Compte-rendu lundi 12 juin 2023

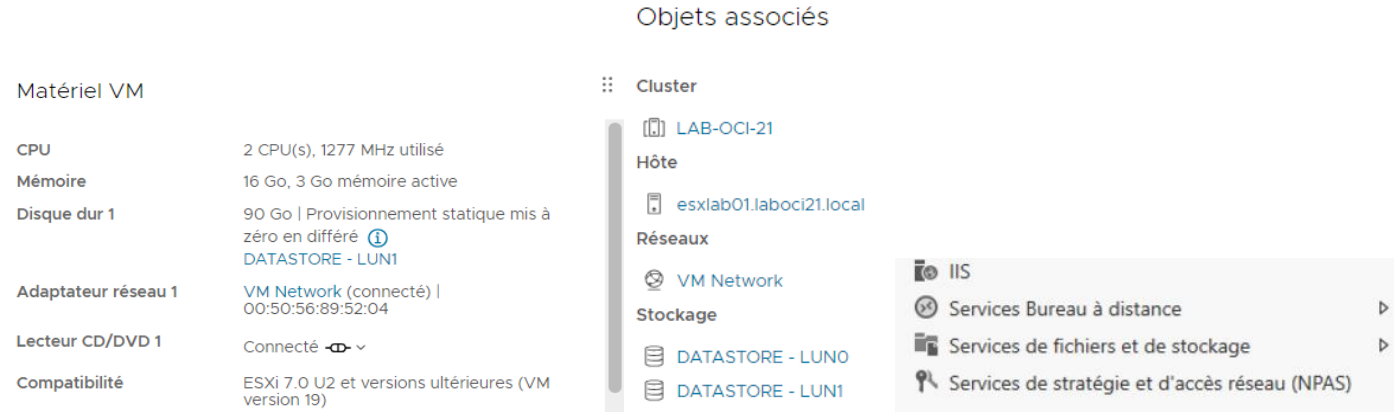
- Nous avons passé la journée à **Dijon Céréale** (Longvic).
- Notre objectif principal était de vérifier que le Vcenter de Dijon Céréale était à jour, (finalement il possédait déjà la dernière mise à jour), ainsi que de **mettre à jour les** ESX et le pare-feu (**WatchGuard**) car récemment beaucoup de faille de sécurité sont découvertes.
- On a veillé à mettre à jour **l'iDRAC** aussi.
- **iDRAC (Integrated Dell Remote Access Controller)** est un composant matériel dans les serveurs Dell qui permet une gestion à distance et un contrôle sur le système, ce qui est crucial pour la surveillance, la configuration et le dépannage efficace des serveurs. Il est important de le mettre à jour régulièrement pour bénéficier des dernières fonctionnalités, améliorations de sécurité et corrections de bugs afin d'assurer la stabilité et les performances optimales du serveur.
- **Le Vcenter est tout simplement le « lieu » / « centre » ou se trouve tous les serveurs ou VM de chez Dijon Céréale.**
- Nous avons veillé à ce que la dernière mise à jour que nous souhaitons appliquer aux ESX soit **compatible avec la version du Vcenter**.
- Il est important de noter que nous avons **besoin des droits nécessaires pour télécharger les différentes mises à jour**.
- Pour mettre à jour les ESX, **nous avons migré les machines virtuelles** (VMs) en cours d'utilisation (à chaud) vers un autre ESX **tout en conservant leur accessibilité**.
- Avant de procéder à la mise à jour, nous avons mis l'ESX concerné en "**Mode maintenance**" afin d'éviter que les autres serveurs ne migrent automatiquement les machines virtuelles vers celui en cours de mise à jour, au cas où ils rencontreraient un problème.
- Nous nous sommes **connectés en ligne de commande pour sauvegarder les données du serveur** en cours de mise à jour et pour effectuer la mise à jour proprement dite.
- Pendant ce temps, nous avons également procédé à la **mise à jour du schéma de l'infrastructure réseau de Dijon Céréales**.
- Nous avons utilisé **LogMeIn Client et ISL** pour effectuer nos tâches.
- **LogMeIn Client** est un logiciel utilisé pour se connecter à distance à des ordinateurs et accéder à leurs fonctionnalités à partir d'un autre emplacement. Il permet de contrôler et de gérer les ordinateurs à distance de manière sécurisée.
- **ISL (Integrated Services Layer)** est une technologie qui offre des services intégrés pour faciliter la gestion et la communication entre différents systèmes informatiques. Il permet d'établir des connexions sécurisées entre les différents composants d'un réseau, facilitant ainsi le transfert de données et la coordination des tâches.

Nos objectifs étaient donc de vérifier et mettre à jour le Vcenter et les ESX de Dijon Céréale, en veillant à la compatibilité des mises à jour, tout en assurant la continuité des opérations en migrant les VMs et en mettant les ESX en mode maintenance. Nous avons également effectué la sauvegarde des données du serveur en cours de mise à jour et mis à jour le schéma de l'infrastructure réseau. Pour réaliser ces tâches, nous avons utilisé LogMeIn Client et ISL.

Compte-rendu mardi 13 juin 2023

Reprise du projet de la semaine dernière sur le Lab, installation d'un serveur RDS et quelques services.

➔ **SRV-RDS-CM (Serveur avec accès bureau à distance)**



- RDS + UPD
- Création raccourci RDS sur les postes des utilisateurs du fichier RDP pour avoir un espace sur le serveur **SRV2-W22-CM.**
- La **fonctionnalité (IIS : Internet Information Services)** fait référence au serveur web. Il fournit une infrastructure d'applications web fiable, gérable et évolutive.
- Le **service de bureau à distance** permet aux utilisateurs d'accéder à distance à un ordinateur ou à un réseau depuis un autre emplacement. Cela permet de travailler sur un ordinateur distant comme si l'on était physiquement présent à cet endroit.
- Les **services de fichiers de stockage** offrent un espace de stockage en ligne pour les utilisateurs, où ils peuvent stocker et partager leurs fichiers. Cela permet un accès facile et sécurisé à ses fichiers à partir de n'importe quel appareil connecté à Internet.
- Les **services de stratégies et d'accès réseau NPAS (Network Policy and Access Services)** sont utilisés pour définir et gérer les politiques de sécurité et d'accès au réseau. Ils permettent de contrôler qui peut accéder au réseau et quelles ressources ils peuvent utiliser.
- Installer ces services sur un serveur présente plusieurs avantages. Tout d'abord, cela centralise la gestion et facilite les mises à jour et les modifications. De plus, un serveur puissant peut offrir des performances supérieures et une meilleure sécurité par rapport à des ordinateurs individuels.
- Faire un raccourci RDS (Remote Desktop Services) sur les PC des utilisateurs leur permettent d'accéder facilement et rapidement au serveur distant. Ils peuvent utiliser les services de bureau à distance et les autres services (fichiers de stockage, stratégies d'accès réseau, etc.) directement à partir de leur propre ordinateur. Cela simplifie l'accès et améliore la productivité, car les utilisateurs n'ont pas besoin de se déplacer physiquement vers le serveur.
- **Mettre en place des disques UPD (User Profile Disks)** dédiés à un utilisateur particulier présente des avantages. Les disques UPD stockent les profils des utilisateurs, y compris leurs données, leurs paramètres et leurs préférences personnalisées. Cela permet à un utilisateur de se connecter à n'importe quel ordinateur du réseau et de retrouver son environnement de travail personnalisé. Les disques UPD simplifient la gestion des profils d'utilisateurs et offrent une expérience cohérente et personnalisée, indépendamment de l'ordinateur utilisé.

Compte-rendu mercredi 14 juin 2023

Installation d'un serveur avec la fonctionnalité WSUS.

WSUS (Windows Server Update Services) est un service de gestion des mises à jour développé par Microsoft. Il permet aux administrateurs de réseau de déployer, gérer et distribuer des mises à jour logicielles à travers un environnement informatique.

Etapes pour configurer les mises à jour automatiques et l'emplacement du service de mise à jour :

1. J'ai été dans "**Outils**" puis dans "**Gestion de stratégie de groupe**" sur mon serveur avec AD.
2. J'ai développé Forêt : **springfield.local > Domaines > springfield.local**.

3. J'ai cliqué avec le bouton droit sur **springfield.local**, puis j'ai sélectionné "**Créer un objet de stratégie de groupe dans ce domaine, puis l'associer ici**".
4. J'ai créé un nouvel objet GPO que j'ai nommé "**WSUS - Auto Updates and Intranet Update Service Location**".
5. J'ai cliqué avec le bouton droit de la souris sur l'objet GPO "**WSUS - Auto Updates and Intranet Update Service Location**" et j'ai sélectionné "**Modifier**".
6. Dans l'éditeur de gestion des stratégies de groupe, je suis allé à l'emplacement "**Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update**".
7. J'ai fait un clic droit sur le paramètre "**Configuration du service Mises à jour automatiques**" et j'ai choisi "**Modifier**".
8. J'ai ouvert la boîte de dialogue "**Configuration du service Mises à jour automatiques**" et j'ai sélectionné "**Activer**".
9. Dans la section "**Options**", j'ai choisi l'option "**3 - Téléchargement automatique et notification des installations**" dans la liste "**Configuration de la mise à jour automatique", puis j'ai cliqué sur "OK**".
10. J'ai fait un clic droit sur le paramètre "**Spécifier l'emplacement intranet du service de mise à jour Microsoft**" et j'ai sélectionné "**Modifier**".
11. Dans la boîte de dialogue "**Spécifier l'emplacement intranet du service de mise à jour Microsoft**", j'ai activé l'option.
12. Sous "**Options**", j'ai saisi **http://192.168.200.76:8530** dans les options "**Définir le service de mise à jour intranet pour la détection des mises à jour**" et "**Définir le serveur de statistiques intranet**", puis j'ai sélectionné "**OK**".

Etapes pour créer des groupes d'ordinateurs dans la console d'administration WSUS

1. J'ai ouvert la console d'administration WSUS sur le serveur **SRV-WSUS-CM**.

2. Je suis allé à l'emplacement **SRV-WSUS-CM\Ordinateurs\Tous les ordinateurs**, puis j'ai cliqué sur "**Ajouter un groupe d'ordinateurs**".

3. J'ai indiqué le nom "**GroupePartage1**" et j'ai cliqué sur "**Ajouter**".

4. J'ai répété ces étapes pour créer le groupe "**GroupePartage2**".

Ensuite, pour affecter manuellement des ordinateurs non affectés à des groupes :

1. Dans la console d'administration WSUS, je suis allé à l'emplacement **SRV-WSUS-CM\Ordinateurs\Tous les ordinateurs\Ordinateurs non attribués**.

2. J'ai sélectionné un des deux ordinateurs, par exemple "**user-bart-cm.springfield.local**", j'ai fait un clic droit sur la sélection, puis j'ai choisi "**Modifier l'appartenance**".

3. Dans la boîte de dialogue "**Définir les groupes d'ordinateurs**", j'ai sélectionné l'anneau de déploiement "**GroupePartage1**", puis j'ai cliqué sur "**OK**".

4. J'ai répété ces étapes pour le deuxième ordinateur, en l'assignant au groupe "**GroupePartage2**".

Maintenant que les ordinateurs ont été affectés à des groupes, ils ne sont plus répertoriés dans le groupe "Ordinateurs non affectés".

Ensuite, pour configurer WSUS afin d'autoriser le ciblage côté client de la stratégie de groupe :

1. J'ai ouvert la console d'administration WSUS et je suis allé à l'emplacement **SRV-WSUS-CM\Options**, puis j'ai cliqué sur "**Ordinateurs**".

2. Dans la boîte de dialogue "**Ordinateurs**", j'ai sélectionné "**Utiliser la stratégie du groupe ou les paramètres des Registres des ordinateurs**", puis j'ai cliqué sur "**OK**".

Maintenant, WSUS est prêt pour le ciblage côté client et nous pouvons utiliser la stratégie de groupe pour le configurer.

Pour cela :

1. J'ai ouvert la console de gestion de stratégie de groupe.

2. J'ai développé "**Forêt\Domaines\springfield.local**".

3. J'ai fait un clic droit sur "**springfield.local**", puis j'ai sélectionné "**Créer un objet GPO dans ce domaine et le lier ici**".

4. Dans la boîte de dialogue "**Nouvel objet GPO**", j'ai saisi le nom "**WSUS - Client Targeting - GroupePartage1**" pour le nouvel objet GPO.

5. J'ai fait un clic droit sur l'objet GPO "**WSUS - Client Targeting - GroupePartage1**" et j'ai sélectionné "**Modifier**".

6. Dans l'éditeur de gestion des stratégies de groupe, je suis allé à l'emplacement "**Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows Update**".

7. J'ai fait un clic droit sur "**Autoriser le ciblage côté client**" et j'ai sélectionné "**Modifier**".

8. Dans la boîte de dialogue "**Autoriser le ciblage côté client**", j'ai sélectionné "**Activer**".

9. Dans la zone "**Nom du groupe cible de cet ordinateur**", j'ai saisi "**GroupePartage1**", qui est le nom de l'anneau de déploiement WSUS dans lequel ces ordinateurs seront ajoutés.

10. J'ai répété ces étapes pour le groupe "**GroupePartage2**".

Enfin, pour définir l'étendue de l'objet GPO à un groupe :

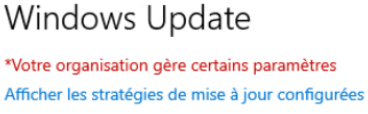
1. Dans GPMC, j'ai sélectionné la stratégie "**WSUS - Client Targeting - GroupePartage1**".

2. J'ai cliqué sur l'onglet "**Étendue**".

3. Dans l'onglet "**Filtrage de sécurité**", j'ai supprimé le groupe de sécurité "**UTILISATEURS AUTHENTIFIÉS**" par défaut, puis j'ai ajouté le groupe "**GroupePartage1**".

4. J'ai répété ces étapes pour le groupe "**GroupePartage2**".

Aide avec : https://learn.microsoft.com/fr-fr/windows/deployment/update/waas-manage-updates-wsus



Voici ainsi ce que l'on voit sur les postes des utilisateurs.

Compte-rendu jeudi 15 juin 2023

Création d'une GPO pour installer / désinstaller / mettre a jour des application automatiquement pour les déployer sur plusieurs PC en même temps.

Étape 1: Création du dossier partagé "Applications"
- J'ai créé un dossier partagé nommé "**Applications**".
- Dans les paramètres de partage, j'ai choisi de le masquer en ajoutant un signe "$" à la fin du nom.
- Dans les paramètres de sécurité, j'ai désactivé l'héritage des autorisations.
- J'ai supprimé le groupe "**Utilisateurs**" et ajouté le groupe "**Ordinateurs du domaine**" avec les droits de lecture, d'exécution, d'affichage du contenu du dossier et de lecture.

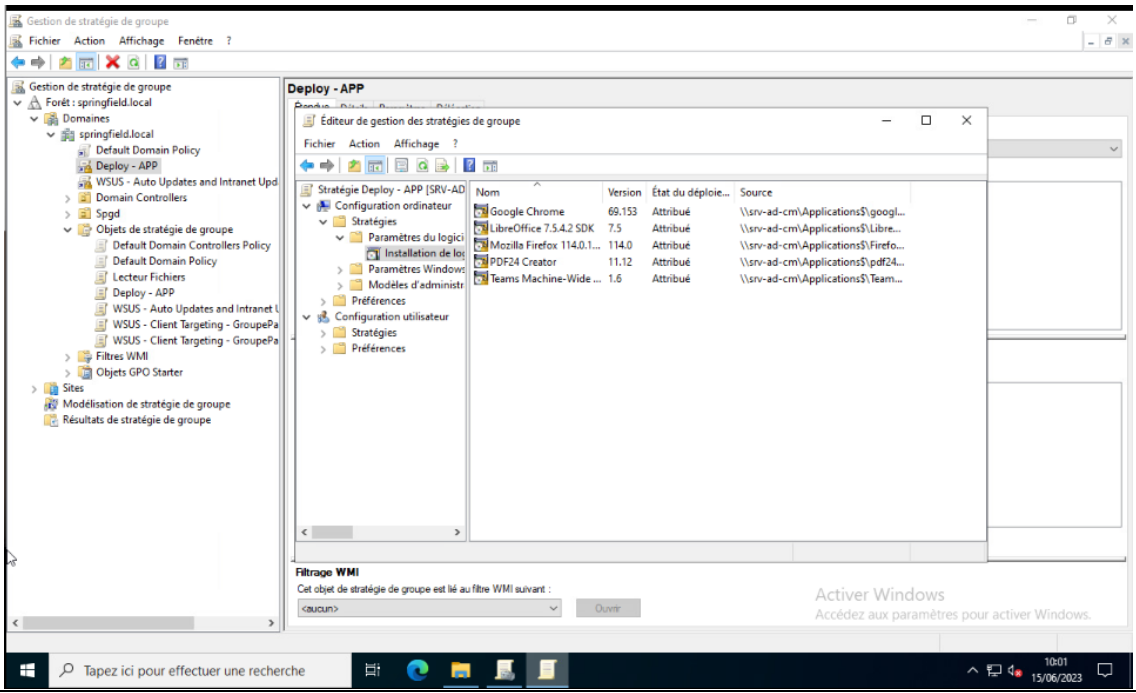
Étape 2: Téléchargement des paquets .msi des logiciels
- J'ai téléchargé les fichiers d'installation (.msi) des logiciels Teams, PDF24, FireFox et Chrome.
- J'ai placé ces fichiers dans le dossier partagé "**Applications**".

Étape 3: Création de la nouvelle GPO "Deploy - APP"
- J'ai créé une nouvelle GPO nommée "**Deploy - APP**".
- J'ai modifié cette GPO en accédant à "**Configuration ordinateur" > "Stratégies" > "Paramètres du logiciel" > "Installation de logiciel".**

Étape 4: Ajout des packages d'installation des logiciels dans la GPO
- Dans la partie de droite de la fenêtre de la GPO, j'ai fait un clic droit et sélectionné **"Nouveau" > "Package"**.
- J'ai indiqué le chemin réseau du package d'installation des logiciels depuis notre dossier partagé.

Étape 5: Attribution des packages d'installation
- J'ai sélectionné l'option "**Attribué**" pour chaque package d'installation des logiciels.
- J'ai répété les étapes 4 et 5 pour chaque paquet d'installation des logiciels (Teams, PDF24, FireFox, Chrome).

On se connecte désormais à une machine cliente (d'un utilisateur).
On se rend dans l'invite de commande puis on exécute la commande « gpupdate /force »
Après redémarrage on voit que les logiciels apparaissent.



Début mise en place d'un un serveur GLPI

➔ SRV-GLPI-CM

Compte-rendu vendredi 16 juin 2023

Installation du rôle Serveur Web (IIS), PHP et des modules CGI / FastCGI afin de pouvoir configurer GLPI que nous venons d'installer dans le serveur IIS (serveur WEB)

0. Après l'ouverture d'une session en mode Administrateur, on ajoute le rôle Serveur Web (IIS)
1. On télécharge le dossier GLPI (https://glpi-project.org/fr/telecharger-glpi/) , on extrait les fichier avec 7zip afin d'avoir un dossier "**myglpi**" avec tous les fichiers de configuration.
2. On met ce fichier dans **C:\inetpub\wwwroot**
3. On ouvre le Gestionnaire de service Web (IIS), puis on fait un clic-droit sur "**Sites**" puis "**Ajouter un site web**". On suit les étapes pour ajouter notre dossier "**myglpi**".
4. J'ai ensuite téléchargé la version appropriée de PHP compatible avec la version d'IIS à partir du site officiel de PHP (https://windows.php.net/download/).
5. J'ai téléchargé l'extension "**PHP Manager**"
6. J'ai extrait les fichiers de l'archive PHP téléchargée dans le répertoire **C:\PHP**.
7. J'ai renommé le fichier "**php.ini-production**" en "**php.ini**".
8. J'ai ouvert le **Gestionnaire des services Internet (IIS**)
9. J'ai développé "**Serveur Web IIS**", "**Serveur Web**" et j'ai coché la case "**Développement d'applications**" (sélectionné la sous-fonctionnalités "**CGI**").
10. J'ai cliqué sur "**OK**" pour installer les fonctionnalités sélectionnées.
11. Dans le Gestionnaire IIS, j'ai cliqué sur mon serveur (**SRV-GLPI-CM**) dans l'arborescence de gauche.
12. Dans la section "**Modules**", j'ai vérifié si les modules "**FastCgiModule**" et "**CgiModule**" sont présent.
13. /!\ Ils sont peut-être présent, mais j'ai dû faire un clic-droit dessus pour les "**Déverrouiller**" et pouvoir y avoir accès à partir de la "**Page d'accueil du serveur**".
14. Dans le Gestionnaire IIS, j'ai double-cliqué sur l'icône "**PHP Manager**" dans la section "**IIS**" pour ouvrir **PHP Manager**.
15. J'ai cliqué sur "**Register new PHP version**" et spécifié le chemin d'accès à l'exécutable "**php-cgi.exe**" que j'ai extrait dans l'étape 2 (**C:\PHP\php-cgi.exe**).

Aide : https://rdr-it.com/glpi-sous-iis-configuration-installation/

COMPTE-RENDU en bref de la semaine : (message envoyé sur ECLAT)

Compte-rendu hebdomadaire du 12 au 16 juin 2023 :

Cette semaine, j'ai consacré mes journées à diverses activités liées à la gestion et à la mise à jour de notre infrastructure informatique. Voici un résumé de nos actions dont mon tuteur à pu vérifier et m'aider tout en apprenant de nouvelles choses :

J'ai d'abord passé la journée à Dijon Céréale (Longvic) pour vérifier et mettre à jour le Vcenter, les ESX et le pare-feu WatchGuard. J'ai effectué la migration des machines virtuelles vers un autre ESX tout en maintenant leur accessibilité, le temps de la mise à jour de l'ESX en question. J'ai également mis à jour le schéma de l'infrastructure réseau. J'ai découvert et utilisé les outils LogMeIn Client et ISL pour une gestion à distance sécurisée et une communication efficace.

Ensuite, j'ai repris le projet du Lab en installant un serveur RDS et divers services connexes tels que l'IIS, les services de fichiers de stockage et les services de stratégies et d'accès réseau NPAS. J'ai créé un raccourci RDS sur les postes des utilisateurs pour faciliter leur accès au serveur distant et aux services disponibles. J'ai également configuré des disques UPD pour chaque utilisateur, leur offrant ainsi un environnement de travail personnalisé.

Après, j'ai installé un serveur WSUS pour gérer les mises à jour logicielles. J'ai configuré les paramètres de stratégie de groupe et organisé les ordinateurs dans des groupes spécifiques pour une gestion efficace des mises à jour.

De plus, j'ai créé une GPO pour automatiser l'installation, la désinstallation et la mise à jour des applications sur plusieurs PC simultanément. J'ai créé un dossier partagé pour stocker les fichiers d'installation des logiciels, et j'ai ajouté les packages d'installation dans la GPO en spécifiant le chemin réseau. J'ai ensuite attribué les packages d'installation à chaque logiciel.

Enfin, j'ai installé et configuré le rôle Serveur Web (IIS), PHP et les modules CGI / FastCGI sur notre serveur IIS pour configurer GLPI. J'ai téléchargé les fichiers GLPI, et je l'ai ajouté au serveur IIS pour créer le site web dans le Gestionnaire de service Web (IIS) et installé la version appropriée de PHP. J'ai également activé les modules CGI / FastCGI et assuré leur bon fonctionnement en utilisant l'outil "PHP Manager".

En résumé, ma semaine a été consacrée à la gestion et à la mise à jour de d'infrastructure informatique. J'ai effectué des tâches telles que la vérification et la mise à jour du Vcenter, des ESX et du pare-feu, l'installation d'un serveur RDS avec divers services associés, la configuration d'un serveur WSUS, la création d'une GPO pour le déploiement d'applications et l'installation et la configuration du Serveur Web (IIS), de PHP et des modules CGI / FastCGI pour GLPI. Ces actions ont permis d'améliorer la sécurité, la gestion des mises à jour logicielles et la facilité d'accès aux services pour les utilisateurs.

Un compte-rendu est joint à ce message, il contient beaucoup plus d'informations, des notes et des définitions de termes informatiques, que j'ai découvert cette semaine.