

Page 212

```
root@mv2-linux:/usr/bin# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
 64 bytes from 192.168.1.100: icmp_req=1 ttl=128 time=4.09 ms
 64 bytes from 192.168.1.100: icmp_req=2 ttl=128 time=0.687 ms
 64 bytes from 192.168.1.100: icmp_req=3 ttl=128 time=0.656 ms
```

Modifions la configuration DNS de notre Linux pour le faire pointer (non plus sur la box mais sur Windows). Le fichier à modifier est `/etc/resolv.conf` et devra ressembler à ceci :

```
root@mv2-linux:~# cat /etc/resolv.conf
domain labocned.local
search labocned.local
nameserver 192.168.1.100
```

Petites vérifications, résolution sur le domaine local :

```
root@mv2-linux:~# nslookup w2008
Server: 192.168.1.100
Address: 192.168.1.100#53
Name: w2008.labocned.local
Address: 192.168.1.100
```

Résolution sur le domaine Internet :

```
root@mv2-linux:~# nslookup www.cned.fr
Server: 192.168.1.100
Address: 192.168.1.100#53
Non-authoritative answer:
Name: www.cned.fr
Address: 194.214.70.2
```

Ok, tout va bien. Continuons : il faut déclarer notre nom « apache » avec comme IP celle de notre Linux : 192.168.1.102. Ajoutons un hôte dans le serveur Windows/DNS :

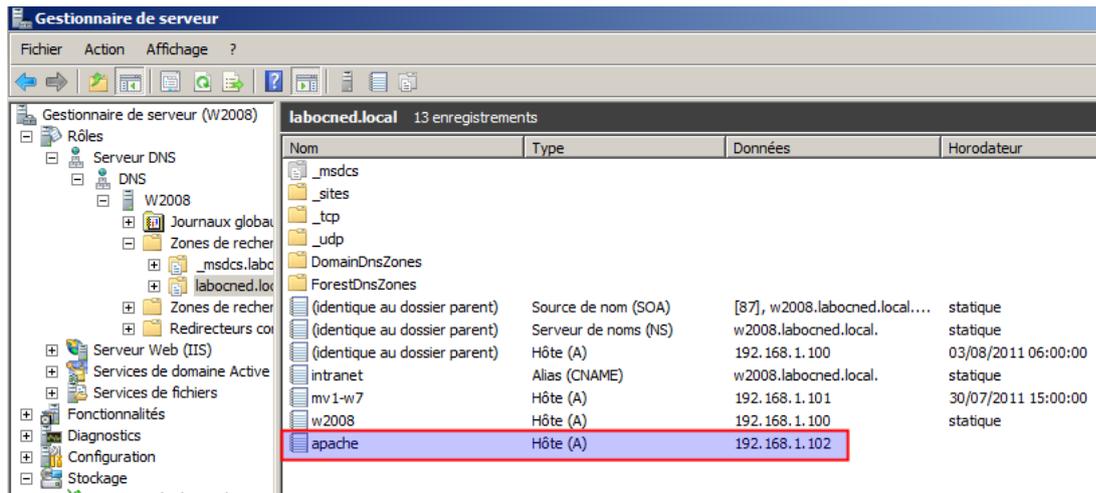


Figure 1 : Ajout d'un hôte pour le serveur

Atelier 17

Installation
d'un serveur Web

2B. Paquets Apache2

Installez les paquets apache2 (le serveur) et apache2-doc (la documentation) :

```
mv2-linux:~# apt-get install apache2 apache2-doc
```

Nous pouvons déjà voir un résultat avant de configurer Apache, depuis Windows, dans la barre du navigateur tapez <http://apache.labocned.local>

Vous devez voir apparaître « It works! »

Pour connaître la version du serveur Apache installé :

```
mv2-linux:~# apache2 -v
Server version: Apache/2.2.16 (Debian)
Server built: Mar 22 2011 21:14:12
```

Page 213

3. Configuration du serveur

Les fichiers de configuration sont bien entendu dans **/etc/apache2** :

```
mv2-linux:~# ls /etc/apache2
apache2.conf  envvars      mods-available  ports.conf  sites-enabled
conf.d        httpd.conf   mods-enabled    magic       sites-available
```

La configuration du serveur proprement dit, des sites et des modules se fait dans de nombreux fichiers (installez le paquet `tree` si nécessaire) :

```
mv2-linux:~# tree /etc/apache2
.
|-- apache2.conf
|-- conf.d
| |-- apache2-doc
| |-- charset
| `-- security
|-- envvars
|-- httpd.conf
|-- mods-available
| |-- actions.conf
| |-- actions.load
| |-- alias.conf
| |-- alias.load
| [...]
|-- mods-enabled
| |-- alias.conf ->../mods-available/alias.conf
| |-- alias.load ->../mods-available/alias.load
| |-- auth_basic.load ->../mods-available/auth_basic.load
| [...]
|-- ports.conf
|-- sites-available
| |-- default
| `-- default-ssl
`-- sites-enabled
   `-- 000-default ->../sites-available/default
```

Atelier 17

Installation
d'un serveur Web

Page 214

3A. Introduction

Dans cette partie, je vais essayer de vous présenter ce que nous utilisons régulièrement dans notre entreprise. Deux constats :

- chaque serveur héberge plusieurs sites web : nous avons besoin des **hôtes virtuels** ;
- nous n'utilisons régulièrement que quelques directives de configuration, nous vous les présenterons par la suite.

3B. Hôtes virtuels

Au démarrage de cet atelier, nous avons vu que le serveur répondait sur l'adresse apache.labocned.local. L'installation d'Apache sous Debian propose un site par défaut pré-configuré. Ses paramètres sont dans le fichier `/etc/apache2/sites-enabled/000-default`

Pour l'instant, n'importe quelle requête http qui arrive sur le port 80 de ce serveur sera dirigé vers ce site. Si l'on veut installer différents sites, il faut configurer Apache de façon à diriger les requêtes http vers le bon site. Mais comment ?

3B1. Requêtes http

Pour comprendre le mécanisme d'hôtes virtuels, il faut bien comprendre comment sont constituées les requêtes http. Comme pour la plupart des services réseau TCP/IP, les échanges entre client et serveur se font en mode texte, ce qui est très bien pour nous !

Rapide historique :

Au commencement, il y avait http 0.9. Il n'y avait qu'une seule méthode (la méthode GET) permettant d'obtenir des pages au format uniquement texte. On peut le mettre en oeuvre et simuler une requête envoyée par un navigateur au serveur. Sous Windows ou Linux, tapez la commande suivante :

```
$ telnet apache.labocned.local 80
Trying 192.168.1.102...
Connected to apache.labocned.local (192.168.1.102).
Escape character is '^]'.
```

Ensuite tapez : **GET /**

```
GET /
<html><body><h1>It works!</h1></body></html>
Connection closed by foreign host.
```

Vous obtenez la page puis la connexion est fermée.

Avec la version 1.0, il y eu pas mal de nouveautés :

- nouvelles méthodes : HEAD (informations sur la ressource) et surtout POST (envoyer des données au serveur)
- les requêtes peuvent contenir des paramètres (informations sur le navigateur, préférences du navigateur par exemple)
- les réponses peuvent aussi contenir des paramètres (et non plus seulement la ressource elle-même) :
 - code réponse : 200 pour une requête réussie, 404 pour une ressource inexistante, 403 pour un accès interdit
 - Date de création de la ressource, taille, date d'expiration, informations sur le serveur, etc.

Voyons cela :

```
$ telnet apache.labocned.local 80
Trying 192.168.1.102...
Connected to apache.labocned.local (192.168.1.102).
Escape character is '^]'.
```

```

GET / HTTP/1.0
                                     Requête du client indiquant la version du protocole
                                     Taper deux fois sur ENTREE

HTTP/1.1 200 OK
                                     Version du protocole supporté par le serveur suivi
                                     du code status HTTP (200 = OK, la ressource est
                                     disponible dans la réponse)

Date: Sat, 06 Aug 2011 22:34:19 GMT En-têtes associés à la réponse
Server: Apache/2.2.16 (Debian)
Last-Modified: Sat, 06 Aug 2011
18:11:21 GMT
ETag: «230dc-2d-48125c2558440»
Accept-Ranges: bytes
Content-Length: 45
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
<html><body><h1>It works!</h1></ La ressource elle-même
body></html>
Connection closed by foreign
host.

```

Tous les détails sur le protocole HTTP 1.0 sont définis dans la RFC1945.

Ce protocole présentait néanmoins des limites, en particulier :

- un seul site par serveur
- pas de persistance des connexions : une connexion est ouverte à chaque requête, ce qui consomme des ressources alors que bien souvent un utilisateur consulte plusieurs pages sur le même site.

Le HTTP 1.1 (RFC 2616) apporte des améliorations et permet en particulier d'héberger plusieurs sites sur un même serveur. Dans la requête, le navigateur doit donc intégrer le nom du site demandé sur le serveur :

```

$ telnet apache.labocned.local 80
Trying 192.168.1.102...
Connected to 06 Aug 2011 (192.168.1.102).
Escape character is '^]'.
GET / HTTP/1.1
Host: apache.labocned.local

HTTP/1.1 200 OK
Date: Sat, 06 Aug 2011 22:50:43 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Sat, 06 Aug 2011 18:11:21 GMT
ETag: "230dc-2d-48125c2558440"
Accept-Ranges: bytes
Content-Length: 45
Vary: Accept-Encoding
Content-Type: text/html

<html><body><h1>It works!</h1></body></html>

```

Remarquez que la connexion n'est pas fermée par le serveur.

3B2. Configuration de deux hôtes virtuels

Nous allons configurer deux sites différents (site1.labocned.local et site2.labocned.local), le site par défaut restera accessible.

Dans un premier temps, modifiez votre serveur DNS pour faire la résolution de noms sur ces deux machines (créez deux alias pour apache.labocned.local).

Dans le répertoire /etc/apache2/sites-available, créez le fichier nommé site1.labocned.local suivant :

```
<VirtualHost *:80>
    ServerName site1.labocned.local

    DocumentRoot /var/www/site1.labocned.local
    ErrorLog /var/log/apache2/error.log

    # Possible values include: debug, info, notice, warn, error, crit,
    # alert, emerg.
    LogLevel warn

    CustomLog /var/log/apache2/site1.labocned.local.access.log combined
</VirtualHost>
```

La directive ServerName identifie l'hôte virtuel. La directive DocumentRoot indique la racine où sont situés les fichiers du site web. Dans /var/www, créez le répertoire site1.labocned.local puis, dans ce répertoire, créez le fichier index.html ci-dessous :

```
<h1>Site1</h1>
```

Au démarrage, Apache tourne sous l'utilisateur root mais ensuite il se divise en sous-processus. Ce sont ces sous-processus qui servent les pages html. Ils tournent quant à eux sous l'utilisateur www-data :

```
# ps aux | grep apache2
root 4203 0.0 1.0 13376 2784 ?        Ss   00:18   0:01  /usr/sbin/
apache2 -k start
www-data 4204 0.0 0.7 13148 1988 ?    S    00:18   0:00  /usr/sbin/
apache2 -k start
www-data 4205 0.0 1.2 234872 3160 ?    Sl   00:18   0:00  /usr/sbin/
apache2 -k start
www-data 4210 0.0 1.1 234720 3076 ?    Sl   00:18   0:00  /usr/sbin/
apache2 -k start
```

Atelier 17

Installation
d'un serveur Web

Page 217

Il est donc conseillé d'adapter les droits d'accès :

```
mv2-linux:~# cd /var/www
mv2-linux:/var/www# ls -la
total 16
drwxr-xr-x 3 root root 4096 mar 7 00:06.
drwxr-xr-x 14 root root 4096 mar 6 19:10..
-rw-r--r-- 1 root root 45 mar 6 19:11 index.html
drwxr-xr-x 2 root root 4096 mar 7 00:06 site1.labocned.local
mv2-linux:/var/www# chown www-data. -R
mv2-linux:/var/www# chgrp www-data. -R
mv2-linux:/var/www# ls -la
total 16
drwxr-xr-x 3 www-data www-data 4096 mar 7 00:06.
drwxr-xr-x 14 root root 4096 mar 6 19:10..
-rw-r--r-- 1 www-data www-data 45 mar 6 19:11 index.html
drwxr-xr-x 2 www-data www-data 4096 mar 7 00:06 site1.labocned.
local
```

Il nous reste maintenant à activer le site et à recharger la configuration d'Apache :

```
# a2ensite site1.labocned.local
# /etc/init.d/apache2 reload
```

Dans votre navigateur, tapez <http://site1.labocned.local>. La page « Site1 » doit s'afficher.

Vous pouvez faire de même avec site2 en adaptant.

Atelier 17

Installation
d'un serveur Web

Page 218

4. Principales directives

Nous vous présentons ici les principales directives que nous utilisons habituellement. Une chose importante à savoir est qu'une configuration réalisée à un certain niveau de l'arborescence des sites se propage à tous les fichiers et répertoires situés en dessous.

4A. DirectoryIndex

Par défaut, si un répertoire du site web ne contient pas de fichier index.html, n'importe qui peut lister son contenu :

```
# cd /var/www/site2.labocned.local
# mkdir rep
```

Maintenant dans le navigateur, si l'on va sur <http://site2.labocned.local/rep>



Figure 2 : Affichage du répertoire

Pour empêcher ceci, dans le fichier de configuration du site /etc/apache2/sites-available/site2.labocned.local, nous ajoutons juste avant la fin du fichier :

```
<Location />
  Options -Indexes
</Location>
</VirtualHost>
```

Ce qui signifie : à partir de la racine (/), l'affichage des répertoires est interdit (-). On recharge la configuration d'Apache, le résultat dans le navigateur est maintenant :



Figure 3 : Interdiction de l'affichage

Référence : <http://httpd.apache.org/docs/2.2/mod/core.html#options>

4B. Redirection

On est fréquemment amené à faire des redirections. L'utilisateur arrive à un endroit du site et il est redirigé soit vers une autre page soit vers un autre site.

Supposons que Site2 soit momentanément indisponible. Nous voulons rediriger l'utilisateur vers Site1.

Commençons par ceci :

```
    Redirect temp / http://site1.labocned.local/  
</VirtualHost>
```

Après rechargement de la configuration, si on essaie d'aller sur <http://site2.labocned.local/rep> on est redirigé au même endroit sur l'autre URL <http://site1.labocned.local/rep> mais ce répertoire n'existe pas.

On peut faire mieux en disant que quel que soit l'endroit où l'utilisateur arrive sur le site2 il est systématiquement redirigé à la racine du site1. On remplace l'instruction par :

```
RedirectMatch temp /* http://site1.labocned.local/
```

Vous pouvez observer la redirection ici :

```
$ telnet 192.168.1.102 80  
Trying 192.168.1.102...  
Connected to www.labocned.local (192.168.1.102).  
Escape character is '^]'.  
GET / HTTP/1.1  
Host: site2.labocned.local  
  
HTTP/1.1 302 Found  
Date: Sun, 07 Mar 2010 00:34:11 GMT  
Server: Apache/2.2.16 (Debian)  
Location: http://site1.labocned.local/  
Vary: Accept-Encoding  
Content-Length: 291  
Content-Type: text/html; charset=iso-8859-1  
  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>302 Found</title>  
</head><body>  
<h1>Found</h1>  
<p>The document has moved <a href="http://site1.labocned.local/">here</a>.</p>  
<hr>  
<address>Apache/2.2.16 (Debian) Server at site2.labocned.local  
Port 80</address>  
</body></html>  
Connection closed by foreign host.
```

Le serveur vous répond FOUND (302) mais vous indique un autre endroit (Location). C'est le navigateur qui utilise cet en-tête de la réponse pour y aller.

Référence : http://httpd.apache.org/docs/2.2/mod/mod_alias.html

4C. Alias

L'alias est un mécanisme différent de la redirection. Il s'agit de la notion de **répertoire virtuel**. On veut par exemple donner accès à un répertoire sur le serveur situé ailleurs que dans le DocumentRoot. Vous verrez par la suite qu'un produit comme Phpmyadmin par exemple, ne s'installe pas dans /var/www mais ailleurs. Or, le serveur web ne peut pas

renvoyer une ressource située en dehors de son DocumentRoot, sauf si on utilise un alias.
Par exemple :

```
Alias /phpmyadmin /usr/share/phpmyadmin
```

Lorsque l'utilisateur demande <http://site1.labocned.local/phpmyadmin>, ce sont des fichiers situés dans /usr/share/phpmyadmin qui sont servis.

Référence : http://httpd.apache.org/docs/2.2/mod/mod_alias.html

4D. Restriction sur IP

Il nous arrive régulièrement, pour des raisons de sécurité, de réserver l'accès à certains sites ou parties de site à certaines adresses IP.

Travaillons sur le site1 et imaginons que celui-ci n'est accessible qu'au réseau IP 172.16.0.0.

```
<Location />
    Order Deny,Allow
    Deny from All
    Allow from 172.16
</Location>
</VirtualHost>
```

Si vous essayez d'accéder au site1, vous aurez un magnifique Forbidden (status HTTP 403).

Référence : http://httpd.apache.org/docs/2.2/mod/mod_authz_host.html

4E. Accès par mot de passe

Une autre manière de protéger l'accès à un site est de demander un mot de passe. Notez bien qu'en http, les mots de passes circulent en clair entre le navigateur et le serveur.

Sur le site1, supprimez la restriction sur l'IP. Puis créez le fichier de mot de passe des utilisateurs autorisés (ce sont donc des comptes indépendants des comptes Unix).

```
# cd /etc/apache2/
mv2-linux:/etc/apache2# mkdir passwd
mv2-linux:/etc/apache2# cd passwd
mv2-linux:/etc/apache2# htpasswd -c /etc/apache2/passwd/passwords
util2
New password:
Re-type new password:
Adding password for user util2
```

Dans le fichier de configuration du site1 :

```
<Location />
    AuthType Basic
    AuthName "Acces protege"
    AuthBasicProvider file
    AuthUserFile /etc/apache2/passwd/passwords
    Require valid-user
</Location>
</VirtualHost>
```

Lorsque l'on accède au site, on obtient (si vous ne voyez pas ceci, il faut probablement vider votre cache ou forcer le rechargement de la page avec CTRL+F5) :

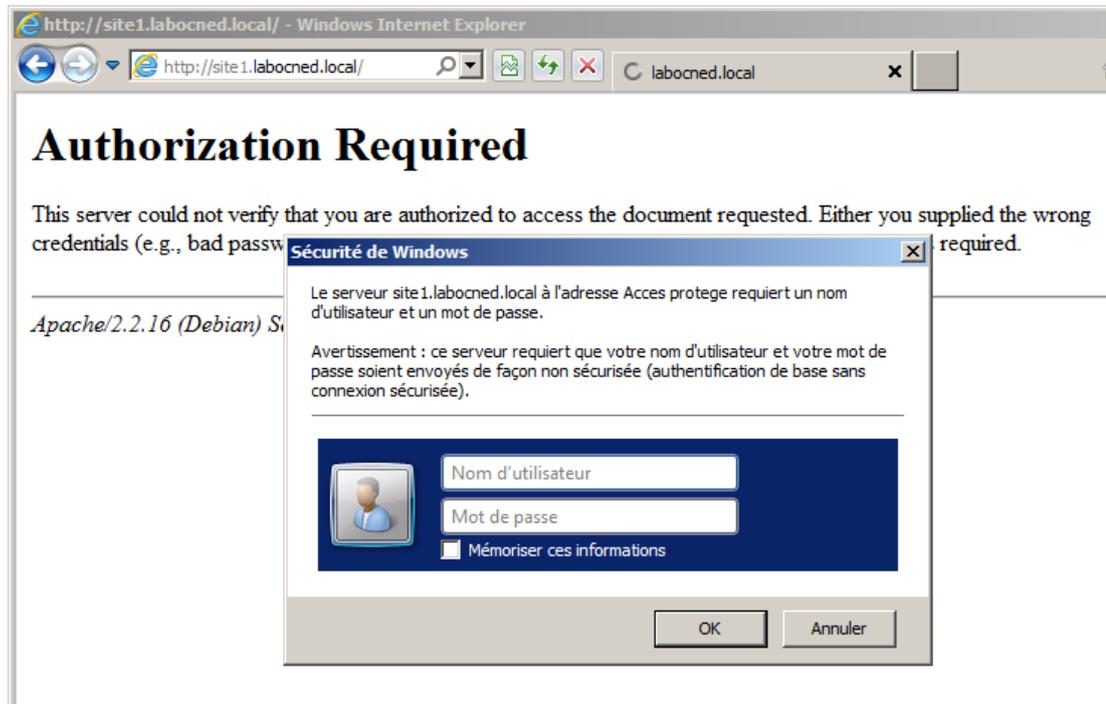


Figure 4 : Contrôle utilisateur

Atelier 17

Installation
d'un serveur Web

Référence : <http://httpd.apache.org/docs/2.2/howto/auth.html>

Page 222

5. Étalonnage

Comment répondre à des questions comme « combien de requêtes http mon serveur est-il capable d'ingérer ? » ou « est-ce que cette nouvelle configuration de mon serveur web est plus efficace ? ». La commande `ab` peut nous donner des éléments. Je vous laisse regarder le man pour voir tous les détails.

Nous lançons la commande ci-dessous qui va réaliser 100 000 requêtes http, 100 à la fois sur le serveur web local :

```
# ab -n 100000 -c 100 http://localhost/
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.
zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking localhost (be patient)
Completed 10000 requests
Completed 20000 requests
Completed 30000 requests
Completed 40000 requests
Completed 50000 requests
Completed 60000 requests
```

```
Completed 70000 requests
Completed 80000 requests
Completed 90000 requests
Completed 100000 requests
Finished 100000 requests
```

Suivant votre configuration matérielle, ce travail prendra un temps plus ou moins long.
Sur ma machine (ancienne), le résultat est le suivant :

```
Server Software: Apache/2.2.16
Server Hostname: localhost
Server Port: 80
```

```
Document Path: /
Document Length: 45 bytes
```

```
Concurrency Level: 100
Time taken for tests: 404.186 seconds
Complete requests: 100000
Failed requests: 0
Write errors: 0
Total transferred: 35714280 bytes
HTML transferred: 4501800 bytes
```

```
Requests per second: 247.41 [# /sec] (mean)
Time per request: 404.186 [ms] (mean)
Time per request: 4.042 [ms] (mean, across all concurrent requests)
Transfer rate: 86.29 [Kbytes/sec] received
```

```
Connection Times (ms)
```

	min	mean	[+/-sd]	median	max
Connect:	1	185	55.3	173	712
Processing:	75	218	70.8	198	1049
Waiting: 41	175	62.0	162	884	
Total: 150	403	95.9	379	1446	

```
Percentage of the requests served within a certain time (ms)
```

50%	379
66%	411
75%	437
80%	455
90%	516
95%	582
98%	692
99%	774
100%	1446 (longest request)

On cherche bien sûr à avoir la plus grande valeur possible pour « Requests per seconds » et la plus faible pour « Time per request ». Mais ces outils sont à manipuler avec précaution car il faut pouvoir « comparer ce qui est comparable ». En effet, suivant le lien réseau qui vous sépare du serveur, la taille des pages demandées, la charge actuelle du serveur si celui-ci est en production, tous ces éléments et certainement d'autres peuvent grandement influencer les résultats.

Atelier 17

Installation
d'un serveur Web

Page 223

6. Dépannage

La commande `apache2ctl -t` permet de valider la syntaxe des fichiers de configuration. Visionnez régulièrement les fichiers `/var/log/apache2` afin de voir l'historique des accès et des erreurs.

À retenir

Http est le protocole à la base du World Wide Web. Apache est le serveur Web le plus répandu.

Toute la configuration se passe dans le fichier `apache2.conf` (niveau global) ou dans les fichiers de configuration des hôtes virtuels.

La plupart des configurations s'appliquent à un niveau du site (`<Location>`) se propagent automatiquement aux niveaux inférieurs (sauf configuration contraire bien sûr).

Les permissions définies sur les répertoires contenant les pages Web sont importantes afin que Apache puisse y accéder.

Un outil comme `ab` permet d'étalonner un serveur et de comparer différentes configurations.

Si vous voulez approfondir

Vous pouvez installer le logiciel `fiddler` (<http://www.fiddler2.com/fiddler2/>) qui vous permettra d'approfondir le fonctionnement du protocole HTTP. Développé avec .NET, ce produit ne tourne que sous Windows...

Consulter la référence et faire les configurations indiquées : <http://www.debian.org/doc/manuals/securing-debian-howto/ch-sec-services.fr.html#s5.8>

Atelier 18

Installation de Php/MySQL

► Objectif

À la fin de cet atelier, vous saurez installer une plate-forme pour héberger des sites Internet dynamiques développés en Php/MySQL. Vous aurez également les outils pour valider l'installation.

► Durée approximative de cet atelier : 2 heures

► Durée approximative de cet atelier

Serveur Linux Debian 6.

► Considérations techniques

Côté serveur, nous allons travailler avec les logiciels suivants :

- le système de gestion de base de données (SGBD) MySQL ;
- le langage de programmation pour site Web dynamique Php.

Sur le client, n'importe quel navigateur fera l'affaire (Firefox, Explorer, Chrome, Safari, etc.).

► Que faire si je bloque ?

Consultez les sites des développeurs des logiciels :

<http://www.php.net/manual/fr/>

<http://www.mysql.com>

► Contenu

1. Introduction	226
2. Installations.....	227
3. Configuration.....	229

1. Introduction

Notre objectif est de préparer un serveur Linux capable d'héberger des sites statiques et dynamiques. Quelle est la différence ?

1A. Site statique

Dans un site Internet statique, toutes les pages HTML sont conçues une fois pour toute, elles font l'objet d'un fichier placé sur le disque du serveur. Celui-ci se contente de répondre aux requêtes des clients du genre « hep toi, envoie-moi la page dont le nom est index.html ». Dans cette architecture basique, seul un logiciel serveur web (Apache en l'occurrence) suffit :

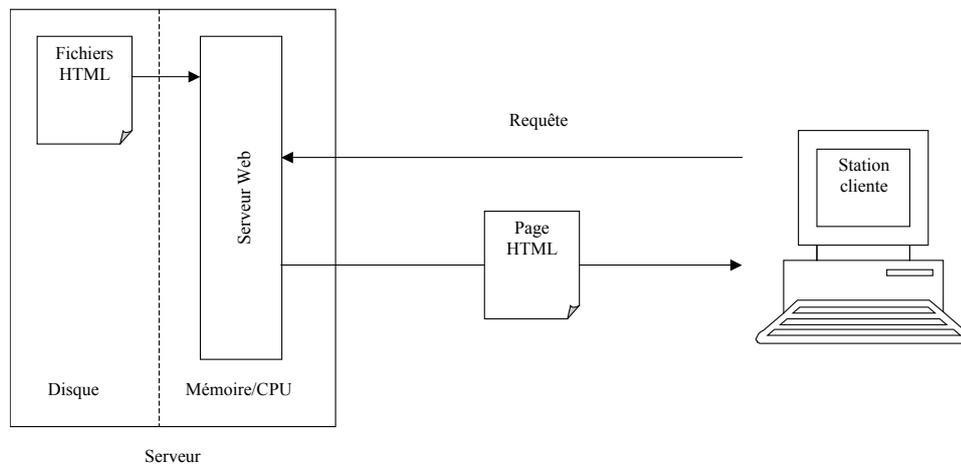


Figure 1 : architecture d'un site Web statique

Atelier 18

Installation
de Php/MySQL

Page 226

1B. Site dynamique

Cette architecture est limitée. Elle convient bien pour un site de présentation d'une société par exemple, mais elle empêche d'envisager certaines activités comme du commerce électronique. En effet, il est impossible de prévoir à l'avance toutes les commandes que pourraient passer les clients. De plus, comment mémoriser les commandes, les produits, les règlements ? Nous avons besoin du web dynamique et plusieurs technologies s'affrontent :

- Java EE (*Java Enterprise Edition*) : un environnement initié par Sun mais supporté par de nombreux opérateurs, y compris libres : nous le mettrons en oeuvre dans le TP suivant (Tomcat/Java) ;
- IIS/.Net : présenté dans la première partie de cet ouvrage, c'est un environnement essentiellement supporté par Microsoft cependant une implémentation libre existe : <http://www.mono-project.com>
- Apache/Php/MySQL pour une solution 100% libre.

Dans ce TP, nous avons retenu la solution LAMP (Linux/Apache/MySQL/Php). Celle-ci présente certains avantages :

- Apache : c'est le serveur web le plus répandu (environ 33% des serveurs web), multi-plateforme (Windows ou Unix like y compris Mac OS X) ;
- MySQL : les dernières versions ont apporté les fonctionnalités lui permettant d'être reconnu dans la cour des grands ;

- Php : langage de type C, facile à appréhender, documentation importante. De nombreux compléments permettent de développer des applications critiques. Néanmoins, il reste des limites concernant la montée en charge.

Dans tous les cas, une architecture de site web dynamique est plus complexe qu'une architecture statique, quelle que soit la solution retenue. Ici, avec LAMP :

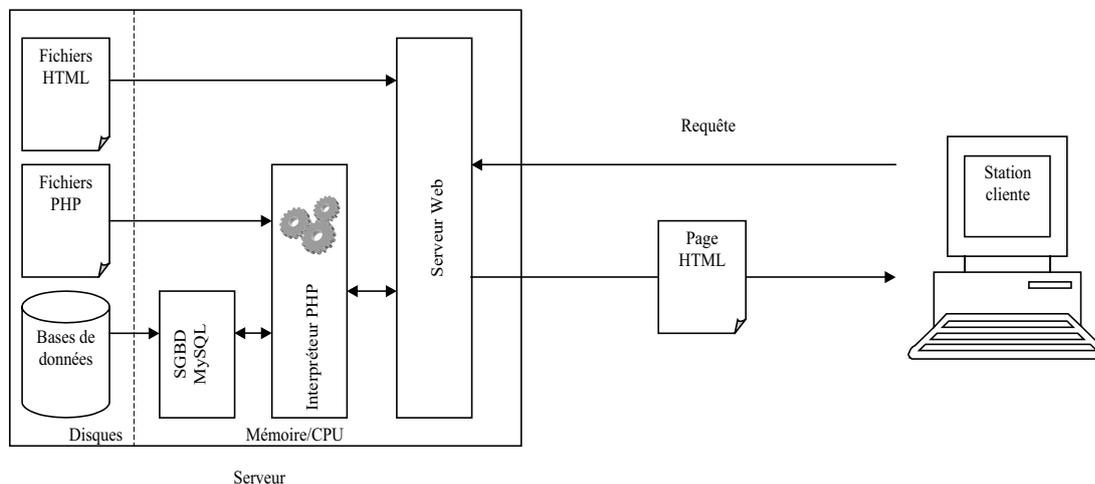


Figure 2 : architecture d'un site Web dynamique

C'est une architecture en couches. Chaque couche se rend mutuellement des services. Le point fondamental à retenir est que **le traitement des programmes PHP est réalisé sur le serveur** (contrairement à Javascript par exemple). L'interpréteur PHP produit une page HTML qui est ensuite transmise au client par le serveur Web. Il peut également dialoguer avec le SGBD afin de stocker ou d'extraire des données d'une base.

Atelier 18

Installation de Php/MySQL

Page 227

2. Installations

2A. MySQL

Vous devez installer le paquet suivant :

```
mv2-linux:/# apt-get install mysql-server
```

Vous indiquez un mot de passe pour l'administrateur de MySQL (qui s'appelle aussi root mais toute ressemblance avec un administrateur ayant déjà existé est purement fortuite).

Il est absolument impératif de le renseigner car les attaques sur mot de passe, en particulier sur PhpMyAdmin sont constantes sur l'Internet.

Nous vérifions que le serveur MySQL est opérationnel :

```
# netstat -plunt | grep mysqld
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN 2977/mysqld
```

Par défaut, MySQL écoute sur le port TCP 3306 sur l'adresse locale 127.0.0.1.

2B. Php

Installez le paquet suivant :

```
# apt-get install php5
```

Notez que : `apache2-mpm-worker` sera enlevé (et remplacé par `apache2-mpm-prefork` comme le préconise <http://www.php.net/manual/fr/install.unix.apache2.php>).

L'atelier sur l'installation de Apache2 nous a appris que lorsqu'il se lance, il se subdivise en sous-processus qui répondent aux requêtes http. Pour simplifier, disons que l'architecture mpm-worker de Apache2 est basée sur des processus légers (ou thread) qui consomment moins de ressources que le prefork. Or, le php pose pas mal de problèmes en mode worker.

Le module permettant l'utilisation de php5 avec Apache2 (`libapache2-mod-php5`) est également installé.

Nous pouvons maintenant faire un petit test. Allez à la racine du serveur web pour créer un fichier qui nous permettra de valider l'installation.

```
# cd /var/www
# vi test.php
```

Le contenu du fichier test.php sera :

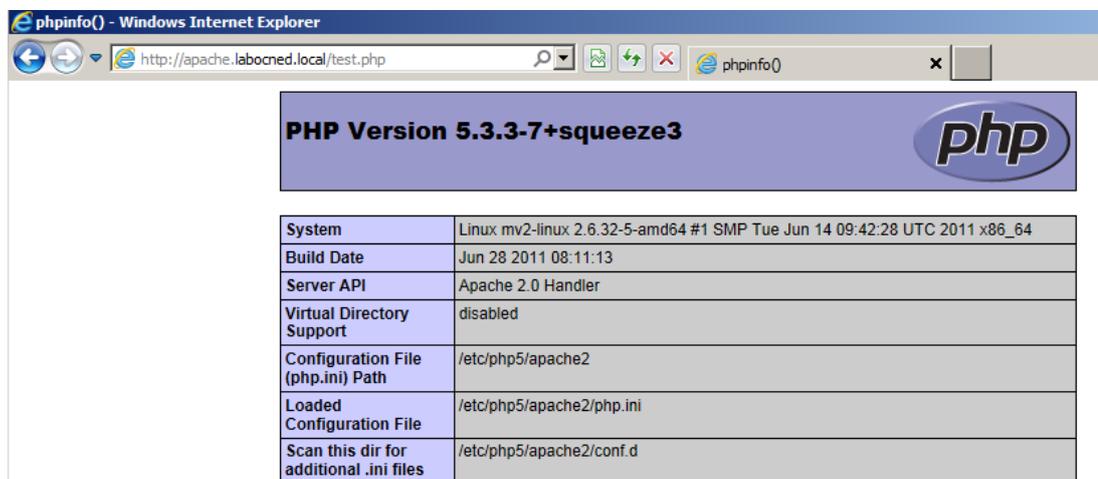
```
<?php
    phpinfo();
?>
```

Il faudra redémarrer Apache puis avec votre navigateur désignez l'adresse réticulaire : <http://apache.labocned.local/test.php>

Atelier 18

Installation
de Php/MySQL

Page 228



System	Linux mv2-linux 2.6.32-5-amd64 #1 SMP Tue Jun 14 09:42:28 UTC 2011 x86_64
Build Date	Jun 28 2011 08:11:13
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d

Figure 3 : Vérification du fonctionnement de Php sous Apache

2C. Interface d'administration du SGBD

MySQL peut être administré par des outils comme MySQL Workbench :

<http://www.mysql.com/products/workbench/>

Et bien sûr tout le monde a entendu parler de phpMyAdmin.

http://www.phpmyadmin.net/home_page/index.php

Dans cet atelier nous allons privilégier phpMyAdmin qui fonctionne en mode web.

```
mv2-linux:/# apt-get install phpmyadmin
```

Pendant le processus, il vous sera demandé de choisir le serveur Web (je vous laisse deviner ;-)) et aussi de configurer une base de données pour phpMyAdmin. Vous devrez indiquer le mot de passe administrateur de Mysql.

Le logiciel est maintenant disponible sur cette URL :

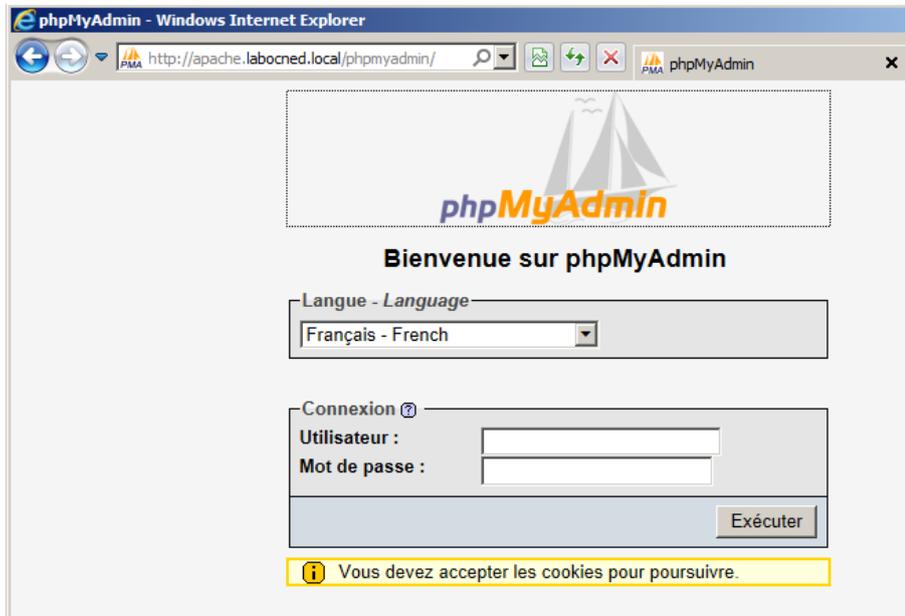


Figure 4 : Page d'accueil de phpMyAdmin

L'interface est installée. Surtout en production, vous ne laissez pas phpMyAdmin en http (nous verrons dans un prochain atelier comment passer en https). De plus, une bonne pratique consiste à limiter dans Apache l'accès à phpMyAdmin sur les IP des machines des administrateurs.

Vous pouvez vous connecter dans l'interface en tant que root et le mot de passe indiqué lors de l'installation de MySQL.

3. Configuration

3A. Apache

Nous profitons de cette installation pour revenir sur la configuration de Apache2. Certains logiciels ont une configuration propre. Celle-ci est chargée par Apache lors de son démarrage (voir les différentes clauses Include dans le fichier /etc/apache2/apache2.conf). La configuration de phpMyAdmin se trouve donc dans /etc/apache2/conf.d/phpmyadmin.conf. Vous remarquerez entre autres la première ligne : Alias.

Pour le php, c'est un peu plus compliqué étant donné qu'il peut aussi s'exécuter en dehors du serveur web. A l'installation, vous avez remarqué que apt a installé par dépendance le module libapache2-mod-php5. Celui-ci fait le lien entre php et Apache. Il dispose de ses propres fichiers de configuration (/etc/apache2/mods-available). En ce qui me

concerne, je n’y ai jamais touché. Par contre, le module php utilise ensuite un fichier de configuration par défaut : /etc/php5/apache2/php.ini dans lequel vous serez tôt ou tard amené à intervenir.

3B. MySQL

Nous abordons ici deux sujets :

- les permissions des utilisateurs
- le suivi de l’activité du serveur.

Nous réalisons ces tâches dans phpmyadmin, mais sachez que cet outil n’est pas indispensable. Tout peut être réalisé dans le shell avec la commande : mysql.

3B1. Les permissions

Deux choses sont à retenir :

- la base des utilisateurs MySQL n’a rien à voir avec la base des utilisateurs Linux (le root de MySQL n’est pas le root de Linux) ;
- il existe trois niveaux de permissions :
 - niveau global : s’applique à toutes les bases de données
 - niveau base de données
 - niveau table d’une base de données.

Nous allons créer une base de données, un utilisateur et lui affecter des permissions.

Lorsque vous êtes connecté en tant que root :

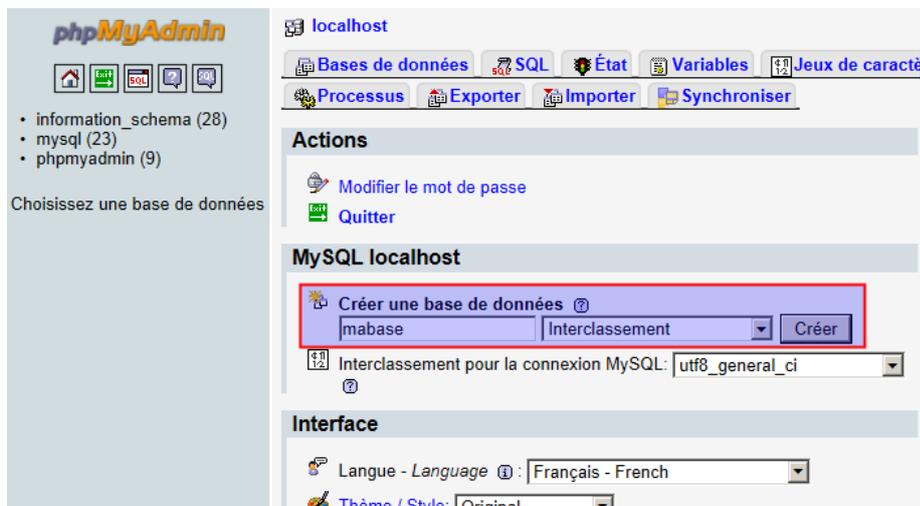


Figure 5 : Création d’une base

Nous créons une table avec un champ :

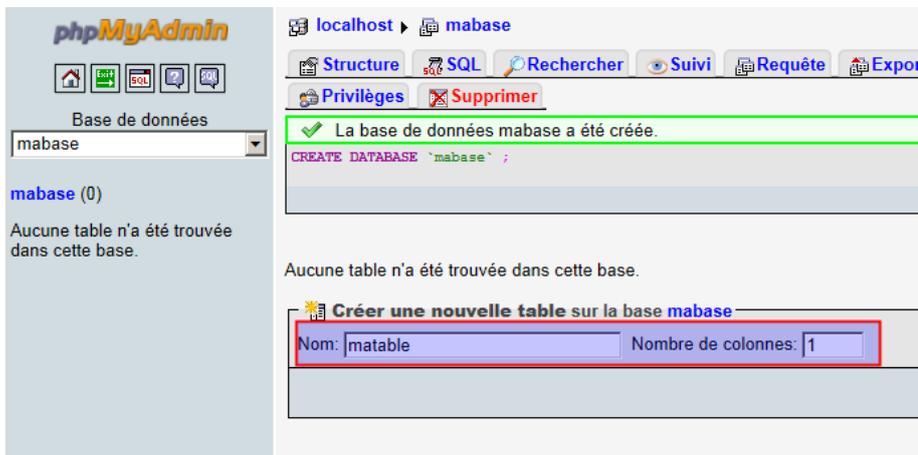


Figure 6 : Création d'une table

Il faut donner un nom au champ et le mettre de type INT :

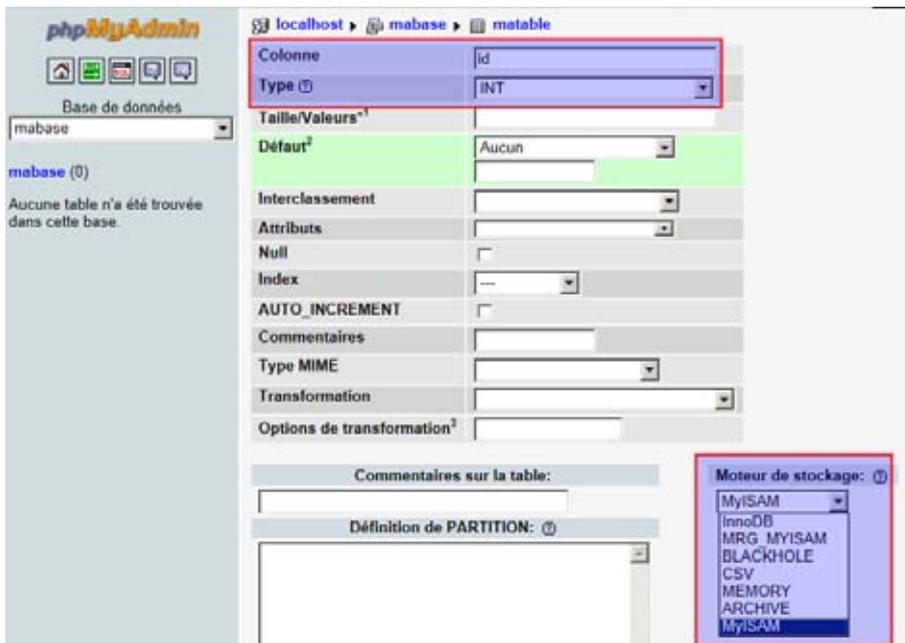


Figure 7 : Déclaration des champs

Le choix du moteur de stockage est important. Les deux les plus utilisés sont MyISAM et InnoDB, chacun avec ses avantages et inconvénients. Disons que MyISAM est destiné aux applications très basiques. InnoDB est plus robuste (gestion des transactions et des contraintes d'intégrité). Il consomme certainement plus de ressources sur la machine (CPU, RAM) mais est réputé pour être très efficace dans les opérations d'écriture.

L'objet de cet atelier ne porte pas sur la base de données proprement dite, nous laissons donc MyISAM mais dans la vraie vie, posez-vous la question ! Par expérience, je peux dire que nous avons regretté d'avoir choisi MyISAM pour une certaine application et qu'ensuite, la bascule vers InnoDB n'est pas simple...

Nous insérons quelques valeurs (root a bien sûr le droit de le faire) :

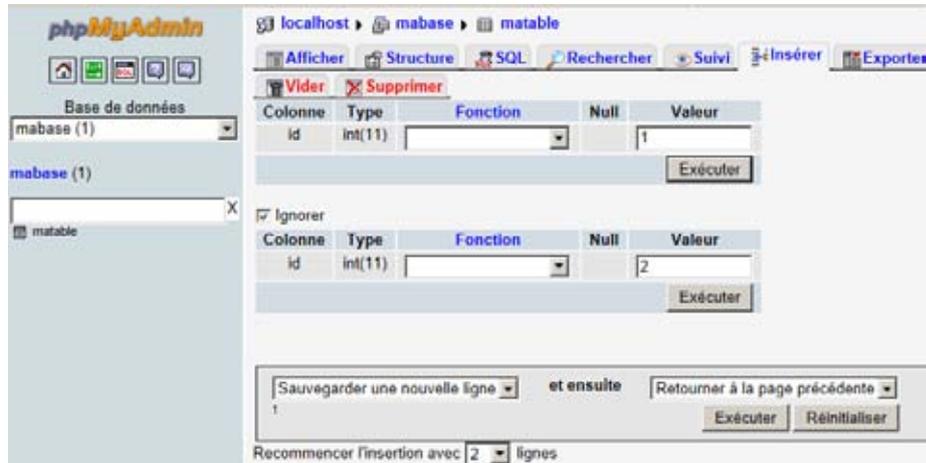


Figure 8 : Insertion de valeurs

Dans l'onglet afficher, nous pouvons lister le contenu de la table :

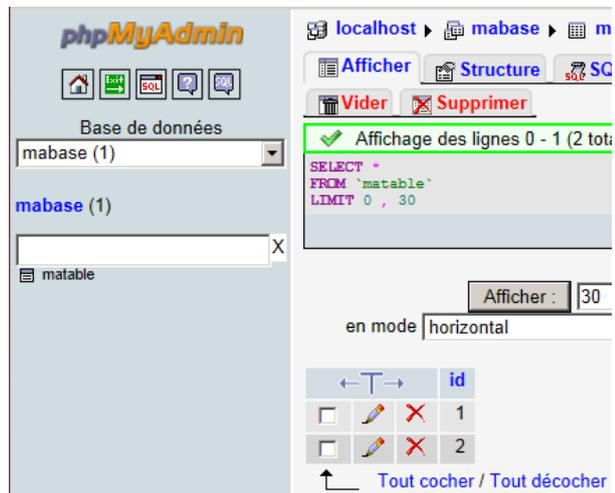


Figure 9 : Affichage des valeurs saisies

Maintenant, affectons des droits à un utilisateur. Vous allez dans le menu Accueil/Privi-
lèges/Ajouter un utilisateur :

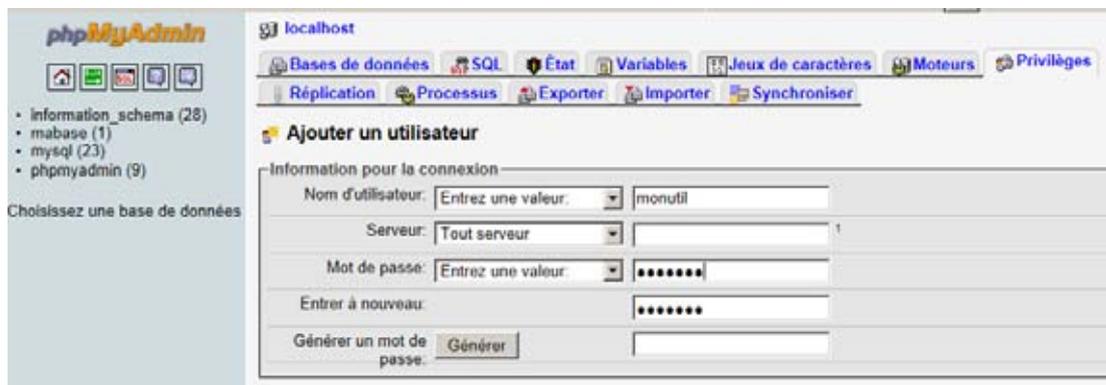


Figure 10 : Création d'un utilisateur

Vous n'affectez aucun privilège global ! C'est une erreur que l'on rencontre trop souvent avec des développeurs php peu scrupuleux !

Maintenant, vous revenez sur l'onglet « Privilèges ». Votre nouvel utilisateur apparaît dans la liste, vous le modifiez en cliquant sur l'icône « crayon » à droite de la liste.

Ensuite, dans le deuxième encadré « Privilèges spécifiques à une base de données », vous choisissez votre base de données et vous vous retrouvez dans la gestion des privilèges de cette base de données. Nous lui affectons des droits de « Select » uniquement (uniquement consultation des données de la base) :



Figure 11 : Définition des privilèges spécifiques à une base

Maintenant, vous vous déconnectez et vous reconnectez sous ce compte utilisateur. Si vous allez dans « Mabase » puis « Matable », vous pouvez afficher le contenu, mais si vous essayez d'insérer une donnée, MySQL vous répond :

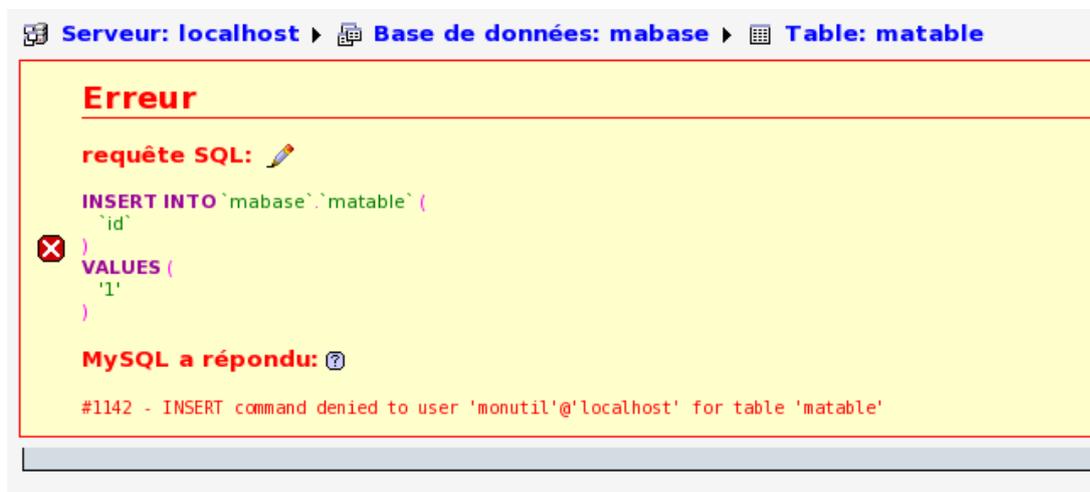


Figure 12 : Tentative d'insertion dans une table

3B2. Suivi de l'activité

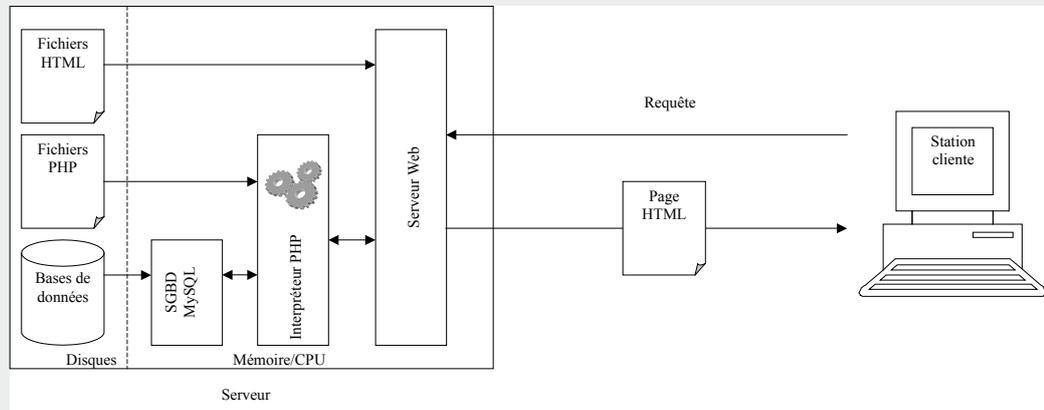
Lorsque votre serveur est en production, il est important de suivre un certain nombre d'indicateurs afin de détecter les problèmes de configuration.

Reconnectez-vous en root puis allez dans « Afficher l'état du serveur ». Dans cette page, Phpmyadmin vous affichera en rouge les paramètres de configuration de MySQL qui semblent poser un problème. Dans la colonne « Description », vous avez des conseils.

Pour changer ces paramètres, il faut parfois intervenir dans le fichier /etc/mysql/my.cnf

À retenir

Php/MySQL permettent de réaliser des sites web dynamiques. Tous les traitements sont réalisés sur le serveur. Le navigateur du client se contente d'afficher une page html qui a été produite par le serveur. Retenez bien ce schéma :



Il faut installer sur le serveur les paquets d'un serveur web compatible avec php, le sgbd MySQL, l'interface d'administration phpMyAdmin (même si, en fait, elle n'est pas obligatoire) et l'interpréteur php.

La gestion des droits des utilisateurs peut se faire à 3 niveaux, le niveau base de données étant celui généralement utilisé.

Le suivi de l'activité du serveur MySQL est importante pour détecter les problèmes de configuration.

Si vous voulez approfondir

Vous avez en main tous les outils pour installer les très nombreux services webs libres ou gratuits fonctionnant sous php/MySQL (cms, forums, wikis, etc.)

La programmation de sites en php/MySQL est un champ d'étude extrêmement large, étant donné que ce sont les outils de développement à la mode ! Si vous voulez vous lancer dans ce domaine, achetez un bon livre (php/MySQL de l'éditeur O'Reilly) et utilisez les nombreux sites qui leur sont dédiés.

Consulter la référence et réaliser les configurations proposées : <http://wiki.phpmyadmin.net/pma/Security>

Atelier 18

Installation
de Php/MySQL

Page 234

Atelier 19

Installation de Java/Tomcat

► Objectif

À la fin de cet atelier, vous saurez installer une plate-forme pour héberger des sites Internet dynamiques développés en Java/Tomcat. Vous saurez interfacier Tomcat avec Apache.

► Durée approximative de cet atelier : 2 heures

► Durée approximative de cet atelier

Serveur Linux Debian 6 avec Apache 2.2

► Considérations techniques

Côté serveur, nous allons travailler avec les logiciels suivants :

- le langage Java 1.6 ;
- le conteneur d'applications Tomcat 6.

Sur le client, n'importe quel navigateur fera l'affaire (Firefox, Explorer, Chrome, Safari, etc.).

► Que faire si je bloque ?

Consultez les sites des développeurs des logiciels :

<http://tomcat.apache.org/>

<http://wiki.apache.org/tomcat/>

► Contenu

1. Introduction	236
2. Installation	236
3. Utilisation basique.....	240
4. Interaction avec Apache.....	241
5. Dépannage.....	243

1. Introduction

Java est une plateforme de développement adaptée pour les applications webs complexes et robustes. Cette technologie initiée par SUN en 1995 connaît un grand succès et de plus en plus de produits l'utilise.

Dans mon contexte professionnel, nous hébergeons des applications « maison » développées dans cet environnement, mais aussi un certain nombre d'applications libres telles Alfresco, CAS, Request Tracker, Lucene, Typo3, etc.

2. Installation

Nous allons installer le serveur Tomcat et vous allez constater que, contrairement à php, où l'installation était très légère, ici nous déployons l'artillerie lourde !

2A. Installation de Java

Java est à Linux/Tomcat ce que.NET est à Windows/IIS. Ces deux environnements de développement ont certes de nombreux points communs mais restent tout de même différents. Une des gros avantages de Java sur.NET est certainement l'aspect multiplateforme au prix d'une certaine lourdeur et lenteur dans l'exécution. Mais ces considérations n'engagent que moi !

Le deuxième débat avant d'attaquer l'installation est : quelle implémentation du JDK (Java Development Kit) installer ? En effet, vous avez deux possibilités :

- le JDK de SUN : le vrai, le pur mais il n'est pas sous une licence libre
- OpenJDK : la version 100% libre

Autres considérations qui n'engagent que moi : si vous voulez être certain de n'avoir aucun problème dans le déploiement des applications et que la problématique des licences ne vous souci pas, alors installez le JDK de SUN. Sinon, pour une installation plus simple et conserver une machine totalement « libre », installez OpenJDK. Celui-ci est réputé pour être à 99% identique à celui de SUN. Mais des fois, ce sont les 1% restant qui comptent ;-)

Pour votre formation, nous installerons le JDK de SUN car cela me permet de vous montrer comment modifier la configuration de apt afin d'aller chercher des paquets dans les dépôts non standards. En effet, ce logiciel n'étant pas libre, il est placé dans un dépôt « non-free » afin de ne pas mélanger les torchons et les serviettes !!!

Il nous faut donc modifier les sources apt pour ce faire :

```
# vi /etc/apt/sources.list
```

et ajouter en fin de fichier cette ligne :

```
deb http://ftp.fr.debian.org/debian/ squeeze non-free
```

ensuite, vous mettez à jour la liste des paquetages :

```
# apt-get update
```

Maintenant installons le logiciel :

```
# apt-get install sun-java6-jdk
```

Vous devrez accepter les termes de la licence SUN pour achever l'installation. Lorsque c'est terminé, nous avons le nécessaire pour développer des applications en Java pour la ligne de commande :

```
# java -version
java version "1.6.0_26"
Java(TM) SE Runtime Environment (build 1.6.0_26-b03)
Java HotSpot(TM) 64-Bit Server VM (build 20.1-b02, mixed mode)
```

2B. Installation de Tomcat

Ensuite, installons Tomcat à proprement parler :

```
# apt-get install tomcat6 tomcat6-admin
```

Par défaut, le serveur Tomcat écoute sur le port 8080 :

```
# netstat -plunt | grep java
tcp6        0      0 :::8080          :::*             LISTEN 6541/java
tcp6        0      0 127.0.0.1:8005  :::*             LISTEN 6541/java
```

Exercice 1

Et le port 8005 ? Hé hé, vous êtes bien accroché à votre fauteuil ? Vous faites un telnet localhost 8005 puis vous tapez SHUTDOWN en majuscules suivi de entrée. Maintenant vous refaites netstat -plunt | grep java.

1. que constatez-vous ?
2. qu'en déduire en termes de sécurité ? En particulier, pensez-vous que cette manipulation puisse être faite au travers du réseau ?

Non vous n'avez pas rêvé. C'est le comportement parait-il « normal » (cf. le wiki officiel de apache : <http://wiki.apache.org/tomcat/FAQ/Security#Q2>). Une solution pour limiter les dégâts consiste à changer le mot utilisé pour l'arrêt. Dans /etc/tomcat6/server.xml, à la ligne suivante :

```
<Server port="8005" shutdown="SHUTDOWN">
```

remplacer le mot SHUTDOWN par un mot plus complexe (une sorte de mot de passe) et de rendre ce fichier accessible uniquement aux utilisateurs root et tomcat6 (enlever le « r » pour « others »).

Revenons à nos moutons. Relancez le démon tomcat6 puis, pour vérifier l'installation, allez à l'adresse : <http://192.168.1.102:8080>

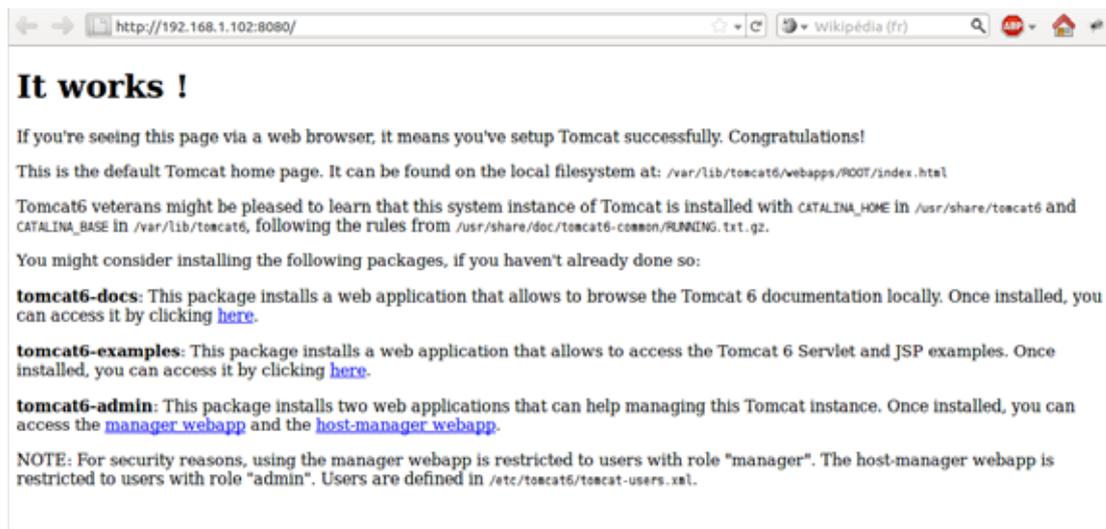


Figure 1 : écran d'accueil de Tomcat

Comme indiqué en bas de l'écran précédent, pour accéder aux outils d'administration, il faut d'abord déclarer un utilisateur :

```
# vi /etc/tomcat6/tomcat-users.xml
```

Modifiez le fichier afin d'obtenir ceci :

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="manager" />
  <role rolename="admin" />
  <user username="admin" password="xxxxxxxxxx" roles="admin,manager" />
</tomcat-users>
```

Contrôlez les droits d'accès à ce fichier accessible uniquement à root et tomcat6.

Redémarrez Tomcat et vous aurez accès aux liens « manager webapp » et « host-manager webapp » de la page d'accueil.

2C. Outils d'administration

Examinons les deux outils d'administration à disposition. Ce sont des webapp, donc des applications web.

Important : même si ces webapps sont protégées par mot de passe, il n'est pas très sain de les laisser accessibles au monde entier sur un serveur de production. On peut très bien s'en passer (et tout faire en ligne de commandes). Sinon, il faut bloquer à l'accès à ces sites sur vos adresses IP d'administration.

2C1. Manager webapp

Cet outil permet de gérer les différentes Webapp déployées sur le serveur (arrêt, redémarrage,...) mais aussi d'en déployer de nouvelles. Lorsqu'une application web Java est compilée, celle-ci est générée sous la forme d'un fichier war (Web Application aRchive). Pour aller vite, disons que c'est un fichier compressé qui contient tout le nécessaire pour déployer et faire fonctionner l'application.

Donc, à partir de cet outil, on peut téléverser un fichier war. Si celui-ci est correct, il sera automatiquement déployé sur Tomcat.



Gestionnaire d'applications WEB Tomcat

Message:

Gestionnaire

[Lister les applications](#) [Aide HTML Gestionnaire](#) [Aide Gestionnaire](#) [Etat du serveur](#)

Applications

Chemin	Nom d'affichage	Fonctionnelle	Sessions	Commandes
/		true	0	Démarrer Arrêter Recharger Retirer Expire les sessions inactives depuis <input type="text" value="30"/> minutes
/host-manager	Tomcat Manager Application	true	0	Démarrer Arrêter Recharger Retirer Expire les sessions inactives depuis <input type="text" value="30"/> minutes
/manager	Tomcat Manager Application	true	1	Démarrer Arrêter Recharger Retirer Expire les sessions inactives depuis <input type="text" value="30"/> minutes

Deployer

Emplacement du répertoire ou fichier WAR de déploiement sur le serveur

Chemin de contexte (requis):

URL du fichier XML de configuration:

URL vers WAR ou répertoire:

Fichier WAR à déployer

Choisir le fichier WAR à téléverser

Figure 2 : écran principal du manager de webapp

Atelier 19

Installation de Java/Tomcat

Page 239

2C2. Host-manager Webapp

Cette webapp concerne la gestion du serveur lui-même. Il est possible de créer des hôtes virtuels, tout comme dans Apache.



Tomcat Virtual Host Manager

Message: OK

Host Manager

List Virtual Hosts HTML Host Manager Help (TODO) Host Manager Help (TODO) Server Status

Host name	Host aliases	Commands
localhost		Start Stop Remove

Add Virtual Host

Host

Name:

Aliases:

App base:

AutoDeploy

DeployOnStartup

DeployXML

UnpackWARs

XmlNamespaceAware

XmlValidation

Manager App

Figure 3 : écran principal du host-manager

Atelier 19

Installation
de Java/Tomcat

Page 240

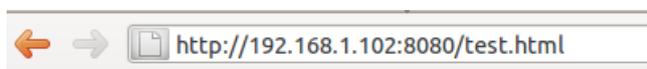
3. Utilisation basique

Tomcat embarque un serveur web dont la racine se trouve (sous Debian) dans `/var/lib/tomcat6/webapps/ROOT/`.

Créez dans ce répertoire un fichier `test.html` dans lequel vous mettez par exemple :

```
<h1>Test Tomcat</h1>
```

Si vous allez à cette URL, vous devez voir :



Test Tomcat

Pour que ceci soit un fichier « Java » interprété par le serveur, il suffit qu'il porte une extension `.jsp`. Donc renommez le fichier `test.html` en `test.jsp` et affichez le dans votre navigateur. Le résultat est le même mais vous avez certainement constaté que le temps de réponse a été nettement plus long ! Normal, toute la machinerie Java/Tomcat s'est mise en route !

Ce fichier `jsp` est vraiment simplissime puisqu'il n'y a aucune instruction Java. Pour le fun, modifions notre fichier `test.jsp` en ceci :

```
<h1>Test Tomcat réalisé le <%= new java.util.Date() %>
</h1>
```

Le résultat est maintenant :



Nous n'irons pas plus loin dans cette voie.

4. Interaction avec Apache

Nous venons de voir que Tomcat intègre un serveur Web qui pourrait être suffisant dans bien des cas. Néanmoins, la pratique généralement répandue consiste à mettre Apache en frontal de Tomcat afin de tirer le meilleur partie des deux produits. Les raisons sont les suivantes :

- performance : Apache est plus rapide à servir des pages html statiques ;
- cohabitation : il est facile avec Apache de faire cohabiter différents langages de développement ;
- clustering
- sécurité

Tous les détails sont ici : <http://wiki.apache.org/tomcat/FAQ/Connectors#Q3>

Apache recevra toutes les requêtes et il transmettra celles qui concernent Tomcat : donc, Tomcat ne recevra plus les requêtes directement.

Installons le module pour Apache2 :

```
# apt-get install libapache2-mod-jk
```

Dans le fichier de configuration de ce module, nous ajoutons :

```
# vi /etc/apache2/mods-enabled/jk.load
LoadModule jk_module /usr/lib/apache2/modules/mod_jk.so
    JkWorkersFile /etc/apache2/workers.properties
    JkLogFile /var/log/apache2/mod_jk.log
    JkLogLevel info
```

Ensuite, il faut créer le fichier /etc/apache2/workers.properties avec ce contenu :

```
workers.tomcat_home=/usr/share/tomcat6
workers.java_home=/usr/lib/jvm/java-6-sun
ps=/
worker.list=worker1
worker.worker1.port=8009
worker.worker1.host=localhost
worker.worker1.type=ajp13
worker.worker1.lbfactor=1
```

À ce stade, nous devons choisir dans quel site la partie Java/Tomcat sera accessible. Supposons que cela soit dans le site par défaut mais n'oublions pas que phpMyAdmin doit continuer à être servi par Apache.

Au début du fichier de configuration du site par défaut (/etc/apache2/sites-enabled/000-default) ajoutons les lignes en gras :

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost

    JkMount /*/ worker1
    JkMount /* worker1

    SetEnvIf Request_URI "/phpmyadmin/*" no-jk
```

Note : le mot worker1 doit être cohérent entre le fichier workers.properties et le fichier de configuration de Apache.

Enfin, dans le fichier /etc/tomcat6/server.xml nous devons activer le port TCP 8009 qui sert de communication entre Apache et Tomcat (ils pourraient donc être sur des machines différentes) :

Recherchez ces lignes :

```
<!--
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
-->
```

Enlevez les commentaires html et remplacez par ceci :

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8080" />
```

Atelier 19

Installation
de Java/Tomcat

Page 242

Il faut redémarrer Tomcat et vérifier que le port est maintenant actif :

```
root@mv2-linux:/var/lib/tomcat6/webapps/ROOT# netstat -plunt | grep
java
tcp6      0      0 :::8080          :::*             LISTEN
8273/java
tcp6      0      0 127.0.0.1:8005  :::*             LISTEN
8273/java
tcp6      0      0 :::8009          :::*             LISTEN
8273/java
```

Puis nous rechargeons la configuration de Apache2 et nous vérifions que le module jk est bien chargé :

```
# /etc/init.d/apache2 reload
Reloading web server config: apache2.
# apache2ctl -M
Loaded Modules:
    core_module (static)
    log_config_module (static)
    logio_module (static)
    mpm_prefork_module (static)
    http_module (static)
    so_module (static)
    alias_module (shared)
    auth_basic_module (shared)
    authn_file_module (shared)
    authz_default_module (shared)
    authz_groupfile_module (shared)
```

```
authz_host_module (shared)
authz_user_module (shared)
autoindex_module (shared)
cgi_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
jk_module (shared)
mime_module (shared)
negotiation_module (shared)
php5_module (shared)
setenvif_module (shared)
status_module (shared)
```

Syntax OK

La page d'accueil de Tomcat est maintenant accessible sur <http://apache.labocned.local>. Mais le site Tomcat est toujours accessible sur <http://192.168.1.102:8080> or cette adresse n'est plus nécessaire, nous pouvons la désactiver dans la configuration de Tomcat. Il faut commenter (commentaires html <!-- -->) le bloc suivant dans le fichier /etc/tomcat6/server.xml :

```
<!--
  <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    URIEncoding="UTF-8"
    redirectPort="8443" />
-->
```

Ensuite, on relance Tomcat (vérifiez avec netstat que le port 8080 n'est plus actif).

Atelier 19

Installation
de Java/Tomcat

Page 243

5. Dépannage

Pensez à vider régulièrement le cache de votre navigateur, celui-ci ne manquera pas de vous jouer quelques tours...

L'analyse des fichiers de logs est à peu près le seul moyen de détecter un problème. Pour ce qui est de Tomcat, les fichiers de logs sont dans /var/log/tomcat6 et principalement le fichier catalina.out.

À retenir

Tomcat est un conteneur d'applications web développées en langage Java.

Il intègre également un serveur de pages html mais il est conseillé d'utiliser Apache comme frontal web. Celui-ci, via le module JK, redirige les requêtes vers Tomcat lorsque cela est nécessaire.

Si vous voulez approfondir

Voir votre cours de développement pour ce qui relève du développement Java.

Atelier 20

Apache et https

► Objectif

Mettre en place des connexions réseau chiffrées afin de rendre les données illisibles à qui n'est pas autorisé.

► Durée approximative de cet atelier : 1 heure 30

Vos services Web Apache et Tomcat doivent être opérationnels.

► Considérations techniques

Nous poursuivons nos pérégrinations dans le logiciel Linux et entamons un point essentiel dans le secteur informatique : le chiffrement des données. Nous mettrons en œuvre ce concept pour le chiffrement des données échangées par un serveur Web (vous avez déjà certainement utilisé le protocole *https* avec votre navigateur).

► Contenu

1. SSL	246
2. HTTPS : le web chiffré	247

Atelier 20

Apache et https

Page 245

1. SSL

Commençons par quelques rappels sur SSL (*Secure Sockets Layer*). Dans le monde TCP/IP, le chiffrement des données repose en grande partie sur ce protocole. Il a été conçu par la société Netscape pour assurer une communication confidentielle et fiable entre deux applications (un client et un serveur), pour identifier le serveur et parfois le client. SSL nécessite un protocole de transport sûr comme TCP pour la transmission et la réception de données. Il permet la sécurisation de tout protocole applicatif s'appuyant sur TCP tels que HTTP ou LDAP.

Le protocole est composé de deux couches qui s'insèrent entre le protocole de transport et les protocoles applicatifs :



Figure 1 : le protocole SSL

Au niveau le plus bas, juste au dessus d'un protocole de transport sûr, se trouve le *SSL Record Protocol* qui permet de transmettre de manière chiffrée les données. Celui-ci est utilisé pour encapsuler d'autres protocoles de plus haut niveau tel que le *SSL Handshake Protocol* qui permet au serveur et au client de s'authentifier et de négocier le fonctionnement de la session. Quatre phases de négociation peuvent être distinguées :

Phase 1 : Établissement des paramètres de sécurité

Cette phase a pour but d'établir le lien sécurisé. Le client envoie au serveur un message *client_hello* contenant des paramètres tels que, sa version de SSL utilisée, son identifiant de connexion, une liste d'algorithmes d'échange de clés et de chiffrement supportée par le client et classée selon la qualité de l'algorithme. Il envoie aussi un jeu de données qui sont générées aléatoirement. Après avoir envoyé ces requêtes, le client attend la réponse du serveur.

Phase 2 : Authentification du serveur et échange des clés

Le serveur envoie *server_hello*, qui contient la version de SSL, les meilleurs algorithmes à utiliser, un jeu de données générées aléatoirement et le certificat¹ s'il existe. Dans le cas où le serveur n'a pas de certificat, ce premier message sera suivi d'un message *server_key_exchange* pour qu'il puisse tout de même transmettre sa clé publique. Ensuite, le serveur peut demander au client un certificat en envoyant un message *certificate_request*. Finalement, le serveur envoie le message *server_done*, qui signifie la fin de cette phase et que le serveur se met en attente.

Phase 3 : Authentification du client et échange des clés

Le client doit vérifier que le certificat envoyé par le serveur est valide et que les autres paramètres sont corrects. Si le serveur a demandé au client d'envoyer un certificat, le client envoie un message *certificate* contenant le certificat (s'il n'a pas de certificat, il envoie un message *no_certificate*).

1. Un certificat est une carte d'identité numérique identifiant une machine. Le certificat contient, entre autres, la clé publique. Nous reviendrons sur cette notion un peu plus loin.

Il génère ensuite à partir de l’algorithme de chiffrement choisi une “pré” clé secrète (*pre_master_key*). Il envoie un message *client_key_exchange* contenant la “pré” clé secrète chiffré à l’aide de la clé publique du serveur. Pour finir cette phase, le client envoie un message *certificate_verify* pour indiquer que le certificat du serveur a été vérifié

Phase 4 : Fin

Le serveur vérifie éventuellement la validité du certificat du client. Il déchiffre ensuite la “pré” clé secrète à l’aide de sa clé privée. Le client et le serveur réalisent une même série d’opérations pour obtenir des clés secrètes de session à partir de la “pré” clé secrète et des données aléatoires échangées précédemment.

Le client envoie enfin le message *finished* qui valide l’échange de clés. Le serveur répond en envoyant son message *finished*. Les deux parties sont maintenant identifiées, le protocole *handshake* est terminé et les communications sécurisées (chiffrées avec la clé secrète générée) peuvent avoir lieu.

Toutes ces manipulations sont réalisées par le protocole mais il est bon que vous les connaissiez. Passons maintenant à l’administration de notre serveur.

2. HTTPS : le web chiffré

2A. Sur le serveur

2A1. Stratégie

L’organisation mise en place actuellement sur notre serveur n’est pas satisfaisante. En effet, les outils d’administration sont accessibles en clair : pas de chiffrement entre le client et le serveur. Les mots de passe saisis peuvent être capturés par un tiers dans l’Internet, ce qui n’est pas acceptable, même dans un réseau local.

Nous allons donc réorganiser notre Apache de la façon suivante :

URL	Techno	Chiffré ?	Commentaire
apache.labocned.local	Java	non	Page d’accueil Java
site1.labocned.local	Php	Non	Site en php
site1.labocned.local	Php	Non	Site en php
secure.labocned.local/phpmyadmin	Php	Oui	Administration de MySQL
secure.labocned.local/manager/html	Java	Oui	Gestion des webapps Java
secure.labocned.local/host-manager/html	Java	Oui	Gestion des hôtes virtuels Tomcat

Tous les sites d’administration en https et le reste en http.

2A2. Installation des outils

Pour passer au Web chiffré, il faut adjoindre à notre Apache un petit module nommé `mod_ssl`. Nous allons également avoir besoin de `openssl` :

```
mv2-linux:~# dpkg -l openssl
Souhait=inconnU/Installé/suppRimé/Purgé/H=à garder
| État=Non/Installé/fichier-Config/dépaqUeté/échec-conFig/H=semi-
installé/W=attnd-traitement-déclenchements
|/ Err?=(aucune)/H=à garder/besoin Réinstallation/X=les deux
(État,Err: majuscue=mauvais)
|/ Nom Version Description
+-+-----+-----+-----+-----+-----+-----+-----+-----+
=====
ii openssl 0.9.8o-4squeeze1 Secure Socket Layer (SSL) binary and
related
```

Vérifions `mod_ssl` avec Apache2 : est-il disponible ?

```
mv2-linux:/# ls /etc/apache2/mods-available | grep ssl
ssl.conf
ssl.load
```

`mod_ssl` est-il activé ?

```
mv2-linux:/# ls /etc/apache2/mods-enabled | grep ssl
[...] Pas de ssl en vue [...]
```

Alors activons-le : (la commande `a2enmod` est une contraction de *apache2 enable module...*)

```
mv2-linux:~# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to
configure SSL and create self-signed certificates.
Run '/etc/init.d/apache2 restart' to activate new configuration!
```

Bien sûr nous relancerons Apache2 le moment venu puisque nous modifions sa configuration. En attendant vérifions l'effet de notre commande :

```
mv2-linux:/# ls /etc/apache2/mods-enabled | grep ssl
ssl.conf
ssl.load
```

`mod_ssl` est maintenant actif.

2A3. Génération du certificat

Nous allons créer un certificat de sécurité pour notre site sécurisé (ça crée donc une clé privée attachée à un certificat de sécurité) :

Nous allons générer une clé privée pour le serveur `secure.labocned.local` :

```

mv2-linux:~# cd /etc/apache2/
mv2-linux:/etc/apache2# mkdir ssl
mv2-linux:/etc/apache2# cd ssl
mv2-linux:/etc/apache2/ssl# openssl genrsa 2048 > secure.labocned.
local.key
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

```

Notes :

- vous pouvez ajouter `-des` ou `-des3` pour chiffrer la clé ce qui permet une meilleure protection. Toutefois, à chaque redémarrage du serveur, il faudra une intervention manuelle pour saisir la *passphrase*... Cela peut être gênant en production...
- vous pouvez ajouter quelque chose du style `-rand/var/log/messages` afin d'ajouter de l'aléatoire et améliorer ainsi la qualité de la clé.

Nous allons maintenant générer une demande de certificat nommée **secure.labocned.local.csr**

```

mv2-linux:/etc/apache2/ssl# openssl req -new -key secure.labocned.
local.key -out secure.labocned.local.csr
You are about to be asked to enter information that will be
incorporated
Into your certificat request.
What you are about to enter is what is called a Distinguished Name
or DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: <tapez fr>
Sate or Province Name (full name) [Some-State]: <laissez vide
ENTER>
Locality Name (eg, city) []: <laissez vide ENTER>
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
<saisissez labocned>
Organizational Unit Name (eg, section) []: <saisissez labocned>
Common Name (eg, YOUR name) []: <très important saisissez le nom
FQDN de la machine : secure.labocned.local>
Email Address []: <laissez vide ENTER>
Please enter the following 'extra' attributes
To be sent with your certificate request
A challenge password []: <laissez vide ENTER>
An optional company name []: <laissez vide ENTER>

```

Ouf!!!

En production, il faut faire signer ce certificat par un tiers de confiance... Comme déjà évoqué avec IIS, nous travaillons avec des certificats auto-signés. Donc, nous allons traiter « nous-même » la demande et signer le certificat, comme si nous étions autorité de certification.

```
mv2-linux:/etc/apache2/ssl# openssl x509 -req -days 365 -in
secure.labocned.local.csr -signkey secure.labocned.local.key -out
secure.labocned.local.crt
Signature ok
subject=/C=fr/ST=Some-State/O=labocned/OU=labocned/CN=secure.
labocned.local
Getting Private key
```

À ce stade, nous sommes positionnés dans /etc/apache2/ssl et regardons ce que nous avons :

```
mv2-linux:/etc/apache2/ssl# ls
secure.labocned.local.crt  secure.labocned.local.csr  secure.
labocned.local.key
```

Le fichier de demande (csr) n'est plus utile, on pourrait le supprimer.

À quoi ressemble un certificat? Regardons secure.labocned.local.crt (évidemment vous n'avez pas le même contenu que moi ;-)

```
mv2-linux:/etc/apache2/ssl# cat secure.labocned.local.crt
-----BEGIN CERTIFICATE-----
[...]
-----END CERTIFICATE-----
```

Atelier 20

Apache et https

Page 250

Il est indispensable d'ajuster les permissions afin de protéger la clé privée :

```
mv2-linux:/etc/apache2# chown -R root:root /etc/apache2/ssl/
mv2-linux:/etc/apache2# chmod -R 400 /etc/apache2/ssl/
```

2A4. Configuration réseau

Il n'est pas recommandé d'exécuter des sites en http et https sur la même adresse IP, cela peut entraîner une faille de sécurité. Il est donc préférable de déclarer une deuxième adresse sur notre machine. En effet, il est tout à fait possible qu'une même machine avec une seule carte réseau possède plusieurs adresses.

Pour ce faire, nous allons dans le fichier /etc/network/interfaces afin d'ajouter les clauses suivantes :

```
auto eth0:1
iface eth0:1 inet static
address 192.168.1.103
netmask 255.255.255.0
```

Après avoir enregistré ce fichier, il suffit de faire un `ifup eth0:1`. Nous pouvons constater le résultat ainsi :

```
root@mv2-linux:~# ifconfig
eth0:1 Link encap:Ethernet HWaddr 08:00:27:9b:49:90
       inet      adr:192.168.1.102          Bcast:192.168.1.255
       Masque:255.255.255.0
       adr inet6: fe80::a00:27ff:fe9b:4990/64 Scope:Lien
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:157 errors:0 dropped:0 overruns:0 frame:0
TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 lg file transmission:1000
RX bytes:16571 (16.1 KiB) TX bytes:19697 (19.2 KiB)
eth0:1 Link encap:Ethernet HWaddr 08:00:27:9b:49:90
       inet      adr:192.168.1.103          Bcast:192.168.1.255
       Masque:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

Enfin, nous ajoutons un hôte dans le DNS Windows afin de résoudre le nom `secure.labocned.local` en `192.168.1.103`.

2A5. Configuration Apache

Un serveur http sécurisé n'écoute pas sur le port 80, mais sur le **port 443**. Dans cette version d'Apache, le port est ouvert dès que l'on active le `mod_ssl`. On complète le fichier `ports.conf` avec les deux adresses IP :

```
mv2-linux:/etc/apache2# vi /etc/apache2/ports.conf
Listen 192.168.1.102:80
Listen 192.168.1.103:443
```

Dans le fichier `/etc/apache2/sites-available/default`, nous effectuons les modifications suivantes :

```
<VirtualHost _default_:80>
    ServerAdmin webmaster@localhost

    #   JkMount /*/ worker1
    JkMount / worker1
    #   SetEnvIf Request_URI "/phpmyadmin/*" no-jk

    DocumentRoot /var/www
```

Deux lignes sont commentées car inutiles (on peut les supprimer). La troisième nous indique que tout ce qui est à la racine du serveur http est redirigé vers Tomcat.

Attaquons-nous maintenant au fichier de configuration du serveur https proprement dit. La Debian Squeeze est livrée avec un squelette de fichier de configuration https satisfaisant, il suffit de l'adapter à notre besoin. Quelles sont les directives nécessaires ?

Actuellement, Apache2 ne supporte pas les hôtes virtuels ssl. Vous pouvez avoir plusieurs sites ssl sur le même serveur mais dans ce cas, ils doivent écouter sur des ip différentes. Donc, vous n'avez pas à configurer de `NameVirtualHost`.

Par contre, une configuration minimale nécessite de définir :

- SSLCertificateFile /etc/apache2/ssl/secure.labocned.local.crt
- SSLCertificateKeyFile /etc/apache2/ssl/secure.labocned.local.key

Ensuite, il faudra ajouter ces lignes pour gérer les sites qui dépendent du https :

```
Alias /phpmyadmin /usr/share/phpmyadmin
JkMount /host-manager/* worker1
JkMount /manager/* worker1
SetEnvIf Request_URI "/phpmyadmin/*" no-jk
```

Note : la première ligne (Alias) doit être supprimée de /etc/apache2/conf.d/phpmyadmin.conf afin de s'assurer que phpmyadmin n'est visible qu'en https.

En utilisant le fichier /etc/apache2/sites-available/default-ssl, vous faites les modifications nécessaires puis vous redémarrez le service :

```
mv2-linux:/etc/apache2# a2ensite default-ssl
Enabling site default-ssl.
Run '/etc/init.d/apache2 reload' to activate new configuration!
mv2-linux:/etc/apache2# /etc/init.d/apache2 reload
Reloading web server config: apache2.
mv2-linux:/etc/apache2#
```

Vérifions que tout a été pris en compte. Contrairement au serveur web classique qui écoute sur le port TCP 80, notre serveur https écoute sur le port 443 :

```
root@mv2-linux:~# netstat -plunt | grep apache2
tcp 0 0 192.168.1.102:80 0.0.0.0:* LISTEN 2061/apache2
tcp 0 0 192.168.1.103:443 0.0.0.0:* LISTEN 2061/apache2
```

Atelier 20

Apache et https

Page 252

2B. Sur le client

Tous les navigateurs web supportent nativement le ssl. Essayons d'aller sur notre site, mais nous aurons, tout comme avec IIS ceci :

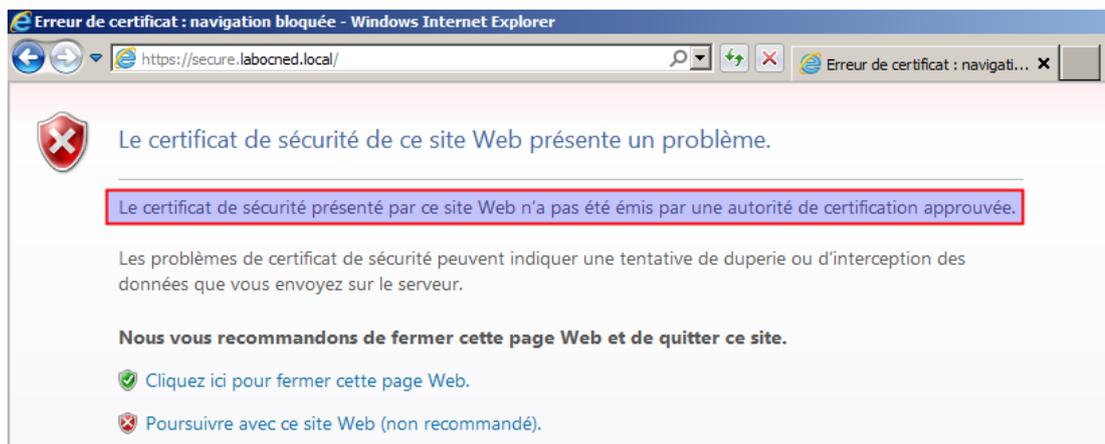


Figure 2 : avertissement certificat

Vous connaissez le principe, cliquez sur « poursuivre avec ce site web » :



Si vous cliquez sur « erreur de certificat », vous pouvez consulter les informations du certificat. En parcourant les différentes rubriques, vous verrez qu'il contient les données suivantes :

Un Certificat Personnel contient les informations suivantes :
<ul style="list-style-type: none">• Le nom de son propriétaire et éventuellement son adresse e-mail : Jean Dupont (jdupont@societe.fr)• Quelques informations optionnelles (adresse physique de la société, fonction de Jean Dupont, etc.)• La clé publique de Jean Dupont à certifier• La date d'expiration du certificat• Un numéro de série unique• Le nom de l'Autorité de Certification qui a délivré le certificat numérique (banque, entreprise, administration, etc.)• La signature de l'Autorité de Certification qui a délivré le certificat numérique (au moyen de la clé secrète de l'Autorité de Certification, sorte de "tampon" de validation d'un passeport électronique).

Notez que vous pouvez « installer » le certificat, de façon à ne plus avoir le message d'erreur puisque le navigateur considérera que vous faites confiance au site.

Maintenant, à vous de vérifier que phpMyAdmin, manager et host-manager sont accessibles en https (et plus en http).

À retenir

Le chiffrement des données permet de les rendre illisibles à qui n'est pas autorisé. La méthode à « clés asymétriques » est la plus répandue. La clé publique du destinataire sert à chiffrer. La clé privée du destinataire lui sert à déchiffrer.

Les clés sont indépendantes et il n'est pas possible d'en générer une connaissant l'autre. Il est théoriquement impossible de générer deux couples de clé identiques.

L'algorithme le plus répandu est SSL (TLS). Il sert à sécuriser les protocoles applicatifs tels http, ldap, etc.

Apache2 supporte le mode https. Il faut générer une clé privée et un certificat pour le serveur. Tant que le certificat n'est pas généré chez une autorité de certification reconnue par les navigateurs (Thawte, Verisign pour ne citer que les plus connues), les navigateurs émettront un message particulièrement dissuasif pour vos utilisateurs.

Dans tous les cas, dès que vous travaillez avec une méthode de chiffrement asymétrique, il faut absolument veiller à la sécurité des clés privées.

Si vous voulez approfondir

Vous pouvez vous documenter sur le fonctionnement des protocoles de chiffrement comme RSA, Idea, Blowfish, etc.

Vous pouvez vous intéresser au chiffrement d'autres protocoles applicatifs (pops, imaps, ldaps, etc.)

Consultez <http://www.gnupgp.org> pour voir comment on peut chiffrer et signer des messages électroniques.

Atelier 21

Virtualisation

► Objectif

Installer et administrer une solution professionnelle de virtualisation.

► Durée approximative de cet atelier : 4 heures

Aucune en particulier sinon d'avoir étudié votre cours bien sûr !

► Considérations techniques

La virtualisation nécessite une infrastructure matérielle importante. Pour réaliser cet atelier dans les meilleures conditions, il vous faudra une machine pour le NAS (éventuellement en VirtualBox pour les tests) mais surtout une machine physique avec de préférence un processeur récent supportant le 64 bits et donc la virtualisation « matérielle » ainsi que quelques Gio de RAM et un espace disque confortable. En effet, vous vous doutez que l'on ne peut pas faire de la virtualisation dans de la virtualisation...

Nous utiliserons le logiciel Proxmox, utilisé dans le milieu professionnel par des hébergeurs comme OVH par exemple.

► Contenu

1. Présentation.....	256
2. Espace de stockage.....	256
3. Virtualisation	262

1. Présentation

Promox est un hyperviseur de type 1. C'est un noyau système très léger en prise directe avec le matériel et qui s'appuie sur une base Linux.

Proxmox propose néanmoins deux modes de virtualisation :

- OpenVZ : c'est un même noyau Linux partagé entre chaque environnement virtuel qui se retrouvent isolés des autres. Cette méthode offre un bon niveau de performance mais cantonne à l'usage de Linux.
- KVM (Kernel-based Virtual Machine) : c'est une véritable solution de virtualisation, chaque machine virtuelle disposant de son matériel. Cette solution permet d'héberger tout type de système d'exploitation mais avec des performances moins bonne qu'OpenVZ.

Avant de développer la partie virtualisation à proprement parler, nous évoquons un sujet central : le stockage.

2. Espace de stockage

2A. Généralités

La sauvegarde est au coeur de la problématique de la virtualisation. En effet, une machine virtuelle n'est finalement qu'un fichier stocké quelque part, mais un fichier qui pèse habituellement plusieurs dizaines de Gio. Le stocker et pouvoir le restaurer en cas de problème avec la machine physique doit donc être une problématique à prendre en compte avant de se lancer dans un tel projet.

Diverses solutions sont disponibles en libre ou non, éventuellement sous la forme de boîtiers pré-installés et pré-équipés de disques. Pour la suite de cet atelier, vous choisissez la solution que vous voulez, la seule contrainte vis-à-vis de l'outil de virtualisation Proxmox que nous allons utiliser toute à l'heure est qu'elle supporte le NFS.

Exercice 1

NAS ? NFS ? Ça veut dire quoi ? Et un SAN alors ?

NAS vs. SAN ? Essayons de résumer très simplement le choix : le NAS est un espace de stockage prévu pour la sauvegarde périodique des machines. On stocke donc quelque part une image à un instant t d'une machine virtuelle, dans le but de la restaurer en cas de besoin (en croisant les doigts pour que jamais cela n'arrive !). Le SAN permet quant à lui de stocker en temps réel les machines virtuelles **en cours d'exécution**, il est alors possible de basculer d'un serveur d'exécution à un autre en cas de panne ou de surcharge par exemple.

Observez la figure suivante :

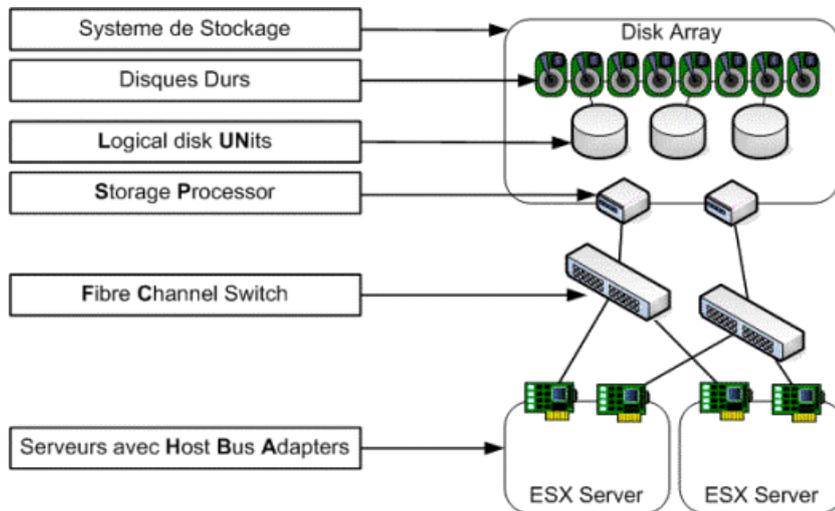


Figure 3 : ESX server et un SAN

Deux serveurs de virtualisation VmWare ESX se partagent un SAN via une connexion Fibre Channel (pour les plus fortunés, sinon iSCSI pour les pauvres).

Comme je n'ai ni iSCSI et encore moins de FC à la maison, nous travaillerons donc avec un NAS ! J'ai choisi Openfiler qui est une solution libre fonctionnant sous Linux et qui peut s'installer sur un PC. Nous ne sommes pas en production bien sûr !

2B. Installation

Téléchargez le logiciel sur le site openfiler.com. Comme maintenant vous êtes grand, je vous laisse gérer l'installation à partir de la documentation officielle du site. En ce qui me concerne, ma machine possède deux disques : un pour le système et un pour le stockage partagé.

Exercice 2

Quelle architecture matérielle proposer pour le serveur en production ?

Lorsque tout est installé, la console du serveur vous donne l'adresse IP du site web d'administration de notre NAS. Chez moi, c'est <https://192.168.1.16:446/> :



Figure 4 : Accueil du site d'administration

J'espère qu'une fois connecté pour la première fois, vous vous êtes empressé de modifier le mot de passe par défaut !

Nous allons maintenant faire les manipulations qui vont nous permettre de créer le partage. Mais d'abord, nous devons déclarer un espace de stockage. Ceci va vous rappeler l'installation de Linux puisque finalement, nous créons un LVM formaté en XFS.

2C. Configuration de l'espace disque

Dans « Volumes », on nous signale qu'il n'existe pas de volume physique. Créons-le :

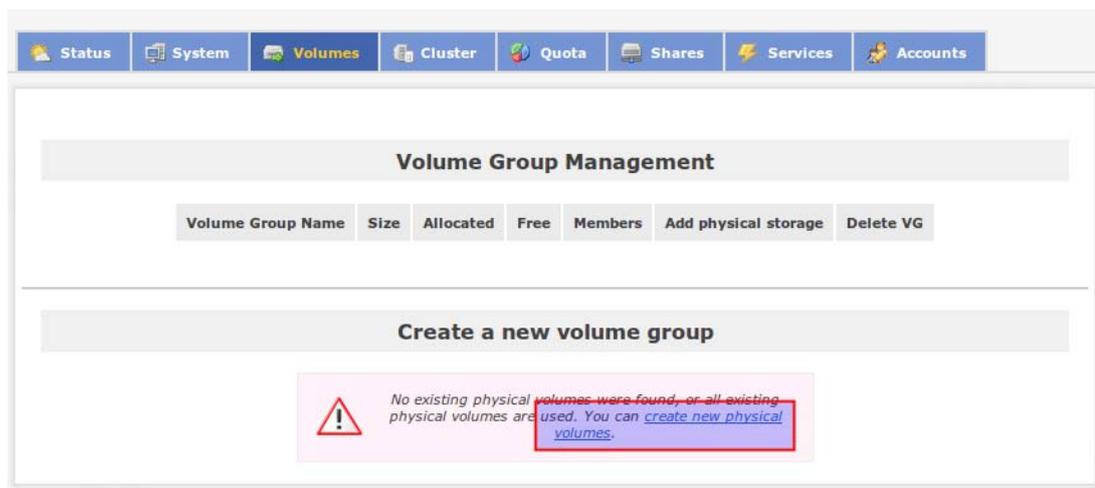


Figure 5 : Gestion des volumes

Atelier 21

Virtualisation

Page 258

Le tableau suivant résume les disques physiques disponibles. Le premier étant réservé au système, nous utiliserons le deuxième. Je choisis donc le disque sdb qui ne contient pour l'instant aucune partition. Une seule partition occupant le disque entier sera créée.

Nous ajoutons maintenant un groupe de volumes qui contient ce volume physique :

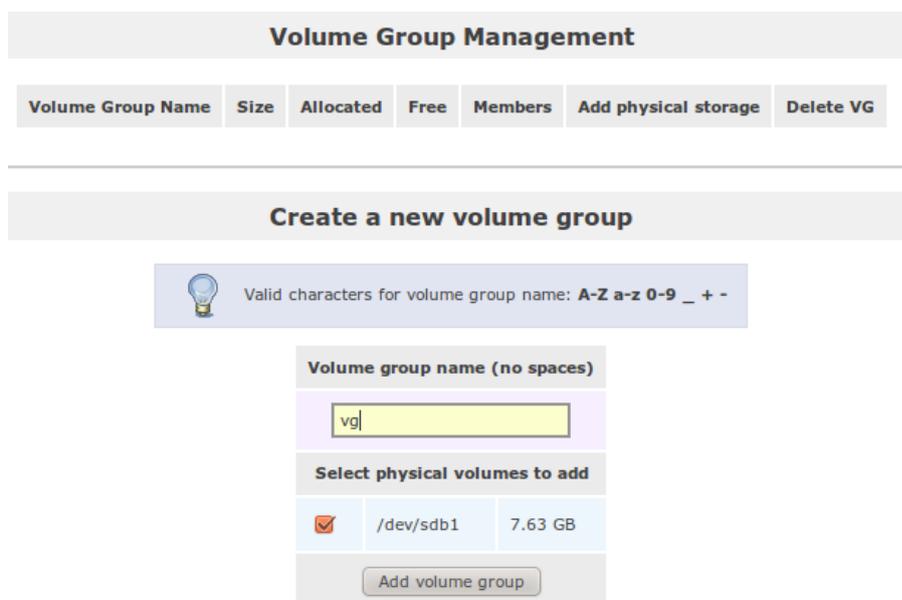
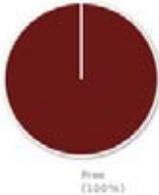


Figure 6 : Création d'un groupe de volumes

Si maintenant nous allons dans l'onglet « Shares », on nous signale qu'il n'y a pas de système de fichiers. Nous allons le créer en mettant tout l'espace disponible formaté en XFS :

Total Space	Used Space	Free Space
7995392 bytes (7808 MB)	0 bytes (0 MB)	7995392 bytes (7808 MB)



Free (100%)

Create a volume in "vg"

Volume Name (*no spaces*. Valid characters [a-z,A-Z,0-9]):

Volume Description:

Required Space (MB):

Filesystem / Volume type:

Figure 7 : Formatage de l'espace disque

Passons maintenant à la configuration réseau.

2D. Configuration réseau

Pour pouvoir partager une ressource, il faut d'abord déclarer le ou les réseaux IP autorisés à y accéder. Allons dans « System/Network Access Configuration » et voyez la configuration que j'ai réalisé sur ma machine :

Network Access Configuration

Delete	Name	Network/Host	Netmask	Type
<input type="checkbox"/>	proxmox1	192.168.1.14	255.255.255.255	Share
<input type="checkbox"/>	proxmox2	192.168.1.15	255.255.255.255	Share
New	<input type="text"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Share"/>

Figure 8 : Configuration d'accès réseau

Exercice 3

J'ai essayé de sécuriser au maximum. Pouvez-vous interpréter l'écran ci-dessus ?
Enfin, il faut activer le service NFS dans le menu « Serveur / Services » :

Manage Services				
Service	Boot Status	Modify Boot	Current Status	Start / Stop
CIFS Server	Disabled	Enable	Stopped	Start
NFS Server	Enabled	Disable	Running	Stop
RSync Server	Disabled	Enable	Stopped	Start

Figure 9 : activation et démarrage de NFS

Ouf ! Passons enfin au partage proprement dit.

2E. Partage

Enfin, créons le partage NFS en allant dans l'onglet « Shares ». Il faut commencer par créer un dossier :



Figure 10 : Création d'un dossier

Puis à le partager :

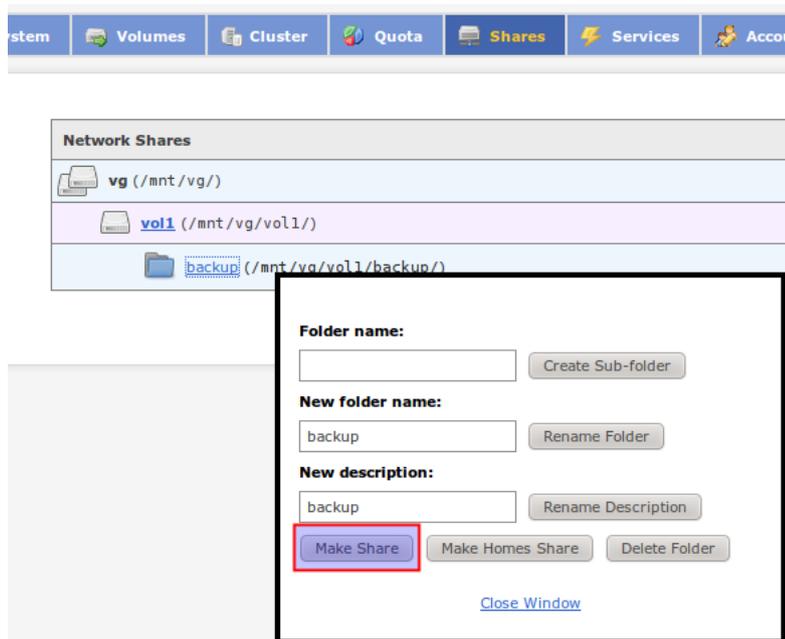


Figure 11 : Partage

Dans l'écran de configuration ci-après nous mettons un accès « public » (*public guest access*) car nous n'avons pas de gestion d'utilisateurs dans Proxmox (cependant Openfiler peut s'intégrer dans un domaine Active Directory ou interroger un annuaire LDAP). Enfin, il faut définir les droits d'accès dans le tableau du bas :

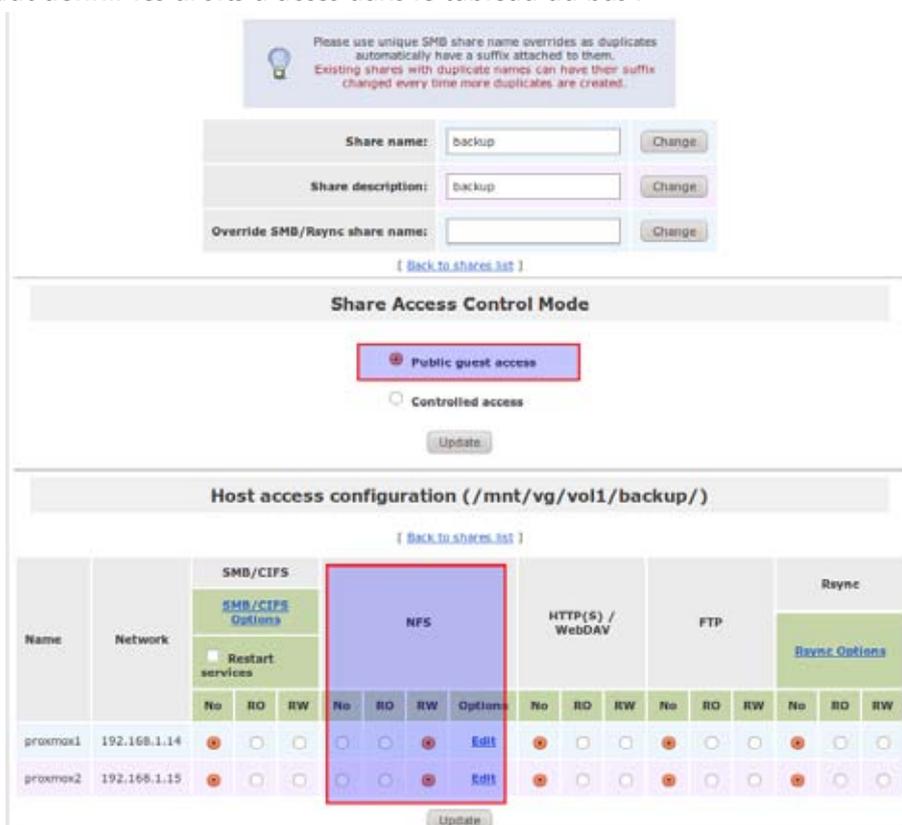


Figure 12 : paramètres du partage

Nos deux machines auront un accès en lecture/écriture (RW).

3. Virtualisation

Téléchargez le logiciel Proxmox sur son site. Avant de vous lancer à corps perdu dans l'installation, veuillez réaliser l'exercice suivant :

Exercice 4

Consultez la page http://pve.proxmox.com/wiki/Installation#System_requirements et donnez la signification des termes :

- Intel VT/AMD-V capable CPU/Mainboard : dans quel cas est-ce nécessaire ?
- 15k rpm SAS, Raid10

3A. Installation

L'installation à proprement parler du logiciel ne doit pas poser de problème particulier. Vous avez le wiki de l'éditeur pour vous aider :



Atelier 21

Virtualisation

Page 262

Une fois installé, le serveur démarre et affiche à la fin, sur la console l'adresse IP de l'interface Web d'administration. Chez moi, c'est <http://192.168.1.14>. Nous observons ci-après la page d'accueil du site qui nous donne un résumé de l'état de la machine :

Vous êtes connectés en tant que 'root'

proxmox

Home | Déconnecter Proxmox Virtual Environment 1.8 www.proxmox.com

Gestionnaire de VM

- Machines virtuelles
- Modèles d'Appliance
- Images ISO

Configuration

- Système
- Storage
- Sauvegarde

Administration

- Serveur
- Logs
- Cluster

Proxmox Virtual Environment

Welcome to the Proxmox Virtual Environment!

For more information please visit our homepage at www.proxmox.com

Local System Status ('proxmox')		Online
Uptime	23:08:33 up 02:23, load average: 0.00, 0.00, 0.00	
CPU(s)	1 x Intel(R) Core(TM) i5 CPU M 480 @ 2.67GHz	
Utilisation CPU	<div style="width: 0.05%; background-color: #008000; border: 1px solid #ccc;"></div> 0.05%	
Retards d'E/S	<div style="width: 0.00%; background-color: #008000; border: 1px solid #ccc;"></div> 0.00%	
Mémoire physique (998MB/181MB)	<div style="width: 181MB; background-color: #008000; border: 1px solid #ccc;"></div> 181MB	
L'espace d'échange (1023MB/0KB)	<div style="width: 0KB; background-color: #008000; border: 1px solid #ccc;"></div> 0KB	
Espace DD root (1.97GB/589MB)	<div style="width: 30.79%; background-color: #008000; border: 1px solid #ccc;"></div> 30.79%	
Version (package/version/build)	pve-manager/1.8/6070	
Version du noyau	Linux 2.6.32-4-pve #1 SMP Mon May 9 12:59:57 CEST 2011	

Figure 13 : état du serveur Proxmox

Les paramètres par défaut de Proxmox sont tout à fait corrects et l'installation d'une machine virtuelle peut se faire immédiatement. Deux modes sont possibles :

- OpenVZ : on peut récupérer sur le site de Proxmox des appliances déjà configurées et installées ainsi que des machines avec un simple système d'exploitation sans applications.
- KVM : on peut faire une installation complète à partir d'une image ISO d'une distribution quelconque de Linux ou de Windows.

Dans le menu « Modèles d'appliance » nous pouvons télécharger les machines suivantes (d'autres sont disponibles sur le site proxmox.com) :

Atelier 21

Virtualisation

Page 263

Gestionnaire de VM

- Machines virtuelles
- Modèles d'Appliance
- Images ISO

Configuration

- Système
- Storage
- Sauvegarde

Administration

- Serveur
- Logs
- Cluster

Modèles d'Appliance

Local Télécharger

Certified Appliances

Description	Version	Type	Nom du paquet
Proxmox Mail Gateway	2.6-2	openvz	proxmox-mailgateway
CYAN Secure Web	1.8.4-1	openvz	cyan-sweb

Section 'admin'

Description	Version	Type	Nom du paquet
Extensible trouble-ticket tracking system	3.8.8-2	openvz	request-tracker
Zenoss Core IT monitoring	2.5.1-1	openvz	zenoss

Section 'system'

Description	Version	Type	Nom du paquet
CentOS 4 (standard)	4.9-1	openvz	centos-4-standard
CentOS 5 (standard)	5.6-1	openvz	centos-5-standard
Debian 4.0 (standard)	4.0-5	openvz	debian-4.0-standard
Debian 5.0 (standard)	5.0-2	openvz	debian-5.0-standard
Debian 6.0 (standard)	6.0-4	openvz	debian-6.0-standard
Fedora 14 (standard)	14-1	openvz	fedora-14-standard
Ubuntu Lucid (standard)	10.04-4	openvz	ubuntu-10.04-standard
Ubuntu Hardy (standard)	8.04-3	openvz	ubuntu-8.04-standard

Section 'www'

Description	Version	Type	Nom du paquet
Acquia Drupal Content Management	1.2.21-1	openvz	acquia
Drupal Content Management	6.20-1	openvz	drupal
Joomla! Content Management	1.6-3	openvz	joomla
MediaWiki	1.15-5	openvz	mediawiki
SugarCRM customer relationship management	6.1.4-1	openvz	sugarcrm
Wordpress	3.1.2-1	openvz	wordpress

Figure 14 : Modèles d'appliance

Après téléchargement, l'appliance sera disponible dans l'onglet « Local » pour être déployée autant que de besoin. Pour ma part, j'ai téléchargé Joomla et donc dans la partie « Machines virtuelles/Créer » cette appliance est proposée comme modèle :

Machines virtuelles

Lister Créer Migrer

Attention: Ce processeur (CPU) ne supporte pas les technologies Intel VT / AMD-V, vous ne pouvez donc pas faire fonctionner de machine virtuelle via KVM.

Configuration

Type: Container (OpenVZ) VMID: 101

Modèle: debian-6.0-joomla_1.6-3_138 Noeud du cluster: proxmox (192.168.1.14)

Nom d'hôte: joomla1 Démarrer au boot:

Mémoire (MB): 512 Espace Disque (GB): 8

Swap (MB): 512

Mot de passe: *****

Confirmer le mot de passe: *****

Réseau

Type de réseau: Ethernet "bridgé" (veth) Domaine DNS: labocned.local

Bridge: vmbr0 Premier serveur DNS: 192.168.1.1

MAC Address: 2E:87:D1:48:D1:F0 Deuxième serveur DNS: 0.0.0.0

create

Figure 15 : Créer une machine virtuelle

Les paramètres à indiquer sont encore plus simples qu'avec VirtualBox ! Une fois créée (très rapidement puisque ce n'est qu'une duplication d'un modèle), il est possible de connaître son état, de la gérer et de s'y connecter en mode « console », donc sans passer par le réseau :

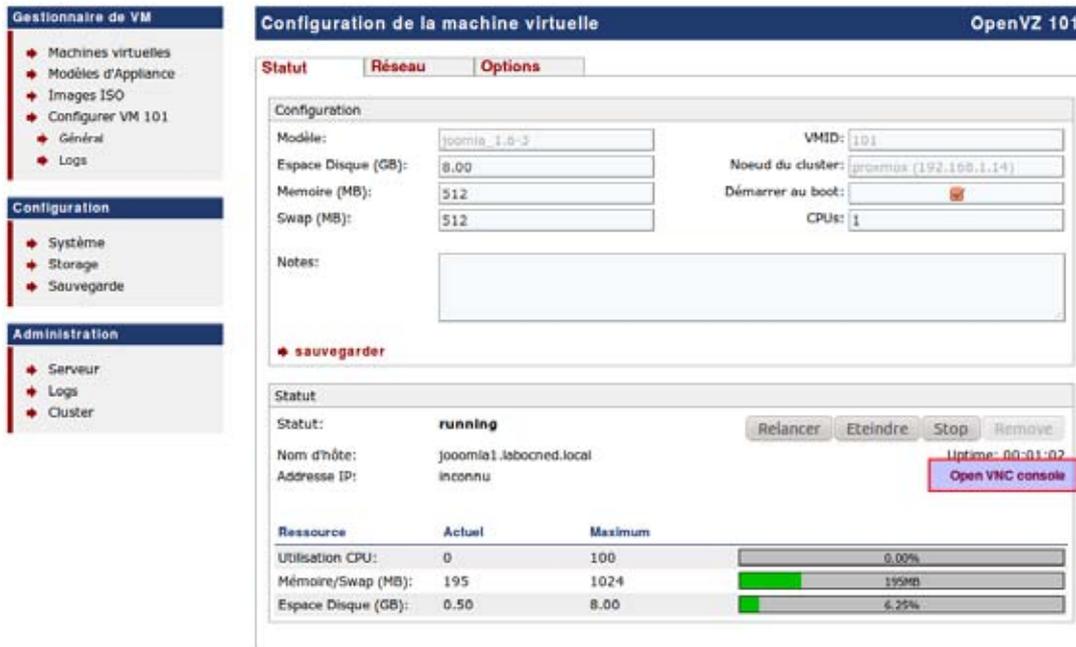


Figure 16 : état d'une machine virtuelle

Atelier 21

Virtualisation

Page 265

3B. Sauvegarde

Référence : http://pve.proxmox.com/wiki/Backup_-_Restore_-_Live_Migration

Pour définir et programmer des sauvegardes périodiques des machines, il faut créer une unité de stockage dans « Storage » :

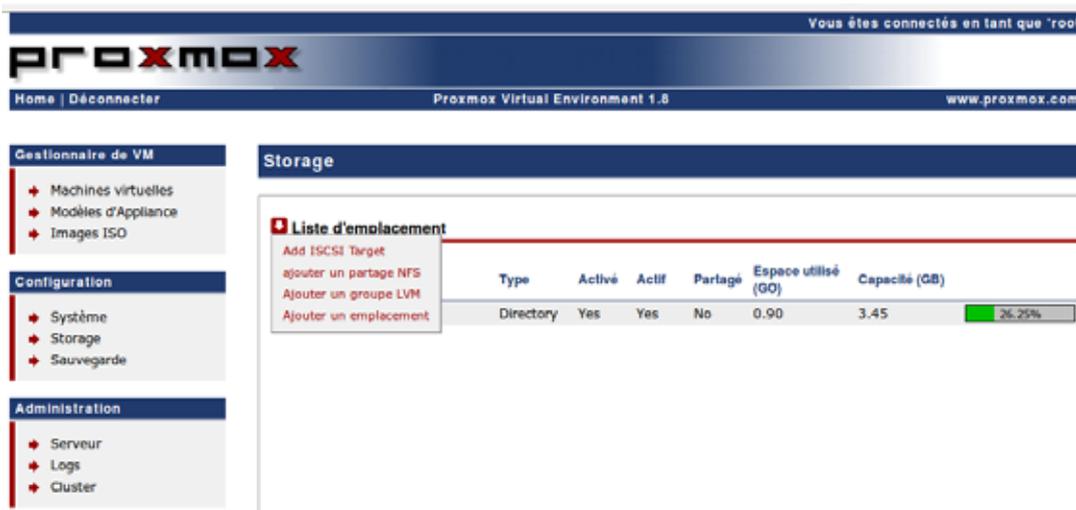


Figure 17 : Storage

4 choix sont proposés :

- add iSCSI Target : stockage sur un SAN
- NFS : partage réseau (sur notre NAS)
- un groupe LVM : disque local au serveur ou sur une unité iSCSI
- emplacement : un répertoire local

Nous choisissons donc NFS. En indiquant l'IP du NAS et en cliquant sur « scan », celui-ci retrouve automatiquement l'espace partagé que nous avons créé tout à l'heure. La liste « contenu » est très importante et sert à définir l'utilité de cette unité de stockage :

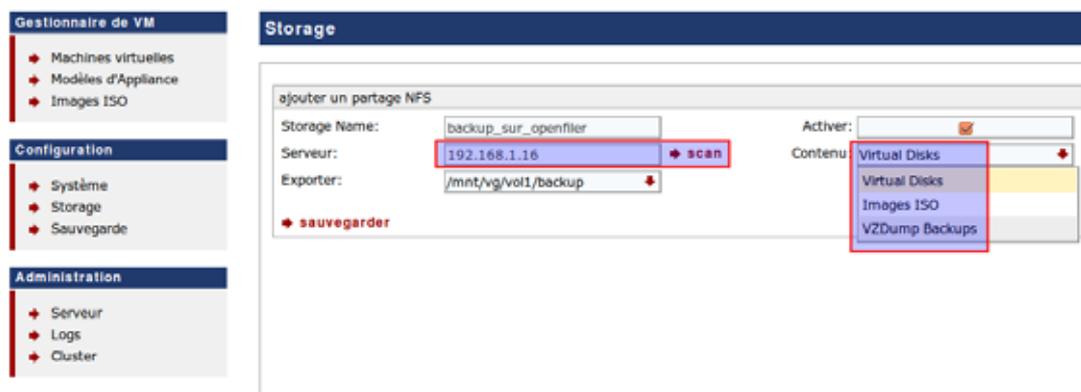


Figure 18 : propriétés de l'unité de stockage

Types de contenu :

- Virtual Disks : disques virtuels, pour des raisons de temps d'accès, ceux-ci doivent être sur la machine locale ou dans un SAN
- Images ISO : dépôt d'images ISO téléchargées sur le serveur (lieu de stockage au choix, déterminera la rapidité d'installation de la machine virtuelle)
- VZDump backups : qui dit sauvegarde, dit externalisation : donc sur un NAS ou un SAN.

Pour la suite de l'atelier, nous choisissons VZDump. Une fois enregistré, si nous allons dans la partie « sauvegarde » puis sur « créer un nouveau job » :

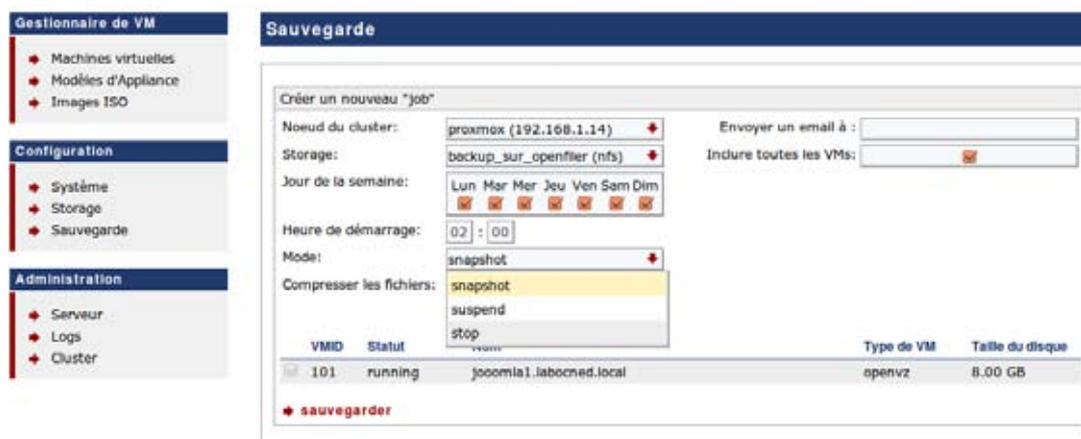


Figure 19 : création d'une tâche de sauvegarde

Cet écran présente des éléments concernant la planification et les VM à sauvegarder. Le « mode » va déterminer le temps d'indisponibilité de la VM. Le mieux est de choisir « snapshot » qui s'appuie sur LVM est sans interruption.

Dans la figure ci-dessous, on peut constater que la sauvegarde a créé un fichier tar sur le NAS. Il contient le snapshot LVM de la machine virtuelle.

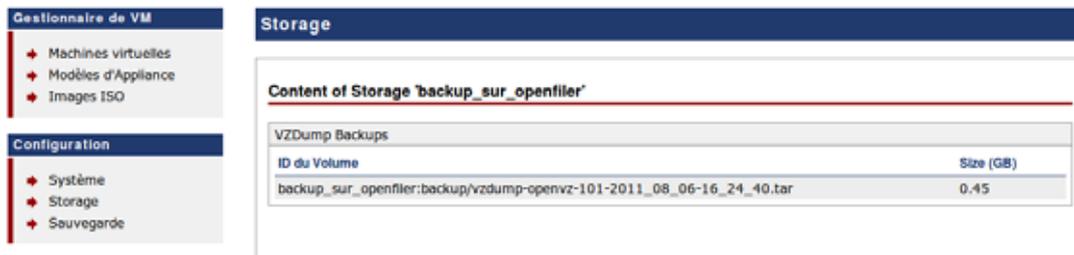


Figure 20 : Fichier de sauvegarde

Par contre, la restauration se fait en ligne de commandes...

3C. Cluster

Référence : http://pve.proxmox.com/wiki/Proxmox_VE_Cluster

Cela va consister à regrouper plusieurs serveurs physiques dans une même entité : le cluster. Ceci va nous aider à améliorer la qualité de service et la tolérance aux pannes. En cas de panne, nous pourrons restaurer relativement rapidement une sauvegarde des VMs sur un autre noeud du cluster. Il est également possible d'utiliser la fonctionnalité de migration à chaud qui permet de basculer une VM pendant son fonctionnement.

Pour réaliser cette étape de l'atelier, il faudra une deuxième installation de Proxmox sur une autre machine.

La création du cluster ne peut se faire qu'en ligne de commande. Connectez-vous dans la console Linux du serveur qui servira de maître puis exécutez la commande suivante :

```
# pveca -c
```

Cette étape crée les clés de chiffrement nécessaires aux communications SSH entre les noeuds du cluster. Une fois réalisé, vous pouvez constater l'état du cluster :

```
proxmox:~# pveca -c
cluster master successfully created
proxmox:~# pveca -l
CID----IPADDRESS----ROLE-STATE-----UPTIME---LOAD---MEM---DISK
1 : 192.168.1.14      M    A           04:09   0.11   24%   31%
proxmox:~# _
```

Maintenant, il faut faire de même sur la deuxième machine en indiquant l'adresse ip du maître du cluster :

```
#pveca -a -h 192.168.1.14
```

Ce qui donne :

```
proxmox:~# pveca -l
CID----IPADDRESS----ROLE-STATE-----UPTIME---LOAD---MEM---DISK
1 : 192.168.1.14      M    A           04:22   0.00   24%   31%
2 : 192.168.1.15      N    A           02:01   0.00   17%   31%
proxmox:~# _
```

Si vous rencontrez des erreurs du type « Ticket authentication failed - invalid ticket... », il faut s'assurer que les deux machines ont des horloges synchronisées (vérifier l'activation et le fonctionnement du service NTP).

Une fois réalisé, lorsque l'on va dans l'interface Web d'un noeud du cluster, on retrouve nos deux serveurs :

Nom d'hôte	Adresse IP	Rôle	état	Uptime	Load	CPU	IODelay	Memory	Disk
proxmox	192.168.1.14	Master	active	04:23	0.00	0%	0%	22%	31%
proxmox2	192.168.1.15	Node	active	02:01	0.05	1%	0%	16%	31%

Figure 21: état du cluster

Il devient alors possible de créer une machine virtuelle sur n'importe quel serveur ou de migrer une machine (la migration doit être lancée depuis le maître, sinon erreur « vous n'avez pas les droits d'accès en écriture ») :

Définir une tâche de migration

Noeud d'origine: proxmox (192.168.1.14) VMID: please select

Noeud de destination: proxmox2 (192.168.1.15) Migration à chaud

[migrate](#)

Figure 22: migration d'une machine virtuelle

Atelier 21

Virtualisation

Page 268

La migration donne ceci :

command finished

```

/usr/sbin/vzmigrate --online 192.168.1.15 101
Starting online migration of CT 101 to 192.168.1.15
Preparing remote node
Initializing remote quota
Syncing private
Live migrating container...
Syncing 2nd level quota
Cleanup
VM 101 migration done
    
```

Figure 22: migration d'une machine effectué

Nous avons fait le tour des principales fonctionnalités de Proxmox.

À retenir

La mise en place d'une solution de virtualisation pose le problème du stockage des machines virtuelles et de leur sauvegarde. Deux scénarii se distinguent, une solution basée sur la sauvegarde sur NAS, une autre basée sur le stockage en temps réel des machines virtuelles sur un SAN. La deuxième solution est idéale car elle permet une reprise d'activité beaucoup plus rapide en cas de problèmes sur un serveur physique mais elle est bien plus coûteuse.

Proxmox est une des solutions de virtualisation du marché informatique. Il permet de créer des machines virtuelles à partir de modèles téléchargés ou de machines vierges. En fonction des caractéristiques CPU du serveur physique, il sera possible de créer des machines virtuelles de type KVM qui supportent les systèmes d'exploitation les plus courant du marché. Sinon, il faudra utiliser une virtualisation basée sur OpenVZ qui ne supporte que Linux.

Proxmox permet de gérer les sauvegardes et permet de constituer des clusters qui assurent un bon niveau de sécurité.

Si vous voulez approfondir

Évaluer d'autres produits de virtualisation (par exemple Hyper-V intégré à Windows 2008 R2 ou VMware vSphere ESXi).

Atelier 1

Exercice 1

RAID 1 : minimum 2 disques en miroir, toute écriture est reportée sur les deux disques.

RAID 5 : minimum 3 disques, chacun contient en plus des données des codes de redondance qui permettent de régénérer les données contenues sur l'un des autres disques en cas de panne.

Un « spare disk » est un disque de rechange qui peut remplacer « à chaud » un disque en panne. Le contrôleur reconstruit le disque pendant que l'activité continue à fonctionner (il est néanmoins préférable que la reconstruction puisse se faire avec le minimum d'activité car le processus peut être long).

Exercice 2

La capacité globale sera de 300 Gio (2 disques) puisque que un disque sert de secours, il n'est donc pas compté et que le RAID 5 consomme l'équivalent d'un disque pour stocker les données de contrôle.

Atelier 2

Exercice 1

La page ci-dessous sert d'index vers la dizaine de pages qui permettent de comprendre les différences entre les versions et les installations complètes/minimales : <http://www.microsoft.com/france/serveur/windowsserver/windows-server-2008-r2/editions-WS2008R2.aspx>

Pour la partie sur les limitations matérielles :

<http://www.microsoft.com/france/serveur/windowsserver/windows-server-2008-R2/r2-comparaison-specificites-techniques.aspx>

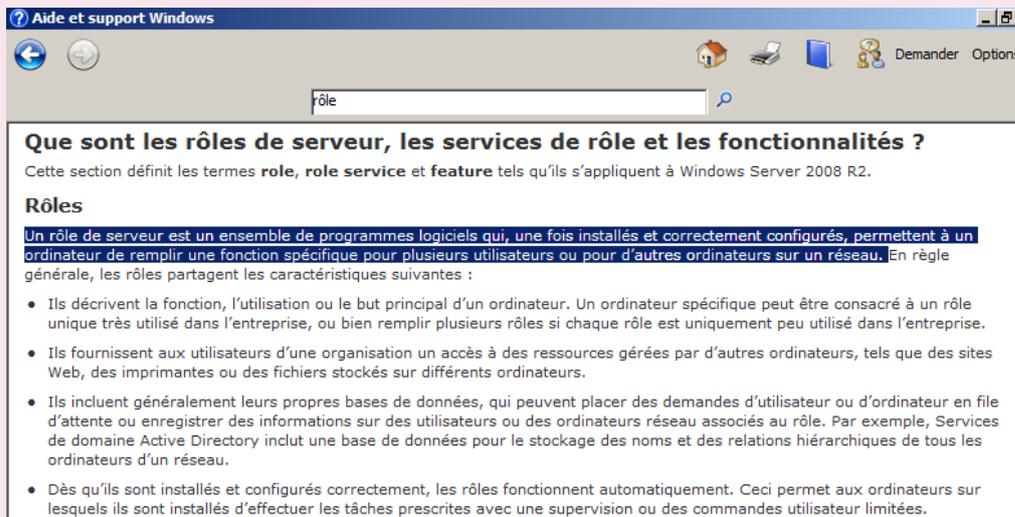
RAM maximum pour une « standard » : 32 Gio

CPU maximum pour une « datacenter » : 64 (emplacements x64)

Atelier 3

Exercice 1

À partir du menu « démarrer », vous avez un menu « aide et support » qui vous permet de faire des recherches :



Exercice 2

Nous pouvons utiliser l'aide en ligne ou Wikipedia pour définir ces termes :

Active Directory (ou AD) est la mise en œuvre par Microsoft des services d'annuaire **LDAP** pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs.

Concernant le framework .NET, il vaut mieux définir cela en deux temps :

- **framework** : un framework est un kit de composants logiciels structurels, qui servent à créer les fondations ainsi que les grandes lignes de tout ou d'une partie d'un logiciel (architecture). En programmation orientée objet un framework est typiquement composé de classes mères qui seront dérivées et étendues par héritage en fonction des besoins spécifiques à chaque logiciel qui utilise le framework.
- **.NET** : a pour but de faciliter la tâche des développeurs en proposant une approche unifiée à la conception d'applications Windows ou Web, tout en introduisant des facilités pour le développement, le déploiement et la maintenance d'applications. Il a besoin d'être installé sur la machine de l'utilisateur final.

Exercice 3

On peut le vérifier dans l'interface graphique ou dans l'interpréteur de commandes :

```
Administrateur : Invite de commandes
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : W2008
Suffixe DNS principal . . . . . : labocned.local
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS. : labocned.local

Carte Ethernet Connexion au réseau local :

Suffixe DNS propre à la connexion. . . :
Description . . . . . : Carte Intel(R) PRO/1000 MT pour station de tra
vail
Adresse physique . . . . . : 08-00-27-06-AC-E7
DHCP activé . . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::f419:f79d:facf:a171%10<préféré>
Adresse IPv4. . . . . : 192.168.1.100<préféré>
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 235405351
DUID de client DHCPv6. . . . . : 00-01-00-01-15-B4-FC-A6-08-00-27-06-AC-E7
Serveurs DNS. . . . . : :1
127.0.0.1
NetBIOS sur Tcpip. . . . . : Activé
```

Serveur DNS = 127.0.0.1 donc localhost donc moi-même : la réponse est donc oui. Vous avez remarqué que Windows a modifié tout seul ce paramètre puisque ce n'est pas ce que nous avons mis après l'installation du système...

Exercice 4

J'imagine que vous avez fait un simple ping avec un site internet pour le vérifier. On peut aussi faire un nslookup pour constater que c'est bien le serveur local qui est sollicité.

Atelier 5

Exercice 1

J'espère que vous n'avez pas répondu 127.0.0.1 ! Celle-ci reflète l'hôte local et en ce sens le serveur est une exception puisque le serveur DNS est installé sur lui. Nous mettrons donc l'adresse IP du serveur, soit 192.168.1.100.

Atelier 11

Exercice 1

Imaginons un ordinateur avec :

- un lecteur de disquette 3" 1/2 ;
- un disque dur SCSI composé de 2 partitions ;
- un disque dur maître sur le premier canal IDE et composé d'une seule partition.

Donnez-moi les noms d'unités

On aura les noms d'unités suivants :

- fd0
- sda1, sda2
- hda1

Atelier 12

Exercice 1

Positionnez-vous sur le terminal numéro 2 puis connectez-vous.

Vous appuyez simultanément sur les touches ALT + F2. Ensuite vous saisissez le nom d'un utilisateur (login) et son mot de passe (password).

Exercice 2

Revenez sur le terminal numéro 1.

Vous appuyez simultanément sur les touches ALT + F1

Exercice 3

1. Définissez le terme d'arborescence.

L'arborescence d'un système de fichiers décrit l'organisation des répertoires sur support de stockage. Cette organisation est assimilée à un arbre. Les répertoires constituant des branches et les fichiers des feuilles.

2. Définissez le terme de racine.

La racine de l'arborescence est le point de départ de l'ensemble du système de fichiers. Sous Unix, il s'agit de / (souvenez-vous de l'installation).

3. Soit l'arborescence suivante :

```
/  +-- bin
   +-- etc
   +-- home    +-- util1
   |           +-- util2 +-- rep
   +-- tmp
```

Sachant que le / représente la racine et que vous vous trouvez dans le répertoire /home/util2, donnez :

- le nom du répertoire courant : util2 (celui où je me trouve)
- le nom du répertoire parent : home (celui immédiatement au-dessus de moi : il n'y a en a qu'un)
- le nom du répertoire enfant : rep (dans ce cas, il n'y en a qu'un)
- le chemin complet de « rep » : /home/util2/rep (la suite des répertoires depuis la racine, séparés par des /).

Exercice 4

- affichez le nom complet du répertoire où vous êtes

```
usercned@mv2-debian:~$ pwd
/home/usercned
```

- créez le répertoire « repertoire_test »

```
usercned@mv2-debian:~$ mkdir repertoire_test
```

- placez-vous dans ce répertoire

```
usercned@mv2-debian:~$ cd repertoire_test
```

- placez-vous à la racine du disque

```
usercned@mv2-debian:~$ cd /
(vérification avec pwd, nous sommes bien au niveau /)
```

- revenez dans votre répertoire personnel

```
usercned@mv2-debian:~$ cd
(vérification avec pwd, nous sommes bien de retour au niveau
/home/usercned)
```

- renommez le répertoire « repertoire_test » en « ajeter »

```
usercned@mv2-debian:~$ mv repertoire_test ajeter
(vérification avec la commande ls)
```

- supprimez le répertoire « ajeter »

```
usercned@mv2-debian:~$ rmdir ajeter
(vérification avec la commande ls)
```

Exercice 5

- Affichez les numéros de lignes

```
ECHAP  
:set number
```

- Modifiez le texte précédent :
 - Remplacer malheur par bonheur

```
ECHAP  
:2s/malheur/bonheur
```

- Remplacer les pièges par les charmes

```
ECHAP  
:3s/pièges/charmes
```

- Remplacer bonheur par grand bonheur

```
ECHAP  
:2s/bonheur/grand bonheur
```

- Remplacer tous les a par des A

```
:1,$s/a/A/g
```

- Recherchez toutes les lignes commençant par un I

```
:/I
```

puis n pour poursuivre la recherche

Copiez la première ligne dans un autre fichier

Se positionner sur la première ligne, taper sur **ECHAP** puis yy pour copier la ligne

Enregistrer le fichier : **ECHAP** puis :w

Ouvrir un autre fichier :vi autrefic

Coller la ligne en tapant sur p

Exercice 6

- recherchez les différences entre les 2 fichiers

```
usercnd@mv2-debian:~$ diff test1.txt test2.txt
1c1
< j'aime bien
---
> j'aime BIEN
```

- rentrez dans le répertoire /bin

```
usercnd@mv2-debian:~$ cd /bin
```

- listez tous les fichiers du répertoire /bin

```
usercnd@mv2-debian:/bin$ ls
arch  dir    gzip    mkdir   pidof   sleep  zccat
bash  dmesg  hostname mknod   ping    sty    zcmp
```

- listez tous les fichiers de /bin qui commencent par ls

```
usercnd@mv2-debian:/bin$ ls ls*
ls  lsmod  lsmod.modutils  lspci
```

- revenez dans votre répertoire personnel

```
usercnd@mv2-debian:/bin$ cd
```

- affichez le contenu du fichier test1.txt

```
usercnd@mv2-debian:~$ cat test1.txt
j'aime bien
linux
```

- copiez le fichier test1.txt en test3.txt

```
usercnd@mv2-debian:~$ cp test1.txt test3.txt
```

- listez les fichiers

```
usercnd@mv2-debian:~$ ls
test1.txt  test2.txt  test3.txt (plus éventuellement si
vous les avez conservés monfic et reptest)
```

- affichez le contenu du fichier test2.txt

```
usercnd@mv2-debian:~$ cat test2.txt
j'aime BIEN
linux
```

- supprimez le fichier test1.txt

```
usercnd@mv2-debian:~$ rm test1.txt
```

- renommez le fichier test3.txt en test4.txt

```
usercnd@mv2-debian:~$ mv test3.txt test4.txt
```

- listez les fichiers

```
usercnd@mv2-debian:~$ ls
test2.txt  test4.txt
```

Exercice 7

- Placez-vous dans votre répertoire personnel.

```
usercncd@mv2-debian:~$ cd
```

- Listez tous les fichiers y compris les fichiers cachés.

```
usercncd@mv2-debian:~$ ls -a
.  .bash_history  .bashrc  test2.txt
.. .bash_profile  monfic   test4.txt
```

- Que représentent les fichiers « . » et « .. » ?
Le . représente le répertoire courant, les .. représentent le répertoire parent.
- Listez tous les fichiers en affichant (au moins) la date et la taille. (exemple du cours)

```
usercncd@mv2-debian:~$ ls -la
total 10
drwxr-xr-x 3 usercncd usercncd 1024 2007-04-08 17:51 .
drwxrwsr-x 4 root      staff    1024 2007-04-03 21:58 ..
-rw----- 1 usercncd usercncd  228 2007-04-08 12:01 .bash_history
-rw-r--r-- 1 usercncd usercncd  567 2007-04-03 21:58 .bash_profile
-rw-r--r-- 1 usercncd usercncd 1834 2007-04-03 21:58 .bashrc
-rw-r--r-- 1 usercncd usercncd   30 2007-04-08 11:48 monfic
```

- Affichez le contenu du fichier .bash_history. Que remarquez-vous ?

```
usercncd@mv2-debian:~$ cat .bash_history
```

Il contient les commandes que j'ai tapé pendant les sessions de travail précédente.

- Affichez tous les fichiers dont le nom commence par test.

```
usercncd@mv2-debian:~$ ls test*
test2.txt  test4.txt
```

Exercice 8

- Placez-vous dans le répertoire /home

```
usercncd@mv2-debian:~$ cd /home
```

- Listez le contenu du répertoire

```
usercncd@mv2-debian:/home$ ls
lost+found  usercncd
```

Le répertoire /home contient tous les répertoires (moi ils sont colorés en bleu...) personnels des utilisateurs du système. Ici, il y en a 2 : lost+found et usercncd

- Recherchez les fichiers dont le nom commence par test

```
usercncd@mv2-debian:/home$ find -name test*
./usercncd/test4.txt
./usercncd/test2.txt
```

- Essayez cette recherche (les fichiers que nous avons créés aujourd'hui doivent sortir).

```
usercnd@mv2-debian:/home$ find -print -ctime 2
```

Atelier 14

Exercice 1

1.

```
mv2-debian:~# more /etc/services
```

2. netstat -ltn

3. Regardez dans l'aide (*man*) et vous apprendrez qu'il suffit de remplacer les options -ltn (t=TCP) par -lun (u=UDP).

Exercice 2

Le mieux est d'utiliser apt-get remove pour enlever purement et simplement les services inutiles. Sur ma machine, je ne conserve que les services suivants (pour l'instant) :

- network : activation des interfaces réseau
- rsyslog : gestion des journaux système
- keytable : chargement des caractéristiques du clavier
- apmd : gestion de l'alimentation et de l'énergie
- cron : gestion de travaux planifiés à exécuter
- dbus : système simple de messages inter-processus
- bootlogs : enregistre un journal sur les événements lors du démarrage
- rc.local : permet d'exécuter des scripts de démarrage locaux (dans /etc/rc.local)
- anacron : gestion des travaux activés par cron mais non terminés
- atd : autre gestion de travaux planifiés à exécuter

Atelier 15

Exercice 1

Recherchez la signification des champs du fichier en tapant la commande : `man group`

Le fichier groupe a la structure suivante (les champs sont séparés par des « : ») :

- nom du groupe
- mot de passe du groupe (rarement utilisé)
- GID : le numéro identifiant le groupe

- Liste des utilisateurs constituant le groupe.

Exercice 2

Indiquez le rôle de chacune des commandes suivantes en consultant l'aide en ligne :

- `groupadd <nom_de_groupe>` : ajoute un groupe
- `groupdel <nom_de_groupe>` : supprime un groupe
- `groupmod <nom_de_groupe>` : modifie les caractéristiques d'un groupe
- `groups <nom_utilisateur>` : indique les groupes auxquels appartient l'utilisateur

Exercice 3

- Créez un groupe d'utilisateurs appelé `bts`

```
mv2-debian:/etc# groupadd bts
```

- Affichez à nouveau le contenu du fichier `/etc/group`

```
mv2-debian:/etc# cat /etc/group
...(mes 3 dernières lignes)
usercncd:x:1000:
telnetd:x:103:
bts:x:1001:
```

Le groupe `bts` a bien été créé, il s'est vu attribuer le numéro 1001.

Exercice 4

- Listez le contenu du fichier `/etc/passwd` (recherchez `man tail...`)

```
mv2-debian:/etc# tail /etc/passwd
...
usercncd:x:1000:1000:usercncd,,,:/home/usercncd:/bin/bash
```

- Recherchez la signification des champs du fichier en tapant la commande : `man 5 passwd`

Le fichier `/etc/passwd` a la structure suivante :

- nom de connexion de l'utilisateur
- mot de passe chiffré (si c'est une étoile, le compte est désactivé)
- numéro identifiant de l'utilisateur
- numéro de groupe principal
- champ inutilisé
- répertoire de connexion de l'utilisateur (son home directory)
- le programme à exécuter après la phase de connexion (en général un interpréteur de commande)

Exercice 5

Indiquez le rôle de chacune des commandes suivantes en consultant l'aide en ligne :

- `useradd <nom_utilisateur>` : ajoute un utilisateur
- `userdel <nom_utilisateur>` : supprime un utilisateur
- `usermod <nom_utilisateur>` : modifie un utilisateur
- `passwd <nom_utilisateur>` : définit un nouveau mot de passe pour l'utilisateur

Exercice 6

- Créez deux utilisateurs `util1` et `util2` (recherchez dans l'aide le paramètre à indiquer pour affecter l'utilisateur au groupe `bts`)

```
mv2-debian:/etc# useradd util1 -g bts
mv2-debian:/etc# useradd util2 -g bts
```

- Visionnez le contenu du fichier `/etc/passwd` pour contrôler la création de ces deux comptes

```
mv2-debian:/etc# tail /etc/passwd
...
util1:x:1001:1001:./home/util1:
util2:x:1002:1001:./home/util2:
```

Nos deux utilisateurs se sont vu attribuer le groupe 1001, donc `bts`. Si ce n'est pas le cas, détruisez l'utilisateur avec `userdel` puis consultez l'aide de `useradd`.

- Vérifiez que `util1` fait bien partie du groupe `bts` (utilisez la commande `groups`)

```
mv2-debian:/etc# groups util1
util1 : bts
```

- Attribuez aux deux utilisateurs un mot de passe. Pour `util1` :

```
mv2-debian:/etc# passwd util1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Tant que vous obtenez des avertissements sur le fait que le mot de passe est trop court ou issu d'un dictionnaire, vous n'avez pas trouvé un mot de passe valable (en termes de sécurité).

Exercice 7

- Faites un `who`.

```
root@mv2-linux:~# who
root      tty1          2011-08-08 13:24
```

- Quel est le sens des 4 colonnes qui apparaissent (`man who` si besoin) ?
Qui / quel terminal / jour de connexion / heure de connexion

Exercice 8

Indiquez le rôle de chacune des commandes suivantes en consultant l'aide en ligne :

`chown <nouveau_propriétaire> <nom_du_fichier>` : modifie l'utilisateur propriétaire d'un fichier.

`chgrp <nouveau_groupe> <nom_du_fichier>` : modifie le groupe propriétaire d'un fichier.

`chmod <permissions> <nom_du_fichier>` : modifie les permissions de l'utilisateur propriétaire, du groupe propriétaire ou des autres utilisateurs sur le fichier.

Exercice 9

À partir de la figure précédente, répondez aux questions concernant la ligne ci-dessous :

```
drwxr-xr-x  2 root  root  4096 mar  6 00:18 travail
```

- Ici, quel est le « mode » ? Que cela signifie-t-il ?

Le « mode » est « d », ce qui signifie directory en anglais et répertoire en français. Les fichiers « classiques » n'ont pas de mode particulier (les fichiers spéciaux en ont, mais ceci est une autre histoire).

- Qui est le propriétaire du répertoire /travail ?

C'est root (le premier sur la ligne).

- Quelles sont les permissions de l'utilisateur root sur /travail ? Que cela signifie-t-il ?

C'est le premier bloc (rwx). Cela signifie tout simple que l'utilisateur root a toutes les permissions sur ce répertoire.

- Quelles sont les permissions des membres du groupe root sur ce répertoire ? Que cela signifie-t-il ?

C'est le second bloc (r-x). Les utilisateurs membres du groupe root peuvent lire des fichiers et exécuter des scripts ou des programmes. Ils ne peuvent rien modifier puisqu'ils ne peuvent pas écrire.

- Quelles sont les permissions des autres utilisateurs (ni l'utilisateur root, ni les membres du groupe root) sur ce répertoire ? Que cela signifie-t-il ?

C'est le troisième bloc (r-x). Tous les utilisateurs non membres du groupe root peuvent lire des fichiers et exécuter des scripts ou des programmes. Ils ne peuvent rien modifier puisqu'ils ne peuvent pas écrire.

Exercice 10

Impossible à vous de jouer pour lui permettre de rentrer à nouveau (mais uniquement rentrer, donc impossibilité de créer un fichier) dans le répertoire.

Il faut attribuer la permission x aux autres utilisateurs (elle a une signification particulière car il s'agit d'un répertoire) :

```
mv2-debian:/# chmod o+x /travail
```

Vérifions :

```
util1@mv2-debian:/$ cd /travail
util1@mv2-debian:/travail$
```

Ça marche. Listons le contenu du répertoire :

```
util1@mv2-debian:/travail$ ls
ls: .: Permission non accordée
```

Impossible. La permission x me permet de rentrer dans le répertoire mais pour l'instant, je ne peux rien faire d'autre.

Exercice 11

- En tant que root, créez dans /travail un dossier que vous appellerez /travail/tplinux.

```
mv2-debian:/# mkdir /travail/tplinux
```

- Faites en sorte que seuls l'utilisateur root et les membres du groupe bts (et uniquement eux) puissent écrire à l'intérieur de tplinux.

```
mv2-debian:/travail# chgrp bts tplinux
mv2-debian:/travail# chmod g+rxw tplinux
```

- Faites en sorte que util1 soit le propriétaire du répertoire.

```
mv2-debian:/travail# chown util1 tplinux
```

Exercice 12

Util1 est propriétaire du répertoire tplinux et il possède les permissions :

```
drwxrwxr-x  2 util1    bts   4096 2007-04-12 14:52 tplinux
```

Pourtant s'il essaie de (essayez...), il obtient :

```
drwxrwxr-x  2 util1    bts   4096 fév 14 04:44 tplinux
```

Permission non accordée

Savez-vous pourquoi ? Proposez une solution pour que util1 puisse supprimer ce répertoire (aide : il faut être root pour résoudre le problème).

Il se trouve que tplinux est dans un répertoire. Lorsque l'on veut supprimer un répertoire, ce sont les permissions du répertoire parent qui s'appliquent. Observons les permissions de travail :

```
mv2-debian:/# ls -la
...
drwxr-xr-x  3 root    root   4096 2007-04-12 14 :52 travail
...
```

util1 ne fait partie du groupe root, il n'a donc que les permissions r et x sur /travail. Il n'a pas la permission w qui lui permettrait de modifier le contenu de ce répertoire. Donc, en tant que root, il suffit de rétablir cette permission :

```
mv2-debian:/# chmod o+w /travail
```

Ensuite, util1 peut détruire ce répertoire :

```
util1@mv2-debian:/travail$ rmdir tplinux
mv2-debian:/travail# ls -la
```

tplinux a disparu !

Atelier 16

Exercice 1

1. Il faut **chiffrer** le message ! C'est bien vous ne dormez pas encore !
2. Je crois que la méthode de chiffrement la plus simple que l'on puisse imaginer consiste à remplacer l'alphabet usuel par un autre alphabet, qui lui correspond régulièrement. L'exemple le plus connu est celui de l'alphabet inversé dans lequel A=Z, B=Y, C=X, ...

Exercice 2

Il faut, d'une façon ou d'une autre, transférer la clé à vos interlocuteurs. Si on l'envoie par un tiers (la poste, un courrier électronique, etc.) le risque est que la clé soit interceptée. Si on choisit de porter nous-même la clé et de la remettre en main propre. Cela devient vite complexe et coûteux lorsque les interlocuteurs sont nombreux. Et de toute façon, une fois que votre interlocuteur possède la clé, si elle existe sous une forme manuscrite par exemple, elle peut être dérobée.

Exercice 3

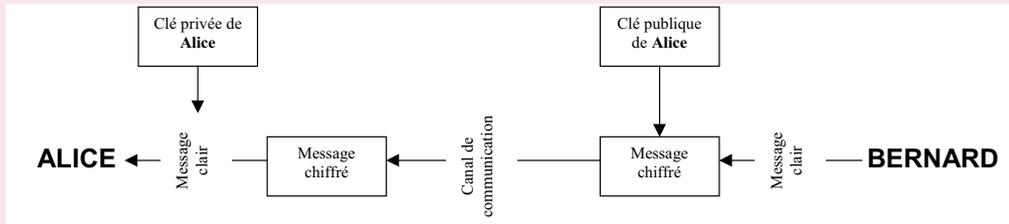
1. Qui est l'émetteur ? Alice. Qui est le destinataire ? Bernard.
2. Qui chiffre ? Alice. Avec quelle clé ? Avec une clé publique. A qui appartient cette clé ? **à Bernard.**
3. Qui déchiffre ? Bernard. Avec quelle clé ? Avec une clé privée. A qui appartient cette clé ? à Bernard.

Exercice 4

Message chiffré de Alice à Charlotte : c'est impossible tant que Charlotte n'a pas fourni sa clé publique à Alice.

Exercice 5

La condition est que Bernard possède la clé publique d'Alice. L'échange chiffré de Bernard vers Alice se déroule ainsi :



Exercice 6

Les fichiers de configuration Linux sont tous stockés dans /etc. Une recherche rapide vous aura appris qu'il existe un répertoire /etc/ssh :

```
mv2-debian: # ls -la /etc/ssh
drwxr-xr-x  2 root root  4096 nov 16 14:47 .
drwxr-xr-x 59 root root  4096 nov 16 14:47 ..
-rw-r--r--  1 root root 125749 oct  1 00:12 moduli
-rw-r--r--  1 root root  1595 oct  1 00:12 ssh_config
-rw-r--r--  1 root root  1874 nov 16 14:47 sshd_config
-rw-----  1 root root   668 nov 16 14:47 ssh_host_dsa_key
-rw-r--r--  1 root root   605 nov 16 14:47 ssh_host_dsa_key.pub
-rw-----  1 root root  1675 nov 16 14:47 ssh_host_rsa_key
-rw-r--r--  1 root root   397 nov 16 14:47 ssh_host_rsa_key.pub
```

On constate que les fichiers de clé publique (fichiers .pub) sont accessibles à tout le monde alors que les autres (fichiers de clé privée sans extension) ne sont accessibles qu'à root. En voilà une bonne chose ! Si jamais ce n'est pas le cas sur votre machine, il est impératif de remettre les choses dans l'ordre. Vous savez comment faire¹ !

Atelier 19

Exercice 1

Et le port 8005 ? Hé hé, vous êtes bien accroché à votre fauteuil ? Vous faites un telnet localhost 8005 puis vous tapez SHUTDOWN en majuscules suivi de entrée. Maintenant vous refaites netstat -plunt | grep java.

1. que constatez-vous ?

Je constate que les deux services Tomcat qui écoutaient sur les ports 8080 et 8005 sont arrêtés.

2. qu'en déduire en termes de sécurité ? En particulier, pensez-vous que cette manipulation puisse être faite au travers du réseau ?

On ne peut pas réaliser cette manipulation depuis le réseau puisque le port 8005 est limité au localhost (127.0.0.1). Par contre, n'importe quel utilisateur lambda connecté sur le serveur (en console ou en ssh) peut le faire...

¹. man chmod sinon...

Atelier 21

Exercice 1

Ces notions ont déjà été présentées dans le cours. Utilisez éventuellement Wikipedia pour vous rafraîchir la mémoire.

NAS = Network Attached Storage, pour résumer, c'est un partage réseau sur une machine. Ces partages s'appuient sur des protocoles de haut niveau (couche application sur TCP ou UDP).

SAN = Storage Area Network, comme un disque dur déporté sur une autre machine. La différence par rapport au précédent, c'est que le serveur croit que le disque est local. Met en oeuvre un protocole de très bas niveau qui est utilisé sur un réseau très rapide (parfois en fibre optique).

NFS (Network File System) : protocole de partage de fichiers au travers d'un réseau (concurrent en quelque sorte des partages Windows ou Samba basés sur le protocole SMB).

Exercice 2

Classiquement, un système basé sur du RAID. Consultez les sites de revendeurs pour voir les spécifications des boîtiers NAS. Comme toujours, dans le détail, il faut mener une étude et estimer les capacités de stockage souhaitées ainsi que le nombre d'accès concurrents qui détermineront la capacité processeur et la RAM nécessaires.

Exercice 3

En examinant le masque réseau à 255.255.255.255, on comprend que l'on a limité l'accès à une seule adresse IP : celle indiquée dans la colonne Network/Host. Ainsi, seules deux machines (.14 et .15) auront accès au partage.

Exercice 4

- Intel VT/AMD-V : comme vu dans le premier module de cours du BTS, il s'agit de technologies et d'extensions aux microprocesseurs de la famille x86 qui assistent le CPU dans la gestion des machines virtuelles. Ces technologies sont indispensables pour le mode de virtualisation KVM (mais pas utile pour OpenVZ).
- 15k rpm SAS RAID 10 : disques de technologie SAS (Serial Attached SCSI) dont les plateaux tournent à 15 000 tours par minute et groupés en RAID 10 (à la fois miroir et volumes agrégés)