

Enzo DUGELAY

Rapport d'alternance

Olivier FERRÉ - Tuteur



Licence Responsable de Projets Informatiques 2023 – 2024

École Normale Supérieure

Support et Gestionnaire de parc informatique

Table des matières

Table des matières	2
1. Remerciements	3
2. Présentation personnelle.....	4
Introduction	4
Parcours scolaire.....	5
Mon CV	6
3. Présentation de l'ENS.....	7
4. Présentation de la DSI et du service SGP (Support et Gestion de Parc)	9
Outils utilisés.....	11
5. Présentation de mes missions	12
6. Projet d'entreprise	13
Présentation du projet.....	13
Contexte du projet.....	13
Objectifs et Problématique du projet.....	14
Cahier des Charges :	14
Solution Proposée.....	15
Présentation de l'existant.....	17
Présentation de la solution.....	18
Ressources temporelles et budgétaires du projet	24
Risques et gestion des risques.....	25
Utilisation du projet.....	26
Bénéfices du projet.....	30
Améliorations futures du projet	31
Conclusion du projet.....	32
7. Synthèse de l'alternance.....	33
Retour d'expérience	33
8. Projet de carrière	34
9. Glossaire technique et liens sources.....	35
10. Annexes	37

1. Remerciements

Premièrement, je souhaite remercier l'équipe de l'ENS de Lyon pour m'avoir accordé leur confiance et avoir facilité mon année d'apprentissage au sein de leur institution.

Ensuite, je tiens à adresser mes remerciements à mes collègues du service SGP. Leur soutien, leur confiance et leurs conseils ont été une aide précieuse tout au long de ma formation :

- ➔ Serge Roux
- ➔ Olivier Ferré
- ➔ Loris Cambi
- ➔ Driss El Hassouni
- ➔ Yves Daoulatian
- ➔ Antonin Martin
- ➔ Bilal Boulahbal
- ➔ Colin Jasseron

De plus, je tiens à remercier les professeurs ainsi que la pédagogie de l'école Isitech pour leur enseignement. Leurs cours et leurs conseils m'ont permis d'acquérir les compétences nécessaires pour réussir cette année de formation.

2. Présentation personnelle

Introduction

Je m'appelle Enzo Dugelay, j'ai 21 ans et je suis ravi de vous présenter mon rapport d'alternance en tant qu'étudiant en Licence Responsable de Projet Informatique à l'école Isitech à Lyon 7. Mon alternance au sein de l'École Normale Supérieure de Lyon a débuté le lundi 18 septembre 2023 et se poursuivra jusqu'au vendredi 27 septembre 2024.

D'ailleurs, cette alternance a pour objectif principal de me permettre de mettre en pratique les connaissances acquises durant ma formation académique, ainsi que mes précédentes, et de développer des compétences spécifiques dans le domaine de la gestion de parc informatique. En outre, mon objectif a été de renforcer ma maîtrise des systèmes informatiques dans un contexte professionnel et de participer aux projets du service SGP (Support et Gestion de Parc). Mon but est également d'acquérir une expérience concrète qui m'aidera à atteindre mes objectifs professionnels à long terme dans le domaine de l'administration des systèmes et de la cybersécurité.

Parcours scolaire

Dans cette section, je vais présenter les différentes étapes de mon parcours scolaire et professionnel qui m'ont conduit à ma formation actuelle.

J'ai obtenu un BAC STI2D (Sciences et Technologies de l'Industrie et du Développement Durable) au lycée René Descartes à Saint-Genis-Laval, où j'ai au départ, développé un intérêt pour le développement ainsi que le réseau. Par la suite, j'ai poursuivi mes études avec un BTS Systèmes Numériques option Informatique et Réseaux au lycée Édouard Branly à Lyon 5, que j'ai complété en deux ans. Durant cette période, j'ai réalisé un stage d'un mois et demi en 2022 chez Vision Systems en tant qu'administrateur systèmes et réseaux. Ces deux années de BTS ont modifié ma vision, me poussant à orienter mes études vers l'administration des systèmes et la cybersécurité.

Actuellement, pour l'année 2023 / 2024, je suis inscrit à l'école Isitech à Lyon 7 pour le diplôme Licence RPI – Responsable de Projets Informatiques. De plus, je continue de me former dans le cadre d'une alternance où je travaille à l'ENS en tant que gestionnaire de parc informatique au sein du service SGP (Support et Gestion de Parc) de la DSI.

Mon CV



ENZO DUGELAY

06 58 68 35 83

enzo.dugelay1@gmail.com

Permis B en cours

LinkedIn : www.linkedin.com/in/enzo-dugelay1

GitHub : <https://github.com/enzo301>

En cours de formation Root-me :

[https://www.root-me.org/enzo_69?](https://www.root-me.org/enzo_69?lang=fr#dd612d3cc429ced4044e39c835b66f3d)

[lang=fr#dd612d3cc429ced4044e39c835b66f3d](https://www.root-me.org/enzo_69?lang=fr#dd612d3cc429ced4044e39c835b66f3d)

COMPÉTENCES COMPLÉMENTAIRES

- Réseau : VPN, SSH, VLAN
- Script : Bash, PowerShell
- Dockerisation
- Gestion de projet : GitHub, Git, Azure DevOps
- OS : Windows, Windows Server (AD), Ubuntu, Debian, MacOS
- Base de données : MySQL
- Développement : C++, Python, PHP, SQL, HTML, CSS

LOGICIELS UTILISÉS

- Analyse de logs : Graylog, Wireshark, MobaXterm
- Virtualisation : VMWare, VirtualBox
- Réseau : Cisco Packet Tracer
- Base de données MySQL : phpMyAdmin

CERTIFICATIONS

- Cybersécurité - Cisco (NetAcad) : Introduction to Cybersecurity IoT Fundamentals : IoT Security
- Réseaux - Cisco (NetAcad) : Cisco : CCNA Introduction to Networks

LANGUES

- Anglais : niveau B2
- Espagnol : niveau scolaire

CENTRES D'INTÉRÊT

- Musculation
- Football (8 ans en club niveau régional)
- Reptiles

CONSULTANT CYBERSÉCURITÉ

Disponibilité octobre 2024

Mobilité sur Lyon et 15km

Contrat d'apprentissage en 2 ans

4 semaines en entreprise / 2 semaines en cours

Compétences Cybersécurité

- Évaluation des risques de sécurité
- Formation des utilisateurs à la sécurité
- Analyse de logs
- Gestion de pare-feu
- Rédaction de scripts
- Déploiement et gestion de solutions de sécurité

Parcours professionnel

Alternance technicien support

ENS | Lyon - Debourg | Sept 2023 - Sept 2024 | 1 an

- Supervision 15-30 utilisateurs par jour : 99% de satisfaction
- Création d'un script PowerShell sous WinPE pour automatiser la récupération de profils et le déchiffrement BitLocker, temps économisé : 2h à 3h par semaine
- Participation aux campagnes de formation cybersécurité

Stage administrateur systèmes et réseaux

Vision Systems | Brignais | Mai 2022 - Juil 2022 | 1 mois et demi

- Administrer les serveurs et gérer le réseau
- Supervision 10-20 utilisateurs par jour : 99% de satisfaction
- Réinstallation de 80 postes (2 à 3 par jour)

FORMATIONS

Mastère Responsable de la Cybersécurité

CSB School | Charbonnière les b. | Oct 2024 - Sept 2026 | 2 ans

- Certifications à venir : CEH, EBIOS RM, ISO 2701, CISSP, Cloud engineer et Cloud security engineer

Licence Responsable de Projets Informatiques

Isitech | Lyon - Gerland | Oct 2023 - Sept 2024 | 1 an

- Projet mise en place d'un gestionnaire de logs Graylog

BTS Systèmes Numériques

Lycée Edouard Branly | Lyon 5 | Sept 2021 - Juil 2023 | 2 ans

- Gestion de baie de brassage (Switch, routeur, ESXi)
- Projet de développement analyse de logs en C++

RÉFÉRENCES PROFESSIONNELLES

- Olivier Ferré
Maître d'apprentissage ENS
olivier.ferre@ens-lyon.fr
- Jean-François Marquette
Professeur Lycée Edouard Branly
jean-francois.marquette@ac-lyon.fr

3. Présentation de l'ENS

L'École Normale Supérieure de Lyon, fondée en 1987, est une institution académique de premier plan en France. Reconnue pour son excellence en enseignement supérieur et en recherche, l'ENS de Lyon se distingue dans divers domaines, notamment les sciences humaines, les sciences sociales, les sciences fondamentales et appliquées.

L'établissement forme des chercheurs, enseignants, et cadres de haut niveau, favorisant l'interdisciplinarité, l'esprit critique, et la créativité. Elle propose des formations allant des Bachelor aux Doctorats dans des domaines variés tels que les sciences fondamentales, les sciences humaines, les sciences sociales, l'économie, et les arts.

L'ENS de Lyon est un acteur majeur de la recherche, avec des laboratoires de renom comme le Laboratoire de Physique, et soutient activement les recherches fondamentales et appliquées. L'école compte actuellement plus de 2 400 étudiants et 1 100 personnels.

L'ENS et Isitech sont deux établissements environnants, l'ENS comporte le site Monod où se situent des laboratoires, des salles de classes et quelques personnels, ensuite le site Descartes où se situent les bureaux de la DSI, les bureaux administratifs, certains laboratoires ainsi que des salles de cours :

Site Descartes



En termes de reconnaissance internationale, l'ENS de Lyon se distingue dans plusieurs classements :

- **Classement QS (2021) :**
 - QS "Citations par enseignants" ratio : 1er en France
 - QS "Enseignants internationaux" ratio : 3e en France
- **Classements de Shanghai (2018 à 2021) :**
 - Performance per capita : 1er en France
- **Classements THE (Times Higher Education) (2024) :**
 - Meilleures universités à taille humaine : 1er en France / 7e mondial

L'ENS de Lyon est également reconnue pour ses contributions majeures dans le domaine de la recherche. Par exemple, Anne L'Huillier, professeure à l'ENS de Lyon, a reçu le prix Nobel en 2023 pour ses travaux innovants en physique. Cette distinction témoigne de la qualité exceptionnelle de la recherche menée au sein de l'institution et de son impact à l'échelle internationale.

Fiche d'identité de l'ENS de Lyon

Raison sociale	<ul style="list-style-type: none"> École normale supérieur de Lyon
Type	<ul style="list-style-type: none"> École normal supérieure
Format juridique	<ul style="list-style-type: none"> Établissement public à caractère scientifique, culturel et professionnel
Président	<ul style="list-style-type: none"> Trizac Emmanuel
Campus	<ul style="list-style-type: none"> Site Descartes – 15 Parvis René Descartes Site Monod – 46 Allée d'Italie
Chiffres-clés	
Étudiants	<ul style="list-style-type: none"> 2 469
Enseignants-chercheurs	<ul style="list-style-type: none"> 548
Personnels administratifs et technique	<ul style="list-style-type: none"> 569
Budget	<ul style="list-style-type: none"> 152.1M€
Quelques prix	<ul style="list-style-type: none"> 53 médailles CNRS depuis 1997 Médailles Fields 2010 42 ERC

4. Présentation de la DSI et du service SGP (Support et Gestion de Parc)

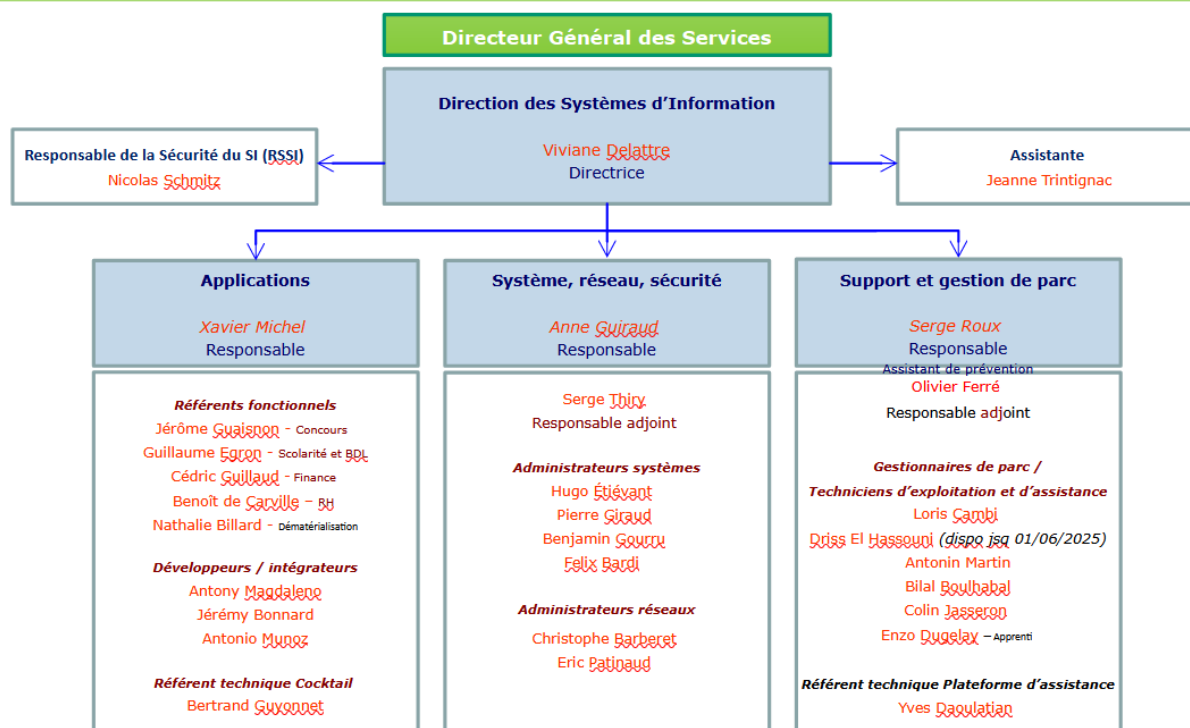
La DSI de l'École Normale Supérieure de Lyon est composée de 30 personnes réparties en plusieurs pôles spécialisés :

- **Pôle Applications** : Gestion des applications ainsi que des droits d'accès associés.
- **Pôle Systèmes, Réseau et Sécurité** : Gestion des réseaux, des systèmes ainsi que de la sécurité.
- **Pôle Support et Gestion de Parc** : Gestion du support technique et la gestion du parc informatique.

Organigramme de la DSI de l'ENS de Lyon :

Services rattachés à la Direction Générale des Services – 01/09/2024

Direction des Systèmes d'Information



Présentation du pôle SGP :

L'équipe du SGP est constituée de 9 professionnels dédiés, incluant :

- Serge Roux – Responsable du service
- Olivier Ferré – Responsable adjoint du service
- Loris Cambi - Technicien
- Yves Daoulatian – Ingénieur d'étude
- Antonin Martin - Technicien
- Bilal Boulahbal - Technicien
- Colin Jasseron - Technicien
- Enzo Dugelay – Technicien

Périmètre du Service Support et Gestion de Parc :

Le pôle SGP prend en charge une variété de tâches cruciales pour le bon fonctionnement du parc informatique : le support et l'assistance, l'installation des postes de travail (Windows, Mac et Linux), la téléphonie, la gestion de certains droits et de mots de passe, la gestion des devis ainsi que la réception des livraisons, le support matériel et logiciel de tout type.

Le matériel à la charge du service est assez varié, il comporte plus de 2 200 ordinateurs (dont 1 500 postes Windows), ainsi qu'environ 250 imprimantes et 50 copieurs, suivi de 1 800 postes téléphoniques dont 100 portables. Le périmètre comprend aussi les stations de travail avec le matériel informatique divers nécessaire.

Les utilisateurs ont trois possibilités de contacter le service support :

1. Physique via l'accueil des bureaux d'assistance
2. Par appel via une hotline active de 8h30-12h à 13h-17h45
3. Via les tickets GLPI (Gestionnaire Libre de Parc Informatique) (Voir annexe page 40, 41)

Outils utilisés

Le pôle SGP assure la maintenance et la gestion du parc informatique à travers une variété d'outils et de solutions. Son périmètre couvre l'installation, le déploiement et la supervision des systèmes d'exploitation, la gestion des imprimantes et des télécommunications, ainsi que le support utilisateur. Les outils principaux utilisés sont :

- **OPSI (Open PC Server Integration)** : Automatisation du déploiement Windows, intégration dans Active Directory, chiffrement et déploiement de packages.
- **GLPI (Gestionnaire Libre de Parc Informatique)** : Gestion du parc, d'inventaire, suivi budgétaire, et tickets d'incidents.
- **TOIP (Telephony over Internet Protocol)** : Gestion des télécommunications via IP, avec OmniVista 8770 pour les terminaux et lignes. (Voir annexe page 44)
- **Munki** : Gestion automatisée des logiciels et mises à jour pour macOS.
- **Récupération** : Script PowerShell via PXE (Preboot Execution Environment) et WinPE (Windows Preinstallation Environment) pour récupérer les données en cas de panne et de remplacement de postes.
- **IPXE** : Outil basé sur la technologie PXE nous permettant d'exécuter des scripts et des déploiements d'images.
- **Serveur Servinst** : Serveur Debian utilisé pour la migration et le partage de fichiers. Ce serveur est aussi utilisé dans mon projet.
- **Checkmk** : Supervision des serveurs et équipements réseau, avec alertes et rapports
- **Dirvish** : Gestion de sauvegarde.
- **Cyberwatch** : Vérification de la conformité d'un poste de travail d'un point de vue sécurité, intégré à l'inventaire GLPI. (Voir annexe page 42)
- **ISL Online** : Connexion à distance permettant la prise en main pour la maintenance.
- **WSUS (Windows Server Update Services)** : Gestion des mises à jour logicielles.
- **Active Directory** : Base de données d'un réseau stockant les comptes utilisateurs, les postes de travail et les droits d'accès.
- **SentinelOne** : Antivirus installé sur les postes, est relié à une console SentinelOne. (Voir annexe page 43)
- **MYQ** : Administration centralisée du parc pour les imprimantes et les copieurs.
- **DokuWiki** : Gestion de documentations utilisé par la DSI pour les procédures techniques, et des informations sur les des applications. (Voir annexe page 38)
- **Checkmk** : Logiciel de supervision, serveur sous Debian pour surveiller en permanence les serveurs, switches et routeurs en cas d'anomalie ou problème.

5. Présentation de mes missions

Au cours de cette année d'alternance, mon travail et mes missions affectées étaient très variés. Voici une liste des missions principales :

- Fournir aux utilisateurs des outils et services informatiques.
- Gérer l'installation et la mise à jour des équipements (tout type de matériel informatique).
- Gestion des droits d'accès utilisateurs.
- Traiter les commandes de matériel informatique : devis, achat, livraison et installation des équipements.
- Installation de postes, téléphones fixes, imprimantes et gérer les renouvellements de matériel.
- Accompagnement des utilisateurs pour toutes demandes.
- Formations et sensibilisation des utilisateurs sur la sécurité.
- Déploiement de logiciels pour Windows, macOS et Ubuntu.
- Gestion d'accueil téléphonique et organiser le support technique.
- Assurer le support technique de premier niveau et de second niveau.
- Administrer le parc informatique : gestion des matériels, logiciels, licences, sécurité et sauvegardes.
- Renforcer la sécurité du parc avec déploiement d'antivirus, chiffrement, pare-feu et authentification forte.
- Rédaction de procédures.
- Exécution de mon projet technique.

De plus, une de mes responsabilités était de gérer sous Ubuntu les tests de déploiement, des scripts, test d'antivirus ainsi que la gestion des logs et d'automatisation. Possédant plus de 300 postes sous Ubuntu, il est crucial de vérifier le fonctionnement de certaines solutions avant de les mettre en œuvre.

6. Projet d'entreprise

Présentation du projet

Le projet consiste en la création et l'optimisation d'un outil visant à faciliter la récupération des données utilisateur sur un poste informatique sous Microsoft Windows. Ce processus est essentiel lors du renouvellement ou de la réinstallation d'un poste, où les données doivent être transférées efficacement et en toute sécurité.

Ce projet aurait parfaitement pu être réalisé en méthode Agile, il a été décidé d'opter pour la méthode en Cascade. En effet, le projet est destiné à une utilisation interne au sein du service SGP. En l'absence de client externe, il a été développé pour répondre aux besoins opérationnels spécifiques de notre équipe. En contrepartie, le fait de suivre un processus Agile avec des sprints aurait impliqué des cycles de réévaluation et d'ajustement, ce qui aurait entraîné une perte de temps en l'absence de client. Comme le cahier des charges était clairement défini dès le départ, la méthode Cascade, avec son approche séquentielle et linéaire, s'est révélée plus appropriée sans qu'il y ait de retour en arrière fréquents suivant une méthode Agile.

Le projet a donc été suivi selon la méthode Cascade qui vise à séquencer les différentes étapes du projet à l'avance afin de les suivre une à une. Une représentation de ces étapes est disponible à la suite de la présentation (page 16).

Contexte du projet

Lors du remplacement ou de la réinstallation d'un poste informatique, il est crucial de garantir que les données des utilisateurs soient correctement transférées. Les sauvegardes traditionnelles peuvent ne pas refléter les données les plus récentes (potentiellement des données jusqu'à J-1, voir plus en cas de période de fermeture). Ce projet vise à pallier ce problème en mettant en place une solution capable de récupérer les données directement à partir du poste en cours, assurant ainsi que les informations soient à jour au moment du transfert.

Objectifs et Problématique du projet

L'objectif principal de ce projet est de simplifier et d'automatiser le processus de récupération des données utilisateurs sur des postes Windows, notamment lors des réinstallations ou renouvellements de machines. Actuellement, ces données sont transférées manuellement ou à partir de sauvegardes qui peuvent ne pas être à jour, ce qui entraîne des erreurs et des pertes de temps.

En outre, la problématique réside dans la diversité des configurations des postes Windows au sein de l'organisation, notamment en termes de matériel et de protection des données (chiffrement BitLocker). Le projet doit donc proposer une solution capable de s'adapter à ces variables tout en assurant un transfert de données automatisé, fiable et sécurisé.

Ensuite, la solution doit être capable de fonctionner sur tout type de poste Windows, qu'il s'agisse de machines récentes ou plus anciennes, avec des configurations variées. Elle doit également pouvoir être exécutée à partir d'un démarrage réseau, garantir la sécurité des données pendant leur transfert, et fonctionner sans intervention humaine prolongée une fois lancée. De plus, le déchiffrement des disques protégés par BitLocker doit être pris en compte, afin de rendre les données accessibles pour leur sauvegarde. Finalement, le projet vise à optimiser le processus en réduisant le temps consacré à la récupération des données.

Cahier des Charges :

- **Démarrage Réseau** : L'outil doit être opérationnel dès le démarrage du poste via un boot réseau, permettant une récupération efficace sans dépendre de systèmes préexistants.
- **Déchiffrement du Disque** : L'outil doit être capable de déchiffrer les disques protégés par BitLocker pour accéder aux données, garantissant ainsi que les informations chiffrées soient récupérées sans compromettre leur sécurité.
- **Sauvegarde des Données** : L'outil doit permettre de sauvegarder les données utilisateurs au moment précis du transfert, assurant la capture des informations les plus actuelles.

- **Stockage Temporaire** : Les données doivent être stockées temporairement sur un serveur avant d'être réinjectées dans le nouveau poste ou le poste réinstallé. Cette étape est essentielle pour la gestion des données durant le processus de transfert.

Démarche : Pour atteindre ces objectifs, une analyse approfondie des outils existants et des technologies disponibles est nécessaire. L'outil pourrait soit utiliser des solutions déjà établies adaptées aux besoins, soit être développé sur mesure en combinant des technologies comme PXE (Preboot Execution Environment) avec l'outil iPXE, WinPE (Windows Preinstallation Environment) et PowerShell, permettant une personnalisation complète du processus de récupération.

Solution Proposée

Il existe plusieurs solutions pour la récupération de profils utilisateurs, comme Microsoft User State Migration Tool (USMT), Clonezilla, ou Dell Data Protection | Endpoint Recovery. Cependant, ces outils peuvent être payants, ou comme Dell Endpoint Recovery, limités à des machines de la marque Dell. En revanche, un script personnalisé offre une solution plus flexible et économique, adaptable à tout type de poste, sans les contraintes des solutions propriétaires.

Justification de l'Utilisation d'un Script :

1. **Flexibilité** (Adapté selon le besoin)
2. **Gain de Temps** (Réduction du temps d'intervention)
3. **Économique** (Pas de coût de licence)
4. **Simplicité d'Utilisation** (Facile à exécuter et personnaliser)

En résumé, l'adoption de ce script automatisé est justifiée par sa capacité à améliorer l'efficacité du processus de récupération des données, à réduire le risque d'erreurs humaines, et à accélérer le temps de traitement, tout en assurant la sécurité des données et la simplicité d'utilisation.

La solution développée pour le projet utilise la méthode Cascade, ce qui a permis de définir les étapes du projet de manière séquentielle dès le départ. Cette approche a facilité une planification claire et structurée, avec des étapes préalablement établies pour assurer une réalisation efficace du projet. Les étapes définies pour le projet sont les suivantes :

Étape	Test	Résultat
1. Création d'un environnement WinPE	En attente	En attente
1.1 Ajout des modules PowerShell, ActiveDirectory et BitLocker	En attente	En attente
2. Rédaction du fichier de configuration startnet	En attente	En attente
3. Rédaction du script recuperation_profil	En attente	En attente
3.1 - Définition des identifiants de connexion	En attente	En attente
3.2 - Récupération du numéro de l'ordinateur	En attente	En attente
3.3 - Récupération de la clé BitLocker dans l'AD puis déchiffrement du disque	En attente	En attente
3.4 - Connexion au serveur Servinst	En attente	En attente
3.5 - Liste des profils à récupérer avec une liste box	En attente	En attente
3.6 - Copie des profils listés sur servinst	En attente	En attente
3.7 - Création d'une clé USB bootable pour les tests	En attente	En attente
4. Montage du projet sur le serveur	En attente	En attente

Présentation de l'existant

Depuis plusieurs années, le transfert des profils se faisait manuellement via le serveur, ce qui nécessitait beaucoup de temps, car certains sous-dossiers situés dans les profils ne devaient pas être copiés (Exemple : les comptes administrateurs, ou certains fichiers de configurations). En moyenne, la copie manuelle pouvait durer plusieurs dizaines de minutes en comptant le tri manuel des fichiers dans chaque profil.

Présentation de la solution

Avant de pouvoir exécuter le script de récupération des profils, il est essentiel de configurer un environnement WinPE adapté.

La rédaction du script ne sera pas détaillée en détail dans le rapport. Les étapes du projet abordées seront la création de l'image WinPE, ainsi que la configuration de son environnement, la rédaction d'un fichier de configuration ainsi que l'utilisation du projet. Des documentations sources seront ajoutées tout du long de l'explication du projet, celles-ci comportent les étapes et les lignes de commande précises lors de l'installation et la configuration de WinPE pour une compréhension plus approfondie.

Cependant, avant d'exécuter le script de récupération, il est crucial de créer et de configurer l'environnement WinPE. En effet, la première grande étape de la solution apportée inclut la création de l'image WinPE, ainsi que l'ajout des modules nécessaires (PowerShell, Active Directory, BitLocker), la configuration de la langue française et la création du fichier de configuration startnet.cmd.

Configuration de l'Environnement WinPE

1. Création d'un Environnement WinPE

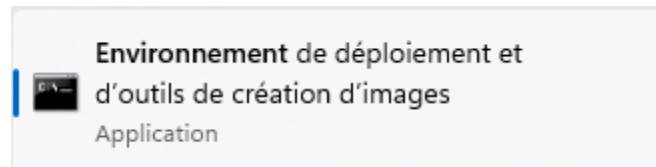
L'objectif consiste à créer un environnement WinPE, essentiel pour exécuter le script de récupération des profils utilisateurs. WinPE est une version allégée de Windows utilisée principalement pour les installations, les réparations et les déploiements. (Voir la documentation dans le Glossaire)

Téléchargement et Installation de l'ADK et WinPE

Pour commencer, il est nécessaire de télécharger et d'installer Windows Automated Installation Kit (ADK) et son composant additionnel Windows PE. Ces outils permettent la création et la gestion d'images Windows. Les liens de téléchargements se trouvent dans le glossaire.

- Windows ADK (version 10.1.26100.1, mai 2024)
- Composant additionnel Windows PE pour Windows ADK (version 10.1.26100.1, mai 2024)

Une fois ces packages installés, nous disposons d'un outil de commande appelé Environnement de déploiement et d'outils de création d'images, qui est crucial pour la création de l'image WinPE. (Voir son utilisation ainsi que les commandes utilisées pour sa configuration en annexe page 39)



Création de l'image WinPE

Une fois les outils installés, il est possible de procéder à la création de l'image WinPE à l'aide du logiciel installé ci-dessus. Cette image permet d'exécuter un environnement léger de Windows directement à partir d'un périphérique USB ou d'un réseau.

Une documentation Microsoft de l'installation exacte de WinPE est située dans le glossaire.

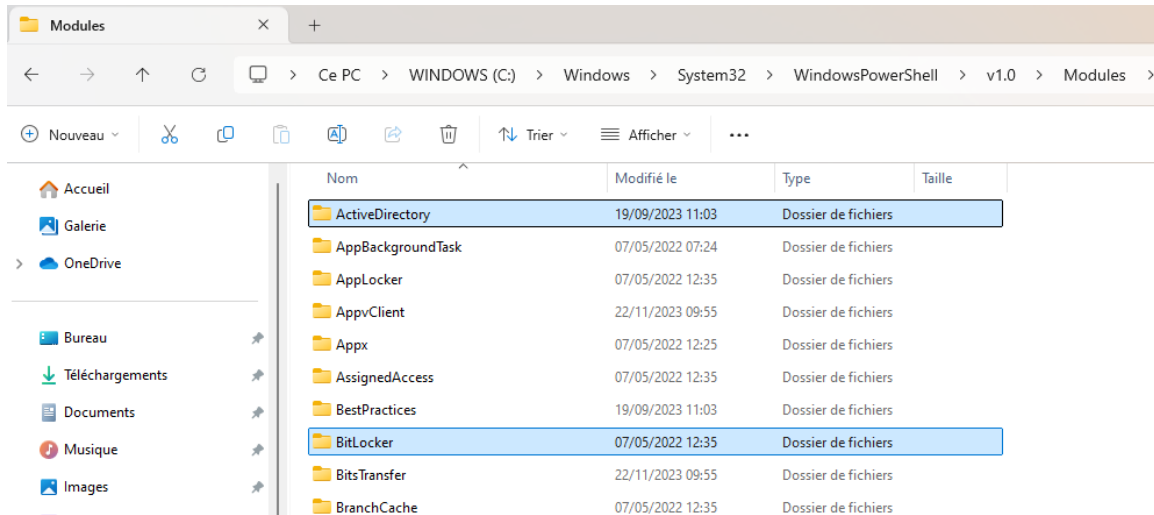
1.1 Configuration de WinPE

Une fois l'environnement WinPE créé, il est nécessaire d'ajouter certains modules spécifiques pour l'utilisation du script :

- **Module PowerShell** : Ce module permet l'automatisation des tâches dans WinPE, tel que l'exécution du script et l'intégration des modules suivants.
- **Modules Active Directory et BitLocker** : Ces deux composants sont essentiels pour se connecter à l'Active Directory afin de récupérer la clé BitLocker, sans ces composants, il serait impossible d'authentifier les utilisateurs ou de déchiffrer les disques, bloquant ainsi l'accès aux données critiques que le script est censé récupérer.

Les modules Active Directory et BitLocker sont des composants de PowerShell qui se trouvent au chemin d'accès suivant :

C:\Windows\System32\WindowsPowerShell\v1.0\Modules



L'installation de ces deux modules seront exceptionnellement détaillées suite à l'absence de documentation sur internet :

```

commandes utilisées.txt - Bloc-notes
Fichier Edition Format Affichage Aide
### Modules ActiveDirectory et BitLocker :
xcopy /E /I "C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ActiveDirectory"
"C:\WinPE_amd64_BL\mount\Windows\System32\WindowsPowerShell\v1.0\Modules\ActiveDirectory"

xcopy /E /I "C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker"
"C:\WinPE_amd64_BL\mount\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker"

xcopy "C:\Windows\Microsoft.NET\assembly\GAC_64\Microsoft.ActiveDirectory.Management.resources\v4.0.10.0.0_fr_31bf3856ad364e35\Microsoft.ActiveDirectory.Management.resources.dll" "C:\WinPE_amd64_BL\mount\Windows\System32"

xcopy "C:\Windows\Microsoft.NET\assembly\GAC_64\Microsoft.ActiveDirectory.Management\v4.0.10.0.0_31bf3856ad364e35\Microsoft.ActiveDirectory.Management.dll" "C:\WinPE_amd64_BL\mount\Windows\System32\WindowsPowerShell\v1.0\Modules\ActiveDirectory"

dism /image:C:\winpe_amd64_BL\mount /add-package /packagepath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

dism /image:C:\winpe_amd64_BL\mount /add-package /packagepath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-SecureStartup.cab"

dism /image:C:\winpe_amd64_BL\mount /add-package /packagepath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-EnhancedStorage.cab"

```

Tout d'abord, les commandes xcopy servent à copier les modules ActiveDirectory et BitLocker, depuis le système vers l'image WinPE montée. Par exemple, la première commande copie de manière récursive le répertoire ActiveDirectory vers l'image WinPE. Ensuite, des fichiers DLL (Dynamic Link Library, bibliothèque de fonctions/ressources) sont copiés dans l'image WinPE, car ils sont nécessaires pour l'utilisation des commandes Active Directory.

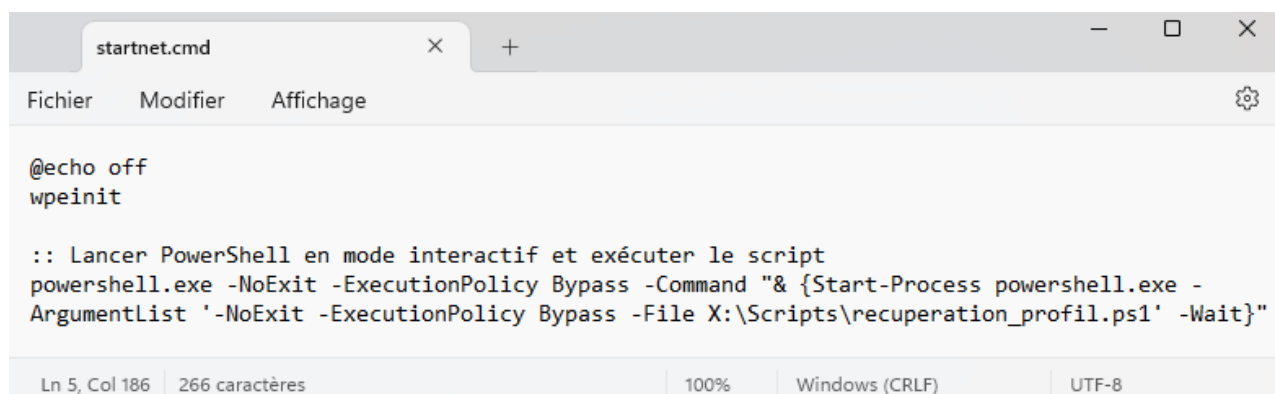
Ensuite, les commandes DISM (Deployment Image Servicing and Management) permettent d'ajouter des packages essentiels comme WinPE-WMI.cab active le support de WMI (Windows Management Instrumentation), WinPE-SecureStartup (gestion BitLocker), et WinPE-EnhancedStorage (gestion des disques chiffrés), assurant que l'image est prête pour la suite des opérations.

- **Module de la langue française et de compatibilité matérielle :**

Après l'ajoute des modules principaux, il est essentiel d'adapter l'environnement à notre configuration spécifique. Cela se fait principalement en intégrant le pack de langue française, afin de garantir une interface adaptée, ainsi que des pilotes matériels pour assurer la compatibilité avec une large gamme de dispositifs.

2. Rédaction du fichier de configuration startnet.cmd

Afin d'automatiser le démarrage du script au démarrage de WinPE, il est nécessaire de créer le fichier nommé **startnet.cmd**. Ce fichier est essentiel car il permet d'exécuter notre script principal avec PowerShell ainsi que de configurer WinPE.



```
@echo off
wpeinit

:: Lancer PowerShell en mode interactif et exécuter le script
powershell.exe -NoExit -ExecutionPolicy Bypass -Command "& {Start-Process powershell.exe -
ArgumentList '-NoExit -ExecutionPolicy Bypass -File X:\Scripts\recuperation_profil.ps1' -Wait}"
```

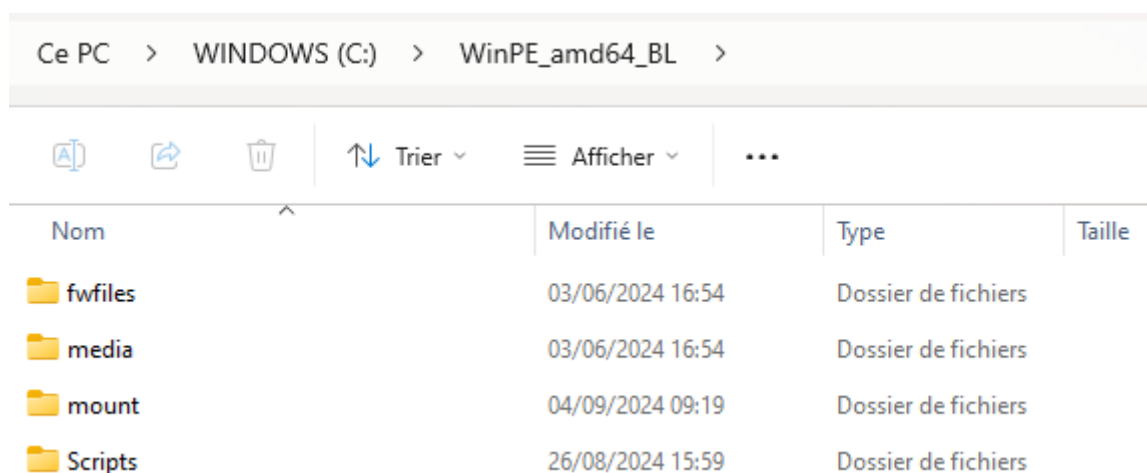
Ln 5, Col 186 | 266 caractères | 100% | Windows (CRLF) | UTF-8

Dans ce fichier, la commande « wpeinit » permet d'initialiser les services WinPE. Ensuite, la commande powershell.exe ouvre PowerShell suivi du script recuperation_profil.ps1 avec les bons paramètres. Nous utilisons l'option « -ExecutionPolicy Bypass » pour permettre au script de s'exécuter sans restriction. De la même manière, les liens sources qui détaillent ce fichier sont disponibles dans le glossaire.

3. Rédaction du script recuperation_profil

Avant de commencer, le dossier où nous allons monter l'image WinPE, C:\WinPE_amd64_BL\mount, est vide. En montant l'image WinPE dans ce dossier, nous accédons directement à son système de fichiers, ce qui nous permet d'ajouter des fichiers nécessaires, comme notre script de récupération de profils ainsi que les modules importés.

Initialement, le script se trouve dans le répertoire C:\WinPE_amd64_BL\Scripts. Suite au montage de l'image WinPE, ce script est placé dans C:\WinPE_amd64_BL\mount\Scripts. Lorsque WinPE est en cours d'exécution, ce répertoire apparaît sous la lettre de lecteur X:, ce qui signifie que le chemin X:\Scripts\recuperation_profil fait référence au dossier de montage C:\WinPE_amd64_BL\mount\Scripts\recuperation_profil.



Nom	Modifié le	Type	Taille
fwfiles	03/06/2024 16:54	Dossier de fichiers	
media	03/06/2024 16:54	Dossier de fichiers	
mount	04/09/2024 09:19	Dossier de fichiers	
Scripts	26/08/2024 15:59	Dossier de fichiers	

Une fois que la configuration de WinPE est terminée, nous devons également évaluer les ressources temporelles et budgétaires investies dans ce projet avant de présenter son utilisation.

4. Montage du projet sur le serveur

Après avoir validé le script de récupération des profils sur une clé USB, il est crucial de déployer le projet sur le serveur pour une utilisation pratique. En effet, ce déploiement permet d'éviter la dépendance aux clés USB et facilite l'accès au script via le réseau.

Effectivement, la configuration sur le serveur inclut le transfert des fichiers nécessaires de WinPE et la configuration des options de démarrage réseau avec iPXE. Une fois le projet monté et configuré, nous détaillerons l'utilisation du projet, incluant le démarrage réseau et la sélection du script depuis l'interface.

Transfert des Fichiers sur le Serveur :

- Les fichiers essentiels pour le démarrage de WinPE (wimboot, BCD, boot.sdi, et boot.wim) doivent être transférés sur le serveur dans le répertoire approprié, généralement /var/www/html. Ce répertoire permet aux clients d'accéder aux fichiers via HTTP.
 - wimboot : Chargeur qui démarre l'image WinPE.
 - BCD : Fichier de configuration de démarrage.
 - boot.sdi : Disque virtuel préparant le système pour le démarrage.
 - boot.wim : Image contenant l'environnement WinPE.

Mise en Place du Menu de Démarrage :

- Il est important de configurer le fichier de démarrage réseau pour pointer vers les fichiers nécessaires sur le serveur. Ce fichier de configuration, qui est démarré via l'iPXE, inclut des lignes indiquant l'emplacement des fichiers vu précédemment sur le serveur.

Ressources temporelles et budgétaires du projet

Étant donné que ce projet est une initiative interne sans client externe ni coûts matériels, il est difficile d'en définir un budget précis. De plus, sachant qu'il n'y a eu aucun achat d'équipement ou coûts externes à considérer. Par conséquent, nous nous concentrons sur le temps de travail consacré et le temps gagné grâce à l'automatisation pour évaluer la rentabilité. En effet, en se basant sur le SMIC horaire, nous avons calculé le coût des heures travaillées et les économies réalisées, ce qui permet de mesurer l'impact du projet en termes de productivité.

Le projet s'étend sur une période de 15 semaines en entreprise sur 5 mois. Pendant ces 15 semaines, prenons une moyenne de 12h de travail par semaine consacrées au projet, ce qui totalise 156 heures de travail.

Dans cet exemple, prenons un smic comme point de repère pour les calculs.

Calcul du coût du projet :

Temps total impliqué : 156h

Taux horaire brut SMIC : 1 747 € / 151,67 heures = environ 11,52 € par heure

Coût total du projet : $156 * 11,52€ = 1\,797,12€$

Il est important de noter qu'aucun coût matériel n'a été impliqué dans ce projet. Ainsi, le coût du projet total en se basant sur un SMIC est de 1 797€.

Risques et gestion des risques

Dans le cadre de ce projet, les risques majeurs sont minimaux. Le développement et l'intégration du script dans l'image WinPE sont réalisés avec une attention particulière pour éviter les erreurs courantes. Les tests rigoureux effectués assurent le bon fonctionnement du script et la configuration correcte de l'environnement WinPE.

Mesures de Gestion des Risques :

Tests multiples : Réalisation de tests pour garantir que l'image WinPE et le script fonctionnent comme prévu.

Suivi continu : Surveillance régulière du projet pour détecter et corriger rapidement toute anomalie éventuelle.

En conclusion, le projet bénéficie d'un suivi détaillé pour assurer la fiabilité du déploiement, réduisant ainsi le risque de problèmes majeurs.

Utilisation du projet

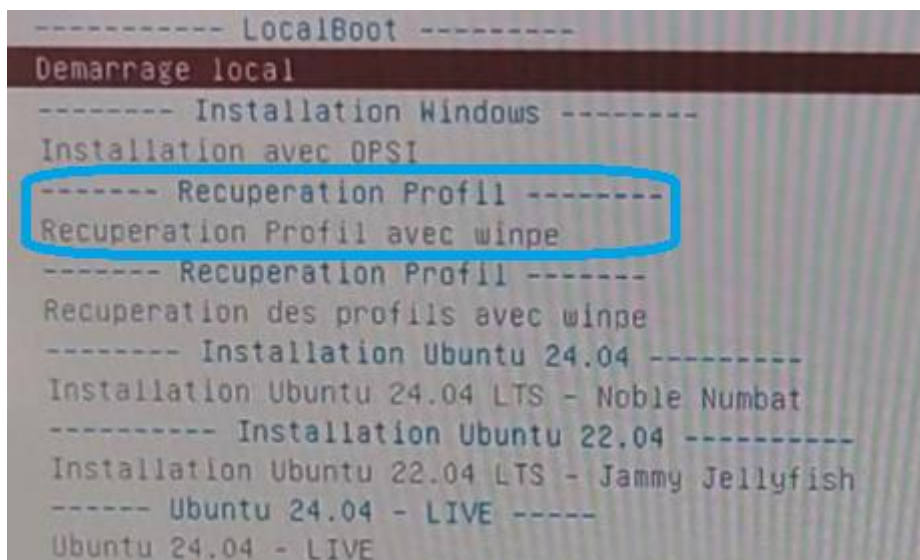
Ensuite, cette partie décrit l'utilisation du script. De plus, la procédure d'exécution du script est disponible en annexe (page 38). Afin d'exécuter le script, nous passons par une technologie de démarrage réseau supportant des menus de démarrage personnalisés ainsi que les scripts, iPXE, se basant sur PXE (Preboot Execution Environment).

En effet, le boot PXE est un protocole de démarrage réseau qui permet à un ordinateur local de démarrer à partir de données situées sur un serveur distant, plutôt que de démarrer à partir du disque local, ou du contenu de la clé USB. Cette méthode de démarrage est souvent utilisée pour le déploiement de postes de travail puisqu'elle va permettre de distribuer le système d'exploitation à installer à partir du réseau.

De plus, le boot iPXE (intelligent Preboot Execution Environment) est un logiciel qui se base sur la technologie PXE. Il permet à un ordinateur de démarrer sur le réseau et ainsi offrir des fonctionnalités supplémentaires telles que :

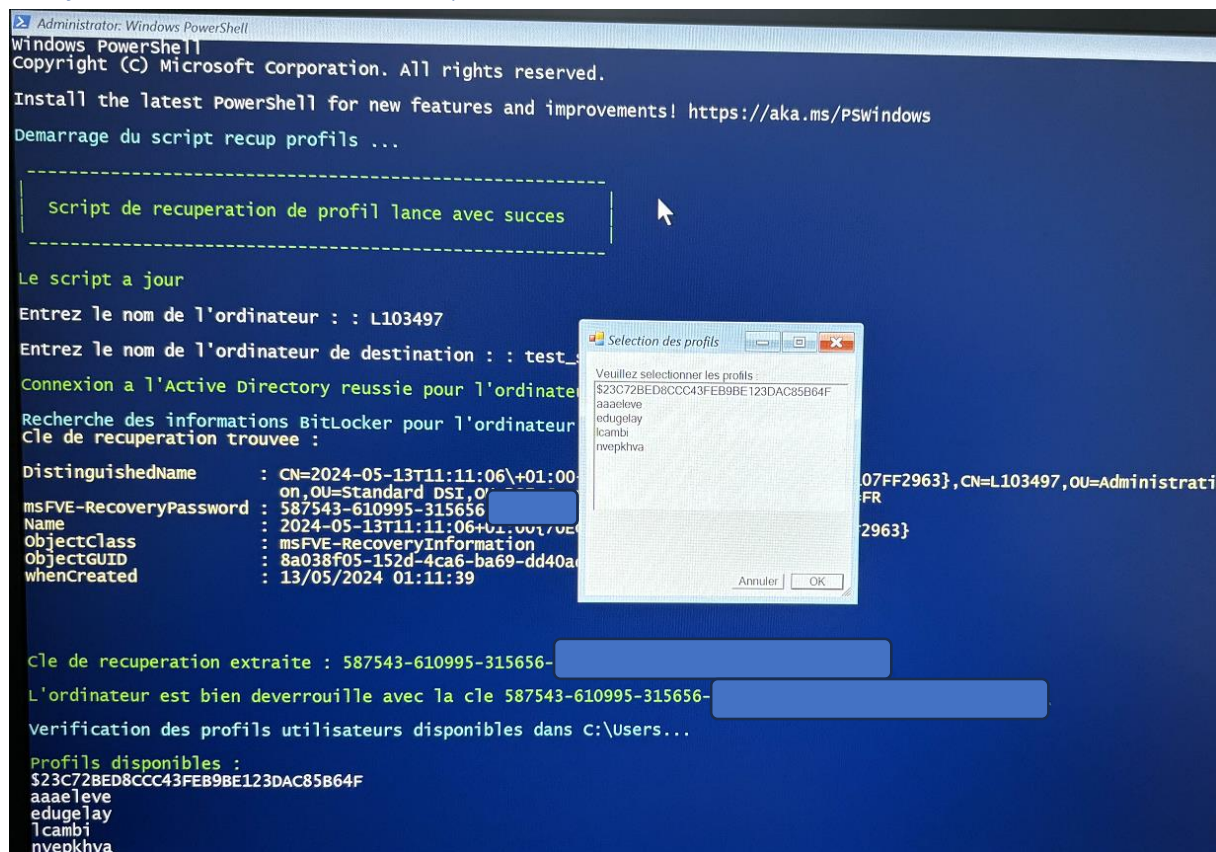
- Le support des scripts
- Le support des menus de démarrage personnalisés

Ensuite, suite au démarrage réseau iPXE, une interface se présente avec différentes possibilités, l'installation de poste avec OPSI (Open PC Server Integration), l'installation d'Ubuntu, ainsi que le script pour récupérer les profils.



Par la suite, le script est exécuté, il est ainsi soumis à des tests de vérifications afin de garantir son fonctionnement. Le script est conçu pour apporter un message d'avertissement à chaque étape lors de la connexion, ces messages permettent au technicien utilisant le script d'avoir un suivi total en cas d'erreur.

Interface lors de l'exécution du script :



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

Demarrage du script recup profils ...

-----
Script de recuperation de profil lance avec succes
-----

Le script a jour
Entrez le nom de l'ordinateur : : L103497
Entrez le nom de l'ordinateur de destination : : test_
Connexion a l'Active Directory reussie pour l'ordinateur
Recherche des informations BitLocker pour l'ordinateur
Cle de recuperation trouvee :
DistinguishedName      : CN=2024-05-13T11:11:06\+01:00...
msFVE-RecoveryPassword : 587543-610995-315656-...
Name                   : 2024-05-13T11:11:06\+01:00\...
ObjectClass             : msFVE-RecoveryInformation
ObjectGUID              : 8a038f05-152d-4ca6-ba69-dd40a...
whenCreated             : 13/05/2024 01:11:39

Cle de recuperation extraite : 587543-610995-315656-...
L'ordinateur est bien deverrouille avec la cle 587543-610995-315656-...
Verification des profils utilisateurs disponibles dans C:\Users...

Profils disponibles :
$23C72BED8CCC43FEB9BE123DAC85B64F
aaaeleve
edugelay
lcambi
nvepkhva
  
```

Le déroulement du script est le suivant :

- Tout d'abord une interface PowerShell se lance comme vu précédemment, il est ensuite affiché un message de départ
- Ensuite, le script demande le nom de l'ordinateur host et de destination. En effet, l'environnement WinPE n'a pas accès à Windows donc il ne peut pas récupérer seul le nom de l'host. Le nommage des postes se font de la manière suivante : L10XXXX, ici L103497, un portable HP EliteBook 840, et prenons « test_script_winpe » comme nom de destination.



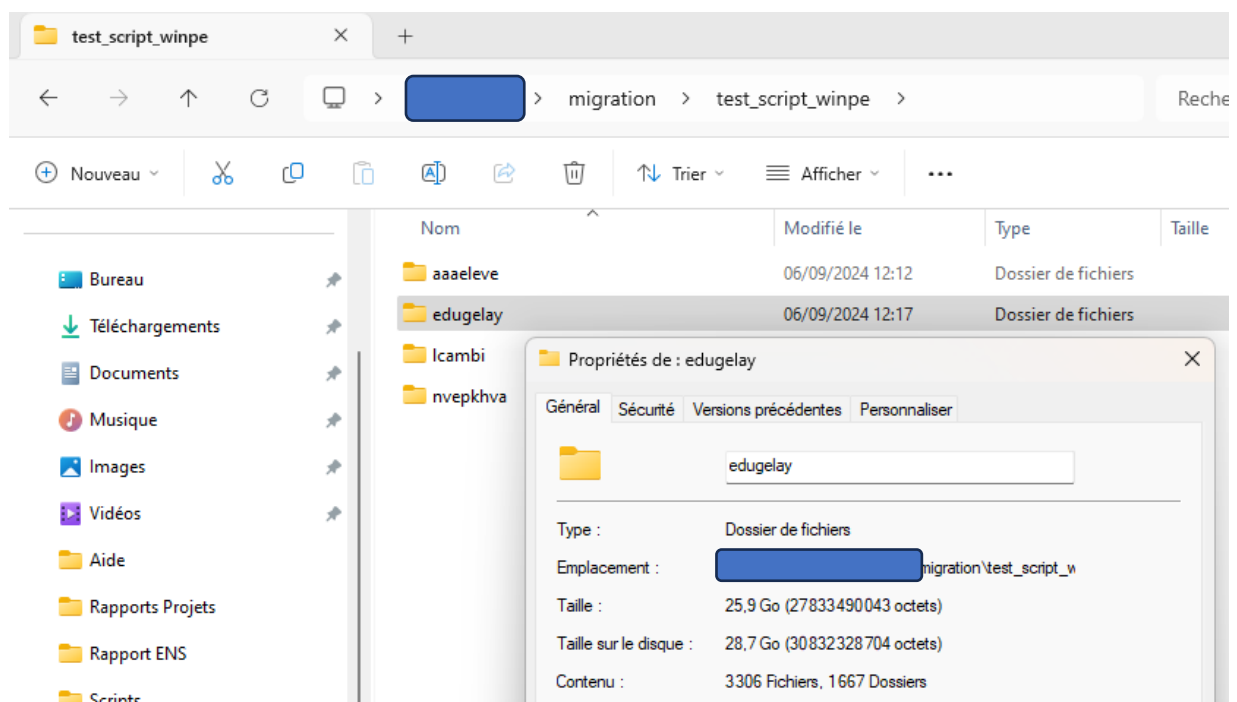
- De plus, le script se connecte à l'Active Directory et recherche ainsi la clé BitLocker liée à l'ordinateur demandé
- Suite à l'obtention de la clé, le script déverrouille l'ordinateur afin d'accéder aux profils.

Certains profils ont été enlevés lors de la récupération, par exemple tous les profils administrateurs, ainsi que les profils « Public », « Default », « All Users » et « Default User ».

- Une listbox est ensuite affichée afin de pouvoir sélectionner les profils voulus.
- Par la suite, un message indiquant que la connexion au serveur Servinst est réussie, ainsi que la copie des profils sélectionnés lors de la listbox démarre. Ensuite, la création du dossier « edugelay », correspondant à mon profil, est réussie.

```
Connexion a \\servinst [redacted] reussie
Creation du dossier test sur Servinst reussie.
Source : C:\Users\edugelay
Destination : M:\test\edugelay
Creation du dossier M:\test\edugelay reussie.
```

Suite à l'exécution du script ainsi que la copie des profils concernés, il est possible de vérifier leur copie sur le serveur Servinst :



Ainsi, les profils utilisateurs sont copiés de manière efficace et fiable grâce à l'automatisation du script. Le processus est rapide, et ne nécessite qu'une intervention manuelle pour le nom d'ordinateur host et de destination, ce qui réduit les erreurs humaines et assure que l'intégralité des données nécessaires est correctement transférée. De plus, la vérification des logs permet de confirmer la réussite de chaque opération de copie.

En effet, il est possible de vérifier le fonctionnement du projet grâce aux étapes prédéfinies avec l'utilisation de la méthode Cascade :

Étape	Test	Résultat
1. Création d'un environnement WinPE	OK	OK
1.1 Ajout des modules PowerShell, ActiveDirectory et BitLocker	OK	OK
2. Rédaction du fichier de configuration startnet	OK	OK
3. Rédaction du script recuperation_profil	OK	OK
3.1 - Définition des identifiants de connexion	OK	OK
3.2 - Récupération du numéro de l'ordinateur	OK	OK
3.3 - Récupération de la clé BitLocker dans l'AD puis déchiffrement du disque	OK	OK
3.4 - Connexion au serveur Servinst	OK	OK
3.5 - Liste des profils à récupérer avec une liste box	OK	OK
3.6 - Copie des profils listés sur servinst	OK	OK
3.7 - Création d'une clé USB bootable pour les tests	OK	OK
4. Montage du projet sur le serveur	OK	OK

Bénéfices du projet

Le script est utilisé en moyenne 8 fois par semaine. Grâce à son efficacité, il permet de gagner environ 2 heures et 40 minutes par semaine (soit 20 minutes par utilisation). En moyenne, ce gain de temps représente environ 10 heures et 40 minutes par mois.

Calcul du Temps et Économies

De la même manière que pour les ressources budgétaires du projet, sur la base du SMIC brut en France (1 747 € par mois en 2024 pour une durée complète de travail), les économies générées par le script peuvent être calculées comme suit :

Temps gagné par semaine : 2h40

Temps gagné par mois : 10h40 (2h40 * 4)

Taux horaire brut SMIC : 1 747 € / 151,67 heures = environ 11,52 € par heure

Économies mensuelles : 10h40 * 11,52 € = 122,21 € (arrondi)

Le script permet donc de réaliser une économie d'environ 122,21 € par mois en termes de coût horaire basé sur le SMIC.

En conclusion, avec un coût total du projet de 1 797€, le projet sera rentabilisé après environ 15 mois à utilisation moyenne, soit 8 fois par semaine.

Par ailleurs, il est envisageable que pendant certaines périodes de l'année, le script peut être utilisé jusqu'à 15 fois par semaine, ce qui générerait une économie de 225 € par mois. Dans ce scénario, le projet serait amorti au bout d'un an, en supposant une utilisation maximale pendant 3 mois.

Améliorations futures du projet

La suite logique du projet serait ensuite d'automatiser la copie des profils vers l'ordinateur de destination. En effet, le script copie sur le serveur les profils dans le dossier `\nom_d'ordinateur_de_destination\`, cependant le projet n'inclut pas la copie de ces profils vers cet ordinateur.

Une autre idée serait d'ajouter une fonctionnalité au script pour automatiser le chiffrement des disques avec BitLocker. Ainsi, les ordinateurs non chiffrés seraient automatiquement sécurisés, la remontée dans l'Active Directory des clés de récupération BitLocker pourrait aussi être automatisée. Après le chiffrement, le script s'exécuterait pour récupérer et transférer les profils.

Conclusion du projet

Pour conclure, le projet a atteint ses objectifs avec succès, avec toutes les fonctionnalités entièrement opérationnelles. Il m'a offert l'occasion d'explorer et de maîtriser diverses technologies telles que iPXE et PXE, WinPE, ainsi que les scripts PowerShell pour l'automatisation. Cette expérience a enrichi mes compétences techniques en scripting, ainsi qu'en gestion des données et des systèmes, tout en approfondissant ma compréhension des environnements de déploiement et de récupération.

7. Synthèse de l’alternance

Retour d’expérience

Mon année d'alternance au Service Support et Gestion de Parc (SGP) m'a offert une expérience précieuse dans la gestion d'un parc informatique. J'ai été impliqué dans l'installation, la mise à jour et le support des équipements, ce qui m'a permis de développer des compétences techniques approfondies. Ce rôle m'a également permis de prendre conscience de l'importance de la responsabilité et de l'organisation dans la gestion des systèmes informatiques. J'ai contribué à améliorer l'efficacité des processus internes, en introduisant des solutions pour automatiser certaines tâches et en optimisant les opérations quotidiennes.

De plus, le projet sur lequel j'ai travaillé m'a permis de me familiariser avec des technologies nouvelles pour certaines, enrichissant ainsi ma compréhension des processus de gestion des systèmes informatiques et de leur automatisation. J'ai apporté une valeur ajoutée à l'entreprise en contribuant à la mise en place de solutions innovantes qui ont simplifié et accéléré les opérations de gestion du parc informatique.

Ma formation à l'école Isitech a complété cette expérience en me fournissant une base solide en théorie ainsi qu'en pratique, que j'ai pu appliquer et approfondir dans un environnement professionnel. Ces années d'études m'ont permis de me développer tant sur le plan professionnel qu'humain. Sur le plan professionnel, j'ai acquis des compétences techniques avancées et une meilleure compréhension des enjeux du secteur. Humainement, j'ai appris à travailler en équipe, à gérer des projets et à faire preuve d'autonomie, ce qui m'a permis de grandir et de m'adapter aux défis rencontrés dans mon rôle.

8. Projet de carrière

À l'issue de cette année de licence à l'école d'Isitech ainsi de l'alternance au sein de l'ENS de Lyon, en conséquence de nombreux projets en cybersécurité durant cette année ainsi que les années précédentes, je souhaite désormais orienter ma carrière vers l'étude de la cybersécurité. Mon objectif est de progresser en tant que Consultant Cybersécurité, Responsable de la Sécurité des Systèmes d'Information (RSSI) ou Analyste SOC (Security Operation Center).

En effet, la suite logique de ce projet est de poursuivre un mastère de cybersécurité. C'est pourquoi durant mes deux années suivantes se dérouleront à l'école CSB School à Charbonnières-les-Bains afin de suivre la formation Responsable de la Cybersécurité en alternance.

9. Glossaire technique et liens sources

Description des termes techniques utilisés :

- ENS : École Normale Supérieure
- RPI : Responsable de Projets Informatiques
- SGP : Support et Gestion de Parc
- OPSI : Open PC Server Integration
- TOIP :
- PXE : Preboot Execution Environment
- iPXE : intelligent Preboot Execution Environment
- WinPE : Windows Preinstallation Environment
- GLPI : Gestionnaire Libre de Parc Informatique
- ADK : Automated Installation Kit
- DLL : Dynamic Link Library
- DISM : Deployment Image Servicing and Management
- WMI : Windows Management Instrumentation

Liens sources utilisés :

Installer l'ADK et WinPE :

Documentation WinPE : <https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/winpe-intro?view=windows-11>

Téléchargement de l'ADK : <https://learn.microsoft.com/fr-fr/windows-hardware/get-started/adk-install>

Téléchargement de WinPE : <https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/download-winpe--windows-pe?view=windows-11#get-the-files-you-need-to-create-winpe-media>

Création et configuration de WinPE :

Création d'un média WinPE : <https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/winpe-create-usb-bootable-drive?view=windows-11>

Ajout du module PowerShell : <https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/winpe-adding-powershell-support-to-windows-pe?view=windows-11>

Ajout des drivers à WinPE : <https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image?view=windows-11>

Monter et personnaliser WinPE : <https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/winpe-mount-and-customize?view=windows-11#add-updates-to-winpe-if-needed>

Script de démarrage WinPE avec startnet.cmd : <https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/wpeinit-and-startnetcmd-using-winpe-startup-scripts?view=windows-11>

Configuration de la langue : <https://guillaume-cortes.fr/creer-iso-winpe-francais/>

Ajout des drivers PC : <https://dl.dell.com/FOLDER11926959M/1/WinPE10.0-Drivers-A34-PCW4V.cab>

PXE et iPXE pour le boot réseau :

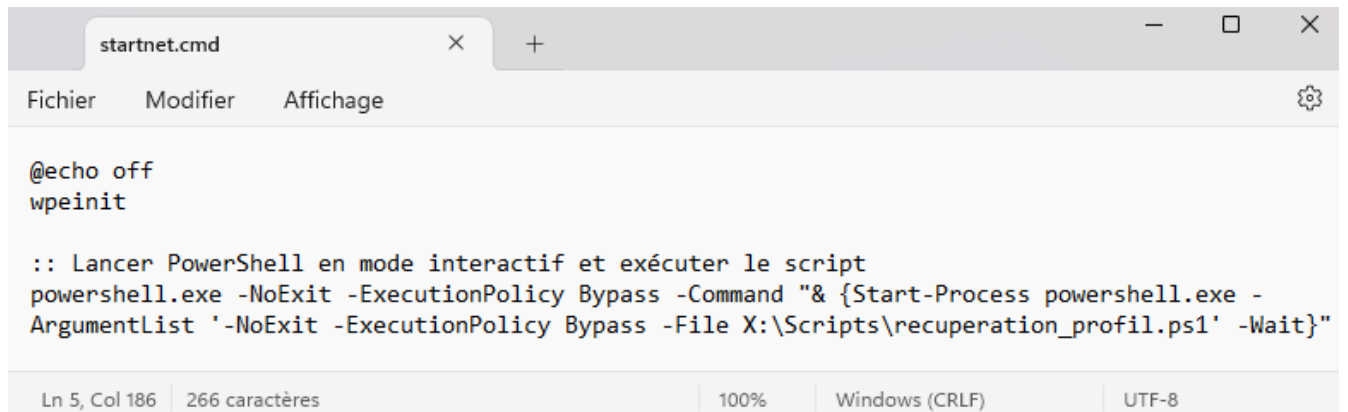
PXE et iPXE : <https://www.it-connect.fr/le-boot-pxe-et-le-boot-ipxe-pour-les-debutants/>

WinPE depuis iPXE : <https://ipxe.org/howto/winpe>

WinPE depuis iXPE : <https://forum.ipxe.org/printthread.php?tid=17332>

10. Annexes

Contenu du fichier de configuration startnet.cmd :



```
@echo off
wpeinit

:: Lancer PowerShell en mode interactif et exécuter le script
powershell.exe -NoExit -ExecutionPolicy Bypass -Command "& {Start-Process powershell.exe -
ArgumentList '-NoExit -ExecutionPolicy Bypass -File X:\Scripts\recuperation_profil.ps1' -Wait}"
```

Ln 5, Col 186 | 266 caractères | 100% | Windows (CRLF) | UTF-8


sgp:recuperation_d_une_sauvegarde_des_profils

Table des matières

- 1) Lancement du script
- 2) Exécution du script
- 3) Problèmes possibles
- ANCIENNE PROCEDURE CI-DESSOUS
- Paramétrages
- Installation d'une nouvelle version linux pour le boot pxe de recupprofil

===== Récupération des profils Windows sur un autre poste =====

1) Lancement du script



Une copie du script se trouve sur \\servinst.ens-lyon.fr\ghost\migration\script\Script Recup ProfilV2.ps1

Le principe est de booter une image WinPe installée sur servinst dans le dossier /var/www/winpe

* Booter en iPXE puis choisir l'entrée du menu "Recuperation profil avec winpe"

* Au démarrage, startnet.cmd lance le script "recuperation_profil.ps1" qui se trouve dans %windir%\System32 du WinPE (généralement X:)

[Modifier](#)

2) Exécution du script

* Tout d'abord, le script demande le nom de l'ordinateur hôte à déchiffrer : cette variable sera utilisée pour chercher la clé Bitlocker dans l'AD (grâce au crédiel d'opsisuppr) et déverrouiller le lecteur C:

* Ensuite, entrer le numéro de l'ordinateur de destination où seront réimplantées les données. Cette étape vérifie, puis crée un dossier correspondant sur Servinst/ghost/migration

* Par la suite, il faut sélectionner les profils que l'on souhaite importer sur Servinst

Certains sous-dossiers ou fichiers comme NTUser.dat ne sont pas copiés car ils sont obsolètes.

[Modifier](#)

3) Problèmes possibles

* Le disque dur doit bien être chiffré lors de l'exécution de la procédure, dans le cas contraire, veuillez le chiffrer

* En cas d'absence de clé BitLocker dans l'Active Directory, il est nécessaire de remonter la clé manuellement depuis l'ordinateur hôte via PowerShell avec ces commandes :

```
$RecoveryKey = ((Get-BitLockerVolume -MountPoint C:).KeyProtector | Where-Object {$_.KeyProtectorType -eq "RecoveryPassword"}).KeyProtector
Backup-BitLockerKeyProtector -MountPoint C: -KeyProtectorId $RecoveryKey
```

[Modifier](#)



Environnement WinPE utilisé pour le configurer :

```
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>dism /Mount-Wim /WimFile:C:\WinPE_amd64_BL\media\sources\boot.wim /index:1 /MountDir:C:\WinPE_amd64_BL\mount

Outil Gestion et maintenance des images de déploiement
Version : 10.0.25398.1

Montage de l'image
[=====100.0%=====]
L'opération a réussi.

C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>notepad C:\WinPE_amd64_BL\mount\Windows\System32\Startnet.cmd
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>notepad C:\WinPE_amd64_BL\mount\Scripts\recuperation_profil.ps1

C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>dism /Unmount-Wim /MountDir:C:\WinPE_amd64_BL\mount /Commit

Outil Gestion et maintenance des images de déploiement
Version : 10.0.25398.1

Fichier image : C:\WinPE_amd64_BL\media\sources\boot.wim
Index de l'image : 1
Enregistrement de l'image
[=====100.0%=====]
Démontage de l'image
[=====100.0%=====]
L'opération a réussi.

C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>
```



Interface ordinateur GLPI :

ENS DE LYON

Chercher dans le menu

Parc

Tableau de bord

Ordinateurs

Moniteurs

Logiciels

Matériels réseau

Périphériques

Imprimantes

Cartouches

Consommables

Téléphones

Baies

Châssis

PDU

Équipements passifs

Équipements non gérés

Câbles

Cartes SIM

Global

Assistance

Gestion

Outils

Accueil / Parc / Ordinateurs

+ Ajouter

Rechercher

Listes

Gabarits

Rechercher

super-admin
...formation (structure complète)

D

Entité racine > Direction Systèmes Information

Sous-entités

Actions

1/1

Ordinateur - I105241

Ordinateur

Analyse d'impact

Systèmes d'exploitation

Composants

Volumes

Logiciels

Connexions

Ports réseau

Connecteurs

Contrôle à distance

Gestion

Contrats

Documents

Virtualisation

Antivirus

Base de connaissances

Tickets

Problèmes

Changements

Liens

Certificats

Verrous

Nom

Lieu

Responsable technique

Groupe technique

Usager numéro

Usager

Utilisateur

Groupe

Commentaires

Dernière date de démarrage

I105241

...SON > DESC_BUISSON_R+2 > D8 245

Dugelay Enzo

edugelay@DSI

Dugelay Enzo

ensl > pres > dgs > dsi > dsi-sgp

2024-09-09 14:53:06

Statut

Type d'ordinateur

Fabricant

Modèle

Numéro de série

Numéro d'inventaire

Réseau

UUID

Source de mise à jour

En service

Ordi portable - PC

Dell Inc.

Latitude 5410

1HXM573

4C4C4544-0048-5810-804D-B1C0

CQ - Resp

Mettre à la corbeille

Sauvegarder

Informations d'inventaire

Agent

UserAgent

Tag d'inventaire

I105241-2023-09-19-11-03-57

GLPI-Agent_v1.7.2

DSI

Adresse publique de contact

Dernier contact

Dernière mise à jour de l'inventaire

140.77.250.129

2024-09-13 17:09

2024-09-13 17:09

Statut de l'agent


Demander un inventaire

Inconnu

Inconnu



Vue personnelle de mes tickets attribués sur GLPI :



ENS DE LYON

Chercher dans le menu

Parc

- Tableau de bord
- Ordinateurs
- Moniteurs
- Logiciels
- Matériels réseau
- Périphériques
- Imprimantes
- Cartouches
- Consommables
- Téléphones
- Baies
- Châssis
- PDU
- Équipements passifs
- Équipements non gérés
- Câbles
- Cartes SIM
- Global

Assistance

- Gestion
- Outils

Accueil

Rechercher

super-admin
...formation (structure complète)

Tableau de bord Vue personnelle Vue groupe Vue globale Flux RSS Formulaires Tableau de bord Tous

TICKETS À TRAITER 1

ID	DEMANDEUR	ÉLÉMENTS ASSOCIÉS	DESCRIPTION
ID : 144398	Roux Serge	Ordinateur - L102364 Ordinateur - L102364 (2) Ordinateur - L102364 (3) Ordinateur - L102364 (4)	Duplication de machine (4 - 0)

NOTES PERSONNELLES

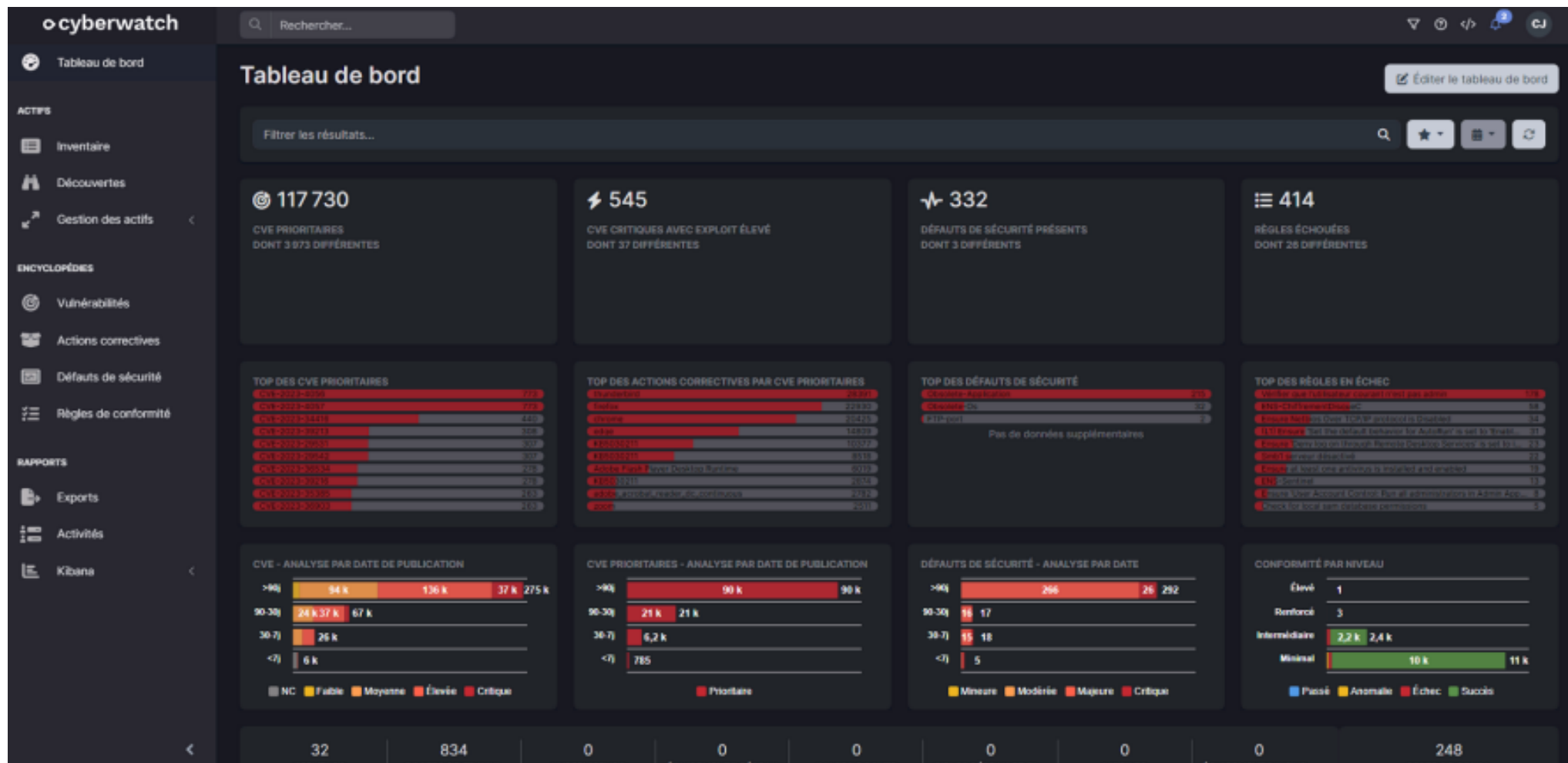
VOTRE PLANNING

Aucun événement à afficher

NOTES PUBLIQUES



Gestion des incidents avec Cyberwatch :





Gestion des ordinateurs sur l'antivirus SentinelOne :

Screenshot of the SentinelOne console interface showing the management of endpoints.

The interface displays the following information:

- Global / ENS LYON** (Top navigation)
- SingularityMarketplace** (Top right)
- Help** and **Colin Jasseron (Admin)** (Top right)
- SENTINELS** (Main navigation)
- ENDPOINTS** (Selected tab)
- TAGS**, **NETWORK ROGUES**, **CLOUD ROGUES**, **POLICY**, **STAR CUSTOM RULES**, **BLOCKLIST**, **EXCLUSIONS**, **NETWORK CONTROL**, **DEVICE CONTROL**, **PACKAGES** (Other tabs)
- Search in network...** (Search bar)
- ENS LYON** (Account: 16 Sites, 1 625 endp...) (Left sidebar)
- CHIMIE** (59), **CIRI** (68), **CRAL** (9), **Default site** (Default) (0), **DSE** (75), **DSI** (834), **DSI_COMPLETE** (157), **ICAR** (11), **IGFL** (48), **LBMC** (101), **LGL** (3), **LIP** (2), **PERSEE** (49), **PHYSIQUE** (72), **RDP** (124), **UMPA** (13) (Left sidebar)
- Select filters...** (Filter bar)
- Load Filter** and **Save Filter** (Buttons)
- Actions** and **Group** (Buttons)
- No Items Selected** (Status)
- 1,625 Endpoints**, **30 Results**, **Columns**, **Export** (Summary and actions)
- Endpoint Name**, **Endpoint Tags**, **Account**, **Site**, **Last Logged In User**, **Group** (Table headers)
- Endpoint Name**, **Endpoint Tags**, **Account**, **Site**, **Last Logged In User**, **Group** (Table rows)

Endpoint Name	Endpoint Tags	Account	Site	Last Logged In User	Group
L100401	N/A	ENS LYON	DSI	cjassero	Default Group
I106666	N/A	ENS LYON	DSI_COMPLETE	oferre	Default Group
I105221	N/A	ENS LYON	DSI_COMPLETE	delhasso	Default Group
I103136	N/A	ENS LYON	DSI_COMPLETE	bguyonne	Default Group
I107512	N/A	ENS LYON	DSI_COMPLETE	ydaoulat	Default Group
I103135	N/A	ENS LYON	DSI_COMPLETE	cguill05	Default Group
I106449	N/A	ENS LYON	DSI_COMPLETE	amunoz	Default Group
I103133	N/A	ENS LYON	DSI_COMPLETE	amunoz	Default Group
L103214	N/A	ENS LYON	DSI_COMPLETE	jgualsno	Default Group
I103154	N/A	ENS LYON	DSI_COMPLETE	patinaud	Default Group



Fiche utilisateur téléphonique sur Omnivista (TOIP) :

OmniVista 8770 - localhost:636 - assistance

Fichier Applications Préférences Action Fenêtre Aide

Réseau

Utilisateurs

Equipements

Configuration

Alarmes

Audit

Maintenance

Utilisateurs

Profils

ENS-LYON [22]

Utilisateurs

Chercher Utilisateurs par attributs communs

Dans ENS-LYON

Avec Nom de famille Contient dugelay

Général Attributs utilisateur Configuration OXE Configuration OT

Dugelay Enzo

Attributs communs	
Hiérarchie	/ ENS-LYON / _CREATIONS
Type d'utilisateur	OXE
Salutation	M.
Nom	Dugelay
Prénom	Enzo
ID d'utilisateur	edugelay
Mot de passe 8770	
Adresse de courrier électronique	enzo.dugelay@ens-lyon.fr
Connexion externe	
Nom de domaine	
Attributs OXE	
Méta profil OXE	
OXE	VMW-TOIP-CALLSERVER
Numéro d'annuaire OXE	1143
Type de terminal	ALE-300
Profil OXE	BUISSON-BASIC
Profil de touches	Aucun
Mot de passe SIP	
Numéro messagerie vocale OXE	1299
Centre de coûts	30
Applications	Aucun