



---

# Installation et supervision d'une architecture d'annuaire

---



EXIA.CESI LYON

*Auteur :*

BLOCHET TANGUY  
SACLIER BAPTISTE  
PONSARD JEAN-GUILLAUME

*Client :*

iSEC GROUP

11 décembre 2017



# Table des matières

<b>1</b>	<b>Situation</b>	<b>1</b>
1.1	Besoins techniques . . . . .	1
1.2	Organisation . . . . .	2
<b>2</b>	<b>Installation des serveurs</b>	<b>2</b>
2.1	Hyperviseur . . . . .	2
2.2	Machines virtuelles . . . . .	2
2.3	Communication inter-VMs . . . . .	3
<b>3</b>	<b>Configuration des serveurs</b>	<b>3</b>
3.1	Serveurs groupe iSEC . . . . .	3
3.1.1	Serveur principal . . . . .	3
3.1.2	Serveur réplica . . . . .	4
3.2	Serveurs groupe Telecom . . . . .	5
3.2.1	Serveur Windows Server . . . . .	5
3.3	Organisation de l'Active Directory . . . . .	5
<b>4</b>	<b>Réponse au besoin</b>	<b>5</b>
4.1	GPO . . . . .	5
4.1.1	Partage Groupe . . . . .	5
4.1.2	Partage Telecom . . . . .	6
4.1.3	Partage par service . . . . .	6
4.1.4	Imprimantes . . . . .	7
4.1.5	Répertoire personnel distant . . . . .	8
4.1.6	Sécurité mot de passe . . . . .	8
4.1.7	Exécution automatique . . . . .	9
4.1.8	Fond d'écran . . . . .	9
4.1.9	Logiciel 7Zip . . . . .	10
<b>5</b>	<b>Supervision</b>	<b>10</b>
5.1	Installation . . . . .	11
5.1.1	Serveur central . . . . .	11
5.1.2	Installation du Poller . . . . .	12
5.2	Configuration . . . . .	12
5.3	Plugins . . . . .	12
5.4	Ajout d'une commande . . . . .	12
5.5	Ajout d'un hôte . . . . .	14
5.6	Ajout d'un service . . . . .	14
5.7	Ajout d'un poller . . . . .	14
5.8	Monitoring . . . . .	15
5.8.1	Reporting . . . . .	15
5.9	Sauvegarde . . . . .	15

<b>6</b>	<b>Bilan</b>	<b>15</b>
6.1	Évolutions possibles . . . . .	15
6.2	Conclusion . . . . .	16
6.2.1	Tanguy Blochet . . . . .	16
6.2.2	Baptiste Saclier . . . . .	16
6.2.3	Jean-Guillaume Ponsard . . . . .	16

# 1 Situation

Ce projet avait pour but de nous faire réaliser une architecture d'annuaire en installant des services qui reposent sur l'Active Directory et la supervision de serveurs. L'architecture à réaliser est pour le compte du groupe iSEC dont l'organisation est schématisé dans la figure 1.

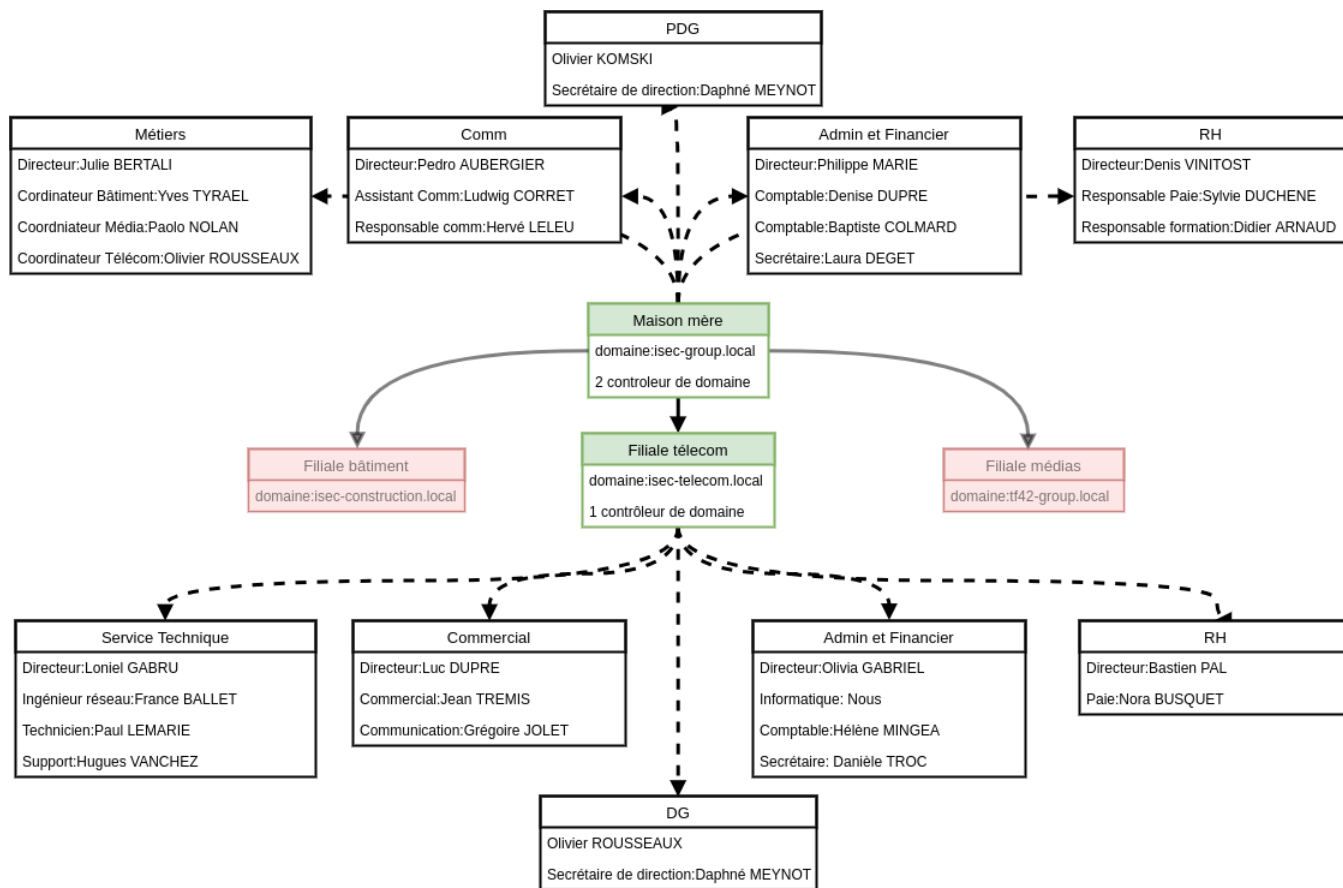


FIGURE 1 – Schéma de l'organisation de groupe iSEC.

Le groupe iSEC, qui vient de racheter une entreprise, est présent dans plusieurs secteurs d'activités et possède donc plusieurs filiales. Il souhaite connecter le réseau de la maison mère avec celle des filiales. Notre but est de mettre en œuvre l'architecture Active Directory de la maison mère et de la filiale télécom uniquement.

## 1.1 Besoins techniques

Les besoins techniques sont nombreux, mais le principal est de relier la maison mère et la filiale télécom avec un Active Directory. Le groupe iSEC doit avoir un contrôleur de domaine principal ainsi qu'un réplique pour la continuité de service. Le groupe télécom lui doit avoir un seul contrôleur de domaine. De plus une **relation d'approbation unidirectionnelle** entre les deux forêts doit être mise en place, les utilisateurs du domaine groupe peuvent accéder aux ressources du domaine de la filiale télécom mais pas l'inverse.

L'arborescence de l'Active Directory doit être créée et organisée selon les organigrammes du groupe et de sa filiale. De nombreux partages doivent ensuite être disponibles entre services, groupes et utilisateurs. D'autres service doivent être proposés par l'Active Directory comme l'installation automatique de 7Zip, la mise en place de fond d'écran et bien d'autre services qui sont décrits dans les procédures d'installation qui suivent.

## 1.2 Organisation

Ce projet a commencé le lundi 4 décembre et se termine le mardi 12 novembre. Les taches ont été découpées comme dans la figure 2 :

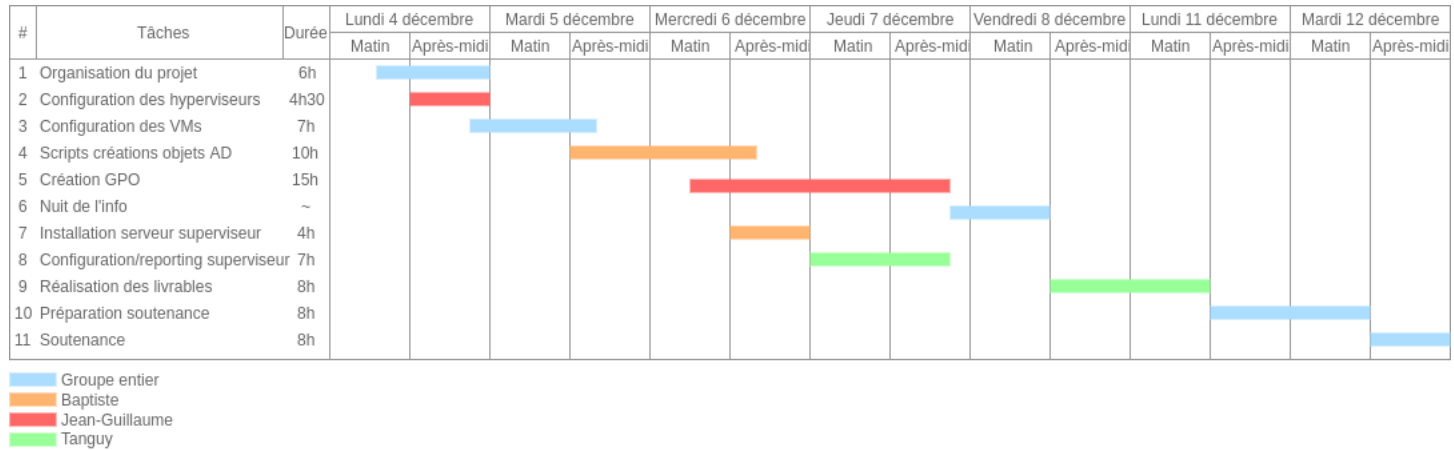


FIGURE 2 – Planning prévisionnel du projet.

Ce planning prévisionnel a été dans l'ensemble respecté, certaines heures supplémentaires ont été nécessaires pour la configuration des serveurs de supervision. Un dépôt Github a été créé afin de conserver les différents scripts utilisés pendant ce projet ainsi que les sources de ce rapport, il est disponible à ce lien : <https://github.com/Exia-epickiwi/Projet-iSEC>

## 2 Installation des serveurs

### 2.1 Hyperviseur

Etant donné la configuration matérielle disponible, nous avons décidé d'installer un hyperviseur de type 1 sur nos serveurs physiques. Cette solution est la plus performante pour notre environnement car l'hyperviseur est directement au niveau de la couche matériel. Nous avons choisi d'utiliser VMware ESXi car c'est un hyperviseur de type 1 rapide, fiable et performant. Il dispose également d'un logiciel de gestion vSphere pour utiliser l'hyperviseur avec une interface graphique. De plus, par défaut, VMware permet d'utiliser les VM en mode pont avec un switch virtuel pour être relié directement au réseau local.

### 2.2 Machines virtuelles

Il faut créer une machine virtuelle en spécifiant les options voulues comme le disque dur, la mémoire vive, les processeurs, la carte réseau. Ensuite, il faut télécharger l'ISO d'installation sur le

serveur pour que celle-ci soit utilisable par la VM. Puis, il faut insérer l'ISO dans la VM et lancer la VM, l'installation du système d'exploitation se fait de la même façon qu'avec un PC.

## 2.3 Communication inter-VMs

Pour la communication entre les VM, nous avons mis en place un réseau physique entre deux serveurs exécutant l'hyperviseur de type 1.

Ce réseau est un réseau local standard composé de deux serveurs, un switch et des postes de chaque technicien d'infrastructure. ESXi dispose d'un système de switch virtuel permettant de former un pont entre les machines virtuelles et le réseau physique. Ainsi, chaque machine virtuelle est directement connectée au réseau.

Pour le bon fonctionnement ce de réseau, un DHCP est installé sur le serveur de base du groupe distribuant les adresses IP et ayant enregistré les adresses statiques des serveurs.

Pour disposer d'un accès à internet, nous avons mis en place un routeur NAT sur une machine Arch Linux à l'aide d'IP tables. Il suffit de configurer le système pour qu'il autorise le transfert de paquet puis configurer le pare-feu interne du système en ajoutant les règles suivantes permettant de transmettre les paquets. L'adresse de la machine NAT est alors donnée dans le DHCP pour que chaque machine aie accès au réseau externe.

Listing 1 – Commandes iptables permettant l'installation d'un NAT

```
1 iptables -t nat -A POSTROUTING -o interface-externe -j MASQUERADE
2 iptables -A FORWARD -i interface-interne -o interface-externe -m
   state --state RELATED,ESTABLISHED -j ACCEPT
3 iptables -A FORWARD -i interface-interne -o interface-externe -j
   ACCEPT
```

## 3 Configuration des serveurs

Afin de configurer un domaine Active Directory au sein d'un réseau Windows sur un serveur Windows Server 2012 R2, il faut suivre les étapes suivantes :

1. L'installation de fonctionnalités sous Windows Server se fait par l'installation de rôles : dans le tableau de bord du gestionnaire de serveur Windows Server 2012, il faut cliquer sur **Gérer** puis **Ajoutez des rôles et fonctionnalités**.
2. Ensuite, il faut cliquer sur **Suivant** puis sélectionner **Installation basée sur un rôle ou une fonctionnalité**, ensuite il faut sélectionner le **Pool de serveur** (nous sélectionnons notre serveur) puis cliquer sur **Suivant**. Il est alors possible de sélectionner les rôles à installer.

### 3.1 Serveurs groupe iSEC

#### 3.1.1 Serveur principal

**Installer le rôle AD DS** Ce rôle permet d'installer l'Active Directory : Annuaire Microsoft permettant de regrouper toutes les informations du réseau.

1. Dans la fenêtre de sélection des rôles, Sélectionner le rôle AD DS. Le fait de sélectionner ce rôle installe automatiquement le rôle DNS (indispensable pour le bon fonctionnement de l'Active Directory).
2. Ensuite, il faut valider jusqu'à l'installation et cliquer sur **Installer**. Il est recommandé d'attribuer une adresse IP fixe au serveur avant d'installer le rôle. De plus ceci sera utile par la suite pour configurer le DHCP.

### Configurer le rôle AD DS

1. Une fois le rôle installé, dans le tableau de bord du gestionnaire de serveur, il faut cliquer sur **Promouvoir le serveur en tant que contrôleur de domaine**. Une fenêtre s'ouvre et demande les actions à effectuer. Il faut sélectionner **Ajouter une nouvelle forêt** et entre le nom de celle-ci : **isec-group.local** puis cliquer sur **Suivant**.
2. Ensuite, il faut renseigner un mot de passe du mode de restauration des services d'annuaire et cliquer sur « Suivant » puis **Suivant** jusqu'à arriver à l'installation. Ensuite, cliquer sur **Installer**. Le serveur redémarrera automatiquement à la fin de cette opération. L'Active Directory est désormais fonctionnel.

### Installer le rôle DHCP

1. Vous devez attribuer une adresse IP statique au serveur avant d'installer le DHCP.
2. Ensuite, il faut sélectionner **Serveur DHCP** dans le menu d'installation des rôles et fonctionnalités et cliquer sur **Suivant** jusqu'à arriver au menu d'installation où il faut cliquer sur **Installer**. Avant de cliquer sur **Fermer**, il faut cliquer sur **Terminer la configuration DHCP** et valider les deux étapes.

### Configurer le DHCP

1. Une fois l'installation terminée, il faut ouvrir le gestionnaire DHCP qui se trouve dans l'onglet **Outils** du gestionnaire de serveur. Il faut faire un clic droit sur IPv4 et ouvrir **nouvelle étendue**. Un assistant de création de la nouvelle étendue s'affiche. Il demande de nommer l'étendue (vous pouvez mettre le nom de votre choix) et de mettre une description (facultative).
2. Ensuite, il faut rentrer l'adresse IP de début et de fin de la plage d'adressage disponible pour les ordinateurs de l'AD. La section **Paramètres de configuration qui se propagent au client DHCP** se remplit automatiquement. Il est ensuite possible d'exclure une plage d'adresse IP si nécessaire. Ensuite, il faut définir la durée du bail des adresses. Ensuite, il est demandé d'indiquer la passerelle par défaut (routeur du réseau), puis le serveur DNS (les options sont automatiquement remplies car le DNS est sur le serveur en question). Il suffit ensuite de cliquer sur **Suivant** jusqu'à arriver à la fin de l'assistant. Le serveur DHCP est maintenant fonctionnel.

#### 3.1.2 Serveur réplica

L'installation du rôle s'effectue de la même manière que pour le serveur ISEC-GROUP-MASTER. Seule la configuration diffère : Lors de la promotion du serveur en tant que contrôleur de domaine, il faut sélectionner **Ajouter ce contrôleur de domaine à un domaine existant** et spécifier le



domaine en question. Il faut ensuite entrer le mot de passe DSRM puis cliquer sur **Suivant**. Ensuite, il faut vérifier que le serveur ISEC-GROUP-MASTER soit sélectionné en tant que source de réplication puis cliquer sur **Suivant** jusqu'à arriver à l'installation. Une fois le redémarrage terminé, le réplica est fonctionnel et il est possible d'accéder aux informations de l'Active Directory.

## 3.2 Serveurs groupe Telecom

### 3.2.1 Serveur Windows Server

L'installation et la configuration de ce serveur est quasi identique à celle de ISEC-GROUP-MASTER à l'exception que le nom de domaine est différent. Il ne faut également pas installer de DHCP car ISEC-GROUP-MASTER dispose déjà d'un DHCP.

## 3.3 Organisation de l'Active Directory

Nous avons remplis l'Active Directory selon les organigrammes fournis dans le sujet du projet.

Chaque groupe à son propre **domaine** à son nom

Chaque groupe (isec et télécom) à une **Unité d'Organisation** à son nom

Chaque service à une **Unité d'Organisation** à son nom

Chaque service à un **groupe de sécurité** à son nom

Chaque poste de l'entreprise (ex : Secrétariat) à un **groupe de sécurité** à son nom

Enfin chaque **utilisateurs** est ajouté dans le **groupe** qui correspond à son poste.

Ce choix d'arborescence a été fait pour faciliter le déploiement des GPOs qui sont différentes d'un service à l'autre et sont donc appliquées à l'UO qui correspond au service. Des groupes de sécurité ont été créés par service car ils sont nécessaires pour le partage de dossier.

Toute l'arborescence de l'Active Directory est créée grâce à un **script powershell**, qui va lire des fichiers **.csv** dans lequel les différents services de l'entreprise ont été ajoutés ainsi que les utilisateurs et leur poste respectif. Ce script va s'occuper de créer les différentes Unités d'Organisation et leur hiérarchie entre elles. Il va créer les groupes pour les services et les postes dans les Unités d'Organisations correspondantes. Il va enfin créer les utilisateurs et les ajouter aux groupes correspondants à leur poste. Ce script va en plus créer les dossiers de partages par services nécessaires au partage. Ce script facilite grandement le déploiement dans l'Active Directory des utilisateurs ainsi que de nouveaux arrivants. Les différents scripts sont disponibles au lien suivant : <https://github.com/Exia-epickiwi/Projet-iSEC/tree/master/Scripts>.

## 4 Réponse au besoin

### 4.1 GPO

#### 4.1.1 Partage Groupe

Ce partage est disponible pour tous les services du groupe iSEC et se trouve sur le contrôleur de domaine principal. Il est ajouté comme lecteur réseau sur le poste de travail avec la lettre **G** : comme

*Groupe.* Pour créer ce partage sur le contrôleur de domaine maître, il faut suivre les procédures suivantes :

1. Créer le dossier qui sera partagé : sur le contrôleur de domaine ce dossier se trouve dans `C:\Shares\` sous le nom de **Groupe**, comme tous les dossiers partagés.
2. Il faut ensuite partager le dossier :
  - (a) Cliquer droit sur le dossier partagé
  - (b) Cliquer sur propriétés
  - (c) Dans l'onglet **Partage**, cliquer sur le bouton **Partager...**
  - (d) Dans la glissière, sélectionner **Rechercher des personnes...**
  - (e) Ajouter le nom du groupe dans le champ de texte, pour ajouter les utilisateurs du domaine, taper **Utilisateurs du domaine** et cliquer sur le bouton **OK**.
  - (f) Sélectionner le **Niveau d'autorisation**, sur **Lecture/écriture** pour les **Utilisateurs du domaine** et cliquer sur **Partager**.
  - (g) (Facultatif) Toujours dans l'onglet **Partage** cliquer sur **Partage avancé....**
  - (h) Cocher la case **Partager ce dossier** et cliquer sur **OK**.
3. Dans le **Gestionnaire de serveur**, ouvrir le **Gestionnaire de stratégie de groupe**
4. Dans l'UO créée précédemment **isec-group**, cliquer droit et cliquer sur **Créer un objet GPO dans ce domaine, et le lier ici....** Nommer la.
5. Cliquer droit sur la GPO créée et cliquer sur **Modifier**.
6. Dans **Configuration utilisateur**, **Préférences**, **Paramètres Windows** cliquer droit sur **Mappages de lecteurs** et cliquer sur **Nouveau** et **Lecteur mappé**.
7. Dans l'onglet **Général** ajouter l'emplacement `\\GROUP-WSERVER-M\Groupe`, cocher la case **Reconnecter**, libeller le en tant que **Groupe**, et utiliser la lettre **G:** dans **Lettre de lecteur**. Dans **Masquer/Afficher ce lecteur** cocher la case **Afficher ce lecteur** et cocher la case **Afficher tous les lecteurs** dans **Masquer/Afficher tous les lecteurs**.
8. Dans l'onglet **Commun**, cocher **Arrêter le traitement des éléments de cette extension si une erreur survient**, **Exécuter dans le contexte de sécurité de l'utilisateur connecté** et **Supprimer l'élément lorsqu'il n'est plus appliqué**.
9. Cliquer enfin sur **OK** et cliquer droit sur la GPO et cliquer sur **Appliqué**.

#### **4.1.2 Partage Telecom**

Le partage Telecom se fait de la même façon que dans le paragraphe 4.1.1, Partage Groupe. La configuration se fait sur le serveur de la filiale Télécom. Il suffit d'ajuster les noms pour qu'ils correspondent au partage Télécom.

#### **4.1.3 Partage par service**

Le partage par service met à disposition un répertoire partagé sous forme de lecteur mappé avec la lettre **S:** comme Share. Chaque répertoire n'est visible que par le service qui lui est propre, sauf le service direction qui voit tous les dossiers de services partagés. Répétez les procédures suivantes pour chaque dossier partagé à mettre en place :

1. Créer le dossier qui sera partagé : sur le contrôleur de domaine ce dossier se trouve dans `C:\Shares\Services\` sous le nom correspondant au service du dossier partagé.
2. Il faut ensuite partager le dossier :
  - (a) Cliquer droit sur le dossier partagé
  - (b) Cliquer sur propriétés
  - (c) Dans l'onglet **Partage**, cliquez sur le bouton **Partager...**
  - (d) Dans la glissière, sélectionner **Rechercher des personnes...**
  - (e) Ajouter le nom du groupe dans le champ de texte, taper le nom de l'UO correspondant au service (ex :service-rh pour le service Ressource humaines) et cliquer sur le bouton **OK**.
  - (f) Sélectionner le **Niveau d'autorisation**, sur **Lecture/écriture** pour le groupe ajouté précédemment et cliquer sur **Partager**.
  - (g) Faites de même pour l'UO correspondant au service direction pour qu'il ai accès à tous les dossiers partagés.
  - (h) (Facultatif) Toujours dans l'onglet **Partage** cliquer sur **Partage avancé....**
  - (i) Cocher la case **Partager ce dossier** et cliquer sur **OK**.
  - (j) Récupérer le nom du partage dans l'onglet **Partage** en dessous de chemin réseau, il sera utile pour la suite.
3. Dans le **Gestionnaire de serveur**, ouvrir le **Gestionnaire de stratégie de groupe**
4. Dans l'UO du service, cliquer droit et cliquer sur **Créer un objet GPO dans ce domaine, et le lier ici....** Nommer la.
5. Cliquer droit sur la GPO créée et cliquer sur **Modifier**.
6. Dans **Configuration utilisateur, Préférences, Paramètres Windows** cliquer droit sur **Mappages de lecteurs** et cliquer sur **Nouveau et Lecteur mappé**.
7. Dans l'onglet **Général** ajouter l'emplacement avec le nom du partage récupéré précédemment, `\\GROUP-WSERVER-M\Nom_de_votre_partage`, cocher la case **Reconnecter**, libeller le en tant que **Groupe**, et utiliser la lettre **G** : dans **Lettre de lecteur**. Dans **Masquer/Afficher ce lecteur** cocher la case **Afficher ce lecteur** et cocher la case **Afficher tous les lecteurs** dans **Masquer/Afficher tous les lecteurs**.
8. Dans l'onglet **Commun**, cocher **Arrêter le traitement des éléments de cette extension si une erreur survient**, **Exécuter dans le contexte de sécurité de l'utilisateur connecté** et **Supprimer l'élément lorsqu'il n'est plus appliqué**.
9. Cliquer enfin sur **OK** et cliquer droit sur la GPO et cliquer sur **Appliqué**.

#### 4.1.4 Imprimantes

PDFCreator a été installé sur le serveur principal et va simuler une imprimante distante pour tous les utilisateurs. Pour ce faire suivez les procédures suivantes :

1. Installation de PDFCreator sur le serveur, une fois installé, modifier les propriétés de sauvegarde pour enregistrer les PDF dans le dossier souhaité et sous le nom souhaité.
2. Ouvrir le gestionnaire de périphériques et imprimantes, cliquer sur l'imprimante PDFCreator et cocher la case **Partagé cette imprimante** dans l'onglet **Partage**.

3. Dans l'onglet **Partage**, récupérer le chemin de partage qui sera utile plus tard.
4. Dans le **Gestionnaire de serveur**, ouvrir le **Gestionnaire de stratégie de groupe**
5. Dans l'UO du groupe, cliquer droit et cliquer sur **Créer un objet GPO dans ce domaine**, et le lier ici.... Nommer la.
6. Cliquer droit sur la GPO créée et cliquer sur **Modifier**.
7. Dans **Configuration utilisateur**, **Préférences**, **Paramètres du Panneau de configuration** et cliquer droit sur **Imprimantes** et cliquer sur **Imprimante** et **Imprimante partagée**.
8. Ajouter le chemin de partage récupéré précédemment dans **Chemin de partage**, et cocher la case **Définir en tant qu'imprimante par défaut**.
9. Dans l'onglet **Commun**, cocher les 3 premières cases.
10. N'oublier pas d'activer la GPO en cliquant droit dessus et cliquer sur **Appliqué**.

#### 4.1.5 Répertoire personnel distant

Chaque utilisateur du domaine a son répertoire personnel **Mes documents** déplacé sur le contrôleur de domaine principal. Dans un dossier **Home**, les différents utilisateurs ont un dossier à leur nom qui contient leurs documents. Pour reproduire cette configuration, suivez les procédures suivantes :

1. Il faut configurer le partage sur le dossier contenant dossiers document des utilisateurs. Créer le dossier et cliquer droit dessus et cliquer sur **Propriétés**.
2. Dans l'onglet **Partage**, cliquez sur le bouton **Partager...** et partager le pour tout le monde en lecture et écriture.
3. Toujours dans l'onglet **Partage** cliquer sur **Partage avancé...**
4. Cocher la case **Partager ce dossier** et cliquer sur **OK**.
5. Dans le **Gestionnaire de serveur**, ouvrir le **Gestionnaire de stratégie de groupe**
6. Dans l'UO du groupe, cliquer droit et cliquer sur **Créer un objet GPO dans ce domaine**, et le lier ici.... Nommer la.
7. Cliquer droit sur la GPO créée et cliquer sur **Modifier**.
8. Dans **Configuration utilisateur**, **Paramètres Windows**, **Redirection de dossiers**, cliquer droit ensuite sur **Documents** dans la liste de droite et cliquer sur **Propriétés**.
9. Dans **Emplacement du dossier cible**, sélectionner **Créer un dossier pour chaque utilisateur sous le chemin d'accès racine**. Ajouter le chemin d'accès **\\GROUP-WSERVER-M\Home**
10. Dans l'onglet **Paramètres**, cocher la case **Accorder à l'utilisateur des droits exclusifs sur Documents** et **Déplacer le contenu de Documents vers le nouvel emplacement** ainsi que **Conserver le dossier dans le nouvel emplacement**.
11. N'oublier pas d'activer la GPO en cliquant droit dessus et cliquer sur **Appliqué**.

#### 4.1.6 Sécurité mot de passe

Les mots de passe sont renouvelés tous les 90 jours et font 8 caractères minimum. Il n'y a pas de complexité forte définie, mais un mauvais mot de passe entré 3 fois de suite verrouille le compte utilisateur. Pour mettre en place cette sécurité de groupe, suivez les procédures suivantes :

1. Déplacer la GPO Default Domain Policy (elle se trouve dans Objets de stratégie de groupe dans la forêt isec-group.local pour le groupe iSEC ou isec-telecom.local. Cliquer droit dessus et Modifier
2. Dans l'arborescence cliquez sur Configuration ordinateur, Stratégies, Paramètres Windows, Paramètres de sécurité et Stratégie de mot de passe.
3. Cliquer droit sur Durée de vie maximale du mot de passe et cliquer sur Propriétés. Cocher la case Définir ce paramètre de stratégie et définir l'expiration sur 90 jours.
4. Cliquer droit sur Le mot de passe doit respecter des exigences de complexité et cliquer sur Propriétés. Cocher la case Définir ce paramètre de stratégie et cocher la case Désactivé.
5. Cliquer droit sur Longueur minimale du mot de passe et cliquer sur Propriétés. Cocher la case Définir ce paramètre de stratégie et définir le minimum sur 8 caractères.
6. Dans l'arborescence cliquer sur Stratégie de verrouillage du compte
7. Cliquer droit sur Seuil de verrouillage du compte et cliquer sur Propriétés. Cocher la case Définir ce paramètre de stratégie et définir le nombre de tentative sur 3.
8. N'oublier pas d'activer la GPO en cliquant droit dessus et cliquer sur Appliqué.

#### 4.1.7 Exécution automatique

Pour des raisons de sécurité l'exécution automatique (AutoRun) sur les périphériques amovibles est désactivé. Suivez les procédures suivantes pour l'appliquer :

1. Comme pour les mots de passe il va falloir modifier la GPO Default Domain Policy, cliquer droit dessus et cliquer sur Modifier.
2. Dans Configuration ordinateur, Stratégies, Modèles d'administration, Composants Windows et cliquer sur Stratégies d'exécution automatique.
3. Cliquer droit sur Désactiver l'exécution automatique et cliquer sur Modifier.
4. Cocher la case Activé, et dans Options dans la liste déroulante sélectionner Lecteurs de CD-ROM et supports amovibles. Cliquer sur OK.
5. Ne pas oublier d'activer la GPO en cliquant droit dessus et cliquer sur Appliqué.

#### 4.1.8 Fond d'écran

Chaque groupe à un fond d'écran qui lui est propre, mais aussi chaque service. Un fond d'écran par service et par groupe a été créé et appliqué sur les UO de chaque service. Pour ce faire, répétez les procédures suivantes pour chaque UO de chaque service et sur les deux groupes :

1. Il faut configurer le partage sur le dossier contenant les papiers peints. Créer le dossier et cliquer droit dessus et cliquer sur Propriétés.
2. Dans l'onglet Partage, cliquez sur le bouton Partager...
3. Dans la glissière, sélectionner Rechercher des personnes...
4. Ajouter le nom du groupe dans le champ de texte et cliquer sur le bouton OK.
5. Sélectionner le Niveau d'autorisation, sur Lecture/écriture pour le groupe précédemment créé et cliquer sur Partager.
6. (Facultatif) Toujours dans l'onglet Partage cliquer sur Partage avancé....

7. Cocher la case **Partager ce dossier** et cliquer sur **OK**.
8. Cliquer droit sur l'UO et cliquer sur **Créer un objet GPO dans ce domaine**, et le lier ici.... Nommer la.
9. Cliquer droit sur la GPO précédemment créée et cliquer sur **Modifier**.
10. Dans **Configuration utilisateur, Stratégies, Modèles d'administration, Bureau**, et cliquer sur **Bureau**. Cliquer droit sur **Papier peint du Bureau** et cliquer sur **Modifier**.
11. Cocher la case **Activé**
12. Dans **Nom du papier peint**, ajouter le nom du partage, suivi du nom du fichier JPG (ex : \\GROUP-WSERVER-M\\Wallpappers\\Servicerh.jpg). Dans le **style du papier peint**, sélectionner **Ajuster**.
13. Ne pas oublier d'activer la GPO en cliquant droit sur la GPO créée et cliquer sur **Appliqué**.

#### 4.1.9 Logiciel 7Zip

Tous les postes ont le logiciel de compression/décompression 7Zip installé sur leur poste. Pour reproduire cette configuration suivez les procédures suivantes :

1. Il faut configurer le partage sur le dossier contenant les fichiers d'installation. Créer le dossier et cliquer droit dessus et cliquer sur **Propriétés**.
2. Dans l'onglet **Partage**, cliquez sur le bouton **Partager...**
3. Ajouter le nom du groupe dans le champ de texte, taper **Utilisateurs du domaine** et cliquer sur le bouton **OK**.
4. Sélectionner le **Niveau d'autorisation**, sur **Lecture/écriture** pour le groupe ajouté précédemment et cliquer sur **Partager**.
5. (Facultatif) Toujours dans l'onglet **Partage** cliquer sur **Partage avancé....**
6. Cocher la case **Partager ce dossier** et cliquer sur **OK**.
7. Dans le **Gestionnaire de serveur**, ouvrir le **Gestionnaire de stratégie de groupe**
8. Dans la forêt, cliquer droit et cliquer sur **Créer un objet GPO dans ce domaine**, et le lier ici.... Nommer la.
9. Cliquer droit sur la GPO créée et cliquer sur **Modifier**.
10. Dans **Configuration ordinateur, Stratégie, Paramètres du logiciel** cliquer droit sur **Installation de logiciel** et cliquer sur **Nouveau et Package**.
11. Sélectionner le fichier .msi installateur de 7Zip et cocher la case **Attribué** pour le type de déploiement.
12. Ne pas oublier d'activer la GPO en cliquant droit sur la GPO et cliquer sur **Appliqué**.

## 5 Supervision

La supervision d'une infrastructure informatique consiste à vérifier à interval régulier la bonne santé des zones critiques pour en assurer la disponibilité. La supervision est un enjeux majeur d'une bonne infrastructure car elle permet d'être averti d'une panne des qu'elle se produit pour agir le plus rapidement possible.

Dans notre infrastructure composée de 2 serveurs et 5 machines virtuelle, nous avons choisi centreon comme superviseur. Centreon est un système tout-en-un permettant de vérifier, à l'aide du protocole SNMP, la bonne santé des équipements. Nous l'avons choisis pour sa facilité d'utilisation et pour sa propriété décentralisé.

Centreon met à disposition une architecture décentralisée permettant de gérer un grand parc de machines. Cette architecture est composée d'un serveur dit *central* qui stock les données et dispose d'une interface d'administration web. On trouve ensuite des serveurs dits *Pollers* en charge de collecter les données des serveurs au travers de *plugins*.

## 5.1 Installation

### 5.1.1 Serveur central

Nous avons installé Centreon sur une nouvelle machine virtuelle. L'installation dispose alors de son propre serveur ce qui nous a permis d'utiliser le disque d'installation de base de Centreon. La procédure d'installation s'effectue comme suit :

1. Envoyer l'image ISO de centreon sur la machine ESXI
2. Démarrer la machine virtuelle puis démarrer l'installation en choisissant le premier élément
3. Suivre les étapes de l'installation en suivant les instructions suivantes
  - Choisir la langue Française
  - Prendre l'ensemble de l'espace disponible sur le disque virtuel
  - Configurer le mot de passe root ; Nous l'avons définis sur **Cesi2017!**
  - Configurer le nom d'hôte ; Nous l'avons définis sur **Centreon-master**
4. Lors de la demande du type de serveur à installer, on choisit **Central server with database** pour disposer d'une base de données et de l'interface web
5. Retirer l'image de la machine virtuelle
6. Redémarrer le système

L'installation faite, il suffit de se rendre, avec un navigateur, sur l'adresse du serveur Centreon pour poursuivre l'installation en ligne.

1. Se connecter en SSH au serveur Centreon
2. Configurer le fuseau horaire PHP
  - Dans le fichier `/etc/php.ini`
  - Ligne 946
  - Décommenter la ligne `date.timezone =`
  - Donner la valeur `date.timezone = Europe/Paris`
3. Redémarrer apache avec `service httpd restart`
4. Retourner dans l'installation web
5. On laissera les valeurs de chemins par défaut
6. Configurer l'utilisateur administrateur, nous utiliserons ici les données de connexion suivantes

**Login** admin

**Password** dcfvgbhn

**First Name** Tanguy

**Last Name Blochet**

**email** tanguy.blochet@viacesi.fr

7. Configurer le mot de passe de la base de données centreon ; nous utiliserons **root**
8. L'installation se poursuit avec la mise en place de la base de données

Après ces étapes, l'installation est complète et centreon pleinement fonctionnel

### 5.1.2 Installation du Poller

L'installation du poller s'effectue comme une installation du central. Mais lors du choix du type de serveur à installer, il faut choisir **Poller server**. De plus il n'y a pas d'installation Web à effectuer.

## 5.2 Configuration

### 5.3 Plugins

Les plugins sont la base de la supervision, ils sont fournis par Centreon et se composent de multiples commandes linux permettant de faire des requêtes normalisés pour contrôler la santé de l'infrastructure.

1. Sur la page *Administration > Extensions*
2. Activer l'extension **centreon-license-manager** et **centreon-pp-manager**.
3. Sur la page *Configuration > Plugin Pack*
4. Installer les plugins **base-generic**, **Linux** et **Windows**

Ces plugins composent la base du fonctionnement de Centreon. Ils donnent une base de commandes permettant de vérifier les systèmes sous différents angles.

### 5.4 Ajout d'une commande

Une commande est une référence, dans centreon, d'un programme présent sur le serveur permettant de vérifier la bonne santé d'une machine.

Ces commandes utilisent les plugins centreon ou nagios interne ou installés à l'aide de plugins.

1. Aller dans la section *Configuration > Commands*
2. Ajouter une commande
3. Donner un nom à la commande
4. Donner le corps de la commande qui sera exécuté dans l'environnement du poller

Il est possible d'ajouter des arguments dans le corps de la commande en utilisant la syntaxe **\$ARG1\$**. On peut alors donner une description des arguments dans la section *Argument Descriptions*.

Ces arguments seront demandés lors de l'utilisation de la commande et ils sont très utiles pour définir des seuils ou des valeurs relatives.

De plus, certains arguments sont prédéfinis et relatifs à l'hôte ou au service. On les retrouve dans la zone à droite du corps de la commande lors de l'édition de celle-ci.



Commande	Description
centreon_linux_snmp.pl -plugin=os : :linux : :snmp : :plugin -mode=cpu	Permet le monitoring de la valeur du CPU sur les machines Linux
centreon_linux_snmp.pl -plugin=os : :linux : :snmp : :plugin -mode=storage	Permet le monitoring du remplissage des disques sur les machines Linux
centreon_linux_snmp.pl -plugin=os : :linux : :snmp : :plugin -mode=storage	Permet le monitoring du remplissage des disques sur les machines Linux
centreon_linux_snmp.pl -plugin=os : :linux : :snmp : :plugin -mode=memory	Permet le monitoring de la mémoire RAM sur les machines Linux
centreon_linux_snmp.pl -plugin=os : :linux : :snmp : :plugin -mode=interface	Permet le monitoring du trafic réseau sur les machines Linux
centreon_windows_snmp.pl -plugin=os : :windows : :snmp : :plugin -mode=cpu	Permet le monitoring de la valeur du CPU sur les machines Windows
centreon_windows_snmp.pl -plugin=os : :windows : :snmp : :plugin -mode=storage	Permet le monitoring du remplissage des disques sur les machines Windows
centreon_windows_snmp.pl -plugin=os : :windows : :snmp : :plugin -mode=storage	Permet le monitoring du remplissage des disques sur les machines Windows
centreon_windows_snmp.pl -plugin=os : :windows : :snmp : :plugin -mode=memory	Permet le monitoring de la mémoire RAM sur les machines Windows
centreon_windows_snmp.pl -plugin=os : :windows : :snmp : :plugin -mode=interface	Permet le monitoring du trafic réseau sur les machines Windows
check_dhcp	Permet de vérifier le fonctionnement du DHCP sur un hôte
check_dns	Permet de vérifier que le serveur DNS renvoie bien la bonne adresse IP sur un nom de domaine spécifique

FIGURE 3 – Commandes utilisés pour le monitoring de l'infrastructure

## 5.5 Ajout d'un hote

Un hote représente, dans centreon, une machine sur le réseau.

1. Aller dans la section *Configuration > Hosts*
2. Ajouter un hote
3. Ajouter le nom et l'alias représentant l'hote de manière unique
4. Ajouter l'ip pour contacter la machine
5. Renseigner la communauté SNMP et la version de SNMP utilisé
6. Définir le poller à utiliser
7. Choisir la commande permettant de vérifier que l'hote est présent dans la section *Check Command*
8. Choisir la fréquence et la periode a observer dans la section *Scheduling Option*

## 5.6 Ajout d'un service

Les services sont des systèmes permettant de vérifier que tout ce que le serveur doit fournir est bien mis a disposition. Ils servent aussi à vérifier certaines valeurs comme le CPU, la RAM, etc.

Les services utilisent les commandes et demandent leurs exécution à interval régulier. Ces commandes permettent de définir un etat au service.

**OK** Le service n'as rien à signaler

**WARNING** Le service est en etat dangereux et demande une attention dans les plus bref délais

**CRITICAL** Le service n'est plus disponible ou les meusures sont dans le rouge ; le serveur demande une intervention immédiate

1. Aller dans la section *Configuration > Services*
2. Ajouter un service et lui donner un nom
3. Donner les hotes utilisant ce service
4. Donner la commande à exécuter dans la section *Check command*
5. Définir la periode de vérification dans la section *Service Scheduling Options*

## 5.7 Ajout d'un poller

Après l'installation d'un poller, il faut l'ajouter à notre serveur central pour qu'ils communiquent.

1. Installer un Poller suivant la procédure donnée précédement
2. Depuis le serveur central, générer une clé pour l'utilisateur **centreon** avec les commandes **su - centreon** et **ssh-keygen**
3. Copier la clé vers le serveur poller avec la commande **ssh-copy-id**
4. Ajouter le poller dans la section web *Configuration > Poller*
5. Ajouter un recuperateur de données en utilisant l'assistant dans **Configuration > Poller**
6. Ajouter au moin un hote au poller dans les paramètres du poller

## 5.8 Monitoring

Le monitoring des services et hotes passent par la section *Monitoring > Services*. Dans cette section on retrouve tout les services associés aux hotes et leurs status.

Une page plus réduite et synthétique peut être trouvée dans la section *Monitoring > Services Grid*






























Hosts ^	Status	Services information
Centreon_poller		 CPU  RAM  DISK  Traffic
Master_centreon		 CPU  RAM  DISK  Traffic
Master_group		 CPU  RAM  DISK  Traffic  DNS isec-group.local  DHCP
Master_telecom		 CPU  RAM  DISK  Traffic  DNS isec-telecom.local
Replic_group		 RAM  DISK  Traffic  DNS isec-group.local  CPU

FIGURE 4 – Exemple d’hotes et de services sur l’interface de centreon

### 5.8.1 Reporting

Le reporting est une fonctionnalité importante de centreon permettant de mesurer son SLA pour chaque Hote.

Pour calculer le reporting, il faut, au préalable, exécuter les commandes suivantes permettant de calculer le reporting pour la journée.

Listing 2 – Commandes permettant de calculer le reporting pour la journée en cours

```
1 /usr/share/centreon/cron/eventReportBuilder
2 /usr/share/centreon/cron/dashboardBuilder
```

On retrouve alors les données du reporting dans la section *Reporting > Dashboard* sur l’interface WEB.

Il est conseillé de mettre ces commandes dans la table cron pour l’exécuter chaque jour.

## 5.9 Sauvegarde

Pour garantir une réinstallation possible, nous avons créé un script permettant d’enregistrer une sauvegarde de la configuration de Centreon. Ce script sauvegarde les fichiers de configuration et les plugins dans des archives TAR. Il s’occupe aussi de sauvegarder la base de données.

Ce script va de paire avec le script de restauration effectuant les opérations inverses pour restaurer les configurations, plugins et bases de données.

**Attention** Vérifiez bien que la version de Centrón utilisé pour la restauration est la même que celle utilisée pour la sauvegarde. Les bases de données sont, le plus souvent, incompatibles.

## 6 Bilan

### 6.1 Évolutions possibles

Les différentes GPOs créées pourraient être déployés avec des scripts powershell afin de recréer les GPO d’un domaine sur un deuxième domaine. De nombreuses autres GPOs pourraient être

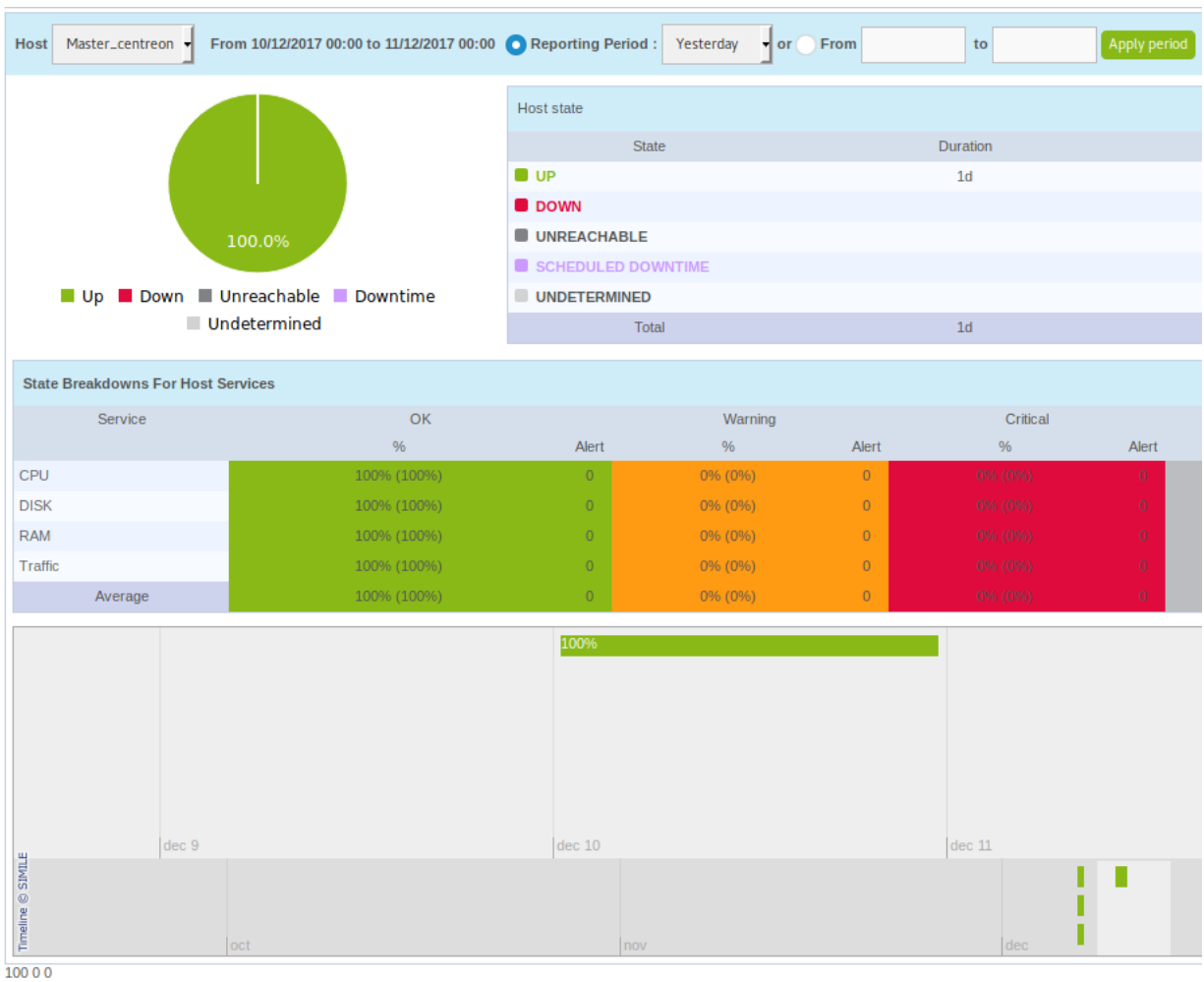


FIGURE 5 – Exemple d'interface de reporting

prises en place, que ce soit au niveau de la sécurité, que de la personnalisation du poste utilisateur.

## 6.2 Conclusion

### 6.2.1 Tanguy Blochet

Ce projet a été très intéressant, il m'a permis de mettre en application toutes les connaissances étudiées en proxit. Il a fallu beaucoup de patience pour ce projet, que ce soit pour l'installation, ou le redémarrage des machines virtuelles. Le groupe a eu une très bonne entente et a très bien fonctionné.

### 6.2.2 Baptiste Saclier

### 6.2.3 Jean-Guillaume Ponsard