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

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 a réaliser est pour le compte du groupe iSEC dont l'organisation est schématisé dans la figure 1.

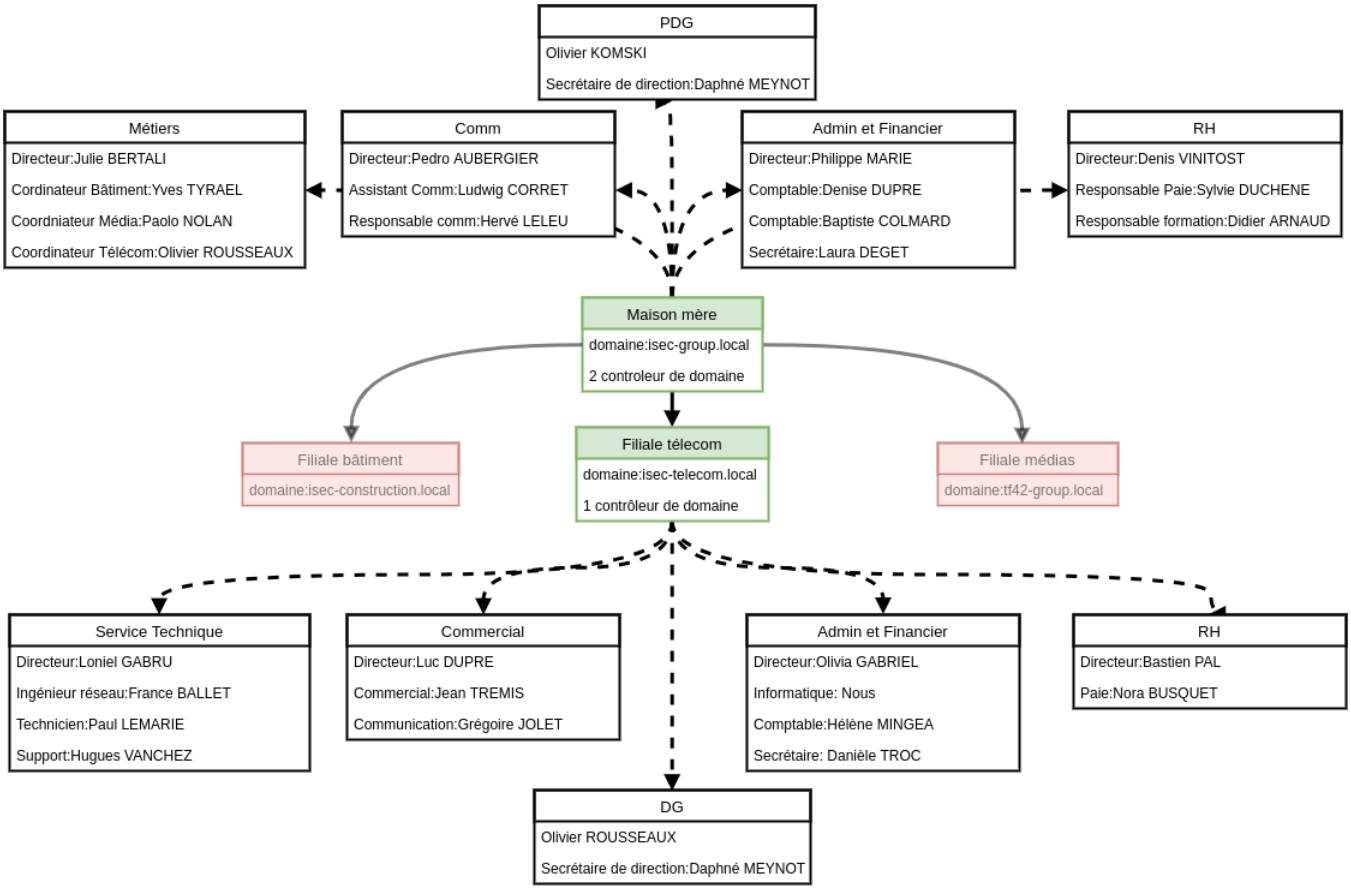

FIGURE 1 – Schéma de l'organisation de groupe iSEC.

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 réplica 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 fôrets 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 décris 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 :

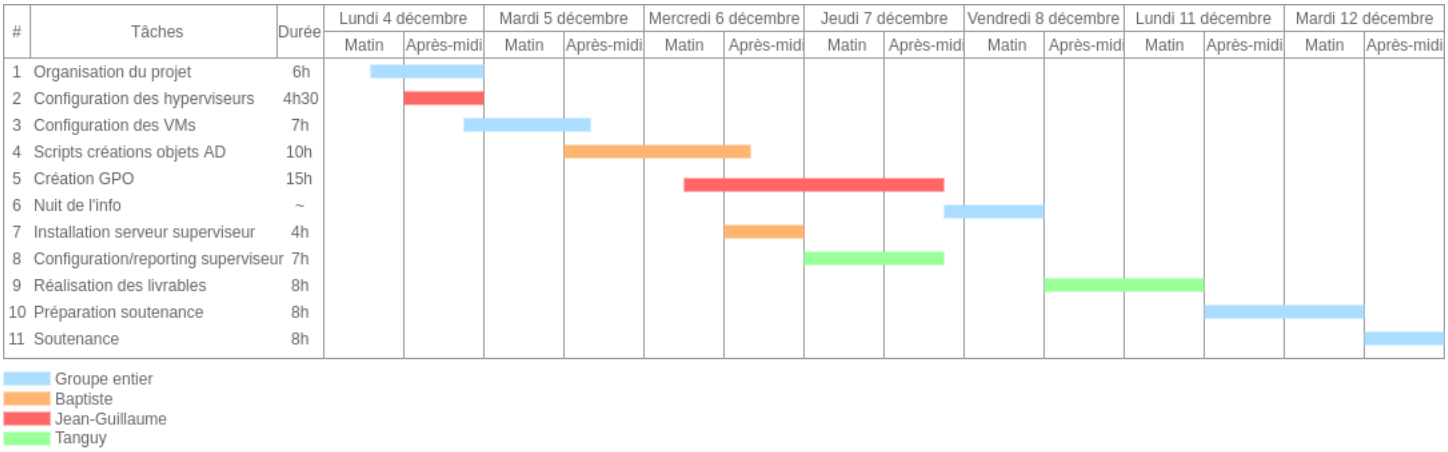

FIGURE 2 – Planning prévisionnel du projet.

Ce planning prévisionnel a été dans l'ensemble respecté, certaines heures supplémentaires ont été nécessaires pour la configuration des serveurs de supervision. Un dépot 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

2.2 Machines virtuelles

2.3 Communication inter-VMs

3 Configuration des serveurs

3.1 Serveurs groupe iSEC

3.1.1 Serveur principal

3.1.2 Serveur réplica

3.2 Serveurs groupe Telecom

3.2.1 Serveur Windows Server

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 créé 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 Scripts

4.2 GPO

4.2.1 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 maitre, il faut suivre la procédure suivante :

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`, cliquez 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`, ouvrer le `Gestionnaire de stratégie de groupe`
4. Dans l'UO créée précédement `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`.

4.2.2 Partage Telecom

Le partage Telecom se fait de la même façon que dans le paragraphe 4.2.1, 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.

4.2.3 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 dossiers partagés 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 précédement 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`, ouvrer 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 précédement, `\\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`.

4.2.4 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. Ouvrer 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`, récupéré le chemin de partage qui sera utile plus tard.
4. Dans le `Gestionnaire de serveur`, ouvrer 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 précédement 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`.

4.2.5 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`, ouvrer 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`, selectionner `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`.

4.2.6 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`.

4.2.7 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`, `Modéles 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`.

4.2.8 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, répetez 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 précédement 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 précédement 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`.

4.2.9 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 précédement 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`, ouvrer 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 disponiblitité. 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 agire 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, a l'aide du protocol SNMP, la bonne santé des équipements. Nous l'avons choisis pour sa facilité d'utilisation et pour sa propriété décentralisé.

Centréon met à disposition une architecture décentralisée permettant de gèrer 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

5.2 Configuration

6 Bilan

6.1 Évolutions possibles

6.2 Conclusion