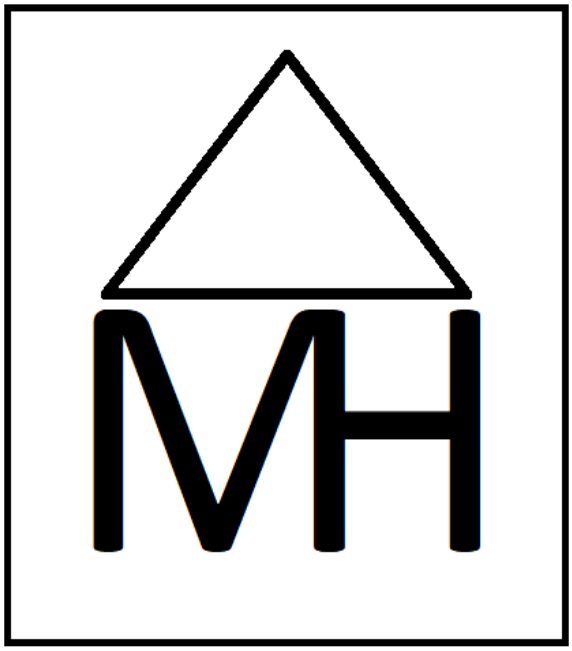
GMSI 16. Cas H 2e partie

RÉPONSE À L'APPEL D'OFFRES PAR

POUR LA **SOCIÉTÉ MODULHAB**



Chirol Pierrick, Gérard Nicolas

2017/2018

Table des matières

1.TRUST-IT

1.1 Qui sommes-nous ?

Trust-IT est une société de services du numérique (ESN) qui s'est développée dans la région lyonnaise à partir des années 2000. Misant avant tout sur l'écoute et la compréhension du besoin du client, notre société a progressivement gagné la confiance des petites et moyennes entreprises si bien que notre aire d'influence a progressivement dépassé le département du Rhône.

Implantation des principaux clients de Trust-IT

Fidèle à ses principes initiaux, Trust-IT reste conscient des enjeux du numérique en se tenant régulièrement au fait des dernières évolutions pour vous apporter un niveau de qualité optimal en pratiquant notamment des activités de :

- **Conseil** : attentif à vos besoins, nous prenant en compte les spécificités de chaque client.
- **Intégration d'infrastructures systèmes & réseaux** : Nous concevons des solutions sur mesure qui s'adapte à votre société.
- **Infogérance** : Votre service informatique peut compter sur le soutien et l'expertise de nos équipes pour vous accompagner au quotidien dans la gestion de votre système d'information afin que vous puissiez vous reconcentrer sur votre cœur de métier.
- **Formation** : Nos experts peuvent assister vos techniciens et vos utilisateurs en dispensant des formations sur les technologies informatiques utilisées afin de faciliter leur prise en main après la livraison de nos solutions.

Passionnés par notre métier, nous sommes soucieux de vous apporter des solutions techniques adaptées à vos besoins tout en vous laissant le choix de l'évolutivité afin de mieux vous accompagner dans la mutation de votre société.

1.2 Mentions légales

Trust-IT est une société à responsabilité limitée (SARL) active depuis 18 ans. Son siège est situé au :

59 rue Denuzière

69002 LYON

SIREN 453 789 124
SIRET 45378912311245
Forme juridique : SARL
Date immatriculation RCS 05-03-2000
Tranche d'effectif : 40-49 salariés
Capital social : 65000,00 €
Chiffre d'affaires 2017 : 5 357 000,00 €

1.3 Partenaires

La sélection de nos partenaires s'est faite selon les critères suivants

- Stabilité & robustesse
- Garanties avantageuses
- Renommée & expertise
- Évolutivité des solutions

	Serveurs
	Routeurs et commutateurs
	Postes informatiques (fixes et portables)
	Administration de serveurs Windows
	Administration de serveurs Linux
	Solution de virtualisation Open Source
	Solutions d'hébergements présentant plusieurs gammes de prestations intéressantes pour les professionnels
	Logiciel de sauvegardes de données
	Solution antivirale

1.4 Certifications

Les compétences de nos équipes s'adaptent à l'évolution des technologies que nous mettons en œuvre pour nos clients en les actualisant au moyen des certifications suivantes :

Certification Microsoft (MCSA, « Microsoft Certified Solutions Associate »)

- MCSA Windows Server 2008
- MCSA Windows Server 2012
- MCSA Windows Server 2016

Certification Linux

- RHCA, Architecte certifié Red Hat (« Red Hat Certified Architect »)
- RHCSA, Administrateur système certifié Red Hat

Certification CISCO

- CCNA
- CCNP

1.5 Équipe chargée d'élaborer votre solution

L'étude du cahier des charges que vous avez émis a été confiée à deux membres de notre équipe qui ont pu échanger avec le DAF et plusieurs responsables des services de Modulhab afin d'adapter notre solution à vos problématiques de travail :

- Pierrick, Administrateur systèmes & réseaux, conseiller.
- Nicolas, Administrateur systèmes, responsables logiciels et maintenance, conseiller.

Ces deux collaborateurs vous accompagnent tout au long de votre projet pour vous apporter leur expertise en pratiquant des activités de conseil dans leur domaine respectif.

2. LE CLIENT MODULHAB

2.1 Présentation de la société

La société ModulHab, créée en 2006, est spécialisée dans la conception et la création d'habitations et de bâtiments modulables qui s'inscrit dans une démarche de développement durable, notamment par l'utilisation de containers fabriqués à partir de matériaux composites naturels.

ModulHab connait une évolution très forte depuis ses dernières années suite à la diversification de ses partenaires en proposant notamment ses services auprès des collectivités (conception de logements sociaux ou étudiants à moindre coût).

Le chiffre d'affaires de ModulHab pour 2017 est de 12 millions d'euros.

La société emploie 272 collaborateurs. Ce chiffre n'a cessé de croître ces dernières années après l'obtention de nombreux appels d'offres importants.

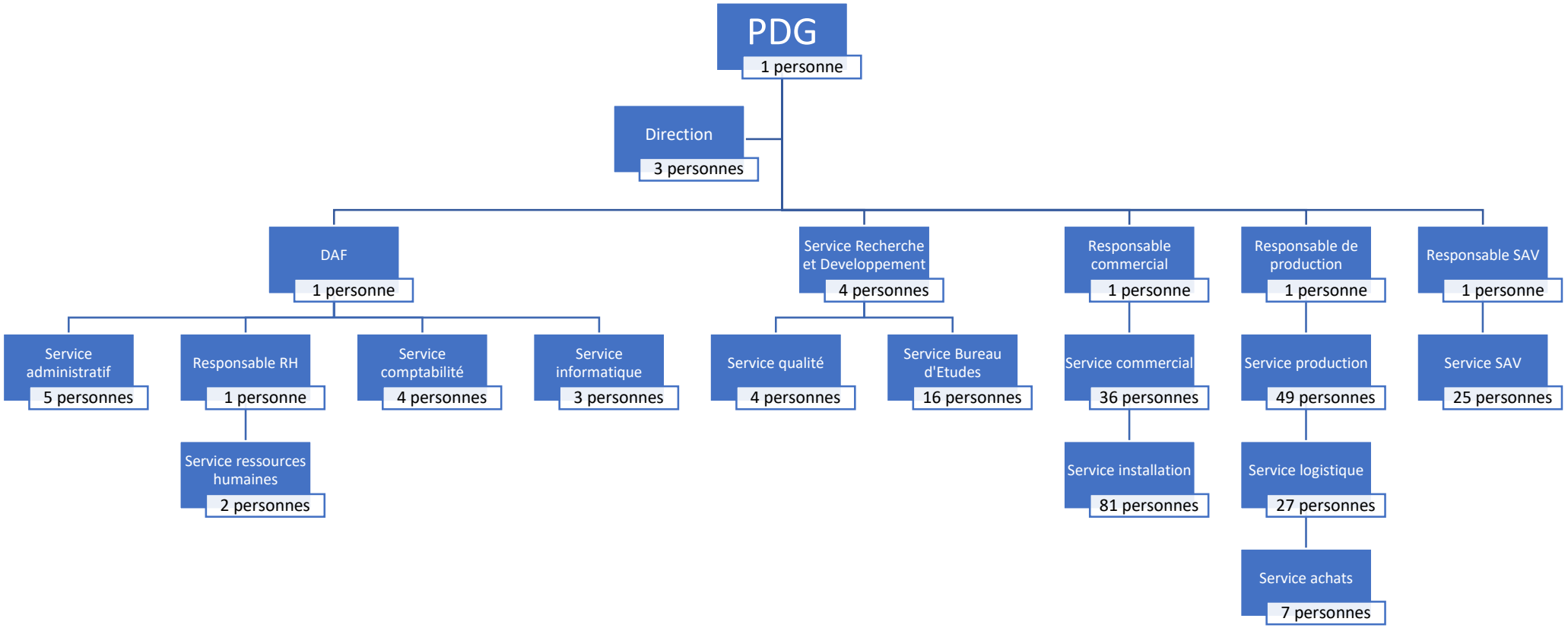
Cette évolution s'est faite de façon exponentielle si bien que ModulHab doit dorénavant consolider sa position dans ce marché tout en s'inscrivant dans une démarche qualitative afin d'optimiser les processus.

La société ModulHab (siège social, site de production et de stockage) est située au 13 rue Jean Grolier - 69007 LYON.

2.2 Organigramme de la société

ModulHab emploie 272 collaborateurs qui se répartissent au sein de 14 services. Parmi ceux-ci, 194 possèdent un poste de travail informatique.

L'organigramme ci-dessous nous a permis de mieux appréhender votre environnement de travail au cours de notre étude.



Organigramme de la société Modulhab

2.3 Problématiques

Suite à l'audit effectué par le service informatique de Modulhab, une série de dysfonctionnements a été porté à notre connaissance :

- × Très forte hétérogénéité des équipements compliquant la maintenance du parc informatique.
- × Aucune politique de maintenance matérielle et logicielle.
- × Aucune gestion des incidents, ni de suivi.
- × Pas de gestion des contrats de maintenance et/ou logicielle.
- × Pas de plan de continuité d'activité informatique.
- × Fortes pertes d'exploitation.
- × Défaillances régulières sur les postes et serveurs.
- × Interventions de dépannage facturées en l'absence de contrat de maintenance.
- × Perte de temps de dépannage.
- × Non-respect de la norme DEEE avec risque d'une amende.

Une perte financière imputable à ces dysfonctionnements est estimée à 92500 €/an, sans compter l'amende à laquelle s'expose Modulhab en ne respectant pas les normes environnementales.

2.4 Cahier des charges

Le cahier des charges fonctionnelles a été établi par le CDP du service informatique de Modulhab en fonction de trois phases de vie qui ont mis en avant trois produits indispensables à la mise en œuvre de la solution que nous vous proposerons plus bas :

2.4.1 Système de gestion de parc

Phase de vie : utilisation normale

FP1 : **Les utilisateurs peuvent déclarer un incident** :

- L'interface doit être simple et intuitive.
- Consulter l'historique des tickets (messages des utilisateurs et réponses du technique).
- Pièces jointes (images, documents, etc.) aux tickets.

FP2 : **Traitement des incidents** :

- Alertes par mail.
- Code couleur pour afficher un ticket en nouvelle information.
- Les tickets doivent pouvoir être attribués aux membres du service informatique, et doivent pouvoir être liés au matériel impacté par l'incident.

FP3 : **Constitution d'une base de connaissances générale :**

- Wiki interne : contribution des utilisateurs de la société.
- Accessible par le service informatique et les utilisateurs (gestion des droits)
- Base de connaissances de documentations de type tutoriels, documentations techniques ou métiers (autres services).

FC1 : **Qualification des incidents** :

- Priorisation donnée aux tickets (ticket bloquant, non bloquant)
- Nature du ticket (incident technique, demande d'information, divers, etc.), n° de ticket, localisation de l'utilisateur, identité du technicien prenant l'incident en charge
- Historique des incidents par thématiques.

FC2 : **Répertorier les ressources matérielles/logicielles** :

- Inventaire des ressources matérielles et logicielles.
- Classement par type : postes fixe, portables, smartphone, imprimante, matériels réseau, serveurs, etc.
- Recherches multicritères en fonction des matériels ou logiciels : n° de série, marque, configuration (processeur, mémoire, disque dur, etc.).
- Durée de garantie (date d'expiration).

FC3 : **Gestion des contrats de maintenance et garantie :**

- Alertes (notifications, mails) à l'approche de l'expiration d'une garantie.
- Fiches des fournisseurs : nom, adresse, hotline, etc.
- Date d'achat.
- Numérisation des contrats.

2.4.2 Politique de maintenance

Phase de vie : entretien

FP1 : Entretien des ressources matérielles & logicielles par le SI (*Maintenance curative*) :

- Procédures d'entretien du matériel *in situ* : dépoussiérage, etc. :
- Procédure d'entretien à distance : mise à jour des logiciels.

FP2 : Sécurisation des ressources matérielles & logicielles (*maintenance préventive*) :

- Déploiement et mise à jour des antivirus
- Mise à jour des logiciels

FP3 : **Homogénéisation des ressources matérielles & logicielles** dans le respect des **normes environnementales** :

- Sélection des fournisseurs œuvrant pour le développement durable.
- Homogénéiser le matériel pour simplifier et optimiser la maintenance.
- Élaborer une stratégie de recyclage pour la fin de vie des équipements dans le respect des normes DEEE.

FC1 : **Perturber le moins possible le travail des utilisateurs** :

- Délais de prévenance de la maintenance.
- Planification et aménagement de plages horaires

2.4.3 Plan de Continuité d'Activité/Plan de Reprise d'Activité

Phase de vie : utilisation normale (mode dégradé)

FP1 : **Assurer la disponibilité** :

- Déterminer le niveau de tolérance d'une panne en mode dégradé
- Expliquer les spécifications techniques et les technologies possibles à mettre en œuvre.

FP2 : **Sauvegarde des données** : Élaborer un plan de sauvegarde en réfléchissant sur :

- La régularité des opérations de backup.
- Les types de sauvegardes.
- Le(s) type(s) de support de sauvegarde choisis.

FP3 : **Éprouver l'efficacité du PRA/PCA** :

- Exécution de tests d'intrusion et des maintenances afin de valider l'efficacité du PCA et la robustesse de l'infrastructure.
- Corriger les défaillances éventuelles.
- Faire évoluer l'infrastructure en assurant une veille technologique.

FC1 : **appréhender les risques** :

- Etudier le site pour déterminer les risques majeurs (voir la méthode AMDEC).
- Caractériser la nature des risques (électriques, sinistres, malveillance, etc.).
- Déterminer l'impact des risques sur la production.
- Chiffrer les pertes d'exploitation par heure.

FC2 : Prendre en **compte les activités critiques** :

- Effectuer un audit pour dégager la liste des services jugés les plus critiques.
- Consulter les responsables des services pour cerner les besoins techniques et humains.

2.5 Enjeux

Il apparait que l'organisation du système d'information de Modulhab doit être complètement repensé. Effectivement, votre société n'a pas réussi à adapter son parc informatique au fil des mutations engendrées par la croissance de ses activités.

Pour Trust-IT, il convient dès à présent de vous proposer une solution qui permettra une reprise en main et une maîtrise complète de votre parc informatique en prenant la mesure des enjeux financiers, organisationnels, technologies et environnementaux à dessein de ne plus répéter les erreurs passées.

3.HOMOGÉNÉISATION DU PARC INFORMATIQUE

3.1 Étude de terrain : hétérogénéité des équipements

L'inventaire du parc existant révèle une très forte hétérogénéité des équipements (postes informatiques, serveurs, équipements réseaux, smartphones) qui se caractérise par des marques de constructeurs différentes et une usure variable (durée d'utilisation).

En outre, l'absence de politique de maintenance a accéléré la vétusté des équipements. Ainsi, des défaillances répétitives ont engendré des pertes d'exploitation qui ont impacté la santé financière de ModulHab.

Nous vous proposons une refonte complète des équipements informatiques critiques afin de diminuer au maximum les risques de pertes financières.

3.2 Infrastructure réseau

Cisco est la marque que nous utiliserons pour la refonte de votre infrastructure. La fiabilité de ses équipements n'est plus à prouver et convient à tout type de réseau.

3.2.1 Renouvellement des équipements réseaux

Routeur Cisco 2901

Deux routeurs seront installés à la tête des deux liaisons FAI. Ce modèle possède les caractéristiques suivantes :

- **2 ports WAN** : la présence de ces deux ports peut être utile pour gérer une double adduction.
- **Protection par Firewall** : le routeur assure une protection avancée au moyen de son firewall qui fiabilisera la connexion en filtrant le trafic internet à la jonction des réseaux LAN et WAN.

Commutateur Cisco Catalyst 2960L-8PS-LL – 8 ports

Nous avons sélectionné ce modèle de commutateur pour interconnecter les commutateurs 48 ports qui alimenteront les postes informatiques et les périphériques (voir ci-dessous). Ainsi, il y en aura un par cœur de réseau (local 1 et 2).

Les caractéristiques de ce modèle sont les suivantes :

- **8 x Gigabit Ethernet 10/100/1000** : Ces ports serviront principalement à l'interconnexion des commutateurs 48 ports et peuvent faire transiter jusqu'à 1 Gbits/s de données.
- **2 x Gigabit SFP** : ces ports ne seront pas utilisés pour les interconnexions.

Commutateur Cisco Catalyst 2960L-48PS-LL - 48 ports

Ce modèle de commutateur a été retenu pour les caractéristiques suivantes :

- **48 x Gigabit Ethernet 10/100/1000** : 194 postes seront interconnectés dans l'infrastructure réseau et les spécifications de ce dernier remplissent les conditions imposées : doté de 48 ports Giganit Ethernet pouvant faire transiter jusqu'à 1 Gbits/s de données, nous prévoyons l'installation de 5 commutateurs (soit 240 ports disponibles). Ces derniers remplaceront les anciens commutateurs dont la bande passante maximale possible n'excédait pas les 10/100 Mbits/s par port.
- **4 x Gigabit SFP** : ces ports permettront d'interconnecter chaque commutateur au moyen de liaisons optiques. Ceci favorisera la fiabilité et l'efficacité du réseau en reliant chaque commutateur par des liaisons insensibles aux perturbations électromagnétiques.
- **Budget PoE+ de 370 W** : cette capacité permet d'alimenter certains équipements au moyen de l'alimentation d'un port Gigabit Ethernet sans recourir à une alimentation électrique supplémentaire. Ceci peut s'avérer particulièrement utile si Modulhab souhaite faire évoluer son parc en connectant d'autres équipements (téléphones sur IP, bornes WIFI, etc.).
- **Protocole de gestion à distance** : SSH (pour les sessions sécurisées) en CLI : nous privilégions l'accès en ligne de commande pour configurer et administrer plus proprement les équipements de l'infrastructure réseau.

3.3 Infrastructure système

3.3.1 Renouvellement des serveurs

PowerEdgeR440

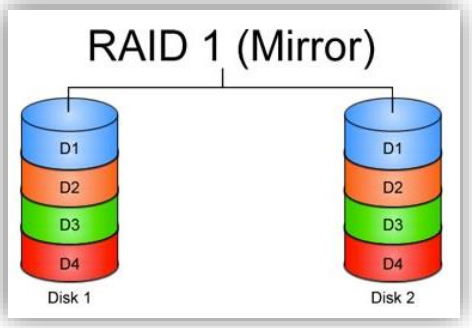
La marque Dell mise sur la robustesse et la fiabilité de ses équipements à destination des professionnels et des entreprises. Nous nous sommes ainsi tournés vers ce constructeur pour nous assurer que l'infrastructure système de Modulhab reposera sur une base physique saine, robuste et performante.

- Processeur : 2 x Intel Xeon Silver 4114 2.2G, 14M Cache X2
- Mémoires : 2 x 16 Go
- Baies disques durs : (2.5") : 10
- RAID 1 : 1 x PERC H730P+ de 2 SSD SAS de 400 Go (2.5')
- RAID 5 : 1 x PERC H730P+ de 3 HDD SAS de 1.2 TB (2.5')
- Alimentation redondée : Dual Hot Plug Redundant Power Supply (1+1) de 550 W
- Garantie : 5 ans avec intervention sur site sous 4 heures

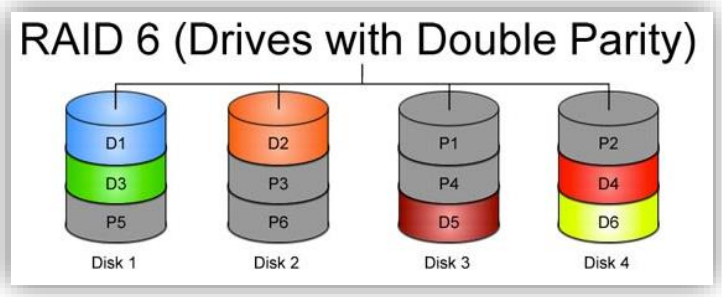
3.3.2 RAID 1 et 6

La technologie RAID (« *Redundant Array of Independent Disks* ») assure la répartition virtuelle des données entre plusieurs disques durs. Cette configuration permet d'accroître les performances et la sécurité des données tout en apportant une tolérance à la panne. L'emploi de cette technologie doit être appréhendé en fonction de la nature des informations que les disques devront stocker (présence d'un OS, stockage de données, base de données, etc.).

RAID 1 : Ce type de RAID nécessite deux disques durs disposés en « miroir » et sur lesquels est effectuée l'écriture simultanée des données. Ainsi, le second disque dur prend le relais en cas de défaillance du premier. En outre, le RAID 1 apporte un rapport sécurité/performances équilibré, ce qui nous encourage à l'appliquer pour l'hébergement des systèmes d'exploitation.



RAID 6 : Ce type de RAID fonctionne avec une grappe de 4 disques durs minimum. Contrairement au RAID 1, le RAID 6 ne réplique pas à l'identique les données sur tous les disques. En effet, chaque disque comporte plusieurs blocs de données ainsi qu'un bloc de parité qui va permettre la reconstruction des données lors de la perte d'un des disques à partir des bits de parité répartis sur les disques restants. Ainsi, toutes les données restent accessibles, moyennant toutefois des performances amoindries le temps de la « reconstruction des données. Contrairement au RAID 5, le RAID 6 tolère la perte de deux disques durs, assurant une très haute disponibilité des données. A contrario, le temps de reconstruction est plus élevé.



Le RAID 6 assurera une protection optimale des données de l'entreprise.

3.3.3 Virtualisation des systèmes

La virtualisation des serveurs s'avère de nos jours indispensables dans l'administration des systèmes. Plusieurs solutions payantes existent sur le marché.

Or, des alternatives libres et fiables sont à présent disponibles tel que Proxmox qui se situe à a même échelle que des solutions payantes telles que VMWare vSphere ou Hyper-V. En développement depuis 2008, **Proxmox VE 5.0** est un logiciel open source basé sur l'hyperviseur KVM et Debian. Il gère la virtualisation des environnements tout en proposant un système de migration à chaud des VM, des snapshots de machines, la prise en charge de sauvegardes ou de restauration de VM.

Bien qu'entièrement gratuit, Proxmox propose plusieurs formules de supports payants par CPU. Il est préférable de souscrire à la formule ***Premium*** car elle apporte le meilleur niveau de prestation et d'accompagnement (accès sur un portail client, ouverture illimitée de ticket, délais de réponse dans la journée, etc.).

Nous vous laissons le choix de souscrire à cette option.

3.4 Renouvellement des postes informatiques

3.4.1 Choix des configurations matérielles

Le choix des postes utilisateurs a été fait en fonction des besoins en ressources matérielles et des différents services de l'entreprise. Cette collecte de renseignements s'est faite en s'entretenant avec les responsables de service et leurs utilisateurs.

Disque dur

Nous avons fait le choix de proposer trois configurations incluant un disque SSD à la place d'un disque dur classique. Les SSD utilisent une mémoire flash (comme les clé USB) alors qu'un disque dur est dit « mécanique » : un bras lit les données sur un ou plusieurs plateaux.

Les avantages du SSD sont multiples :

- Taux de transfert plus élevé qu'un disque dur classique (3 Go/s contre 200 Mo/s pour les HDD).
- Temps de réponse (=temps d'accès moins élevé).
- Meilleure ergonomie : plus silencieux, léger et robuste (résistant, aux chocs et vibrations).
- Faible consommation.

L'un des seuls avantages d'un disque dur classique est son coût qui est beaucoup moins onéreux qu'un SSD. Cependant, il apparait désormais inutile de disposer d'une capacité de stockage importante sur les postes des utilisateurs. En effet, la plupart des entreprises (exceptées les TPE) centralisent toutes leurs données sur un serveur de fichiers.

Par ailleurs, une société de presque 194 collaborateurs telle que ModulHab, n'a aucun intérêt à mettre en place des postes informatiques dotés d'un disque dur classique, au risque de voir ce type de matériel rapidement dépassé. Selon une étude récente de Statista, la vente de SSD dépassera en 2021 celle de disque dur.

Si l'on souhaite disposer d'un parc informatique facile à maintenir doté de postes performants en termes de rapidité (démarrage des sessions, ouverture des applications, etc.) le choix d'un SSD hébergeant uniquement le système d'exploitation et des applications apparait comme une évidence.

Mémoire RAM

Pour une configuration dotée de Windows 10 et axée bureautique (internet, suite office, applications métiers diverses), 4 Go de RAM seront suffisants pour apporter un confort d'utilisation raisonnable (avec possibilité d'évolution par l'ajout de RAM si l'utilisation de certains postes l'exige).

Les postes du bureau d'études devront quant à eux disposer de 8 Go de ram, tout comme les pcs portables, qui sont utilisés lors d'interventions en clientèle (techniciens nomades et commerciaux), pour une question de fluidité dans les usages.

Besoin de performance

Les postes du bureau d'études requièrent des performances matérielles plus élevées. Un processeur performant et une carte graphique seront nécessaires pour ces postes dotés de logiciels de production graphique exigeants en ressources.

Choix du fournisseur

Trois modèles (pc portable, fixe et station de travail) respectant les critères ci-dessus ont été retenus. Après avoir effectué un comparatif parmi les plus grandes marques, nous avons sélectionné Lenovo, qui propose des garanties avec intervention en J+1

sur site pour un coût moindre. Chaque poste possède une licence Windows 10 Professionnel.

Les garanties sont les suivantes :

- Postes fixes bureautiques : 5 ans
- Pcs portables : 3 ans.
- Stations de travail :3 ans.

3.4.2 Présentation des modèles

Poste bureautique : **Lenovo ThinkCentre M710q**

Un grand avantage de cette configuration se situe dans sa praticité de mise en place, ce qui facilite donc également la maintenance, et éventuellement une évolution physique du parc (facile à déplacer) : l'unité centrale proposée est extrêmement compacte (volume d'1 litre), et pour un poids de 1.3kg. Ce poste peut être placé à l'horizontale, à la verticale, fixé à un mur ou derrière un écran.

Ses performances sont en adéquation avec une **utilisation bureautique**.

- Processeur : Intel i3-7100T (3.4 Ghz, cache 3 Mo)
- RAM : 4 Go
- Disque dur : Intel SSD : 256 Go
- Garantie : 5 ans J+1 (jour ouvrable)

Ce modèle est facile à entretenir dans le cadre d'une **maintenance** ou d'un **upgrade matériel** (composants facilement accessibles, ajout de ram possible, format minimal et léger, etc.) tandis que sa garantie avantageuse apporte un amortissement assuré du coût du parc sans surprise de frais supplémentaires éventuels.

Station de travail : **ThinkStation P520c**

Cette station de travail dispose d'un processeur et d'une carte graphiques performants avec la possibilité d'un affichage double écran. Son SSD assure une rapidité d'accès aux applications et aux fichiers tandis que sa quantité de RAM fera fonctionner des logiciels exigeants en ressources (conception 3D, etc.).

Ce poste dispose également de certifications **ISV** « *Independent Software Vendor* » ce qui est gage de sécurité et de fiabilité en termes de fonctionnement des logiciels et applications. Il est également équipé de mémoire ram ECC, à correction d'erreurs, plus fiable et plus sûre. Disposant des labels **EPEAT Gold** et **Energy Star 6.1**, la station est certifiée **GREENGUARD** qui garantit une efficacité énergétique optimale.

- Processeur : Intel Xeon W-2102 (2.90 Ghz, cache 8.25 M)
- RAM : 8 Go (DDR4, RDIMM 2666 Mhz ECC)
- Disque dur : SSD 256 Go
- Carte graphique : NVIDIA NVS 310 1Go

PC portable : **ThinkPad T470p**

Les PC portables de la gamme ThinkPad sont réputés pour leur fiabilité et leur robustesse ce qui a contribué à leur renommée au fil des années. Les PC portables sont amenés à être utilisés sur le terrain par des techniciens et commerciaux itinérants, ce qui accroit les risques de dommages. C'est pourquoi nous les avons sélectionnés afin de proposer des performances et une sûreté suffisante dans un contexte de terrain (à noter que les ThinkPad sont soumis à 12 tests de robustesse et plus de 200 contrôles qualité avant leur commercialisation).

Nous avons choisi un modèle avec un très bon rapport qualité/prix, proposant des performances efficaces pour un encombrement minime, ainsi qu'une très bonne autonomie.

- Processeur : Intel Core i5-7300 HQ (3.5 Ghz, cache 6 Mo).
- RAM : 8 Go DDR4.
- Disque dur : 256 Go SSD
- Écran : 14 pouces Full HD.

Des stations d'accueil sont également proposées pour les commerciaux, qui sont amenés à se connecter régulièrement au siège, et pourront ainsi utiliser un écran externe pour travailler plus confortablement.

Le choix d'une seule marque pour 3 modèles types procure les avantages suivants :

- Optimisation de maintenance : gestion de garantie avec un seul fournisseur, facilitant le suivi des contrats de garantie en cours.
- Tarifs très concurrentiels.
- Garantie longue et qualitative.

Ces arguments montrent que Lenovo, un des principaux fabricants de PC au monde, se démarque de ses concurrents en commercialisant du matériel doté d'un rapport qualité/prix très attractif.

4.Normes DEEE et développement durable

La sélection du matériel ci-dessus s'est opérée selon une stratégie financière mais également environnementale. En effet, votre société a commis des infractions vis-à-vis des normes environnementales DEEE qui s'illustre par :

- Aucune stratégie de gestion de fin de vie des équipements.
- Aucune stratégie de sélection des fournisseurs œuvrant pour le développement durable.

Le service qualité sécurité environnement de Modulhab a spécialement insisté sur ces aspects en réclamant la mise en place du recyclage des machines dans le respect des normes DEEE.

4.1 Stratégie de fin de vie et politique de recyclage

On comprend par **DEEE** (ou **D3E**), les « *Déchets d'Équipements Électriques et Électroniques* » qui englobe l'ensemble des matériels contenant des substances ou composants dangereux pour l'environnement à base de mercure, de plomb, etc.

Or, ces matériaux présentent un fort potentiel de recyclage. Ainsi, le traitement de ce type de déchets représente un véritable enjeu pour les sociétés qui se débarrassent chaque année de leur équipements électroniques.

L'Union Européenne a défini la gestion de ces déchets au travers d'une directive, la **RoHS** (2002/95/CE du 27 janvier 2003, voir annexe 4) et la directive 2002/96/CE du 27 janvier 2003 qui portent sur les DEEE. Face à l'augmentation du remplacement de ces matériels, ces directives ont été révisées avec la directive **RoHS II** (2011/68/EU du 8 juin 2011) et **DEEE II** (2012/19/UE du 14 juillet 2012).

Ainsi, les articles L.541-10-2 et R.543-172 du Code de l'environnement réglementent l'organisation de la filière DEEE pour la reprise des équipements électriques et électroniques usagés.

Nous optons ainsi pour la reprise des équipements par la société **Rachat-DEEE** qui prend en charge la reprise des tours d'ordinateurs, des serveurs, pc portables et toutes sortes de composants informatiques. Cette société rachète ainsi le matériel informatique. Les tarifs en vigueur pour l'année 2018 sont les suivants :

RACHAT-DEEE.fr

- Ordinateur de bureau (UC) : 285 €/tonne
- Ordinateur portable (sans batterie) : 485 €/tonne

Ayant prévu d'écouler les vieux postes au fur et à mesure du remplacement du matériel, Modulhab traitera régulièrement avec cette société.

Contact :
Rachat-DEEE.fr
3014 Route de Ravel
69440 Mornant
Téléphone : 04 78 19 36 15

Il est indispensable de **prendre un rendez-vous** avant se rendre sur place.

Pour prendre rendez-vous, 2 solutions :

- A l'aide du **formulaire en ligne** (réponse dans les 24 heures)
- **Par téléphone** au 04.78.19.36.15 (du lundi au jeudi, de 08:00 à 12:00 et de 14:00 à 16:00 et vendredi de 09h00 à 12h00).

Aucun accueil ne sera fait sans rendez-vous.

4.2 Stratégie de sélection des fournisseurs

Il est parfois difficile d'associer informatique et développement durable. Afin de proposer à ModulHab des postes alliant à la fois performance, faible coût, qualité et respect de l'environnement, nous nous sommes basés sur des normes, certifications et labels reconnus en matière de respect environnemental.

Nous les détaillons ici, accompagnés du label des équipements mentionnés précédemment.

Energy Star : Il s'agit d'un label américain créé en 1992 et qui a été depuis adopté par la Commission Européenne. Il ne s'agit pas d'une norme obligatoire mais d'un « écolabel » faisant état de l'efficacité énergétique d'un produit (équipements électroménagers, électroniques, etc.) en certifiant du rendement efficace de son alimentation. Cette efficacité énergétique implique souvent un coût un peu plus élevé du produit à l'achat avec à la clé des économies d'ordre énergétique.

NB : La station de travail proposée pour le renouvellement du parc est certifiée Energy Star 6.1.

EPEAT, « *Electronic Product Environmental Assessment Tool* ». Il s'agit d'un écolabel distinguant les produits répondant à des critères de performance environnementale selon trois classes (Gold, Silver, Bronze). L'équipement informatique est évalué selon différents critères obligatoires et optionnels (51 au total) :

- Composants respectant l'environnement
- Longévité du produit (disponibilité d'une garantie supplémentaire de 3 ans, par exemple)
- Emballage recyclable ou non.
- Etc.

La classe EPEAT Gold est attribuée lorsque 75% des critères sont respectés.

NB : La station de travail proposée pour le renouvellement du parc est dotée de ce label.

GREENGUARD. Cette certification identifie les produits et matériaux ayant de faibles émissions chimiques, dans le but d'obtenir une meilleure qualité de l'air. Cette certification impose donc des limites d'émission à ne pas dépasser.

NB : La station de travail proposée pour le renouvellement du parc est dotée de cette certification.

Certification CTO. La certification de développement durable pour les produits informatique TCO fondée il y a plus de 25 ans est mondialement reconnue. Afin d'obtenir la certification TCO, les fabricants doivent mettre en œuvre des conditions de travail socialement responsables dans les usines où sont fabriqués les produits. Ils sont également chargés de corriger les non-conformités. Ce label a pour but de réduire l'empreinte environnementale et de protéger les droits humains. Il améliore aussi la durabilité informatique et favorise plus globalement la responsabilité sociale et environnementale tout au long du cycle de vie du produit.

NB : Le PC fixe Lenovo ThinkCentre Tiny M710q et le PC portable Lenovo ThinkPad T470p possèdent cette certification.

RoHS, « *Restriction of Hazardous Substances* ». Cette directive vise à limiter l'utilisation de substances dangereuses notamment le plomb, le mercure, le cadmium, etc. Elle a été revue en 2011 et encourage désormais l'écoconception, le tri sélectif et le recyclage des composants. Désormais, pour qu'un produit soit certifié « CE » pour sa commercialisation sur le marché Européen, il doit également être certifié RoHS.

NB : Tous les modèles proposés précédemment sont certifiées RoHS.

En somme, nous pouvons affirmer que nous avons respecté les conditions de Modulhab en termes de développement durable pour le renouvellement des postes et sa politique de recyclage des déchets électroniques.

Pour un complément d'informations sur la notion de GreenIT, de normes ou encore de cycles de vie des équipements, se reporter à l'annexe 4).

5. Surveillance des équipements

5.1 Principes de la surveillance (évènements, monitoring, supervision, etc.)

Suivant les recommandations d'ITIL, l'***exploitation des services*** englobe la ***gestion des évènements*** (et la ***gestion des incidents***, voir partie 6.1.2) qui doit être mise en œuvre au sein d'une société au moyen d'outils de surveillance.

Les « évènements » correspondent aux notifications :

- Information : ne nécessite aucune action
- Avertissement : il signale l'approche d'un seuil à ne pas dépasser et nécessite des actions pour éviter une exception (voir ci-après)
- Exception : cet évènement signale le fonctionnement anormal d'un service et a un caractère impactant sur la production.
- Alerte : notification pour une intervention humaine.

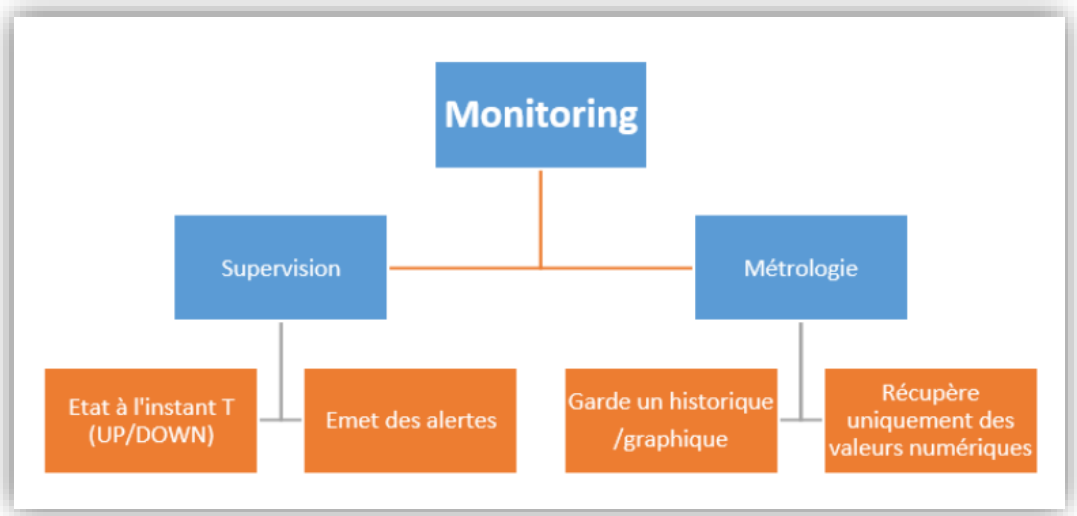
Votre société à récemment connu des pannes au niveau des serveurs qui auraient pu être évitées si des outils de supervision avaient pu alerter à temps les équipes pour intervenir de façon proactive.

Nous proposons ainsi l'installation d'outils qui surveilleront et alerteront vos équipes des signes avant-coureurs ou des pannes éventuelles de vos équipements.

NB : Attention à la différence des termes :

- Monitoring : action consistant à surveiller l'état actuel et passé d'un équipement.
- Supervision : action consistant à récupérer l'état à l'instant T d'un équipement.
- Métrologie : action consistant à tracer une valeur numérique d'une charge dans le temps au moyen de graphiques

Aujourd'hui, supervision et métrologie tendent à se mélanger avec des systèmes d'alertes qui s'appliquent sur des seuils de charge.



5.2 Choix de la solution

De nombreuses solutions payantes et gratuites existent sur le marché. Soucieux de vous proposer des outils robustes et efficients, Trust-IT oriente régulièrement ses clients sur des solutions Open Source afin de minimiser les investissements dans les licences pour alléger vos dépenses.

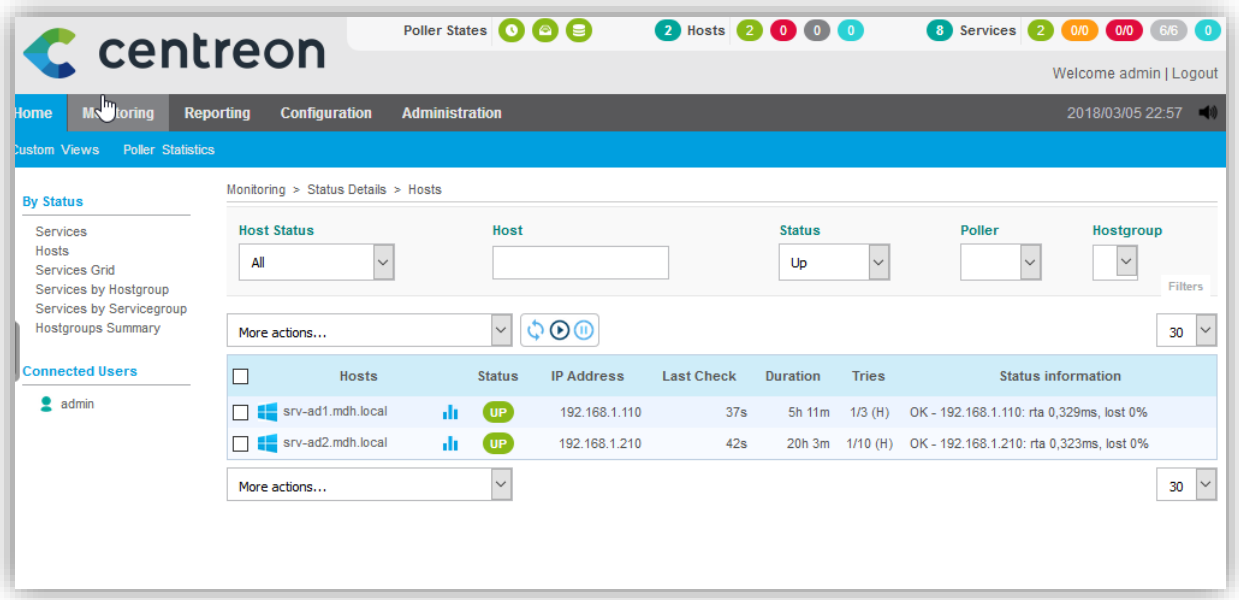
Plusieurs logiciels libres de surveillance systèmes et réseaux existent tels que **Nagios** qui assure la supervision des équipements en informant du statut de l'état UP/DOWN à l'instant T. Cependant, les logiciels **Munin** ou **Cacti** émettent des valeurs pour tracer l'évolution d'une charge (il faudra rajouter des plugins pour qu'ils puissent émettre des alertes).

Des logiciels plus complets comme **Zabbix** existent pour venir concurrencer Nagios en ayant une supervision plus étendue sur des équipements variés mais notre choix se reportera sur **Centreon**, une amélioration du projet Nagios combinant des outils de supervision et de métrologie et bénéficiant surtout d'une communauté active de 185000 utilisateurs à travers le monde, parmi lesquelles 19000 contributeurs, ce qui facilitera son support durant sa mise en production.

5.3 Centreon

Centreon est un logiciel libre de supervision et de monitoring. Historiquement basé sur Nagios, il est depuis 2012 doté de son propre moteur de collecte (Centreon Engine) et de son gestionnaire d'évènements (Centreon Broker). Il possède de nombreuses fonctionnalités accessibles via l'interface web d'un navigateur :

- État des machines supervisées (serveurs, équipements réseaux, etc.)
- Consultation de la métrologie.
- Mécanismes de surveillance actifs/passifs
- Gestion des notifications : possibilité de définir des périodes de surveillance avec des remontées d'alertes.
- Gestion des utilisateurs (importation LDAP).
- Chiffrement des communications (authentification des flux par l'utilisation de certificats).



Supervision des serveurs AD1 et AD2

Des « services » basés sur des commandes peuvent être configurés avec des remontées d'erreur (exemple, espace disque à 80 %) qui peuvent se faire par mail. De plus, des « temps d'arrêts » sont paramétrables pour éviter d'envoyer des messages d'alertes lorsqu'un serveur est en maintenance. Il ne s'agit que d'un bref aperçu des fonctionnalités de Centreon qui présente l'avantage d'être hautement configurable tout en s'adaptant facilement à votre environnement systèmes et réseaux.

Centreon sera installé sur une machine virtuelle exclusivement dédiée à la supervision afin de superviser l'ensemble des VM présentent sur vos serveurs (voir annexe 3 pour la procédure d'installation).

Pour une meilleure ergonomie, l'accès à son interface s'effectuera depuis votre navigateur avec l'adresse suivante :

monitoring.mdh.local/centreon/ (correspondant à l'adresse 192.168.1.10)

La gestion des évènements est un service essentiel pour administrer un parc informatique.

Grâce à un logiciel de supervision tel que Centreon, votre SI disposera des outils nécessaires pour détecter immédiatement les pannes et dysfonctionnements ou d'anticiper ces derniers aux moyens du monitoring.

6.SOLUTION DE GESTION DE PARC

Notre choix s'est orienté sur GLPI qui est une solution Open Source, notamment pour les raisons suivantes :

- Authentification LDAP
- Collecteurs mails (notifications, alertes)
- Système avancé de profils, permissions et droits
- Recherche multi-critères
- Personnalisation avancée de l'interface (couleurs, logos, etc.)
- Sauvegarde et restauration des bases de données.
- Exportation des données en différents formats (PDF, Excel, etc.)
- « ITIL compliant » : conforme aux principes ITIL.

En plus d'être une solution ultra complète, GLPI est gratuit tout en restant conforme aux principes ITIL. Nous sommes ainsi certains que cette solution vous apportera les bases nécessaires pour repenser l'organisation de la gestion du parc de Modulhab.

Abordons maintenant ces fonctionnalités.

6.1 Logiciel de gestion de parc : GLPI

GLPI (« *Gestionnaire Libre de Gestion de Parc* ») est un logiciel Open Source de gestion de parc dont l'utilisation est partagée entre le SI d'une société et ses utilisateurs. Il apporte ainsi une vue sur l'ensemble du parc tout en fournissant les services nécessaires pour le suivi des incidents et l'assistance auprès des utilisateurs (ServiceDesk).

GLPI se présente exclusivement sous la forme d'une application web, ce qui apporte de grandes facilités pour le déployer auprès de tous les utilisateurs dont l'accès s'effectue via un simple navigateur.

Par ailleurs, l'ensemble des ressources sont inventoriables ce qui procure une visibilité globale et un cadre simplifié pour la gestion des actifs d'un point de vue administratif et financier.

6.1.1 Mise en œuvre avec FusionInventory

Concernant la mise en œuvre du GLPI, se reporter à l'annexe 2 pour la démarche d'installation.

Notons que l'agent FusionInventory sera déployé sur l'ensemble des postes informatiques de Modulhab. Il s'agit d'un logiciel qui facilite l'inventaire des équipements et de leur configuration matérielle et logicielle.

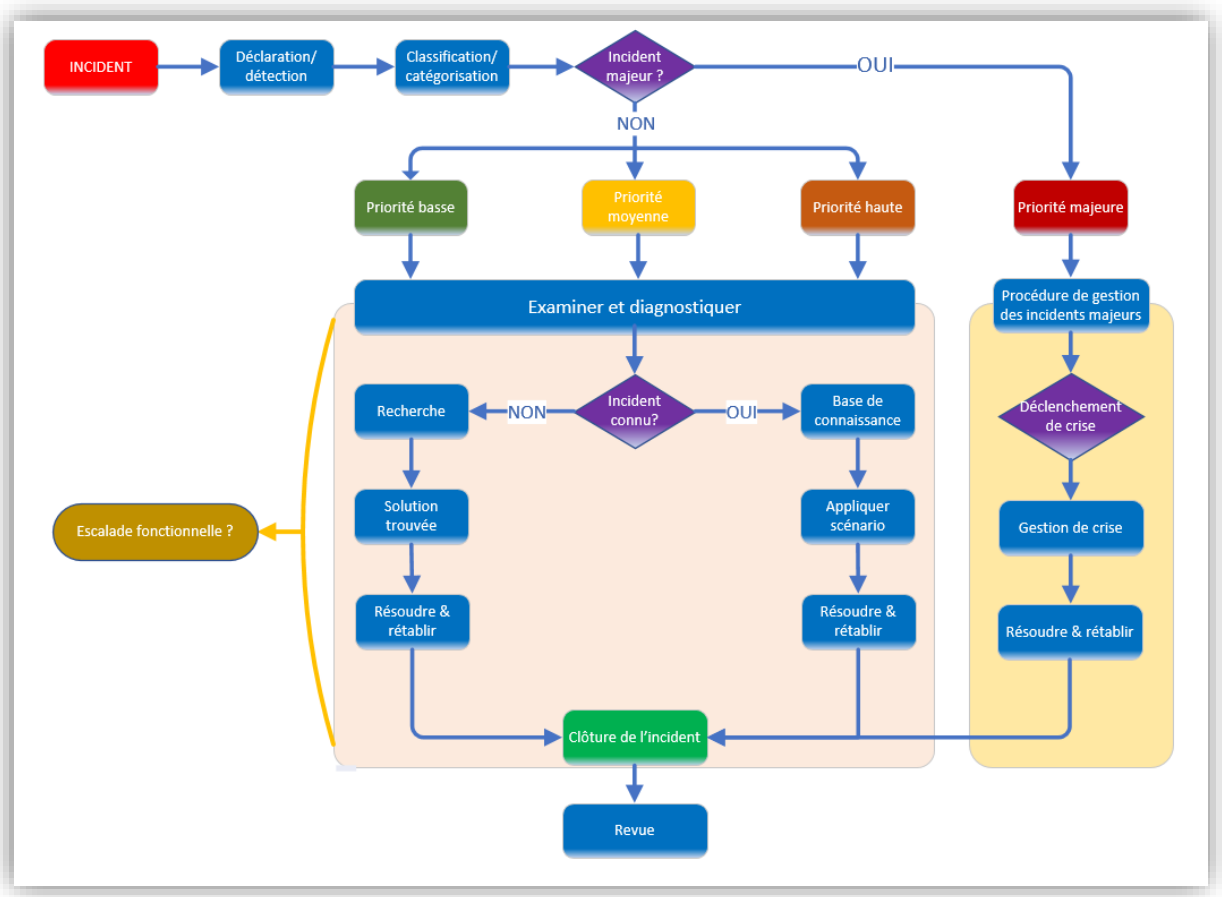
6.1.2 Gestion des incidents

La bonne utilisation des outils sous GLPI induit la connaissance d'un cadre théorique décrivant les différents scenarii à envisager lors d'un incident, de sa déclaration à sa résolution. Sur la procédure d'ouverture d'un ticket et les moyens mis à disposition de l'utilisateur, voir annexe 2).

Il convient ainsi de sensibiliser le SI de Modulhab à ce système en introduisant un mode opératoire pour le traitement des incidents.

Processus dans le traitement de incidents

La gestion des incidents est un processus faisant partie de la phase exploitation des services ITIL. Ce processus englobe tout le cycle de vie de la gestion de tous les incidents et vise à rétablir le plus rapidement possible l'exploitation d'un service en impactant le moins possible la production.



Une formation sera dispensée aux membres du SI pour les sensibiliser à la démarche et à la compréhension de ce système en détaillant les processus présents dans ce schéma (voir annexe 4). Ceci est indispensable pour appréhender correctement chaque situation d'incident.

Priorité des incidents et SLA

Les incidents font l'objet d'une hiérarchisation selon le niveau de gravité qui doit être évalué en fonction de deux facteurs :

- L'**urgence** : il s'agit de l'évaluation de la criticité par rapport à l'activité de l'utilisateur.
- L'**impact** : Il concerne le volume et l'ampleur de l'incident sur l'entreprise.

Ces éléments issus des recommandations d'ITIL ont été repris dans GLPI sous la forme d'une matrice de calcul de priorité.

Sur la base de ces éléments, et pour partir sur une priorisation simplifiée et efficace des incidents, nous proposons de partir sur quatre types de qualification pour les tickets :

- **Priorité majeure** : cette qualification concerne les incidents que l'on peut qualifier de « **majeurs** » lorsque les caractères urgent et impactant sont à leur maximum. Ce type d'incident nécessite un rétablissement sous 1 heure et doit rester exceptionnel.
- **Priorité haute** : cette qualification concerne les incidents de criticité haute qui devront faire l'objet d'une résolution rapide sous 4 heures.
- **Priorité moyenne** : cette qualification concerne les incidents de criticité moyenne qui devront faire l'objet d'une résolution rapide sous 8 heures.
- **Priorité basse** : cette qualification concerne les incidents qui ne sont pas suffisamment impactant sur la production de l'entreprise. Traitement de la demande sous une semaine.

Chaque niveau de criticité induit un délai de résolution sous forme de **GTR** (« *Garantie de Temps de Rétablissement* »). Ceci est précisé dans le cadre d'un **SLA** (« *Service Level Agreement* ») ou engagement de contrat de service qui stipule le niveau de qualité et de disponibilité des services d'une société.

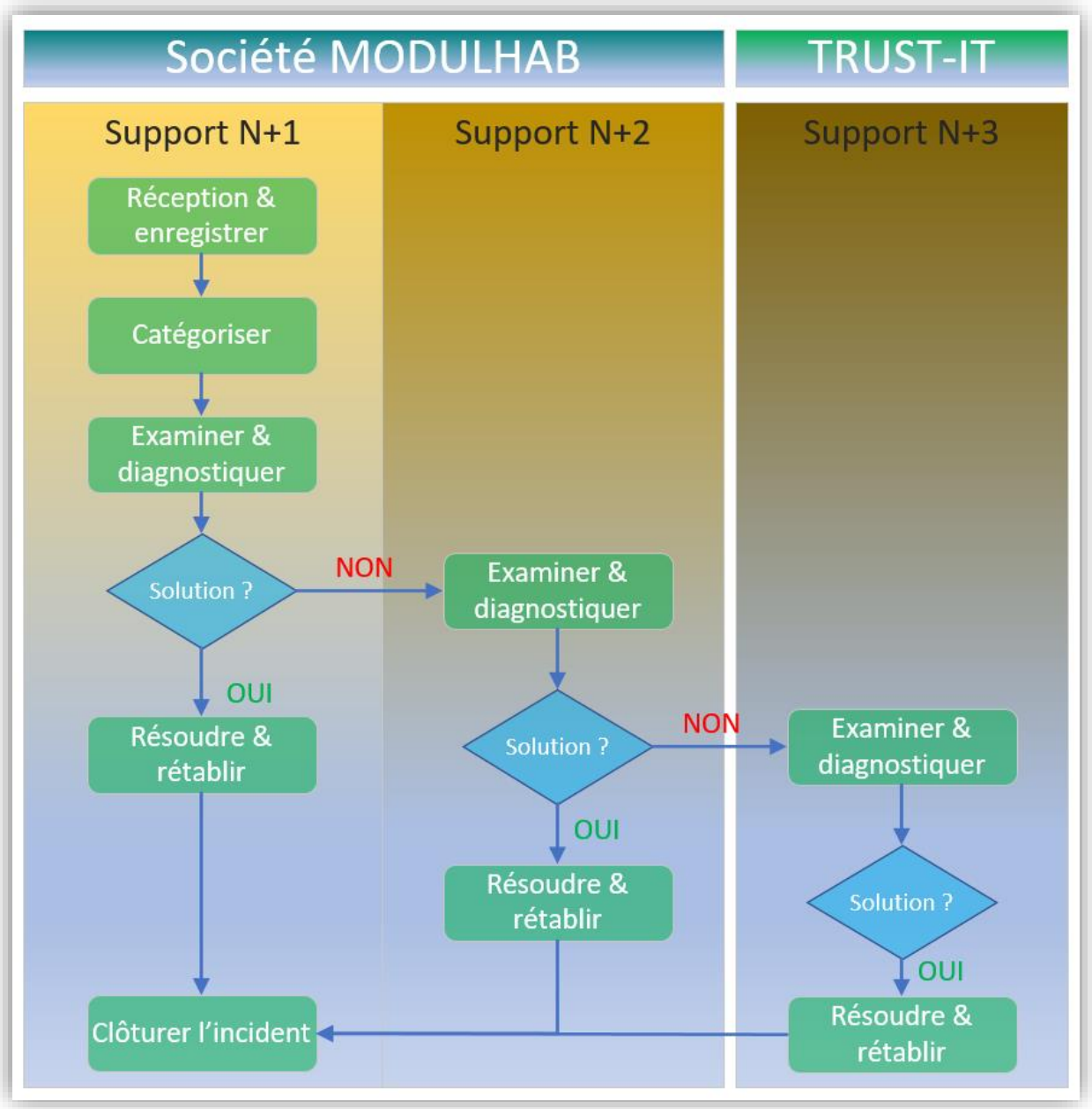
Comme chaque situation est différente selon les sociétés, il conviendra de mener une enquête au sein de l'entreprise pour définir les métiers/services/fonctions dont l'activité peut atteindre un niveau d'urgence et d'impact suffisamment sensible pour compromettre les intérêts de Modulhab. Les conclusions de cette étude seront synthétisées dans les SLA.

Escalade des incidents

L'escalade consiste à transférer la gestion de l'incident à une équipe possédant un plus haut niveau d'expertise. L'escalade s'opère lorsqu'un niveau N+x considère qu'il ne pourra pas respecter la **SLA** liée à un service/métier.

On identifie deux types d'escalade :

- **Fonctionnelle** : Cette escalade est prévue dans les processus pour transférer un incident vers un niveau supérieur. Elle intervient lorsqu'il y a un manque de connaissance ou d'expertise du niveau en cours ou lorsqu'un délai de résolution de l'incident risque d'être dépassé.
- **Hiérarchique** : cette escalade n'est pas prévue réellement dans les processus et intervient lorsque la résolution ne pourra pas respecter la SLA.



La composition du SI permettra la mise en place de deux niveaux de support N1 et N2. Si un incident n'arrive pas à être résolu par votre équipe, notre contrat de maintenance prévoit la prise en charge des incidents à distance des techniciens de Trust-IT en support N3.

Les incidents majeurs

Les incidents qualifiés de « majeurs » ont impact extrême et nécessitent une prise en charge spécifique avec des échelles de temps plus réduites due à la criticité absolue de l'incident. Le risque de dépasser le temps de résolution mentionné dans les SLA est élevé.

Un incident peut être majeur lorsqu'il impacte :

- × Les éléments actifs de la haute disponibilité (serveurs de fichiers/d'applications, accès internet, téléphonie, etc.)
- × Une application métier critique.
- × Des éléments logistiques majeurs (incident électrique, climatisation, etc.).
- × La production de l'entreprise, sans possibilité de contournement.

La méthode de prise en charge des incidents majeurs peut engendrer la mise en place d'une **cellule de crise** mais ce n'est pas systématique. Ses caractéristiques sont les suivantes :

- Réactivité maximale.
- Plus de rigueur dans les processus.
- Mobilisation d'experts métiers en plus des autres acteurs.
- Niveau de communication adapté à la criticité de l'incident.

Des procédures spécifiques à la nature du problème (issues d'une base de connaissance) sont appliquées pour une gestion efficace de l'incident. Cependant, les phases de la gestion d'incidents demeurent les mêmes que pour un incident classique. Il est important que la résolution s'accompagne d'un bilan de l'incident pour tirer les leçons de cet évènement.

Le niveau d'expérience et de maturité de votre SI n'est pas suffisant pour que ce dernier puisse assumer pour le moment le suivi d'un incident majeur requérant une cellule de crise.

Si un tel scénario venait à arriver, l'équipe de la DSI de Modulhab devra s'en remettre à l'*Incident Manager* de TrustIT pour la supervision d'une cellule de crise.

6.1.3 Inventaire du parc et gestion des garanties

Les postes remontés dans GLPI grâce au plugin FusionInventory (procédure d'installation en annexe 1) apparaissent dans l'onglet « Parc » puis « Ordinateurs »

Nom	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation - Nom	Lieu	Dernière modification	Composants - Processeur
BFADM04		VMware, Inc.	VMware-56 4d 26 02 19 8b ea fa-18 e6 ca 41 64 c6 ce 8b	VMware	VMware Virtual Platform	Windows		2018-02-14 14:00	Intel(R) Core(TM) i7-4700MQ CPU @ 2.40GHz
Server16		VMware, Inc.	VMware-56 4d 07 6c f1 30 94 bb-b4 4c 06 b2 1f 08 07 c9	VMware	VMware Virtual Platform	Windows		2018-03-05 18:16	Intel(R) Core(TM) i7-4700MQ CPU @ 2.40GHz

Les logiciels apparaissent quant à eux dans « Parc » puis « Logiciels »

Nom	Éditeur	Versions - Nom de la version	Versions - Système d'exploitation	Licences - No
7-Zip 18.01 (x64)	Igor Pavlov	18.01	Windows	1
FusionInventory Agent 2.4 (x64 edition)	FusionInventory Team	2.4	Windows	1
FusionInventory Agent 2.4 (x86 edition)	FusionInventory Team	2.4	Windows	1
Internet Explorer	Microsoft Corporation	11.0.15063.0 11.2007.14393.0	Windows	2

Depuis la fiche d'un poste, on peut voir notamment les détails concernant le système d'exploitation (architecture, noyau, version, édition, numéro de série, etc.).

Ces détails peuvent s'avérer extrêmement pratiques afin de vérifier la bonne homogénéisation du parc. En effet, si l'on constate par exemple la présence d'éditions Familiales de Windows au sein du parc, on pourra faire une liste des postes à mettre à jour en version Professionnelle. Grâce à la recherche multicritère, il est d'ailleurs possible de rechercher directement une version spécifique répertoriée dans le parc.

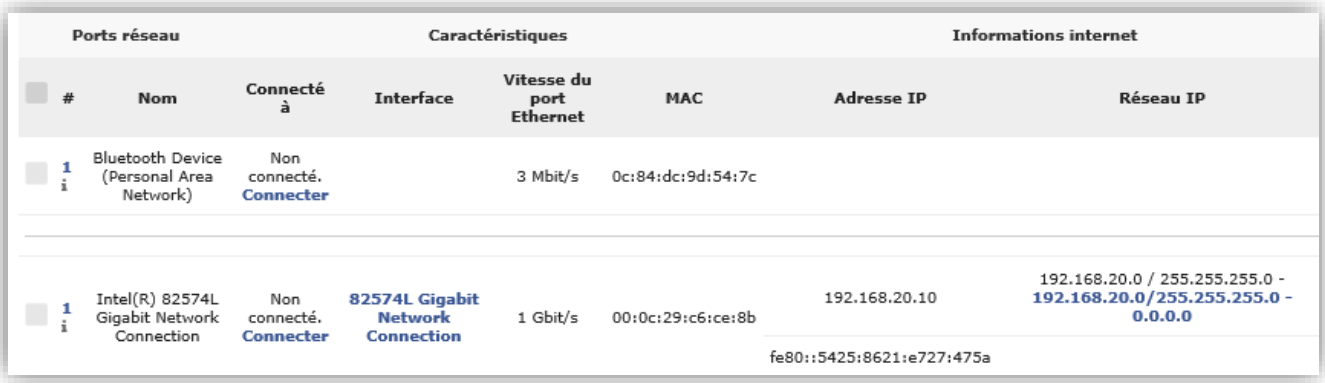
Aperçu des détails d'un système d'exploitation

Parmi les autres informations remontées, nous avons les composants ainsi que les espaces disque des différents volumes des postes :

Nom	Inventaire automatique	Partition	Point de montage	Système de fichiers	Taille totale	Taille libre	Pourcentage libre
C:	Oui		C:	NTFS	59.51 Gio	43.35 Gio	73%
Réservé au système	Oui	Réservé au système	Réservé au système	NTFS	499 Mio	181 Mio	36%

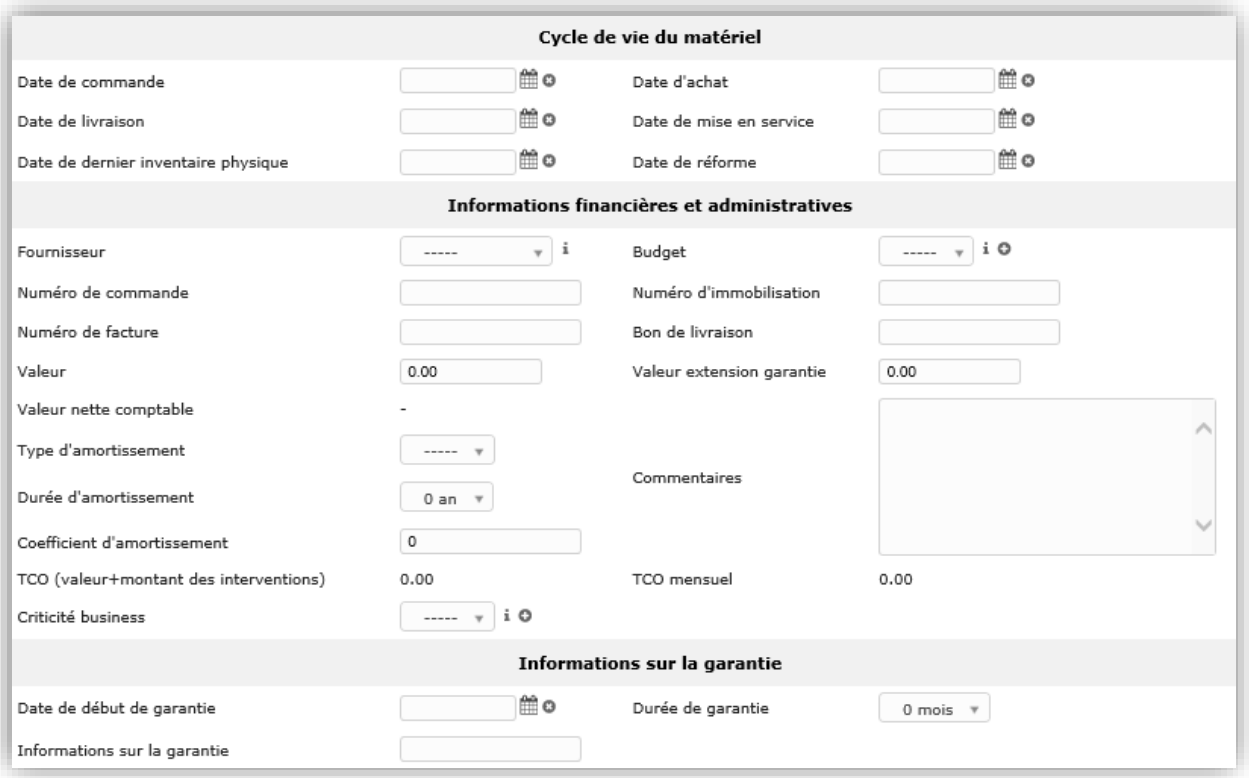
Il est ainsi possible de voir la capacité utilisée sur les différentes partitions d'un poste.

Les connexions réseaux sont également remontées avec des informations telles que les adresses MAC et IP, ce qui peut s'avérer très pratique à l'usage.



Ports réseau			Caractéristiques			Informations internet	
#	Nom	Connecté à	Interface	Vitesse du port Ethernet	MAC	Adresse IP	Réseau IP
1	Bluetooth Device (Personal Area Network)	Non connecté. Connecter		3 Mbit/s	0c:84:dc:9d:54:7c		
1	Intel(R) 82574L Gigabit Network Connection	Non connecté. Connecter	82574L Gigabit Network Connection	1 Gbit/s	00:0c:29:c6:ce:8b	192.168.20.10 fe80::5425:8621:e727:475a	192.168.20.0 / 255.255.255.0 - 192.168.20.0/255.255.255.0 - 0.0.0.0

Un onglet « Gestion » permet d'ajouter toutes les informations financières et administratives ainsi que les dates de garantie, les dates d'achats voire encore le prix de l'équipement.



Cycle de vie du matériel

Date de commande		Date d'achat	
Date de livraison		Date de mise en service	
Date de dernier inventaire physique		Date de réforme	

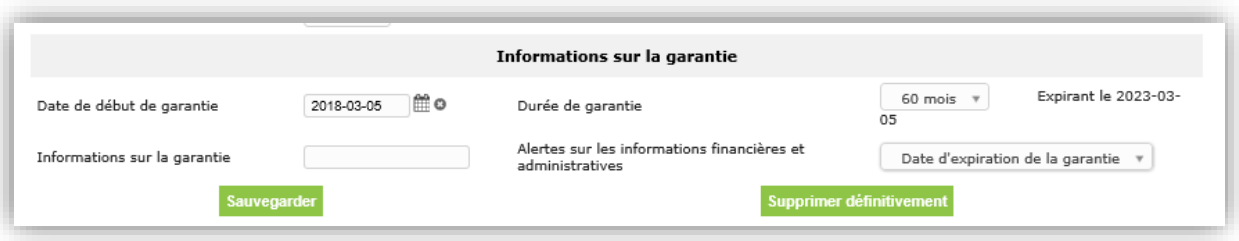
Informations financières et administratives

Fournisseur	-----	Budget	-----
Numéro de commande		Numéro d'immobilisation	
Numéro de facture		Bon de livraison	
Valeur	0.00	Valeur extension garantie	0.00
Valeur nette comptable	-		
Type d'amortissement	-----	Commentaires	
Durée d'amortissement	0 an		
Coefficient d'amortissement	0		
TCO (valeur+montant des interventions)	0.00	TCO mensuel	0.00
Criticité business	-----		

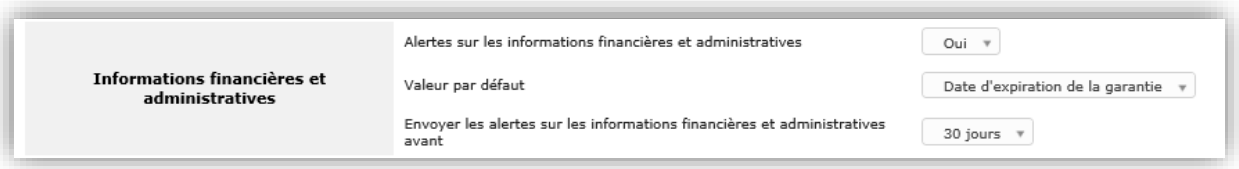
Informations sur la garantie

Date de début de garantie		Durée de garantie	0 mois
Informations sur la garantie			

Les dates de garantie permettent également de recevoir des notifications par mail en cas d'approche d'une date de fin de garantie.

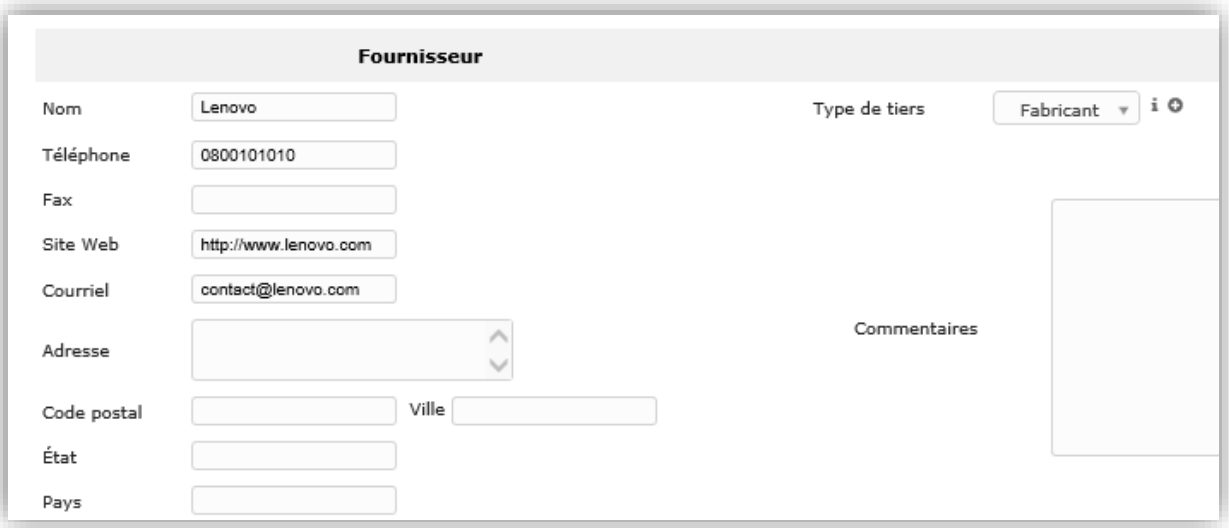


Il faudra ensuite activer les paramètres « Informations financières et administratives » dans l'administration des entités, afin de recevoir les notifications avant les dates d'expiration de garantie.

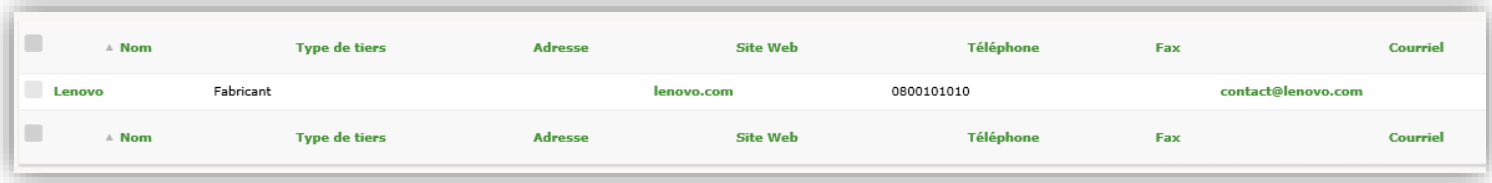


6.1.4 Gestion des fournisseurs

Il est possible de gérer les fournisseurs dans GLPI, afin de centraliser toutes les informations nécessaires (lien vers le site web, numéro de téléphone, adresse mail, contrats en cours, documents PDF…)

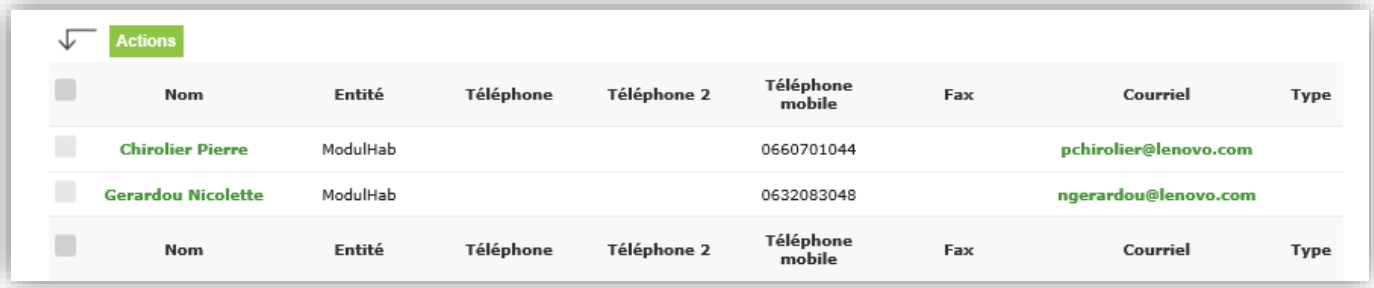


Une fois le fournisseur ajouté, les informations les plus utiles apparaissent dans la liste des fournisseurs : lien cliquable vers le site Internet, numéro de téléphone et adresse mail cliquable.



Il est également possible d'ajouter plusieurs contacts, par exemple un numéro de support, une secrétaire, des commerciaux etc., le tout depuis la même fiche fournisseur.

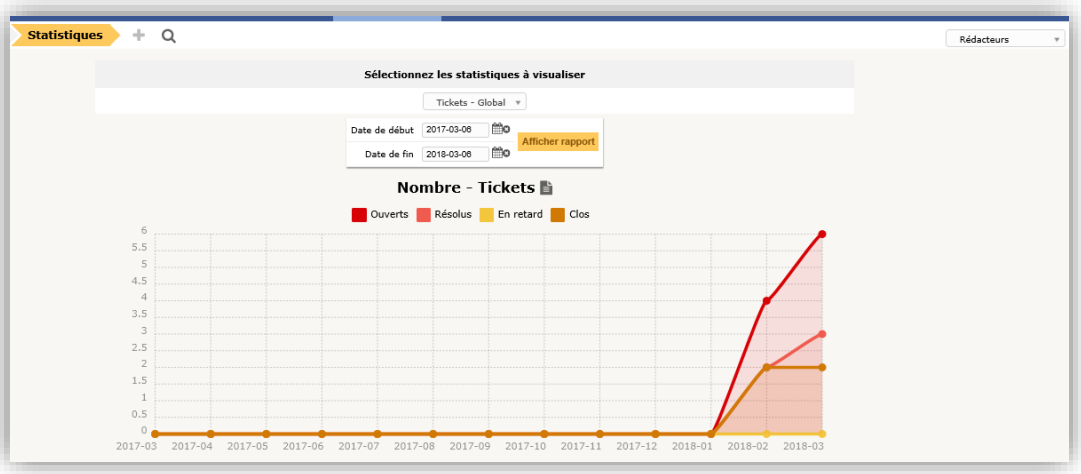
Ces contacts seront également répertoriés dans la liste globale de tous les contacts ajoutés, disponibles depuis l'onglet « Gestion » puis « Contacts ».



6.1.5 Tenue de statistiques

Les statistiques sont présentes par défaut dans GLPI, et peuvent également être complétées par des plugins tels que ***Dashboard*** (tableau de bord) qui affiche des statistiques sur les tickets et le parc, sous forme de différents graphiques.

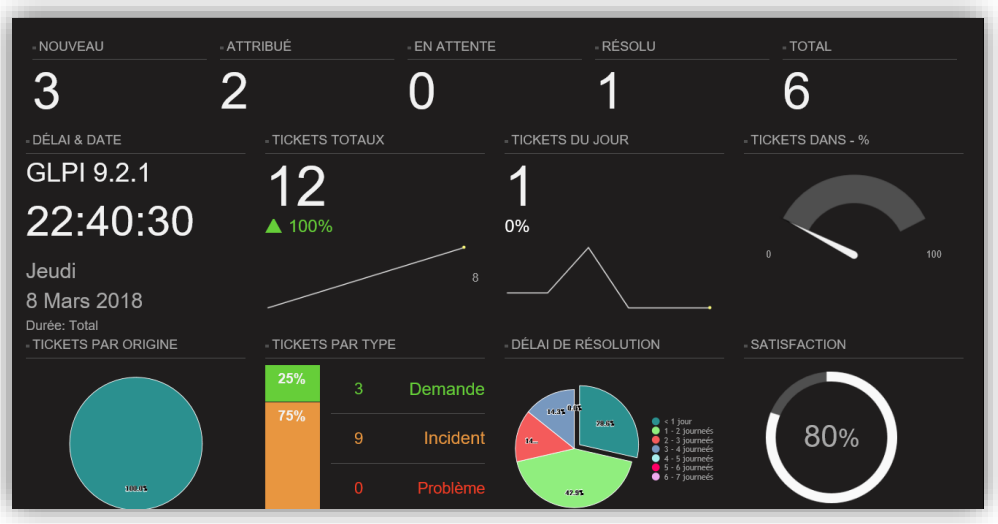
Les statistiques incluent le nombre de tickets ouverts, la durée moyenne de



Statistiques affichant le nombre de tickets sur une période donnée

clôture/résolution, la satisfaction des utilisateurs.

Le plugin Dashboard se présente sous la forme d'un affichage de métriques sur un écran au sein du service informatique. Cela peut être source de motivation pour le service pour l'encourager à améliorer la qualité des services rendus, notamment en visualisant le nombre de nouveaux tickets, les délais de résolution ou encore le taux de satisfaction des utilisateurs



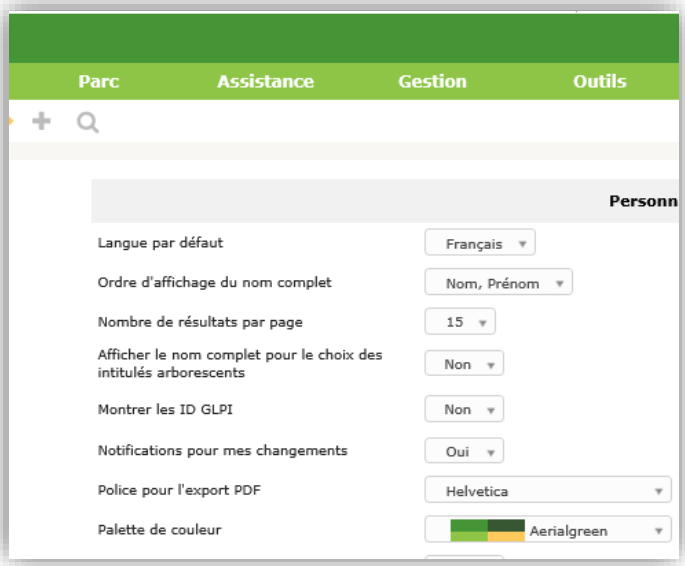
Affichage des métriques avec le plugin Dashboard

Enfin, la tenue des statistiques peut être très utiles pour le service comptabilité, notamment pour visualiser les entrées et sorties de stocks. Le but étant que GLPI soit un logiciel qui facilite les services métiers dans leurs tâches quotidiennes.

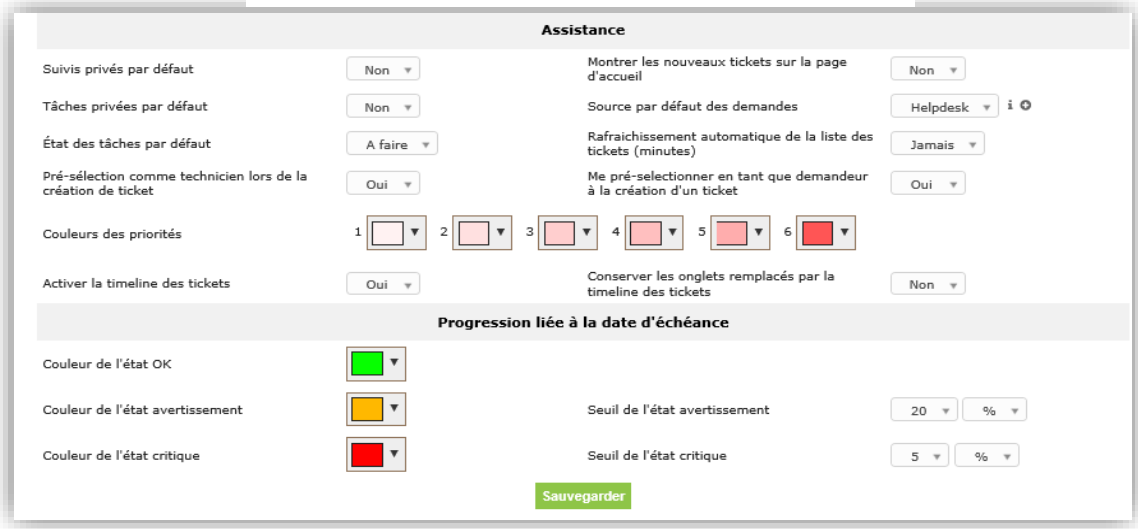
6.1.6 Personnalisation de GLPI

GLPI est entièrement paramétrable et personnalisable. Il est possible d'adapter cet outil aux couleurs de l'entreprise en remplaçant le logo GLPI par celui de ModulHab.

Il est également possible de modifier les couleurs du GLPI grâce à de nombreuses palettes de couleurs. Les différentes couleurs utilisées pour les priorités ou pour les états (OK, avertissement, critique) peuvent également être modifiées, tout comme la disposition des onglets, les formats de dates, etc.



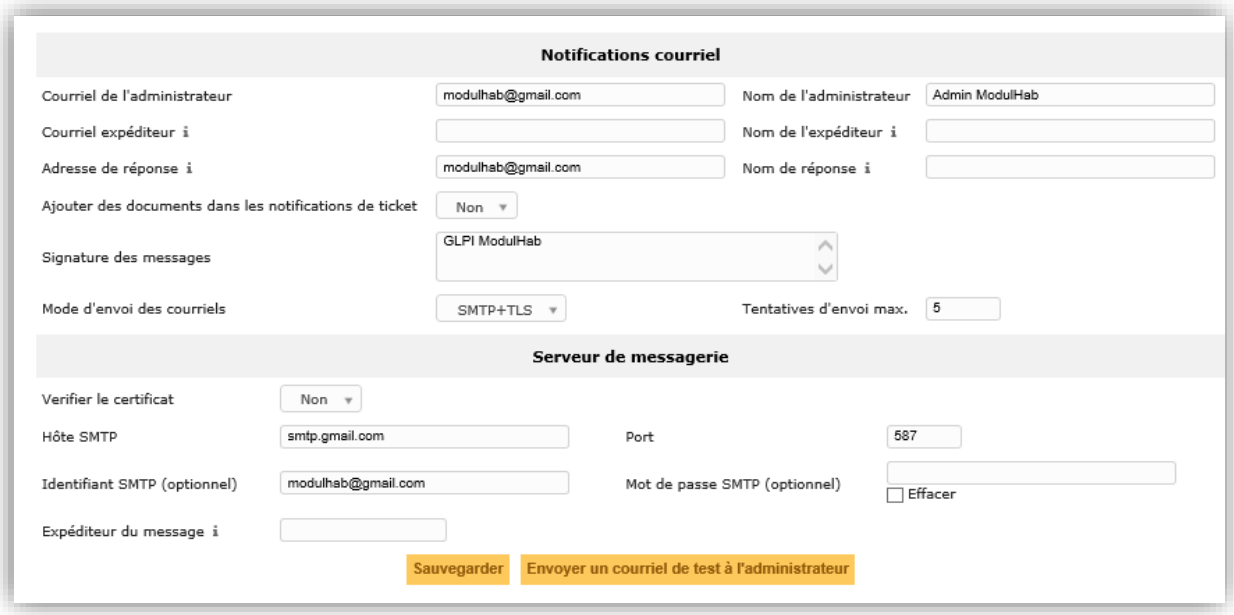
Modification de la palette de couleurs



Exemple de paramètres pour l'assistance et les dates d'échéances

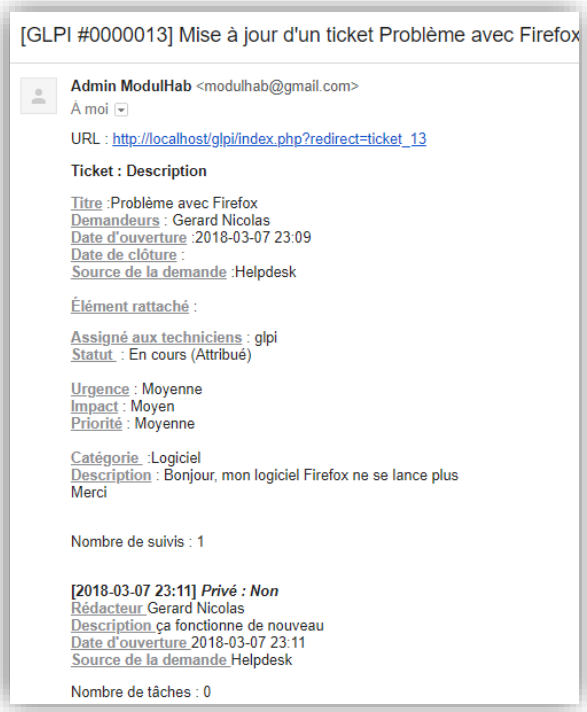
Notifications mail

Les notifications par mail peuvent être configurées en renseignant les différents paramètres du serveur mail utilisé. Voici un exemple de configuration avec une adresse Gmail :

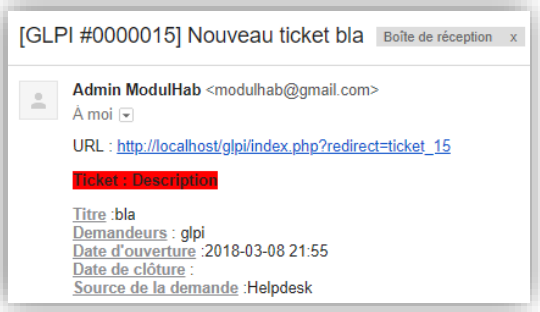


Voici un exemple de mail entrant concernant la mise à jour d'un ticket. Il s'agit d'un modèle de notification par défaut, qui peut bien entendu être édité à souhait.

Le ticket est accessible par un lien accompagné de toutes ses informations principales dont le titre et le contenu du ticket.



Notification mail

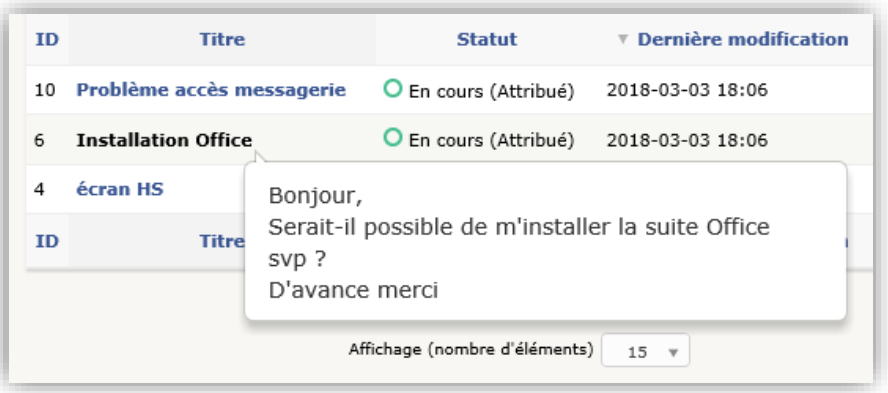


Exemple d'un mail édité (modification de la couleur du titre par exemple)

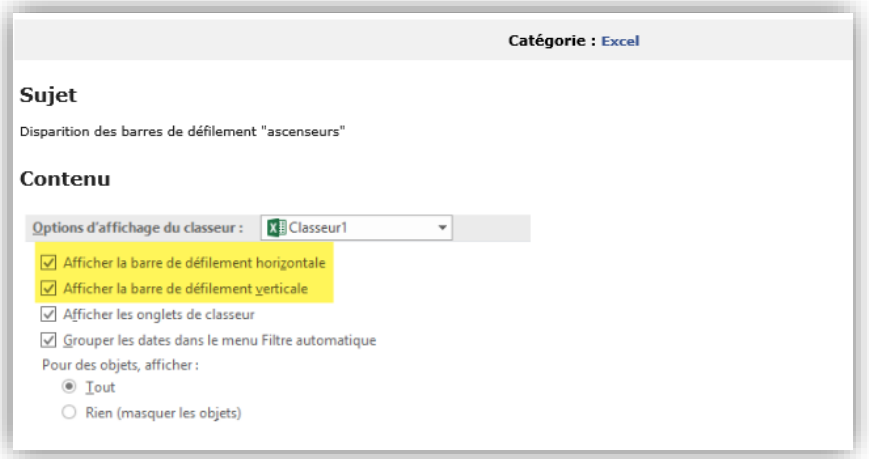
6.1.7 Intuitivité de GLPI

GLPI est une solution complète et entièrement personnalisable. De prime abord surchargé et compliqué à prendre en main, nous veillerons à le paramétrer pour l'adapter aux besoins du technique, avant de la proposer aux utilisateurs. Son ergonomie sera améliorée en épurant son interface (champs inutiles à masquer, gestion des droits, etc.) pour une meilleure appropriation.

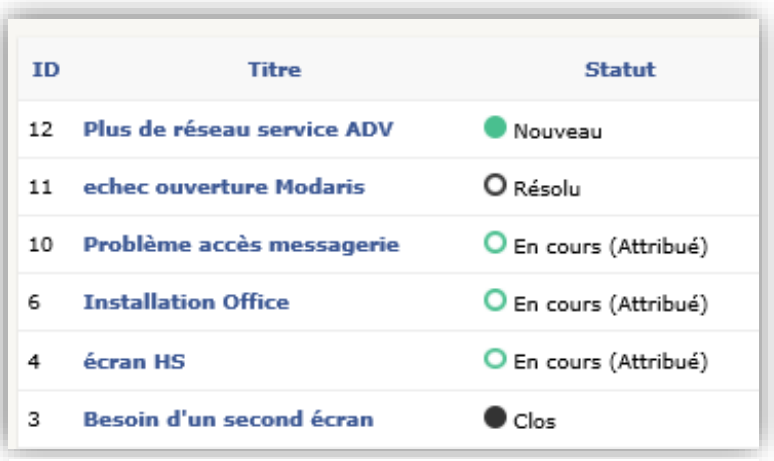
Voici quelques fonctionnalités permettant d'améliorer l'intuitivité de GLPI :



Affichage d'une bulle avec le contenu de la demande lors du survol sur le titre

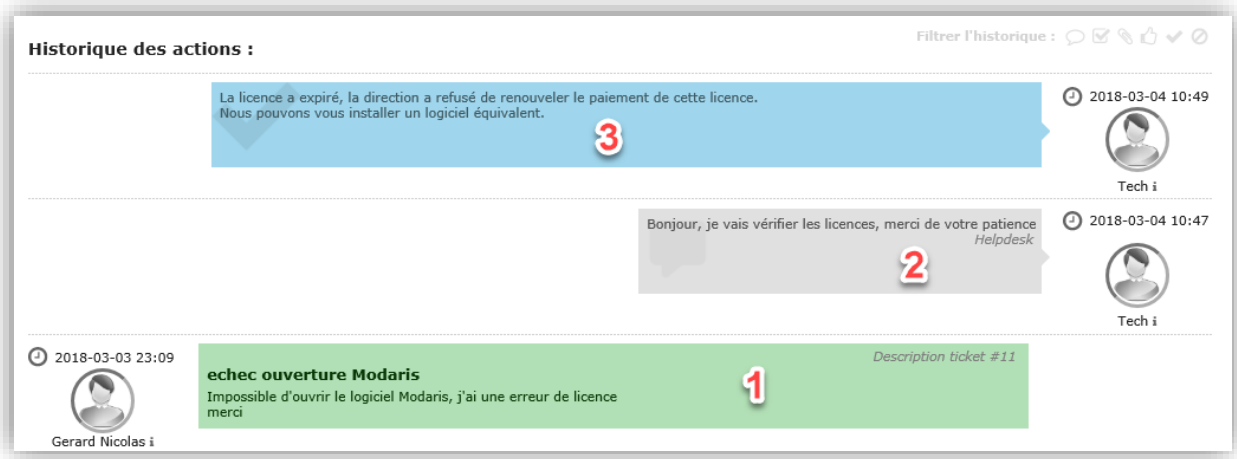


Intégration des images dans le contenu d'un article de la base de connaissances



Codes couleur indiquant le statut d'un ticket

Aperçu miniature d'une image ajoutée à un ticket



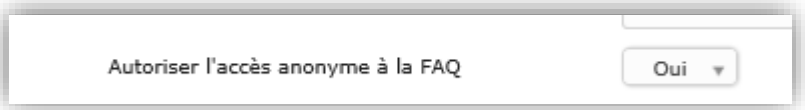
Couleurs pour les différents messages d'un ticket (1 : description initiale, 2 : suivi technicien, 3 : solution apportée)

Concernant l'accès au portail et l'utilisation de GLPI, se reporter

6.1.8 Base de connaissances

La base de connaissances est administrée uniquement par le Service Informatique qui gère les droits d'accès et d'écriture. Le plus souvent, les utilisateurs peuvent ajouter des articles pour leur métier.

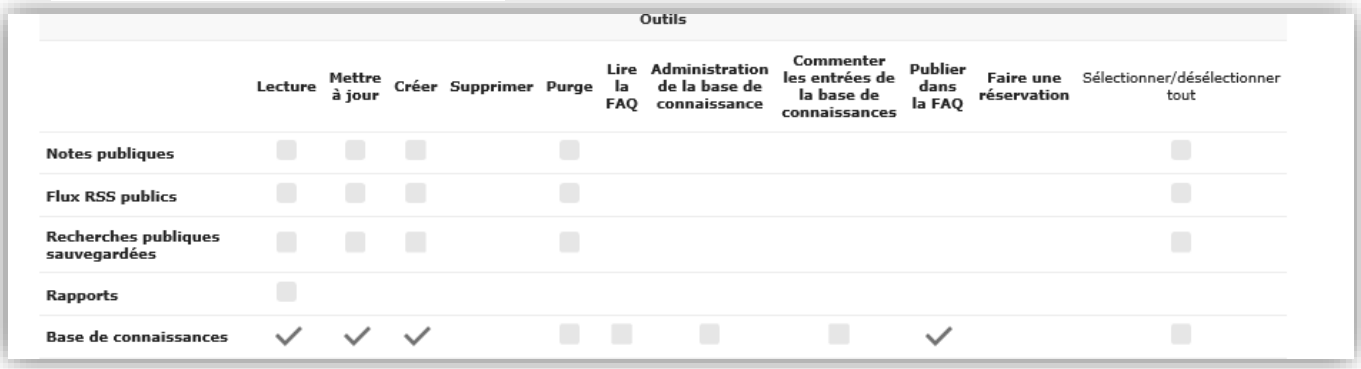
L'accès anonyme à la base de connaissances peut être activé depuis le panel d'administration. De cette manière, le contenu de la FAQ est visualisable sans avoir à saisir d'identifiants : un nouvel arrivant qui ne dispose pas d'identifiants Windows pourra donc se connecter au GLPI et accéder à la documentation depuis l'accueil.



Paramètre à modifier pour autoriser l'accès anonyme, depuis l'onglet « Configuration » puis « Générale »

Un lien « Accéder à la Foire Aux Questions » apparait sous la zone de connexion.

Des profils « rédacteurs » peuvent être paramétrés avec des permissions spécifiques pour que des collaborateurs des différents puissent apporter leur contribution en ajoutant une documentation sur les diverses applications métiers utilisées.



6.1.9 Communication et satisfaction des utilisateurs

Communication

La communication tient un rôle très important dans d'une société si bien que le service IT doit user de ces procédés pour maintenir un bon relationnel avec l'ensemble des services.

La satisfaction des utilisateurs repose ainsi sur la qualité des communications avec le service informatique dont la tâche consiste à exploiter l'épine dorsale de l'entreprise en gérant les données de tous les services. En conséquence, le niveau de satisfaction est un élément à prendre en compte pour cimenter et les liens entre le technique et le reste de la société pour maintenir un niveau de confiance et de crédibilité optimal.

Pédagogie

Le service informatique détient un rôle de vulgarisateur. Le but étant de sensibiliser les utilisateurs sur les bonnes pratiques à adopter dans l'usage de l'outil informatique en rappelant des règles élémentaires de sécurité. Ceci peut se faire par le biais de formations qui peuvent également expliquer le fonctionnement de certains logiciels de la vie courante. L'important est de pouvoir se faire comprendre sans rester dans un discours trop technique en utilisant des métaphores ou des analogies qui facilitent la communication.

Une bonne connaissance du terrain

Une bonne communication avec les utilisateurs améliore et facilite la qualité du dépannage et la résolution des problèmes. Ceci requière une bonne connaissance des différents métiers et de leur problématique au sein de l'entreprise.

Il est important de communiquer dès l'apparition d'un problème ou d'une panne informatique afin d'informer les utilisateurs le plus vite possible. Cela aura plusieurs avantages :

- Démontrer la réactivité du service informatique.
- Éviter de laisser les utilisateurs dans le flou, ce qui a tendance à émettre plusieurs appels et/ou à ouvrir plusieurs tickets pour un même problème.
- Rassurer les utilisateurs en leur apportant des informations supplémentaires.

Informer

Toutefois, il ne faut pas communiquer uniquement lors d'incidents, ce qui placerait le service informatique dans une posture de justification. Ainsi, il est important d'échanger avec les utilisateurs sur la mise en place de nouveautés pour les informer que tel changement améliorera leurs conditions de travail. Il est par ailleurs important de rassurer les utilisateurs en leur faisant part des mises à jour importantes des logiciels ou bien de campagnes anti-ransomware afin de les sensibiliser et les placer comme acteurs de la sécurité de l'entreprise.

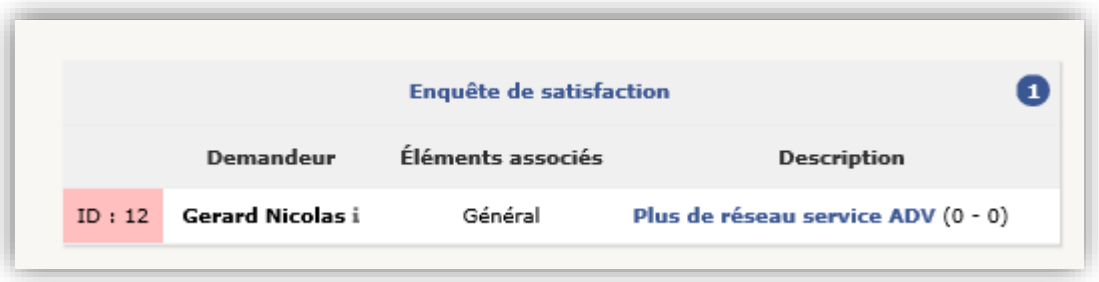
En somme, tous ces éléments de communications sont essentiels et évitent de véhiculer l'image négative d'un service informatique distant qui ne serait là que pour la résolution des problèmes. Il apparait donc essentiel de se placer dans la posture d'un bon communiquant pour regagner la confiance et instaurer un climat de confiance entre les utilisateurs et le service informatique interne.

Mise en place de la satisfaction utilisateurs sous GLPI

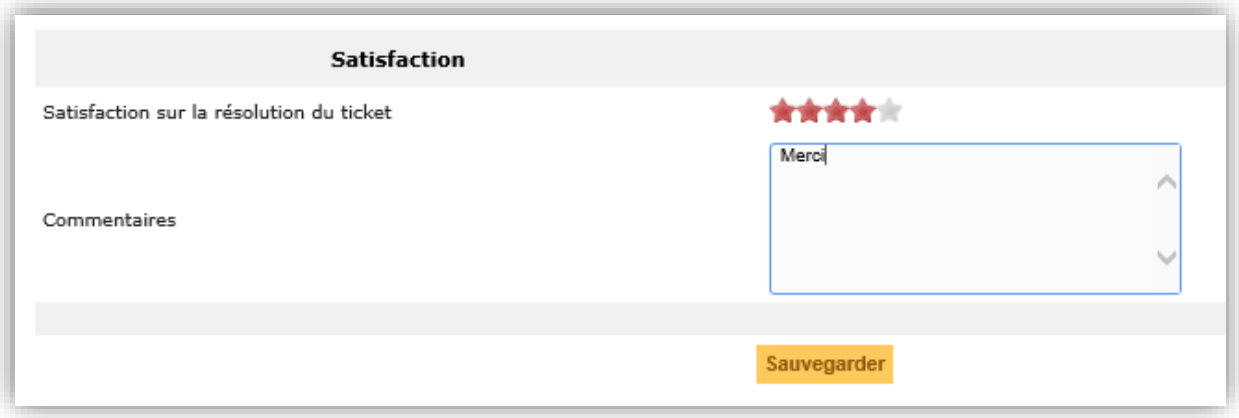
Un pourcentage d'enquêtes de satisfaction peut être paramétré : par exemple, on peut définir un taux à 100% d'enquêtes afin de déclencher une enquête après chaque clôture de ticket.

Ces enquêtes de satisfaction contribuent à améliorer la qualité de service et l'image du SI ce qui aura pour conséquence d'améliorer et faciliter les liens avec les utilisateurs.

Une fois un ticket fermé par le technicien, un nouvel encart apparait sur la page d'accueil GLPI de l'utilisateur, avec le nom du ticket associé à l'enquête.



L'utilisateur peut alors ajouter une note, sur 5 étoiles, ainsi qu'un commentaire.



Les notes données serviront donc à alimenter les statistiques au sein du GLPI avec une représentation du niveau de satisfaction des utilisateurs par des graphiques (voir partie 6.1.5).

En définitive, GLPI est une solution qui s'adapte complètement à l'ensemble des points mis en avant dans le cahier des charges. Plus globalement, il contribuera à améliorer la gestion du parc sur les aspects techniques, organisationnels et humains en opérant un rapprochement certain entre le SI et les utilisateurs pour un meilleur suivi des incidents et des maintenances et de l'évolution du système d'information.

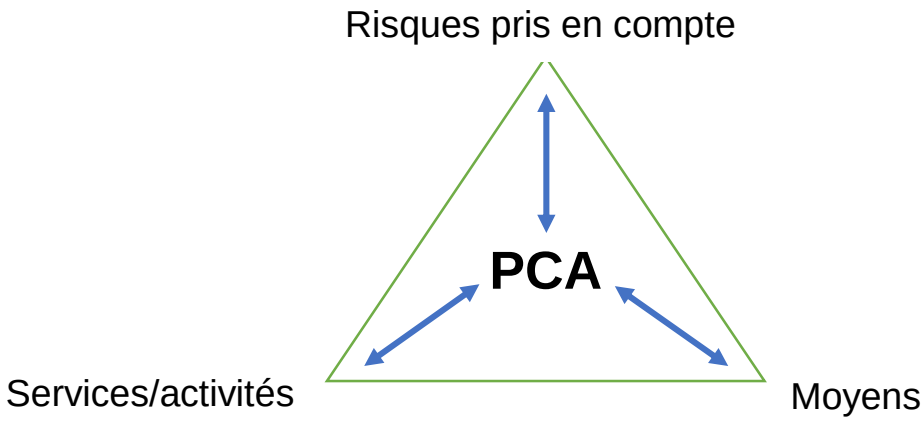
7.CONTINUITÉ D'ACTIVITÉS

L'audit interne réalisé par Modulhab a mis en exergue l'incapacité de la société à affronter les moments de crises tels que les défaillances des équipements informatiques qui ont occasionné des pertes financières considérables. Effectivement, aucun plan de continuité d'activité (PCA) ou plan de secours informatique (PSI) n'a été implémenté pour faire face aux risques auquel Modulhab s'expose.

7.1 Synthèse sur le PCA et PSI

La planification de la continuité d'activité requière l'identification des menaces potentielles et ses impacts sur les activités d'une organisation. Un cadre est alors défini pour prendre en compte les caractéristiques inhérentes de l'entreprise et à partir desquelles la *résilience* du système informatique de la société pourra être élaborée. Le but est d'apporter des réponses efficaces face aux risques majeurs tout en préservant l'activité et les intérêts d'une organisation.

Dans le cadre de cette réflexion, un PCA (« Plan de Continuité d'Activité ») est élaboré. Il consiste en plusieurs processus qui visent à assurer le maintien opérationnel des services d'une société en mode dégradé lors d'un scénario de crise majeur et ce, jusqu'à la reprise des activités. Un PCA prend en compte les risques de sinistres, les activités de l'entreprise et les moyens à déployer.



Acteurs impliqués : La plupart des services d'une entreprise doivent être partie prenante dans l'élaboration d'un PCA :

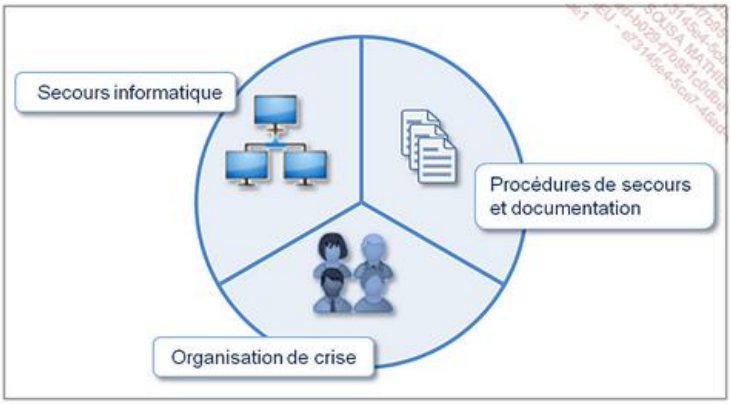
- La **Direction générale** joue un rôle de pilote en validant la stratégie à adopter et sa mise en œuvre.
- Les **différents services** sont au cœur du dispositif et doivent être consultés pour qu'ils puissent formuler l'impact d'une crise sur leur activité.
- Le **service informatique** intervient en tant qu'équipe opérationnelle qui déploie les solutions de secours informatique.

Il faut noter que le monde informatique s'est approprié le terme de PCA pour l'appliquer à ses propres problématiques alors que son acception est plus générale. Il sera alors plus judicieux de parler de **PSI** (« plan de secours informatique ») qui est activé lors d'une crise. Il implique cependant les mêmes acteurs évoqués ci-dessus dans le cadre de sa conception.

7.2 PSI (« Plan de Secours Informatique »)

Le PSI est une étude technique qui entre dans le cadre du PCA. Ce plan adopte la même démarche que le PCA à la différence près qu'il se cantonne au périmètre de l'informatique.

Un PSI concentre un ensemble de dispositifs qui sont nécessaires pour le redémarrage d'un système d'information après un sinistre :



Composants du plan de secours informatique (source : Plan de Continuité d'Activité, ENI édition)

- **Secours informatique** : ensemble des serveurs et réseaux de secours.
- **Procédures de secours** : correspond au **PRI** (« plan de reprise informatique »), décrivant les procédures, l'architecture du secours, des manuels, etc.
- **Organisation de crise** : liste des personnes à mobiliser en cas de sinistre.

Les principaux domaines qu'englobe le PSI sont :

Domaines d'application	Technologie
Système d'informations	➢ Serveurs ➢ Stockage ➢ Logiciels
Réseau	➢ Réseau local (LAN) ➢ Réseau distant (WAN)
Téléphonie	➢ VoIP

La gestion de la téléphonie étant dévolue à l'opérateur de la société Modulhab, nous traiterons seulement des solutions techniques qui s'appliquent aux domaines des systèmes et des réseaux.

Les documents livrables pour le PSI sont :

- Plan de Reprise Informatique (PRI) : décrit la cinématique globale après le redémarrage du système d'information après une coupure franche.
- Procédures de secours informatique : comprend l'ensemble des procédures à mettre en œuvre pour activer le secours des systèmes et des applications.

7.3 Risques, impacts métiers : étude des besoins de continuité

7.3.1 Analyse des risques

Le besoin de continuité dans les différents secteurs de l'entreprise s'évalue sur le degré d'utilisation et d'intégration du système d'information et des outils informatiques dans l'ensemble des processus de production. Autrement dit, plus les services s'appuieront sur l'outil informatique, plus la gravité d'une interruption aura un impact critique sur la survie de l'entreprise.

Nous avons fait la synthèse des différentes menaces qui peuvent occasionner l'indisponibilité du système d'information :

- **Risques humains** : maladresse, manque de formation du personnel, mauvais entretien, malveillance.
- **Risques techniques** : mauvaise conception, piratage, panne matérielle et logicielle, piratage.
- **Risques environnementaux** : inondations, incendie, foudre, chaleur excessive.

À la lumière des risques identifiés, il convient d'évaluer maintenant l'impact que peut engendrer l'indisponibilité du système d'information sur les métiers de Modulhab.

7.3.2 Analyse d'impacts métiers (BIA)

L'élaboration d'un PSI commence par la définition du périmètre dans lequel sont comprises les activités de l'entreprise qu'il faudra secourir en priorité. Cette étude, validée par la Direction Générale, a été menée en étroite collaboration avec les acteurs de l'entreprise et leurs représentants. Elle nous a permis de cerner l'expression des besoins des métiers en prenant en compte les pertes financières, de productivité, l'impact sur l'image/réputation de la société ou encore les conséquences juridiques.

Pour ce faire, nous avons utilisé deux indicateurs de durée :

- **DIMA**, « Durée d'Interruption Maximale Admissible » : Délai de mise à disposition d'une application après une interruption. Ceci induit un délai de reprise d'activité : s'il est dépassé, l'entreprise s'expose à de sérieuses pertes.
- **PDMA**, « Perte de Données Maximale Admissible » : Délai pendant lequel la perte de données est tolérée.

Ces durées permettent de traduire le niveau de criticité des services tout en exprimant leur besoin en termes de continuité :

	Besoin de continuité d'activité		
Services de l'entreprise	DIMA	PDMA	Postes de travail
Administratif	H+8	H+8	6
Ressources humaines	H+8	H+8	3
Comptabilité	H+8	H+8	4
Recherche & Développement	J	J	4
Qualité	J	J	4
Bureau d'étude	J	J	16
Commerce	J	J	37
Installation	H+4	H+4	51
Production	H+4	H+4	15
Logistique	H+4	H+4	14
Achats	H+8	H+8	7
SAV	J	J	26

Les besoins par activités ont été collectés par des entrevues avec les responsables des services ou réalisés par ces derniers.

A titre d'exemple, on considère acceptable le temps d'indisponibilité du SAV à 24h (J) car son engagement de service contractuel est d'une journée, suite à quoi s'applique des pénalités. Il en est de même pour le service commercial dont les contrats en cours et les cycles de vente s'étalent sur plusieurs jours.

En guise de synthèse, les services qui ont un besoin de continuité d'activité ont été classés dans ce tableau, d'un niveau de criticité allant de plus fort au plus faible.

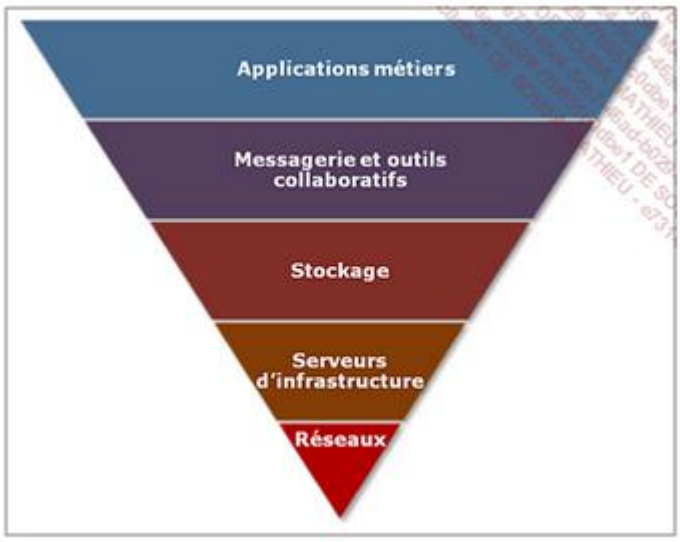
Critique (inférieure ou égale à 4 heures (H+4)	Installation Production Logistique
Sensible (inférieure ou égale à 8 heures (H+8)	Administratif Ressources humaines Comptabilité Achat
Annexe (inférieure ou égale à 24 heures (J)	Recherche & Développement Qualité Bureau d'étude Commerce SAV

Par cette action, nous visualisons mieux la stratégie de continuité à appliquer en fonction des services pour la continuité et la reprise d'activité en cas de sinistre. Nous

savons que cette priorité devra s'appliquer pour les services **Installation**, **Production** et **Logistique**. Dans une moindre mesure, les services **Administratif**, **Ressources humaines**, **Comptabilité** et **Achats** viendront dans la suite des priorités précédemment énoncées.

7.4 Solutions de secours

Le système d'information peut être conceptualisé sous la forme d'une pyramide inversée comportant plusieurs couches qui s'empilent les unes sur les autres selon un ordre logique. Les deux dernières couches hautes constituent l'ensembles des applications bureautiques et métiers sur lesquelles s'appuient les services de l'entreprise.



Pyramide d'un système d'information (source : Plan de Continuité d'Activité, ENI édition)

À la lumière de ce schéma, les couches réseaux et serveurs (que l'on peut amalgamer avec la couche stockage) présentent une criticité importante puisque les applications reposent sur ce matériel physique. Le PSI doit ainsi prévoir des solutions pour les couches réseaux et serveurs afin d'assurer la pérennité des applications.

7.4.1 Redondance de l'infrastructure réseau

Il n'est pas concevable que votre société soit pénalisée par une coupure internet prolongée puisqu'un tel incident couperait les services en relation continue avec :

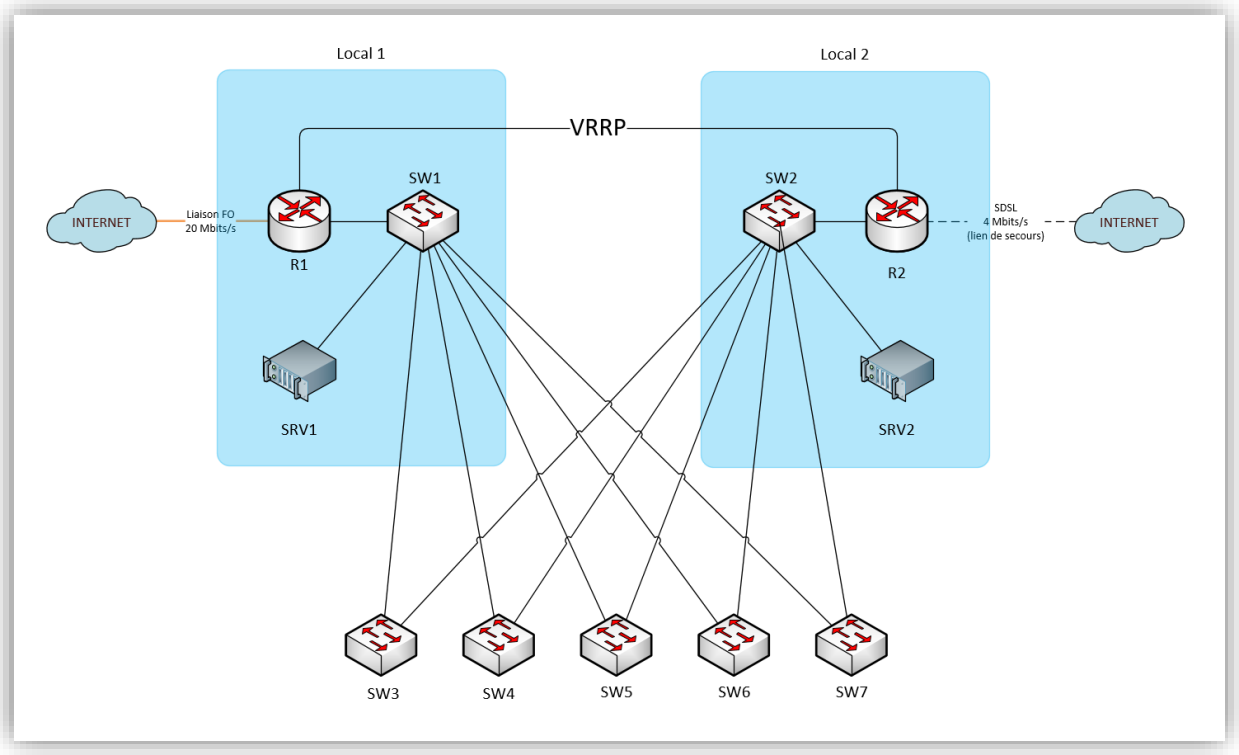
- La clientèle.
- Les prestataires/fournisseurs.
- Les équipes itinérantes dotées d'un ordinateur portable avec accès VPN.
- Votre prestataire informatique (Trust-IT).

Partie WAN

L'activité de plusieurs services repose sur l'utilisation d'internet et une coupure excédant 30 minutes aurait des répercussions sérieuses sur l'activité générale de l'entreprise.

Nous vous recommandons sans réserve d'opter pour une double liaison internet (dite double adduction) avec une liaison principale (maître) basée sur la fibre et une secondaire basée sur une SDSL (backup) : si une panne affecte la liaison principale, une bascule automatique s'opérera, sans provoquer d'interruption d'internet. Ce type d'offre est proposé par des opérateurs télécoms fournissant des services orientés professionnels.

Nous exploiterons cette configuration en manageant vos deux routeurs. Ces deux derniers utiliseront le protocole **VRRP** (« *Virtual Router Redundancy Protocol* ») qui consiste à augmenter la disponibilité de la passerelle par défaut (en somme, la porte de sortie qui permet à tout poste informatique d'accéder à internet) au moyen d'une IP WAN virtuelle associant le groupe de deux routeurs : R1, dit « *master* » et R2 dit « *backup* ». Si R1 tombe, R2 qui était *backup* devient *master*.



Topologie logique de l'infrastructure réseau de Modulhab.

Pour accroître la robustesse et la disponibilité de ce dispositif, il sera nécessaire de faire parvenir les deux adductions dans deux locaux séparés et distants (ou chaque serveur sera déjà installé).

Partie LAN

Pas moins de 7 commutateurs seront nécessaires pour véhiculer les trames entre les quelques 200 postes du parc. Les dispositions nécessaires à la mise en œuvre de la haute-disponibilité du réseau sont les suivantes :

- Double interconnexion des 5 commutateurs 48 ports (SW3-7) avec les 2 commutateurs 8 ports (SW1-2).
- Configuration de VLAN (« *Virtual Local Area Network* ») pour les services de l'entreprise.
- Des commutateurs supplémentaires et préconfigurés seront présents dans le spare.

La double interconnexion des commutateurs SW3 à 7 qui alimentent tous les postes informatiques et les périphériques apporte de la haute-disponibilité car la perte

complète du local 1 assurera une continuité d'activité totale (accès à internet et communication pérenne de tous les postes utilisateurs).

La configuration de VLAN ou sous-réseaux virtuels regroupement un ou plusieurs services optimisera la bande passante tout en sécurisant le réseaux intranet : si un service sature la bande passante disponible, ce dérangement n'affectera pas les autres sous-réseaux.

Bien que robuste et sujet à des risques de pannes assez faible, des commutateurs préconfigurés stockés en spare permettront un remplacement rapide si une défaillance devait survenir sur l'un des commutateurs.

Services	VLAN	Adressage
▪ Direction ▪ Administratif ▪ RH ▪ Comptabilité ▪ SI	10	192.168.10.0/24
➢ Recherche & développement ➢ Qualité ➢ Bureau d'étude	20	192.168.20.0/24
➢ Commerce ➢ Installation	30	192.168.30.0/24
➢ Production ➢ Logistique ➢ Achat	40	192.168.40.0/24
➢ SAV	50	192.168.50.0/24

7.4.2 Réplication des données : comparaison des solutions

Deux types de solutions existent pour organiser la réplication des données :

- La réplication matérielle.
- La réplication logicielle dite « *host based* ».

Ces solutions requièrent au minimum deux serveurs basés sur le modèle maître/esclave.

Réplication	Avantages	Inconvénients
Matérielle	➢ Volumes intégralement répliqués (application, données, base de données. ➢ Serveurs peu sollicités pour la réplication des données.	➢ Solution très onéreuse. ➢ Ressources réseaux importantes. ➢ Délais de mise en œuvre important (3 mois en moyenne)
Logicielle	➢ Nécessite peu de matériel. ➢ Solution peu onéreuse. ➢ Mise en œuvre plus rapide.	➢ Sollicitation plus importante des serveurs. ➢ Réplication à mettre en œuvre au cas par cas.

La réplication matérielle synchrone ou asynchrone est basée sur les disques d'un SAN auquel sont reliés des serveurs. Cette architecture est généralement combinée avec un système de cluster. Le grand avantage réside dans sa capacité à assurer dans des délais minimes une continuité d'activité tout en répliquant l'intégrité des volumes de stockage en cas de perte d'un serveur. Cependant, cette solution est très onéreuse et demande des ressources réseaux importantes tandis que sa mise en œuvre assez lourde peut courir sur plusieurs mois.

A contrario, la réplication logicielle permet d'assurer une continuité d'activité dans des délais court avec peu de ressources matérielles, ce qui rend la solution moins onéreuse. Cependant, cette solution doit être mise en œuvre au cas par cas en fonction des applications (ce qui ne serait pas le cas avec un SAN qui globalise l'ensemble du système d'information).

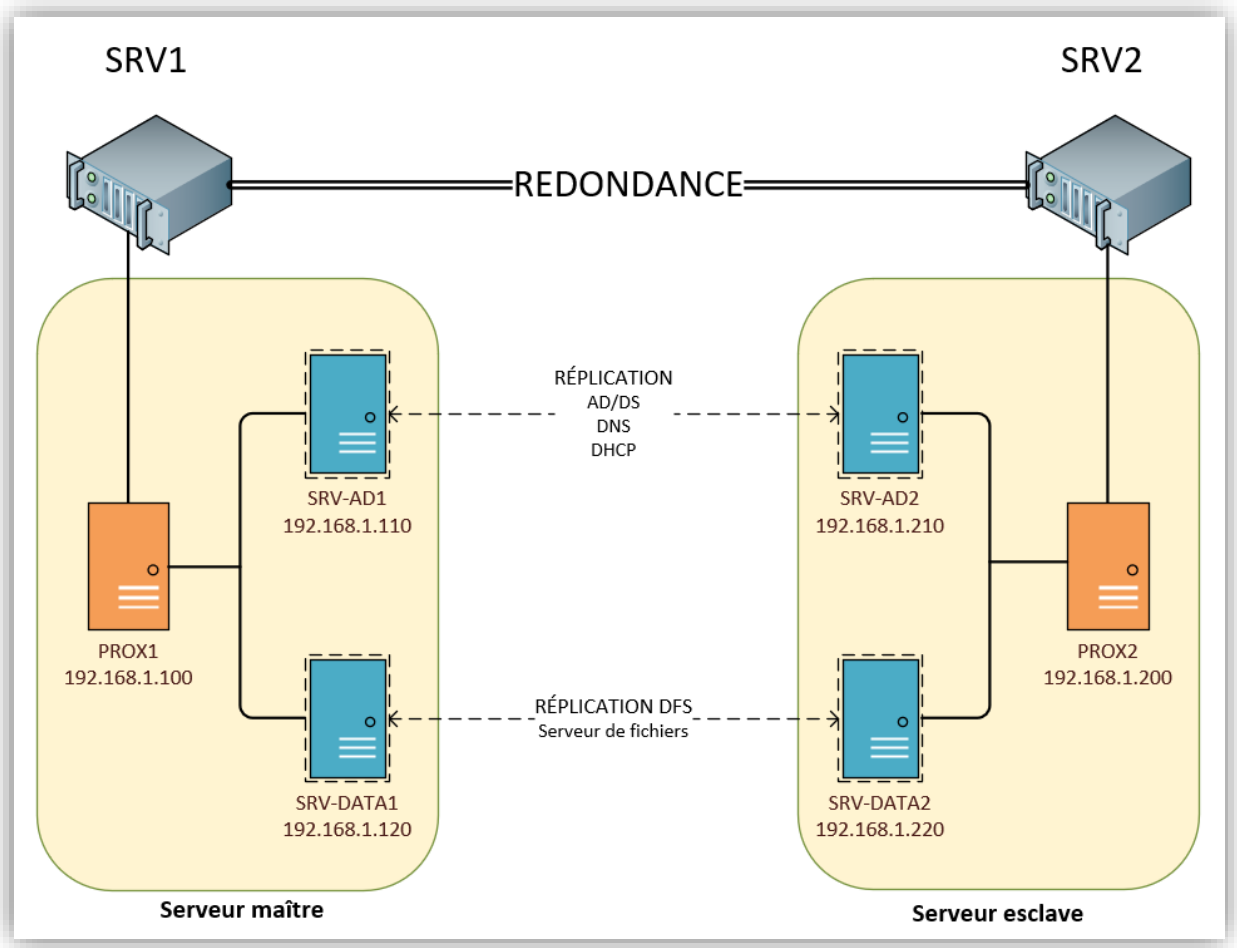
Nous proposons ainsi cette dernière solution qui, en l'état actuel du besoin, garantira la continuité d'activité pour les services les plus critiques de Modulhab.

7.4.3 Configuration de la haute disponibilité

Conformément aux recommandations de sécurité énoncées par la CNIL, il est fortement déconseillé d'héberger en un seul endroit toutes les données d'entreprise. Ainsi, dans le cadre de la réplication des données, les serveurs maître et esclave seront installés dans des locaux différents du même bâtiment.

Plusieurs systèmes d'exploitation utiles dans le fonctionnement du système d'information seront virtualisés au moyen de ***VM*** (« *Virtual Machine* », machine virtuelle). Cette segmentation permet de répartir la charge d'utilisation tout en fiabilisant le fonctionnement général de l'infrastructure.

En outre, nous pourrons nous appuyer sur plusieurs VM pour configurer la haute disponibilité du système.



Organisation de la redondance des principaux services de l'infrastructure système.

Une première VM (SRV-AD1) hébergeant les services système essentiels (Active Directory, DNS, Contrôleur de domaine, DHCP) seront répliqués sur une VM présente sur le 2e serveur (SRV-AD2).

La même configuration est prévue pour le serveur de fichiers (SRV-DATA1) dont les données seront répliquées sur une autre VM (SRV-DATA2) hébergée dans le serveur esclave. Nous opterons par une réplication synchrone, 24/24h, 7/7j dans la configuration du serveur de fichiers DFS.

Ainsi, en cas de sinistre engendrant une perte de SRV1, une bascule automatique s'effectuera sur SRV2, faisant passer ce dernier du statut de serveur esclave à serveur maître. Cette configuration possède le double avantage d'équilibrer la charge d'utilisation des serveurs pour certains services tout en assurant, de façon transparente, une continuité de service et un accès continu aux données utilisateurs.

À noter que le dimensionnement des VM pourra dépendre du niveau de besoin des services comme abordé précédemment (analyse BIA, partie 7.3.2).

7.4.4 PRI (« Plan de Reprise Informatique)

Le PRI est déclenché après un sinistre afin de basculer sur un système de relève pour activer le redémarrage des activités indispensables à la survie de l'entreprise.

Supervision de la bascule en cas de sinistre

La haute disponibilité du système d'information étant basée sur la redondance des équipements, il sera du ressort du SI de Modulhab de surveiller que la bascule automatique des équipements s'est déroulée correctement. Le cas inverse, Trust-IT vous aidera à superviser d'encadrer la reprise du système si la bascule ne s'effectue pas.

Principes de la sauvegarde

La redondance des données ne doit pas être confondue avec la sauvegarde de données. En l'absence d'un plan de sauvegarde, une entreprise s'expose à la perte irrémédiable de données. Il est ainsi impératif de définir et d'instaurer une politique de sauvegarde des données les plus critiques de l'entreprise : ce dispositif est une des composantes clés du Plan de Reprise Informatique (PRI).

Conformément aux recommandations de la CNIL et de l'ANSSI, les données feront l'objet de deux types de sauvegarde :

- Sauvegarde complète mensuelle.
- Sauvegarde incrémentale quotidienne.

L'analyse d'impact métiers sera déterminante pour définir les priorités de sauvegarde, notamment dans le cadre de la sauvegarde incrémentale dont les processus peuvent impacter les performances du réseau.

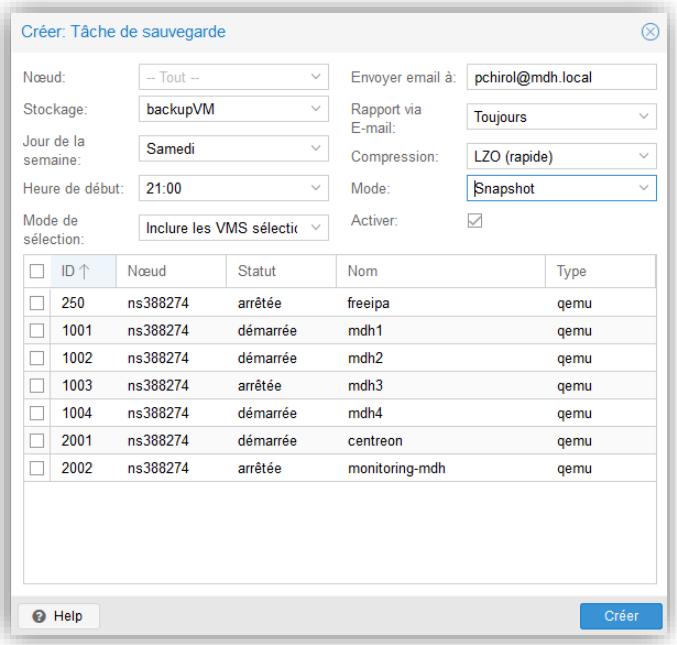
Acronis

Le logiciel Acronis Backup permet de configurer les sauvegardes incrémentielles ou complète de manière automatisée. Nous vous proposons cette solution car sa prise en main est intuitive est simple. En outre, Acronis présente l'avantage de s'intégrer facilement dans un environnement Windows Server en reconnaissant les utilisateurs d'un Active Directory.

Sauvegardes des VMs avec Proxmox

Proxmox possède des outils de sauvegarde et de restauration des VMs. Ainsi, si une machine est corrompue ou ne fonctionne plus, il est possible de revenir en arrière en restaurant la machine qui a été sauvegardée la veille.

Il est possible de régler et les jours de la semaine tout en sélectionnant les VMs de notre choix.



Nous contrôlerons régulièrement l'efficacité des sauvegardes par des tests de restauration dans le but d'éprouver l'efficacité des procédures mis en place.

Liste des intervenants

Plusieurs acteurs interviennent dans le PRI :

- Le SI de Modulhab qui doit disposer des outils de supervision pour détecter la moindre défaillance des serveurs.
- Le prestataire (Trust-IT) qui doit pouvoir accéder à la supervision et réagir immédiatement en cas de problème.
- Les fournisseurs qui doivent pouvoir intervenir rapidement pour maintenir les équipements en défaut en cas de défaillance.

7.4.5 Sécurisation des locaux

Les locaux accueillant le cœur de l'infrastructure système et réseau seront protégés par une série de dispositifs destinés à assurer la protection physique des équipements.

Incendie : Des détecteurs de fumée doivent être installés dans les locaux afin d'émettre une alerte si un feu se déclare. De plus, des extincteurs à CO2 de classe B devront équiper chaque local : cette catégorie d'extincteur est adaptée pour l'extinction des feux d'origine électrique. Ils doivent être remplacés obligatoirement chaque année tandis qu'une inspection visuelle tous les trois mois est conseillée pour vérifier leur conformité.

Inondation : Ce risque peut survenir suite à une canalisation d'eau rompue ou un sinistre naturel (crue, pluies intenses, infiltration, etc.). Les équipements seront rackés à bonne hauteur pour les préserver d'un dégât des eaux.

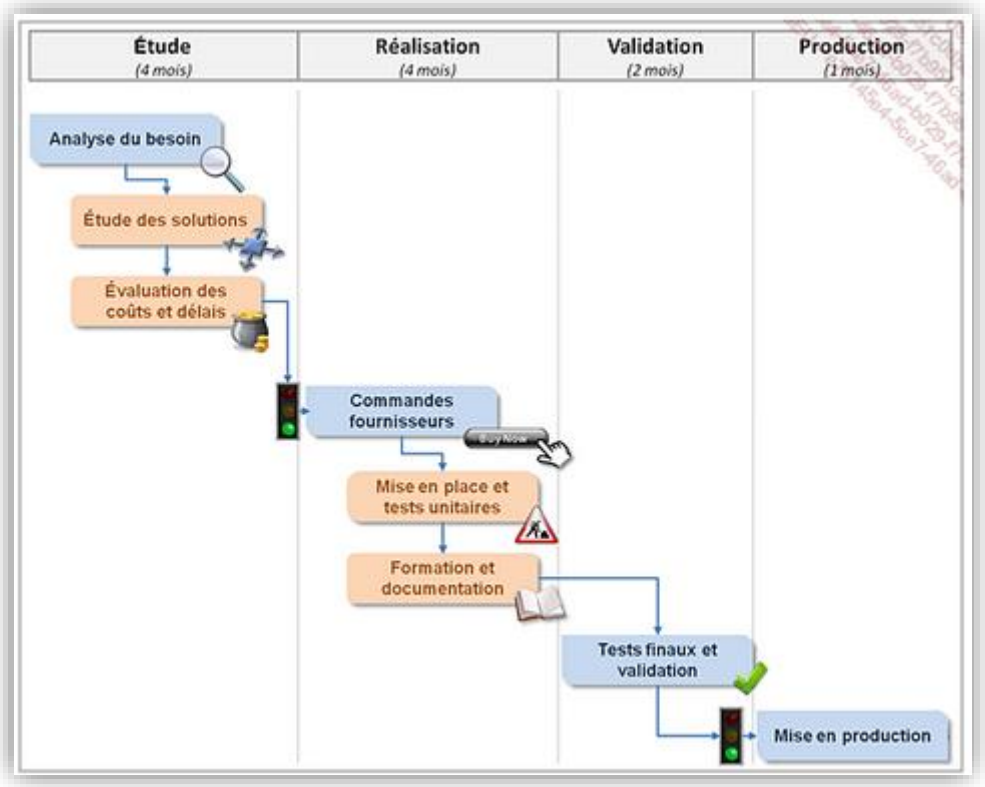
Surchauffe : Les équipements informatiques génèrent une grande quantité de chaleur qui peut s'accroître dans des espaces confinés. Nous installerons des climatisations qui maintiendront une température ambiante comprise entre 24 et 27°.

Surtension : Des onduleurs seront installés dans chaque baie informatique pour protéger les équipements de surtension (risque de foudre, etc.).

7.5 Mise en place du PSI

La mise en production d'un PSI se déroulera sur quatre grandes phases au cours d'une période d'environ 11 mois :

- Étude : 4 mois
- Réalisation : 4 mois
- Tests et validation : 2 mois
- Mise en production : 1 mois



Étapes d'élaboration du plan de secours informatiques (source : Plan de Continuité d'Activité, ENI édition)

Étude : L'analyse du besoin durant la phase d'étude concerne l'expression du besoin des services de l'entreprise au moyen des DIMA et PDMA ainsi que l'étude des risques et l'analyse d'impact métiers dite BIA (voir partie 7.3.2).

Le présent exposé se situe à la fin de cette première étape depuis la réponse à l'appel d'offres il y a environ 4 mois. Nous sommes dorénavant en mesure d'avancer les coûts et les délais nécessaires à la mise en œuvre de la solution.

Réalisation : Après avoir obtenu le feu vert des travaux, nous dispenserons une **formation** au SI interne afin que vos techniciens se familiarisent avec les premiers gestes techniques en cas d'activation du plan de secours. La rédaction de la **documentation** comportera les procédures de secours informatique à appliquer (même en cas de bascule automatique) : il s'agit du PRI qui est un livrable du PSI.

Validation : Cette phase est décisive car elle implique les maîtres d'ouvrage en charge de la validation d'une solution de secours dans le périmètre fonctionnel d'un service : il ne s'agit pas recréer un sinistre mais de vérifier qu'une application métier fonctionne correctement sans impact négatif sur son déroulement normal. La fin de cette étape

donne lieu à la rédaction d'un PV de validation qui fait office de 2e feu vert pour la mise en production du PSI : les parties prenantes sont la maîtrise d'ouvrage, le SI et le prestataire.

Mise en production : Nous veillerons à relever l'impact de la migration de l'ancien vers le nouveau système. Un plan de communication sera élaboré en amont pour informer de l'avancée des opérations.

7.6 Test et maintien opérationnel du PSI

Cette phase fait suite à la mise en production. Le test de secours du PSI consiste à réaliser un test global pour tester sa robustesse et son efficacité. Cet exercice s'effectuera une fois par an en reproduisant un scénario de sinistre (destruction, panne, coupure électrique, etc.) pouvant entrainer la perte d'une salle serveur.

Le périmètre technique des tests englobera les serveurs et le réseau. C'est au cours d'un scénario de panne que le PRI sera appliqué pour tester son efficacité.

Un procès-verbal sera dressé à la fin de chaque test pour attester du bon fonctionnement du PSI. Tout défaut détecté fera l'objet d'une analyse d'impact.

Pour plus de détail sur cette opération, voir la partie concernant la maintenance du PSI (partie 8.3).

8. PLAN DE MAINTENANCE INFORMATIQUE

L'absence de plan d'action pour maintenir les équipements matériels et les logiciels dans un état fonctionnel a énormément pesé sur la santé de l'entreprise en occasionnant des pertes financières conséquentes (coût de remplacement et perte d'exploitation à 92500 €/an). Cette situation alarmante s'est aggravée en entamant la confiance que les utilisateurs et la Direction accordaient à son service informatique.

Nous avons ainsi défini intégralement la politique de maintenance à appliquer sur le parc informatique de Modulhab afin de réinstaurer et consolider un climat de confiance avec le SI tout en minimisant au maximum les risques de pertes financières.

Selon l'AFNOR (NF EN 13306 X 60-319), la maintenance consiste à mettre en œuvre toute une série d'actions dans l'objectif de maintenir un bien dans son état opérationnel afin qu'il puisse effectuer la fonction pour laquelle on l'utilise. Ces moyens d'actions sont d'ordres technique et organisationnel et s'appliquent sur tout le cycle de vie de l'objet.

Le plan d'action proposé s'articule autour de deux types de maintenance : préventive et curative.

8.1 Maintenance préventive

La maintenance préventive consiste à intervenir sur un équipement avant que ce dernier ne devienne défaillant. Par cette action, il est possible de diminuer la probabilité d'apparition d'une panne.

Rappel des dysfonctionnements rencontrés sur le matériel :

- Surcharges au niveau de la mémoire
- Sollicitation trop importante des serveurs
- Surchauffe du matériel
- Manque d'entretien du matériel (exemple : poussière dans les pc).
- Pas de gestion des garanties/contrats de maintenance.

La liste n'est pas exhaustive et il faudra aller au-delà de cet inventaire succinct pour la politique de maintenance.

8.1.1 Entretien des postes informatiques :

- Dépoussiérage périodique des ordinateurs : une tournée d'inspection suivie au besoin de nettoyage se déroulera 2 fois par an.
- Planification des mises à jour système Windows : Un serveur WSUS sera configuré afin de télécharger puis diffuser les mises à jour sur chaque poste à la pause déjeuner de chaque mercredi. Cette configuration évite d'engorger la bande passante du réseau intranet lorsque des postes effectuent des mises à jour de façon autonome.
- Planification des mises à jour antivirus : après chaque journée de travail.
- Nettoyage des systèmes : Activation de la fonction « Nettoyage de disque » au moyen d'une GPO une fois par semaine, chaque vendredi en fin de journée.

- Gestion des garanties/contrats de maintenance : l'outil de supervision effectuera des alertes sur l'échéance des durées des garanties.

8.1.2 Entretien des serveurs :

- Planification des mises à jour système : Cette tâche sera programmée la nuit pour ne pas perturber l'administration générale des postes informatiques.
- Planification de la mise à jour de l'antivirus : Cette dernière s'effectuera chaque week-end avec l'antivirus Bitdefender (voir comparatif des solutions, annexe 6).
- Supervision : La supervision s'effectuera via le logiciel Centreon (partie 5 sur la supervision et le monitoring).

Par ces actions Modulhab entreverra de nombreux avantages, parmi lesquels :

- Un gain économique substantiel.
- Prolongation de la durée de vie du matériel.
- La réduction du temps d'arrêt des équipements.
- L'amélioration des conditions de travail.
- Diminue la fréquence des interventions de dépannage, souvent très onéreuses.
- Maîtrise de la consommation d'énergie grâce à l'optimisation des équipements.
- Meilleure anticipation dans l'achat des pièces à changer.

8.2 Maintenance curative

La maintenance curative consiste à intervenir sur un équipement lorsque ce dernier subit un dysfonctionnement ou est défectueux. Le but est de le remettre en service rapidement en éliminant l'avarie tout en essayant de comprendre les causes de la panne.

Pour rappel, l'absence de maintenance curative s'est traduite par :

- L'absence de gestion des incidents.
- Absence d'une base de connaissances.
- Panne d'un matériel empêchant son utilisation durant 4 jours (perte d'exploitation mesurée à 10000 euros).
- Absence de pièces de remplacement (coût 2500 euros).
- Expiration de la garantie d'un 1 an et demi.
- Perte de temps dans le dépannage des postes (2 heures/semaine)
- Défaillance matérielle engendrant des indisponibilités :
    - Serveurs : 1 heure.
    - Postes de travail : 4 heures.

Une stratégie d'escalade doit être mise en place pour faciliter la déclaration d'une panne (partie 6.1.2 – gestion des incident et annexe 2) jusqu'à sa résolution rapide.

Un contrat de maintenance sera signé entre Modulhab et Trust-IT pour définir le niveau d'escalade des incidents en fonction de la criticité du problème rencontré.

Ce qui suit est à mettre en lien avec l'application des processus dans la gestion des incidents : merci de vous reporter à la partie 6.1.2.

8.2.1 Postes utilisateurs :

La plupart des interventions sur les postes utilisateurs concernent les points suivants :

- × Remplacement de matérielle défectueux (écrans, claviers, etc.).
- × Problèmes d'ordre logiciel.
- × Diminution de performance (surcharge mémoire).

La gestion de ces incidents sera prise en charge essentiellement par le SI de Modulhab. N'étant pas familier avec la gestion des incidents, une formation sera dispensée au SI afin que les techniciens se familiarisent avec les processus de prise en charge d'un incident, de sa déclaration jusqu'à sa résolution et qui consiste aux étapes suivantes :

- Réception de la déclaration d'incident.
- Intervention à distance ou sur site.
- Réparation/échange de la pièce défectueuse.
- Tests de bon fonctionnement.
- Fin de l'incident.

À noter que le remplacement de tout ou partie d'un équipement se déroulera dans le respect des normes environnementales et dans une démarche d'homogénéisation du matériel du parc informatique.

8.2.2 Serveur et réseau

Nous mettrons à disposition les outils de monitoring nécessaire à la supervision des équipements serveur et réseau (pour Centreon, voir partie 5.2).

En cas de dysfonctionnement ou de panne insurmontable, le SI pourra escalader l'incident en le déclarant auprès de notre hotline en ouvrant un ticket d'incident via le portail client de Trust-IT.

Si le niveau de criticité l'exige, l'incident sera escaladé vers une équipe spécialisée qui pourra apporter son expertise via un système de télémaintenance : nos techniciens prendront les commandes à distance via un tunnel chiffré pour intervenir sur les équipements critiques de l'entreprise pour des tâches telles que :

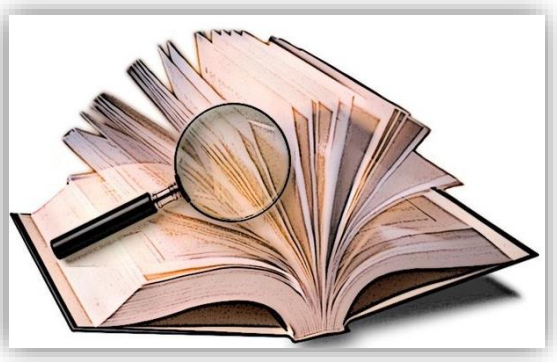
- ➢ Configuration des équipements réseaux.
- ➢ Restauration d'une sauvegarde si pertes de données.
- ➢ Configuration de services divers (applications, droits, d'accès, etc.).
- ➢ Installation/mise à jour de logiciels.
- ➢ Nettoyage (piratage, virus, malware, etc.).

Nos équipes se tiennent à votre entière disposition du lundi au vendredi, de 8h00 à 18h00 :

Hotline : 04 78 47 18 59

Mail : contact@trust-it.com

Base de connaissances



Il sera indispensable que les techniciens N1 et N2 de Modulhab participent à l'enrichissement d'une base de connaissance contenant :

- Une documentation technique.
- Des procédures d'intervention à appliquer dans le cadre d'incidents types.
- Procédures d'installation.

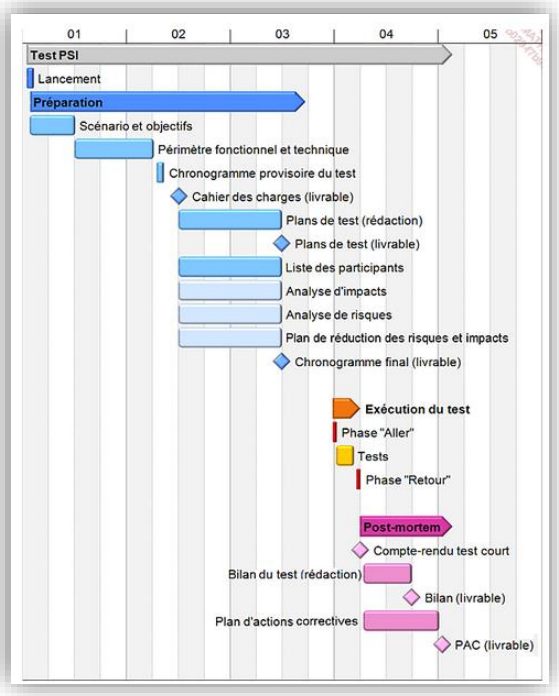
Cette documentation favorise la compréhension des défaillances et de leur origine en analysant leurs causes. Son maintien à jour optimisera les processus à appliquer pour traiter plus efficacement les incidents dans une démarche d'amélioration continue.

8.3 Maintenance du PSI

8.3.1 Planification des tests

La maintenance du Plan de Secours informatique s'effectuera une fois par an et fera l'objet d'une préparation au préalable qui peut prendre plusieurs mois selon la complexité de l'organisation.

Cette phase préparatoire donne lieu à l'élaboration d'un macroplanning qui contient l'ensemble des tâches à effectuer comme résumé dans le tableau ci-dessous :

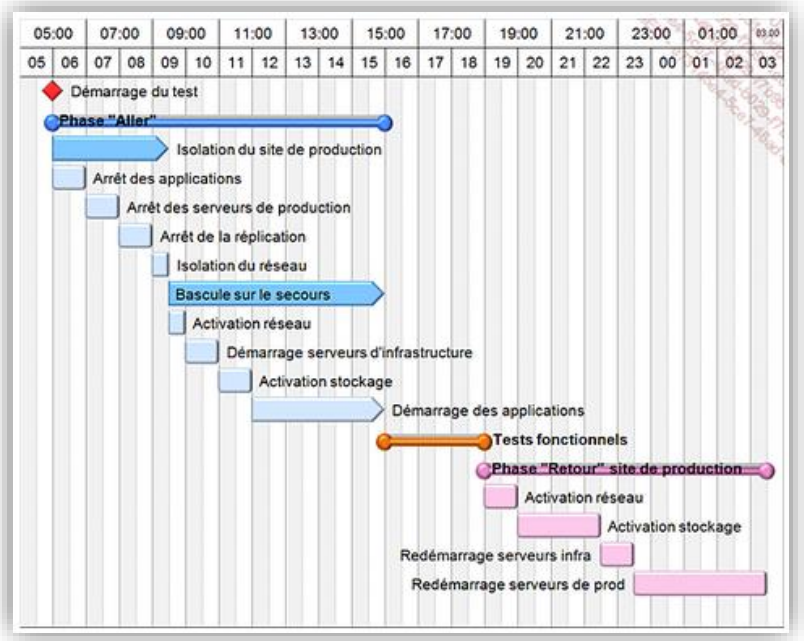


Le planning de test du PSI est un livrable que nous vous ferons parvenir un mois avant le lancement des tests. Les éléments les plus importants sont les suivants :

- Scénario : le type de sinistre simulé (panne électrique, perte d'un local serveur, etc.).
- Le périmètre fonctionnel et technique : Serveurs ou/et réseaux ; la liste des applications basculées sur le site de secours.
- Liste des participants : le service informatique ; le(s) service(s) impliqué(s) ; Trust-IT.
- Analyse d'impacts : Il s'agit d'identifier les impacts la simulation du sinistre sur les métiers et les utilisateurs.
- Analyse de risques : Il s'agit des risques d'incidents qui peuvent survenir lors de l'exécution du test (problème de redémarrage du système d'information, risques de panne matérielle, erreurs humaines, etc.).
- Exécution du test : peut s'étaler sur une journée entière
- Bilan du test (« Post-mortem ») : livrable
- PAC (« Plan d'Actions Correctives » : livrable

8.3.2 Phase de test

Le test du PSI donne lieu à la rédaction d'un cahier des charges qui fait partie des livrables de cette opération de maintenance. Ce dernier décrit l'enchainement des opérations réalisées pour simuler un sinistre jusqu'à la reprise d'activité au moyen d'un chronogramme.



Exemple de phase de test (source : (source : Plan de Continuité d'Activité, ENI édition)

Au travers d'une trame horaire, ce dernier comporte les phases suivantes :

- Phase « aller », isolation du local 1 :
  - Arrêt du serveur maître.
  - Bascule sur le serveur de secours (local 2).
  - Démarrage du serveur esclave en serveur maître.
- Phase intermédiaire :
  - Démarrage des applications.
  - Tests fonctionnels.
- Phase « retour » :
  - Réactivation du serveur du local 1 qui redevient maître.
  - Redémarrage du serveur et de ses applications.

Comme vu dans la partie précédente, la fin de cette phase de test donne lieu à la rédaction d'un bilan du test et d'un **PAC** (« Plan d'Action Corrective ») qui constituent les deux livrables à fournir à l'entreprise en guise de procès-verbal attestant de la fin des opérations de tests.

9. PRESTATIONS COMMERCIALES ET CALENDRIER PRÉVISIONNEL

9.1 Planification du déploiement

9.1.1 Déploiement et migration

Étant bien certain qu'il est irréaliste de renouveler en une fois tous les équipements de votre parc informatique, le déploiement des équipements doit se dérouler en considérant les critères suivants :

- Le niveau de criticité des équipements à remplacer qui indique le caractère urgent d'un remplacement.
- La disponibilité des différents services métiers.
- Les délais de livraisons de nos fournisseurs.
- Le budget alloué par période de déploiement.

En prenant en considération ces paramètres, les priorités seront les suivantes selon le niveau de criticité :

- Déploiement des serveurs en parallèle des anciens jusqu'au remplacement progressif de ces derniers.
- Migration systèmes (annuaire AD, applications métier, etc.).
- Masterisation et déploiement des premiers postes informatiques.
- Déploiement des équipements réseaux.

Nous allons vous fournir ici le calendrier prévisionnel de déploiement qui pourra faire l'objet d'ajustement ou de rectifications en concertation avec votre Direction.

Le coût d'une intervention d'un jour s'élève à 730 HT.

Préparation des deux serveurs	**Intervention**	**Durée**	**Coût (€ HT)**
	▪ Paramétrage (RAID, installation VM, installation physique ▪ Installation onduleur ▪ Sécurisation des salles serveurs	1 jour	730
	▪ Configuration et administration (configuration OS, MAJ, etc. ▪ Configuration réseau ▪ Test de la redondance	2 jours	1460
	TOTAL	3 jours	**2190 €**

Migration et configuration système	**Intervention**	**Durée**	**Coût (€ HT)**
	▪ Migration de la base d'annuaire ▪ Mise en veille des anciens serveurs et bascule sur les nouveaux ▪ Phase de tests ▪ Configuration antivirus	2 jours	1460
	TOTAL	2 jours	**1460 €**

Installation des routeurs et switchs	Intervention	Durée	Coût (€ HT)
	▪ Paramétrage	1 jour	730
	▪ Installation ▪ Phase de test ▪ Formation	1 jour	730
	TOTAL	2 jours	**1460 €**

Déploiement des postes (par 50)	Intervention	Durée	Coût (€ HT)
	▪ Installation des ordinateurs. ▪ Configuration réseau ▪ Préparation d'un master. ▪ Déploiement des licences ▪ Installation des logiciels métiers spécifiques.	3 jours	1460
	TOTAL	3 jours	**2190 €**

A noter que le déploiement des postes se fera progressivement sur plusieurs services à la fois. L'objectif est de tester la stabilité des postes et le bon déroulement des processus mis en place.

Nous prévoyons 4 sessions de déploiement de 50 postes par trimestre pour les 194 postes informatiques de la société Modulhab. Pour le déploiement, se rapporte à l'annexe 7)

9.1.2 Prestation PSI

Pour rappel, les phases de test du PSI sont les suivantes

- Étude : 4 mois
- Réalisation : 4 mois
- Tests et validation : 2 mois
- Mise en production : 1 mois

En prenant en compte l'ensemble du temps consacré à la réflexion, la préparation et la mise en œuvre du PSI avec l'implication respective des différents acteurs (experts techniques, techniciens, temps passé avec les services de votre Société), le coût total de la prestation s'élève à **29050 €** (ceci comprend aussi les heures de formation dispensées à l'équipe chargée de comprendre l'infrastructure sur place.

La phase finale du PSI correspond à la mise en production définitive des serveurs redondés.

Total des prestations sur toutes la phase d'installation : **42920 €** (HT)

9.1.3 Option phase de test PRI

Cette dernière se déroule sur 18h pour simuler les conséquences d'une bascule et la reprise d'activité informatique suite à l'arrêt d'un serveur.

Il est conseillé d'effectuer cette vérification une fois par an pour éprouver la robustesse de votre infrastructure. Coût total **4750 € HT**.

9.2 Proposition commerciale et synthèse des coûts

9.2.1 Devis matériel

Trust-IT
59 rue Denuzière
69002 LYON
Tél. : 04 78 47 18 59
Mail : contact@trust-it.com

DEVIS n°18309M
Date : 09/03/2018

Société Modulhab
13 rue Jean Grolier
69007 LYON

Date : 09/03/2018
N° de client : 3458H

Objet : Devis matériel

Produits	*Quantité*	*Prix unitaire (HT)*	*Total (HT)*
Routeur Cisco 2901	2	1814,40	3628,80
Switch Cisco Catalyst 2960L-8PS-LL-8 ports	3	392,75	1178,26
Switch Cisco Catalyst 2960L-48PS-LL-48 ports	6	1648,91	9893,47
Serveur Dell PowerEdge R440	2	9212,99	18425,99
SSD (spare)	4	962,28	3849,12
HDD (spare)	4	511,92	2047,68
ThinkPad T470p (pc portable)	57	1140,39	65002,44
ThinkCentre M710q (pc fixe)	119	588,06	69979,14
ThinkStation P520c (Station de travail)	18	1388,34	24990,12
Station d'accueil Lenovo	40	188,10	7524,14
Onduleur Eaton 5PX 1500i RT2U	2	755,95	1511,89
Détecteur de fumée	2	21,49	42,98
Extincteur CO2	2	64,80	129,60
		TOTAL (HT)	208203,63 €

Les quantités peuvent fluctuer en fonction de la disponibilité des produits chez nos fournisseurs.

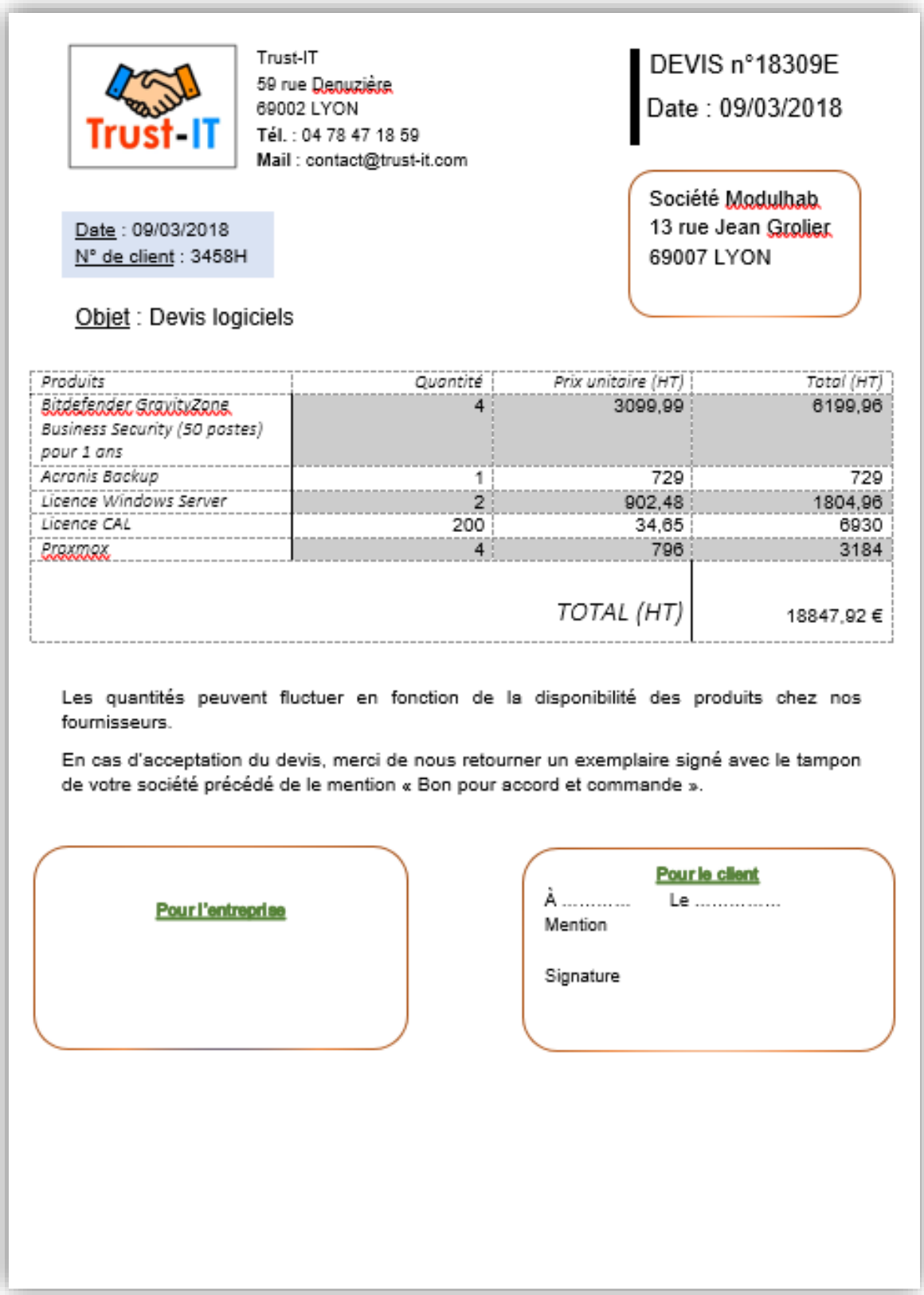
En cas d'acceptation du devis, merci de nous retourner un exemplaire signé avec le tampon de votre société précédé de le mention « Bon pour accord et commande ».

Pour l'entreprise

Pour le client
À ..... Le .....
Mention

Signature

9.2.2 Devis logiciels



Trust-IT
59 rue Denuzière
69002 LYON
Tél. : 04 78 47 18 59
Mail : contact@trust-it.com

DEVIS n°18309E
Date : 09/03/2018

Société Modulhab
13 rue Jean Grolier
69007 LYON

Date : 09/03/2018
N° de client : 3458H

Objet : Devis logiciels

Produits	*Quantité*	*Prix unitaire (HT)*	*Total (HT)*
Bitdefender GravityZone Business Security (50 postes) pour 1 ans	4	3099,99	6199,96
Acronis Backup	1	729	729
Licence Windows Server	2	902,48	1804,96
Licence CAL	200	34,65	6930
Proxmox	4	796	3184
		TOTAL (HT)	18847,92 €

Les quantités peuvent fluctuer en fonction de la disponibilité des produits chez nos fournisseurs.

En cas d'acceptation du devis, merci de nous retourner un exemplaire signé avec le tampon de votre société précédé de le mention « Bon pour accord et commande ».

Pour l'entreprise

Pour le client
À ..... Le .....
Mention

Signature

9.2.3 Devis des prestations

Trust-IT
59 rue Denuzière
69002 LYON
Tél. : 04 78 47 18 59
Mail : contact@trust-it.com

DEVIS n°18309P
Date : 09/03/2018

Société Modulhab
13 rue Jean Grolier
69007 LYON

Date : 09/03/2018
N° de client : 3458H

Objet : Devis prestations

Produits	*Quantité*	*Prix unitaire (HT)*	*Total (HT)*
Préparation des serveurs	1	2190	2190
Migration et configuration système	1	1460	1460
Installation routeurs/switch	1	1460	1460
Déploiement des postes (50 par trimestre)	4	2190	8760
Prestation PSI	1	29050	29050
		TOTAL (HT)	42920 €

Les quantités peuvent fluctuer en fonction de la disponibilité des produits chez nos fournisseurs.

En cas d'acceptation du devis, merci de nous retourner un exemplaire signé avec le tampon de votre société précédé de le mention « Bon pour accord et commande ».

Pour l'entreprise

Pour le client
À ..... Le .....
Mention

Signature

9.2.4 Devis total

Nous présentons ici l'ensemble des devis proposés avec leurs options possibles :

Devis	Coûts € (HT)	Statut de l'offre
Matériel	208203,63	Offre de base
Logiciel	18847,92	
Prestation	42920	
Total	269970,63 €	
Formation GLPI (2 jours)	1950	Offre additionnelle
Test PRI annuel	4750	
Total	276670,63 €	

10. CONCLUSION

Au terme de cette étude, nous pouvons affirmer que notre solution prend en compte tous les points abordés dans le cahier des charges dont notamment :

- Proposition d'une solution de gestion de parc révolutionnant complètement les pratiques anciennes qui engendraient des pertes d'exploitation.
- Simplification de la gestion du parc grâce à son homogénéisation progressive.
- Établissement d'un plan de maintenance de toute l'infrastructure.
- Regain de confiance certain auprès des utilisateurs par l'établissement de nouvelles pratiques.
- Consolidation de l'infrastructure par l'établissement d'un PCI et PRI prévoyant notamment la continuité d'activité en cas de sinistre et la sauvegarde régulière des données.
- Une réelle prise en compte de vos besoins et des secteurs critiques de Modulhab
- Le respect des normes environnementales dans le choix des fournisseurs.

Le budget initial que Modulhab souhaitait consacrer au renouveau du parc était de 200000 €. Ces frais recouvrent globalement le renouvellement complet du parc mais, l'ensemble de notre prestation s'élève à près de 270000 euros.

Cependant, ayant opté pour un renouvellement progressif du parc avec un rythme trimestriel, les dépenses peuvent s'échelonner dans le temps avec la possibilité d'adapter le calendrier de mise en production en fonction de votre budget.

Mieux, la plupart des équipements étant garantis sur 5 ans et en prenant en considération que les pertes d'exploitation engendraient une perte de 92500 euros par an, le retour sur investissement calculé sur la période de garantie s'élève à plus de 70%[1], prouvant que cette stratégie d'investissement est viable à l'échelle de l'avenir.

En sélectionnant la solution proposée par Trust-IT, vous opterez pour un parc neuf, garantie sur une longue durée, avec l'assurance d'appréhender plus sereinement l'évolution de votre système d'information tout en vous reconcentrant sur votre cœur de métier.

[1] 92500 € (perte d'exploitation annuelle) x 5 ans = 462500, ce qui donne 462500-270000/270000 = 0.71.

11. GLOSSAIRE

ANSSI, « Agence Nationale de la Sécurité des Systèmes Informatiques ». Ce service à compétence national est rattaché au SGDSN (« Secrétaire Général de la Défense et de la Sécurité Nationale »). Il publie des méthodes, des guides et tout en ensemble de préconisations à l'attention des organisations et entreprises des secteurs public et privé afin de promouvoir les bonnes pratiques à adopter afin de gérer efficacement la sécurité des systèmes d'information.

CNIL, « Commission Nationale de l'Informatique et des Libertés ». Il s'agit d'une autorité administrative indépendant française dont la mission consiste à assurer une veille juridique et un contrôle sur l'usage de l'informatique afin de protéger les droits et la vie privée des citoyens sur internet. Elle est automatiquement consultée par le gouvernement lorsque des mesures sont proposées mais son avis demeure consultatif.

BIA, « *Business Impact Analysis* ». Le BIA est une analyse d'impacts de métiers qui pour objectif d'étudier le fonctionnement d'une entreprise et d'évaluer notamment le niveau de criticité des différents métiers et les conséquences de leur interruption. Cette étude permet d'exprimer la Durée d'Interruption Maximale Admissible (***DIMA***) pour chaque service.

Cahier des charges. Le CDC est un document rédigé par un client et dans lequel ce dernier formule son besoin au moyen de plusieurs fonctions qui précisent les services qui seront rendus par un produit/service tout en se conformant aux contraintes de son environnement. Ce document est souvent émis lors d'un appel d'offres par un client et doit être respecté par la société qui sera retenue pour apporter des solutions au cahier des charges.

DIMA, « Durée d'Interruption Maximale Admissible ». Cette donnée évalue la durée pendant laquelle l'indisponibilité des applications n'est pas jugée suffisamment préjudiciable à l'entreprise.

Haute disponibilité. Ensemble des moyens mis en œuvre pour rendre un service disponible à un taux proche de 100% lors d'une panne matérielle.

Incident. Appliqué au domaine de l'informatique, un incident correspond à l'interruption non planifiée partielle ou totale d'un service informatique. On parle d'incident majeur lorsque le degré d'impact est le plus haut. On parlera alors de situation bloquante pour l'utilisateur ou le service impacté.

ITSM, « *Information Technology Service Management* ». Appelée en français « Gestion des services informatiques » qui correspond à une approche de la gestion des systèmes d'information axée sur des processus dans le cadre de la gestion des

incidents. Ces processus sont des activités combinant des ressources et des capacités organisationnelles. Cette démarche fournit de la valeur aux clients/utilisateur sous la forme de services.

ITIL, « *Information Technology Infrastructure Librairy* ». Il s'agit d'une documentation rassemblant l'ensemble des bonnes pratiques à adopter dans le management du système d'information. Elle s'adresse à des organisations informatiques qui délivrent des services à leurs utilisateurs. Ces pratiques se composent de processus applicables dans divers domaines tels que la gestion des incidents, le support utilisateurs (« Service Desk »), la gestion des configurations, etc. Depuis 2007, ITIL a évolué dans sa version V3 et met l'accès sur la maîtrise des cycles de vie des services.

Norme environnementale D3E (ou **DEEE**). Cette norme définie dans le cadre de l'Union européenne, réglemente la gestion des DEEE (« Déchets d'Équipements Électriques et Électroniques ») qui comportent des risques sanitaires et environnementaux (directives 2002/95/CE et 2002/96/CE). Elle a ainsi engendré la mise en place d'une filière de collecte et de gestion de ces déchets opérationnelle depuis le 22 juillet 2005.

Parc informatique. Un parc comprend l'ensemble des équipements matériels (serveurs, ordinateurs, etc.), réseaux (routeurs, commutateurs, etc.) et logiciels utilisés au sein d'une société ou d'une organisation. Le parc est généralement sous la responsabilité d'un DSI qui organise sa gestion, son entretien et son évolution.

PDMA, « Perte de Données Maximale Admissible ». Cette donnée évalue la perte de données acceptable après reprise en cas de sinistre. Elle permet de fixer des objectifs de reprise et influe dans le choix de la technologie informatique qui permettra d'y parvenir.

PCA, « Plan de Continuité d'Activité ». Ce plan englobe l'ensemble des processus qui visent à assurer le fonctionnement en mode dégradé d'une société impactée par un sinistre majeur. Ainsi, la continuité de l'activité garantie la survie de l'entreprise durant cet évènement.

PRI, « Plan de Reprise Informatique ». Il s'agit d'un document décrivant l'ensemble des procédures à effectuer pour le redémarrage du système d'information lors de l'activation du secours (exemple, serveur redondé) suite à un sinistre. L'enchainement chronologiques de ces procédures est visible dans un macroplanning qui présente la chronologie globale du plan. Le PRI est un document livrable du PSI.

PSI, « Plan de Secours Informatique ». Il correspond à l'ensemble des dispositifs nécessaire à la reprise du système d'information lors d'un sinistre en mode dégradé. Il vise à conserver les données de l'entreprise et à assurer le rétablissement des activités en un temps limité.

RAID, « *Redondant Array of Independent Disk* ». Cette technique consiste à répartir des données sur plusieurs supports de stockage tels que des disques durs afin de prévenir la perte de données en cas de panne de l'un d'entre eux.

Sinistre majeur. Il se rapporte à tous les évènements pouvant mettre en péril la pérennité d'une société en affectant l'ensemble des bâtiments d'un site. Il s'oppose à un sinistre mineur qui impacte qu'une partie des bâtiments d'un site.

SNMP, « *Simple Network Management Protocol* ». SNMP est un protocole de communication qui permet de surveiller l'état et le fonctionnement des éléments actifs (routeur, switch, serveur, etc.) d'un réseau informatique. Les flux SNMP assure le dialogue entre le superviseur (console permettant d'exécuter des requêtes de gestion) et l'agent (programme présent sur l'interface des équipements) pour récolter des informations sur l'état des équipements à surveiller.

VLAN, « *Virtual LAN* ». Le VLAN est un réseau logique et indépendant basé sur le protocole 802.1Q et qui a pour but de séparer les flux afin d'optimiser la gestion du réseau tout en améliorant la sécurité.

VRRP, « *Virtual Router Redundancy Protocol* ». Ce protocole est utilisé dans les réseaux afin d'augmenter la disponibilité de la passerelle par défaut utilisée par les hôtes. La passerelle par défaut est une IP virtuelle référençant généralement un routeur maître et esclave afin d'assurer une continuité de service : en cas d'indisponibilité du premier, le routeur esclave devient maître.

WAN, « *Wide Area Network* ». WAN peut être traduit par réseau étendu en français et désigne un réseau informatique ou de télécommunication englobant une vaste zone géographique.

12. ANNEXES

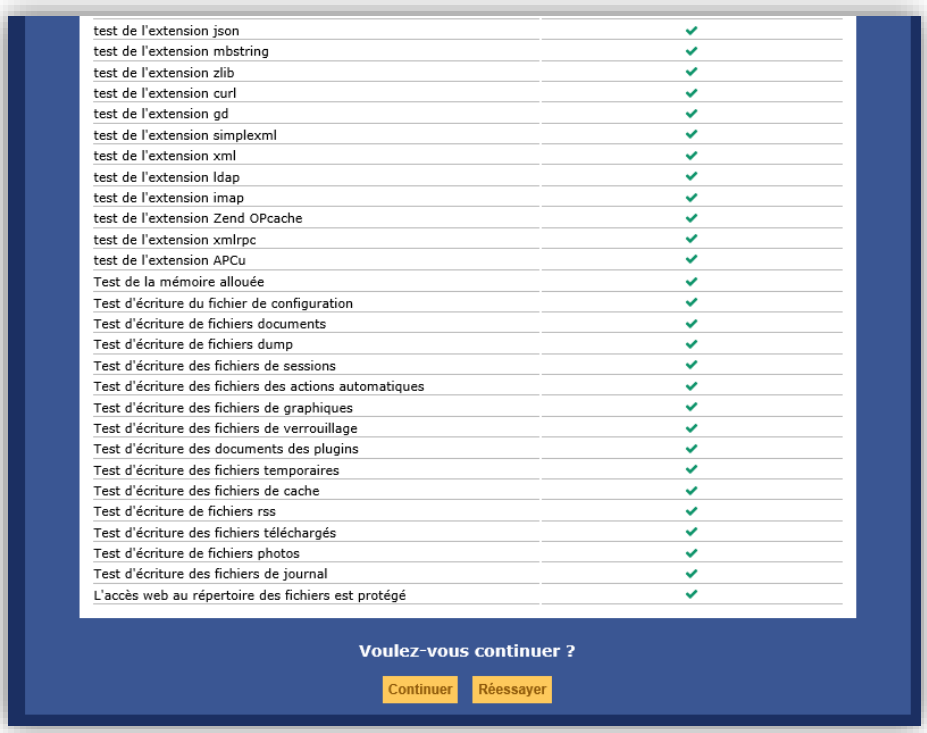
12.1 Annexe 1. Installation de GLPI/FusionInventory

Après avoir placé les fichiers d'installation de GLPI sur le serveur Apache, on se rend sur l'adresse du serveur par l'adresse http://localhost/glpi/ via le navigateur pour débuter l'installation.

- Sélectionner le langage souhaité :

- Lancement de l'installation :

- On peut voir ensuite que les fichiers de GLPI ont bien été installés :



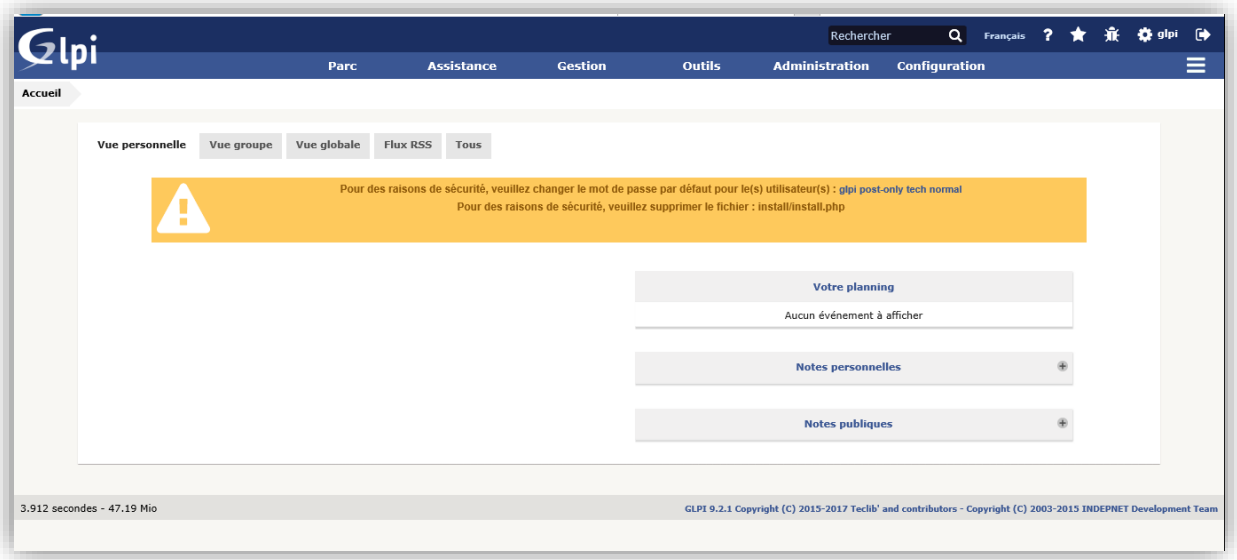
- Indiquer ensuite les paramètres et identifiants de la base de données :

- Créer une nouvelle base de données nommée « glpi » :

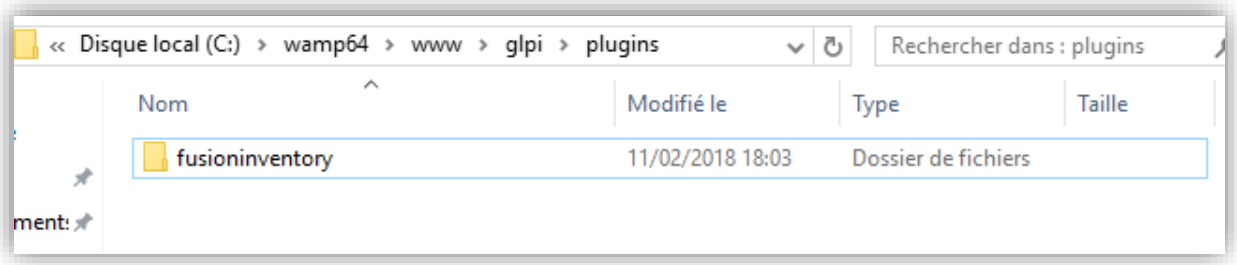
- La base de données a bien été créée :

- L'installation est terminée, les identifiants de connexion par défaut sont indiqués :

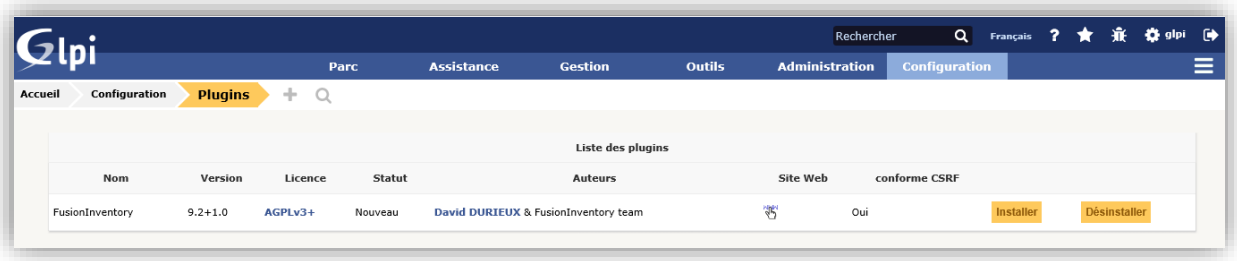
- L’accès au GLPI est opérationnel :



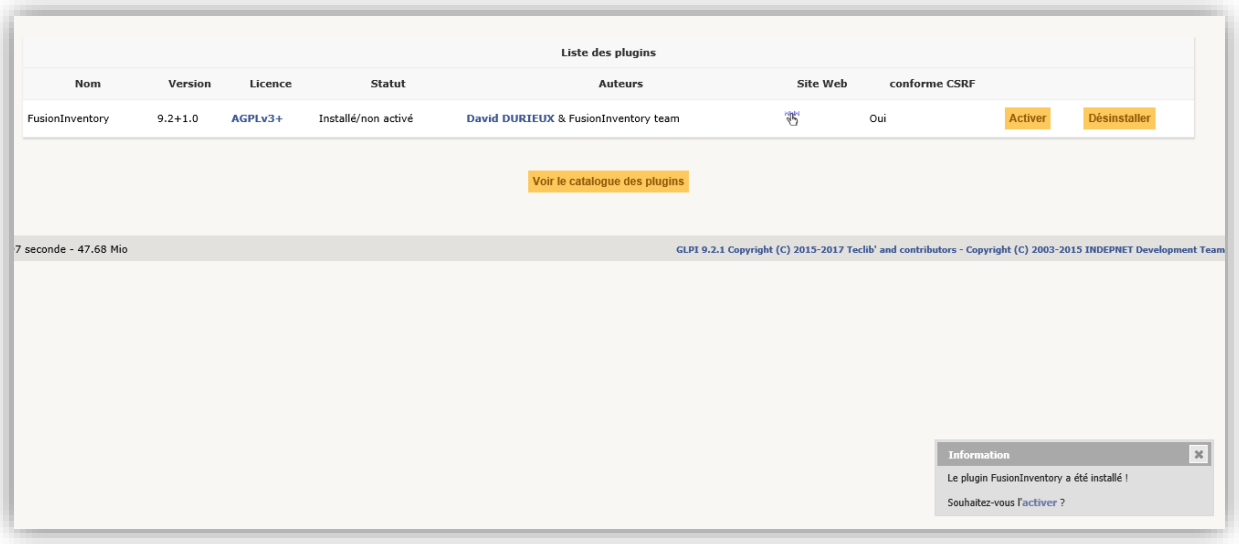
- On peut ensuite installer des plugins. Par exemple avec FusionInventory, on place le dossier d’installation dans le dossier « plugins » au niveau de l’installation du GLPI sur le serveur :



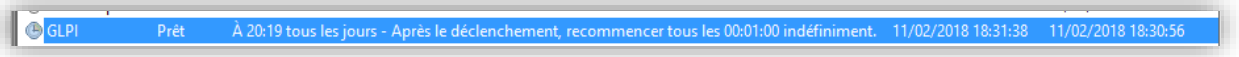
- Le plugin apparait ensuite dans l’onglet « configuration > plugins ». Cliquer sur « installer »

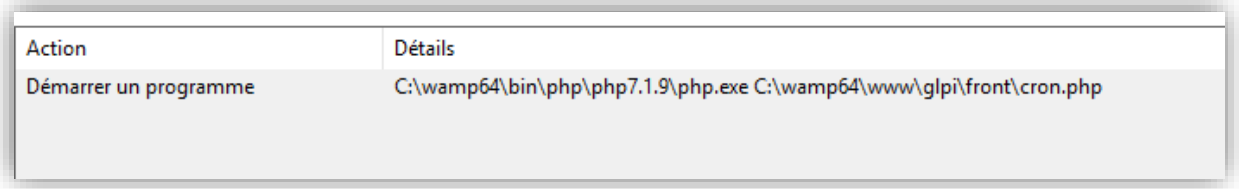


- Après l'installation du plugin, cliquer sur « activer » pour activer le plugin :



- Créer une tâche planifiée afin d'exécuter le « cron » de FusionInventory, nécessaire pour le bon fonctionnement de la découverte réseau :

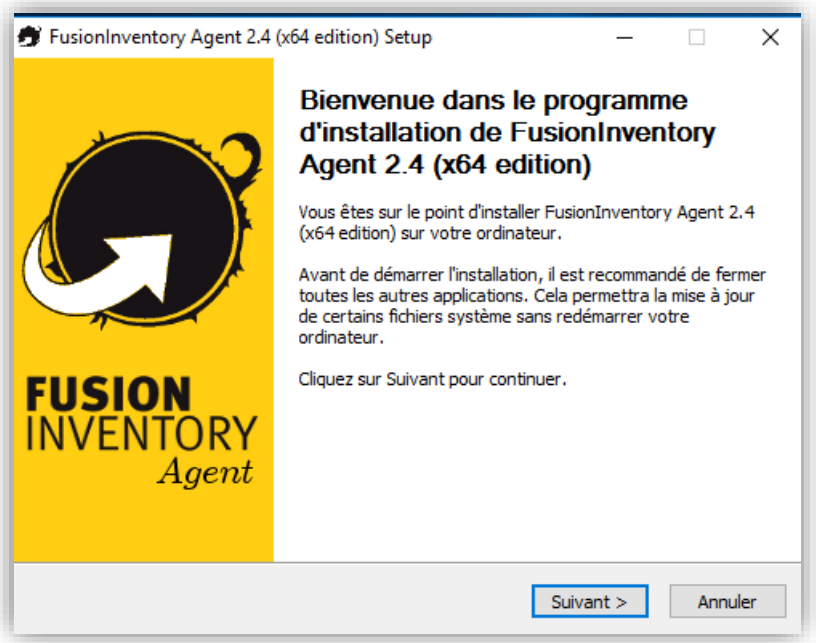




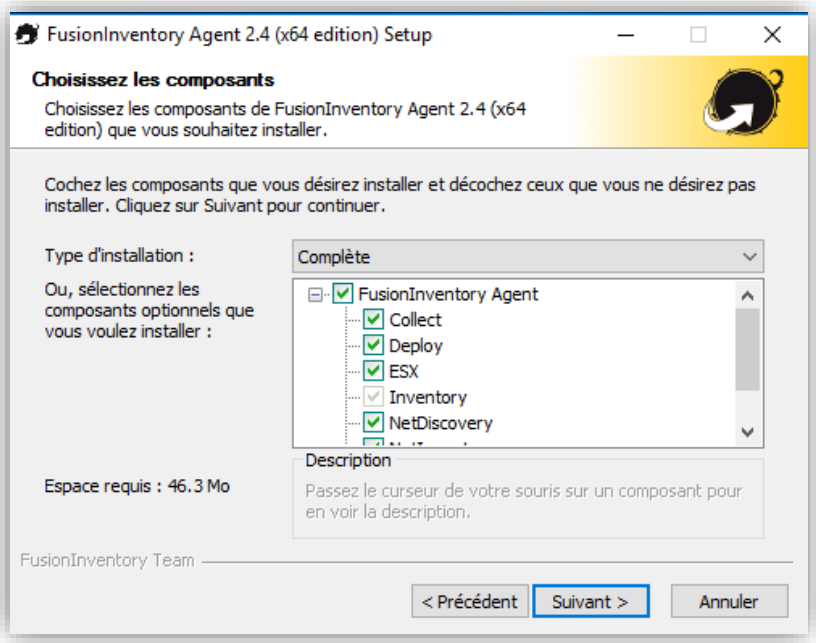
Installation d'un agent Fusion Inventory

L'installation de l'agent FusionInventory sur un poste est très rapide. Nous allons présenter ici une installation manuelle. Une installation dans un parc avec de multiples PC, et disposant d'un serveur Active Directory, se fera cependant par GPO avec l'utilisation d'un script VBS, qui est fourni sur le site de FusionInventory.

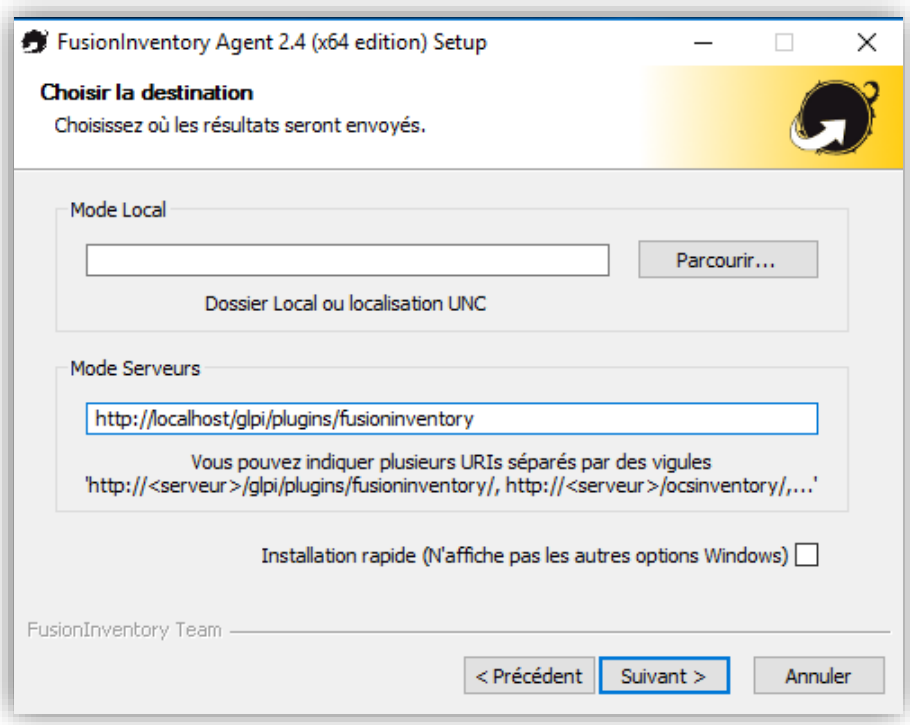
- Lancement de l'agent sur un poste Windows :



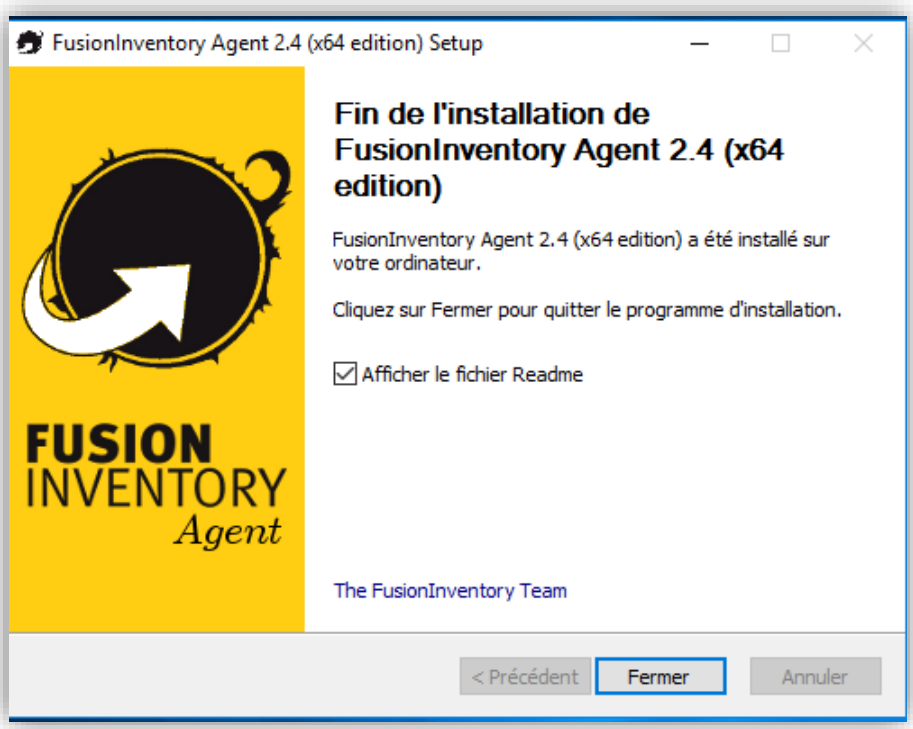
- Choisir les composants à installer :



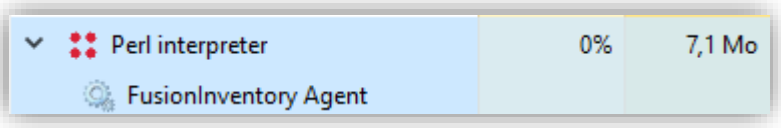
- Ajouter le chemin d’accès au plugin FusionInventory sur le serveur GLPI :



- L’installation est terminée :



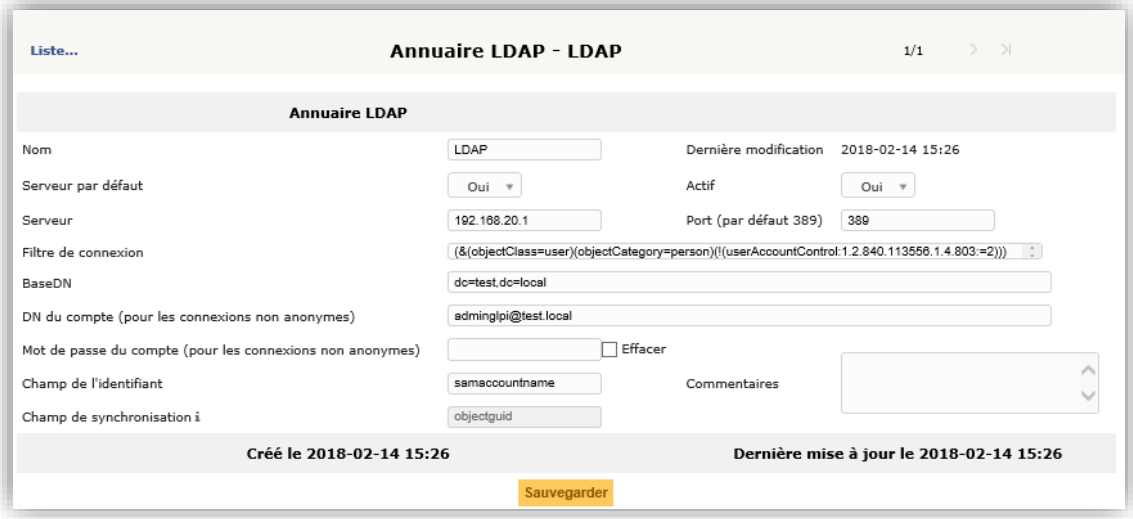
Le processus correspondant à l'agent Fusion Inventory apparait ensuite dans le gestionnaire des tâches :



Configuration LDAP pour GLPI

Pour lier l'Active Directory au GLPI et permettre aux utilisateurs de se connecter avec leurs identifiants d'ouverture de session, il faut mettre en place une liaison LDAP.

- Voici les paramètres à renseigner afin d'effectuer la connexion LDAP :



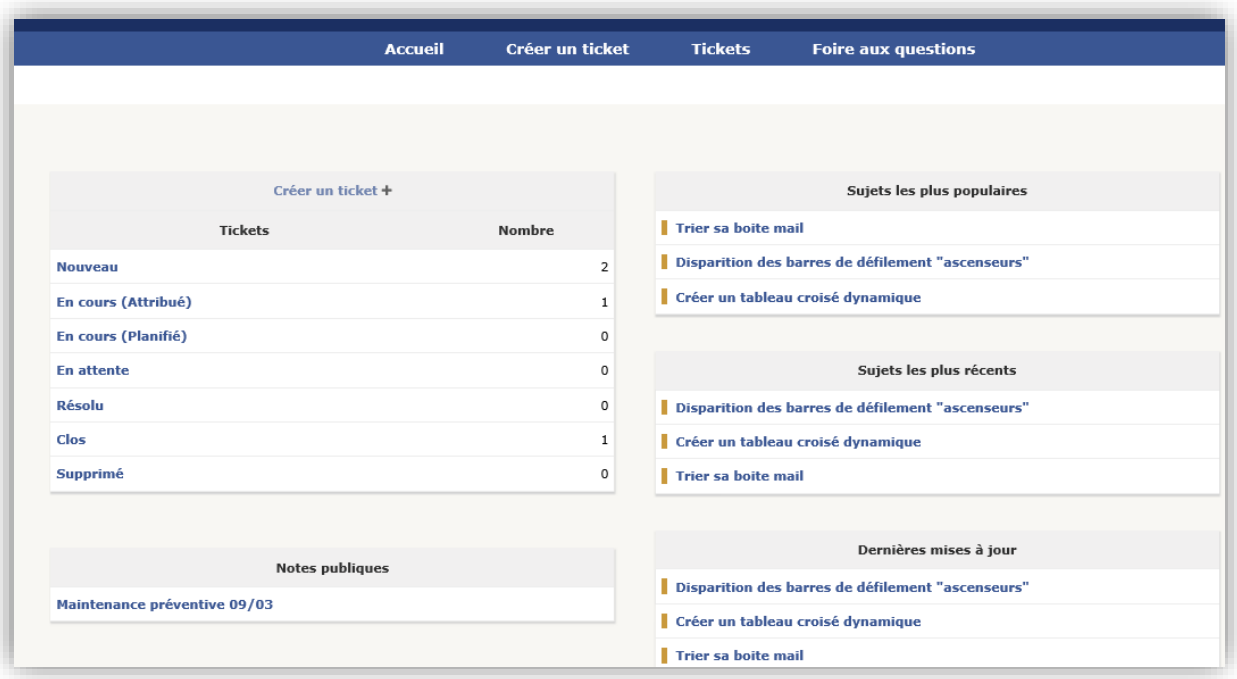
- On peut ensuite tester la connexion, puis importer les utilisateurs de l'Active Directory. Voici un exemple d'utilisateur importé :

12.2 Annexe 2. GLPI : description de l'interface utilisateur :

GLPI peut être intégré directement au sein d'un portail interne (intranet) ou l'utilisateur cliquera sur un bouton « support informatique » par exemple, afin de créer son ticket. Depuis l'interface de connexion, l'utilisateur devra renseigner son identifiant et son mot de passe (les mêmes que sa session Windows).

Sur l'accueil, l'utilisateur peut visualiser les différentes fonctionnalités telles que :

- Les tickets en cours créés par l'utilisateur
- Les notes publiques
- Tutoriels et articles issus de la base de connaissances (Foire aux questions)

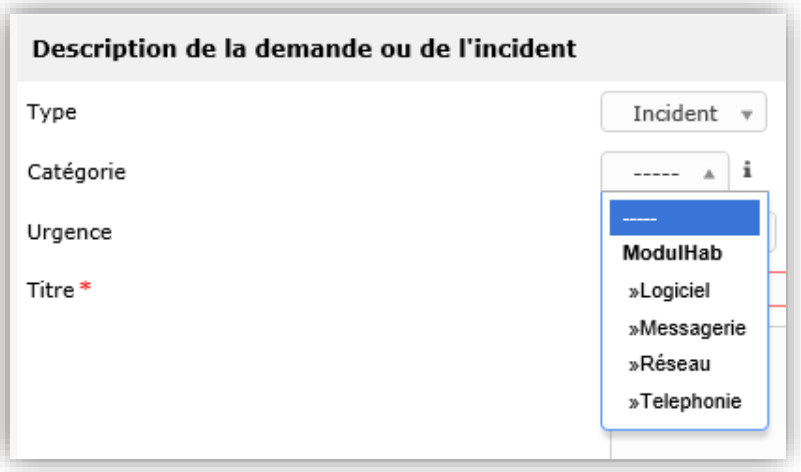


L'ensemble des tickets et leur statut sont explicitement visibles. C'est depuis cette interface qu'un nouveau ticket sera créé par l'utilisateur.

Création d'un nouveau ticket

L'interface a été épurée par rapport à la configuration de base en ne conservant que le strict nécessaire pour améliorer l'ergonomie de l'outil pour l'utilisateur.

- **Type** : ce champ permet de choisir s'il s'agit d'un incident ou d'une demande.
- **Catégorie** : On précise ici sur quoi porte le ticket (logiciel, téléphone, etc.). Ces catégories peuvent être généralistes (exemple : « logiciel ») ou bien plus précises (exemple : « Excel »). Il s'agit de ne pas avoir une quantité trop grande de choix possibles. Nous avons laissé ce choix comme non obligatoire, car nous estimons qu'il peut être rempli par le technicien, qui saura mieux qualifier le ticket que l'utilisateur.



Urgence : Définie par l'utilisateur selon l'impact de l'incident sur sa productivité. Cette dernière peut être requalifiée par le technicien si la nature de la demande n'est pas en adéquation avec le statut (exemple : demande d'un second écran : impact très faible). Si tout le service Administration Des Ventes ne peut plus passer d'appel téléphonique, l'urgence pourra être classée comme « très haute ».

- **Titre** et la **description** : Ces champs sont paramétrés comme obligatoires afin que le technicien ne perde pas de temps à remplir ces champs. Ceci habituera l'utilisateur à renseigner un titre court sans ajouter tout l'intitulé de sa demande dans le champ titre (ceci est fréquent…). Le but est d'inciter les utilisateurs à formuler leur besoin correctement en intégrant des bonnes pratiques.

Un **fichier** peut être ajouté en pièce jointe pour apporter des informations supplémentaires sur le dérangement rencontré.

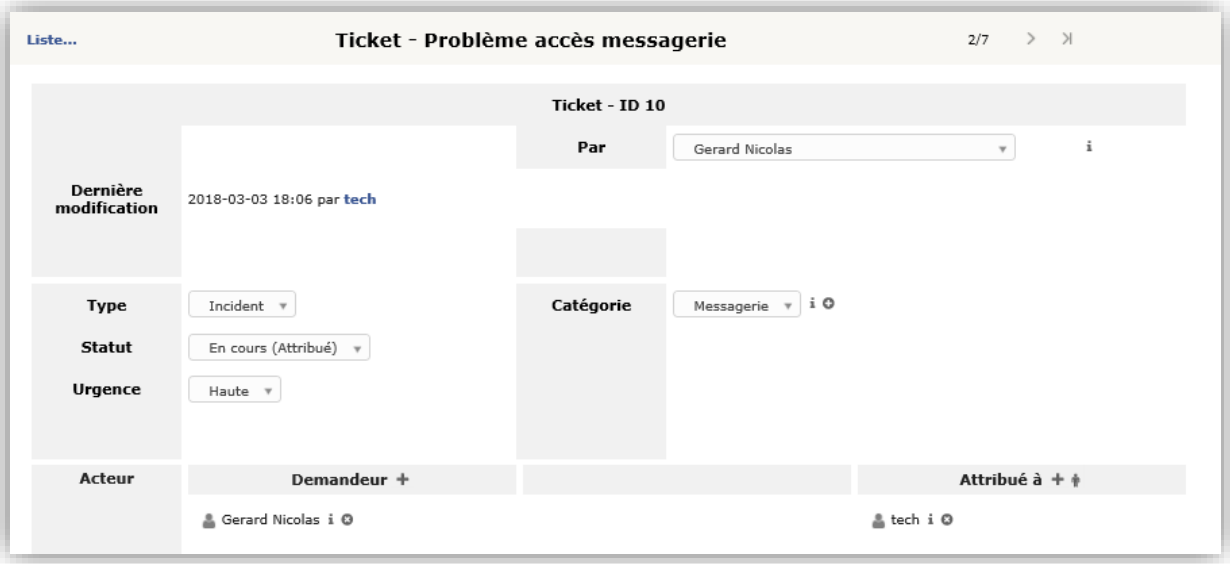
Consultation des tickets

Aperçu de l'interface de consultation des tickets créés (côté utilisateur) :

ID	Titre	Statut	Dernière modification	Date d'ouverture	Priorité	Demandeur - Demandeur	Attribué à - Technicien	Catégorie	Temps de résolution
10	Problème accès messagerie	En cours (Attribué)	2018-03-03 18:06	2018-03-03 18:01	Haute	Gerard Nicolas	tech	Messagerie	
6	Installation Office	En cours (Attribué)	2018-03-03 18:06	2018-03-03 10:44	Basse	Gerard Nicolas	tech	Logiciel	
4	écran HS	En cours (Attribué)	2018-02-28 21:34	2018-02-28 21:30	Haute	Gerard Nicolas	glpi		
ID	Titre	Statut	Dernière modification	Date d'ouverture	Priorité	Demandeur - Demandeur	Attribué à - Technicien	Catégorie	Temps de résolution

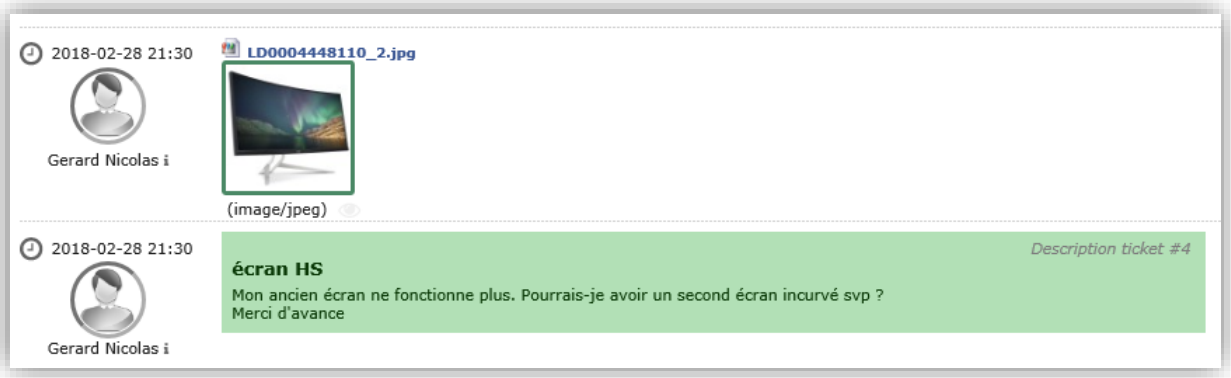
On retrouve les différents champs principaux associés au ticket, dont un champ qui est « rempli » automatiquement par GLPI, il s'agit de l'ID.

L'**ID** est l'identifiant unique du ticket dans la base de données. L'utilisateur peut éventuellement le fournir à un membre du service informatique (lors d'un appel téléphonique) pour que celui-ci retrouve le ticket plus rapidement.



En cliquant sur un ticket, l'utilisateur visualise les détails du ticket avec la mention du technicien en charge de la demande.

Un onglet « **traitement du ticket** » affiche le suivi du ticket dans un mode « conversation ». L'utilisateur peut ajouter un suivi ou un document et consulter les



Aperçu du traitement du ticket : description initiale et ajout d'une photo par l'utilisateur

réponses du technicien.

Cycle de vie d'un ticket

Voici les différents statuts d'un ticket, sur GLPI :

Un ticket est « **nouveau** » lorsqu'il vient d'être créé et n'est pas encore attribué à un technicien.

Un ticket est « **en cours (attribué)** » lorsqu'un technicien s'est attribué le ticket.

Un ticket est « **en cours (planifié)** » lorsqu'un technicien s'est attribué le ticket et a planifié une tâche visant à résoudre le problème.

Un ticket peut être mis « **en attente** » par le technicien, si celui-ci a posé une question à l'utilisateur et attend un retour, ou bien si l'intervention.

Un ticket est « **résolu** » lorsque le technicien a apporté une solution, qui est en attente d'acceptation par l'utilisateur.

Un ticket est « **clos** » lorsque la solution a été acceptée par l'utilisateur ou si le technicien décide de clore le ticket sans validation de l'utilisateur. Selon la configuration du service informatique, ce peut être également le responsable du service qui décide de la clôture du ticket.

Un ticket « **supprimé** » existe encore et est placé dans une « corbeille ». Il peut être supprimé définitivement (par une personne ayant les droits)

Ces différents statuts sont ceux préconisés par ITIL, qui se place du côté du « client » et non du technicien. Par exemple, le statut « En attente » ne doit normalement pas être utilisé si le technicien attend l'intervention d'un prestataire : le ticket doit rester en cours.

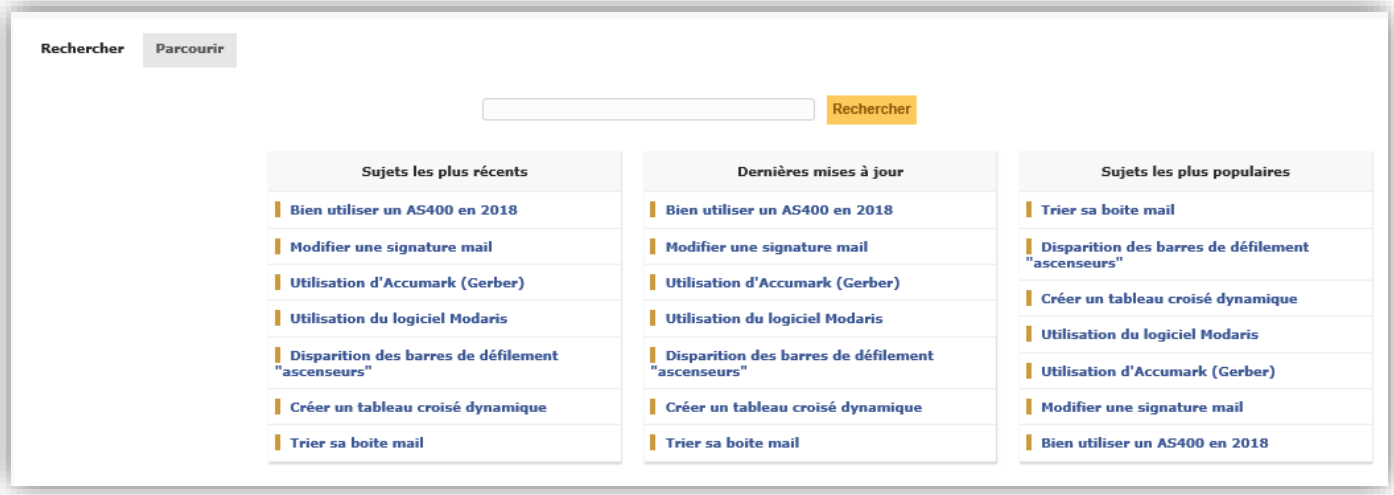
Notes publiques

Les notes publiques sont ajoutées par le service informatique. Les responsables de services peuvent avoir accès à la gestion de ces notes pour en ajouter afin d'apporter des informations importantes à l'ensemble de l'entreprise.

Exemple de note publique

Une visibilité peut être ajoutée à la note, afin de planifier sa disparition automatique. Un document peut également être ajouté à la note (par exemple pour donner des informations complémentaires).

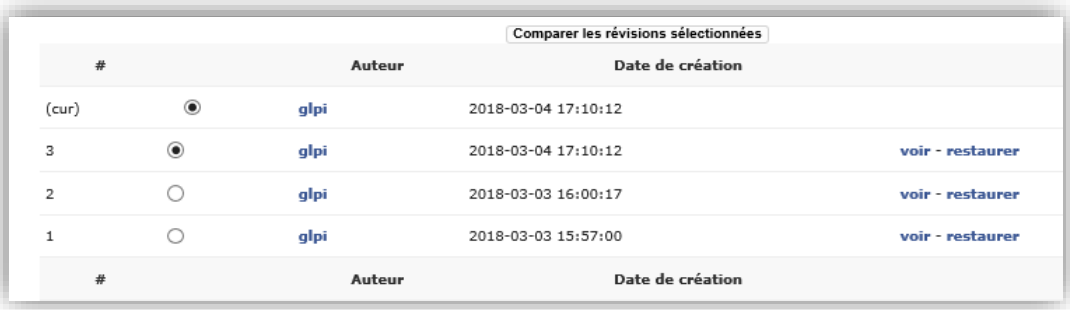
Foire aux questions



La **foire aux questions** permet de proposer des procédures (tutoriels) aux utilisateurs ou bien des solutions aux problèmes fréquemment rencontrés. Elle peut comporter par exemple de la documentation des différents logiciels et applications métiers

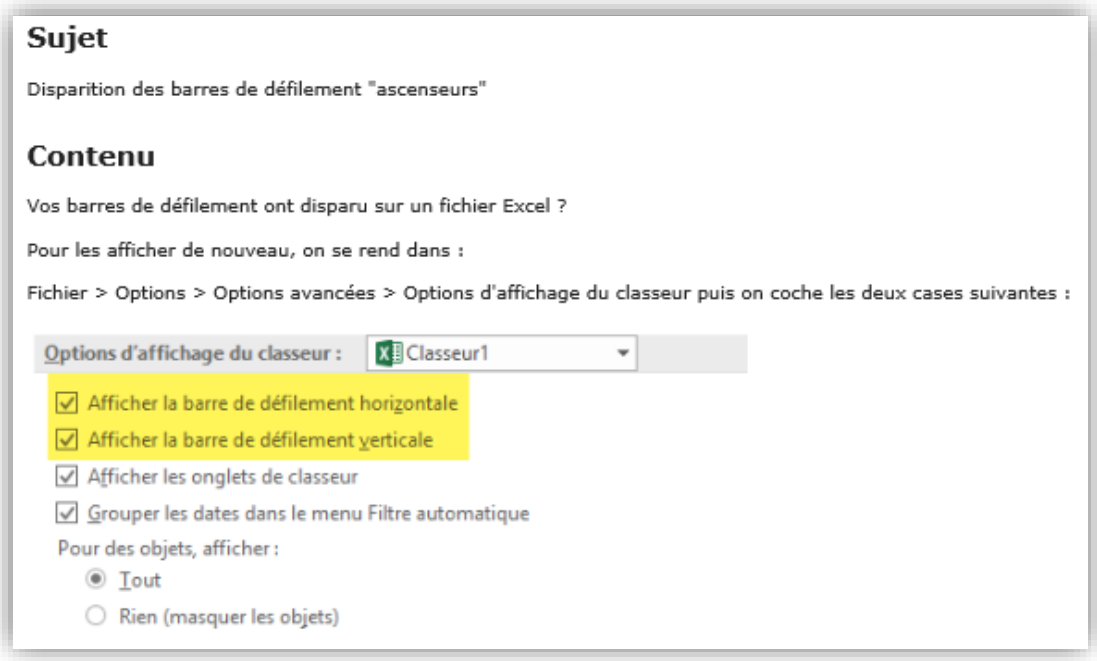
Le service informatique peut donc créer des articles (avec titres, contenus, images) et associant des documents tels qu'une documentation en PDF d'un fournisseur par exemple).

Des **révisions** permettent de voir l'état d'un article avant une modification, et éventuellement restaurer une version antérieure.



Aperçu des différentes révisions d'un article

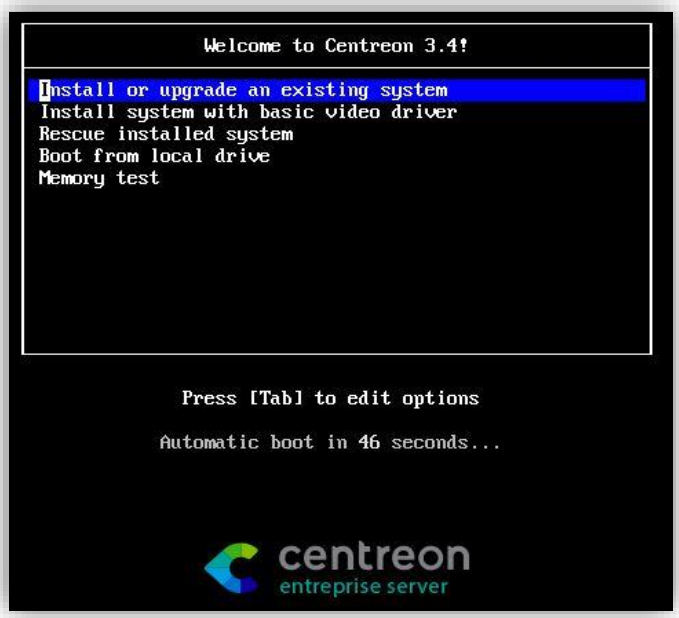
Exemple d'article visualisé par l'utilisateur :



12.3 Annexe 3. Installation de Centreon

Lancer d'ISO d'installation de Centreon Enterprise Server depuis une VM vierge puis choisir **Install or upgrade an existing system**

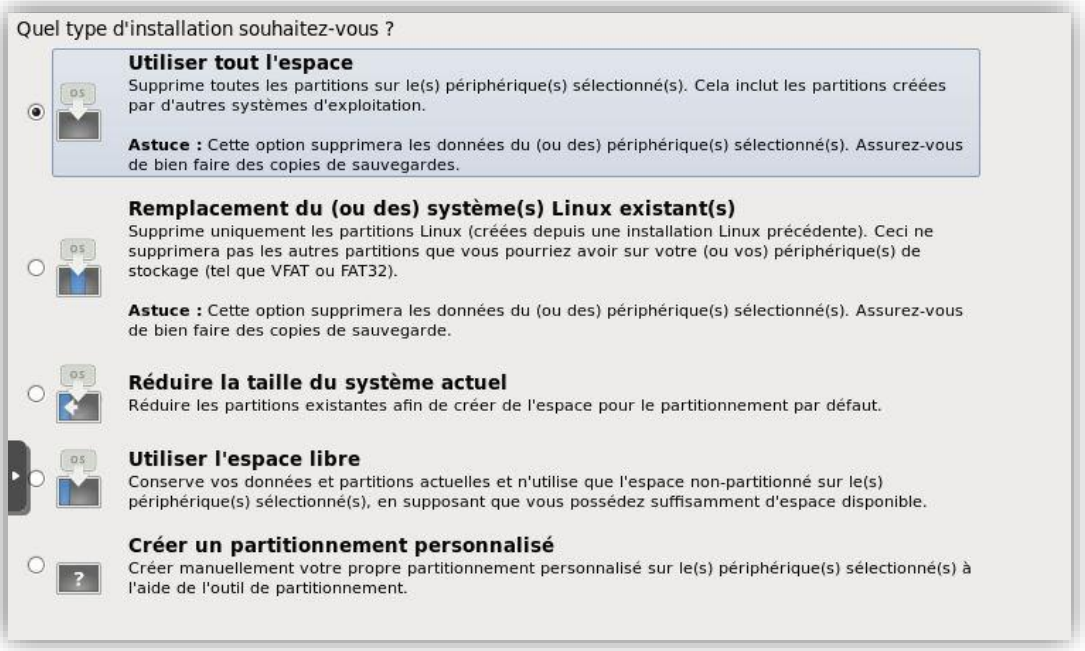
Sélectionner Skip pour procéder directement à l'installation :



La suite de l'installation est assez classique :

- Sélectionner la langue désirée (système et clavier)
- Choisir le type de périphérique désiré (en fonction de l'architecture en place).
- Choisir le nom de la machine (ici, « monitoring »).
- Sélectionner le bon fuseau horaire (Europe/Paris).
- Saisir un mot de passe « root » puis confirmer.

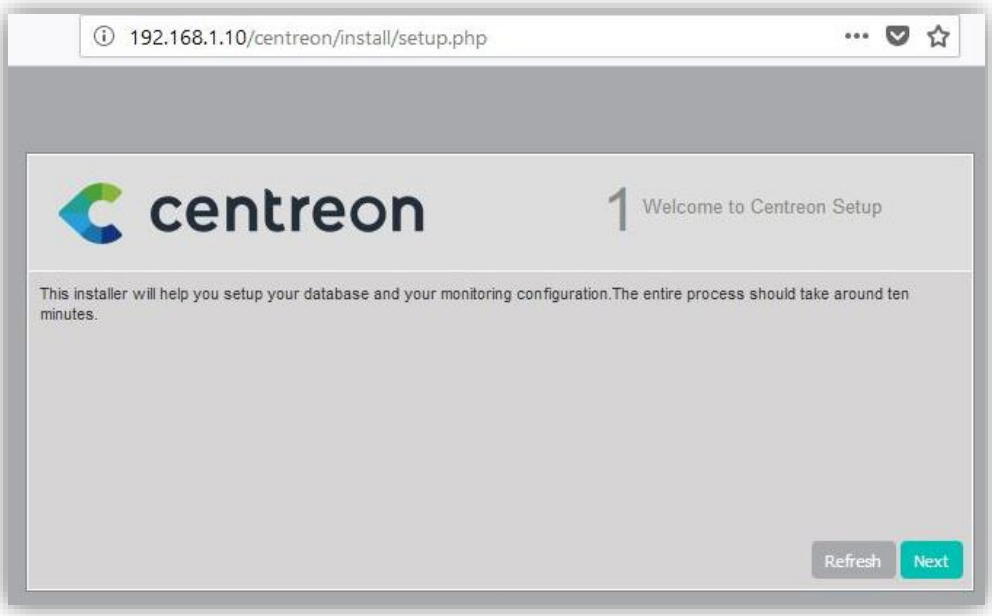
- Dans le choix du type d'installation, sélection « utiliser tout l'espace » :



- Sélectionner **Central server with database** pour installer le serveur de supervision avec sa base de données.

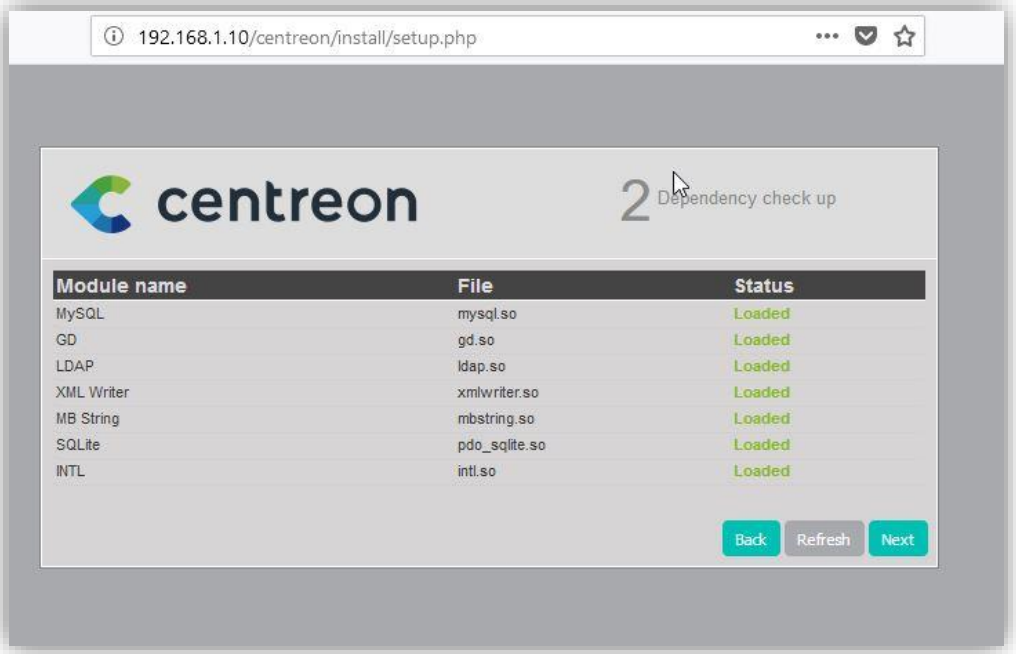
- Une fois l'installation terminée, se connecter sur l'interface web en renseignant l'adresse IP du serveur sous la forme **http://192.168.1.10/centreon** :

  Un assistant de configuration s'affiche. Cliquer sur suivant :

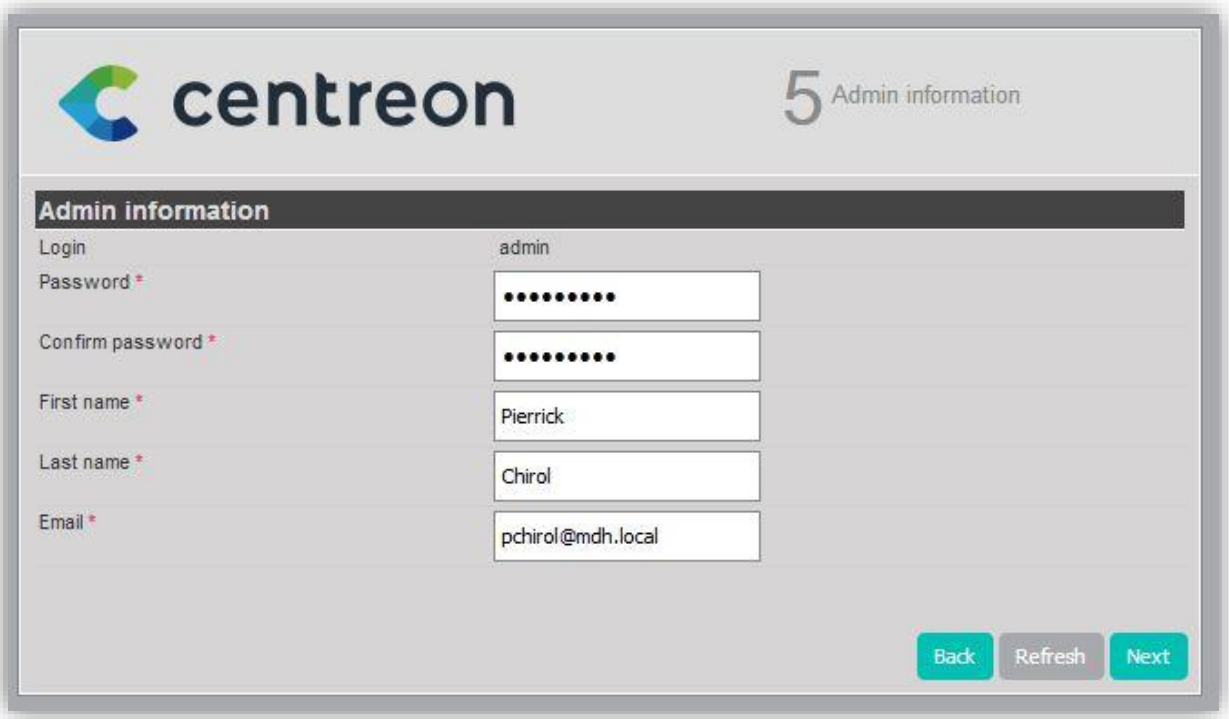


- L'étape suivante révèle une erreur sur la timezone qui n'est pas définie.
  Se rendre sur le host pour éditer le fichier **/etc/php.ini** dans la section [Date] :

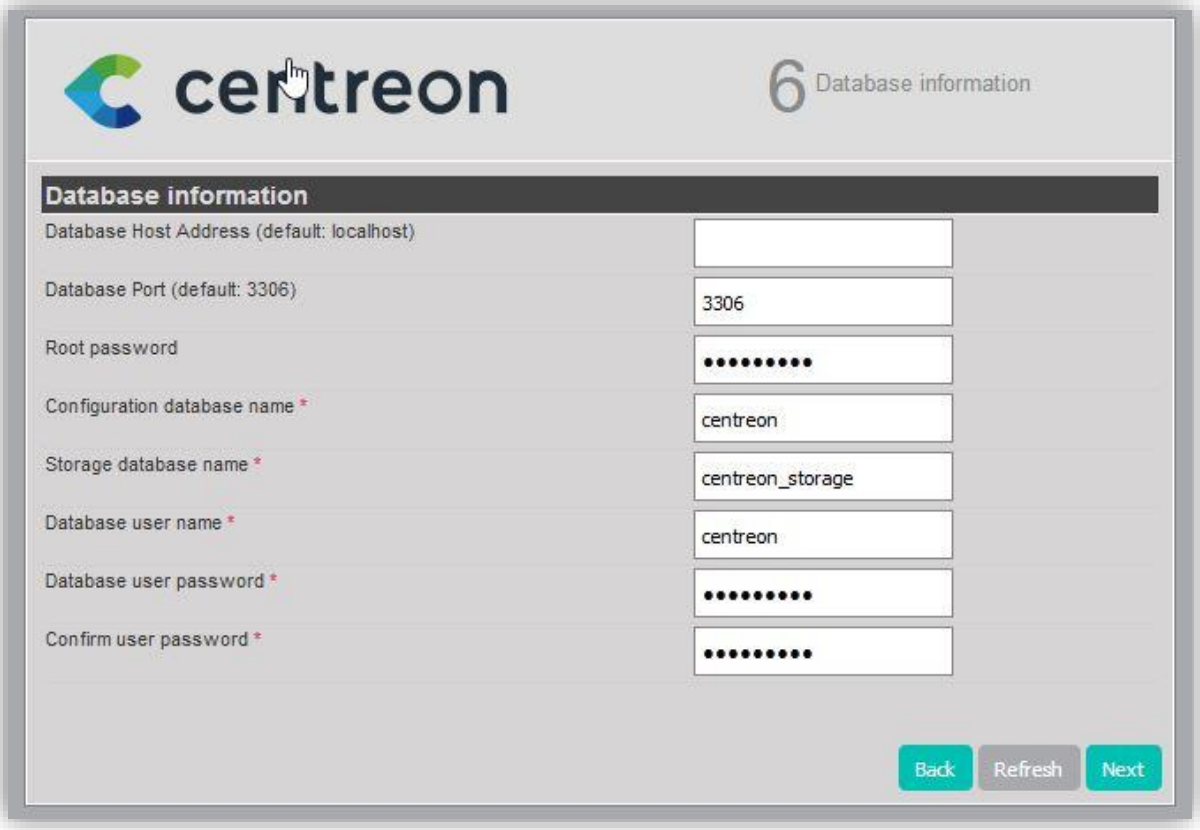
```
[Date]
; Defines the default timezone used by the date functions
; http://www.php.net/manual/en/datetime.configuration.php#ini.date.timezone
date.timezone = "Europe/Paris"
```



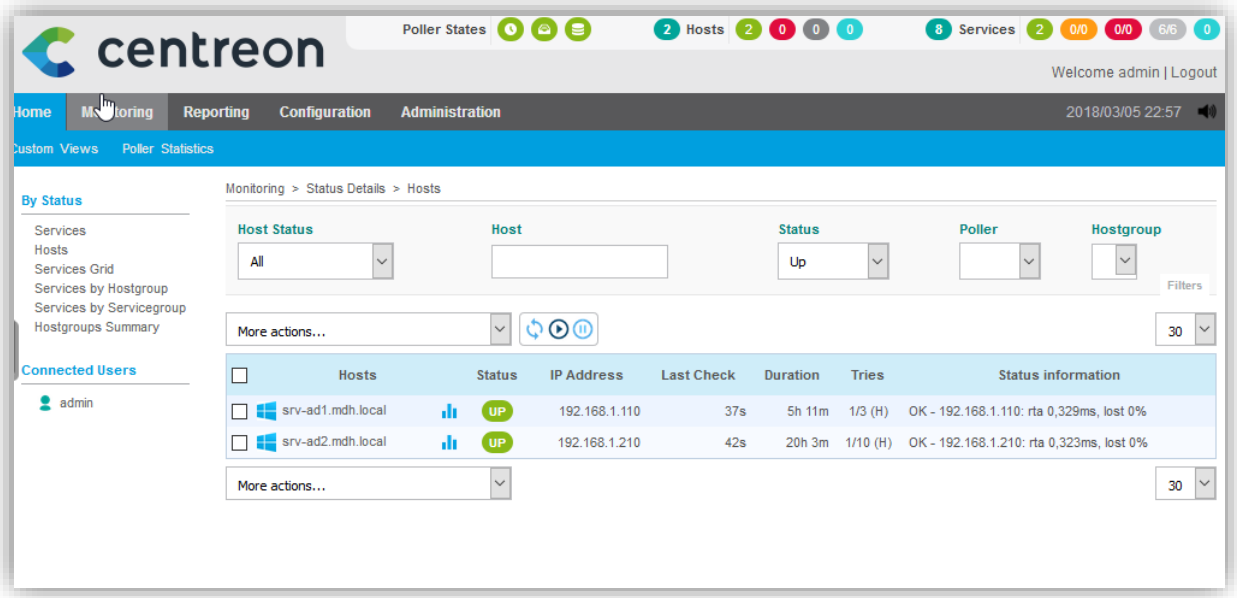
- Cliquer sur suivant au cours des deux prochaines étapes :
- Renseigner les identifiants permettant de se connecter à l'interface web :



- Renseigner le mot de passe de la base de données :



- Se logger une fois l'installation terminée :



12.4 Annexe 4. Normes et développement durable

GREEN IT : ModulHab est une société qui souhaite s'inscrire dans une démarche de développement durable par l'utilisation notamment de matériaux composites naturels pour ces constructions. Désireuse de véhiculer une image plus positive au regard de l'environnement, Modulhab souhaite développer une démarche de développement durable interne à l'entreprise, actuellement inexistante.

Alors que les enjeux environnementaux sont de plus en plus importants (préservation de la biodiversité, efficacité des ressources, économies d'énergie, réduction et valorisation des déchets, etc.), il devient important de mettre en place une démarche

RSE (« *Responsabilité Sociale des Entreprises* »). La RSE est « la responsabilité des entreprises vis-à-vis des effets qu'elles exercent sur la société » (Commission Européenne, 2011). Une démarche RSE efficace s'appuie sur des certifications, des normes et des préconisations diverses.

Normes ISO : Les normes ISO ne sont pas des obligations légales, elles reposent sur le volontariat. Elles donnent des avantages économiques pour les entreprises, notamment en améliorant l'image de marque et la compétitivité. On peut citer la norme ISO 26000, qui traite de la RSE en lien avec la responsabilité environnementale des entreprises.

L'ISO 26000 n'est pas une certification mais une norme de recommandations qui fournis un cadre de réflexion et d'action à l'image d'un guide. Sa mise en œuvre peut cependant conduire à une certification ISO 9001 (management de la qualité) ou ISO 14001 (management environnemental). La norme ISO 14001 est destinée aux entreprises souhaitant s'inscrire dans une maîtrise des impacts environnementaux, et disposer d'un système permettant de s'améliorer sur la question environnementale.

Cycle de vie : Lorsqu'un équipement a atteint sa « fin de vie » en entreprise, cela signifie très rarement que l'objet n'est plus en état de marche, mais simplement qu'il est devenu trop lent, plus assez performant au regard des avancées technologiques et numériques. Un équipement informatique trop lent a un impact direct sur la performance des employés ce qui génère un impact financier pour l'entreprise.

Plus de la moitié des directeurs informatiques renouvelle son parc tous les 3-4 ans (étude du site Internet Spiceworks auprès de 353 responsables informatique, 2016). En effet, la plupart des garanties constructeurs ne vont pas au-delà de 3 ans. Les plus grosses entreprises renouvellent plus souvent leur parc (2-3 ans). Il est cependant plus conseillé de renouveler son parc moins fréquemment mais en sélectionnant des postes performants.

Il est déconseillé de changer un parc informatique tous les ans : cela entraine des coûts inutiles (les postes sont encore performants) tout en étant néfaste pour l'environnement.

Une notion très importante en informatique est la notion d'obsolescence. On fera toutefois la différence entre obsolescence et obsolescence programmée.

L’obsolescence concerne un objet encore fonctionnel, mais dont l’usage a perdu de son intérêt. En informatique, l’obsolescence peut donc être matérielle ou logicielle.

Lorsque des postes utilisent le système d’exploitation Windows XP, avec une ancienne version d’Office, il s’agit d’une obsolescence logicielle : des produits plus récents, disposants de plus de fonctionnalités « actuelles » (intégration au cloud, fonctions BYOD – Bring Your Own Device) existent, tels que Windows 10 et Office 2016.

Les sites Internet et les technologies utilisées évoluent, de nouvelles fonctionnalités sont ajoutées (lecture de vidéo, images interactives, etc.) requérant une puissance toujours plus élevée.

L’obsolescence programmée est quant à elle illégale, et implique qu’un produit a une durée de vie programmée ou réduite volontairement (pièces fragiles, etc.). Le terme d’obsolescence programmée est bien souvent utilisé à tort pour parler d’obsolescence.

Il arrive toutefois un moment où un poste informatique doit être changé : soit parce qu’il devient trop lent et a atteint ses limites d’évolutivité (obsolescence), soit parce qu’il devient trop coûteux en maintenance (nombreuses pannes, changements de pièces etc).

10 millions de tonnes de déchets d’équipements électriques et électroniques (DEEE) sont produits chaque année par 28 Etats de l’Union Européenne. Sur ces 10 millions de tonnes, seuls 1/3 sont dépollués et recyclés. Le reste de ces déchets se retrouve pour la plupart importé illégalement, en Afrique et en Chine, dans des décharges.

Avant de penser au recyclage, il faut penser à la réutilisation. En effet, un poste qui n’est plus suffisamment performant pour l’entreprise, peut très bien être réutilisé après avoir été testé, réparé et reconditionné. Il s’agit donc là d’une prolongation de la durée de vie de l’objet, pour deux avantages principaux :

- Réduction des déchets.
- Création d’emplois (en logistique, réparation, recyclage et dépollution).

Un troisième avantage non négligeable, pour l’entreprise qui privilégie le réemploi de ces postes, est l’amélioration de l’image de la société. En effet, la société peut mettre en avant cet acte responsable et écologique dans sa communication.

12.5 Annexe 5. Rappel du cahier des charges fonctionnelles

Système de gestion de parc informatique :

Phase de vie : utilisation normale

	Critère	Niveau	Flexibilité
Fonctions principales			
FP1 : Permettre aux utilisateurs de **déclarer** des incidents	Ergonomie de l'interface	270 personnes	F3
FP2 : Permettre au SI de **traiter** des incidents	Déclenchement d'alertes	GTR (en heure)	F3
FP3 : Doit **être constitué** d'une base de connaissances sur le matériel informatique et les logiciels utilisés	Mise en place d'un wiki interne	Illimité	F2
Fonctions contraintes			
FC1 : Doit permettre de **qualifier** les incidents	Cerner la nature des incidents Définir la criticité des incidents	2 types de statuts (bloquant, non bloquant)	F3
FC2 : Doit **répertorier** et **localiser** les ressources matérielles & logicielles	Caractéristiques techniques de classification	194 postes informatiques	F3
FC3 : Doit **faciliter** le suivi des garanties et contrats de maintenance	Alertes de rappel	Durée des contrats	F3

Observations :

FP1 : **Les utilisateurs peuvent déclarer un incident** :

- L'interface doit être simple et intuitive.
- Consulter l'historique des tickets (messages des utilisateurs et réponses du technique).
- Pièces jointes (images, documents, etc.) aux tickets.

FP2 : **Traitement des incidents** :

- Alertes par mail.
- Code couleur pour afficher un ticket en nouvelle information.
- Les tickets doivent pouvoir être attribués aux membres du service informatique, et doivent pouvoir être liés au matériel impacté par l'incident.

FP3 : **Constitution d'une base de connaissances générale :**

- Wiki interne : contribution des utilisateurs de la société.
- Accessible par le service informatique et les utilisateurs (gestion des droits)
- Base de connaissances de documentations de type tutoriels, documentations techniques ou métiers (autres services).

FC1 : **Qualification des incidents** :

- Priorisation donnée aux tickets (ticket bloquant, non bloquant)
- Nature du ticket (incident technique, demande d'information, divers, etc.), n° de ticket, localisation de l'utilisateur, identité du technicien prenant l'incident en charge
- Historique des incidents par thématiques.

FC2 : **Répertorier les ressources matérielles/logicielles** :

- Inventaire des ressources matérielles et logicielles.
- Classement par type : postes fixe, portables, smartphone, imprimante, matériels réseau, serveurs, etc.
- Recherches multicritères en fonction des matériels ou logiciels : n° de série, marque, configuration (processeur, mémoire, disque dur, etc.).
- Durée de garantie (date d'expiration).

FC3 : **Gestion des contrats de maintenance et garantie :**

- Alertes (notifications, mails) à l'approche de l'expiration d'une garantie.
- Fiches des fournisseurs : nom, adresse, hotline, etc.
- Date d'achat.
- Numérisation des contrats.

Politique de maintenance

Phase de vie : entretien

	Critère	Niveau	Flexibilité
Fonctions principales			
FP1 : Doit permettre au SI d'**entretenir** les ressources matérielles & logicielles	Mise en place de procédures d'entretien	Ensemble du parc	F3
FP2 : Doit permettre au SI de **sécuriser** les ressources matérielles & logicielles	MAJ Antivirus	Ensemble du parc	F3
FP3 : Doit permettre d'**homogénéiser** les ressources matérielles & logicielles dans le respect des normes environnementales	Simplification de la maintenance	Ensemble du parc	F2
Fonctions contraintes			
FC1 : **Perturber** le moins possible le travail des utilisateurs	Planifier et prévenir les utilisateurs	Ensemble du parc	F3
FC2 : doit **prendre en compte** les contrats de maintenance/garanties	Remplacement du matériel	Ensemble du parc	F3

Observations :

FP1 : Entretien des ressources matérielles & logicielles par le SI (*Maintenance curative*) :

- Procédures d'entretien du matériel *in situ* : dépoussiérage, etc. :

- Procédure d'entretien à distance : mise à jour des logiciels.

FP2 : Sécurisation des ressources matérielles & logicielles (*maintenance préventive*) :

- Déploiement et mise à jour des antivirus
- Mise à jour des logiciels

FP3 : **Homogénéisation des ressources matérielles & logicielles** dans le respect des **normes environnementales** :

- Sélection des fournisseurs œuvrant pour le développement durable.
- Homogénéiser le matériel pour simplifier et optimiser la maintenance.
- Élaborer une stratégie de recyclage pour la fin de vie des équipements dans le respect des normes DEEE.

FC1 : **Perturber le moins possible le travail des utilisateurs** :

- Délais de prévenance de la maintenance.
- Planification et aménagement de plages horaires

Plan de Continuité d'Activité (PCA)/Plan de Reprise d'Activité (PRA)

Phase de vie : utilisation anormale (mode dégradé)

	Critère	Niveau	Flexibilité
Fonctions principales			
FP1 : Doit **assurer** la disponibilité des données/applications lors d'une panne	Déterminer les fonctions vitales	Nombre de serveurs à déterminer	F3
FP2 : Doit **prévoir** la sauvegarde des données	Plan de sauvegarde	Toutes les semaines /mois	F3
	Sélection des supports		
FP3 : Doit permettre au SI d'**éprouver l'efficacité** d'un PCA/PRA	Phase de test et de maintenance	Tests périodiques	F3
	Faire évoluer l'infrastructure	Coût de maintenance	
Fonctions contraintes			
FC1 : doit **appréhender** l'ensemble des risques	Analyser préalablement les risques	Taux de probabilité du risque	F3
FC2 : doit **prendre en compte** les activités critiques de l'entreprise	Privilégier les services critiques	Nombre de services	F3
FC3 : doit **s'adapter** au budget	Trouver un compromis financier	Voir budget dans la synthèse	

Remarques : Nous avons appréhendé le PRA comme faisant partie intégrante du PCA. C'est pour cette raison que nous utilisons les deux termes.

Observations :

FP1 : **Assurer la disponibilité** :

- Déterminer le niveau de tolérance d'une panne en mode dégradé
- Expliquer les spécifications techniques et les technologies possibles à mettre en œuvre.

FP2 : **Sauvegarde des données** : Élaborer un plan de sauvegarde en réfléchissant sur :

- La régularité des opérations de backup.
- Les types de sauvegardes.
- Le(s) type(s) de support de sauvegarde choisis.

FP3 : **Éprouver l'efficacité du PRA/PCA** :

- Exécution de tests d'intrusion et des maintenances afin de valider l'efficacité du PCA et la robustesse de l'infrastructure.
- Corriger les défaillances éventuelles.
- Faire évoluer l'infrastructure en assurant une veille technologique.

FC1 : **appréhender les risques** :

- Etudier le site pour déterminer les risques majeurs.
- Caractériser la nature des risques (électriques, sinistres, malveillance, etc.).
- Déterminer l'impact des risques sur la production.
- Chiffrer les pertes d'exploitation par heure.

FC2 : Prendre en **compte les activités critiques** :

- Effectuer un audit pour dégager la liste des services jugés les plus critiques.

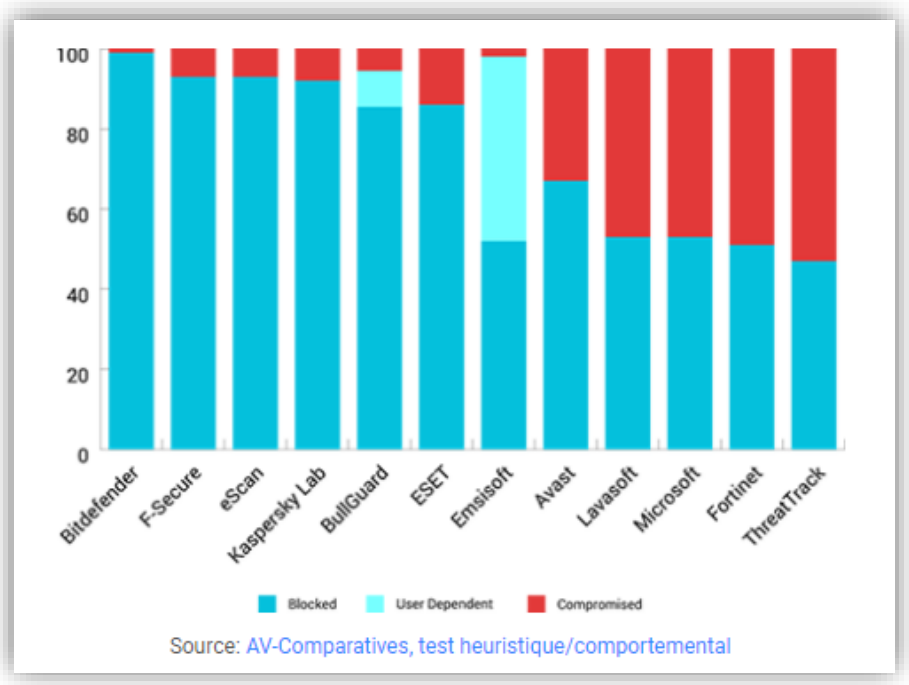
Consulter les responsables des services pour cerner les besoins techniques et humains.

12.6 Annexe 6. Comparatif des solutions antivirales

Afin de protéger l'ensemble du parc informatique de ModulHab, nous avons sélectionné l'antivirus Bitdefender parmi un ensemble de solutions.

Bitdefender est un antivirus très utilisé en milieu professionnel. Plus de 500 millions d'utilisateurs ont adopté la solution et Bitdefender gère 11 milliards de requêtes par jour sur ses serveurs. Cette solution adopte des techniques innovatrices telles que le Machine Learning, l'intelligence artificielle et la corrélation d'évènements afin de détecter les menaces de manière proactive, à la recherche de comportements malveillants.

Bitdefender se différencie également de ses concurrents par un taux de faux-positifs moins élevés.



Exemple de test de différentes solutions antivirales par l'institut AV-Comparatives : Bitdefender a détecté 99% des menaces inconnues

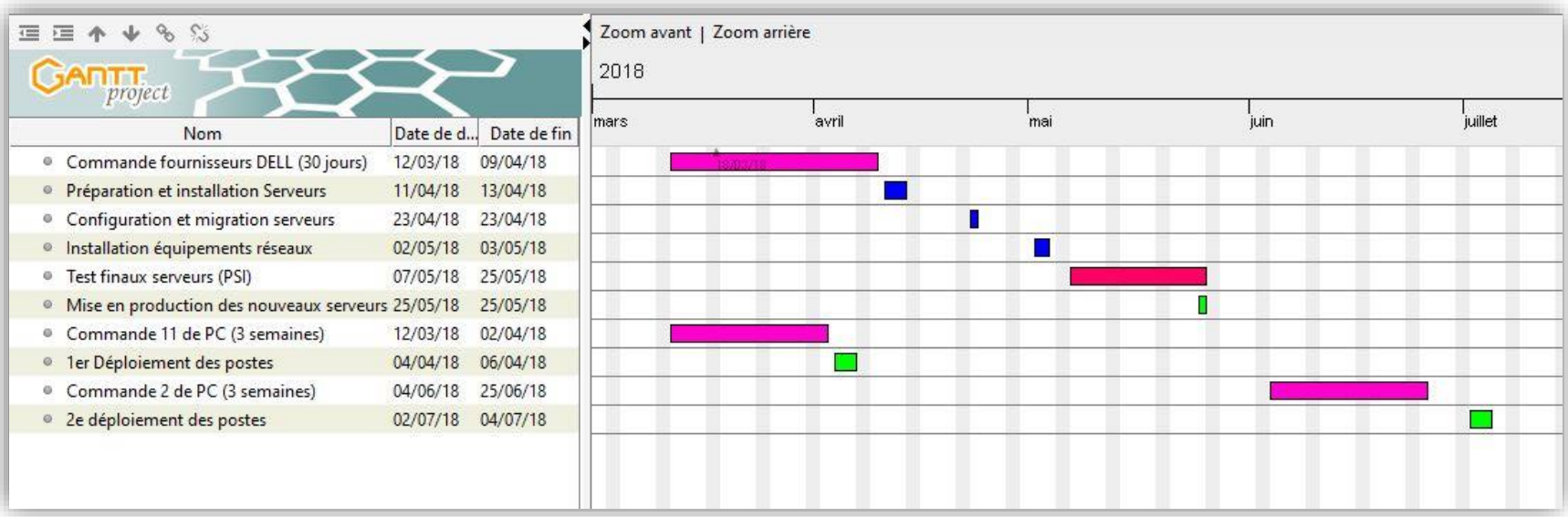
Bitdefender dispose d'un « Control Center » accessible depuis le Web, et donc sans logiciel à installer. Il s'agit donc d'une solution adaptée si l'on recherche de la mobilité. Le Control Center peut être hébergé sur les serveurs de Bitdefender ou bien au sein de l'entreprise.

Des rapports et graphiques détaillés sont également disponible depuis le panel d'administration afin d'avoir un visuel sur l'activité du parc.

BitDefender est régulièrement placé en tête de liste des meilleurs antivirus dans les rapports AV-Test. AV-Test est un institut indépendant allemand spécialisé dans la sécurité informatique et la recherche antivirus.

De plus, cette solution est peu onéreuse. Selon le choix de durée de contrat, la licence reviendra à 21€HT par poste par an (contrat de 3 ans) ou 31€HT par poste par an (contrat de 1 an).

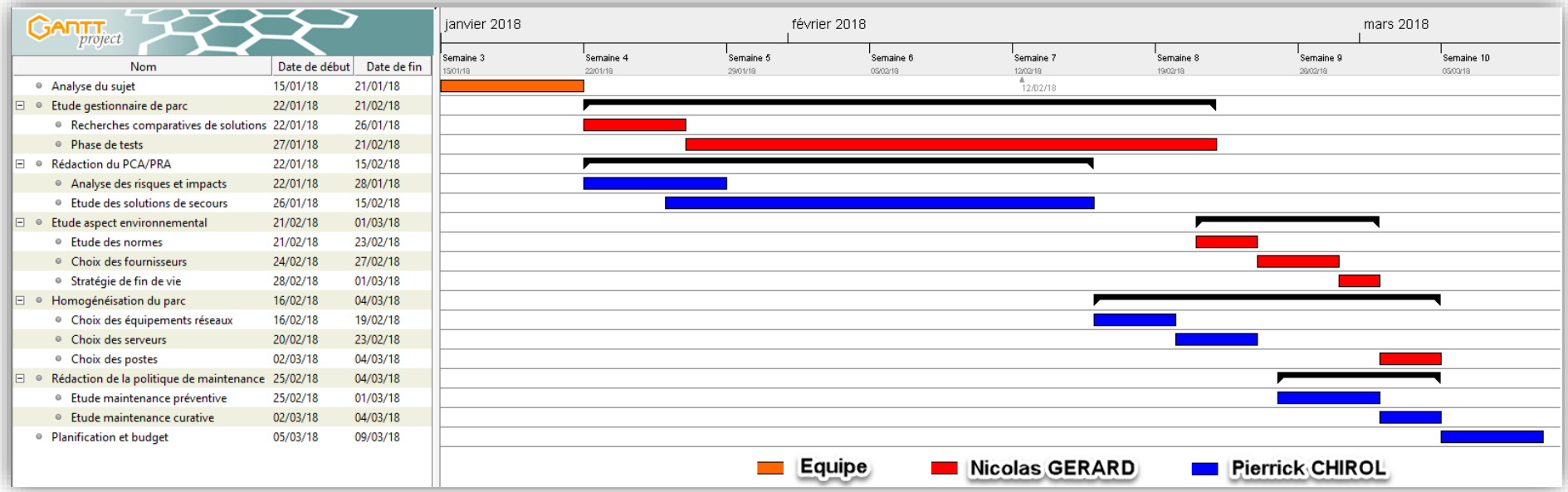
12.7 Annexe 7. Calendrier prévisionnel d'installation du parc



Nom	Date de d...	Date de fin
Commande fournisseurs DELL (30 jours)	12/03/18	09/04/18
Préparation et installation Serveurs	11/04/18	13/04/18
Configuration et migration serveurs	23/04/18	23/04/18
Installation équipements réseaux	02/05/18	03/05/18
Test finaux serveurs (PSI)	07/05/18	25/05/18
Mise en production des nouveaux serveurs	25/05/18	25/05/18
Commande 11 de PC (3 semaines)	12/03/18	02/04/18
1er Déploiement des postes	04/04/18	06/04/18
Commande 2 de PC (3 semaines)	04/06/18	25/06/18
2e déploiement des postes	02/07/18	04/07/18

Ce dernier s'étale sur les 4 premiers mois suivant le déclenchement du renouvellement des infrastructures.

12.8 Annexe 8. Répartition des tâches pour le projet cas H



Nom	Date de début	Date de fin
Analyse du sujet	15/01/18	21/01/18
Etude gestionnaire de parc	22/01/18	21/02/18
Recherches comparatives de solutions	22/01/18	26/01/18
Phase de tests	27/01/18	21/02/18
Rédaction du PCA/PRA	22/01/18	15/02/18
Analyse des risques et impacts	22/01/18	28/01/18
Etude des solutions de secours	26/01/18	15/02/18
Etude aspect environnemental	21/02/18	01/03/18
Etude des normes	21/02/18	23/02/18
Choix des fournisseurs	24/02/18	27/02/18
Stratégie de fin de vie	28/02/18	01/03/18
Homogénéisation du parc	16/02/18	04/03/18
Choix des équipements réseaux	16/02/18	19/02/18
Choix des serveurs	20/02/18	23/02/18
Choix des postes	02/03/18	04/03/18
Rédaction de la politique de maintenance	25/02/18	04/03/18
Etude maintenance préventive	25/02/18	01/03/18
Etude maintenance curative	02/03/18	04/03/18
Planification et budget	05/03/18	09/03/18

13. SOURCES

Bibliographie :

PESSOA A., PLANCHE A., CARREZ B., Plan de Continuité d'Activité. Concepts et démarche pour passer du besoin à la mise en œuvre d'un PCA, *Édition ENI*, 2013.

Guide d'hygiène informatique. Renforcer ma sécurité de son système d'information en 42 mesures, ANSSI, version 2.0, 2017.

Guide pour réaliser un plan de continuité d'activité, SGDSN (*Secrétariat Général de la Défense et de la Sécurité Nationale*), édition 2013.

Les guides de la CNIL, La sécurité des données personnelles, édition 2017.

Webographie :

DEEE :

https://www.ecologique-solidaire.gouv.fr/dechets-dequipements-electriques-et-electroniques

https://www.ecologic-france.com/citoyens/ou-deposer-mes-dechets.html

Recyclage Lenovo :

https://www3.lenovo.com/us/en/social_responsibility/sustainability/ptb_france

http://b2btool.earn-service.com/lenovo

RAID :

https://fr.wikipedia.org/wiki/RAID_(informatique)#RAID_05

http://www.tomshardware.fr/articles/nas-raid-entreprise,2-898-4.html

https://buzut.fr/tirez-le-meilleur-de-vos-disques-durs-avec-raid/#raid10

ITIL :

http://www.itilfrance.com/

http://www.itilfrance.com/index.php?pc=pages/docs/itilv2/12-03.inc&pe=haut_entete_itilv2.inc&pt=Concepts%20de%20base

http://www.itilfrance.com/index.php?pc=pages/docs/pratique-01/110-02.inc&pe=haut_entete_pratique.inc&pt=Le%20processus%20de%20gestion%20des%20incidents

http://www.itilfrance.com/index.php?pc=pages/docs/pratique-01/110-02.inc&pe=haut_entete_pratique.inc&pt=Le%20processus%20de%20gestion%20des%20incidents

http://www.newsitweb.info/avril06/itil_avril06.html

http://www.itilfrance.com/pages/docs/itilv2/12-03.inc

Monitoring :

https://www.centreon.com/

https://www.monitoring-fr.org/solutions/centreon/

http://www.open-source-guide.com/Solutions/Infrastructure/Supervision-et-la-metrologie

https://documentation-fr.centreon.com