PROJET SECURITE

Règlement Général sur la Protection des Données

Alternant

Yann Gauthier

GMSI B3 2016/2018

Tuteur

Yann Fournier

Table des matières

I- INTRODUCTION

La nouvelle directive européenne (RGPD), entrée en application le 25 mai 2018, transfert aux entreprises la responsabilité de la protection des accès et des données.

Par la nature de son activité de gestion externalisée, Webhelp se doit de proposer à ses clients des solutions de sécurité maximale.

Dans le cadre de mon contrat de professionnalisation ; dans les missions qui m'ont été confiées et que j'ai réalisées, l'une des plus importantes est cette sécurisation des données.

C'est pourquoi, en concertation avec la direction et mon tuteur, j'ai choisi de vous présenter cette partie de mon travail.

Après présentation de l'entreprise, je vais développer la thématique de sécurisation des données en abordant les différentes composantes de sa mise en place.

II- GROUP WEBHELP

a- Présentation

Créé en juin 2000 par Frédéric Jousset et Olivier Duha, Webhelp proposait à l'origine un service d'assistance en ligne en temps réel pour internautes néophytes. L'entreprise a ensuite lancé des opérations de centres d'appels, fournissant des services de hotline (centre d'assistance), de télémarketing et des solutions de traitement d'Emails et de lettres.

Aujourd'hui Webhelp est le leader mondial de l'expérience client et de l'externalisation des processus métiers (BPO*).

L'équipe de Webhelp qui compte plus de 35 000 collaborateurs, fournit des services de gestion de processus métiers et des services externalisés à certaines entreprises comme Sky, Vodafone, Shop Direct, Bouygues, Direct Énergie, KPN et AXA.

Webhelp, dont le siège social est situé à Paris, a augmenté ses revenus de 265% entre 2011 et 2015 en se concentrant sur l'externalisation transformationnelle, l'engagement omnicanal et l'analyse de données pour créer des expériences optimales à destination des clients.

Depuis, Webhelp a grandi suite à une forte croissance de son chiffre d'affaires et grâce à plusieurs acquisitions. L'entreprise est présente dans 28 pays, avec plus de 90 sites d'expérience clients et de services de paiement et plus de 35 000 personnes desservant plus de 500 clients.

*BPO : Business Process Outsourcing

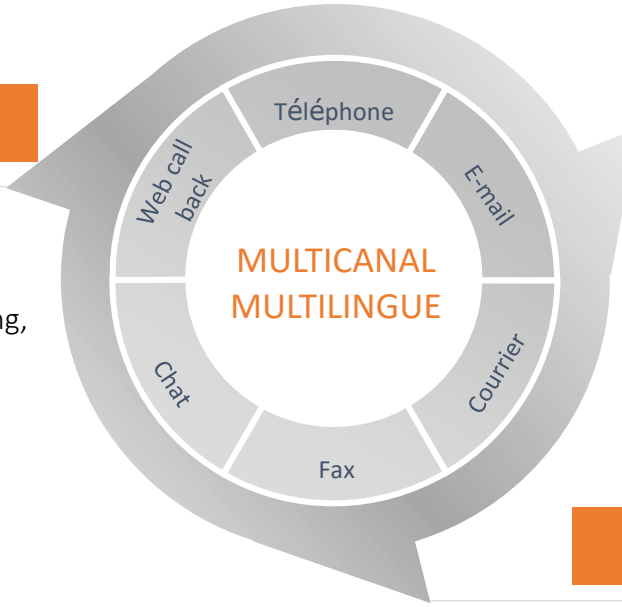
b- Qui sommes-nous ?

Le Groupe Webhelp est spécialisé dans la gestion externalisée de la relation client :

- Multicanal (Téléphone, E-mail, Courrier, Fax, Chat)
- Multiservices (Conseil, Intégration, Edition de technologie et Prestation de services)
- Multilingue

CONQUÊTE

- Acquisition et prise de commande, télévente/télémarketing, prise de rendez-vous…



GESTION

- Service client / SAV, assistance commerciale ou technique, recouvrement, télésecrétariat

FIDÉLISATION

- Gestion de réclamations, rétention, vente additionnelle

Webhelp intervient pour le compte d'un large éventail de clients, démontrant ainsi sa capacité à intégrer des problématiques métiers spécifiques et complexes : Télécoms & Médias, VPC & E-commerce, Services financiers (Assurance, Crédit, Banque), Transport & Energie, Tourisme & Loisirs, Service à la personne, Santé, Informatique, Services aux entreprises…

c- Nos valeurs

Reconnaissance

Respecter la contribution et valoriser la réussite de chacun autour de nous.

Exemplarité

Par notre attitude et notre intégrité, montrer l'exemple en toute circonstance.

Engagement

Tenir sans faille nos promesses envers nos clients et nos collègues.

Unité

Faire passer la réussite commune à long terme avant notre ego et notre intérêt personnel.

Wahou

Créer l'heureuse surprise chez les personnes avec lesquelles nous travaillons.

1- WEBHELP MONTCEAU LES MINES

a- Historique

Webhelp est une société par actions simplifiée en activité depuis septembre 2009 sur le site de Montceau Les Mines.

Elle est spécialisée dans le secteur d'activité des centres d'appels.

Webhelp France préside l'entreprise Webhelp Montceau

b- Capacité

Site 1 : 183 positions

Site 2 : 283 positions + 76 positions formation

c- Effectifs

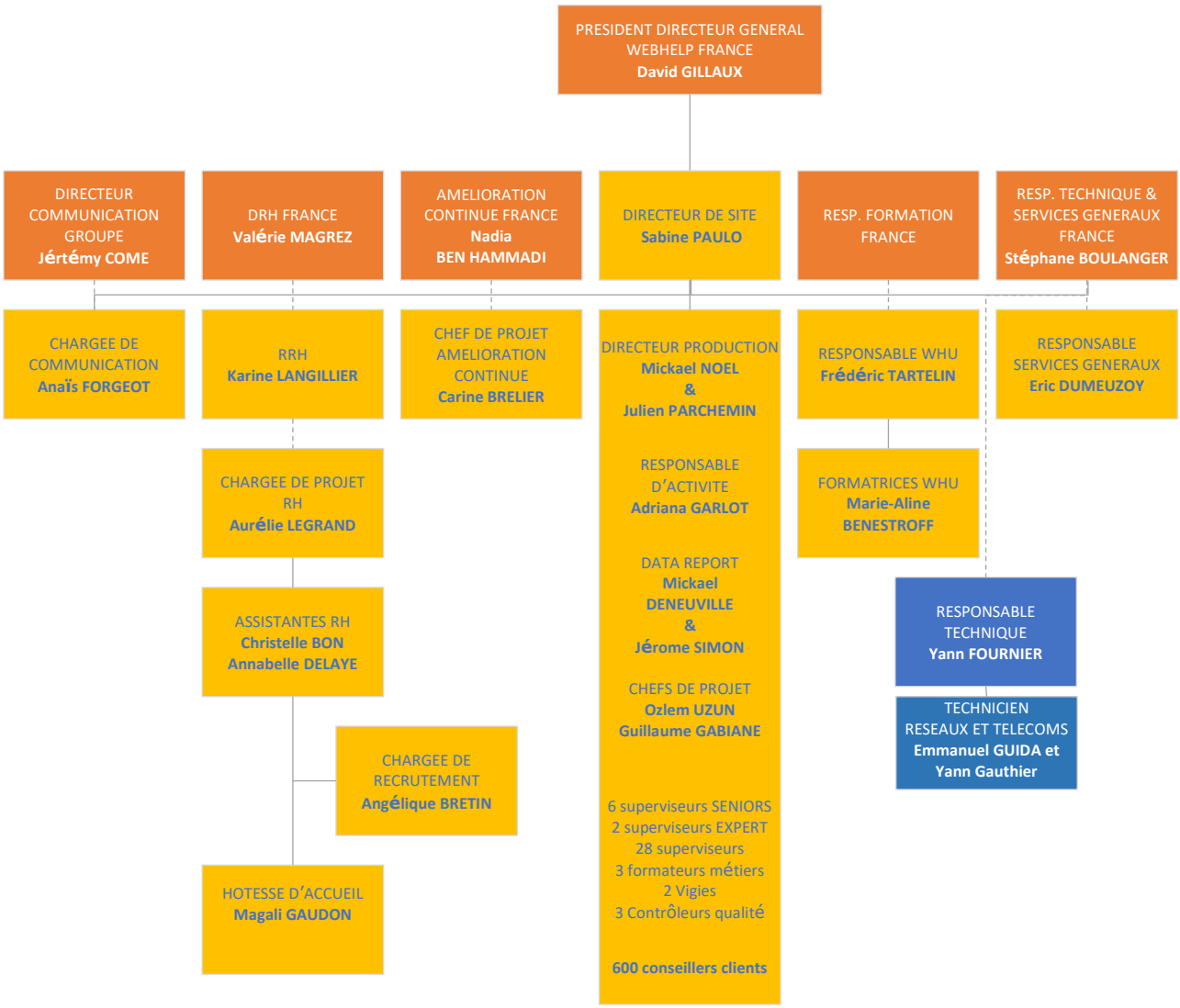
Fin 2009 : 10 collaborateurs

Fin 2014 : 550 collaborateurs, dont 85% de Conseillers Clients.

d- Dix neufs projets clients

SEB, SPECIAL T, BUT, PRIMAGAZ, SAMSUNG, OPAC, LACOMPAGNIE, LDE, BOSH, IPECA, FIOULREDUC, COSTA, AGRICA, VSC (Voyage SNCF), CREDIT FONCIER France, ING BANQUE, MODELAB, ENEDIS, POLE EMPLOI.

e- Organigramme



f- Périmètre d'intervention

- Intervenir dans l'installation et la configuration des systèmes informatiques et télécoms en fonction des spécifications des demandes internes, de la politique de l'entreprise et des législations en vigueur
- Maintenir les systèmes informatiques et télécoms sur le plan hardware et software
- Optimiser les ressources techniques pour prévenir les pannes et les dysfonctionnements
- Veiller à l'application des procédures de maintenance préventive
- Maintenir les systèmes d'échange de données avec les sites distants
- Veiller à la sauvegarde des données et à l'intégrité de ces dernières sur leur site d'affectation
- Veiller à la mise en application des règles de sécurité, de lutte contre le piratage et le vol
- Aider les utilisateurs à l'emploi des matériels et logiciels en production.

III- PRESENTATION PROJET

Ce projet s'inscrit dans le cadre de la nouvelle loi informatique : le Règlement Général Européen sur la Protection des Données (RGPD : règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, entré en application le 25 mai 2018).

Ce règlement renforce la responsabilité des entreprises qui doivent elles-mêmes assurer et mettre en conformité la protection optimale de leur données.

Dans le cadre de ce projet je suis en charge de la remise à niveau du serveur de fichiers, de la sécurisation du parc et de la veille du système de protection des données.

1- La sécurité des données personnelles

- Apprécier les risques engendrés par chaque traitement
- Identifier les impacts potentiels sur les droits et libertés des personnes concernées, pour les trois évènements suivants :
    - Accès illégitime à des données
    - Modification non désirée de données
    - Disparition de données
- Identifier les sources de risques : (qui ou quoi pourrait être à l'origine de chaque évènement redouté), en prenant en compte des sources humaines internes et externes (ex : administrateur informatique, utilisateur, attaquant externe, concurrent), et des sources non humaines internes ou externes (ex : eau, matériau dangereux, virus informatique non ciblé).
- Identifier les menaces réalisables : (qu'est-ce qui pourrait conduire à ce que chaque événement redouté survienne ?). Ces menaces se réalisent via les supports des données (matériels, logiciels, canaux de communication, supports papier, etc.), qui peuvent être :
    - Modifiés
    - Perdus
    - Détériorés
- Déterminer les mesures existantes ou prévues qui permettent de traiter chaque risque (ex : contrôle d'accès, sauvegarde, traçabilité, sécurité des locaux, chiffrement, anonymisation).

2- L'authentification des utilisateurs

Pour s'assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques.

- Définir un identifiant unique par utilisateur et interdire les comptes partagés entre plusieurs utilisateurs. Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, exiger une validation de la hiérarchie et mettre en œuvre des moyens pour les tracer.
- Respecter les recommandations de la CNIL dans le cas d'une authentification des utilisateurs basée sur des mots de passe, notamment en stockant les mots de passe de façon sécurisée et en appliquant les règles de complexité suivantes pour le mot de passe :
    - Au moins 8 caractères comportant 3 des 4 types de caractères (majuscules, minuscules, chiffres, caractères spéciaux) si l'authentification prévoit une restriction de l'accès au compte (cas le plus courant) comme :

- Une temporisation d'accès au compte après plusieurs échecs
- Une « Captcha »
- Un verrouillage du compte après 10 échecs

- 12 caractères minimum et 4 types de caractères si l'authentification repose uniquement sur un mot de passe ;
- Plus de 5 caractères si l'authentification comprend une information complémentaire. L'information complémentaire doit utiliser un identifiant confidentiel d'au moins 7 caractères et bloquer le compte à la 5ème tentative infructueuse ;
- Le mot de passe peut être réduit à 4 caractères si l'authentification s'appuie sur un matériel détenu par la personne et si le mot de passe est utilisé uniquement pour déverrouiller le dispositif matériel détenu en propre par la personne (par exemple une carte à puce ou téléphone portable) et que celui-ci se bloque à la 3ème tentative infructueuse.

3- La sécurisation des postes de travail

Les risques d'intrusion dans les systèmes informatiques sont importants et les postes de travail constituent un des principaux points d'entrée.

- Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné
- Installer un « pare-feu » (« firewall ») logiciel, et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail
- Utiliser des antivirus régulièrement mis à jour et prévoir une politique de mise à jour régulière des logiciels
- Configurer les logiciels pour que les mises à jour de sécurité se fassent automatiquement dès que cela est possible
- Favoriser le stockage des données des utilisateurs sur un espace régulièrement sauvegardé accessible via le réseau de l'organisme plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation
- Limiter la connexion de supports mobiles (clés USB, disques durs externes, etc.) à l'indispensable
- Désactiver l'exécution automatique (« autorun ») depuis des supports amovible.

Pour l'assistance sur les postes de travail :

- Les outils d'administration à distance doivent recueillir l'accord de l'utilisateur avant toute intervention sur son poste, par exemple en répondant à un message s'affichant à l'écran
- L'utilisateur doit également pouvoir constater si la prise de main à distance est en cours et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

4- Protection du réseau informatique interne

- Limiter les accès Internet en bloquant les services non nécessaires (VoIP, pair à pair, etc.)
- Gérer les réseaux Wi-Fi en utilisant un chiffrement dans les règles de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe)
- Etablir une séparation entre le réseau interne et les réseaux ouverts aux invités

- Imposer un VPN pour l'accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.)
- S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet. La télémaintenance doit s'effectuer à travers un VPN
- Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

5- Sécurisation des serveurs

- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
- Utiliser des comptes de moindres privilèges pour les opérations courantes
- Adopter une politique spécifique de mots de passe pour les administrateurs. Changer les mots de passe, au moins lors de chaque départ d'un administrateur et en cas de suspicion de compromission
- Installer les mises à jour critiques sans délai, que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire
- En matière d'administration de bases de données
    - Utiliser des comptes nominatifs pour l'accès aux bases de données et créer des comptes spécifiques à chaque application
    - Mettre en œuvre des mesures contre les attaques par injection de code SQL, de scripts, etc.
    - Effectuer des sauvegardes et les vérifier régulièrement
    - Mettre en œuvre le protocole TLS*(en remplacement de SSL*), ou un protocole assurant le chiffrement et l'authentification, au minimum pour tout échange de données sur internet et vérifier sa bonne mise en œuvre par des outils appropriés.

**TLS / SSL : Transport Layer Security, et son prédécesseur Secure Sockets Layer.*

6- Chiffrage, garantie de l'intégrité ou signature

Les fonctions de hachage permettent d'assurer l'intégrité des données. Les signatures numériques, en plus d'assurer l'intégrité, permettent de vérifier l'origine de l'information et son authenticité.
Le chiffrement, parfois improprement appelé cryptage, permet de garantir la confidentialité d'un message. L'utilisation d'un algorithme reconnu et sûr est indispensable**,** par exemple, les algorithmes suivants :

- SHA-256, SHA-512 ou SHA-3 comme fonction de hachage
- HMAC utilisant SHA-256, AES ou AES-CBC pour le chiffrement symétrique
- RSA-OAEP pour le chiffrement asymétrique
- Pour les signatures, RSA-SSA-PSS
- Utiliser des tailles de clés suffisantes : pour AES il est recommandé d'utiliser des clés de 128 bits et pour les algorithmes basés sur RSA, des modules et exposants secrets d'au moins 2048 bits ou 3072 bits
- Protéger les clés secrètes, au minimum par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr
- Rédiger une procédure indiquant la manière dont les clés et certificats vont être gérés en prenant en compte les cas d'oubli de mot de passe de déverrouillage.

IV- ANTIVIRUS

1- Fonctionnement

Un logiciel antivirus vérifie les fichiers, les courriers électroniques, les secteurs de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont Internet), etc.

Deux méthodes sont possibles :

- Les principaux antivirus du marché se concentrent sur des fichiers et comparent alors la signature virale du virus aux codes à vérifier ;
- La méthode heuristique est la méthode la plus puissante, tendant à découvrir un code malveillant par son comportement. Elle essaie de le détecter en analysant le code d'un programme inconnu. Parfois de fausses alertes peuvent être provoquées.

Les antivirus peuvent balayer le contenu d'un disque dur, mais également la mémoire vive de l'ordinateur. Pour les antivirus les plus modernes, ils agissent en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux descendant (téléchargement) que montant (téléversement ou upload). Ainsi, les courriels sont examinés, mais aussi les fichiers copiés sur ou à partir de supports amovibles tels que cédéroms, disquettes, connexions réseau, clefs USB…

a- Approche

On distingue plusieurs types de logiciels antivirus selon leur fonctionnement. La première méthode est celle du dictionnaire. Les créateurs de logiciels antivirus ayant préalablement identifié et enregistré des informations sur des virus, comme le ferait un dictionnaire, le logiciel antivirus peut ainsi détecter et localiser la présence d'un virus.
On appelle ce dictionnaire la base de définition virale qui contient les signatures de virus.
Lorsque cela se produit, l'antivirus dispose de trois options, il peut :

- Effectuer la suppression du fichier contaminé
- Tenter de réparer le fichier endommagé en éliminant le virus
- Déplacer le fichier dans une zone de quarantaine afin qu'il ne puisse être accessible aux autres utilisateurs et logiciels. Cette action permet d'éviter que le virus se répande (par autoréplication), et éventuellement de réparer le fichier ultérieurement.

Afin de maximiser le rendement de l'antivirus, il est essentiel d'effectuer de fréquentes mises à jour en téléchargeant des versions plus récentes. Des internautes consciencieux et possédant de bonnes connaissances en informatique peuvent identifier eux-mêmes des virus et envoyer leurs informations aux créateurs de logiciels antivirus afin que leur base de données soit mise à jour.
Généralement, les antivirus examinent chaque fichier lorsqu'il est créé, ouvert, fermé ou lu. De cette manière, les virus peuvent être identifiés immédiatement. Il est possible de programmer le système d'administration pour qu'il effectue régulièrement un examen de l'ensemble des fichiers sur l'espace de stockage (disque dur…).
Même si les logiciels antivirus sont très performants et régulièrement mis à jour, une attention soutenue et permanente est indispensable car les créateurs de virus font tout aussi souvent preuve d'inventivité.

b- Comportement suspect

Une autre approche pour localiser les virus consiste à détecter les comportements suspects des programmes. Par exemple, s'il survient une tentative d'écriture des données sur un programme exécuté, de modification ou de suppression de fichiers système, l'antivirus détectera ce comportement suspect et en avisera l'utilisateur qui choisira les mesures à suivre.

V- SYMANTEC ENDPOINT PROTECTION

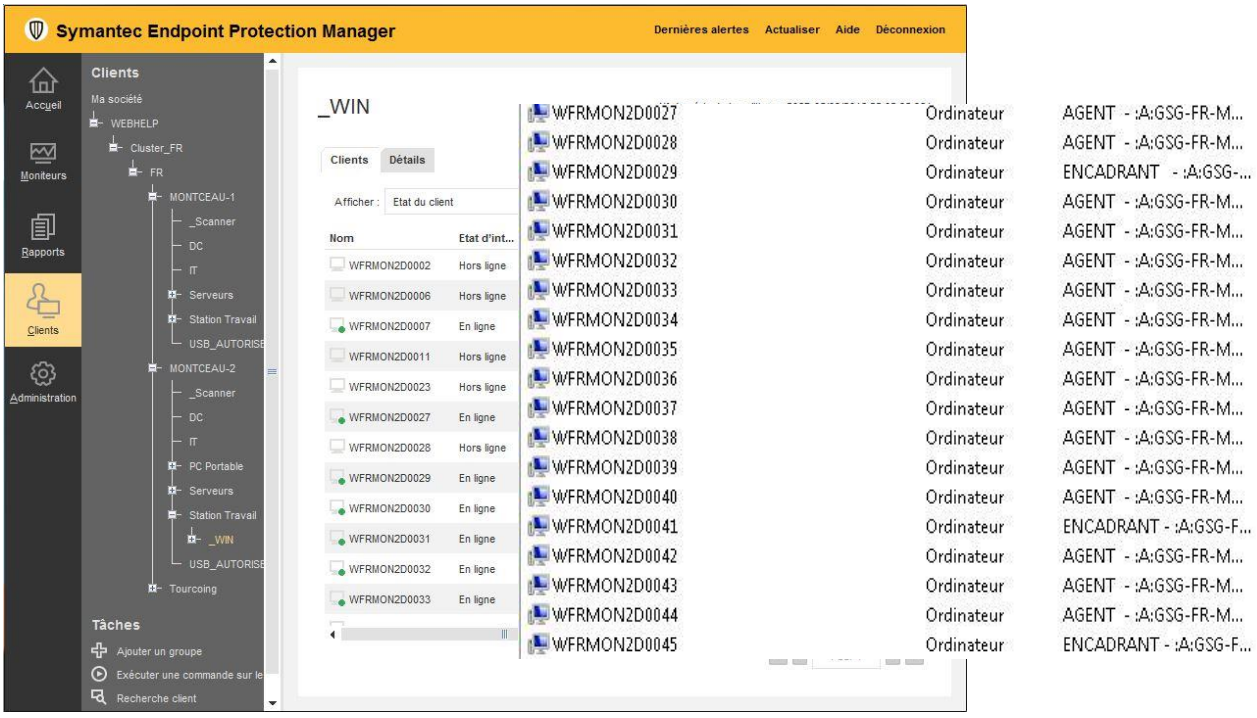
1- Objectif

Webhelp a choisi la solution de sécurité Symantec Endpoint Protection.
Pour garantir une efficacité optimale de protection trois objectifs ont été définis :

1. Equipement de 100% du parc informatique existant
2. Installation systématique sur les nouveaux postes
3. Mise à jour régulière pour l'ensemble du parc

a- Première étape

Symantec Endpoint Protection fourni l'outil console distante Symantec Endpoint Protection Manager.
Celui-ci permet de voir les postes équipés de Symantec, ainsi que la définition virale et la version du client installé sur chaque poste.
Dans le cadre du premier objectif j'ai dû référencer tous les postes manquants dans la console.
Pour cela, je me suis basé sur le contrôleur de domaine.

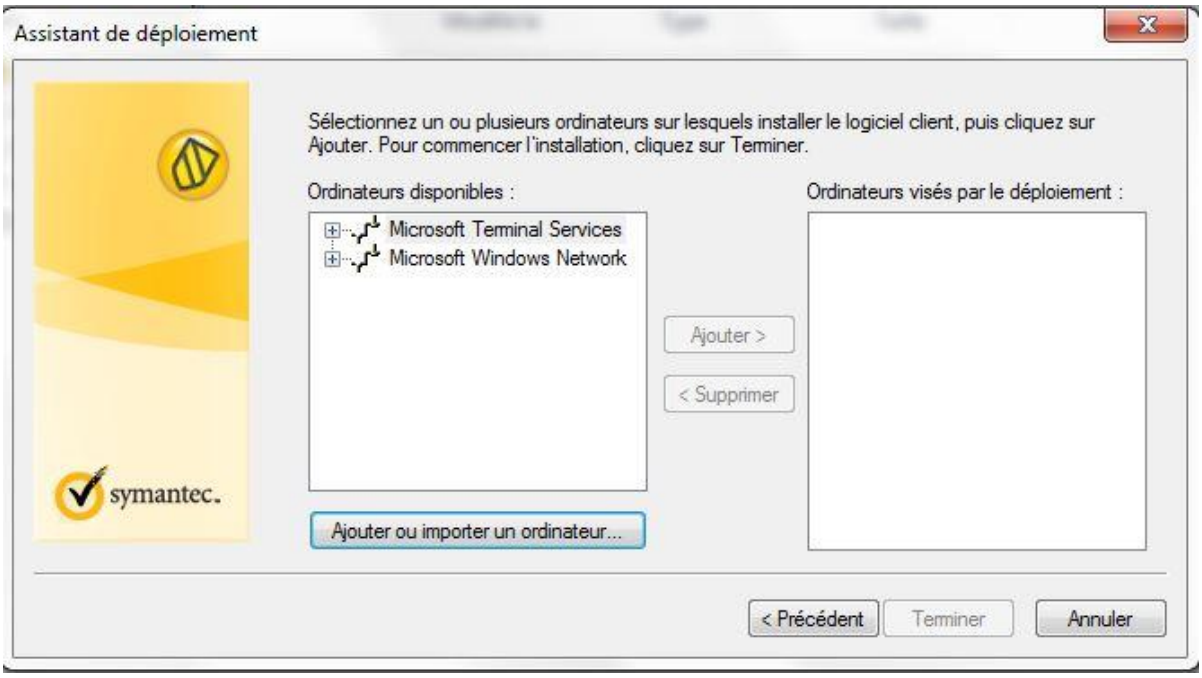


b- Deuxième étape

Il existe deux façons de procéder au déploiement de l'antivirus :

1- Utiliser Push Déploiement Wizard de Symantec
2- Installer l'outil directement sur le poste, en manuel

Dans la plupart des cas j'utilise Push Déploiement Wizard pour chaque nouveau poste à déployer.



Le logiciel de gestion de parc LanSweeper, me permet de détecter quel poste est équipé ou non de l'antivirus.

Workstation: All workstations without Anti-virus software (6)

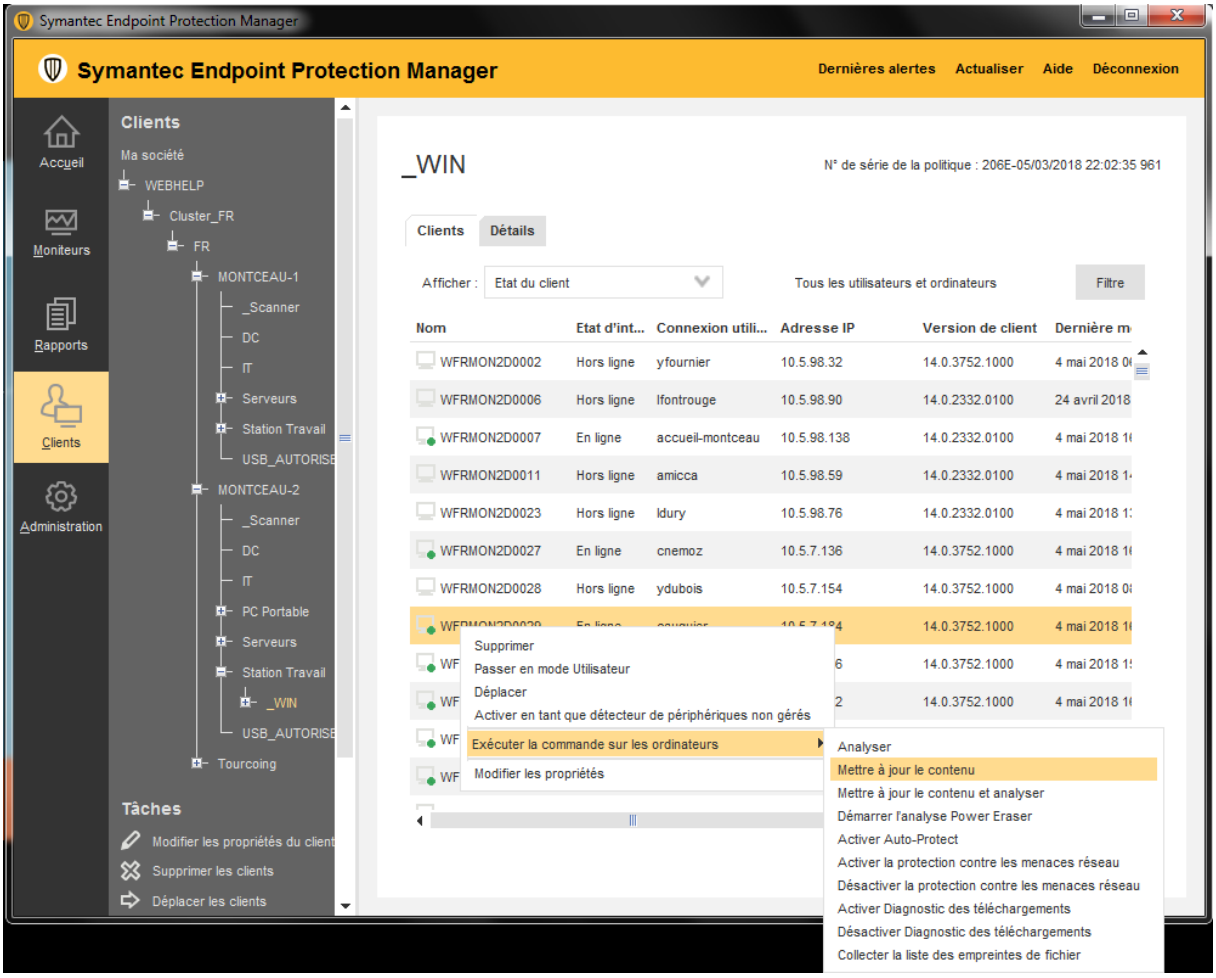
AssetName	Domain	Username	Userdomain	IPAddress	Description
WFRCOM1D9124	WEBHELP	aWebhelp	WFRCOM1D9124	10.5.140.67	
WFRFON1SON01	WEBHELP	tech	WFRFON1SON01	10.5.65.100	
WFRGRA1BKP11	WEBHELP	drosain	WEBHELP	10.5.34.13	Poste Téléco
WFRGRA1BKP15	WEBHELP	lbodart	WEBHELP	10.5.34.16	Poste Téléco
WFRMON2D0041	WEBHELP	pilotage-cff	WEBHELP	10.5.98.144	
WFRMON2D0565	WEBHELP	abretin	WEBHELP	10.5.98.37	

Une fois l'antivirus déployé sur 100% du parc, il est faut le maintenir à jour. Pour cela je regarde la définition antivirus du poste, et la version du client installé sur le poste.

Nom	Etat d'int...	Connexion utili...	Adresse IP		Version de client	Dernière m
WFRMON2D0002	Hors ligne	yfournier		1	14.0.3752.1000	4 mai 2018 0
WFRMON2D0006	Hors ligne	lfontrouge		2	14.0.2332.0100	24 avril 2018

En complément des alertes mail ont été automatisées pour m'informer des postes non mis à jours depuis un certain temps.
Si la version du client est obsolète je redéploye la bonne version. Si la version du client est récente je mets à jour la base virale.

Je dois m'assurer de la mise à jour automatique de l'antivirus. Si je constate une anomalie à ce niveau, je suis chargé de le forcer par l'intermédiaire de la console d'administration de Symantec.



c- Unité d'Organisation (OU)

La console d'administration de Symantec, se compose de plusieurs OU.

Nous retrouvons une « OU FR » où les postes se placent par défaut, une fois l'antivirus installé.

Je dois ensuite déplacer le postes en fonction de leur localisation, pour notre part Montceau 1 ou Montceau 2, afin qu'ils reçoivent les bonnes définitions virales.

VI- CHIFFREMENT DES PC PORTABLES

1- Principales caractéristiques

La méthode de cryptage de Symantec utilisée sur les laptops est PGP* - Cryptage fort et performant, construit avec la technologie PGP Hybrid Cryptographic Optimizer (HCO) et exploitant l'optimisation matérielle AES-NI pour des vitesses de cryptage encore plus rapides.

a- SSO : Single-Sign-On

Single-Sign-On (SSO signifie moins de mots de passe à retenir pour les utilisateurs).

Récupération de clés : plusieurs options de récupération permettent aux organisations de déterminer la solution qui leur convient pour minimiser les verrouillages potentiels et réduire les appels HelpDesk.

Prise en charge du contrôleur de domaine : les stratégies ainsi que les clés individuelles et de groupes peuvent être synchronisées avec le contrôleur de domaine pour accélérer les déploiements et réduire les charges administratives.

Gestion hétérogène : Les capacités de gestion ont été étendues pour inclure la prise en charge de FileVault2 (solution de chiffrement OS native d'Apple), ainsi que la prise en charge des lecteurs à chiffrement automatique.

b- Avantages des clés

Conviviales : l'installation et l'enregistrement sont totalement transparents pour les utilisateurs, tandis que l'utilisation du processeur pendant le cryptage initial est minimisée pour garantir que les utilisateurs puissent continuer à être productifs pendant le cryptage en arrière-plan.

Flexibles : prend en charge les déploiements multi-utilisateurs dans des environnements Active Directory et non Active Directory

Collaboratives : les utilisateurs peuvent accéder aux données chiffrées sur un support amovible en toute sécurité, même sur les systèmes sans Symantec Endpoint Encryptions.

Évolutives : l'architecture de gestion évolutive s'adapte facilement aux environnements des entreprises.

Protection renforcée - Le logiciel DLP (Data Loss Prevention) leader de Symantec s'intègre au chiffrement amovible des supports pour analyser les données avant leur transfert et chiffrer automatiquement les données sortantes sensibles.

*PGP : Pretty Good Privacy

2- Symantec Endpoint Encryption

a- Objectifs

Les objectifs du chiffrement des laptops sont :

- 100% des laptops chiffré
- Permettre un accès unique et sécurisé
- Sécuriser les données en cas de vol de celui-ci

b- Première étape

Le chiffrement des laptops est nécessaire, car ils sont utilisés en extérieur de l'entreprise, et peuvent subir le risque de vol ou de perte.

Le chiffrement se fait par l'intermédiaire de Symantec Endpoint Encryption. Le logiciel utilise le chiffrement en PGP.

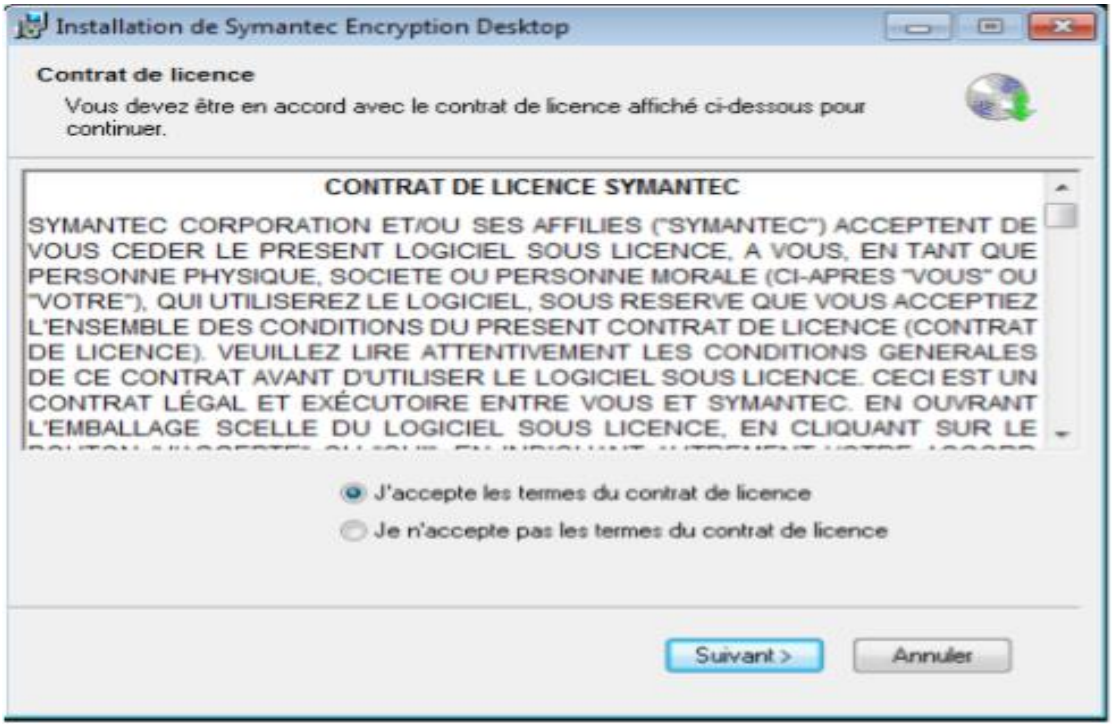
Le chiffrement des laptops se faisant manuellement, il faut installer sur celui-ci Symantec Endpoint Encryption.

La consultation du contrôleur de domaine m'aide à déterminer à qui appartient le laptop.

Cela me permet de demander ensuite aux personnes concernées leur PC, pour effectuer le chiffrement. Cela concerne principalement les personnes ayant des fonctions supports (direction, chefs de projet, superviseur, etc..).

Nom	Type	Description
WFRMON1L0004	Ordinateur	PORTABLE USER ASTREINTE BSH - :A:GSG-FR-...
WFRMON1L0006	Ordinateur	PORTABLE SUPPORT COMM - :A:aforgeot:A:
WFRMON1L0011	Ordinateur	PORTABLE SUPPORT TECH - :A:GSG-FR-MON...
WFRMON1L0013	Ordinateur	PORTABLE USER ASTREINTE BSH - :A:GSG-FR-...
WFRMON1L0016	Ordinateur	PORTABLE SUPPORT Élodie (DELL 5440) - :A:e...
WFRMON1L0021	Ordinateur	PORTABLE SUPPORT Yann - :A:yfournier:A:
WFRMON1L0024	Ordinateur	PORTABLE SUPPORT Mickael Noel - :A:mnoel:A:
WFRMON1L0026	Ordinateur	PORTABLE SUPPORT Nadège COSTA - :A:ncos...
WFRMON1L0027	Ordinateur	PORTABLE DIRECTRICE HP - :A:spaulo:A:
WFRMON1L0028	Ordinateur	PORTABLE SUPPORT HP Adriana - :A:agarlot:A:
WFRMON1L0029	Ordinateur	PORTABLE SUPPORT HP Special T Laetitia - :A:...
WFRMON1L0030	Ordinateur	PORTABLE SUPPORT HP LDE Joelle - :A:jmame...
WFRMON1L0031	Ordinateur	PORTABLE SUPPORT HP SFR Chaouki - :A:cdja...

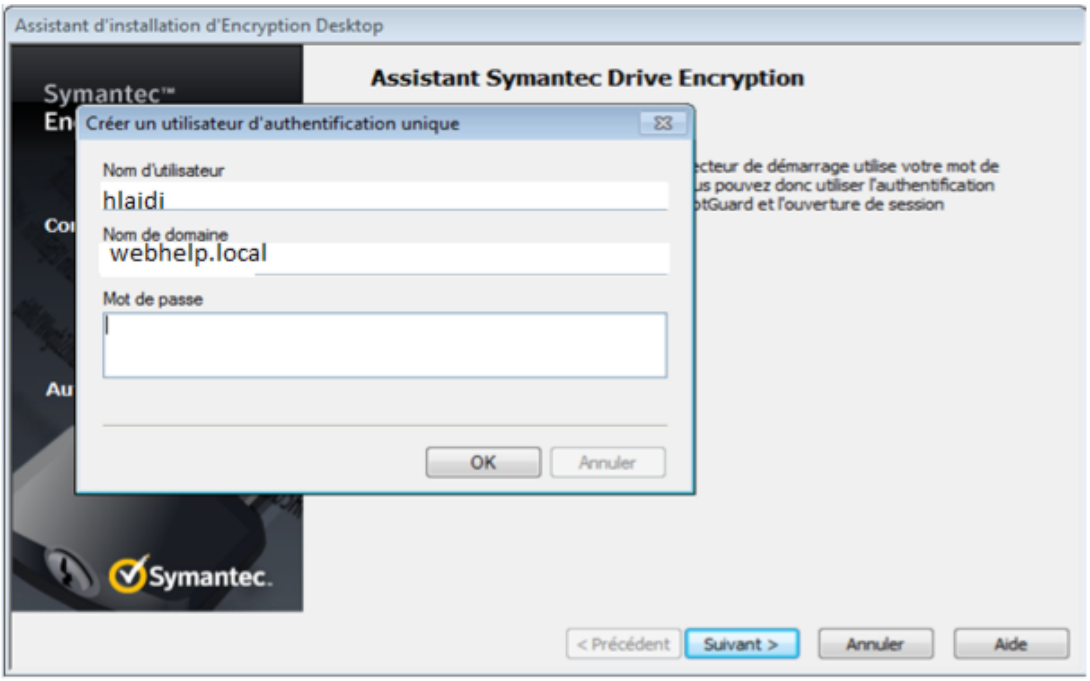
Puis j'installe Symantec Endpoint Encryption.



Une fois cet outil installé, je saisis les sessions administrateurs dans le logiciel, afin qu'en cas de panne je puisse intervenir sur le PC.

Je demande à chacun de rentrer sa session respective, d'abord à mes collègues du service informatique, puis à l'utilisateur du PC.

Cette procédure effectuée, je lance le chiffrement. La durée est d'environ 2h pour un PC avec SSD et environ 6h pour un HDD.



L'information de bonne exécution du chiffrement est confirmée par une icône en forme de petit cadenas

c- Deuxième étape

Une fois le chiffrement terminé je redémarre le poste et je guide l'utilisateur pour se connecter à sa session.

Lors du démarrage de Windows une page Symantec s'affiche et demande le nom d'utilisateur puis son mot de passe.

On peut sélectionner le domaine, donc pour ce qui nous concerne c'est le domaine Webhelp.

En cas d'oubli de mot de passe, l'accès à la console Web de Symantec, me permet de débloquer le PC concerné.

VII- SERVEUR DE FICHIERS

Dans le cadre de la sécurisation des données à caractère personnel et le respect de la réglementation en vigueur en termes de durée de rétention, il est demandé d'unifier tous les partages réseau et les nomenclatures des dossiers sur les serveurs du site.

Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu.

La sécurité des systèmes d'information vise les objectifs suivants :

1. La disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installés avec le temps de réponse attendu
2. L'intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets
3. La confidentialité : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que :

1. La traçabilité (ou « preuve ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables
2. L'authentification: l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange
3. La non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Une fois les objectifs de la sécurisation déterminés, les risques pesant sur chacun de ces éléments peuvent être estimés en fonction des menaces. Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Il faut pour cela estimer :

1- La gravité des conséquences au cas où les risques se réaliseraient ;
2- La vraisemblance des risques (ou leur potentialité, ou encore leur probabilité *).*

1- Mise en place du nouveau serveur de fichier

a- Objectifs

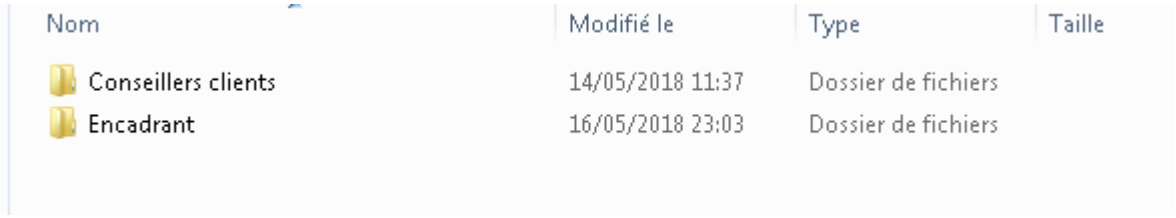
- Sécuriser les informations et l'accès aux dossiers du serveur
- Elaborer une arborescence unique des dossiers du partage réseau
- Définir les types de documents et fichiers sauvegardés dans ces dossiers : doc, xlsx, .png …
- Fixer la durée de rétention de ces fichiers
- Gagner de l'espace sur le serveur de stockage.

b- Première étape

1- Avant la Migration.

a- Définition de l'architecture.

La direction a défini une architecture type que je dois mettre en place avec mon tuteur.



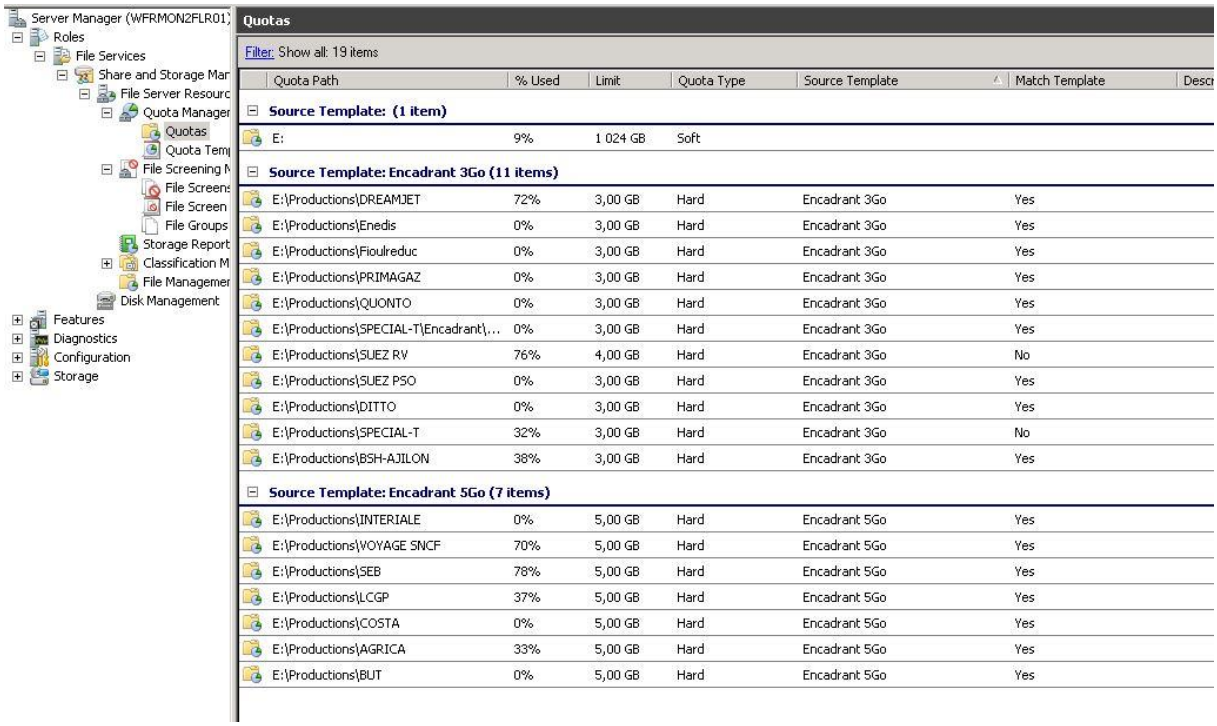
Mon tuteur adapte cette architecture à nos besoins, pour lesquels j'ai créé des dossiers en fonction des projets présents sur notre site.

Une fois cette architecture mise en place je suis chargé de finaliser le paramétrage d'utilisation des répertoires, dossiers et fichiers

2- Création des quotas

a- Mise en place des quotas et de leur capacité

Pour effectuer ce travail, je m'appuis sur les instructions définies par mon tuteur et la direction.



Quota Path	% Used	Limit	Quota Type	Source Template	Match Template
Source Template: (1 item)					
E:	9%	1 024 GB	Soft		
Source Template: Encadrant 3Go (11 items)					
E:\Productions\DREAMJET	72%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\Enedis	0%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\Fioulreduc	0%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\PRIMAGAZ	0%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\QUONTO	0%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\SPECIAL-T\Encadrant\...	0%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\SUEZ RV	76%	4,00 GB	Hard	Encadrant 3Go	No
E:\Productions\SUEZ PSO	0%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\DITTO	0%	3,00 GB	Hard	Encadrant 3Go	Yes
E:\Productions\SPECIAL-T	32%	3,00 GB	Hard	Encadrant 3Go	No
E:\Productions\BSH-AJILON	38%	3,00 GB	Hard	Encadrant 3Go	Yes
Source Template: Encadrant 5Go (7 items)					
E:\Productions\INTERIALE	0%	5,00 GB	Hard	Encadrant 5Go	Yes
E:\Productions\VOYAGE SNCF	70%	5,00 GB	Hard	Encadrant 5Go	Yes
E:\Productions\SEB	78%	5,00 GB	Hard	Encadrant 5Go	Yes
E:\Productions\LCGP	37%	5,00 GB	Hard	Encadrant 5Go	Yes
E:\Productions\COSTA	0%	5,00 GB	Hard	Encadrant 5Go	Yes
E:\Productions\AGRICA	33%	5,00 GB	Hard	Encadrant 5Go	Yes
E:\Productions\BUT	0%	5,00 GB	Hard	Encadrant 5Go	Yes

Il a été décidé que les projets de plus de 15 positions agents dit « gros projet » ont un quota limité de 5 GB et les projets en dessous de 15 position agent dit « petit projet » ont un quota limité de 3 GB.

Encadrant 3Go	3,00 GB	Hard	Encadrant 3Go
Encadrant 5Go	5,00 GB	Hard	Encadrant 5Go

b- Mise en place des restrictions du type de fichier par dossier

Pour plus de sécurité, il a été décidé de restreindre le type de fichier mis sur le réseau.

Pour certains dossiers j'autorise uniquement les fichiers Word, Excel et texte. Tous les autres fichiers seront refusés.

Filter: Show all: 4 items

File Screen Path	Screening Type	File Groups	Source Template	Match Ter
Source Template: (2 items)				
E:\Productions\SPECIAL-T\Encadrant\6- ...	Exception	Allow: Audio and Video Files, Image Files, I...		
E:\Productions\SPECIAL-T\Encadrant\7- ...	Exception	Allow: Images à autoriser		
Source Template: Production: block (2 items)				
E:\	Passive	Warn: Audio and Video Files, Backup Files, ...	Production: block	No
E:\Productions	Passive	Warn: Audio and Video Files, Backup Files, ...	Production: block	No

c- Mise en place des droits par dossier (script).

Nous utilisons le script pour pouvoir mettre en place les droits rapidement en cas de problème avec le serveur de fichiers.

L'utilitaire de Windows Serveur, Icacls.exe, me permet de définir ces droits.

Pour la mise en place du script j'ai procédé à une recherche sur le web, pour pouvoir mieux comprendre son fonctionnement ainsi que son écriture.

Ce script sert uniquement à mettre les droits sur les dossiers du serveur de fichier.

```
icacls "E:\Productions\SPECIAL-T" /T /Q /C /reset

icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-AGENTS":(RX)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-FORMATION-FRANCE":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-FORMATION-MONTCEAU":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-ANALYSTE-MONTCEAU":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-CODIR-MONTCEAU":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-DIRECTION-MONTCEAU":(OI)(CI)M
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-TECHNIQUE-MONTCEAU":(OI)(CI)F
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-LOCAL-it":(OI)(CI)F

icacls "E:\Productions\SPECIAL-T\Conseillers clients" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-ALL":(OI)(CI)
(RX,WD)
icacls "E:\Productions\SPECIAL-T\Conseillers clients" /grant "GSG-FR-MON1-FORMATION-FRANCE":(OI)(RX,WD)

icacls "E:\Productions\SPECIAL-T\Encadrant" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(RX)
icacls "E:\Productions\SPECIAL-T\Encadrant" /grant "GSG-FR-MON1-FORMATION-FRANCE":(RX)
icacls "E:\Productions\SPECIAL-T\Encadrant" /grant "GSG-FR-MON1-FORMATION-MONTCEAU":(RX)

icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-
NOTAGENTS":(OI)(CI)(RX)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Gestion flux planification\Rapport planification"
/grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Gestion flux planification\Prévision" /grant "GSG-FR-
MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Instances\Comité Pilotage" /grant "GSG-FR-MON1-NESTLE-
SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Instances\Comité Production" /grant "GSG-FR-MON1-
NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Contrat - Facturation\Finances\Efficiency" /grant
"GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
```

Montage du script pour l'accès au dossier Production à ALL-NOT-AGENT (Encadrant) : \\WFRMON2FLR01\Productions.

```
icacls "E:\Productions\SPECIAL-T" /T /Q /C /reset

icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-AGENTS":(RX)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-FORMATION-FRANCE":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-FORMATION-MONTCEAU":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-ANALYSTE-MONTCEAU":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-CODIR-MONTCEAU":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-DIRECTION-MONTCEAU":(OI)(CI)M
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-TECHNIQUE-MONTCEAU":(OI)(CI)F
icacls "E:\Productions\SPECIAL-T" /grant "GSG-FR-MON1-LOCAL-it":(OI)(CI)F

icacls "E:\Productions\SPECIAL-T\Conseillers clients" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-ALL":(OI)(CI)
(RX,WD)
icacls "E:\Productions\SPECIAL-T\Conseillers clients" /grant "GSG-FR-MON1-FORMATION-FRANCE":(OI)(RX,WD)

icacls "E:\Productions\SPECIAL-T\Encadrant" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(RX)
icacls "E:\Productions\SPECIAL-T\Encadrant" /grant "GSG-FR-MON1-FORMATION-FRANCE":(RX)
icacls "E:\Productions\SPECIAL-T\Encadrant" /grant "GSG-FR-MON1-FORMATION-MONTCEAU":(RX)

icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-
NOTAGENTS":(OI)(CI)(RX)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Gestion flux planification\Rapport planification"
/grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Gestion flux planification\Prévision" /grant "GSG-FR-
MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Instances\Comité Pilotage" /grant "GSG-FR-MON1-NESTLE-
SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Instances\Comité Production" /grant "GSG-FR-MON1-
NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\2- Top management\Contrat - Facturation\Finances\Efficiency" /grant
"GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)

icacls "E:\Productions\SPECIAL-T\Encadrant\1- Annuaire projet" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-
NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\1- Annuaire projet" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-
NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\3- Middle Management" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-
NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\4- Reporting Performances" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-
MONTCEAU-NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\5- Gestion RH" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":
(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\6- Qualité - Formation" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-
NOTAGENTS":(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\7- Technique" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":
(OI)(CI)(RX,WD)
icacls "E:\Productions\SPECIAL-T\Encadrant\OLD_SPECIAL-T" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-NOTAGENTS":
(OI)(CI)M
icacls "E:\Productions\SPECIAL-T\Encadrant\Transfert à arbitrer" /grant "GSG-FR-MON1-NESTLE-SPECIAL-T-MONTCEAU-
NOTAGENTS":(OI)(CI)M
```

c- Deuxième étape

Pour un bon déroulement de la mise en place du serveur du fichier, un planning de la migration a été défini.

1- Planning de la migration

- à J-1, la veille de la migration, la copie du projet concerné est envoyée vers le dossier de sauvegarde Productions\Projet\Encadrant\OLD_PROJET

- au jour J, les modifications des macros des fichiers Excel sont effectuées, puis l'encadrant du projet est guidé pour déplacer les fichiers copiés dans OLD_PROJET vers le nouveau dossier du projet dans les bons dossiers et sous-dossiers

- à J+1, le lendemain, le dossier OLD_PROJET est mis en lecture seule et conservé 10 jours avant d'être supprimé

- Les dossiers projets de l'ancien serveur seront supprimés au bout de 30 jours.

VIII- CONCLUSION

WEBHELP, en tant que fournisseur mondial de BPO (externalisation de services) est soucieux de satisfaire ses clients. Dans cet objectif, en respect de la nouvelle loi informatique au niveau européen (RGPD), l'entreprise répond à cette obligation.

Dans ce cadre, j'assure le développement de la sécurité du système d'information, avec le soutien de mon tuteur et de mon autre collègue.

J'ai donc participé activement à l'installation du logiciel antivirus sur toutes les postes informatiques du site de Montceau Les Mines (environ 600) et je suis en cours de finalisation sur les PC portables.

La performance de la protection antivirale est conditionnée à une veille permanente afin d'assurer les mises à jour indispensables à une défense efficace. Celle-ci est effectuée hors du site de Montceau Les Mines mais une de mes tâches quotidiennes consiste à contrôler que les mises à jour soient effectives sur tout le parc informatique (version client, définition virale).

En cas de défaillance de la mise à jour automatique je force celle-ci par l'intermédiaire de la console Symantec.

J'interviens également sur le serveur de fichier, pour sécuriser les informations en appliquant les règles de la RGPD.

La mise en place de ces nouvelles règles européennes a été un challenge pour l'entreprise, que nous avons réussi collectivement malgré quelques problèmes internes de mise en place que nous avons su résoudre.

En ce qui me concerne, ces contraintes ont été positives pour ma formation et m'ont permis de mener à bien mon projet. Cette expérience a amélioré mes savoirs et m'a fait progresser dans l'acquisition de compétences, dont la rigueur et l'organisation indispensables dans le domaine informatique. Elle m'a également permis de gagner en autonomie en ayant une plus grande confiance en moi dans la résolution des problèmes auxquels j'ai été confronté.

La sécurité des données des entreprises ou personnelles, qu'elles soient privées ou déposées sur les réseaux sociaux, est un sujet d'actualité mondial. La lutte contre le vol, la modification ou disparition de données, ainsi que les ransomware et cyberattaques ne peuvent que s'amplifier et motiver une plus grande attention de la part des responsables des systèmes d'information. De nouveaux métiers se sont développés et me semble être un créneau porteur d'emplois vers lesquels je pourrais éventuellement me tourner.

IX- REMERCIEMENTS

Je remercie la direction de Webhelp de m'avoir accordé sa confiance en acceptant mon contrat de professionnalisation au sein de l'équipe informatique de Montceau Les Mines.

J'ai ainsi pu mener, pendant ces deux années, mon projet personnel dans de très bonnes conditions matérielles et intellectuelles, grâce à mon tuteur Yann FOURNIER qui m'a guidé et épaulé tout au long de ce cursus.

Je remercie également mon collègue Emmanuel GUIDA pour m'avoir formé et aussi accompagné.

J'ai découvert un univers professionnel que j'ai appris à mieux connaître et apprécier, au sein d'une entreprise dynamique, performante et accueillante.

J'ai été conforté dans la voie professionnelle que j'ai choisie et pour laquelle j'ai acquis et développé des compétences solides et durables, complétées par l'enseignement du CESI que je remercie ici également, pour son appui éducatif, son professionnalisme et son sérieux.

Les semaines passées au CESI, ont été très productives et m'ont aidé à mener à bien ce dossier. J'y ai trouvé une ambiance de travail collective agréable et profitable. Pour cela, je remercie les intervenants et l'ensemble de mes camarades de formation pour le travail effectué en commun.

X- ANNEXES

1- Détail du Script

icacls "chemin_complet_du_dossier" /T /Q /C /RESET #Permet de remettre à plat les droits affectés au dossier

takeown /F e:\test /R /D y #Permet de devenir le propriétaire du dossier

Syntax

Add or remove permissions:

ICACLS Name

[/grant[:r] User:Permission[...]]

[/deny User:Permission[...]]

[/remove[:g|:d]] User[...]]

[/inheritance:e|d|r]

[/setintegritylevel Level[...]]

[/T] [/C] [/L] [/Q]

Store ACLs for one or more directories matching name into aclfile for later use with /restore:

ICACLS name /save aclfile [/T] [/C] [/L] [/Q]

Restore ACLs to all files in directory:

ICACLS directory [/substitute SidOld SidNew [...]]

/restore aclfile [/C] [/L] [/Q]

Change Owner:

ICACLS name /setowner user [/T] [/C] [/L] [/Q]

Find items with an ACL that mentions a specific SID:

ICACLS name /findsid Sid [/T] [/C] [/L] [/Q]

Find files whose ACL is not in canonical form or with a length inconsistent with the ACE count:

ICACLS name /verify [/T] [/C] [/L] [/Q]

Replace ACL with default inherited acls for all matching files:

ICACLS name /reset [/T] [/C] [/L] [/Q]

This is equivalent to “Replace all child permission entries with inheritable permission from this object” in the GUI.

Key

name The File(s) or folder(s) the permissions will apply to.

/T Traverse all subfolders to match files/directories. This will apply permission changes to all subfolders whether or not they are set to inherit permissions from the parent. On very large directory structures this may take some time as the command has to traverse the entire tree.

/C Continue on file errors (access denied) Error messages are still displayed.

/L Perform the operation on a symbolic link itself, not its target.

/Q Quiet - supress success messages.

/grant :r user:permission

Grant access rights, with :r, the permissions will replace any previouly granted explicit permissions (for the given user). Otherwise the permissions are added.

/deny user:permission

Explicitly deny the specified user access rights. This will also remove any explicit grant of the same permissions to the same user.

/remove[:[g|d]] User

Remove all occurrences of User from the acl.

:g remove all granted rights to that User/Sid.

:d remove all denied rights to that User/Sid.

/inheritance:e|d|r

e - Enable inheritance

d - Disable inheritance and copy the ACEs

r - Remove all inherited ACEs

/setintegritylevel [(CI)(OI)]Level

Add an integrity ACE to all matching files.

level is one of L,M,H (Low Medium or High)

A Directory Inheritance option for the integrity ACE can precede the level and is applied only to directories:

user A user account, Group or a SID

/restore Apply the acls stored in ACLfile to the files in directory

permission is a permission mask and can be specified in one of two forms:

a sequence of simple rights:

D - Delete access

F - Full access (Edit_Permissions+Create+Delete+Read+Write)

N - No access

M - Modify access (Create+Delete+Read+Write)

RX - Read and eXecute access

R - Read-only access

W - Write-only access

a comma-separated list in parenthesis of specific rights:

DE - Delete

RC - read control

WDAC - write DAC

WO - write owner

S - synchronize

AS - access system security

MA - maximum allowed

GR - generic read

GW - generic write

GE - generic execute

GA - generic all

RD - read data/list directory

WD - write data/add file

AD - append data/add subdirectory

REA - read extended attributes

WEA - write extended attributes

X - execute/traverse

DC - delete child

RA - read attributes

WA - write attributes

inheritance rights can precede either form and are applied only to directories:

(OI) - object inherit

(CI) - container inherit

(IO) - inherit only

(NP) - don’t propagate inherit

(I) - Permission inherited from parent container

2- Références

Règlement Générale sur le Protection des donnée :

https://www.cnil.fr

Antivirus et chiffrage des PCs :

https://www.symantec.com/fr/fr

Serveur de Fichier :

https://www.amj-groupe.com/securite-des-systemes-dinformation/

et :

Webhelp