RAPPORT TECHNIQUE

PROJET ANNUAIRE ET SUPERVISION

GROUPE 5 :

- KOUEDEU MOUKAM CINDY LAURA
- ATOUGA II EMMANUEL DESIRE
- SIGNE TASING KAMTHEU CAMPBELL
- NKOUKA SOREL BIENVENU CHRIST

Annéé académique : 2024-2025

Table des matières

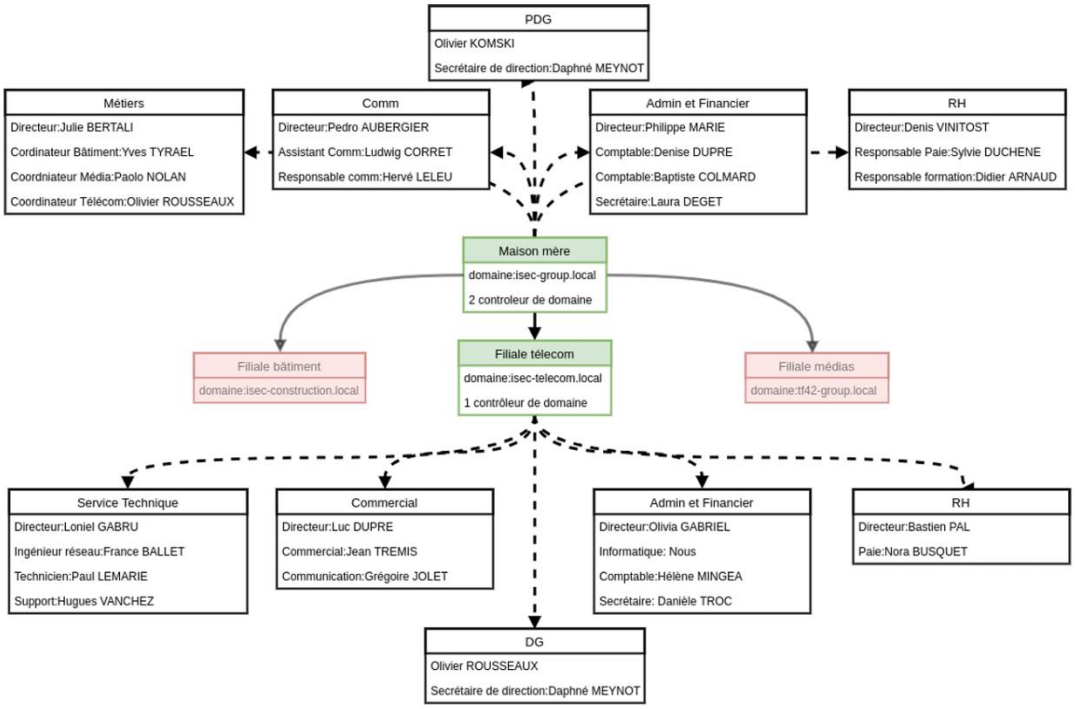
I. Situation

Ce projet visait à concevoir une architecture d'annuaire en installant des services basés sur Active Directory et la supervision des serveurs. L'architecture à mettre en place est destinée au groupe iSEC dont l'organisation est schématisé comme suit :

Le groupe iSEC, récemment devenu propriétaire d'une nouvelle entreprise, opère dans plusieurs secteurs d'activité et dispose de nombreuses filiales. Il souhaite interconnecter le réseau de la maison mère avec celui de ses filiales. Notre objectif est de mettre en œuvre l'architecture Active Directory pour la maison mère et la filiale télécom uniquement.

II. Besoins techniques

Les exigences techniques sont nombreuses, mais l'objectif principal est de relier la maison mère à la filiale télécom via Active Directory. Le groupe iSEC doit disposer d'un contrôleur de domaine principal et d'un réplica pour garantir la continuité du service, tandis que la filiale télécom nécessitera un seul contrôleur de domaine. De plus, une relation d'approbation unidirectionnelle entre les deux forêts doit être établie, permettant aux utilisateurs du domaine du groupe d'accéder aux ressources de la filiale télécom, sans réciprocité.

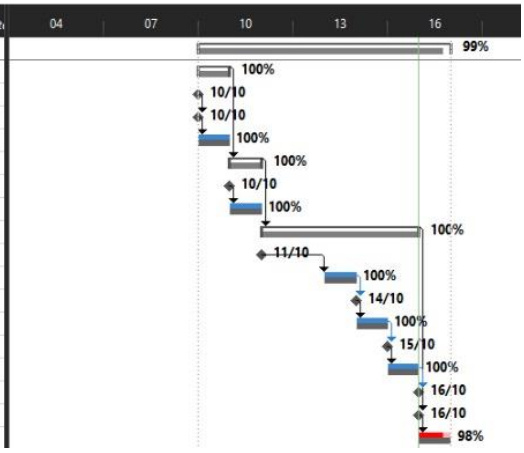


L'arborescence de l'Active Directory doit être créée et organisée en fonction des organigrammes du groupe et de sa filiale. De nombreux partages doivent ensuite être mis à disposition entre services, groupes et utilisateurs. D'autres services doivent également être fournis par l'Active Directory, tels que l'installation automatique de 7Zip, la mise en place de fonds d'écran, ainsi que d'autres services détaillés dans les procédures d'installation à suivre.

III. Organisation du projet

Ce projet a commencé le Jeudi 10 Octobre et se termine le Jeudi 17 Octobre, les taches ont été découpées comme suit :

Mode Tâche	Nom de la tâche	Durée	Début	Fin		Noms ressources	Coût
	PROJET ANNUAIRE ET SUPERVISION	**6 jours**	**Jeu 10/**	**Jeu 17/**			**$5 110,00**
✓	**PRISE DE CONNAISSANCE**	**1 jour**	**Jeu 10/**	**Jeu 10/**			**$1 190,00**
✓	Compréhension du sujet	0 jour	Jeu 10/	Jeu 10/		ATOUGA;Chef d	$0,00
✓	Mise en contexte	0 jour	Jeu 10/	Jeu 10/	3	ATOUGA;Chef d	$0,00
✓	Enumérations des différents be	1 jour	Jeu 10/	Jeu 10/	4	ATOUGA;Chef d	$1 190,00
✓	**INSTALLATION**	**1 jour**	**Jeu 10/**	**Ven 11/**	2		**$1 190,00**
✓	Initialisation de l'environnemen	0 jour	Jeu 10/	Jeu 10/		ATOUGA;Chef d	$0,00
✓	Installation des différents serve	1 jour	Ven 11/	Ven 11/	7	ATOUGA;Chef d	$1 190,00
✓	**CONFIGURATION**	**3 jours**	**Ven 11/**	**Mer 16/**	6		**$2 100,00**
✓	Ajout des rôles ad ds et dns aux	0 jour	Ven 11/	Ven 11/		ATOUGA;Chef d	$0,00
✓	Création du contrôleur de doma	1 jour	Lun 14/	Lun 14/	10	ATOUGA;SIGNE	$560,00
✓	Création des UO,groupes et Utili	0 jour	Lun 14/	Lun 14/	11	Chef de projet(C	$0,00
✓	Configuration des services	1 jour	Mar 15/	Mar 15/	12	Chef de projet(C	$630,00
✓	Création des dossiers partagés	0 jour	Mar 15/	Mar 15/	13	ATOUGA;NKOUK	$0,00
✓	Mise sur pied des gpo	1 jour	Mer 16/	Mer 16/	14	ATOUGA;Chef d	$910,00
✓	Connexion des utilisateurs et trc	0 jour	Mer 16/	Mer 16/	15	ATOUGA;Chef d	$0,00
✓	GESTION DES RELATIONS D'APPROE	0 jour	Mer 16/	Mer 16/	9	ATOUGA;NKOUK	$0,00
	SUPERVISION	1 jour	Jeu 17/	Jeu 17/	17	Chef de projet(C	$630,00

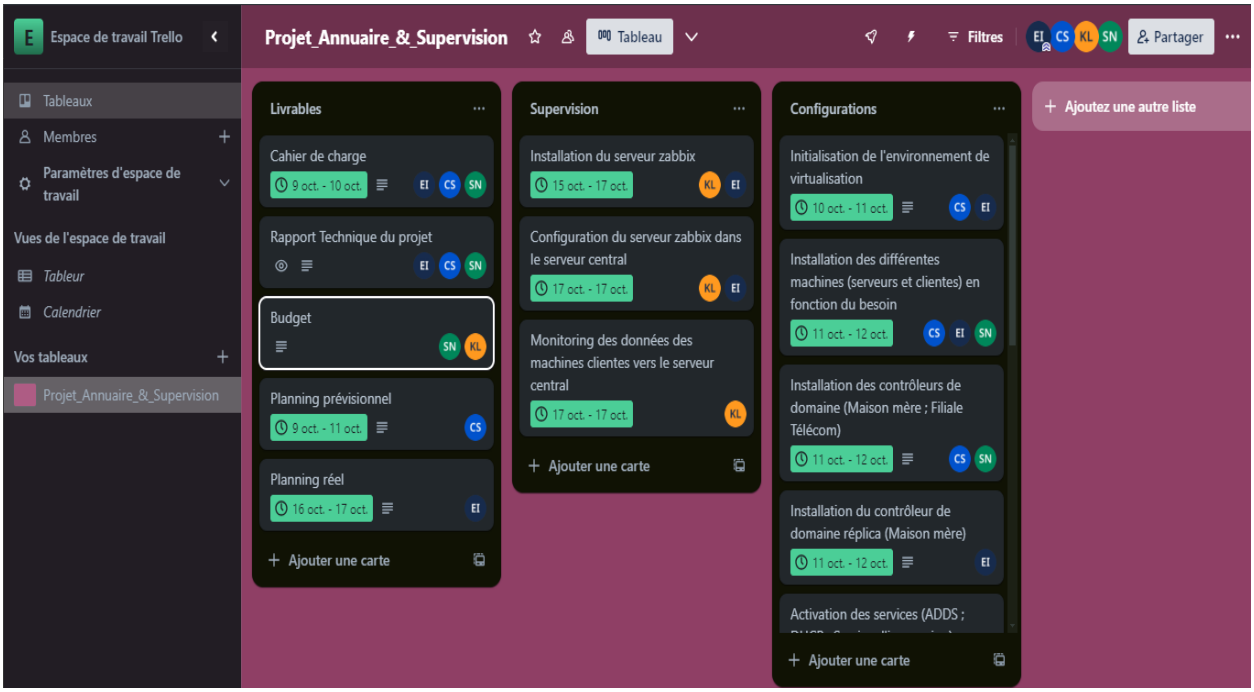


IV. BUDGETISATION

BUDGET DU PROJET			
		PRIX UNITAIRE	PRIX TOTAL
LICENCES Windows Serveur 2022	Edition Datacenter	644.326f	3.718.174f
	CALs	13.260f	13.260f
RESSOURCES HUMAINES	4 Administrteurs reseau	50.000/J	1.400.000f
3SERVEUR	Lenovo ThinkSystem ST50 V2	1.140.051f	3.420.153f
MACHINE	Bundle Complet Dell Station	114.792f	3.558.552f
SOMME TOTAL			12.110.139f
REFERENCE	https://softtrader.fr/prix-de-windows-server-2022/amp/		
	https://www.ldlc.pro/fiche/PB00593373.html/		
	https://www.amazon.fr/Complet-Station-Moniteur-Certifi%C3%A9-Reconditionn%C3%A9/dp/B0D98P7TLS/ref=sr_1_51?__mk_f		

V. GESTION DE PROJET

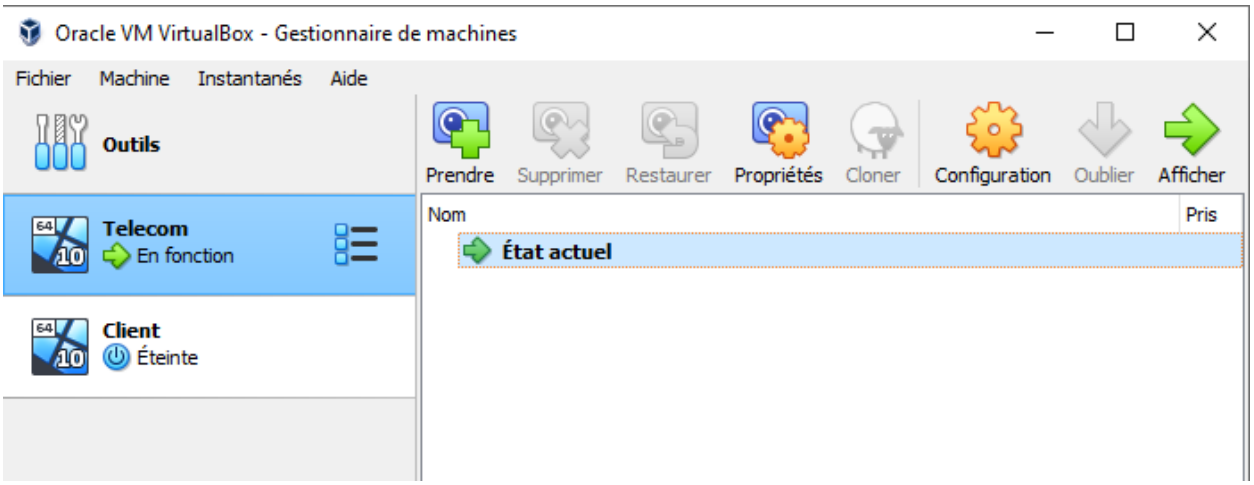
Dans le cadre de la gestion de notre projet, nous avons choisi d'utiliser Trello, un outil de gestion visuelle qui nous aide à organiser et à suivre efficacement nos tâches. Trello repose sur un système de tableaux, de listes et de cartes, ce qui facilite une approche collaborative et intuitive pour gérer les différentes étapes de notre projet. Grâce à ses fonctionnalités flexibles, nous avons pu définir clairement nos objectifs, assigner des responsabilités et suivre l'avancement en temps réel. Cette méthode nous a permis de rester organisés et de favoriser la communication au sein de notre équipe, tout en garantissant que chaque membre est aligné sur les priorités et les délais.



VI. Installation des serveurs

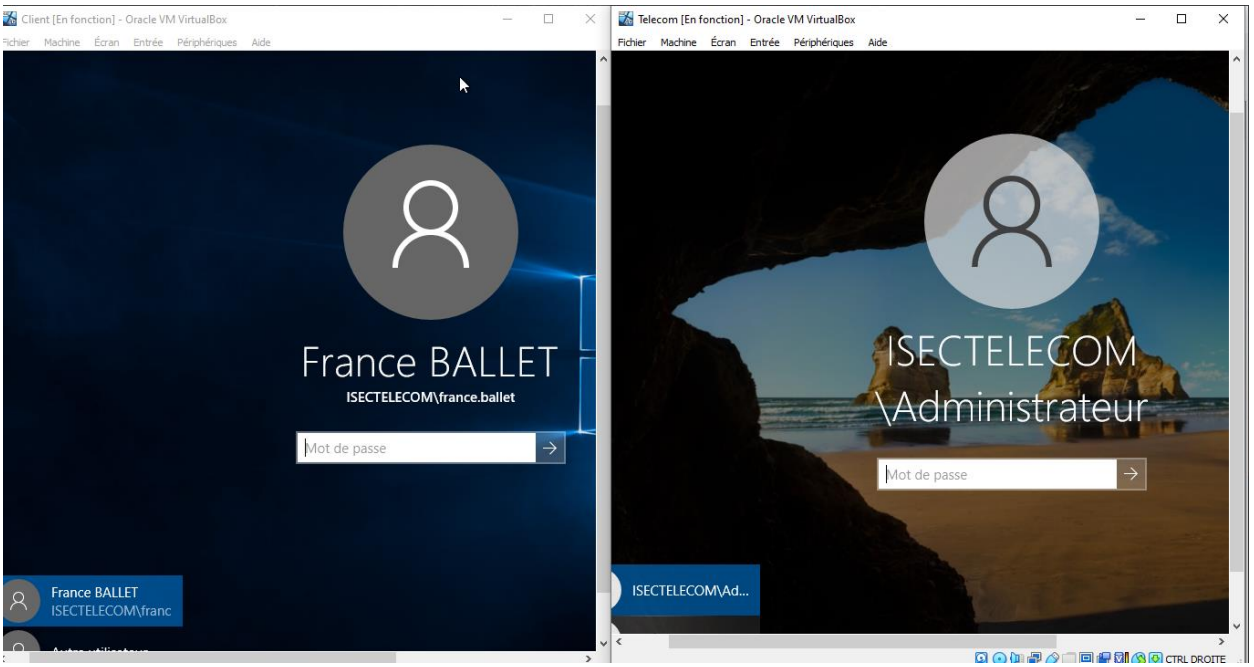
A. Hyperviseurs

Étant donné la configuration matérielle disponible, nous avons décidé d'installer un hyperviseur de type 2 sur nos serveurs physiques. Cette solution est adaptée à notre environnement, car VirtualBox s'exécute sur un système d'exploitation hôte tout en offrant une performance satisfaisante. Nous avons choisi d'utiliser Oracle VirtualBox, car c'est un hyperviseur convivial et flexible. Il propose également une interface graphique intuitive pour gérer les machines virtuelles. De plus, VirtualBox permet de configurer les VMs en mode pont, les connectant ainsi directement au réseau local via un adaptateur réseau virtuel.



B. Machines Virtuelles

Pour créer une machine virtuelle sur Oracle VirtualBox, ouvrez l'application et cliquez sur "Nouvelle". Configurez le nom, le type et la version de l'OS, puis allouez la mémoire et créez un disque dur virtuel. Après avoir configuré les paramètres réseau si nécessaire, cliquez sur "Démarrer" et sélectionnez le fichier ISO du système d'exploitation à installer.



VII. Configuration des serveurs

Pour configurer un domaine Active Directory sur un serveur Windows Server 2022, nous avons procédé comme suit :

1. L'installation des fonctionnalités sous Windows Server se fait en ajoutant des rôles. Dans le tableau de bord du Gestionnaire de serveur de Windows Server 2022, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.

2. Cliquez sur 'Suivant', puis sélectionnez **Installation basée sur un rôle ou une fonctionnalité**. Choisissez le pool de serveurs (sélectionnez votre serveur) et cliquez sur **Suivant**. Vous pourrez alors sélectionner les rôles à installer.

C. Serveurs groupe ISEC

a. Serveur principal

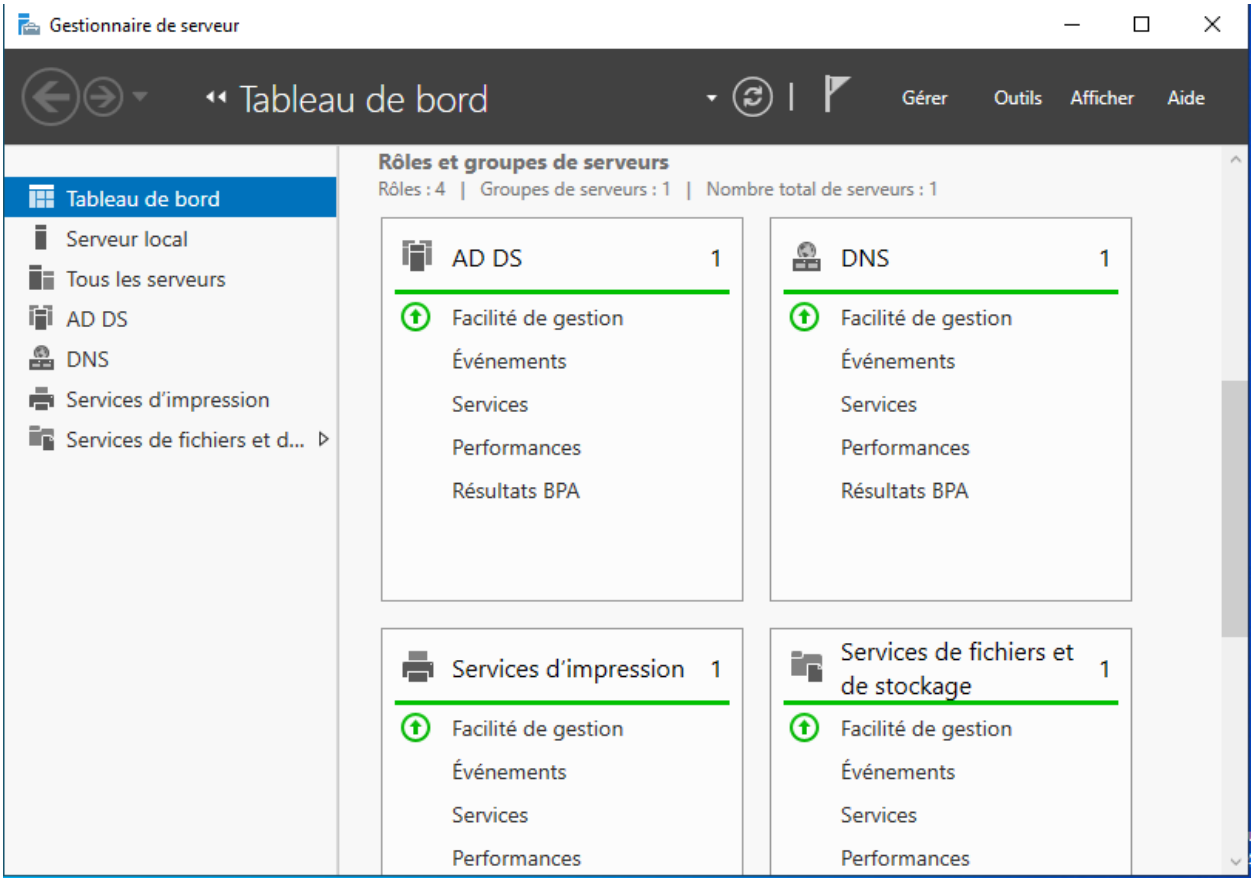
Installer le rôle AD DS

Ce rôle permet d'installer Active Directory, l'annuaire Microsoft qui regroupe toutes les informations du réseau.

1. Dans la fenêtre de sélection des rôles, choisissez le rôle **AD DS**. En sélectionnant ce rôle, le rôle **DNS** sera automatiquement installé, ce qui est essentiel au bon fonctionnement d'Active Directory.
2. Validez les options jusqu'à arriver à l'installation et cliquez sur **Installer**. Il est conseillé d'attribuer une adresse IP statique au serveur avant d'installer le rôle, ce qui sera également utile pour la configuration ultérieure du DHCP.

Configurer le rôle AD DS

1. Une fois le rôle installé, dans le tableau de bord du Gestionnaire de serveur, cliquez sur **Promouvoir le serveur en tant que contrôleur de domaine**. Une fenêtre s'ouvre pour demander les actions à effectuer. Sélectionnez **Ajouter une nouvelle forêt** et entrez le nom de celle-ci : **isecgroup.local**, puis cliquez sur **Suivant**.
2. Renseignez ensuite un mot de passe pour le mode de restauration des services d'annuaire et cliquez sur **Suivant**, puis continuez jusqu'à l'installation. Enfin, cliquez sur **Installer**. Le serveur redémarrera automatiquement à la fin de cette opération, et Active Directory sera désormais fonctionnel.



Installer le rôle DHCP

1. Avant d'installer le DHCP, attribuez une adresse IP statique au serveur.
2. Sélectionnez **Serveur DHCP** dans le menu d'installation des rôles et fonctionnalités, puis cliquez sur **Suivant** jusqu'à atteindre le menu d'installation, où vous cliquerez sur **Installer**. Avant de fermer, assurez-vous de cliquer sur **Terminer la configuration DHCP** et validez les deux étapes.

Configurer le DHCP

1. Une fois l'installation terminée, ouvrez le Gestionnaire DHCP dans l'onglet **Outils** du Gestionnaire de serveur. Faites un clic droit sur **IPv4** et sélectionnez **Nouvelle étendue**. Un assistant de création de nouvelle étendue apparaît, vous demandant de nommer l'étendue (choisissez le nom souhaité) et de fournir une description (facultative).
2. Entrez ensuite 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** pour les clients DHCP se remplira automatiquement. Vous pouvez exclure une plage d'adresses si nécessaire, définir la durée du bail des adresses, indiquer la passerelle par défaut (routeur du réseau) et spécifier le serveur DNS (ces options sont automatiquement remplies car le DNS est sur le même serveur).

Cliquez sur **Suivant** jusqu'à la fin de l'assistant. Le serveur DHCP est maintenant opérationnel.

b. Serveur replica

L'installation du rôle s'effectue de la même manière que pour le serveur **ISEC-GROUP-MASTER**. La seule différence réside dans la configuration : 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 concerné. Ensuite, entrez le mot de passe du mode de restauration des services d'annuaire (DSRM) et cliquez sur **Suivant**.

Ensuite, vérifiez que le serveur **ISEC-GROUP-MASTER** est sélectionné comme source de réplication, puis continuez en cliquant sur **Suivant** jusqu'à atteindre l'installation. Une fois le redémarrage terminé, le réplica sera opérationnel, et vous pourrez accéder aux informations de l'Active Directory.

D. Serveurs groupe Telecom

c. Serveur window 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 de DHCP car ISEC-GROUP-MASTER dispose déjà d'un DHCP.

d. Organisation de l'Active Directory

Nous avons configuré l'Active Directory en fonction des organigrammes fournis dans le projet. Chaque groupe a son propre domaine nommé en conséquence. Les groupes (ISEC et Télécom) possèdent chacun une Unité d'Organisation (UO) dédiée. Chaque service a également une UO qui lui est propre, ainsi qu'un groupe de sécurité correspondant. De plus, chaque poste au sein de l'entreprise (comme le secrétariat) dispose de son propre groupe de sécurité. Enfin, chaque utilisateur a été intégré dans le groupe correspondant à son poste.

Cette structure a été choisie pour simplifier le déploiement des GPO, qui varient d'un service à l'autre et sont donc appliquées à l'UO associée. Des groupes de sécurité ont été créés pour chaque service, car ils sont essentiels pour le partage de dossiers.

VIII. Reponses aux différents besoins

GPO

Partage groupe

Le partage est accessible à tous les services du groupe iSEC et se situe sur le contrôleur de domaine principal. Il est mappé en tant que lecteur réseau sur les postes de travail avec la lettre G:. Voici les étapes à suivre pour créer ce partage sur le contrôleur de domaine maître :

1. Créer le dossier partagé : Sur le contrôleur de domaine, créez le dossier dans C:\Shares\ sous le nom "Groupe", conformément à la convention pour les dossiers partagés.

2. Partager le dossier :

- Faites un clic droit sur le dossier créé.

- Sélectionnez "Propriétés".

- Dans l'onglet "Partage", cliquez sur "Partager...".

- Dans la glissière, choisissez "Rechercher des personnes...".

- Ajoutez le nom du groupe dans le champ de texte. Pour inclure tous les utilisateurs du domaine, tapez "Utilisateurs du domaine" et cliquez sur "OK".

- Sélectionnez le niveau d'autorisation : choisissez "Lecture/écriture" pour "Utilisateurs du domaine" et cliquez sur "Partager".

- (Facultatif) Dans l'onglet "Partage", cliquez sur "Partage avancé...".

- Cochez la case "Partager ce dossier" et cliquez sur "OK".

3. Configurer la stratégie de groupe :

- Dans le Gestionnaire de serveur, ouvrez le Gestionnaire de stratégie de groupe.

- Cliquez avec le bouton droit sur l'UO créée précédemment (isec-group) et sélectionnez "Créer un objet GPO dans ce domaine" et le lier ici. Donnez-lui un nom.

- Cliquez avec le bouton droit sur la GPO créée et sélectionnez "Modifier".

4. Configurer le mappage de lecteur :

- Dans "Configuration utilisateur", allez à "Préférences", puis "Paramètres Windows". Cliquez avec le bouton droit sur "Mappages de lecteurs" et sélectionnez "Nouveau" > "Lecteur mappé".

- Dans l'onglet "Général", ajoutez l'emplacement \\GROUP-WSERVER-M\Groupe, cochez "Reconnecter", nommez-le "Groupe" et attribuez la lettre G: au lecteur.

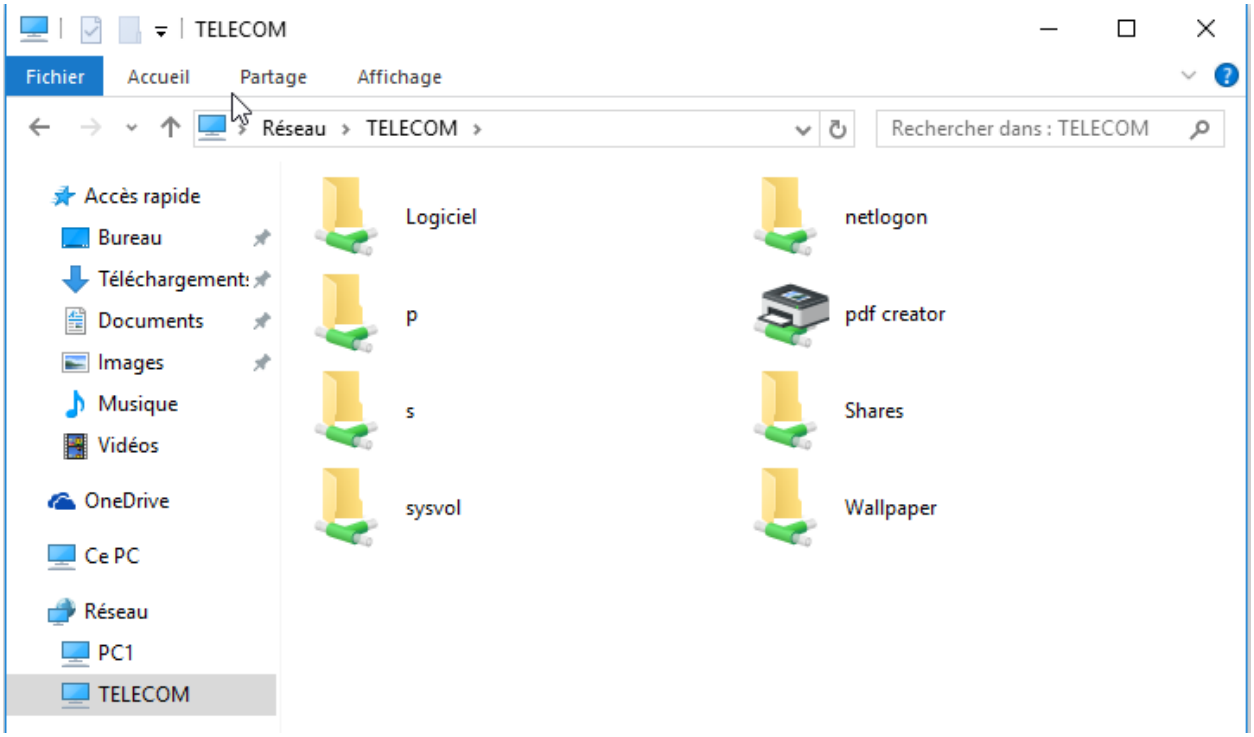
- Dans "Masquer/Afficher ce lecteur", cochez "Afficher ce lecteur" et "Afficher tous les lecteurs".

- Dans l'onglet "Commun", cochez "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".

5. Finaliser la configuration :

- Cliquez sur "OK" et faites un clic droit sur la GPO pour sélectionner "Appliquer".

Ces étapes permettront d'établir le partage de dossiers et de le rendre accessible à tous les utilisateurs des services du groupe iSEC.



Partage Telecom

Le partage Telecom se fait de la même façon que le paragraphe précédent 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 Telecom

Partage par service

Le partage par service permet de créer un répertoire partagé accessible sous la forme d'un lecteur mappé avec la lettre S: pour "Share". Chaque répertoire est uniquement visible par le service qui lui est attribué, à l'exception du service de direction qui peut voir tous les dossiers partagés. Voici les étapes à suivre pour chaque dossier partagé à créer:

1.Créer le dossier partagé : Sur le contrôleur de domaine, créez le dossier dans C:\Shares\Services\ en utilisant le nom correspondant au service.

2. Partager le dossier:

- Faites un clic droit sur le dossier créé.
- Sélectionnez "Propriétés".
- Dans l'onglet "Partage", cliquez sur "Partager...".
- Dans la fenêtre, choisissez "Rechercher des personnes...".
- Ajoutez le nom du groupe dans le champ de texte. Pour cela, tapez le nom de l'UO correspondant au service (par exemple : service-rh pour le service Ressources humaines) et cliquez sur "OK".
- Définissez le niveau d'autorisation sur "Lecture/écriture" pour le groupe ajouté précédemment, puis cliquez sur "Partager".
- Répétez cette étape pour l'UO du service de direction afin qu'il ait accès à tous les dossiers partagés.
- (Facultatif) Dans l'onglet "Partage", cliquez sur "Partage avancé...".
- Cochez la case "Partager ce dossier" et cliquez sur "OK".
- Notez le nom du partage dans l'onglet "Partage" sous "Chemin réseau", car il sera utile pour les étapes suivantes.

3. Configurer la stratégie de groupe :

- Ouvrez le Gestionnaire de serveur, puis le Gestionnaire de stratégie de groupe.
- Dans l'UO du service, faites un clic droit et sélectionnez "Créer un objet GPO dans ce domaine" et le lier ici. Donnez-lui un nom.

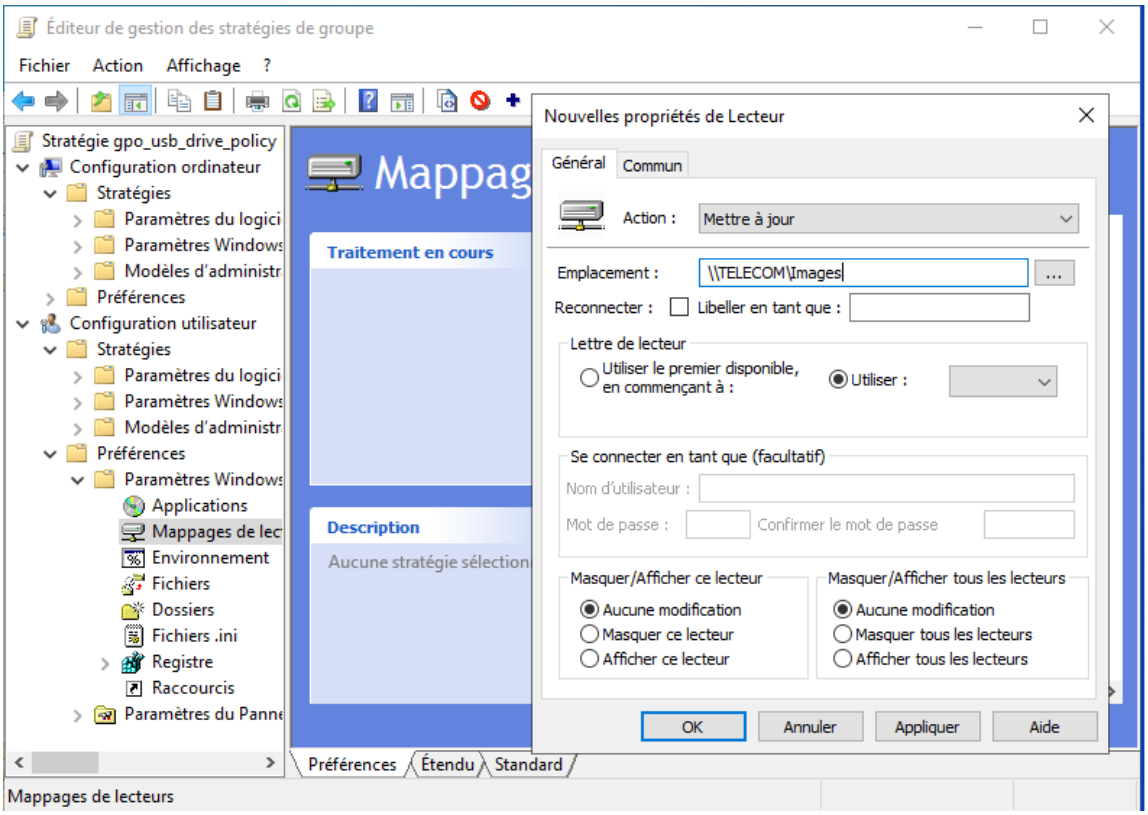
4. Modifier la GPO :

- Cliquez avec le bouton droit sur la GPO créée et sélectionnez "Modifier".

5. Configurer le mappage de lecteur :

- Dans "Configuration utilisateur", allez à "Préférences", puis "Paramètres Windows". Cliquez avec le bouton droit sur "Mappages de lecteurs" et choisissez "Nouveau" > "Lecteur mappé".

- Dans l'onglet "Général", ajoutez l'emplacement avec le nom du partage que vous avez noté précédemment, soit \\GROUP-WSERVER-M\Nom_de_votre_partage. Cochez "Reconnecter", nommez-le "Groupe", et assignez-lui la lettre G:. Dans "Masquer/Afficher ce lecteur", cochez "Afficher ce lecteur" et "Afficher tous les lecteurs".



6. Finaliser la configuration:

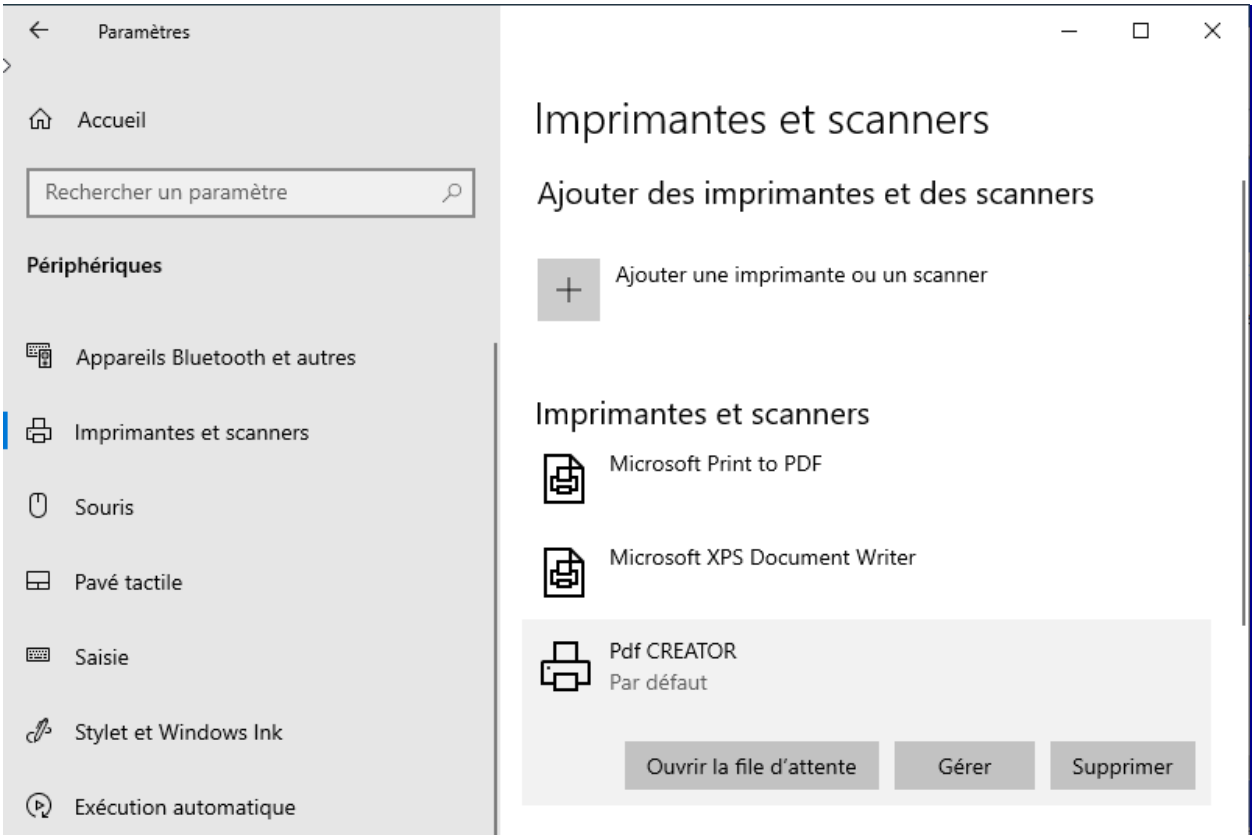
- Dans l'onglet "Commun", cochez "Arrêter le traitement des éléments de cette extension si une erreur survient", "Exécuter dans le contexte de sécurité de l'utilisateur connecté" et "Supprimer l'élément lorsqu'il n'est plus appliqué".

- Cliquez sur "OK", puis faites un clic droit sur la GPO et sélectionnez "Appliquer".

Imprimantes

PDFCreator a été installé sur le serveur principal pour simuler une imprimante distante accessible à tous les utilisateurs. Voici les étapes à suivre pour le configurer :

1. Installer PDFCreator : Une fois installé sur le serveur, modifiez les propriétés de sauvegarde afin d'enregistrer les fichiers PDF dans le dossier de votre choix et sous le nom souhaité.



2. Partager l'imprimante:

- Ouvrez le Gestionnaire de périphériques et d'imprimantes.

- Faites un 66clic droit sur l'imprimante PDFCreator et cochez la case "Partager cette imprimante" dans l'onglet "Partage".

3. Récupérer le chemin de partage: Notez le chemin de partage indiqué dans l'onglet "Partage", car il sera nécessaire pour les étapes suivantes.

4. Configurer la stratégie de groupe:

- Ouvrez le Gestionnaire de serveur, puis le Gestionnaire de stratégie de groupe.

- Dans l'UO du groupe, faites un clic droit et sélectionnez "Créer un objet GPO dans ce domaine" et le lier ici. Donnez-lui un nom.

5. Modifier la GPO:

- Cliquez avec le bouton droit sur la GPO créée et sélectionnez "Modifier".

6. Ajouter l'imprimante partagée :

- Dans "Configuration utilisateur", allez à "Préférences", puis "Paramètres du Panneau de configuration". Faites un clic droit sur "Imprimantes" et choisissez "Imprimante" > "Imprimante partagée".

- Ajoutez le chemin de partage noté précédemment dans le champ "Chemin de partage" et cochez la case "Définir en tant qu'imprimante par défaut".

7. Configurer les paramètres communs:

- Dans l'onglet "Commun", cochez les trois premières cases.

8. Activer la GPO : N'oubliez pas d'activer la GPO en cliquant avec le bouton droit dessus et en sélectionnant "Appliquer".

Ces étapes permettront à tous les utilisateurs d'accéder à l'imprimante PDFCreator comme s'il s'agissait d'une imprimante distante.

Répertoire personnel distant

Chaque utilisateur du domaine a son répertoire personnel "Mes Documents" déplacé sur le contrôleur de domaine principal, dans un dossier "Home" où se trouve un sous-dossier à leur nom. Voici comment configurer cette structure :

1. Configurer le partage : Créez le dossier contenant les documents des utilisateurs. Faites un clic droit sur ce dossier et sélectionnez "Propriétés".

2. Partager le dossier:

- Dans l'onglet "Partage", cliquez sur le bouton "Partager..." et partagez-le avec tous les utilisateurs en leur accordant des droits en lecture et écriture.

3. Partage avancé :

- Toujours dans l'onglet "Partage", cliquez sur "Partage avancé...".

- Cochez la case "Partager ce dossier" et cliquez sur "OK".

4. Configurer la stratégie de groupe :

- Ouvrez le Gestionnaire de serveur, puis le Gestionnaire de stratégie de groupe.

- Dans l'UO du groupe, faites un clic droit et sélectionnez "Créer un objet GPO dans ce domaine" et le lier ici. Nommez-le.

5. Modifier la GPO:

- Cliquez avec le bouton droit sur la GPO créée et sélectionnez "Modifier".

6. Configurer la redirection des dossiers :

- Dans "Configuration utilisateur", allez à "Paramètres Windows", puis "Redirection de dossiers". Faites un clic droit sur "Documents" dans la liste de droite et sélectionnez "Propriétés".

7. Définir l'emplacement du dossier cible :

- Dans "Emplacement du dossier cible", sélectionnez "Créer un dossier pour chaque utilisateur sous le chemin d'accès racine". Ajoutez le chemin d'accès \\GROUP-WSERVER-M\Home.

8. Configurer les paramètres :

- Dans l'onglet "Paramètres", cochez les cases "Accorder à l'utilisateur des droits exclusifs sur Documents", "Déplacer le contenu de Documents vers le nouvel emplacement" et "Conserver le dossier dans le nouvel emplacement".

9. Activer la GPO : N'oubliez pas d'activer la GPO en cliquant avec le bouton droit dessus et en sélectionnant "Appliquer".

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 il est nécessaire de respecter les étapes suivantes

1. Modifier la GPO Default Domain Policy :

- Localisez la GPO "Default Domain Policy" dans les Objets de stratégie de groupe de la forêt isecgroup.local pour le groupe iSEC ou isectelecom.local.

- Faites un clic droit dessus et sélectionnez "Modifier".

2. Configurer les paramètres de mot de passe :

- Dans l'arborescence, accédez à : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégie de mot de passe.

3. Définir la durée de vie maximale du mot de passe:

- Faites un clic droit sur "Durée de vie maximale du mot de passe" et sélectionnez "Propriétés".

- Cochez la case "Définir ce paramètre de stratégie" et réglez l'expiration sur 90 jours.

4. Configurer les exigences de complexité du mot de passe :

- Faites un clic droit sur "Le mot de passe doit respecter des exigences de complexité" et sélectionnez "Propriétés".

- Cochez la case "Définir ce paramètre de stratégie" et sélectionnez "Désactivé".

5. Définir la longueur minimale du mot de passe :

- Faites un clic droit sur "Longueur minimale du mot de passe" et sélectionnez "Propriétés".

- Cochez la case "Définir ce paramètre de stratégie" et fixez la longueur minimale à 8 caractères.

6. Configurer la stratégie de verrouillage du compte :

- Dans l'arborescence, accédez à "Stratégie de verrouillage du compte".

7. Définir le seuil de verrouillage du compte:

- Faites un clic droit sur "Seuil de verrouillage du compte" et sélectionnez "Propriétés".

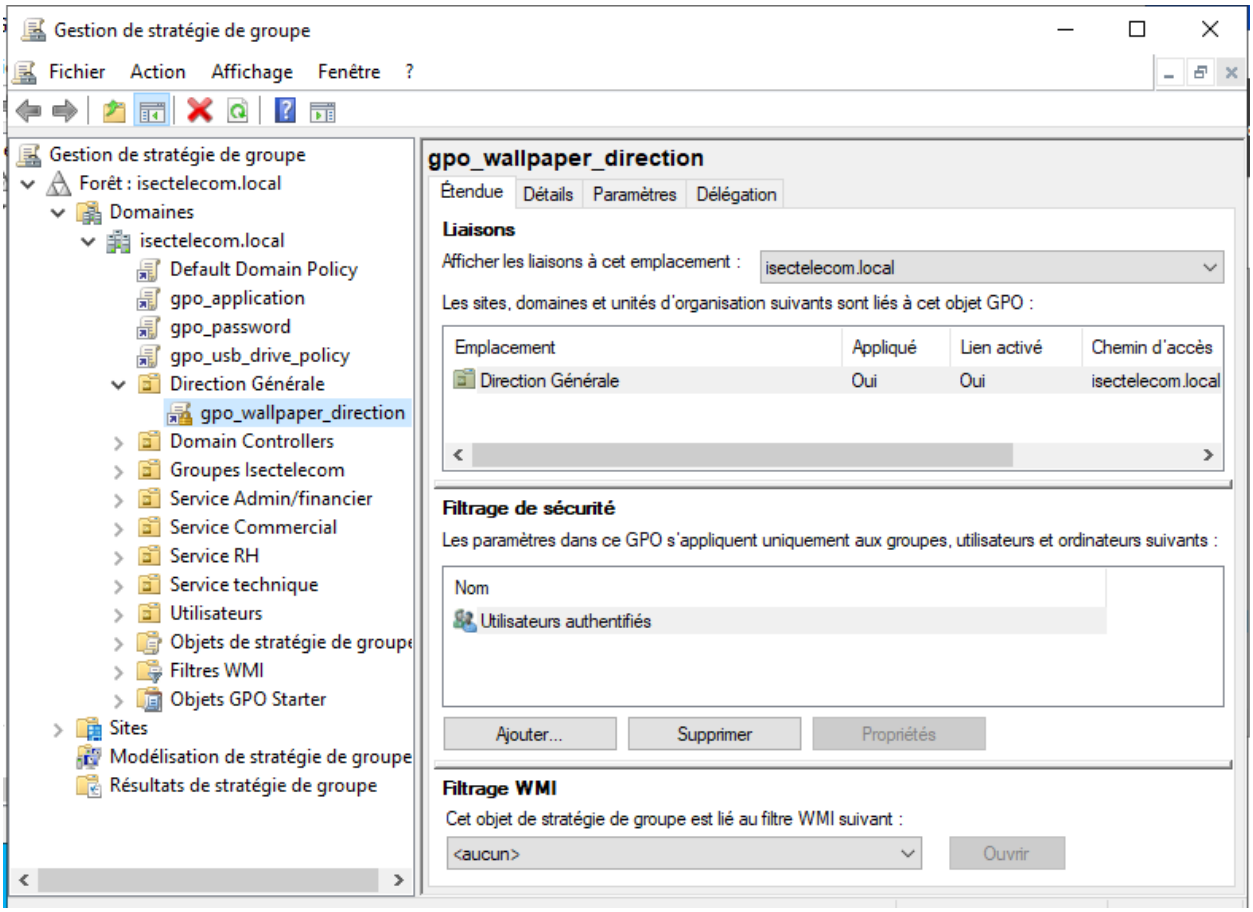
- Cochez la case "Définir ce paramètre de stratégie" et définissez le nombre de tentatives à 3

8. Activer la GPO :

- N'oubliez pas d'activer la GPO en faisant un clic droit dessus et en sélectionnant "Appliquer".

Ou en tapant gpupdate /force.

Ces étapes permettront d'assurer une gestion efficace des mots de passe et de la sécurité des comptes utilisateurs.



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.

Fonds d'écran

Chaque groupe a 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 , nous avons répéter les procédures suivantes pour chaque UO de chaque service et sur les deux groupes

Pour appliquer un fond d'écran spécifique à chaque groupe et service, suivez les étapes ci-dessous pour chaque Unité d'Organisation (UO) des services et pour les deux groupes :

1. Configurer le partage du dossier de fonds d'écran :

- Créez un dossier pour les papiers peints. Faites un clic droit sur ce dossier et sélectionnez "Propriétés".

2. Partager le dossier :

- Dans l'onglet "Partage", cliquez sur le bouton "Partager...".

- Dans la fenêtre, sélectionnez "Rechercher des personnes...".

- Ajoutez le nom du groupe dans le champ de texte et cliquez sur "OK".

- Sélectionnez le niveau d'autorisation sur "Lecture/écriture" pour le groupe précédemment créé, puis cliquez sur "Partager".

3. Partage avancé (facultatif) :

- Toujours dans l'onglet "Partage", cliquez sur "Partage avancé...".

- Cochez la case "Partager ce dossier" et cliquez sur "OK".

4. Créer une GPO pour chaque UO:

- Faites un clic droit sur l'UO et sélectionnez "Créer un objet GPO dans ce domaine", puis liez-le ici. Nommez la GPO.

5. Modifier la GPO :

- Cliquez avec le bouton droit sur la GPO créée et sélectionnez "Modifier".

6. Configurer le papier peint du bureau:

- Dans "Configuration utilisateur", allez à "Stratégies", puis "Modèles d'administration", et sélectionnez "Bureau". Cliquez sur "Bureau".

- Faites un clic droit sur "Papier peint du Bureau" et sélectionnez "Modifier".

7. Activer la configuration :

- Cochez la case "Activé".

8. Définir le nom du papier peint:

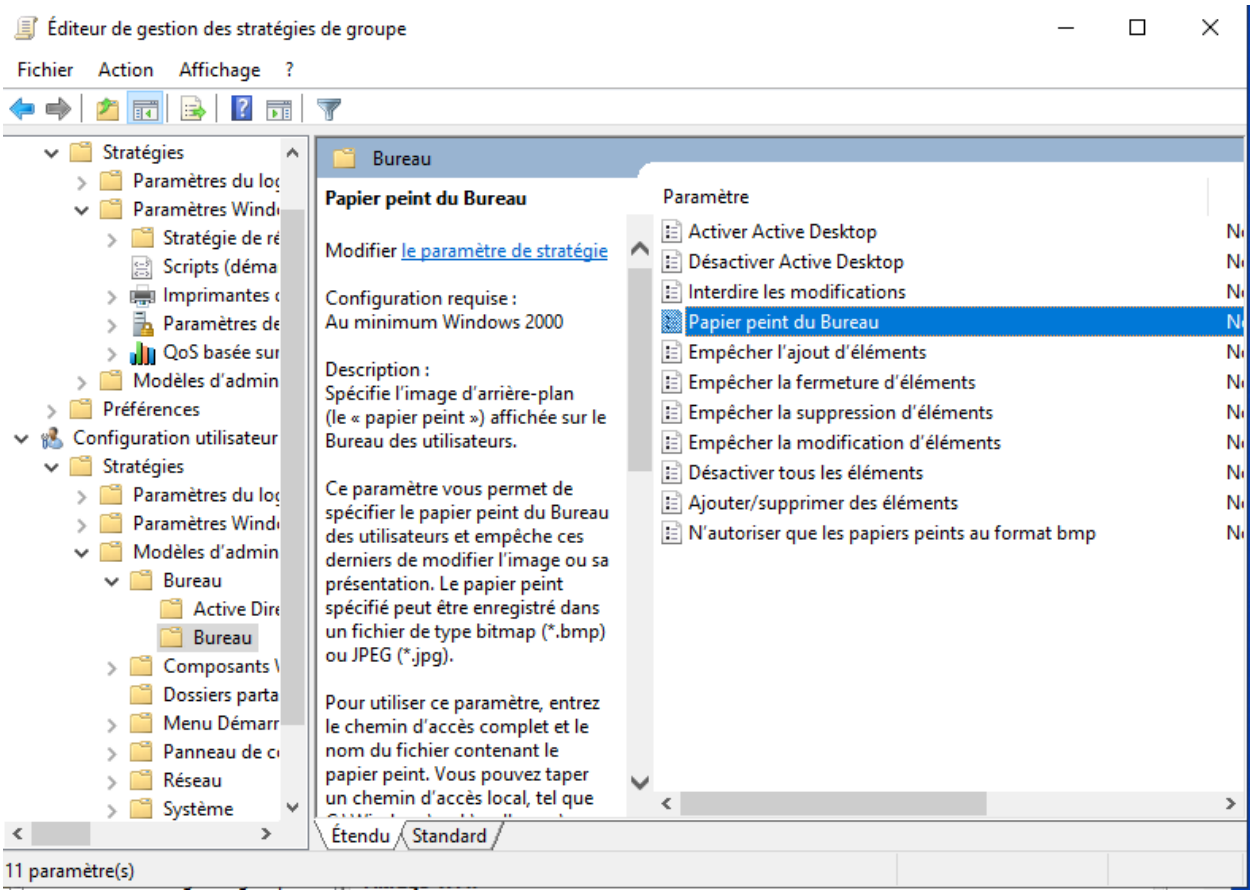
- Dans "Nom du papier peint", ajoutez le chemin de partage suivi du nom du fichier JPG (par exemple : \\GROUP-WSERVER-M\Wallpapers\Servicerh.jpg).

- Dans "Style du papier peint", sélectionnez "Ajuster".

9. Activer la GPO:

- N'oubliez pas d'activer la GPO en cliquant avec le bouton droit dessus et en sélectionnant "Appliquer".

Répétez ces étapes pour chaque UO de chaque service et pour les deux groupes afin de garantir que tous les utilisateurs aient le fond d'écran approprié.



ISEC TELECOM

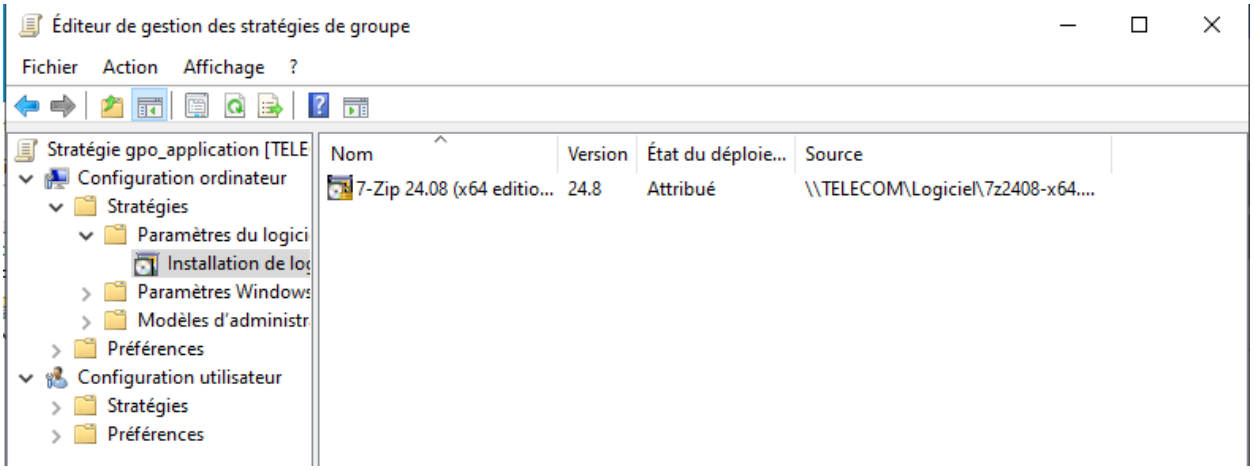
Service Technique

Logiciel 7Zip

Pour installer le logiciel de compression/décompression 7Zip sur tous les postes, suivez les étapes ci-dessous :

1. Configurer le partage du dossier d'installation:

- Créez un dossier contenant les fichiers d'installation de 7Zip. Faites un clic droit sur ce dossier et sélectionnez "Propriétés".



2. Partager le dossier :

- Dans l'onglet "Partage", cliquez sur le bouton "Partager...".

- Ajoutez le nom du groupe dans le champ de texte, tapez "Utilisateurs du domaine", puis cliquez sur "OK".

- Sélectionnez le niveau d'autorisation "Lecture/écriture" pour le groupe ajouté précédemment et cliquez sur "Partager".

3. Partage avancé (facultatif):

- Toujours dans l'onglet "Partage", cliquez sur "Partage avancé...".

- Cochez la case "Partager ce dossier" et cliquez sur "OK".

4. Configurer la stratégie de groupe :

- Ouvrez le Gestionnaire de serveur, puis le Gestionnaire de stratégie de groupe.

- Dans la forêt, faites un clic droit et sélectionnez "Créer un objet GPO dans ce domaine" et liez-le ici. Nommez la GPO.

5. Modifier la GPO :

- Cliquez avec le bouton droit sur la GPO créée et sélectionnez "Modifier".

6. Déployer le logiciel :

- Dans "Configuration ordinateur", allez à "Stratégie", puis "Paramètres du logiciel". Faites un clic droit sur "Installation de logiciel" et sélectionnez "Nouveau" > "Package".

- Sélectionnez le fichier .msi d'installation de 7Zip et cochez la case "Attribué" pour le type de déploiement.

7. Activer la GPO:

- N'oubliez pas d'activer la GPO en cliquant avec le bouton droit dessus et en sélectionnant "Appliquer".

IX. Approbation

Une relation d’approbation unidirectionnelle nous a été démandé dans le projet afin que les utilisateur de la maison mère puisse accéder à la filiale Télécom, voici les étapes que nous avons mis en œuvres :

Étape 1: Identification des Contrôleurs de Domaine

Nous avons identifié les deux contrôleurs de domaine que nous voulons connecter pour établir une relation d'approbation.

Étape 2: Ouverture de la Console Gestionnaire des Utilisateurs et des Ordinateurs

Nous avons ouvert la console "Gestionnaire des Utilisateurs et des Ordinateurs" sur l'un des contrôleurs de domaine en utilisant la commande `dsa.msc`.

Étape 3: Création de la Relation d'Approbation

1. Nous avons cliqué avec le bouton droit sur le domaine pour lequel nous voulons établir la relation d'approbation, puis sélectionné "Propriétés".

2. Dans les propriétés du domaine, nous avons accédé à l'onglet "Relations d'approbation" et cliqué sur "Nouvelle relation d'approbation".

Étape 4: Configuration de la Relation d'Approbation

1. L'assistant de configuration de la relation d'approbation s'est ouvert et nous avons cliqué sur "Suivant" pour commencer.

2. Nous avons choisi le type d'approbation souhaité : bidirectionnel ou unidirectionnel, en fonction de nos besoins.

Étape 5: Sélection du Domaine Partenaire

1. Nous avons saisi le nom du domaine du contrôleur de domaine partenaire avec lequel nous voulons établir la relation d'approbation.

2. Nous avons sélectionné le type d'approbation : réciproque ou unidirectionnelle.

3. Nous avons fourni les informations d'identification d'un compte autorisé à établir la relation.

Étape 6: Validation et Finalisation

1. En suivant les instructions de l'assistant, nous avons finalisé la configuration de la relation d'approbation.

2. Une fois la relation d'approbation établie, nous avons testé la connectivité entre les contrôleurs de domaine pour vérifier que la communication fonctionnait correctement.

Étape 7: Répétition du Processus

Nous avons répété les étapes ci-dessus sur l'autre contrôleur de domaine pour établir une relation d'approbation bidirectionnelle complète.

X. Supervision

La supervision d'une infrastructure informatique consiste à vérifier régulièrement la santé des zones critiques afin d'assurer leur disponibilité. C'est un enjeu essentiel, car cela permet de détecter rapidement les pannes et d'intervenir efficacement.

Dans notre infrastructure, qui comprend 2 serveurs et 5 machines virtuelles, nous avons choisi Zabbix comme outil de supervision. Zabbix est un système complet qui utilise le protocole SNMP pour surveiller l'état des équipements. Nous avons opté pour ce logiciel en raison de sa convivialité et de sa capacité à fonctionner de manière décentralisée.

Zabbix propose une architecture décentralisée, idéale pour gérer un large parc de machines. Cette architecture comprend un serveur central qui stocke les données et offre une interface d'administration web, ainsi que des agents Zabbix ou des serveurs Proxy, chargés de collecter les données des serveurs à l'aide de divers plugins.

Installation

Serveur central

Pour installer Zabbix sur une nouvelle machine virtuelle, voici un guide étape par étape. L'installation de Zabbix peut se faire de manière similaire à celle de Centreon, avec quelques différences dans la configuration et les composants à installer.

Étapes d'Installation de Zabbix :

a. Installer le Dépôt Zabbix
Documentation
Désactivez les paquets Zabbix fournis par EPEL, si vous l'avez installé. Éditez le fichier /etc/yum.repos.d/epel.repo et ajoutez la ligne suivante :

[epel]

...

excludepkgs=zabbix*

Ensuite, procédez à l'installation du dépôt Zabbix :

 # rpm -Uvh https://repo.zabbix.com/zabbix/7.0/alma/9/x86_64/zabbix-release-latest.el9.noarch.rpm

 # dnf clean all

b. Installer le Serveur, l'Interface et l'Agent Zabbix
Pour installer les composants nécessaires, exécutez la commande suivante :

 # dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-policy zabbix-agent

c. Créer la Base de Données Initiale
Documentation
Assurez-vous que votre serveur de base de données est opérationnel. Exécutez les commandes suivantes sur votre hôte de base de données :

 # mysql -uroot -p

motdepasse

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;

mysql> create user 'zabbix'@'localhost' identified by 'motdepasse';

mysql> grant all privileges on zabbix.* to 'zabbix'@'localhost';

mysql> set global log_bin_trust_function_creators = 1;

mysql> quit;

Sur l'hôte du serveur Zabbix, importez le schéma et les données initiales. Vous serez invité à entrer le mot de passe que vous venez de créer :

 # zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix

Après l'importation du schéma de base de données, désactivez l'option log_bin_trust_function_creators :

 # mysql -uroot -p

motdepasse

mysql> set global log_bin_trust_function_creators = 0;

mysql> quit;

d. Configurer la Base de Données pour le Serveur Zabbix
Éditez le fichier /etc/zabbix/zabbix_server.conf et définissez :

DBPassword=motdepasse

e. Démarrer les Processus du Serveur et de l'Agent Zabbix
Démarrez les processus du serveur et de l'agent Zabbix, et configurez-les pour qu'ils démarrent au démarrage du système :

 # systemctl restart zabbix-server zabbix-agent httpd php-fpm

 # systemctl enable zabbix-server zabbix-agent httpd php-fpm

f. Ouvrir la Page Web de l'Interface Zabbix
L'URL par défaut pour l'interface Zabbix lorsque vous utilisez le serveur web Apache est :

http://host/zabbix

Installation du Poller

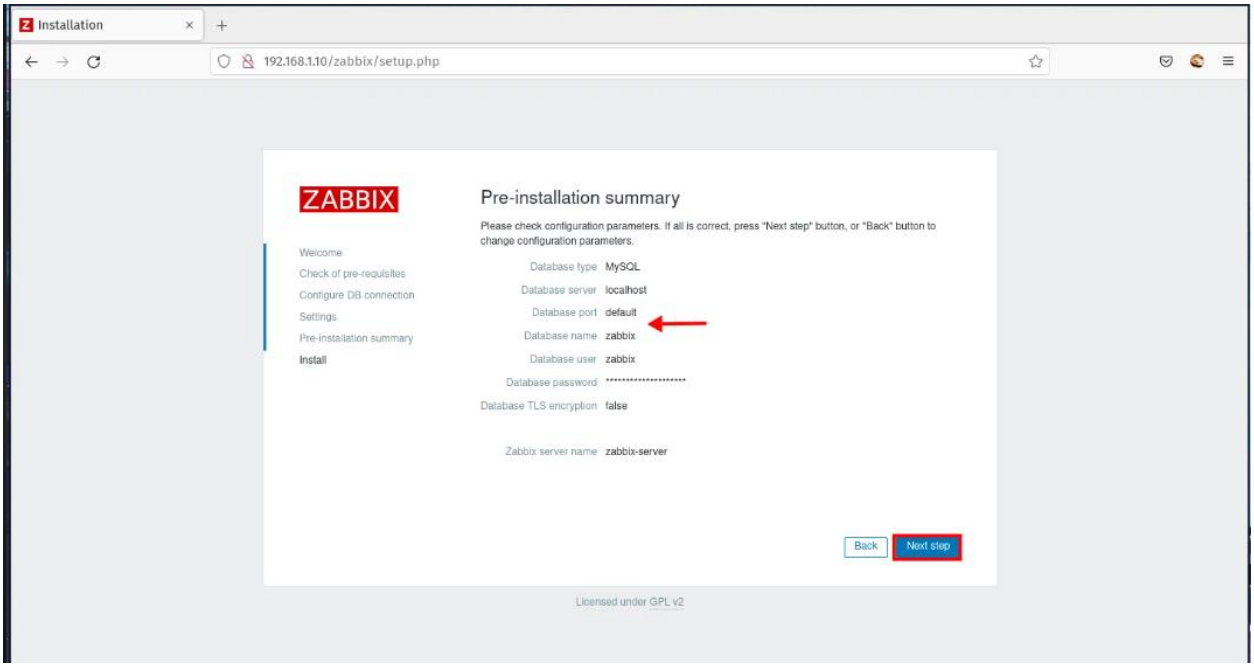
Pour installer un Poller Zabbix, suivez une procédure similaire à celle du serveur central, mais lors du choix du type de serveur, sélectionnez Zabbix Poller. Il n’y a pas d’étape d'installation web pour le poller, car il s'agit d'un composant qui fonctionne en arrière-plan.

Configuration

Plugins

Voici une procédure de configuration des plugins dans Zabbix:

Configuration des Plugins dans Zabbix



1. Accéder à l'interface Zabbix:

- Connecte-toi à l'interface web de Zabbix avec tes identifiants.

2. Vérifier les prérequis :

- Assure-toi que ton instance Zabbix est correctement installée et que tous les services nécessaires (serveur Zabbix, agent Zabbix) sont en cours d'exécution.

3. Installer des plugins:

- Les plugins pour Zabbix peuvent être sous forme d’éléments externes ou de templates. Tu peux les télécharger depuis des dépôts GitHub ou le site de Zabbix.

4. Accéder à la section Configuration :

- Va dans Configuration > Templates pour gérer les modèles de monitoring.

5. Importer des templates :

- Si tu as téléchargé des templates (par exemple, pour Linux, Windows, ou d'autres services spécifiques), tu peux les importer :

  - Clique sur Importer dans l'onglet Templates.

  - Télécharge le fichier XML du template.

6. Configurer les hôtes :

- Dans Configuration > Hosts, sélectionne l'hôte sur lequel tu souhaites appliquer les plugins.

- Clique sur Link new templates et sélectionne les templates que tu viens d'importer.

7. Activer des éléments spécifiques:

- Une fois les templates liés, vérifie les éléments qui seront surveillés. Va dans Configuration > Hosts et sélectionne l'hôte.

- Clique sur Items pour voir les éléments configurés par le template. Assure-toi qu'ils sont activés.

8. Vérifier les autorisations :

- Assure-toi que les agents Zabbix sur les hôtes disposent des permissions nécessaires pour exécuter les commandes des plugins.

9. Tester le fonctionnement :

- Va dans Monitoring > Latest Data pour vérifier que les données remontent correctement depuis les hôtes surveillés.

10. Configurer des déclencheurs (facultatif) :

- Si des éléments critiques sont surveillés, configure des déclencheurs dans Configuration > Hosts> Triggers pour être alerté en cas de problèmes.

Ajouter un hôte

Voici comment ajouter un hôte dans Zabbix :

Ajout d'un hôte dans Zabbix

1.Accéder à la section Configuration :

- Connecte-toi à l'interface web de Zabbix et va dans Configuration > Hosts.

2. Ajouter un nouvel hôte:

- Clique sur le bouton Create host pour ajouter un nouvel hôte.

3. Nommer l'hôte :

- Dans le champ **Host name**, entre un nom unique représentant l'hôte. Tu peux également ajouter un Visible name si tu souhaites un nom d'affichage différent.

4.Ajouter l'adresse IP :

- Dans la section Interfaces, clique sur Add et renseigne l'adresse IP de l'hôte dans le champ IP address. Sélectionne le type d'interface (généralement "Agent").

5. Configurer SNMP (si applicable) :

- Si tu utilises SNMP, dans la section Interfaces, choisis le type SNMP et indique la communauté SNMP ainsi que la version SNMP (v1, v2c, ou v3).

6. Définir le groupe d'hôtes :

- Dans la section Groups, sélectionne un groupe existant ou crée un nouveau groupe pour organiser tes hôtes.

7. Ajouter des templates:

- Dans la section Templates, clique sur Select et choisis les templates que tu souhaites appliquer à cet hôte pour activer la surveillance appropriée.

8. Configurer les options de vérification :

- Dans la section Macros, tu peux ajouter des macros personnalisées si nécessaire, bien que cela ne soit pas obligatoire.

9. Configurer la fréquence de vérification :

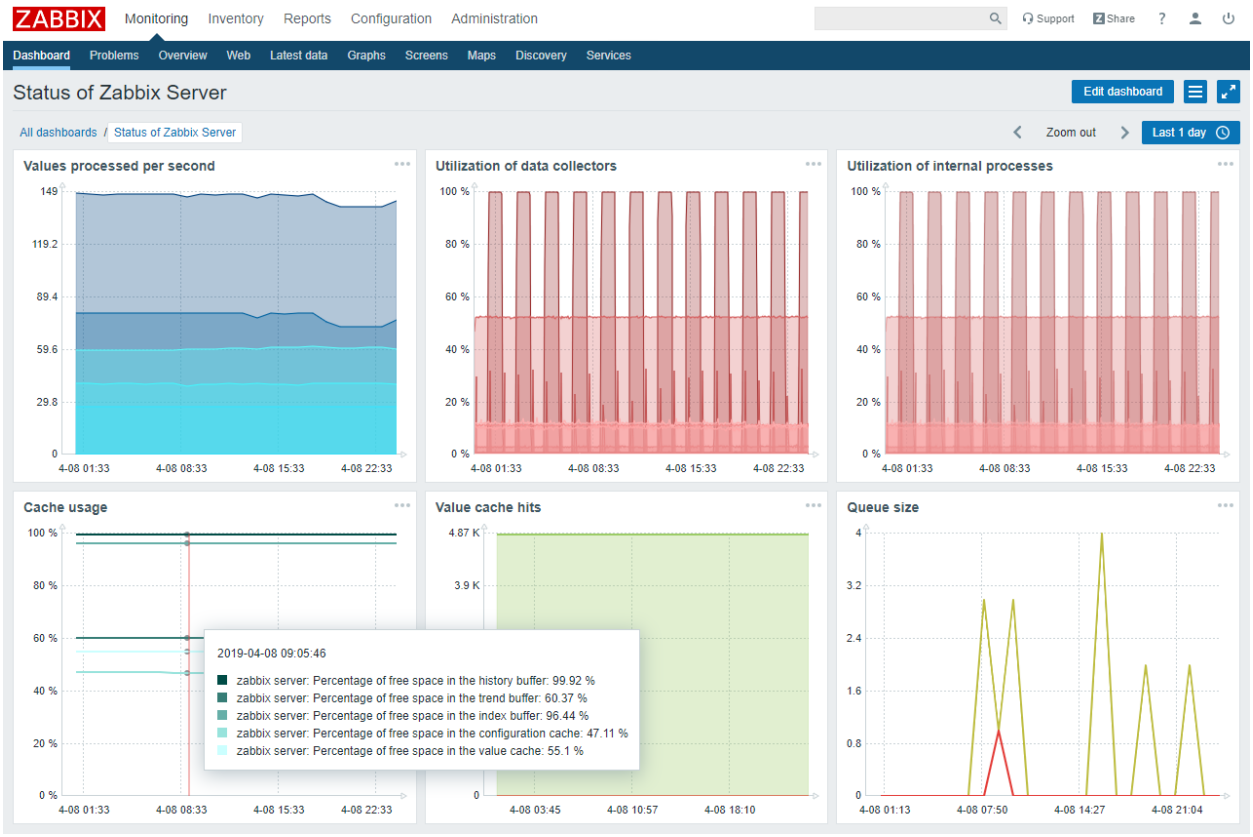
- Par défaut, Zabbix utilise des intervalles prédéfinis pour le polling. Tu peux ajuster la fréquence de vérification des éléments dans les templates que tu as liés à l'hôte.

10. Enregistrer l'hôte:

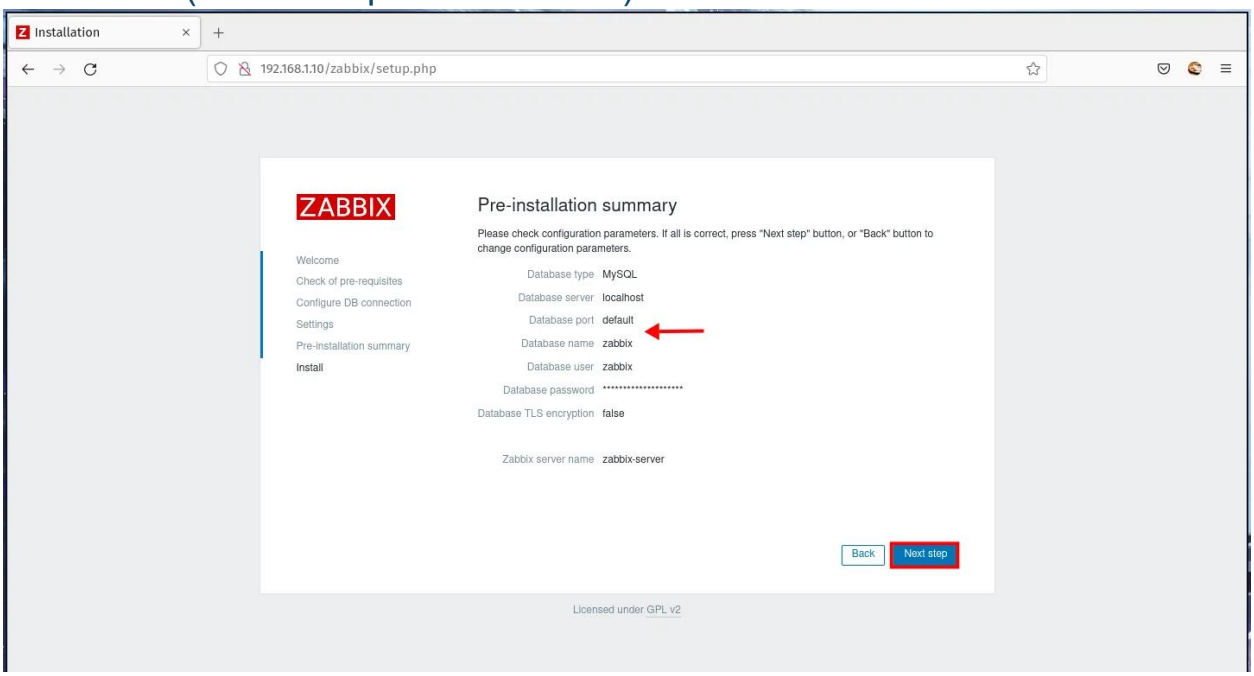
- Une fois toutes les informations saisies, clique sur le bouton Add en bas de la page pour enregistrer l'hôte.

Vérification

- Une fois l'hôte ajouté, tu peux vérifier son état dans Monitoring > Hosts pour t'assurer qu'il est actif et que les données sont collectées correctement.



XI. PRA (Plan de reprises d'activité)



Voici les actions concrètes à entreprendre pour assurer un plan de reprise d'activité solide pour notre projet réseau d'annuaire Windows et de supervision avec Zabbix :

1. Identification des Risques

- Après avoir réalisé une analyse détaillée des risques détaillée pour identifier les menaces il en ressort comme risque dans l'ordre croissant :

Les Pannes matérielles,

Les Pannes logicielles,

Les Attaques par ransomware,

Les Perte de connectivité réseau.

2. Stratégie de Sauvegarde

- Mettre en place des sauvegardes régulières des bases de données de l'annuaire Windows et des configurations de Zabbix, en les stockant sur des supports externes sécurisés.

- Automatiser le processus de sauvegarde pour garantir la cohérence des données.

3. Documentation et Procédures

- Ce document est un manuel de reprise d'activité détaillé comprenant les étapes spécifiques pour l'ensemble des configurations de l'annuaire Windows et Zabbix en cas de sinistre.

4. Infrastructure de Secours

- Nous avons mis en place un site de secours ou un centre de données alternatif au niveau de la Maison mère capable de prendre en charge les opérations critiques en cas d'indisponibilité du serveur principal.

- Nous avons assuré la synchronisation en temps réel ou quasi-réel des données entre les sites principal et de secours.

5. Tests et Exercices

- Planifier et réaliser des exercices de simulation de sinistres réguliers pour évaluer la préparation de l'équipe et l'efficacité du plan de reprise d'activité.

- Documenter les résultats des exercices et apporter des améliorations en conséquence.

6. Sensibilisation et Formation

- Former régulièrement le personnel sur les procédures de reprise d'activité et les tâches assignées en cas d'incident.

- Organiser des sessions de sensibilisation pour garantir que chaque membre de l'équipe comprenne son rôle et ses responsabilités.

7. Surveillance Continue

- Nous avons mis en place des outils de surveillance avancés pour surveiller en permanence l'état de l'infrastructure, les performances du système et la disponibilité des services sous zabbix.

- Nous avons configuré des alertes pour informer rapidement l'équipe en cas de défaillance ou de comportement anormal.

8. Révision et Amélioration

- Planifier des revues régulières du plan de reprise d'activité pour l'actualiser en fonction des changements dans l'infrastructure IT et des leçons apprises.

- Implémenter un processus d'amélioration continue pour renforcer la résilience du système face aux nouveaux défis.

XII. REFERENCES

https://fr.search.yahoo.com/search?fr=mcafee&type=E210FR885G0&p=ZABBBIX

https://fr.search.yahoo.com/search;_ylt=AwrFBC.aJxFnroIC4qsk24lQ;_ylc=X1MDMTM1MTIxMTgxMgRfcgMyBGZyA21jYWZlZQRmcjIDc2ltdG9wBGdwcmlkA3NNUHlKaWRWVHY2YjlZUXNKQlE4U0EEbl9yc2x0AzAEbl9zdWdnAzEwBG9yaWdpbgNmci5zZWFyY2gueWFob28uY29tBHBvcwMwBHBxc3RyAwRwcXN0cmwDMARxc3RybAMxNgRxdWVyeQNBY3RpdmUlMjBkaXJlY3RvcnkEdF9zdG1wAzE3MjkxNzc1MzM-?p=Active+directory&fr=mcafee&type=E210FR885G0&fr2=sb-top

https://fr.search.yahoo.com/search;_ylt=AwrFBC.9JxFnH5QCAn0k24lQ;_ylc=X1MDMTM1MTIxMTgxMgRfcgMyBGZyA21jYWZlZQRmcjIDc2ltdG9wBGdwcmlkA1kuOGRPM1BqU182S3VEMzFrUGRkNkEEbl9yc2x0AzAEbl9zdWdnAzAEb3JpZ2luA2ZyLnNlYXJjaC55YWhvby5jb20EcG9zAzAEcHFzdHIDBHBxc3RybAMwBHFzdHJsAzE4BHF1ZXJ5A2NvbnRyb2xldXIlMjBkb21haW5lBHRfc3RtcAMxNzI5MTc3NTU5?p=controleur+domaine&fr=mcafee&type=E210FR885G0&fr2=sb-top