

Table des matières

INTRODUCTION GENERALE	1
Chapitre 1 : Présentation du cadre du Projet.....	3
Introduction	3
1. Présentation de la société d'accueil.....	3
1.1 Information générale	3
1.2 Activités.....	3
1.3 Organigramme général de l'UNPA.....	4
2 Cadre du projet.....	5
2.1 Description de projet	5
2.2 Présentation du département d'accueil	5
2.2.1 Service Architecture et Réseaux	5
2.2.2 Service Applications.....	5
2.2.3 Service sécurité informatiques	6
2.2.4 Service Support Utilisateur	6
2.2.5 Mission de la direction système d'information.....	7
2.3 Présentation générale du projet.....	7
2.4 Répartition des tâches d'équipe.....	7
2.5 Mission principale de Projet	9
Conclusion	10
Chapitre 2 : État de de l'art.....	11
Introduction	11
1 Etude de l'existant.....	11
1.1 Architecture de système d'information	11
1.2 Problématique et cahier des charges.....	12
1.3 Solutions proposées.....	13
2 Contexte général du projet.....	14
Introduction.....	14
2.1 La Gestion de parc informatique	14
2.1.1 Objectif de gestion de parc informatique.....	14
2.1.2 SOLUTIONS DE GESTION DE PARC INFORMATIQUE.....	16
2.1.3 Critère de sélection.....	17
2.1.4 CHOIX DE LA SOLUTION	18
2.2 La supervision	18

2.2.1	Définition.....	18
2.2.2	Objectif.....	18
2.2.3	Solution de supervision	19
2.2.4	Choix de la solution.....	19
	Conclusion.....	19
Chapitre 3 : Etude et conception de La solution		11
Introduction		21
1	Besoin Fonctionnel de solution	21
2	Processus IT maitrisés par la solution :	22
2.1	ITIL référentiel de bonne pratique	22
2.1.1	Définition d'ITIL.....	22
2.1.2	Le principe d'ITIL	22
2.1.3	Les processus ITIL	22
2.2	Règles d'implémentation de processus informatique.	23
2.2.1	Processus inventaire et Gestion de configurations	23
2.2.2	Processus Gestion des incidents	24
2.2.3	Processus Contrôle d'accès au système d'information.....	25
3.	Etude Technique des solutions :	27
3.1	Présentation GLPI :.....	27
A.	Architecture du GLPI :.....	27
B.	Conception technique de GLPI :	28
3.2	Présentation de la solution FAN :.....	29
A.	Architecture de FAN	34
Conclusion		35
Chapitre 4 : Implémentation et test de La Solution		36
Introduction		36
1	Architecture Adopté :	36
2	Environnement de travail.....	37
2.1	Environnement matériel.....	37
2.2	Environnement Logiciel	38
2.3	Présentation et validation de la solution	38
2.3.1	Sécurité et authentification.....	38
2.3.2	Processus gestion de la configuration et inventaire.....	39
2.3.3	Processus Gestion des incidents	44
2.3.4	Processus Contrôle d'accès au système d'information.....	46
2.3.5	Processus Supervision de système informatique	54

2.3.6 Notification par Email	62
<i>Conclusion</i>	65
<i>CONCLUSION GENERALE</i>	66
<i>Annexe</i>	68
Annexe A : Préparation de machine virtuelle	68
Annexe B : Installation de FAN	71
Annexe C : Configuration réseaux	74
Annexe D : Installation de GLPI	77
Annexe E : installation des agents d’inventaire et supervision	83
Annexe F : Configuration Nagios avec Centreon	97

LISTE DES FIGURES

Figure 1. Diagramme UNPA -----	4
Figure 2. LAN EPIDOR-----	12
Figure 3. Processus ITIL -----	22
Figure 4. Architecture de GLPI -----	28
Figure 5.Plugin Nsclient-----	31
Figure 6. Plugin NRPE -----	32
Figure 7. Protocol SNMP -----	33
Figure 8.Architecture de FAN -----	34
Figure 9. Architecture adopté-----	36
Figure 10. server power Edge r720 -----	37
Figure 11. Authentification GLPI-----	39
Figure 12. Authentification NAGIOS -----	39
Figure 13. Inventaire des PC -----	40
Figure 14. Inventaire des imprimantes -----	40
Figure 15. Inventaire de Logiciel-----	41
Figure 16. Caractéristique d'un switch Cisco -----	41
Figure 17. Configuration des ports d'un Switch Cisco -----	42
Figure 18. Inventaire des hôtes VMWARE -----	43
Figure 19. Interface Création de ticket -----	44
Figure 20. Interface Attribution d'un ticket -----	45
Figure 21. Interface Ticket attribué -----	45
Figure 22. Interface Résolution de ticket -----	46
Figure 23.Formualire demande Ligne GSM-----	48
Figure 24. Profil par défaut Self-Service -----	48

Figure 25. Profil form-creator	49
Figure 26.interface d'accueil Formulaire	49
Figure 27. Remplissage d'un formulaire	50
Figure 28. Notification Formulaire en attente	51
Figure 29. Validation d'un formulaire	51
Figure 30. Notification état d'un formulaire	52
Figure 31. Suivi d'un formulaire interface GLPI	52
Figure 32. Formulaire demandeur	53
Figure 33.Etat d'un formulaire	53
Figure 34. Formulaire Valideur	54
Figure 35. Vue General de Ngios	55
Figure 36. Host Detail	56
Figure 37. Service Details	56
Figure 38. Information Avancés	57
Figure 39. Service Problem	58
Figure 40 : Service OK	59
Figure 41.Trends	60
Figure 42. Availability	61
Figure 43. Alert History	62
Figure 44. Notification Nouveau Ticket	62
Figure 45. Alert Ticket attribué	63
Figure 46. Alert ticket résolu	63
Figure 47.Vu alerte Nagios	64
Figure 48. Exemple d'alerte Nagios	64

LISTE DES TABLEAU

Tableau 1 . INFORMATION GENERALE DE SOCIETE.....	3
Tableau 2. DETAIL DES TACHES A REALISER	8

INTRODUCTION GENERALE

Actuellement toutes les entreprises sont équipées d'un réseau local et des réseaux de longues distances pour les plus importantes d'entre elles. Leurs parcs informatiques englobent une dizaine et une centaine d'équipements, engendrés par des serveurs de bases de données et des serveurs de traitements.

Vu que ces systèmes informatiques sont au cœur des activités des entreprises, leur maîtrise devient primordiale. Ils doivent fonctionner pleinement et en permanence pour garantir la fiabilité et l'efficacité exigées, et surtout travailler à réduire les problèmes de défaillances, les pannes, les coupures et les différents problèmes techniques qui peuvent causer des pertes considérables. De ce fait, les administrateurs réseau font appel à des logiciels de gestion parc, de surveillance et de supervision de réseaux afin de faire le suivi, la vérification de l'état du réseau en temps réel de l'ensemble du parc informatique sous leur responsabilité.

Grâce à un tel système, les délais d'interventions sont fortement réduits et les anomalies peuvent être aussitôt prises en main avant même qu'un utilisateur peut s'en apercevoir via la notification automatique (par email, par SMS) des concernés en cas de problèmes ou incident à l'aide des outils de gestion et de supervision de parc informatique qui s'avère nécessaire et indispensable. Elle permet entre autre d'avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau, de faciliter

l'intervention et la résolution et aussi d'avoir des indicateurs sur la performance de son architecture.

Dans ce cadre, le présent rapport se base sur trois axes principaux.

- Présenter les notions de base de la gestion et la supervision de parc informatique et de ses logiciels les plus utilisés actuellement.
- Etudier la solution choisie parmi plusieurs en énumérant ses fonctionnalités et apport
- Implémenter la solution proposée choisie.

Chapitre 1 : Présentation du cadre du Projet

Introduction

Dans ce chapitre, nous allons donner une brève description de la société d'accueil, et présenter son organigramme ensuite nous allons expliquer le cadre général de notre projet et ses objectifs.

1. Présentation de la société d'accueil

1.1 Information générale

Nom de la société . UNPA Habib Mellouli / L'Epi D'or
Catégorie . Agriculture et Agro-alimentaire (Céréales et dérivés)
Année de Création . 1973
Adresse . RTE DE M'SAKEN, 4000 – Sousse, Tunisie
Tél . (+216)73 233 055 Fax . (+216)73 232 746
Email . mellouli.epidor@planet.tn Site . http://www.lepidor.com.tn/

Tableau 1 .INFORMATION GENERALE DE SOCIETE

1.2 Activités

Crée en 1972 par Habib Mellouli, connue sous le nom commercial de « l'EPI d'OR » est spécialisée dans la production des semoules, farines, pâtes alimentaires et couscous. Parfait exemple d'entreprise familiale, elle bénéficie d'une longue expérience renforcée par une capacité d'innovation exceptionnelle. La transmission de père en fils du savoir-faire traditionnel a été garante du maintien d'une qualité de produits irréprochable, appréciée par des milliers de consommateurs qui se transmettent de génération en génération leurs secrets de cuisine.

1.3 Organigramme général de l'UNPA

L'UNPA dispose de plusieurs directions. Chacune des directions a une relation étroite avec la production. L'organigramme général de l'UNPA se présente comme suit :

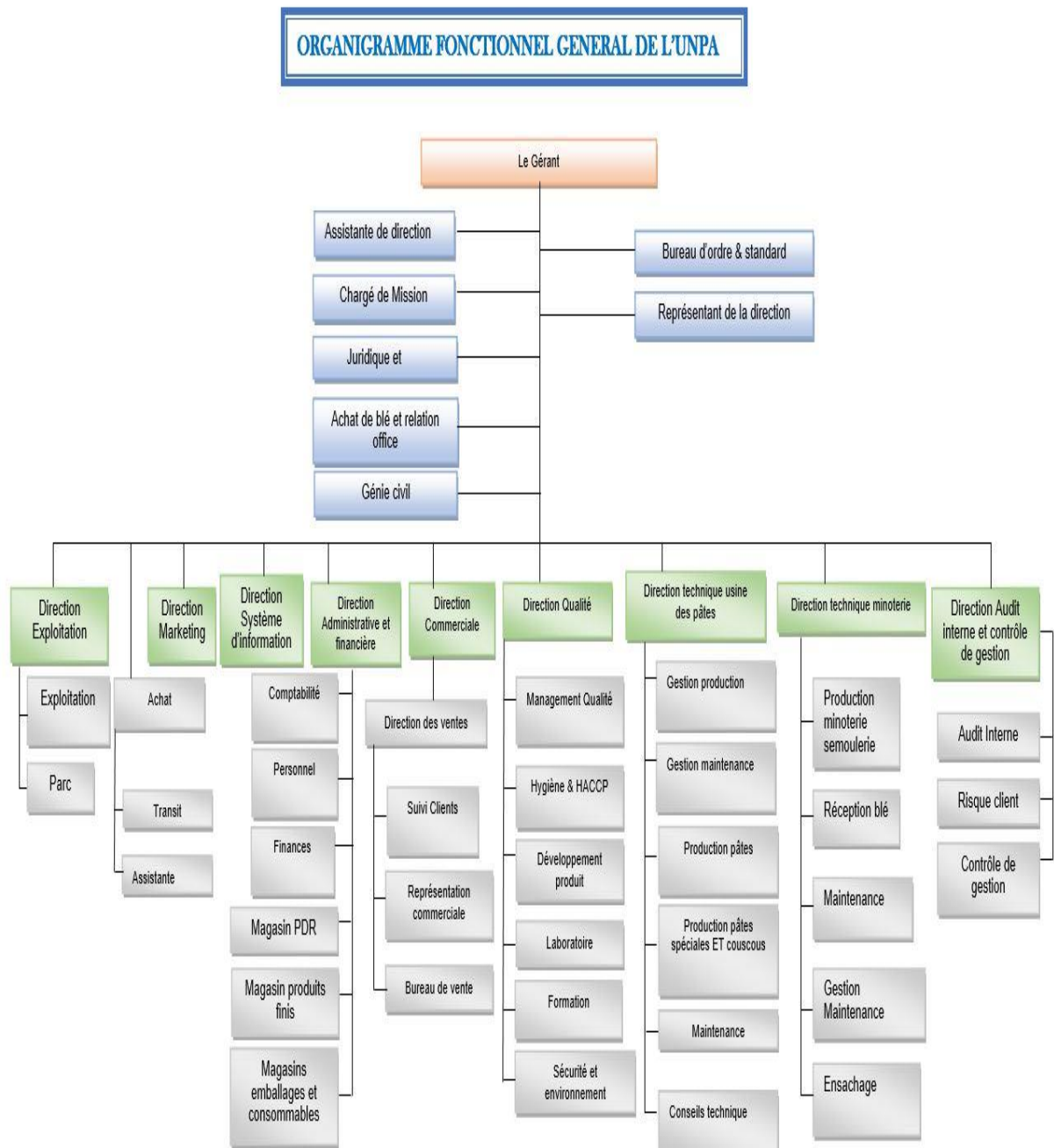


Figure 1. Diagramme UNPA

2 Cadre du projet

2.1 Description de projet

Ce projet a été initié par le département système d'information de groupe « L'EPI D'OR », le thème principal celui qui sera développé dans ce rapport, à savoir "La mise en place d'un outil qui permet la gestion des incidents, des demandes d'accès et la supervision pour tout le système d'information". Pour simplifier le travail, nous allons utiliser cet outil comme un moniteur de supervision et gestionnaire de parc et de support « helpdesk ».

Le but d'un tel programme est de surveiller les services et les machines se trouvant dans le département informatique ainsi les accès, les problèmes et les incidents. Si un problème survient, le moniteur de supervision nous prévient un (email, SMS) ou peut entreprendre certaines actions (relancer un service, tuer un processus, demander un redémarrage, ou lancer un processus de gestion des incidents et des problèmes...). Toutes ses tâches seront traitées et sauvegardées dans l'outil de gestion de parc informatique.

2.2 Présentation du département d'accueil

La direction système d'information de L'EPI D'or est composée du.

2.2.1 Service Architecture et Réseaux

Le service Architecture Réseaux a pour vocation de construire l'infrastructure du Système d'information, ses missions sont :

- Concevoir, maintenir et moderniser l'architecture du SI.
- Administrer et exploiter les équipements.
- Conduire les projets techniques.
- Fournir une assistance technique aux autres services.
- Veille technologique afin d'anticiper les évolutions technologiques.

2.2.2 Service Applications

Le service applications assure la mise en place des solutions ou d'outils informatique moderne et d'assurer leur fonctionnement et leur évolution.

Il a pour mission d'assurer la maintenance, l'administration technique et l'évolution des applications métiers et le développement des applications spécifiques en cas de besoin.

2.2.3 Service sécurité informatiques

Sa principale fonctionnalité est d'évaluer les vulnérabilités du système d'information de l'entreprise, définir et mettre en œuvre la politique de sécurité de l'entreprise. Il met en place des solutions pour garantir la disponibilité, la sécurité et l'intégrité de système information et des données, sa mission est :

- Réaliser des audits du système de sécurité, le plus souvent avec l'aide de prestataires.
- Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité.
- Définir et faire évoluer la politique de sécurité des systèmes d'information du groupe (PSSI).
- Établir un plan de prévention des risques informatiques et un plan de continuité d'activité (PCA).
- Définir ou faire évoluer les mesures et les normes de sécurité, en cohérence avec la nature de l'activité de l'entreprise et son exposition aux risques informatiques.
- Choisir les dispositifs techniques les plus appropriés aux besoins de l'entreprise (firewall, programmes de back-up, cryptographie, authentification...).
- Participer à la définition et au contrôle de la gestion des habilitations.
- Participer au comité des risques.

2.2.4 Service Support Utilisateur

Le service support utilisateurs est l'un des plus actifs parmi tous les services il assure le fonctionnement, dans les meilleures conditions, du parc matériel et logiciels de l'entreprise. Son principale mission est :

- La Gestion, installation et maintenance du matériel informatique (laptop, imprimantes, ordinateurs, périphériques,...).
- Administration et exploitation de serveurs.
- Aide à la gestion, installation et maintenance des logiciels/
- Assistance et support technique (matériel et logiciel) auprès des utilisateurs
- Gestion des sauvegardes sur les applications et serveurs internes.

- Présentation des ressources informatiques aux nouveaux utilisateurs.
- Sensibilisation des utilisateurs sur la sécurité informatique et sur les règles de bonnes pratiques.
- Aide à la gestion de la téléphonie sur IP, assistance aux utilisateurs et maintenance des installations.
- Participation aux projets informatiques de l'entreprise.

2.2.5 Mission de la direction système d'information

La principale mission de la direction informatique est l'implémentation et la gestion de service informatique de qualité, correspondant aux visions et besoins de business.

Pour améliorer la qualité et la performance de service la direction système d'information vise à appliquer un référentiel de bonne pratique ITIL et ISO 27000 pour la gestion de service et de sécurité.

Pour atteindre ce but stratégique la direction informatique veille à la bonne formation et évolution de leurs équipes et à la mise en place des meilleurs outils informatiques nécessaires.

2.3 Présentation générale du projet

Ce projet a été initié par le comité de sécurité informatiques « COSI » de groupe « L'EPI D'OR ». Suite à une mission d'audit, un plan d'action est lancé comportant plusieurs tâches parmi lesquelles deux grands parties qui sont :

- La mise en place d'un outil qui permet la gestion des incidents, des demandes d'accès et la supervision pour tout le système d'information.
- Mise en place d'un système de management de sécurité pour la gestion des événements des intrusions, des vulnérabilités et des indisponibilités.

2.4 Répartition des tâches d'équipe

Vu que mon projets et celui de mon binôme sont lancés par la même direction et vont être réalisé dans le même environnement technique et pour avoir une meilleur collaboration et garantir la réussite nous avons décidé de commencer une réunion avec la direction système d'information suite à laquelle un plan d'exécution est lancé.

Ce plan comporte des taches communes et des taches propres à chaque membre de projet.

Le tableau ci dessous illustre de façon globale les différentes taches à réaliser :

Tache	Détails des tache à réalises		Période
Etude théorique - Etat de l'art - Etude de l'existant - Spécification des besoins - Conception	- Réunion du comité de direction et lancement du projet - Rédaction d'un PV détaillé. - Etude de l'existant concernant la sécurité et la gestion des incidents. - Comparaison des choix technique. - Choix du thème a implémenté après confirmation de la direction selon les PSSI (politique de sécurité de système d'information) et procédures de la société - Planning des tâches du projet géré par IT Project Manager de l'équipe.		1mois
Travail Technique - Réalisation de l'application - Test et Validation - Rédaction de rapport final	Tache à faire Projet Ossim	Tache à faire Projet GLPI	3mois
	- Selon les Règles de PSSI on est demandé de préparer la documentation. - Préparation de l'environnement de l'installation des serveurs OSSIM pour la gestion des évènements et des vulnérabilités - Préparation de l'environnement d'installation du serveur Nagios et Réunion avec le comité pour suivre l'avancement de projet et Test d'applicatif.	- Préparation de l'environnement virtuelle d'installation de serveurs Nagios et GLPI - Installation et configuration de GLPI et ses composants - Installation et configuration de Nagios	
- Vérification de l'application - Vérification de rapport	- Optimisation du projet techniquement - Finalisation de la rédaction du rapport	- Optimisation de projet techniquement - Finaliser la radication du Rapport	15jours

Tableau 2. DETAIL DES TACHES A REALISER

2.5 Mission principale de Projet

Mon projet intitulé « La mise en place d'un outil qui permet la gestion des incidents, des demandes d'accès et la supervision du système d'information ». Pour simplifier le travail, nous allons utiliser cet outil de supervision et gestionnaire de parc et de support « helpdesk ». Le but d'un tel programme est de surveiller les services et les machines qui se trouvent dans le département informatique ainsi les accès, les problèmes et les incidents. Si un problème survient, le moniteur de supervision nous prévient (email, SMS) ou entreprendre certaines actions (relancer un service, tuer un processus, demander un redémarrage, ou lancer un processus de gestion des incidents et des problèmes...). Tous ses tâches seront traités et sauvegardés avec l'outil de gestion de parc informatique.

L'administrateur réseau devra surveiller son réseau via une interface web sécurisée de Nagios. Cette interface devra donc être protégée par un mot de passe. Elle devra comporter une vue de monitoring du réseau, présentant les différents postes utilisateurs, les serveurs, les éléments actifs. Cette vue devra explicitement décrire l'état de ces machines et de vérifier si les services tournent correctement ou non. Dans le même concept l'outil GLPI permet de gérer l'inventaire de parc informatique, les tickets des incidents et des demandes d'assistance et d'intervention.

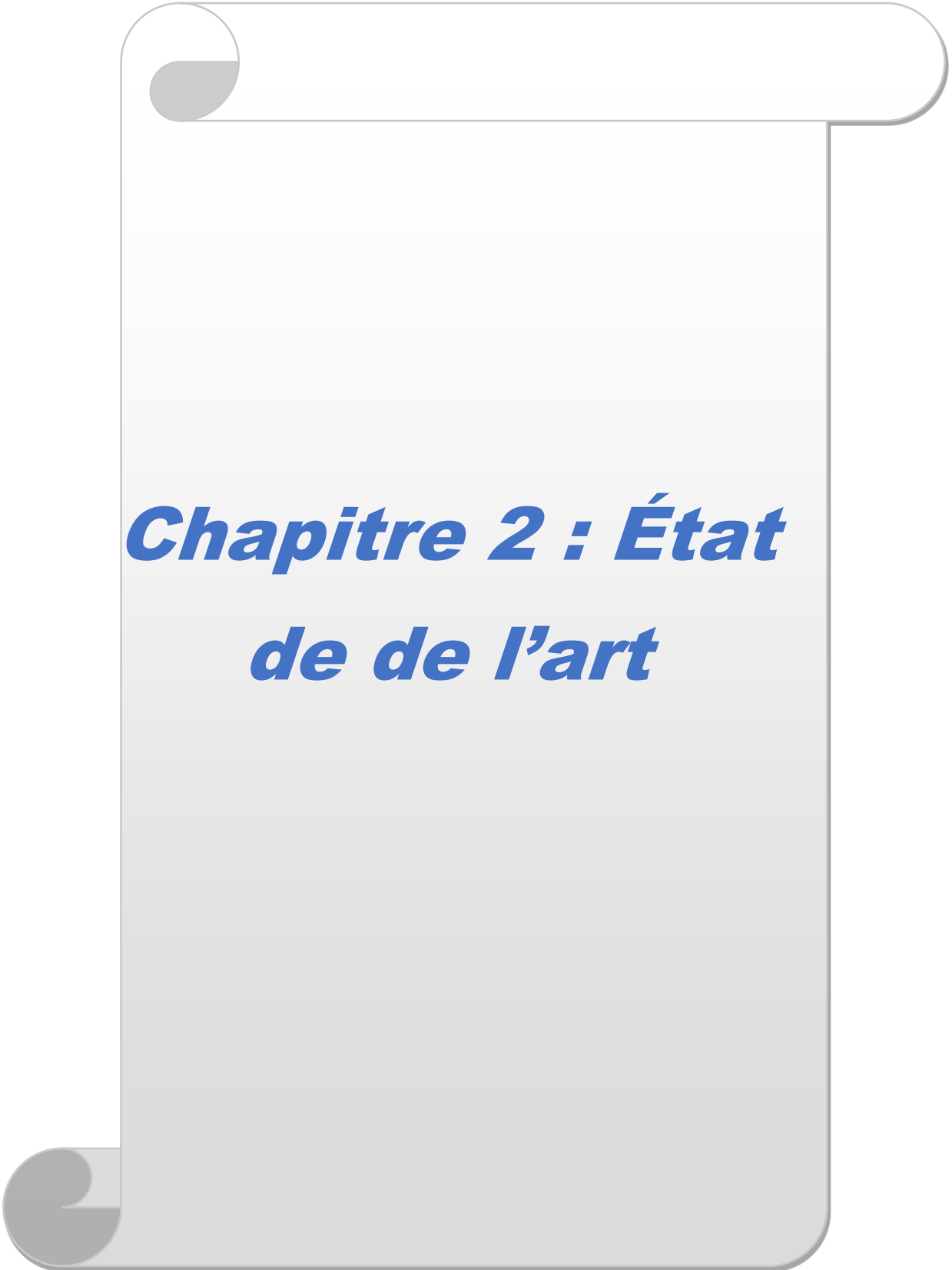
A travers Nagios et GLPI, des renseignements supplémentaires sur les différentes machines (charge CPU, espace disque, mémoire disponible, etc.) aussi que les incidents et les demandes pourront être renseignés. Enfin, lorsque des problèmes et des demandes surviendront, l'administrateur devra être notifié par un courriel dont le contenu indiquera le service et/ou la machine défectueuse ou le ticket de demande d'intervention. La solution devra bien entendu être la moins chère possible.

La supervision et la gestion d'un réseau nécessite des outils adaptés aux différents composants du notre réseau qui est doté de machines sous Linux, Windows. Nous devons donc trouver, comme tout bon produit de supervision et de gestion de parc, un produit capable de superviser l'ensemble des équipements provenant de différents constructeurs et ayant des modes de gestion hétérogènes. Il s'agit alors de trouver un produit reposant sur un protocole ou un environnement normalisé afin de pouvoir servir de point d'entrée unique pour regrouper toutes les informations du réseau.

Conclusion

Ce chapitre a été conçu pour familiariser l'environnement du travail en présentant l'entreprise d'accueil et l'architecture réseau dont elle dispose et le cadre général de projet.

Rapport-Gratuit.com



Chapitre 2 : État de de l'art

Introduction

Dans ce chapitre nous allons présenter des concepts de base et quelques termes primordiaux de la supervision des systèmes d'information et de l'administration des réseaux. Puis une description générale de la sécurité informatique. Ensuite nous enchaînerons avec les différentes plateformes open source existantes dans le domaine de la surveillance réseau, la gestion des logs basées sur la corrélation de ceux-ci ainsi qu'une notion d'évaluation des risques, en décrivant leurs avantages et leurs inconvénients pour arriver enfin à la sélection de la plateforme adoptée dans notre projet suite à des critères de besoins escomptés par l'utilisateur de notre système d'information étudié auparavant.

1 Etude de l'existant

1.1 Architecture de système d'information

Le système d'information se compose de multitudes d'applications métiers, d'applications de sécurité et d'application de support, l'ensemble de ces applications de sauvegarde qui fonctionnent sur une infrastructure serveurs virtuels qui se compose des éléments suivants.

Un Datacenter est composé de deux serveurs hyperviseurs au niveau desquelles sont installés l'ensemble de nos serveurs virtuels applicatifs. Les différents utilisateurs locaux de l'entreprise se connectent aux serveurs virtuels à travers un réseau devisé en plusieurs (VLAN) comportant des switchers Cisco niveau 2 et 3.

Les utilisateurs distants se connectent via un accès VPN géré par deux Firewall Cyberoam et deux lignes internet FO et FH fonctionnant en mode HA (haute disponibilité).

La figure ci dessous illustre l'architecture de notre SI.

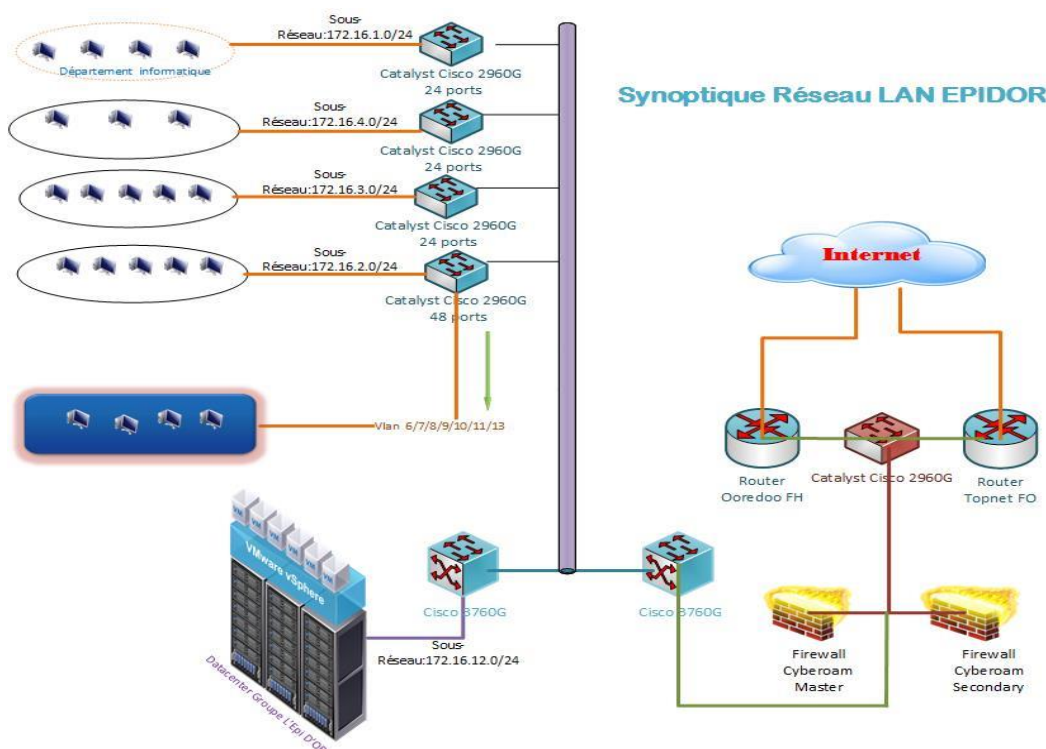


Figure 2. LAN EPIDOR

1.2 Problématique et cahier des charges

En informatique, chaque application fournit plus ou moins directement un service au client, qu'il soit interne à la société ou client final. Chez « L'EPI D'OR » comme dans beaucoup de sociétés, l'informatique occupe une place de premier plan dans le fonctionnement de l'entreprise. Si les services informatiques sont indisponibles, les employés ne peuvent plus être aussi productifs et il y a perte de valeur.

Fournir un service informatique de qualité a donc une valeur primordiale, et l'un des buts de mon projet a été de travailler à son amélioration avec le reste de l'équipe.

Les nouveaux services mis en place devenant le cœur du système informatique présent sur chaque département, leur disponibilité est devenue extrêmement critique. En effet, en cas d'arrêt de nombreux services sont interrompus (production, vente, achat, facturation...).

Cependant, le réseau informatique et l'infrastructure ayant évolués suite à des extensions et aux rachats d'autres sociétés disposants chacune de leurs systèmes informatiques.

La problématique peut être résumée en comment assurer une qualité de service optimale et sans arrêt dans un environnement comportant un parc informatique composé de plusieurs machines, équipements réseaux et des serveurs d'applications. L'administrateur ne peut pas déterminer directement d'où vient le problème lorsqu'une machine sera inaccessible ou quelle est la machine éteinte ou l'interface réseau qui est hors service. L'administrateur ne peut pas déterminer si un service particulier sur un serveur donné fonctionne correctement ou non à cause de l'absence de récupération instantanée des informations sur ces machines.

Dans l'environnement quotidien des utilisateurs, des ressources matérielles que logicielles sont distribuées entre plusieurs parties du réseau et sont disponibles sur des systèmes très variés. Un administrateur doit gérer son réseau pour obtenir des informations en temps réel sur le trafic et les caractéristiques des performances aussi que l'accès des utilisateurs. Etant donné l'importance de ces derniers besoins mon but était comment je peux améliorer le réseau informatique existant en offrant à l'administrateur réseau une souplesse et une efficacité au niveau des tâches de contrôle et de surveillance pour toutes les ressources ou les utilisateurs présentent sur le réseau.

L'administrateur système et demander à gérer un grands parc informatique en terme de nombre de poste de travail et des périphériques réseaux, ce qui représente un grand défi. Un grand flux des demandes d'assistances et d'intervention par les utilisateurs de parc informatique ce qui nécessite la présence d'un outil qui permet la sauvegarde, la priorisation, la traçabilité des incidents et des interventions ainsi l'analyse des coûts de maintenance et la gestion d'inventaire de parc informatique.

Donc ces critères rentrent dans le domaine de la supervision de réseau, essentiel pour assurer une disponibilité du système informatique de l'entreprise.

1.3 Solutions proposées

Notre projet est la mise en place d'une solution de supervision, d'inventaire et de gestion des incidents et demande des utilisateurs.

2 Contexte général du projet

Introduction

Dans cette partie, nous commençons par une étude théorique sur la gestion du parc et la supervision et ses objectifs ensuite analyser de près les fonctionnalités de la solution proposée, réaliser une comparaison entre les différents produits existant pour pouvoir choisir le produit qui répond mieux à nos besoins.

2.1 La Gestion de parc informatique

Aujourd'hui Chaque organisme qui veut augmenter son chiffre d'affaires doit doter son entreprise d'un parc informatique. Pour ce faire, il doit savoir ce que c'est, les dangers auxquels il est exposé et comment mettre en place un parc informatique de qualité et sécurisé.

Le terme de parc informatique désigné l'ensemble des ressources matérielles et logicielles qui composent votre système informatique.

Le parc informatique comprend évidemment l'ensemble

- ❖ des postes de travail, unités centrales, écran, claviers...etc.
- ❖ Les périphériques. imprimantes, scanner, tablettes, ...
- ❖ Les serveurs.
- ❖ Le Cloud.
- ❖ Le réseau physique.
- ❖ Les données informatiques.
- ❖ L'ensemble des logiciels et applications utilisés ainsi que leurs licences.
- ❖ Les appareils mobiles, smartphones et tablettes.

2.1.1 Objectif de gestion de parc informatique.

La gestion de parc informatique regroupe un ensemble de tâches visant :

- ❖ À entretenir, développer et optimiser l'ensemble des ressources informatiques de l'entreprise.
- ❖ Recenser et localiser l'ensemble des éléments du parc informatique.
- ❖ Définir l'organisation du système informatique.

- ❖ Protéger le parc informatique.
- ❖ Maintenance et dépannage.
- ❖ Procédures.
- ❖ Formations et usages.
- ❖ Charte informatique.
- ❖ Prestataires de services (dépannage, hébergement, logiciels, infogérance)
- ❖ Etablir une base de données de configuration.

Nous devons disposer d'une base de données recensant l'ensemble de notre matériel informatique et les entités qui constituent notre parc informatique. Il s'agit d'une CMDB, ou Configuration Management Data Base. Cette base de données ne fait pas seulement état du matériel mais aussi de l'ensemble des licences, contrats d'infogérance ou d'assistance, informations techniques... Constituer un inventaire précis des licences permet d'évaluer correctement nos besoins et d'éviter de payer des licences inutiles. Une liste des programmes et licences utilisées permet de réaliser jusqu'à 15% d'économies.

- ❖ Maintenir le parc informatique à jour.

Il faut impérativement maintenir notre système informatique à jour. Les mises à jour logiciels apportent de nouvelles fonctionnalités mais permettent surtout de corriger les failles de sécurité des programmes. La plupart des mises à jour peuvent être réalisées automatiquement. Maintenir nos programmes à jour est un élément important de la sécurité de notre parc informatique. Les mises à jour en question doivent être réalisées sur l'ensemble des machines du parc informatique.

- ❖ Augmenter la durée des équipements.

Une bonne gestion de parc informatique permet d'augmenter la durée de vie des machines. , on peut par la suite anticiper les problèmes, résoudre les pannes informatiques et optimiser le fonctionnement de notre système d'information. Une bonne protection contre les virus, un nettoyage régulier contre les malwares et les fichiers inutiles et des mises à jour logiciel régulières permettent d'augmenter la durée de vie du matériel informatique en évitant les pannes les plus courantes et les lenteurs de fonctionnement.

2.1.2 SOLUTIONS DE GESTION DE PARC INFORMATIQUE

Il existe de nombreux logiciels permettant de gérer un parc informatique. Ils ne répondent pas toujours aux réels besoins des administrateurs du parc, peuvent être coûteux à l'acquisition ou en maintenance. On distingue :

a. ISILOG WEB SYSTEM

La solution de gestion de parc informatique Isilog Web System s'appuie sur une architecture client-serveur. En effet un serveur Isilog Web System collecte les informations transmises par l'agent de scan installé sur chaque poste. Le logiciel installé sur le serveur permet de classer et organiser les informations remontées. Ces informations sont cependant accessibles uniquement depuis ce serveur. L'agent de scan des postes de travail doit être installé manuellement. Pour pouvoir utiliser Isilog Web System, il faut s'acquitter d'une licence annuelle de plus de 5 000 €. La garantie et le support sont pris en charge par Isilog, le coût inhérent étant intégré à la licence. Isilog Web System ne contient pas de FAQ (Foire Aux Questions). Le module Isiscan, composant d'Isilog Web System, permet de relever automatiquement les différents composants matériels des ordinateurs, des imprimantes, les logiciels et leurs licences. Les possibilités d'évolution de cette solution sont très bonnes, mais le coût des modules complémentaire à mettre en place est très élevé. Ce coût est du au fait que seul Isilog a le droit de développer de nouveaux modules pour Isilog Web System. La mise en place de cette solution est assez compliquée, puisqu'il faut créer et administrer complètement le serveur de base de données sur lequel s'appuiera le serveur Isilog. Le prix est très élevé, puisque d'après le commercial la formule la plus basique requiert le paiement d'une licence annuelle de plus de 8000 € HT. La consultation des données est accessible, mais il faudra un temps d'adaptation avant de maîtriser l'interface. Enfin, il n'existe pas à ce jour de possibilité de déploiement automatique de l'agent de scan. Chaque nouvelle machine doit être scannée localement, ensuite le serveur est capable de mettre à jour ses données automatiquement, mais le fait de devoir passer sur chaque poste la première fois est un paramètre déterminant

b. MANDRIVA PULSE 2

Mandriva Pulse 2 est un module de Mandriva serveur. Pulse2 existe depuis 2006, date de sortie de la première préversion (version alpha). Ce module est dédié à la collecte d'informations d'un parc informatique, dans le but d'automatiser la fonction d'inventaire. Ainsi, après le déploiement du programme de scan des postes de travail, la base de données est remplie automatiquement par les valeurs relevées lors de l'inventaire. L'installation est

très simple et rapide, et ne demande aucune compétence particulière. En opposition, le classement des données n'est pas très ergonomique, il faut un temps d'adaptation. Le module Mandriva a de très bons arguments avec la gestion du déploiement, le déploiement régulé d'applications, de patches, de mises à jour ainsi que l'outil de régulation de la bande passante. La communauté d'utilisateurs de Pulse 2 est assez réduite, de plus, le support technique est payant (100€/an).

c. GLPI (*Gestion Libre de Parc Informatique*)

Est un projet open-source sous licence GPL. Ce produit a été lancé en 2003. GLPI est un outil qui permet de classer, organiser et exploiter les données récoltées lors d'un inventaire. L'inventaire devra être effectué par un autre logiciel fusionInventory qui est lui aussi soumis à la licence GPL.

L'installation de la solution est longue, mais très bien expliquée par le forum officiel. GLPI dispose d'un avantage puisque son installation nécessite seulement un serveur web compatible PHP et une base de données MySQL.

L'utilisation de GLPI et fusionInventory permet une multitude de fonctions qu'ils intègrent. Au niveau de l'inventaire, GLPI est le plus complet de la gestion de parc et helpdesk. L'évolution de GLPI est constante, par des mises à jour ou la création de nouveaux plugins. Enfin, le support, assuré par la communauté d'utilisateurs est efficace. La base de connaissance et les livres blancs très nombreux sont aussi une aide appréciable.

2.1.3 Critère de sélection.

- Inventaire des ordinateurs. Micro-ordinateur (marque, modèle, numéro de série) ; Processeur (nombre de cœurs et fréquence) ; Mémoire vive (quantité et fréquence) ; Disque dur (capacité et partitionnement) ; Carte graphique (fréquence processeur et mémoire) ; Ecran (marque, modèle, numéro de série)
- Inventaire logiciels. Connaître les systèmes d'exploitation et leurs versions ; Connaître les logiciels installés sur chaque micro-ordinateur et leurs versions ; Voir les numéros de licences des logiciels
- Inventaire actif réseau. Marque, modèle et numéro de série ; Switch ; Wi-Fi
- Inventaire imprimantes et copieurs. Marque, modèle et numéro de série ; Capacité
- Contraintes techniques. Mise en place rapide ; Environnement Microsoft et Linux

- Simplicité de l'administration et de la maintenance
- Support et help desk aux utilisateurs (gestion des incidents, des demandes et des problèmes.)

2.1.4 CHOIX DE LA SOLUTION

Suite au comparatif réalisé entre les différents produits, il apparaît que la solution la plus adaptée est GLPI. Mandriva Pulse 2 est très performant mais tiré vers le bas par son coût réel et son absence de support gratuit. Isilog est lui bien moins performant et moins polyvalent. Il ne sera par exemple possible de ne pas répertorier les switch et les bornes wifi, ce qui ne correspond pas avec mes objectifs. En conclusion, GLPI, répond à toutes mes exigences et propose de nombreuses possibilité d'évolution. Le support est excellent de par la taille impressionnante de la communauté d'utilisateurs. Son utilisation, bien qu'assez complexe, est intuitive. Enfin, la sauvegarde et la restauration sont très simples à mettre en place.

2.2 La supervision

2.2.1 Définition

La supervision de réseaux peut être définie comme l'utilisation de ressources réseaux adaptées dans le but d'obtenir des informations (en temps réel ou non) sur l'utilisation ou la condition des réseaux et de leurs éléments afin d'assurer un niveau de service garanti, une bonne qualité et une répartition optimale et de ceux-ci.

La mise en place d'une supervision réseau, a donc pour principale vocation de collecter à intervalle régulier les informations nécessaires sur l'état de l'infrastructure et des entités qui y sont utilisés, de les analyser et de les rapporter.

2.2.2 Objectif

L'objectif d'une supervision de réseaux peut ainsi se résumer en trois points.

Etre réactif en alertant l'administrateur (e-mail ou sms) en cas de dysfonctionnement d'une partie du système d'information.

Etre pro actif en anticipant les pannes possibles.

Cibler le problème dès son apparition afin d'agir rapidement de la façon la plus pertinente possible.

2.2.3 Solution de supervision

Il existe des solutions de supervision libres et professionnelles. Parmi les plus répandues, reconnues du moment nous pouvons citer FAN Nagios et Eyesofnetwork. L'avantage de ces logiciels libres est la gratuité, la disponibilité du code source et la liberté d'étudier et de modifier le code selon nos besoins et de le diffuser.

De plus, il existe une communauté importante d'utilisateurs et de développeurs qui participent à l'amélioration des logiciels et apportent une assistance par la mise en ligne des documentations et les participations

D'autre parts il existe des solutions commerciales comme exemple (HPOpenview, Bi Brother, etc...) nécessitent un investissement important pour leur mise en place, et pour des raisons propres à l'entreprise, toutes ces solutions sont à écarter de mon liste de choix.

2.2.4 Choix de la solution.

Pour garantir une compatibilité dans mon projet avec la première partie de mon projet dans laquelle j'ai choisi de travailler avec l'outil open source GLPI et fusion inventory j'ai décidé de compléter la deuxième partie avec un autre outil de même genre FAN Nagios qui répond bien à mon besoin. En effet, grâce à ses plugins, FAN Nagios possède une architecture facilement adaptable à l'environnement. Ces derniers pouvant être ajoutés, modifiés ou même personnalisés et permettent de spécifier les tâches pour aboutir au résultat voulu. De plus FAN Nagios est une solution stable, dispose d'une grande communauté de développeurs et utilisé aussi bien dans les petites et moyennes infrastructures que dans les grands parcs informatiques et utilisé surtout par plusieurs entreprises de renommé

De plus FAN couple Nagios à Centrerons qui est un logiciel qui lui servira de couche applicative afin de faciliter la configuration et d'établir des interfaces plus ergonomiques et compréhensibles.

Conclusion

Dans Ce chapitre, j'ai commencé une étude de l'existant au niveau de parc informatique de l'EPI d'or pour déterminer la problématique et proposé des solutions techniques.

Par la suite j'ai terminé mon travail par une étude théorique sur le thème de mon projet qui porte sur la gestion et la supervision de parc informatique et finalement j'ai réalisé un

comparatif entre les produits existant sur le marché pour pouvoir sélectionner le plus adapté à mes besoins.

***Chapitre 3 :
Etude et
conception de
La solution***

Introduction

Après une étude de l'existant et choix de solution, dans ce chapitre je vais présenter de manière approfondi les solutions retenus de point de vu fonctionnalités et architectures.

1 Besoin Fonctionnel de solution

Une solution informatique de gestion et de supervision de parc informatique doit au moins répondre au besoin fonctionnel suivant

- ❖ Superviser les ressources systèmes

Espace disque : pour afficher l'espace disque utilisé et l'espace disque libre

Mémoire disponible : pour indiquer l'espace mémoire utilisé et celui disponible.

Charge de machine (Load)

Charge CPU

- ❖ Superviser les services réseaux

Le service FTP : transfert des fichiers

Le service DHCP : attribution dynamique d'adresses IP

Le service SMTP : envoi des emails

Le service DNS : conversion des noms de domaines en adresses IP

Le service SSH : connexion au serveur de l'EPI d'OR avec une liaison sécurisée

Le service SNMP : récupération des données et envoi des alertes (traps SNMP) en cas de problème au niveau des équipements

Le service HTTP : communication client-serveur.

Le service MYSQL : un système de gestion de bases de données relationnelles.

Le service TCP : un protocole de transport fiable en mode connecté

- ❖ Gérer l'inventaire de parc informatique
- ❖ Gérer les incidents, les demandes et les problèmes
- ❖ Gestion de traçabilité et gestion de connaissance.
- ❖ Notification des alertes, des demandes et des incidents.

2 Processus IT maîtrisés par la solution :

2.1 ITIL référentiel de bonne pratique

2.1.1 Définition d'ITIL

ITIL (Information Technology Infrastructure Library) Lancé fin des années 1980, ITIL est devenu un standard international de fait dans la Gestion des Services Informatiques ITIL s'impose comme une démarche pour garantir une qualité de services informatiques.

ITIL développé par l'OGC britannique est adopté par les grandes entreprises internationales tant dans le secteur public que privé, est un référentiel des meilleures pratiques de la gestion des services informatiques.

2.1.2 Le principe d'ITIL

ITIL propose un cadre de développement structuré en processus et centré sur le client. Le client est en effet au cœur de l'approche. C'est le point fondateur de la démarche.

2.1.3 Les processus ITIL

ITIL décrit les processus suivants.

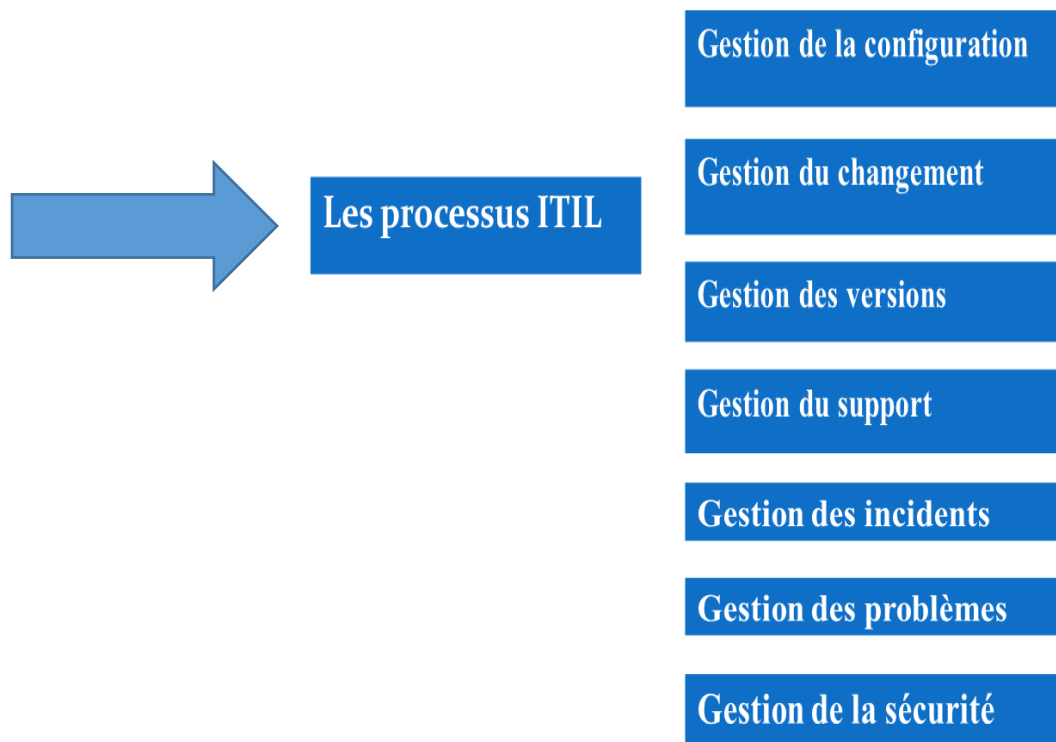


Figure 3. Processus ITIL

2.2 Règles d'implémentation de processus informatique.

Comme indiqué dans la figure ITIL décrit le service informatique sous forme d'un ensemble de processus structuré pour faciliter sa gestion.

L'implantation de tous ses services est compliquée car il nécessite de temps important et des procédures spécifiques qui doit être réalisé par la direction système d'information est validé par la direction Qualité et la direction général ce pour cette raison que la direction système d'information a décidé de commencer par l'implémentations des processus de gestion de configuration (inventaire), gestion des demande et des incidents reçus des utilisateurs ou à partir des systèmes de supervision .

2.2.1 Processus inventaire et Gestion de configurations

Selon ITIL, le but de la Gestion des Configurations est de fournir un modèle logique de l'infrastructure IT en identifiant, contrôlant, maintenant à jour et vérifiant les versions de tous les Eléments de Configuration (CI) existants. La Gestion des Configurations se positionne au cœur d'une gestion efficace des services informatiques. Ainsi, la Gestion des Configurations fournit un service d'information facilitant la planification, la Mise en Production et la mise en œuvre efficace et efficiente des Changements de service en informatique.

Le processus Gestion des biens et de configurations doit être appliqué conformément à règles suivantes.

- Chaque entité établit un inventaire des biens et le met à jour régulièrement pour chacun de ses Systèmes d'Information. Chaque bien doit être clairement identifié et documenté (localisation...) conformément aux recommandations du COSI.
- L'ensemble des applications installé sur les postes de travail doit être suivi et maitrisé.
- Une cartographie des applications est formalisée et régulièrement mise à jour en fonction des nouvelles applications et de celles sortant du périmètre. Cette cartographie applicative est nécessaire dans le cadre de projets structurants, comme la mise en place d'un Plan de Continuité d'Activité ou tout autre projet en lien avec un ensemble d'applications.
- Attribuer le niveau de protection requis pour chaque bien des Systèmes d'Information.

- Une classification qui attribue les besoins et priorités de protection est établie. Cette classification repose sur les 4 axes correspondant aux besoins en termes de Disponibilité, d'Intégrité, de Confidentialité et de Traçabilité (DICT). La classification des biens s'appuie sur la procédure opérationnelle de classification des biens.
- Il convient de classer les biens sensibles pour indiquer le besoin, les priorités et le degré souhaité de protection lors de leur usage.
- A tout bien, et en particulier toute information sensible, doit être associé sa classification de sécurité (sur les 4 axes DICT).
- La sensibilité d'un bien évolue dans le temps. Chaque responsable de biens des Systèmes d'Information doit donc périodiquement revoir la classification des biens dont il a la responsabilité.

2.2.2 Processus Gestion des incidents

La gestion des incidents est un processus inclus dans la démarche ITIL et ISO 20000.

La gestion des incidents est un processus de gestion du cycle de vie de tous les incidents. Elle s'assure que.

- l'exploitation normale des services soit rétablie le plus rapidement possible et que l'impact sur le business soit réduit au minimum.
- L'exploitation normale des services est définie dans l'accord sur les niveaux de service (SLA). Il décrit le service informatique, documente les cibles de niveau de service et spécifie les responsabilités du fournisseur de service informatique et du client

Il a pour objectif de :

- Garantir la mise en place d'une politique cohérente et efficace pour la gestion des incidents liés à la sécurité de l'information.
- Garantir la remontée des événements et failles de sécurité.
- Etablir un reporting sur les incidents de sécurité.
- Permettre la mise en œuvre d'actions correctives ou préventives dans les meilleurs délais.

Le processus gestion des incidents doit être appliqué conformément à règles suivantes :

- En cas d'infection (vers, virus, cheval de Troyes, ransomware), faille de sécurité ou incident de sécurité constatée ou soupçonnée sur un poste de travail, une procédure de réaction connue de tous les utilisateurs est mise en œuvre.
- Une surveillance permanente des systèmes, des alertes et des vulnérabilités est mise en œuvre afin de détecter les dysfonctionnements liés à la sécurité de l'information.
- Une synthèse des incidents de sécurité et des propositions d'actions pour les corriger ou les éviter est présentée trimestriellement par le RSSI au D.SI.
- La présentation de l'analyse des incidents de sécurité donne lieu pour chaque entité à un plan d'action (actions préventives ou curatives) permettant d'améliorer les mesures existantes et, selon le besoin, d'en créer de nouvelles.
- La supervision doit être liée aux processus de gestion des incidents. Ce lien s'applique notamment sur deux points.
 - génération atomique d'incident pour les alertes critiques fonctionnelles remontées par l'outil de supervision,
 - liaison direct avec la "knowledge base" de la gestion des incident.

2.2.3 Processus Contrôle d'accès au système d'information

Il permet de décrire le circuit pour la création, modification ou suspension des accès utilisateurs aux systèmes informatiques.

Il a pour objectif de :

- Garantir un contrôle efficace d'accès aux informations.
- Suivre et maîtriser les accès aux SI.
- Assurer la conformité entre les habilitations et l'existant.

Le processus Contrôle d'accès doit être appliqué conformément à règles suivantes :

- L'identification de la personne se connectant au réseau est effectuée de façon formelle et non ambiguë.

- Toute création, modification et clôture de compte (utilisateur, administrateur, service, etc.) doit pouvoir être suivie, tracée par le RSSI ou le référent sécurité de l'entité.
- Accès utilisateurs aux systèmes informatiques et téléphonique, à savoir.
 - Création, modification ou suppression d'un compte utilisateur sur le domaine.
 - Création d'une adresse email.
 - Création, modification ou suppression des accès aux applications IT.
 - Création ou désactivation d'un accès VPN (accès à distance).
 - Mise à disposition d'un ordinateur fixe ou portable lors d'un recrutement.
 - Mise à disposition d'une Ligne GSM business.
 - Suspension d'une ligne GSM Business.
 - Mise à disposition d'un appareil téléphonique.
 - Mise à disposition d'un accès aux lignes directes du standard téléphonique.
 - Suspension d'un accès aux lignes directes du standard téléphonique.
 - Récupération d'ordinateur fixe ou portable lors d'un départ ou changement de poste.
 - Mise à disposition d'un appareil téléphonique, tablette ou PDA.
 - Récupération d'un appareil téléphonique, tablette ou PDA lors d'un départ ou changement de poste.

3. Etude Technique des solutions :



3.1 Présentation GLPI :

GLPI (Gestion Libre de Parc Informatique) est une solution open-source de gestion de parc informatique et de helpdesk, GLPI est une application Full Web pour gérer l'ensemble des problématiques de gestion de parc informatique. De la gestion de l'inventaire des composantes matérielles ou logicielles d'un parc informatique à la gestion de l'assistance aux utilisateurs. Couplé à FusionInventory, l'inventaire complet de votre parc se fait automatiquement. Et tout devient paramétrable et gérable à partir d'une simple interface graphique Web comme par exemple la gestion des tickets pour le dépannage ou bien d'un planning pour l'emprunt du matériel (vidéoprojecteurs, portables...) et même déployer des logicielles est possible.

A. Architecture du GLPI :

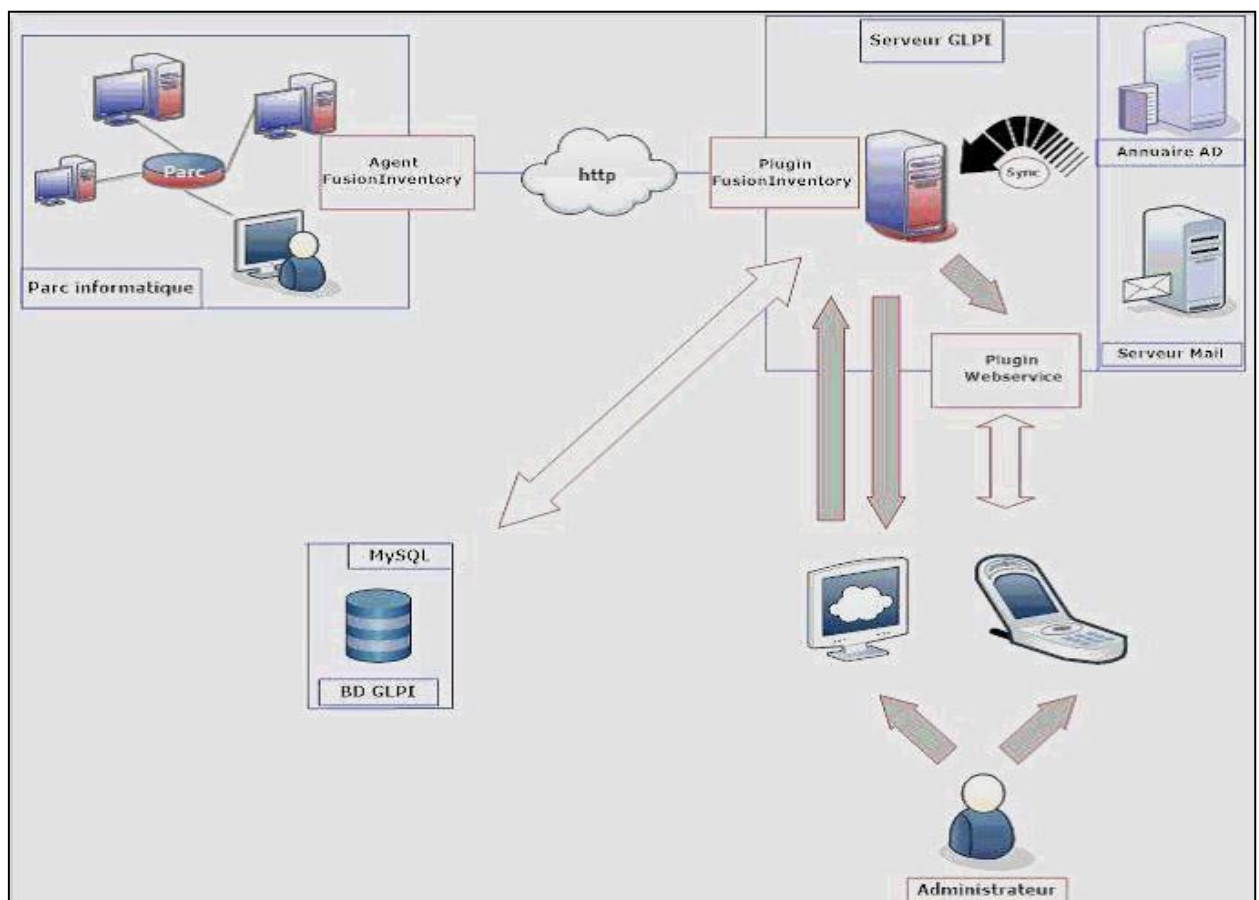


Figure 4. Architecture de GLPI

Les agents FusionInventory sont installés sur les machines du parc informatique.

Le plugin FusionInventory intégré dans le serveur GLPI permet de donner des informations sur des ressources physiques se trouvant dans le réseau du parc.

La communication entre l'agent et le serveur se fait via le protocole http ou https. En cas d'absence d'un agent, les équipements dans le réseau communiquent directement avec le serveur via le protocole SNMP. Les données de l'inventaire sont stockées dans la base de données de GLPI.

Le serveur GLPI effectue une synchronisation avec le plugin FusionInventory dans le but d'avoir des remontées automatisées des informations venant du parc.

Ce serveur effectue également une synchronisation avec Active Directory afin que chaque acteur à travers son compte Active Directory puisse accéder à l'interface graphique de GLPI et s'authentifier en tant qu'utilisateur, technicien ou administrateur.

La synchronisation des serveurs GLPI et de messagerie permet d'avoir un suivi de la gestion des tickets par mail.

B. Conception technique de GLPI :

GLPI est une solution multiplateforme qui peut être installé sur un environnement physique ou virtuelle Windows ou linux dans mon cas j'ai choisi l'environnement virtuel avec un système linux pour garantir le maximum de stabilité et de disponibilité de l'application.

Le fonctionnement de GLPI nécessite la présence de :

- D'un accès FTP pour l'installation de fichier.
- Serveur Apache avec PHP 5.0 ou plus.
- Serveur Base de données MySQL version 4.1.2 minimum.
- Un serveur Active directory pour authentification.
- Un serveur Mail pour l'envoi des alertes.



3.2 Présentation de la solution FAN :

Fan a été créé dans le but de réunir tous les outils les plus utilisés dans la communauté Nagios. Nagios (Anciennement appelé Net saint) et une application libre (sous licence GPL*) de supervision réseaux fonctionnant sur la plateforme qui permet de remonter les éventuels problèmes dans le parc informatique de manière rapide et spontanée. Il effectue des contrôles intermittents sur les hôtes et services en utilisant des plugins externes qui retournent un statut d'état à Nagios (4 états voir ci-après). Il peut envoyer des notifications de plusieurs manières. Email, SMS, Messagerie instantanée, etc... Une interface Web est en place ce qui facilite la lecture, et la supervision de n'importe quel poste (Avec une authentification lors de la connexion.) Il peut être complété de nombreux plug-ins qui le perfectionnent et le rendent encore plus compatibles avec certains matériels, et qui permet d'être bien plus performant pour la supervision. Il permet donc de :

- Superviser des services réseau. (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP, etc...).
- Superviser les ressources des serveurs (charge du processeur, occupation des disques durs, utilisation de la mémoire paginée) sur la plupart des systèmes d'exploitation.
- Interface avec le protocole SNMP.
- La supervision à distance peut utiliser SSH* ou un tunnel SSL*. [x] La vérification des services se fait en parallèle.
- Possibilité de définir une hiérarchie dans le réseau pour pouvoir faire la différence entre un serveur en panne et un serveur injoignable.
- La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins
- Acquiescement des alertes par les administrateurs.
- Gestion des escalades pour les alertes.
- Limitation de la visibilité, les utilisateurs peuvent avoir un accès limité à quelques éléments.
- Capacité de gestion des oscillations (nombreux passages d'un état normal à un état d'erreur dans un temps court).

- Chaque test renvoie un état particulier.
- OK (tout va bien)
- WARNING (le seuil d'alerte est dépassé)
- CRITICAL (le service a un problème)
- UNKNOWN (impossible de connaître l'état du service)

FAN est composé de :

- ❖ Centreon qui a été développé par une équipe Française.

Centreon permet de configurer Nagios via une interface web. En effet, le gros problème de Nagios est la configuration des hôtes et services. Sous Nagios, toute la configuration se réalise avec plusieurs fichiers de configurations. On doit écrire ligne par ligne chacun des hôtes et services, ce qui peut impliquer beaucoup de temps suivant le nombre important d'équipements à superviser.

Centreon permet de résoudre cette lacune tout en gardant les fonctionnalités du moteur de Nagios. Il gère également des modèles d'hôtes et de service, ce qui permet de dupliquer très rapidement les machines concernées. Ainsi, Le gain de temps avec Centreon est conséquent. Il permet de plus de générer automatiquement les fichiers « textes » de Nagios. Il ne reste par conséquent que l'écriture ligne par ligne à effectuer.

De plus, l'interface graphique proposée par Centreon est plus agréable que celle de Nagios, et entièrement francisée. Les données sont également mieux interprétées par Centreon, ce qui lui permet de proposer des graphiques beaucoup plus détaillés que sous Nagios.

- ❖ Nagvis : Module qui permet de créer des Schémas de la supervision. Il est possible de coupler Nagvis à un Schéma réseau et ainsi mettre en relation les données de Nagios en temps réel sur le schéma.

Pour suivre l'état des équipements Nagios utilise les plugins qui sont des programmes exécutables ou script (perl, shell,...) capables de fournir au moteur un code de retour qui est différent selon le seuil défini par l'administrateur. On définit 3 seuils

Seuil « **OK** », le seuil « **Warning** », et le seuil « **Critical** ».

Par exemple, lorsqu'on vérifie la CPU d'un serveur, on peut définir 2 seuils.



- Le seuil **Warning** à 80%
- Le seuil **Critical** à 90%.

Dès lors qu'un serveur dépasse 80% de charge CPU, Nagios émettra une alerte **Warning**, et une alerte **Critical** à 90% d'utilisation de CPU.

Il existe principalement deux types de plugins destinés aux serveurs, pour les serveurs Windows (nsclient++) et les serveurs linux (nrpe).

Pour les systèmes Windows.

NsClient est appelé aussi « Nsclient++ », il n'utilise pas le protocole de supervision SNMP, en fait il utilise ses propres données puisque le système est un système Client-serveur, comme le montre le schéma ci-dessous.

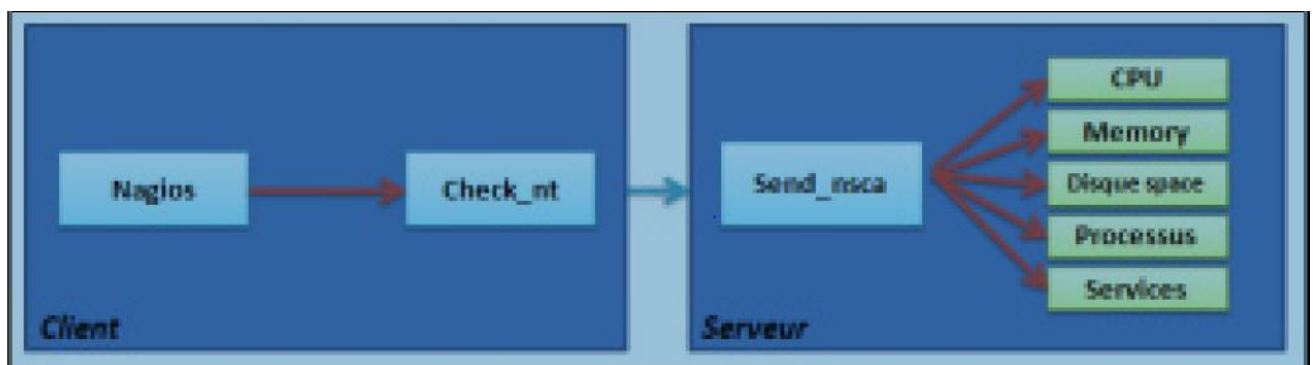


Figure 5.Plugin Nsclient

C'est un plugin qui permet de récupérer un nombre important d'informations. Il faut tout d'abord savoir que le logiciel Nsclient++ est destiné aux machines Windows. Il existe également un plugin destiné aux machines linux, présenté ci-dessous. La partie cliente (nommée **check_nt**), doit être présente sur le serveur Nagios. La partie serveur (**Nsclient++**) est à installer sur chacune des machines Windows à surveiller. Ce plugin permet de retourner de nombreuses informations telles que la charge de la CPU, la mémoire utilisée, ou encore l'espace disque...).

Pour les systèmes linux on utilise NRPE afin de mettre en place une supervision de machines. Le principe est le suivant :

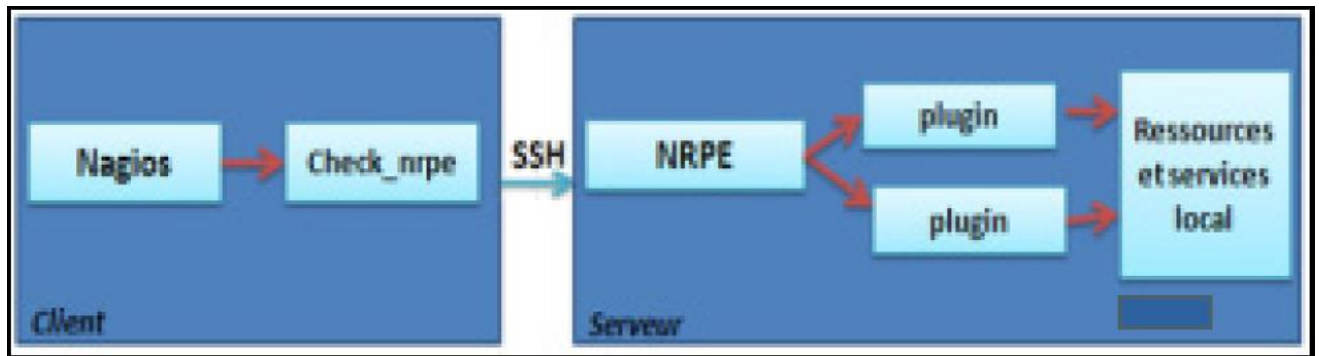


Figure 6. Plugin NRPE

Il est nécessaire de modifier les deux équipements, la machine hébergeant Nagios ainsi que les machines Linux à surveiller. Il faut aussi installer le démon NRPE sur la machine hôte Linux seulement. Afin de communiquer les deux machines utilisent un tunnel SSL pour crypter les informations. Une installation d'openssl (logiciel libre pour SSL) est donc indispensable sur les deux équipements.

Le protocole SNMP fonctionne sous forme de questions-réponses entre un serveur (dans notre cas Nagios) et des équipements réseau (hôtes) (Serveurs, Switch, Hubs, Ordinateur, routeurs...) ayant ce protocole installé.

Le client peut émettre un message vers le serveur sans nécessiter de réponse. Le message visant à alerter l'administrateur d'une défaillance (par exemple, l'espace disque d'un serveur ayant dépassé un seuil défini au préalable par le technicien).

Il peut récupérer toutes sortes d'informations sur l'état actuel d'un équipement réseau. Ces informations sont stockées dans une base de données arborescente appelée MIB (management information base). Ce protocole n'est plus l'unique moyen de supervision. En effet les logiciels de supervision d'aujourd'hui tendent vers l'utilisation d'agents propriétaires afin de remplacer le protocole SNMP et ce dans le but de fournir toujours plus d'informations à l'utilisateur. Cependant le protocole SNMP reste le seul moyen de surveiller l'activité d'équipements réseaux tels que les commutateurs ou les routeurs, étant donné que ces matériaux offrent rarement la possibilité d'installer des logiciels tiers.

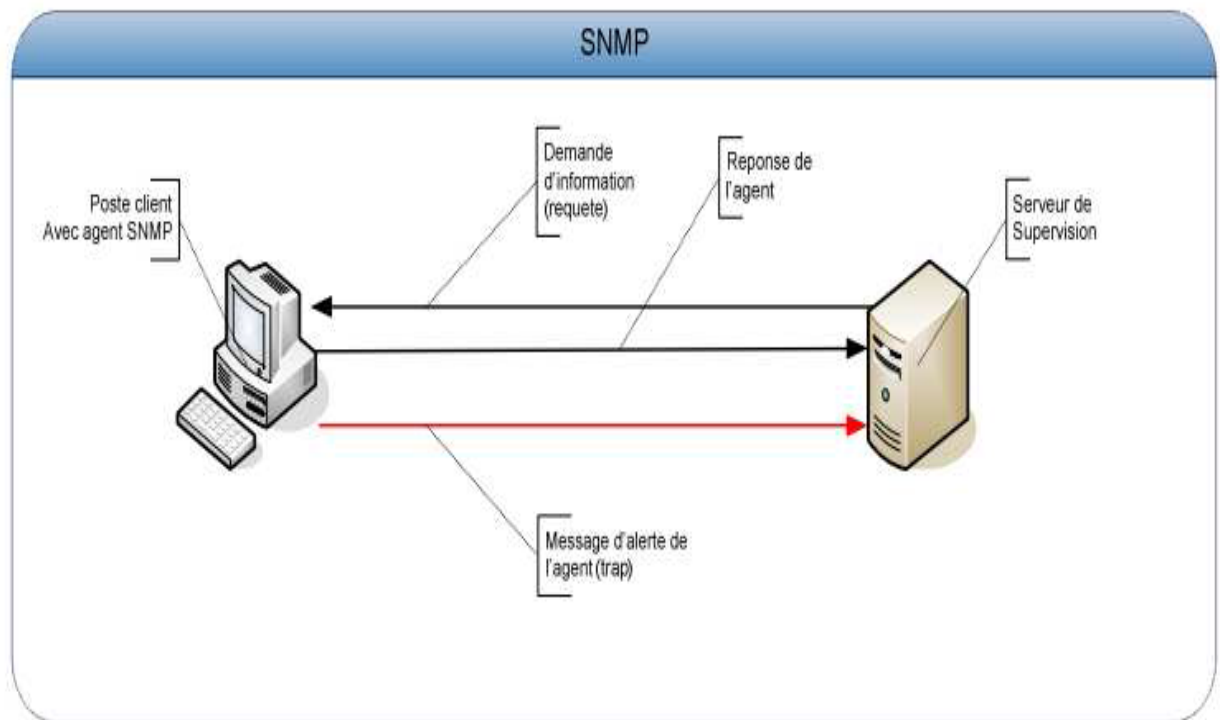


Figure 7. Protocol SNMP

A. Architecture de FAN

L'architecture du composant Nagios est présentée dans le schéma suivant :

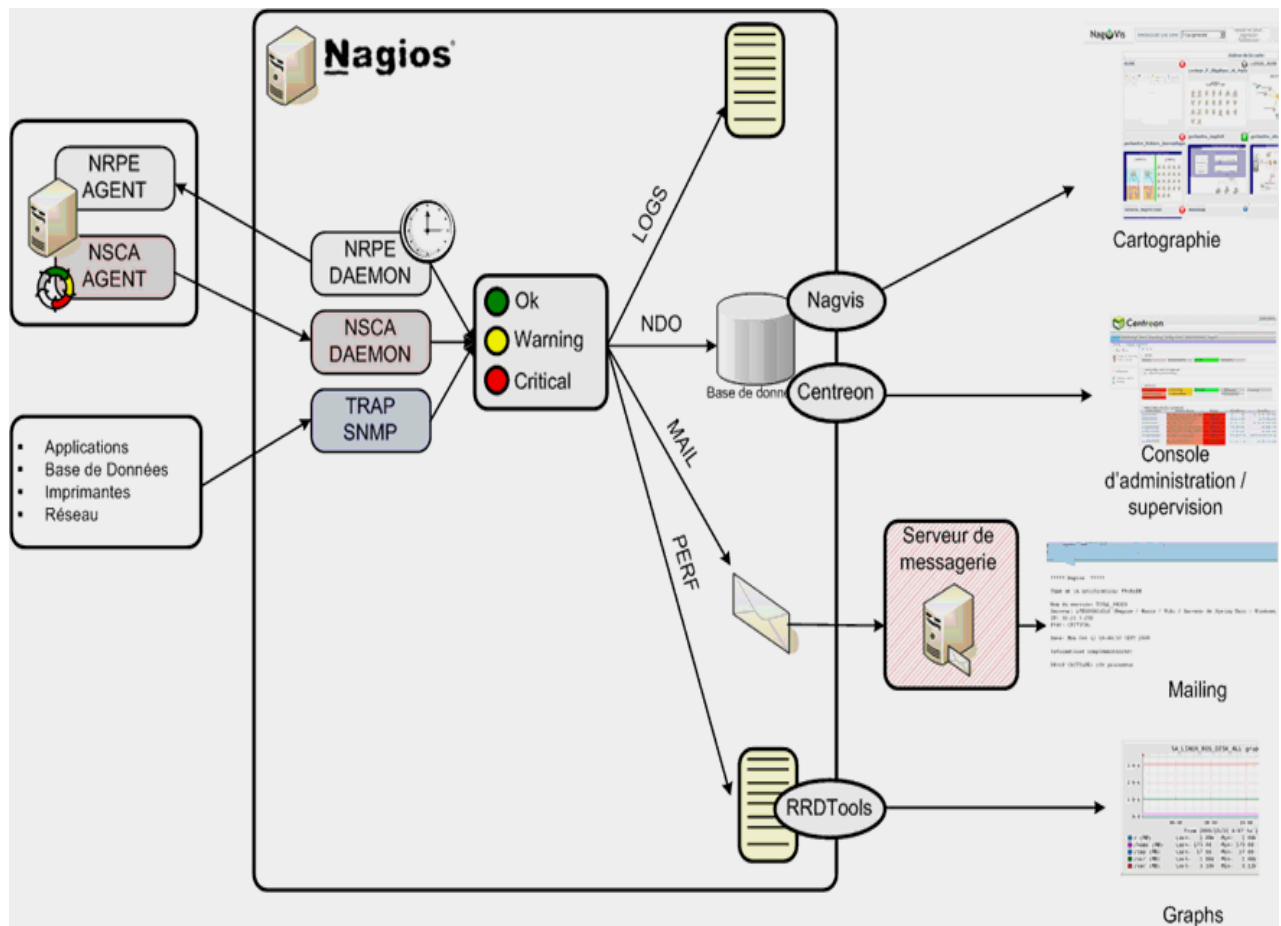


Figure 8. Architecture de FAN

La supervision est réalisée de différentes manières.

- Déploiement d'un agent NRPE sur les serveurs qui communique avec Nagios et déclenche à la demande de Nagios des check locaux et transmet le résultat.
- Déploiement d'un agent NSCA sur les serveurs qui déclenche de lui-même des check locaux et transmet le résultat.
- Le serveur Nagios est à l'écoute de communication SNMP pouvant être déclenché par certains composants actifs du SI comme (BD, imprimante, switcher)
- Le serveur NAGIOS peut déclencher des checks distant par le biais du serveur SSH.

Le serveur Nagios analyse les remontées des check et alimente différents moyens de communication

La base NDO est ensuite utilisée comme source de données pour des interfaces web de visualisation des check (Nagios, Centreon) et des interfaces web de visualisation de cartographies (Nagvis).

Les graphs RRD sont utilisés comme source de données pour des interfaces web de visualisation (Nagiosgrapher, Centreon, PNP).

Conclusion

Ce chapitre nous permis de mettre en amont les phases nécessaires à la réalisation de notre application. L'architecture et les composants du système a cette étape sont démontrés avant de passer au chapitre suivant où nous allons parler sur le test et l'implémentation de la solution.

***Chapitre 4 :
Implémentation
et test de La
Solution***

Introduction

Dans cette partie de projet je vais entamer la partie réalisation dans laquelle je vais mettre en pratique ce qui déjà vu précédemment.

Je vais commencer par une description de l'architecture globale de solution puisque mon projet est composé de deux parties différentes Nagios et GLPI.

Dans une deuxième partie je vais présenter l'environnement matériel et logiciel et je finirai par l'installation et le test et validation.

1 Architecture Adopté :

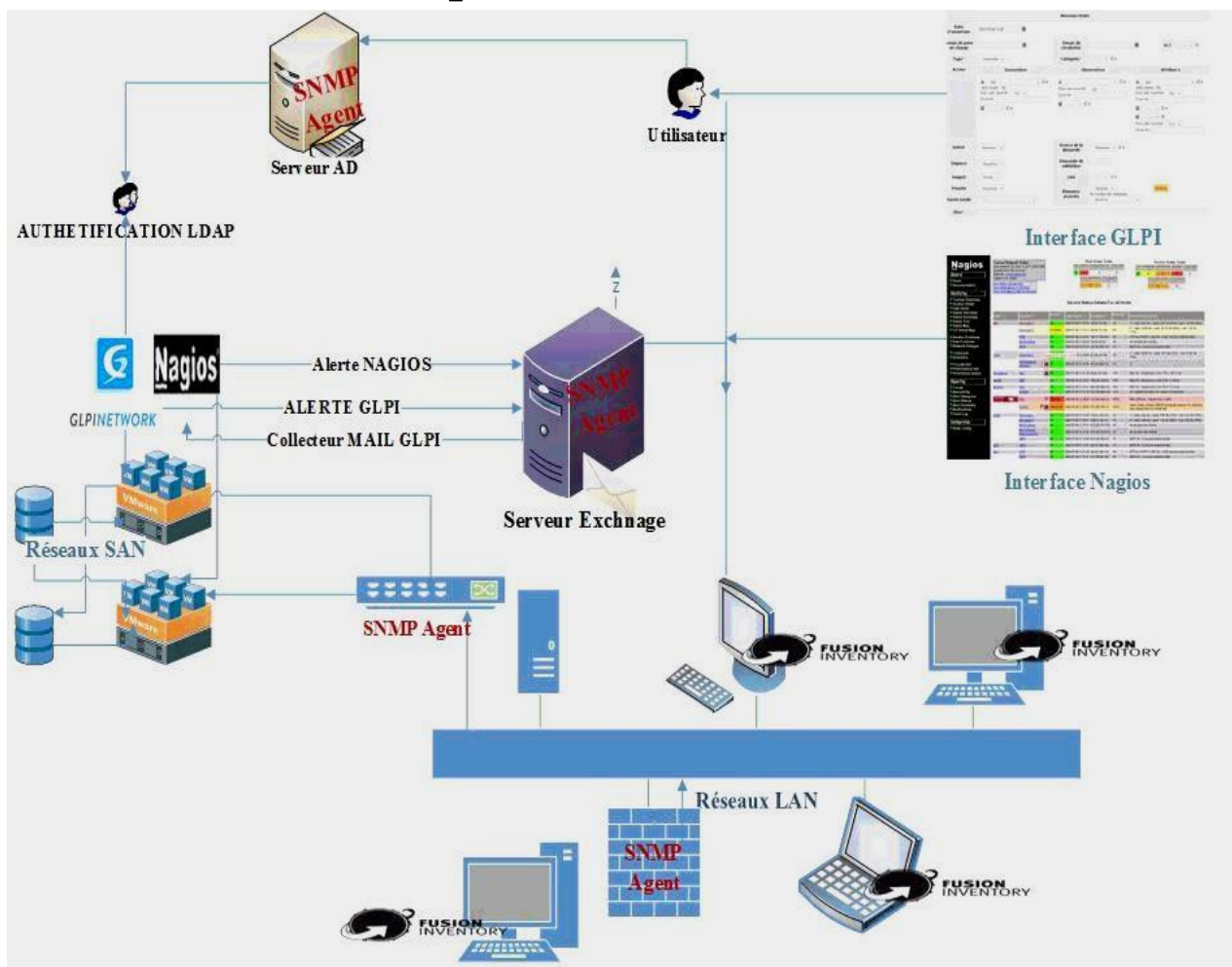


Figure 9. Architecture adopté

La figure présente l'architecture globale de solution de gestion de parc informatique et de supervision .un utilisateur s'authentifie sur le serveur GLPI à travers ses

paramètres AD pour exploiter le système selon ses droits (administrateur, technicien ou simple utilisateur).

L'utilisateur GLPI peut ouvrir un ticket soit directement à travers l'interface GLPI, par Email dans ce cas il envoie un mail de support à travers le serveur Exchange, le serveur GLPI récupère l'Email par son collecteur et le transforme en un ticket GLPI.

Les agents fusion inventory et snmp sont utilisés pour réaliser les inventaires et suivre l'état des différents équipements actifs sur les réseaux.

Lorsqu'un événement est détecté par le système de supervision sur un équipement ce dernier envoie un message d'alerte à l'administrateur à travers le serveur Exchange, ce mail peut être récupéré par le collecteur de GLPI et un ticket incident va être créé.

2 Environnement de travail

2.1 Environnement matériel

Suite à l'optimisation de notre plateforme virtuelle par l'extension au niveau RAM et stockage nous avons décidé d'implémenter notre solution sous forme d'une machine virtuelle.

L'installation se fait sur un serveur Power Edge R720 avec la configuration suivante :

- 2 x Intel Xeon E5-2650 2.00GHz, 20M Cache, 8.0GT/s QPI, Turbo, 8C, 95W, DDR3-1600MHz
- 8 x 16GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4
- 2 x 146GB, SAS 6Gbps, 2.5-in, 15K RPM Hard Drive (Hot-plug)
- PERC H310 Integrated RAID Controller, 1GB NV Cache
- Broadcom 57800 2x10Gb DA/SFP+ +2x1Gb BT Network Daughter Card
- Broadcom 57810 DP10Gb DA/SFP+ Converged Network Adapter



Figure 10. server power Edge r720

Le serveur Power EDGE R720 est géré par un hyperviseur VMware ESXi 5.5 est administré par VMWARE VCenter 5.5 et VMWARE vClient 5.5

2.2 Environnement Logiciel

Concernant la partie logicielle j'ai choisi d'utiliser la distribution FAN (Fully Automated Nagios)

C'est une distribution linux centos sous forme d'un pack de logicielle désigné pour la supervision.

La compilation FAN possède la liste des logicielle suivants .

- Nagios :pour la supervision
- Centrerons :pour faciliter l'administration de Nagios
- MySQL :serveur de base de donné
- Apache :serveur WEB
- Le plugin NDOutils : pour le stockage des données de Nagios dans la base de données

Avec tous ses composants j'ai besoin de :

- plugin NS Client pour la supervision des serveurs Windows.
- Le plugin NRPE pour la supervision des serveurs Linux

Pour la partie gestion de parc et help desk l'idée et d'ajouter GLPI a la compilation de FAN Nagios pour avoir une solution complète de gestion et de supervision de parc informatique.

2.3 Présentation et validation de la solution

Je vais valider dans cette partie de projet le respect de ma solution aux besoins fonctionnels exprimés dans le cahier de charge.

2.3.1 Sécurité et authentification

Pour utiliser l'application (Nagios ou GLPI) il faut passer par une interface d'authentification.

Pour GLPI plusieurs utilisateurs accèdent au système en tapant le login et mot de passe de session Windows (Authentification AD).

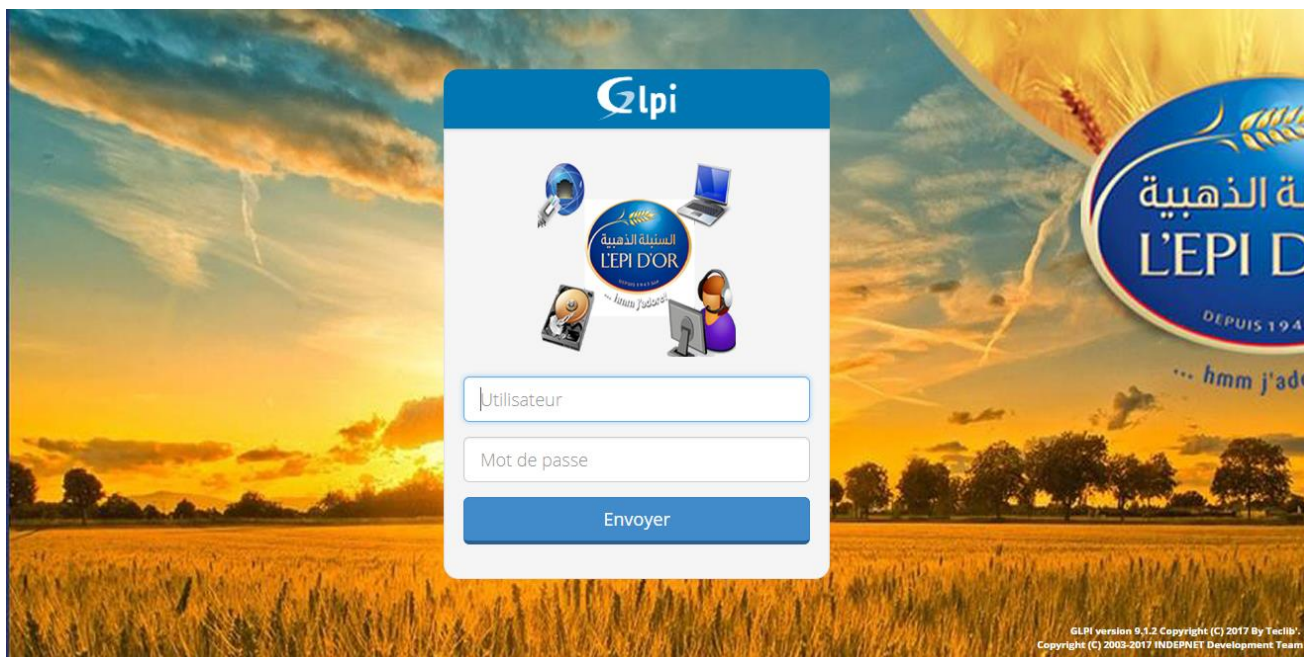


Figure 11. Authentification GLPI

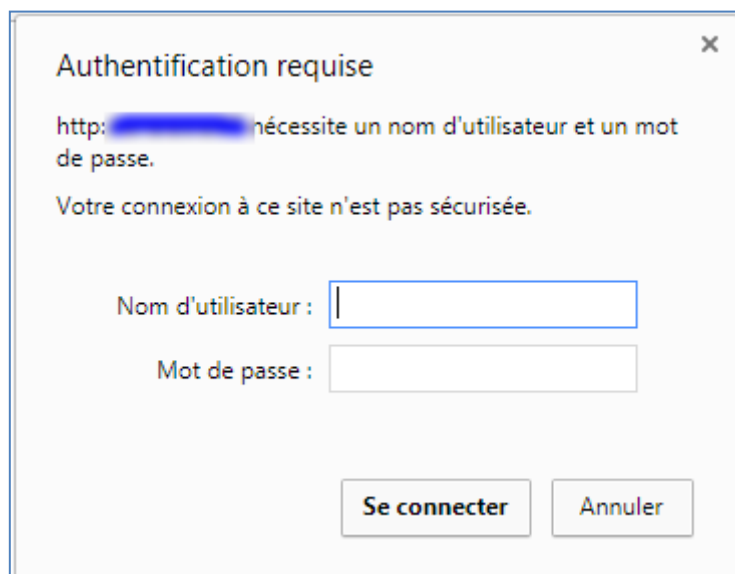


Figure 12. Authentification NAGIOS

2.3.2 Processus gestion de la configuration et inventaire

L'inventaire de parc est une partie intéressante dans GLPI elle est réalisée par l'interaction entre les plugins GLPI fusion-inventory et les agents fusion-inventory et SNMP installé sur les différents équipements de réseaux.



a. Inventaire des postes clients

	Nom	Réseau - IP	Utilisateur	Groupe	Lieu	Commentaires	Dernière modification	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation	Composants - Processeur	Composants - Fréquence du processeur
					Direction technique minoterie		2017-07-27 09:07	Affecté	Dell Inc.	H80XB82	Mini Tower	OptiPlex 3020	Windows	Intel(R) Core(TM) i3-4150 CPU @ 3.50GHz	3 500 MH
					Direction qualité		2017-07-26 10:20	Affecté	Dell Inc.	DC01T4J	Mini Tower	OptiPlex 380	Windows	Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz	2 930 MH
					Laboratoire		2017-07-26 08:15		HP	CND6093MD5	Notebook	HP Notebook	Windows	Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz	2 200 MH
					Magasin PDR		2017-07-26 07:50	Affecté	Dell Inc.	8J9074J	Mini Tower	OptiPlex 760	Windows	Intel(R) Core(TM)2 Duo CPU E7300 @ 2.66GHz	2 660 MH

Figure 13. Inventaire des PC

Après avoir installé les agents Fusion-Inventory sur le poste clients, les caractéristiques de ce dernier (Modèle, type, RAM, Processeur, logiciel....) sont envoyés au serveur GLPI,

b. Inventaire des imprimantes

Canon LBP6020	Usines pâtes spéciales	2017-05-22 13:44	Non	Non	Oui	Non	Non	0000B1D1KBHe
EPSON L220 Series	Direction GMA	2017-05-20 11:27	Non	Non	Oui	Non	Non	574E32503030303766
Canon LBP2900	Direction GMA	2017-05-20 11:27	Non	Non	Oui	Non	Non	0000B183ENN9
EPSON LQ-590 ESC/P2 (Copie 2)	Direction GMA	2017-05-24 07:32	Non	Non	Oui	Non	Non	
Canon LBP6310 (Copie 1)	Direction GMA	2017-07-20 08:10	Non	Non	Oui	Non	Non	2C9EFC1DC356
HP Color LaserJet Pro MFP M176 PCLmS	Direction GMA	2017-07-23 13:59	Non	Non	Oui	Non	Non	CNG7H7G9PR
EPSON LX-350 ESC/P	Direction EDEX - EDIS CO	2017-07-21 07:28	Non	Non	Oui	Non	Non	003081511041501420

Figure 14. Inventaire des imprimantes

Les agents fusion-inventory envoi au serveur GLPI les équipements connectés aux postes de travail tel que les imprimantes avec des informations intéressantes comme le modèle et le numéro de série qui nous permet de suivre sa durée de vie.

c. Inventaires des logiciels

	Nom	Éditeur	Versions - Nom de la version	Versions - Système d'exploitation	Licences - Nombre d'installations	Licences - Nombre de licences	Licences - Numéro de série de la licence
	VNC Enterprise Edition E4.5	RealVNC Ltd.	E4.5		0	0	
	Intel(R) Management Engine Components	Intel Corporation	9.5.13.1706 9.5.23.1766 7.1.70.1205 11.5.0.1020 1.0.0.0 11.0.0.1167 8.1.0.1252 11.0.0.1163 11.0.6.1194	Windows	37	0	
	Adobe Reader 9.4.0 - Français	Adobe Systems Incorporated	9.4.0	Windows	6	0	
	Microsoft SQL Server 2005 Express Edition	Microsoft Corporation	9.3.4035.00 9.4.5000.00	Windows	0	0	
	KMSpico v9.2.3		9.2.3	Windows	5	0	
	NVIDIA PhysX System Software 9.15.0428	NVIDIA Corporation	9.15.0428	Windows	1	0	

Figure 15. Inventaire de Logiciel

La figure ci-dessus nous donne les informations sur les logiciels installés sur notre parc tel que l'éditeur, la version, le nombre d'installation et le nombre de licence de chaque logiciel inventorié.

d. Inventaires des équipements réseaux

Liste...
Matériel réseau - SW-CORE-UNPA
8/10
>
>

Matériel réseau

Nom	SW-CORE-UNPA	Statut	----- ⓘ +
Lieu	Direction générale ⓘ +	Type	cisco ⓘ +
Responsable technique	----- ⓘ	Fabricant	cisco ⓘ +
Groupe technique	informatique ⓘ +	Modèle	Catalyst 3750-24/48 ⓘ +
Usager numéro		Numéro de série	FDO1811ZDJU
Usager		Numéro d'inventaire	
Utilisateur	----- ⓘ	Réseau	----- ⓘ +
Groupe	informatique ⓘ +		
Domaine	LEPIDOR ⓘ +		
L'adresse MAC et l'adresse IP de l'équipement sont inclus dans un port réseau agrégé		Commentaires	
Firmware	12.2(55)SE5 ⓘ +		
Mémoire (Mio)	256		

FusionInventory

Figure 16. Caractéristique d'un switch Cisco

[Légende]											
Nom	MTU	Vitesse	Statut Interne	Dernier changement	Trafic reçu/envoyé	Erreurs reçues/encoyées	Duplex	MAC interne	VLANs	Connecté à	Conn
Po10	Agrégation de port	1500	10 Mbps	●	57.57 seconds	- / -	- / -		[0] U *		
Gi1/0/23		1500	1 Gbps	●	1 minute, 17.42	1 Go / 2 Go	- / -	Full	64:12:25:54:f8:97	informatique a4:0c:c3:92:2c:b1	
Gi1/0/24		1500	1 Gbps	●	1 minute, 17.67	29 Mo / 3 Go	- / -	Full	64:12:25:54:f8:98	informatique a4:0c:c3:92:2c:b2	
Po60	Agrégation de port	1500	10 Mbps	●	57.58 seconds	- / -	- / -		[0] U *		
Gi1/0/10		1500	1 Gbps	●	1 minute, 19.32	2 Go / 4 Go	- / -	Full	64:12:25:54:f8:81	SW-Bridge 18:ef:63:f6:89:83	
Gi1/0/20		1500	1 Gbps	●	1 minute, 17.61	2 Go / 833 Mo	- / -	Full	64:12:25:54:f8:82	SW-Bridge 18:ef:63:f6:89:86	
Gi1/0/30		1500	1 Gbps	●	1 minute, 16.82	2 Go / 833 Mo	- / -	Full	64:12:25:54:f8:83	SW-Bridge 18:ef:63:f6:89:88	
Gi1/0/40		1500	1 Gbps	●	1 minute, 16.87	2 Go / 833 Mo	- / -	Full	64:12:25:54:f8:84	SW-Bridge 18:ef:63:f6:89:82	

Figure 17. Configuration des ports d'un Switch Cisco

Pour réaliser l'inventaire des équipements réseaux fusion inventory pour GLPI utilise le protocole SNMP pour récupérer les informations sur les équipements réseau

Dans mon cas j'ai récupérer les informations sur mes switch Cisco le nom, l'adresse IP, le modèle, la version de système d'exploitation ainsi que l'état des ports et sa liaison avec les différents équipements de parc informatiques.

e. Inventaire des hôtes VMWARE :

Liste des machines virtuelles								
Nom	Inventaire automatique	Système de virtualisation	Modèle de virtualisation	État de la machine virtuelle	UUID	Nombre de processeurs	Mémoire (Mio)	Machine
VMware ESXi 5.5U1	Oui	VMware		running	564de385-a2c0-83d8-895c-6c409d0b1333	8	16384	
VMware ESXi 5.5U1	Oui	VMware		running	421e18fd-7a15-7053-9445-d17a2faf1c6c	4	12288	
VMware ESXi 5.5U1	Oui	VMware		running	421c5f85-95fa-240c-e9d2-3bb939802427	2	4096	
VMware ESXi 5.5U1	Oui	VMware		running	564d0bdf-015d-71a0-244e-f8616614ee3b	8	12288	
VMware ESXi 5.5U1	Oui	VMware		running	564d7bf3-9266-27e5-fb58-555ad1d80e8f	4	8192	
VMware ESXi 5.5U1	Oui	VMware		running	421c1c8f-dc9d-7fbc-a8b8-adaa39a2af79	2	4096	
VMware ESXi 5.5U1	Oui	VMware		running	564dde5f-55a7-4091-1789-61b9fbfde573	2	8192	
VMware ESXi 5.5U1	Oui	VMware		running	421eba01-d24d-a3fa-bdef-e7a992fc4a0b	4	16384	
VMware ESXi 5.5U1	Oui	VMware		running	4236c12e-a841-47cb-e276-c84d026b5875	16	32768	
VMware ESXi 5.5U1	Oui	VMware		running	564d8b21-c905-4334-5cc4-34de3f782cf8	8	16384	
VMware ESXi 5.5U1	Oui	VMware		running	421e8739-543d-9cce-096e-0b1ef7754ec6	16	32768	
Nom	Inventaire automatique	Système de virtualisation	Modèle de virtualisation	État de la machine virtuelle	UUID	Nombre de processeurs	Mémoire (Mio)	Machine

Figure 18. Inventaire des hôtes VMWARE

Cette partie d’inventaire permet de récupérer les informations sur les hôtes VMware ESXi, (Modèle, composant, et les états des machines virtuelle qui le support).

2.3.3 Processus Gestion des incidents

a. Demande d'intervention et création de ticket

Ce ticket me concerne

Suivi par courriel

Courriel :

Description de la demande ou de l'incident

Type*

Catégorie*

Urgence

Le ticket porte sur

Ou recherche complète

Lieu

Observateurs

Courriel :

Titre*

Formats

Description*

Fichier (128 Mio maximum)

Figure 19. Interface Création de ticket

Avec notre système GLPI, un utilisateur qui a eu un incident informatique peut envoyer une demande d'intervention au service informatique en remplissant le formulaire nouvelle ticket ci-dessous ou en envoyant directement un mail sur adresse mail support@lepidor.com.tn qui va être transformé par la suite en ticket mail à travers le collecteur mail de GLPI.

b. Traitement de ticket par administrateur

Accueil

Assistance

Tickets

+

Q

≡

✓

LEPIDOR

Ticket

Traitement du ticket 0

Statistiques

Validations

Éléments

Coûts

Tâches de projet

Problèmes

Changements

Historique 2

Processus - Cas

Tous

Ticket - ID : 29 (LEPIDOR)

Date d'ouverture2017-07-27 13:10

Temps de prise en charge

Parglpi

TypeIncident

StatutNouveau

UrgenceMoyenne

ImpactMoyen

PrioritéMoyenne

Temps de résolution

Dernière modification2017-07-27 13:11 par glpi

CatégorieLogiciel > Bureautique

Source de la demandeHelpdesk

ValidationNon soumis à validation

Lieu

Éléments associés

Ajouter

Acteur

Demandeur +

Observateur +

Attribué à +

Utilisateur

glpi

normal

tech

ACHEK Karim

BAHRI Sami

Titre

installation Microsoft office 2016

Figure 20. Interface Attribution d'un ticket

Un utilisateur autorisé à modifier un ticket généralement un administrateur peut vérifier tous les tickets en cours, l'attribuer entre les techniciens selon la catégorie et la priorité en lui indiquant le temps de résolution.

Les techniciens vont être notifiés par mail sur les nouvelles tâches attribuées.

c. Traitement d'un ticket par un technicien

ID	Titre	Statut	▼ Dernière modification	Date d'ouverture	Priorité	Demandeur - Demandeur	Attribué à - Technicien	Catégorie	Temps de résolution
29	installation Microsoft office 2016	En cours (Attribué)	2017-07-27 13:20	2017-07-27 13:10	Moyenne	glpi	BAHRI Sami	Logiciel > Bureautique	
26	Ligne GSM	En cours (Attribué)	2017-04-17 10:08	2017-04-17 10:00	Moyenne	glpi	BAHRI Sami		2017-04-17 22:00
ID	Titre	Statut	▼ Dernière modification	Date d'ouverture	Priorité	Demandeur - Demandeur	Attribué à - Technicien	Catégorie	Temps de résolution

Figure 21. Interface Ticket attribué

Figure 22. Interface Résolution de ticket

Après résolution de ticket, le technicien doit changer l'état de son ticket de l'état attribué à l'état résolu et doit décrire la solution et enregistrer le type de la solution .il peut aussi enregistrer la solution dans la base de connaissance pour les partager avec des autre techniciens et le garder en historique.

Après enregistrement le demandeur de ticket va être notifié par mail sur la résolution de son ticket pour accepter ou refuser la solution.

2.3.4 Processus Contrôle d'accès au système d'information

Pour réaliser cette partie de projet j'ai utilisé le plugin GLPI « **Formcreator** » pour créer des workflow qui permet de contrôler les demandes d'accès au système d'information.

« **Formcreator** » permet la création des formulaires personnalisés simples d'accès aux utilisateurs aboutissant à la création d'un ou plusieurs tickets GLPI, il a pour fonctionnalités :

- Accès par menu direct en interface self-service
- Mise en avant de formulaires en pages d'accueil
- Accès des formulaires contrôlés. accès public, accès utilisateurs identifiés, accès restreint à certains profils

- Des formulaires simples et personnalisables
- Des formulaires organisés par catégories, par entités et par langues.
- Des questions ouvertes ou fermées, de tout type de présentation. Champs textes, listes, LDAP, fichiers, etc.
- Organisation des questions par sections. Choix de l'ordre d'affichage.
- Possibilité de n'afficher une question que selon certains critères (réponse à une autre question)
- Un contrôle pointu sur les réponses de formulaires. Texte, nombres, taille des champs, e-mail, champs obligatoires, expressions régulières, etc.
- Création d'un ou plusieurs tickets ou changements à partir des réponses aux formulaires
- Ajout de description par champs, par section de questions, par formulaires, par entités et langues.
- Formatage du/des ticket(s) créé(s). réponses aux questions à afficher, gabarits de tickets.
- Prévisualisation du formulaire créé directement dans la configuration.

Parmi le workflow demandé par la direction système d'information un workflow gestion des demandes de création ou modification des droits d'accès, workflow Demande ligne GSM et un workflow de Mise à disposition matériel IT

a. Création de formulaire

Le formulaire demandé comporte les champs type de la demande (Nouveau, suppression, modification), ...

La demande est renseignée en premier lieu par le directeur du département est validé par direction ressources humaines.

Après validation, un ticket sera créé automatiquement.

Demande ligne et Forfait GSM

Type demande

Demande *

☒ Nouveau
☐ Suppression
☐ Modification

Demande ligne GSM

Matricule

Nom et prénom

Société

U.N.P.A

Forfait GSM

Connexion internet

☒ Non
☐ Oui

Choisissez un valideur *

Envoyer

Figure 23. Formulaire demande Ligne GSM

a. Connexion au formulaire :

Connecter à l'interface GLPI avec votre login et mot de passe actuel, dans le cas où le formulaire n'est pas affiché par défaut sur la page d'accueil.

Ci-dessous comment passer de profil par défaut « self-service » au profil « form-crédation ».



+ 9 6 0 ? ★ BAHRI Sami ⚙

Accueil Créer u... Tickets Réservations Foire aux ques...

Créer un ticket +

Tickets	Nombre
Nouveau	1
En cours (Attribué)	2
En cours (Planifié)	0
En attente	0
Résolu	15
Clos	26
Supprimé	6

Notes publiques

Flux RSS publics

Self-Service

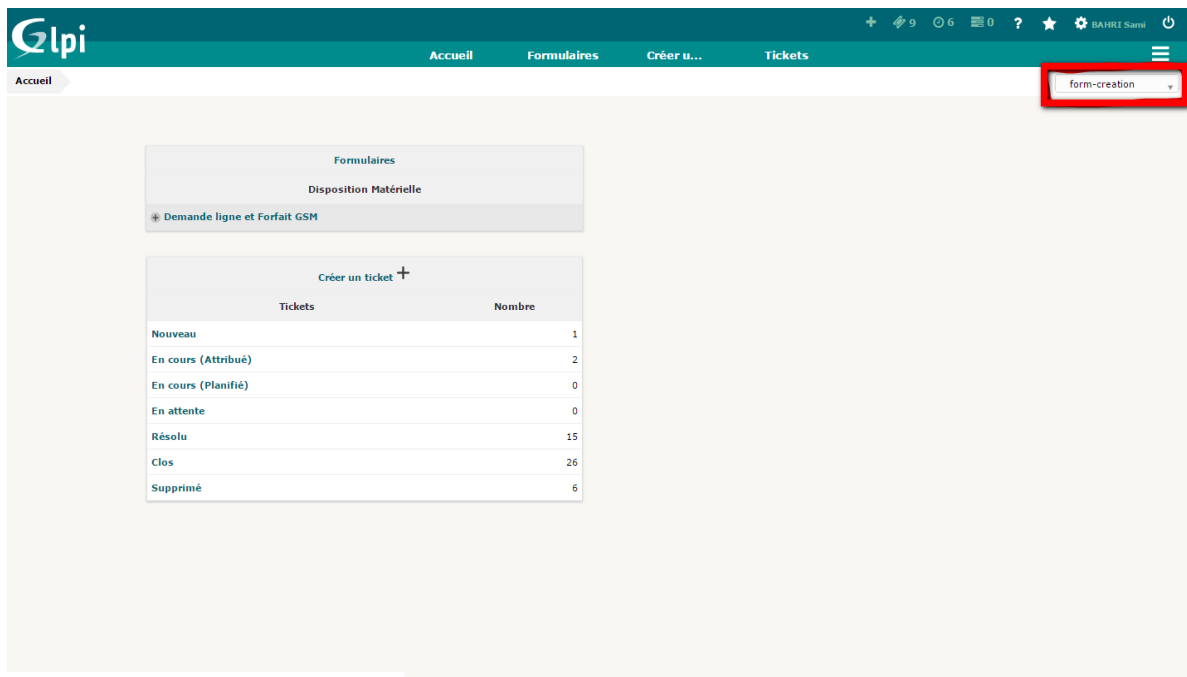


Figure 25. Profil form-creator

Le menu formulaire apparaît

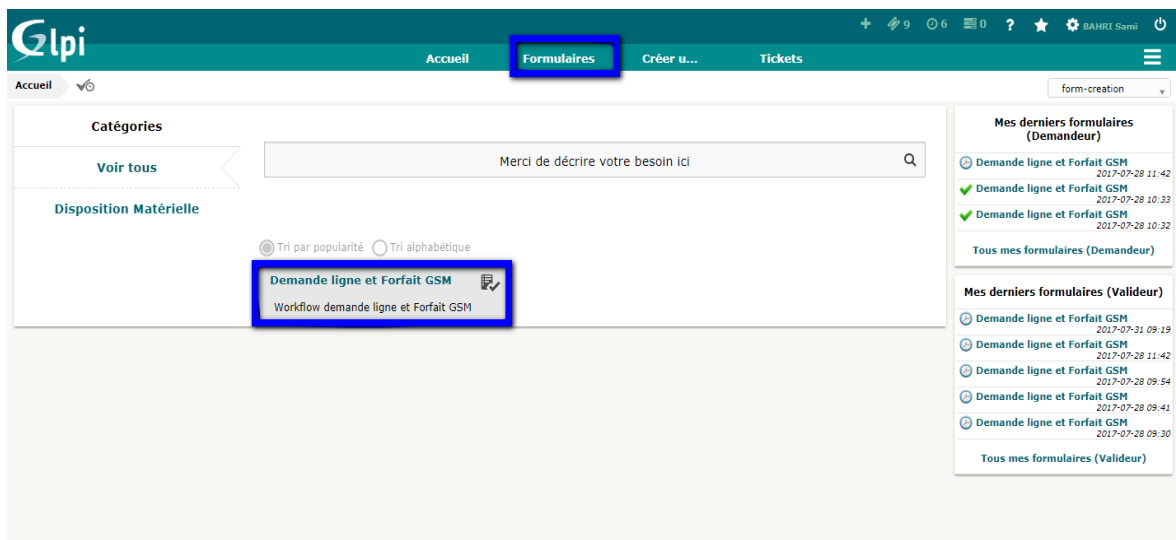


Figure 26.interface d'accueil Formulaire

b. Remplissage de formulaire

Ouvrir le formulaire, remplir les champs nécessaires (nouveau, modification ou suppression) d'une ligne GSM.

Finalement choisir le validateur et cliquez sur envoyer.

The screenshot shows a web form titled "Demande ligne et Forfait GSM" with a printer icon. The form is divided into several sections:

- Type demande**: A section with three radio buttons: "Nouveau" (selected), "Suppression", and "Modification".
- Demande ligne GSM**: A section containing several input fields:
 - Matricule**: A text input field containing "2276".
 - Nom et prénom**: A text input field containing "Bahri Sami".
 - Société**: A dropdown menu showing "U.N.P.A".
 - Forfait GSM**: A dropdown menu showing "60".
 - Connexion internet**: Two radio buttons, "Non" (selected) and "Oui".
 - Choisissez un valideur ***: A dropdown menu showing "-----".
- Envoyer**: A yellow button at the bottom right of the form.

Figure 27. Remplissage d'un formulaire

c. Validation et suivi de Formulaire par E-mail Notification

Le validateur reçoit une notification par E-mail qui indique un formulaire GLPI est en attente de validation.

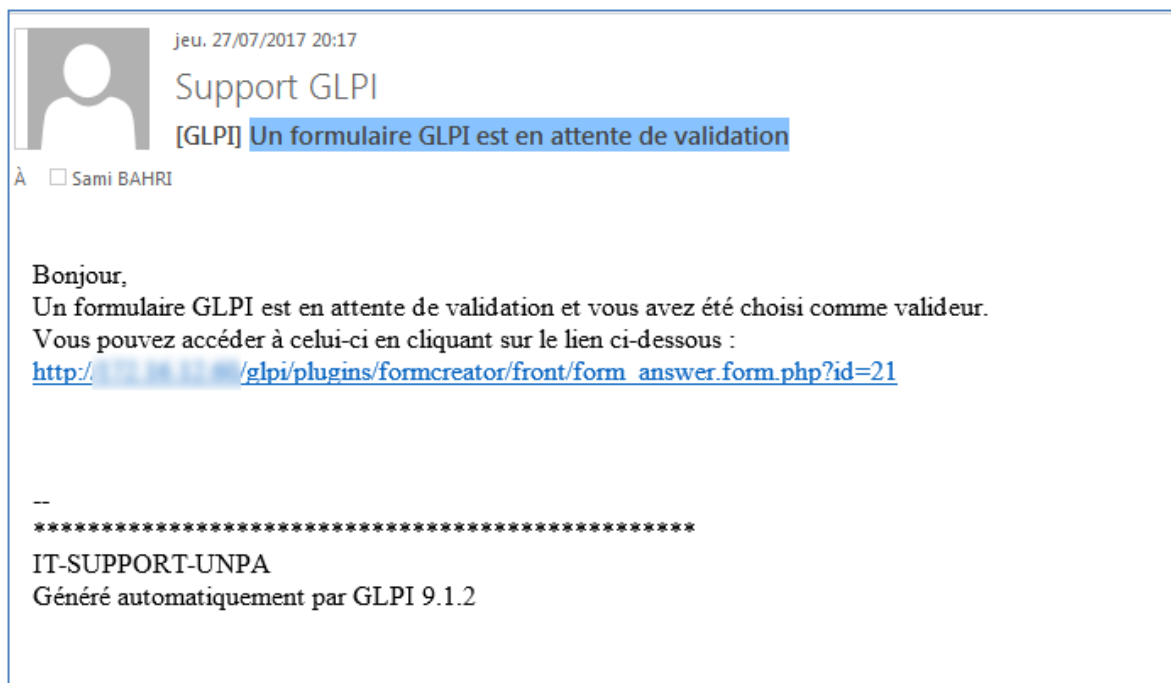


Figure 28. Notification Formulaire en attente

Vous pouvez accéder directement à celui-ci en cliquant sur le lien pour accepter ou refuser la demande, en cas de refus il faut décrire la raison dans les champs commentaire.

Figure 29. Validation d'un formulaire

Après acceptation ou refus le demandeur reçoit une alerte par mail lui indiquant l'état de ça demande.

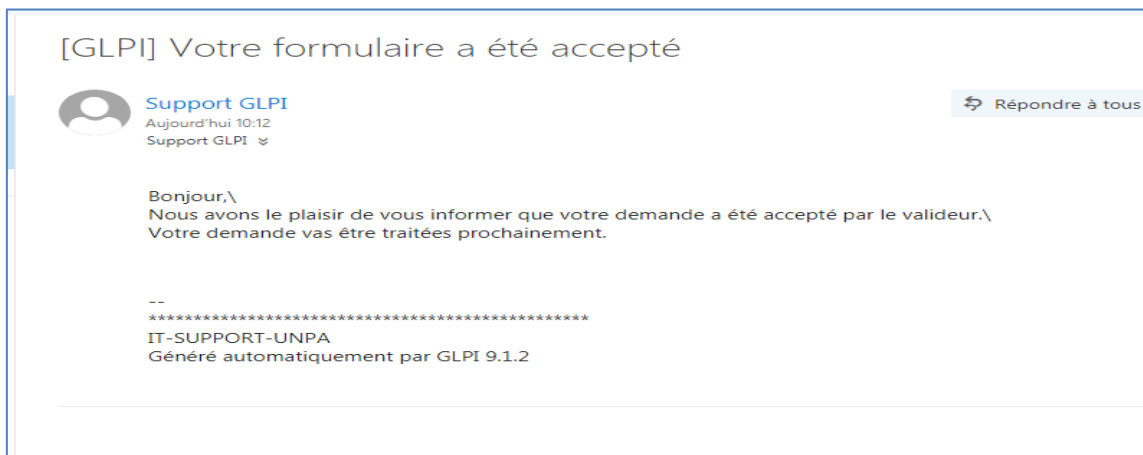


Figure 30. Notification état d'un formulaire

d. Validation et suivi de Formulaire par l'interface GLPI

Dans le cas où on n'pas reçu un mail de notification sur le formulaire on peut faire le suivi de ce dernier à partir de l'interface GLPI.

Pour faire le suivi des formulaires **demandeurs** on doit cliquer sur ce dernier à droite.

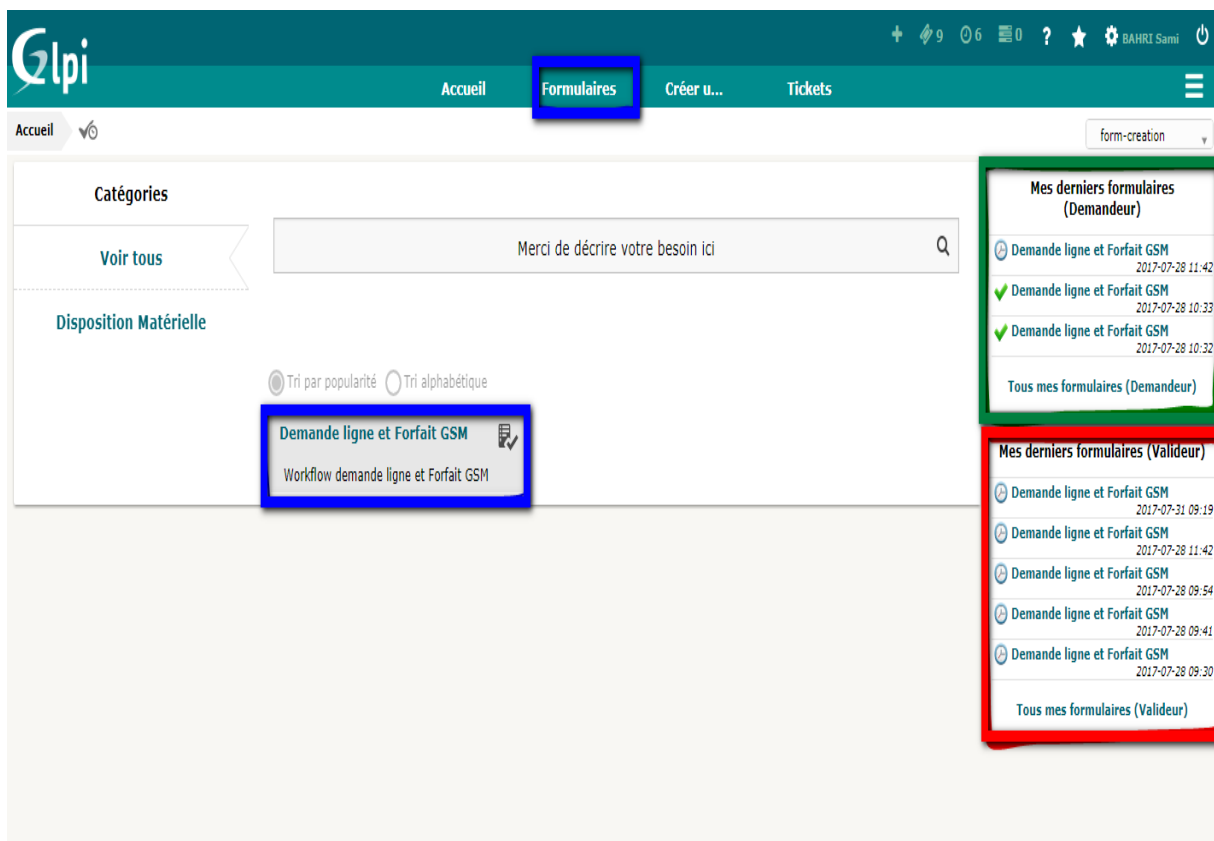


Figure 31. Suivi d'un formulaire interface GLPI



Figure 32. Formulaire demandeur

On peut voir l'état de notre demande (accepté, refusé ou en attente de validation).

Formulaire saisi
Demande ligne et Forfait GSM
Formulaire accepté par le valideur.
Type demande
Demande Modification
Demande ligne GSM
Matricule 2276
Nom et prénom Bahri Sami
Société U.N.P.A
Connexion internet Non
Numéro GSM 29537520

Figure 33. Etat d'un formulaire

Dans le cas où vous êtes choisie comme **valideur** une deuxième liste va apparaître.



Figure 34. Formulaire Valideur

A partir de cette liste vous pouvez valider ou refuser la demande.

Formulaire saisi	
Demande ligne et Forfait GSM	
Type demande	
Demande Nouveau	
Demande ligne GSM	
Matricule 2589	
Nom et prénom test	
Société U.N.P.A	
Forfait GSM 60	
Connexion internet Non	
Commentaire * 	
Obligatoire en cas de refus	
Refuser	Accepter

2.3.5 Processus Supervision de système informatique

Cette partie de projet est géré par le système de supervision NAGIOS qui offre des vues de monitoring permettant de connaître l'état des équipements et des services supervisés, et éventuellement d'effectuer des actions sur ces derniers.

Les vues principales disponibles sont les suivantes :

a. Le vue générale Tactical Overview

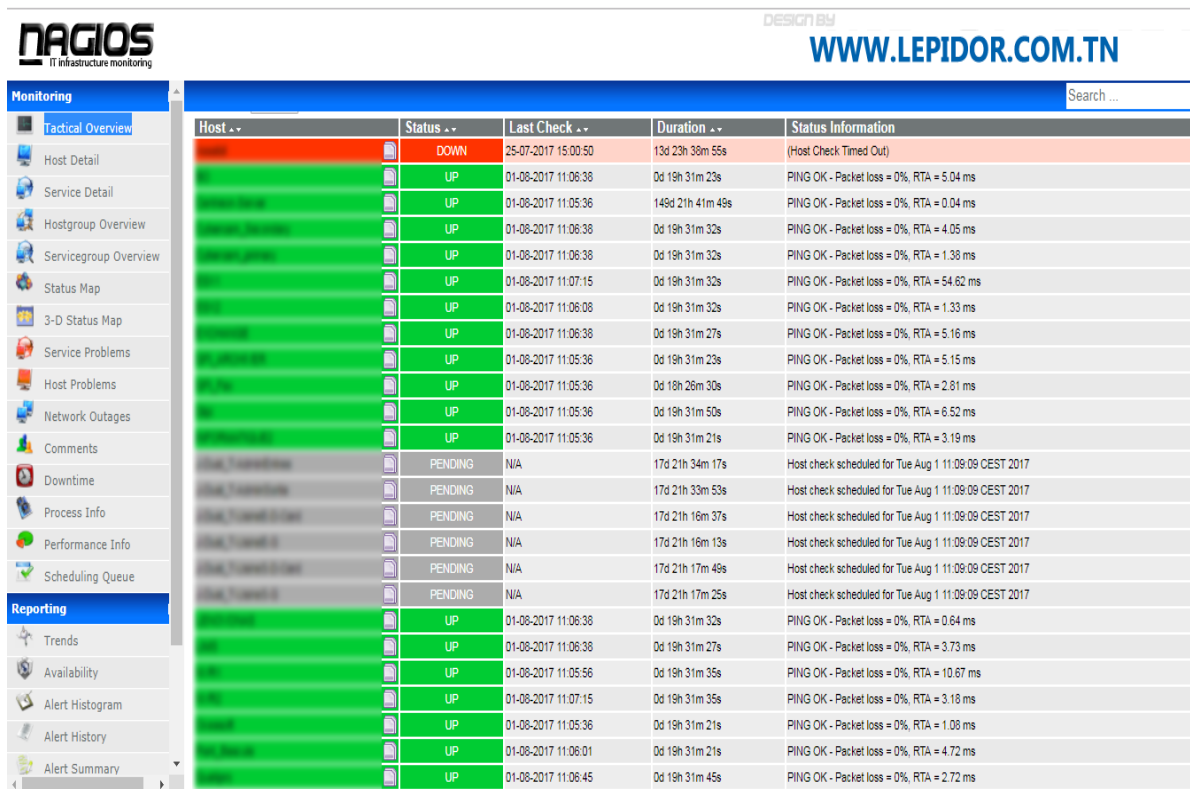
« Tactical Overview » permet d'avoir une vue globale sur les statuts des équipements et des services, une vue très légère pour avoir un aperçu rapide de l'état réseau.



Figure 35. Vue General de Nagios

b. Host Détail : vue des hôtes supervisés

« Host Détail » permet de voir le statut de manière globale de tous les équipements, savoir si ils sont en ligne (UP) ou si ils ont un autre statut (Down, Pending).



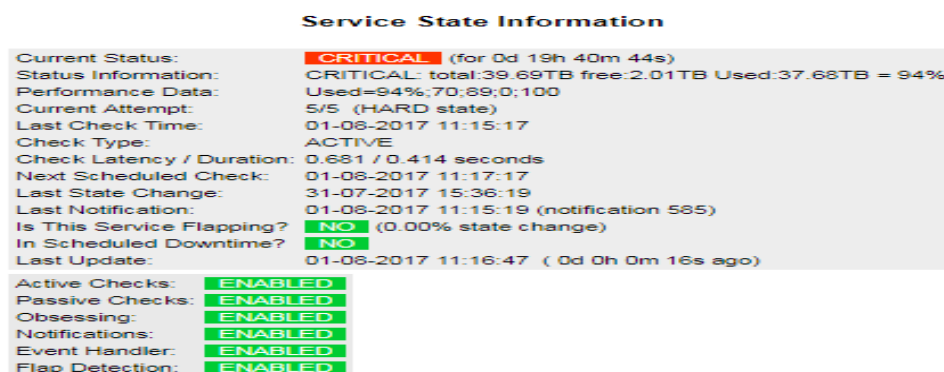
The screenshot shows the Nagios Host Detail page. The left sidebar contains navigation links for Monitoring (Tactical Overview, Host Detail, Service Detail, Hostgroup Overview, Servicegroup Overview, Status Map, 3-D Status Map, Service Problems, Host Problems, Network Outages, Comments, Downtime, Process Info, Performance Info, Scheduling Queue) and Reporting (Trends, Availability, Alert Histogram, Alert History, Alert Summary). The main content area displays a table of hosts.

Host	Status	Last Check	Duration	Status Information
Host1	DOWN	25-07-2017 15:00:50	13d 23h 38m 55s	(Host Check Timed Out)
Host2	UP	01-08-2017 11:08:38	0d 19h 31m 23s	PING OK - Packet loss = 0%, RTA = 5.04 ms
Host3	UP	01-08-2017 11:05:36	149d 21h 41m 49s	PING OK - Packet loss = 0%, RTA = 0.04 ms
Host4	UP	01-08-2017 11:08:38	0d 19h 31m 32s	PING OK - Packet loss = 0%, RTA = 4.05 ms
Host5	UP	01-08-2017 11:08:38	0d 19h 31m 32s	PING OK - Packet loss = 0%, RTA = 1.38 ms
Host6	UP	01-08-2017 11:07:15	0d 19h 31m 32s	PING OK - Packet loss = 0%, RTA = 54.62 ms
Host7	UP	01-08-2017 11:08:08	0d 19h 31m 32s	PING OK - Packet loss = 0%, RTA = 1.33 ms
Host8	UP	01-08-2017 11:08:38	0d 19h 31m 27s	PING OK - Packet loss = 0%, RTA = 5.16 ms
Host9	UP	01-08-2017 11:05:36	0d 19h 31m 23s	PING OK - Packet loss = 0%, RTA = 5.15 ms
Host10	UP	01-08-2017 11:05:36	0d 18h 26m 30s	PING OK - Packet loss = 0%, RTA = 2.81 ms
Host11	UP	01-08-2017 11:05:36	0d 19h 31m 50s	PING OK - Packet loss = 0%, RTA = 6.52 ms
Host12	UP	01-08-2017 11:05:36	0d 19h 31m 21s	PING OK - Packet loss = 0%, RTA = 3.19 ms
Host13	PENDING	N/A	17d 21h 34m 17s	Host check scheduled for Tue Aug 1 11:09:09 CEST 2017
Host14	PENDING	N/A	17d 21h 33m 53s	Host check scheduled for Tue Aug 1 11:09:09 CEST 2017
Host15	PENDING	N/A	17d 21h 16m 37s	Host check scheduled for Tue Aug 1 11:09:09 CEST 2017
Host16	PENDING	N/A	17d 21h 16m 13s	Host check scheduled for Tue Aug 1 11:09:09 CEST 2017
Host17	PENDING	N/A	17d 21h 17m 49s	Host check scheduled for Tue Aug 1 11:09:09 CEST 2017
Host18	PENDING	N/A	17d 21h 17m 25s	Host check scheduled for Tue Aug 1 11:09:09 CEST 2017
Host19	UP	01-08-2017 11:08:38	0d 19h 31m 32s	PING OK - Packet loss = 0%, RTA = 0.64 ms
Host20	UP	01-08-2017 11:08:38	0d 19h 31m 27s	PING OK - Packet loss = 0%, RTA = 3.73 ms
Host21	UP	01-08-2017 11:05:56	0d 19h 31m 35s	PING OK - Packet loss = 0%, RTA = 10.67 ms
Host22	UP	01-08-2017 11:07:15	0d 19h 31m 35s	PING OK - Packet loss = 0%, RTA = 3.18 ms
Host23	UP	01-08-2017 11:05:36	0d 19h 31m 21s	PING OK - Packet loss = 0%, RTA = 1.08 ms
Host24	UP	01-08-2017 11:06:01	0d 19h 31m 21s	PING OK - Packet loss = 0%, RTA = 4.72 ms
Host25	UP	01-08-2017 11:06:45	0d 19h 31m 45s	PING OK - Packet loss = 0%, RTA = 2.72 ms

Figure 36. Host Detail

c. Service Détail : vue des services supervisés

« Service détail » donne une vue générale de tous les services qu'on souhaite les supervisés, on peut y voir leurs statuts (par exemple le pourcentage d'espace libre/occupé qu'il reste sur un disque). On peut savoir aussi leur Uptime qui Indique depuis quand ils sont actives « UP ».



The screenshot shows the Nagios Service State Information page. It displays detailed status and performance data for a service.

Service State Information	
Current Status:	CRITICAL (for 0d 19h 40m 44s)
Status Information:	CRITICAL: total:39.69TB free:2.01TB Used:37.68TB = 94%
Performance Data:	Used=94%;70;89;0;100
Current Attempt:	5/5 (HARD state)
Last Check Time:	01-08-2017 11:15:17
Check Type:	ACTIVE
Check Latency / Duration:	0.681 / 0.414 seconds
Next Scheduled Check:	01-08-2017 11:17:17
Last State Change:	31-07-2017 15:36:19
Last Notification:	01-08-2017 11:15:19 (notification 585)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	01-08-2017 11:16:47 (0d 0h 0m 16s ago)
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

Figure 37. Service Details

d. Les vues «Host Group » et « Service Group »

Permettent de lister de manière claire les groupes d'équipements et les groupes de services que l'on a créés.

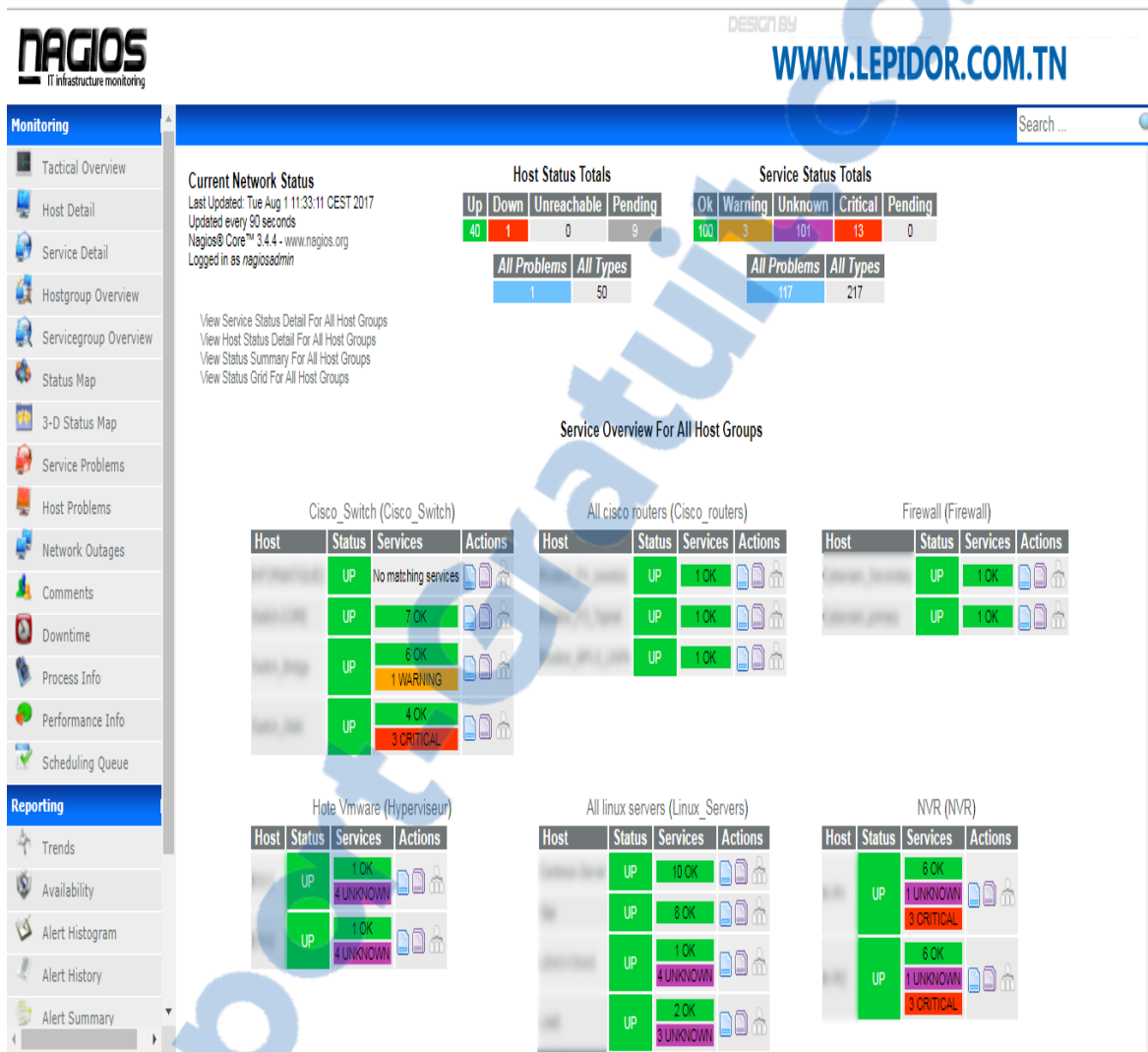


Figure 38. Information Avancés

e. Les vues «Host problem » et « Service problem»

Donner une vue sur tous les hôtes ET services sur laquelle une intervention est nécessaire.

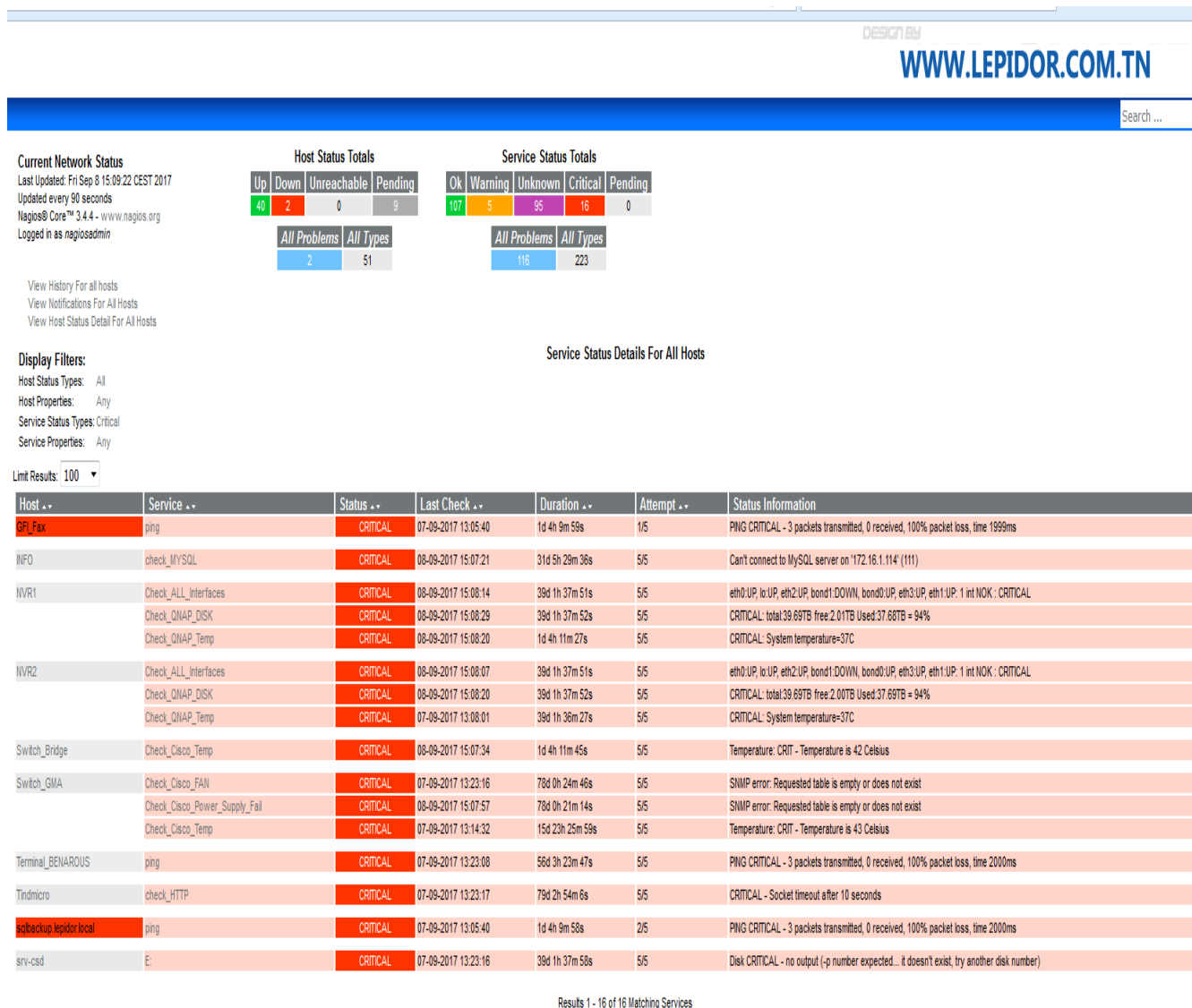


Figure 39. Service Problem

2 > »

Results 0 - 100 of 109 Matching Services

Host ..	Service ..	Status ..	Last Check ..	Duration ..	Attempt ..	Status Information
Assabil	C:	OK	08-09-2017 15:09:14	0d 10h 47m 26s	1/5	Disk OK - C: TOTAL: 119.656GB USED: 28.143GB (23%) FREE: 91.513GB (77%)
	Swap	OK	07-09-2017 13:14:31	1d 4h 13m 45s	1/5	Disk OK - Virtual Memory TOTAL: 13.812GB USED: 2.064GB (14%) FREE: 11.748GB (86%)
	cpu	OK	08-09-2017 15:10:43	0d 10h 48m 5s	1/5	CPU utilization percentage : 0.75%
	memory	OK	08-09-2017 15:09:14	0d 10h 47m 26s	1/5	Disk OK - Physical Memory TOTAL: 12.000GB USED: 1.325GB (11%) FREE: 10.675GB (89%)
	ping	OK	07-09-2017 13:06:41	1d 4h 14m 33s	1/1	PING OK - rtt min/avg/max/ndev = 0.498/0.615/0.746/0.103 ms
BO	check_HTTP	OK	08-09-2017 15:10:29	11d 2h 52m 53s	1/5	HTTP OK: HTTP/1.1 200 OK - 1890 bytes in 0.013 second response time
	ping	OK	08-09-2017 15:09:21	0d 6h 20m 55s	1/5	PING OK - rtt min/avg/max/ndev = 0.494/0.653/0.953/0.213 ms
Centreon-Server	/	OK	07-09-2017 13:14:31	188d 3h 50m 21s	1/5	Disk OK - / TOTAL: 73.558GB USED: 5.370GB (7%) FREE: 68.187GB (93%)
	Check_DDOS	OK	08-09-2017 15:10:44	37d 5h 3m 6s	1/5	No DDOS attack detected (0/9).
	Check_DDOS_SYN	OK	08-09-2017 15:10:14	51d 4h 40m 2s	1/5	No DDOS detected (0 / 50)
	Check_NB_Users_Connected	OK	08-09-2017 15:10:40	24d 22h 57m 34s	1/5	USERS OK - 1 users currently logged in
	Check_SSH	OK	08-09-2017 15:09:34	79d 2h 7m 21s	1/5	SSH OK - OpenSSH_4.3 (protocol 2.0)
	check_HTTP	OK	07-09-2017 13:14:31	37d 5h 4m 46s	1/5	HTTP OK: HTTP/1.1 200 OK - 3136 bytes in 0.000 second response time
	check_MYSQL	OK	08-09-2017 15:10:29	79d 2h 18m 15s	1/5	Uptime: 94192 Threads: 12 Questions: 1287493 Slow queries: 3 Opens: 221 Flush tables: 1 Open tables: 64 Queries per second avg: 13.669
	load	OK	08-09-2017 15:10:43	1d 4h 2m 32s	1/5	Load average: 0.36, 0.36, 0.30
	memory	OK	08-09-2017 15:10:40	188d 3h 47m 51s	1/5	Total memory used : 6% ram used : 55% swap used 0%
	ping	OK	08-09-2017 15:10:44	188d 3h 46m 36s	1/5	PING OK - rtt min/avg/max/ndev = 0.012/0.031/0.064/0.023 ms
Cyberoam_Secondary	ping	OK	08-09-2017 15:09:05	39d 1h 39m 50s	1/5	PING OK - rtt min/avg/max/ndev = 0.309/0.860/1.796/0.665 ms
Cyberoam_primary	ping	OK	07-09-2017 13:23:14	39d 1h 39m 50s	1/5	PING OK - rtt min/avg/max/ndev = 0.527/0.669/0.750/0.105 ms
ESX1	ping	OK	07-09-2017 13:23:14	11d 18h 41m 7s	1/5	PING OK - rtt min/avg/max/ndev = 0.344/0.501/0.659/0.129 ms
ESX2	ping	OK	07-09-2017 13:23:14	20d 15h 11m 36s	1/5	PING OK - rtt min/avg/max/ndev = 0.323/0.517/0.724/0.164 ms
EXCHANGE	check_POP	OK	08-09-2017 15:09:57	39d 1h 38m 59s	1/5	POP OK - 0.011 second response time on port 110 [+OK The Microsoft Exchange POP3 service is ready.]
	check_SMTP	OK	07-09-2017 13:14:31	39d 1h 38m 59s	1/5	SMTP OK - 0.016 sec. response time
	ping	OK	08-09-2017 15:09:06	12d 16h 30m 59s	1/5	PING OK - rtt min/avg/max/ndev = 0.492/0.600/0.780/0.130 ms
GFL_ARCHIVER	ping	OK	08-09-2017 15:09:07	10d 16h 32m 4s	1/5	PING OK - rtt min/avg/max/ndev = 0.433/0.489/0.592/0.072 ms
Gipi	/	OK	08-09-2017 15:09:34	29d 7h 8m 19s	1/5	Disk OK - / TOTAL: 158.740GB USED: 5.463GB (3%) FREE: 153.277GB (97%)
	Check_SSH	OK	08-09-2017 15:09:34	29d 7h 7m 44s	1/5	SSH OK - OpenSSH_4.3 (protocol 2.0)
	Swap	OK	07-09-2017 13:14:31	29d 7h 8m 26s	1/5	Disk OK - Swap space TOTAL: 3.914GB USED: 0.000GB (0%) FREE: 3.914GB (100%)
	check_HTTP	OK	08-09-2017 15:10:29	29d 7h 8m 6s	1/5	HTTP OK: HTTP/1.1 200 OK - 3142 bytes in 0.012 second response time
	check_MYSQL	OK	08-09-2017 15:10:55	29d 7h 7m 42s	1/5	Uptime: 366215 Threads: 13 Questions: 5523526 Slow queries: 1 Opens: 485987 Flush tables: 1 Open tables: 400 Queries per second avg: 15.082
	load	OK	08-09-2017 15:10:55	29d 7h 7m 44s	1/5	Load average: 0.08, 0.02, 0.01
	memory	OK	07-09-2017 13:08:01	29d 7h 8m 6s	1/5	Total memory used : 9% ram used : 23% swap used 0%
	ping	OK	08-09-2017 15:08:55	15d 17h 8m 21s	1/5	PING OK - rtt min/avg/max/ndev = 0.498/0.604/0.775/0.123 ms

Figure 40 : Service OK

f. Les vues de Reporting

Les vues de reporting permettent de créer, à la volée, des rapports sur l'activité du système d'information, en fonction des données collectées par Nagios. Les rapports pourront alors intégrer des graphiques.

Les vues principales disponibles sont les suivantes.

- Trends : permet de grapher des données mesurables en fonction du temps



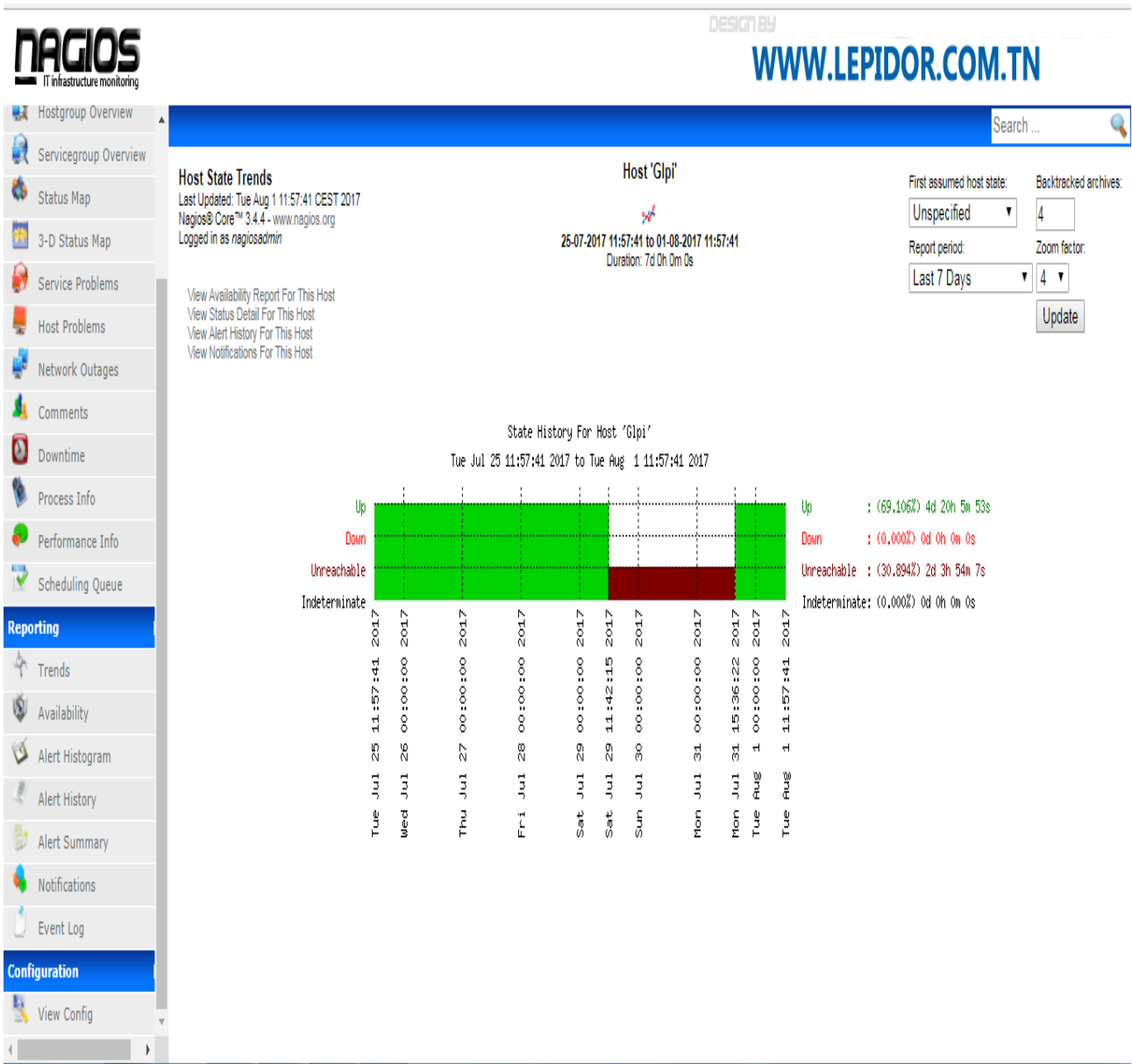


Figure 41.Trends

- Availability : permet de créer des rapports de disponibilité des équipements

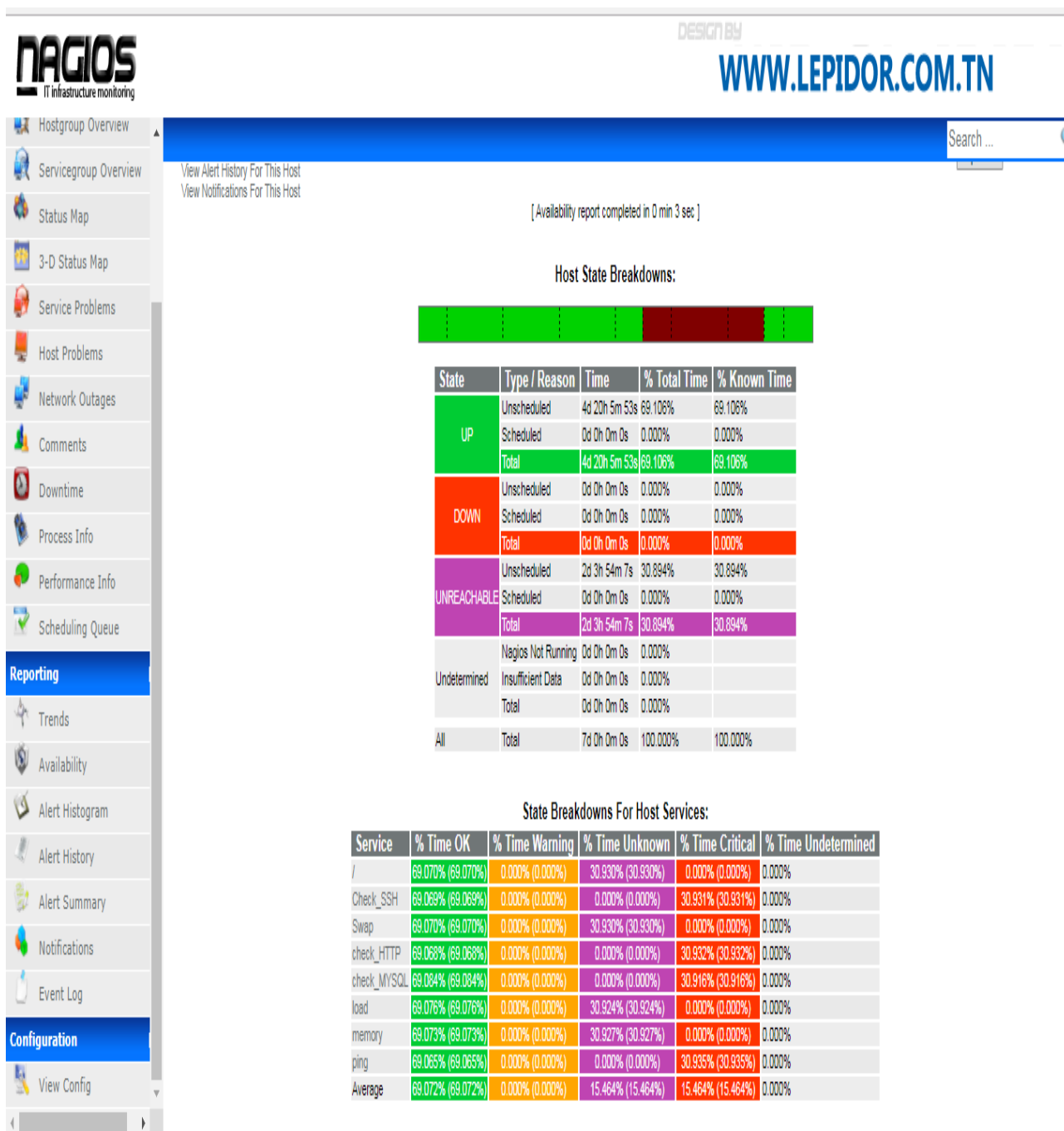


Figure 42. Availability

- Alert History : permet d'avoir un historique des alertes

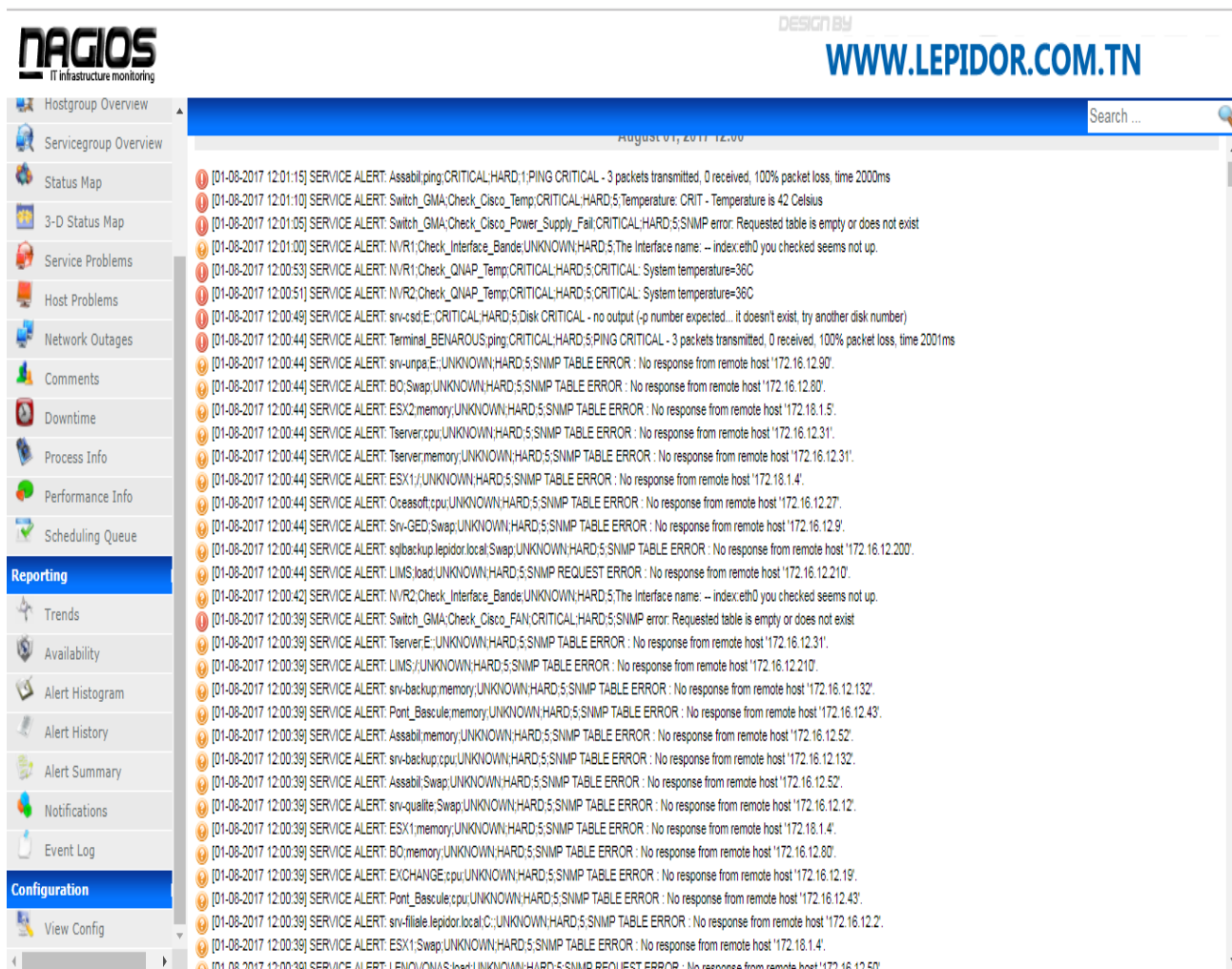


Figure 43. Alert History

2.3.6 Notification par Email

Parmi les fonctionnalités essentielles demandées dans le cahier de charge et la fonctionnalité de notification par email pour faciliter et accélérer les interventions des administrateurs.

J'ai réussi dans mon projet d'activer la notification pour les deux produits GLPI et Nagios.

Pour GLPI lorsqu'un utilisateur crée un ticket ou une demande un mail de notification est envoyé à l'administrateur.



Figure 44. Notification Nouveau Ticket

Lorsque l'administrateur traite le ticket est l'attribue à un technicien ce dernier sera par la suite notifié par email.

Ticket : Description

Titre :Incentaire matériel informatique SOMECE
Demandeurs : ERNEZ Karim
Date d'ouverture :2017-07-24 10:26
Date de clôture :
Source de la demande :Helpdesk

Assigné aux techniciens : BAHRI Sami
Statut : En cours (Attribué)

Urgence : Moyenne
Impact : Moyen
Priorité : Moyenne

Catégorie :Inventaire
Description : à Inventorier le matériel informatique SOMECE avec pour chaque poste:

Figure 45. Alert Ticket attribué

Par la suite lorsque le technicien résolu le ticket le demandeur sera informé pour valider ou refuser la solution.


 Support GLPI
 [GLPI #0002478] Ticket résolu Internet et mail coupés chez Ezzedinne Zbidi
 À Sami BAHRI

Date de résolution : 2017-07-26 09:22
Type de solution : Prise réseaux
Solution :

 le problème réseaux et bien résolue.

Ticket : Description

Titre :Internet et mail coupés chez Ezzedinne Zbidi
Demandeurs : ERNEZ Karim
Date d'ouverture :2017-07-26 08:21
Date de clôture :
Source de la demande :Helpdesk

Assigné aux techniciens : GOLLI Hamdi
Statut : Résolu

Figure 46. Alert ticket résolu

Pour le système de supervision nagios lorsque l'état d'un services ou host passe d'un état normal à un état de défaillance, un mail de notification est envoyé après une certaine tentative paramétrable selon la criticité de l'équipement.

Hostgroup Overview						
Servicegroup Overview						
Status Map						
3-D Status Map						
Service Problems						
Host Problems						
Network Outages						
Comments						
Downtime						
Process Info						
Performance Info						
Scheduling Queue						
Reporting						
Trends						
Availability						
Alert Histogram						
Alert History						
Alert Summary						
Notifications						
Event Log						
Configuration						
View Config						
Host	Service	Type	Time	Contact	Notification Command	Information
Assabil	Check_ALL_interfaces	CRITICAL	01-08-2017 12:03:31	Bahri_SAMI	host-notify-by-sendmailhost	eth0:UP,lo:UP,eth2:UP,bond1:DOWN,bond0:UP,eth3:UP,eth1:UP: 1 int NOK : CRITICAL
Assabil	Check_ALL_interfaces	CRITICAL	01-08-2017 12:03:30	nagiosadmin_nagiosadmin	notify-by-sendmailservices	eth0:UP,lo:UP,eth2:UP,bond1:DOWN,bond0:UP,eth3:UP,eth1:UP: 1 int NOK : CRITICAL
Assabil	N/A	HOST DOWN	01-08-2017 12:03:29	Bahri_SAMI	host-notify-by-sendmailhost	(Host Check Timed Out)
Assabil	N/A	HOST DOWN	01-08-2017 12:03:28	nagiosadmin_nagiosadmin	host-notify-by-sendmailhost	(Host Check Timed Out)
Assabil_000	Check_Cisco_Temp	CRITICAL	01-08-2017 12:03:14	Bahri_SAMI	host-notify-by-sendmailhost	Temperature: CRIT - Temperature is 42 Celsius
Assabil_000	Check_Cisco_Temp	CRITICAL	01-08-2017 12:03:13	nagiosadmin_nagiosadmin	notify-by-sendmailservices	Temperature: CRIT - Temperature is 42 Celsius
Assabil_000	Check_Cisco_Power_Supply_Fai	CRITICAL	01-08-2017 12:03:04	Bahri_SAMI	host-notify-by-sendmailhost	SNMP error: Requested table is empty or does not exist
Assabil_000	Check_Cisco_Power_Supply_Fai	CRITICAL	01-08-2017 12:03:03	nagiosadmin_nagiosadmin	notify-by-sendmailservices	SNMP error: Requested table is empty or does not exist
Assabil	Check_QNAP_Temp	CRITICAL	01-08-2017 12:02:57	Bahri_SAMI	host-notify-by-sendmailhost	CRITICAL: System temperature=36C
Assabil	Check_QNAP_Temp	CRITICAL	01-08-2017 12:02:56	nagiosadmin_nagiosadmin	notify-by-sendmailservices	CRITICAL: System temperature=36C
Assabil	Check_QNAP_Temp	CRITICAL	01-08-2017 12:02:55	Bahri_SAMI	host-notify-by-sendmailhost	CRITICAL: System temperature=36C
Assabil	Check_QNAP_Temp	CRITICAL	01-08-2017 12:02:54	nagiosadmin_nagiosadmin	notify-by-sendmailservices	CRITICAL: System temperature=36C
Assabil	E:	CRITICAL	01-08-2017 12:02:53	Bahri_SAMI	host-notify-by-sendmailhost	Disk CRITICAL - no output (-p number expected... it doesnt exist, try another disk number)
Assabil	E:	CRITICAL	01-08-2017 12:02:52	nagiosadmin_nagiosadmin	notify-by-sendmailservices	Disk CRITICAL - no output (-p number expected... it doesnt exist, try another disk number)
Assabil_000	ping	CRITICAL	01-08-2017 12:02:51	Bahri_SAMI	host-notify-by-sendmailhost	PING CRITICAL - 3 packets transmitted, 0 received, 100% packet loss, time 1999ms
Assabil_000	ping	CRITICAL	01-08-2017 12:02:50	nagiosadmin_nagiosadmin	notify-by-sendmailservices	PING CRITICAL - 3 packets transmitted, 0 received, 100% packet loss, time 1999ms
Assabil_000	Check_Cisco_FAN	CRITICAL	01-08-2017 12:02:42	Bahri_SAMI	host-notify-by-sendmailhost	SNMP error: Requested table is empty or does not exist
Assabil_000	Check_Cisco_FAN	CRITICAL	01-08-2017 12:02:41	nagiosadmin_nagiosadmin	notify-by-sendmailservices	SNMP error: Requested table is empty or does not exist
Assabil	Check_ALL_interfaces	CRITICAL	01-08-2017 12:02:36	Bahri_SAMI	host-notify-by-sendmailhost	eth0:UP,lo:UP,eth2:UP,bond1:DOWN,bond0:UP,eth3:UP,eth1:UP: 1 int NOK : CRITICAL

Figure 47.Vu alerte Nagios



mar. 18/07/2017 13:02

nagios@localhost.localdomain

Host DOWN alert for Assabil!

À Sami BAHRI

******* FAN Notification *******

Type: PROBLEM
Host: ^ _ _ _ _
State: DOWN
Address: 1 _ _ _ _
Info: (Host Check Timed Out)
Date/Time: 18-07-2017 14:02:25

Figure 48. Exemple d'alerte Nagios

Conclusion

Ce chapitre dont l'objectif principal était de présenter le produit final obtenu.

A cet effet, j'ai présentés les outils matériels et logiciels utilisés d'une part, puis j'ai vérifié le respect de mon produit aux besoins fonctionnels demandés dans le cahier de charge.

CONCLUSION GENERALE

Ce document a été rédigé au terme du projet de fin d'études réalisé au sein de « L'EP ID'OR ». Il s'agissait en effet de mettre en place un **«Mise en place d'un système de gestion des demandes, d'incidents, gestion de parc et de supervision»**, qui devrait booster la gestion des ressources des entreprises.

La première phase de ce rapport était consacrée à la présentation de l'organisme d'accueil suivi de l'état de l'art, dans laquelle j'ai présenté le projet et ses problématiques pour arriver à proposer notre solution intitulée mise en place d'une solution de supervision, d'inventaire et de gestion des incidents et demande des utilisateurs. Ces parties ont été suivies d'une analyse sur les applications existantes et leurs limites, ce qui nous a permis choisir les produits open source GLPI et NAGIOS.P our la partie réalisation de notre projet qui comporte une partie d'étude de l'architecture matériel et logicielle de solution ,une partie installation détaillé dans l'annexe et une partie présentation de l'application dans laquelle j'ai essayé de valider les besoins fonctionnelle décrit dans le cahier de charge avec les fonctionnalités offerts par la solution .

Enfin donc, il est important de souligner que ce projet a atteint les objectifs fixés au départ, et au-delà du sentiment de satisfaction qui s'en suit, il nous a permis de bénéficier de nouvelles connaissances venues compléter celles que nous avons acquises tout au long de notre formation.

Cependant, nous pouvons toujours y apporter quelques améliorations qui feront de cette application un outil incontournable tant dans le domaine de gestion de parc informatique que dans le domaine de supervision.

Rapport-Gratuit.com

Annexe

Annexe A : Préparation de machine virtuelle

Sur le serveur ESXi suivre les étapes nécessaires pour créer une nouvelle machine virtuelle

Créer une nouvelle machine virtuelle

Nom et emplacement
Spécifier un nom et un emplacement pour cette machine virtuelle

Version de machine virtuelle : 8

Configuration
Nom et emplacement
 Stockage
 Système d'exploitation client
 Réseau
 Créer un disque
 Prêt à terminer

Nom :
 Gestion Parc

Les noms de VM peuvent contenir jusqu'à 80 caractères et doivent être uniques dans chaque dossier de VM vCenter Server.
 Les dossiers de VM ne sont pas visibles une fois connectés directement à un hôte. Pour consulter les dossiers de VM et spécifier un emplacement pour cette VM, connectez-vous à vCenter Server.

Aide < Précédent Suivant > Annuler

Créer une nouvelle machine virtuelle

Système d'exploitation client
 Désignez le système d'exploitation client à utiliser avec cette machine virtuelle.

Version de machine virtuelle : 8

[Configuration](#)
[Nom et emplacement](#)
[Stockage](#)
Système d'exploitation client
 Réseau
 Créer un disque
 Prêt à terminer

Système d'exploitation client :

☐ Windows
☒ Linux
☐ Autre

Version :
 CentOS 4/5/6 (64 bits)

L'identification du système d'exploitation client permet à l'assistant de fournir les valeurs par défaut appropriées pour l'installation du SE.

[Aide](#) [< Précédent](#) [Suivant >](#) [Annuler](#)

Créer une nouvelle machine virtuelle

Stockage
 Choisir un stockage de destination pour les fichiers de machine virtuelle

Version de machine virtuelle : 8

[Configuration](#)
[Nom et emplacement](#)
Stockage
[Système d'exploitation client](#)
 Réseau
 Créer un disque
 Prêt à terminer

Choisir un stockage de destination dans lequel enregistrer les fichiers de machine virtuelle :

Nom	Type de lec.	Capacité	Alloué	Libre	Type	Thin Pro
datastore1	Non-SSD	32,50 Go	972,00 Mo	31,55 Go	VMFS5	Pris en d

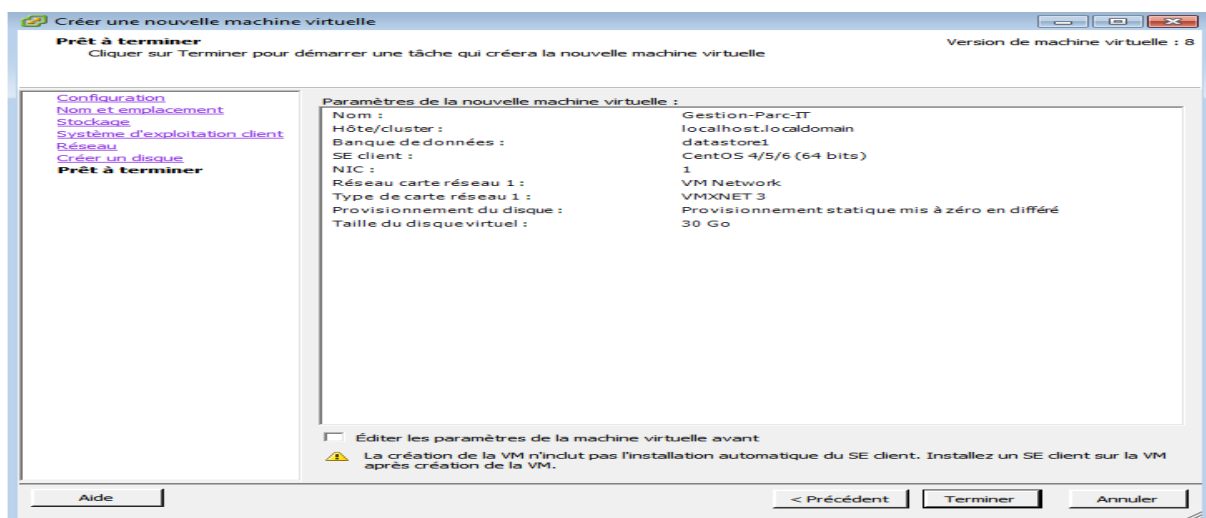
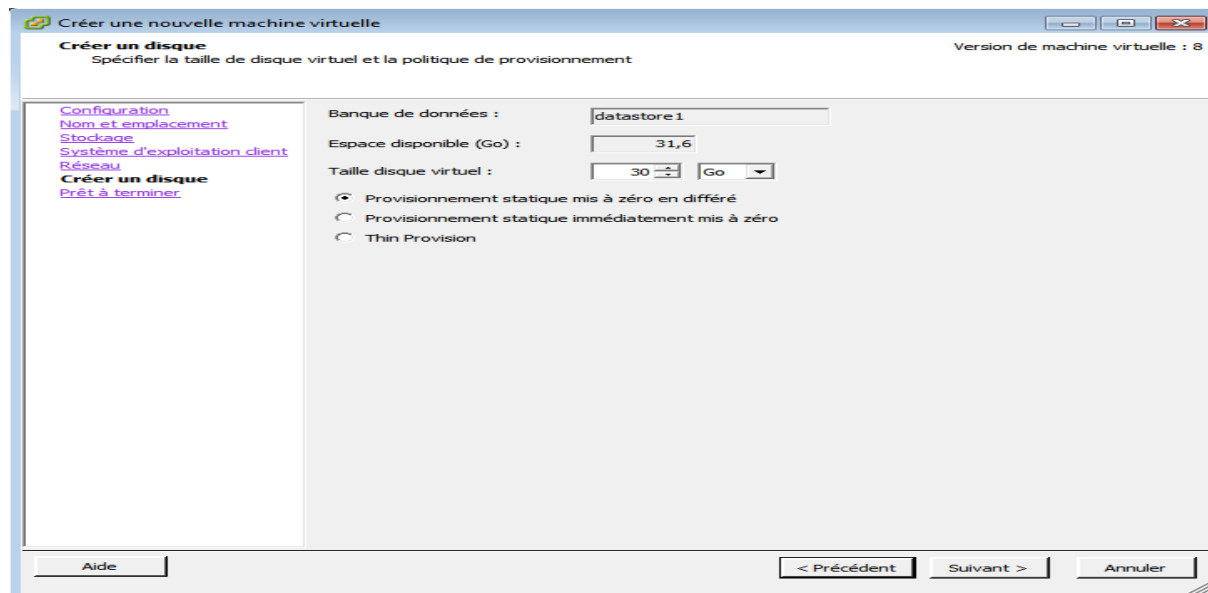
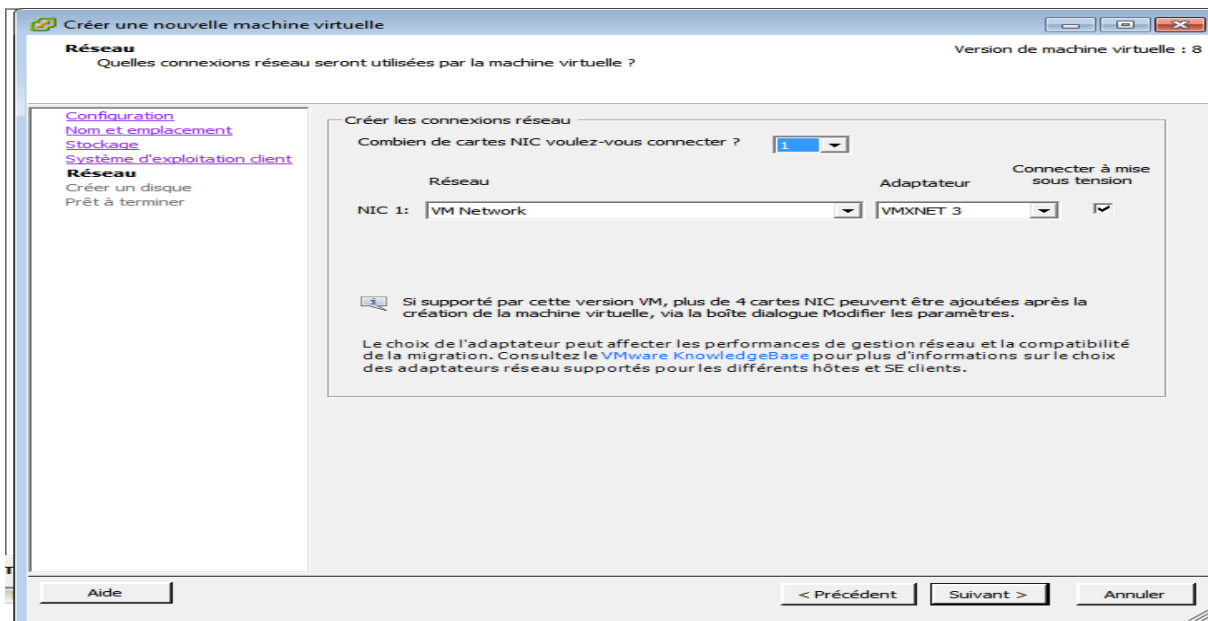
☐ Désactiver le DRS de stockage pour cette machine virtuelle

Sélectionner une banque de données :

Nom	Type de lec.	Capacité	Alloué	Libre	Type	Thin Pro
-----	--------------	----------	--------	-------	------	----------

[Aide](#) [< Précédent](#) [Suivant >](#) [Annuler](#)





Gestion-Parc-IT

Démarrage | **Résumé** | Allocation ressources | Performance | Événements | Console | Autorisations

Général

SE client : CentOS 4/5/6 (64 bits)
Version VM : 8
CPU : 1 vCPU
Mémoire : 2048 Mo
Charge mémoire : 118,02 Mo
VMware Tools : Inactif (Non installé)
Adresses IP :

Nom DNS :

État : Hors tension
Hôte : localhost.localdomain
vMotion activé :
Protection vSphere HA : S/O

Ressources

Consommation CPU hôte :
Consommation mémoire hôte :
Mémoire invitée active : [Actualiser utilisation stockage](#)

Stockage provisionné : **32,21 Go**
Stockage non-partagé : **30,00 Go**
Stockage utilisé : **30,00 Go**

Stockage	Type de lecteur	Capacité
datastore1	Non-SSD	32,50 Go

Réseau	Type
VM Network	Groupe de ports standard

Commandes

Activer
 Modifier les paramètres

Annotations

Remarques : [Modifier](#)

Annexe B : Installation de FAN

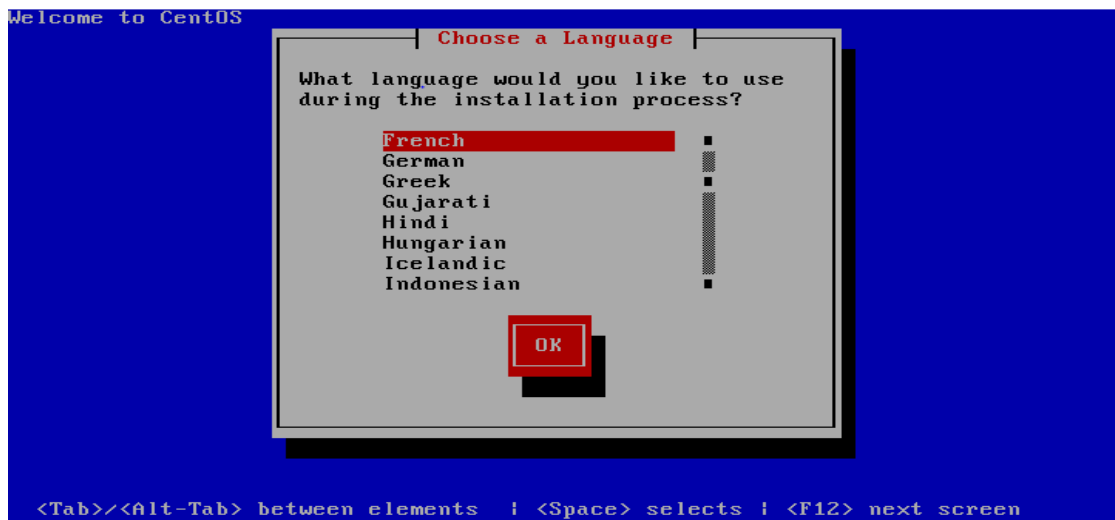
Les étapes d'installation et configuration de FAN seront détaillé dans l'annexe B

Télécharger ISO FAN à partir de site <http://www.fullyautomatednagios.org/download/>

Copier l'ISO dans le DATASTORE de plateforme virtuelle et l'attacher au machine virtuelle déjà créer.



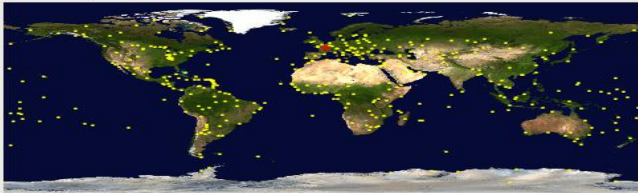
Démarrer la machine virtuelle l'installation va commencer



**Fan**

Fully Automated Nagios

Veuillez sélectionner la ville la plus proche de votre fuseau horaire :



Europe/Paris

☐ Horloge système en UTC

 Notes de mise à jour

 Revenir

 Suivant

**Fan**

Fully Automated Nagios

 Le compte root est utilisé pour administrer le système. Saisissez un mot de passe pour l'utilisateur root.

Mot de passe root :

Confirmer :

 Notes de mise à jour

 Revenir

 Suivant



Annexe C : Configuration réseaux

Éditer le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` avec l'éditeur VI

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
BOOTPROTO=static
BROADCAST=[REDACTED]
IPADDR=[REDACTED]
NETMASK=255.255.255.0
NETWORK=[REDACTED]
DHCPCLASS=
HWADDR=[REDACTED]
ONBOOT=yes
NM_CONTROLLED="no"
```

Éditer le fichier `/etc/sysconfig/network` avec l'éditeur VI

[illegible]

Éditer le fichier `/etc/resolv.conf` avec l'éditeur VI

```
-
search lepidor.local
nameserver [REDACTED]
nameserver [REDACTED]
nameserver 8.8.8.8

...

"/etc/resolv.conf" 8L, 143C
```

Pour terminer il faut redémarrer le service réseaux avec la commande `service network restart` et se connecter à l'interface web de l'application en tapant le lien `http://ip/`

Vous serez redirigé ver interface web de FAN



Annexe D : Installation de GLPI

Les Etapes d'installation et de configuration de GLPI seront détaillé dans l'annexe C

Vérification d'Apache, PHP et MySQL

L'installation de GLPI nécessite la présence d'apache, PHP et MySQL et puisque je vais travailler sur la distribution FAN dans laquelle ses produits sont déjà installés je vais juste procéder à une vérification du bon fonctionnement de ses produits.

Pour Apache il faut lancer la commande de vérification `rpm -qa |grep -i httpd`

```
[root@GLPI ~]# rpm -qa |grep -i httpd
httpd-2.2.3-92.el5.centos
```

Dans le cas d'une nouvelle installation il faut lancer la commande `yum install httpd`

Pour PHP il faut lancer la commande de vérification `php -v`

```
PHP 5.5.38 (cli) (built: Dec 10 2016 19:34:37)
```

Dans le cas d'une nouvelle installation il faut lancer la commande de `yum install php php-mysql php-mbstring`

Pour mysql il faut lancer la commande de vérification `rpm -qa |grep -i mysql`

```
[root@GLPI ~]# rpm -qa |grep -i mysql
nagios-plugin-mysql-health-2.0.4-fan.3
perl-DBD-MySQL-3.0007-2.el5
mysql-server-5.5.54-1.el5.remi
rsyslog-mysql-3.22.1-7.el5
php-mysqldb-5.5.38-6.el5.remi
mysql-libs-5.5.54-1.el5.remi
mysqlclient15-5.0.90-2.el5.art
mysql-5.5.54-1.el5.remi
```

Dans le cas d'une nouvelle installation il faut lancer la commande yum install mysql-server

Pour terminer démarrer le service MySQL et apaches tapant les commandes

/etc/init.d/mysqld start

```
[root@GLPI ~]# /etc/init.d/mysqld start
Démarrage de mysqld : [ OK ]
[root@GLPI ~]#
```

/etc/init.d/httpd start

```
[root@GLPI ~]# /etc/init.d/httpd start
Démarrage de httpd : httpd: apr_sockaddr_info_get() failed for GLPI.LEPIDOR.LOCAL
httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
[ OK ]
[root@GLPI ~]#
```

Création de base de données GLPI

Se connecter au serveur MySQL à Travers la commande mysql -u root -p (Mot de passe root)

```
[root@GLPI ~]# mysql -u root -p
Enter password: [ ]
```

Taper la commande create database glpidb pour créer la base de données glpidb

```
mysql> create database glpidb;
Query OK, 1 row affected (0.00 sec)
```

Il faut donner les bons privilèges à l'utilisateur « user » sur les tables de la base de données « glpidb » en tapant la commande

grant all privileges on glpidb.* to glpi@localhost identified by 'glpi';

```
mysql> grant all privileges on glpidb.* to glpi@localhost identified by 'glpi';
Query OK, 0 rows affected (0.00 sec)
```

Paramétrage Apache

Il faut changer la propriétaire de dossier GLPI à l'utilisateur apache pour lui permettre l'accès en écriture dans le fichier config

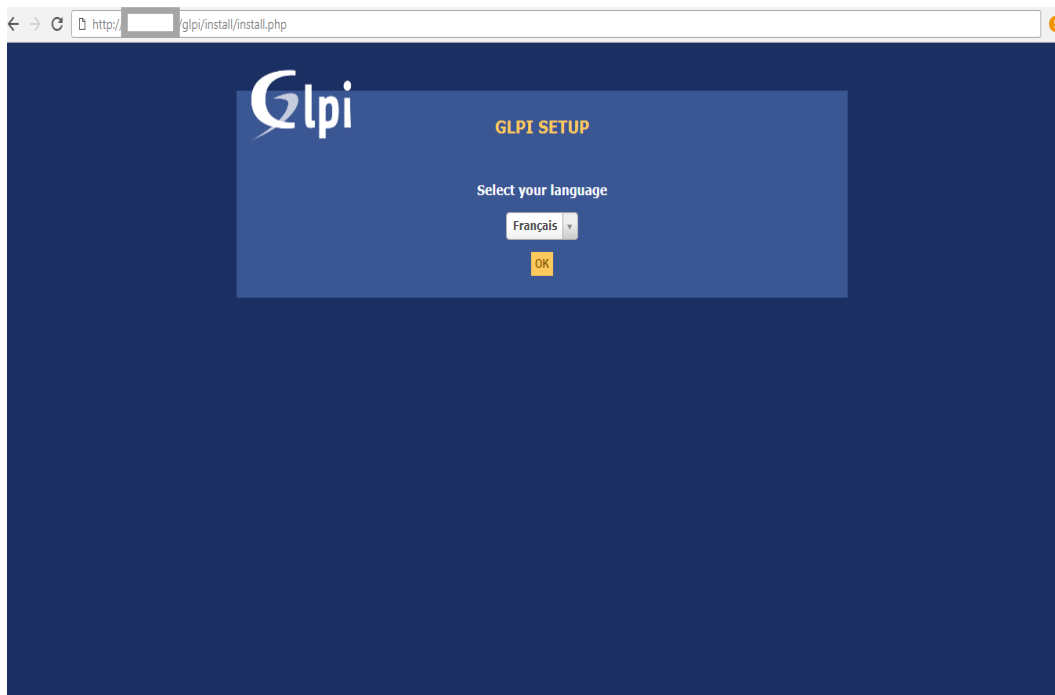
Taper les commandes

```
cd /var/www/html
```

```
chown -R apache glpi
```

Après que tous les paramétrages sont réalisés on peut terminer l'installation de GLPI

Accéder à l'adresse <http://@ip/glpi/>





GLPI SETUP

Licence

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

[Des traductions non officielles sont également disponibles](#)



J'ai lu et **ACCEPTÉ** les termes de la licence énoncés ci-dessus.



J'ai lu et **N'ACCEPTÉ PAS** les termes de la licence énoncés ci-dessus

Continuer

Étape 0

Vérification de la compatibilité de votre environnement avec l'exécution de GLPI

Tests effectués	Résultats
Test du Parseur PHP	✓
Test des sessions	✓
Test de l'utilisation de Session_use_trans_sid	✓
test de l'extension mysqli	✓
test de l'extension ctype	✓
test de l'extension fileinfo	✓
test de l'extension json	✓
test de l'extension mbstring	✓
test de l'extension zlib	✓
test de l'extension curl	✓
test de l'extension gd	✓
test de l'extension ldap	✓
test de l'extension imap	✓
Test de la mémoire allouée	✓
Test d'écriture du fichier de configuration	✓
Test d'écriture de fichiers documents	✓
Test d'écriture de fichiers dump	✓
Test d'écriture des fichiers de sessions	✓
Test d'écriture des fichiers des actions automatiques	✓
Test d'écriture des fichiers de graphiques	✓
Test d'écriture des fichiers de verrouillage	✓
Test d'écriture des documents des plugins	✓
Test d'écriture des fichiers temporaires	✓
Test d'écriture de fichiers rss	✓
Test d'écriture des fichiers téléchargés	✓
Test d'écriture de fichiers photos	✓
Test d'écriture des fichiers de journal	✓



GLPI SETUP

Étape 1

Configuration de la connexion à la base de données

Paramètres de connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

Utilisateur SQL

Mot de passe SQL

Continuer



GLPI SETUP

Étape 2

Test de connexion à la base de données

Connexion à la base de données réussie

Veuillez sélectionner une base de données :

☒ glpidb

☐ test

☐ Créer une nouvelle base ou utiliser une base existante :

Continuer



GLPI SETUP

Étape 3

Initialisation de la base de données.

OK - La base a bien été initialisée

Continuer



GLPI SETUP

Étape 4

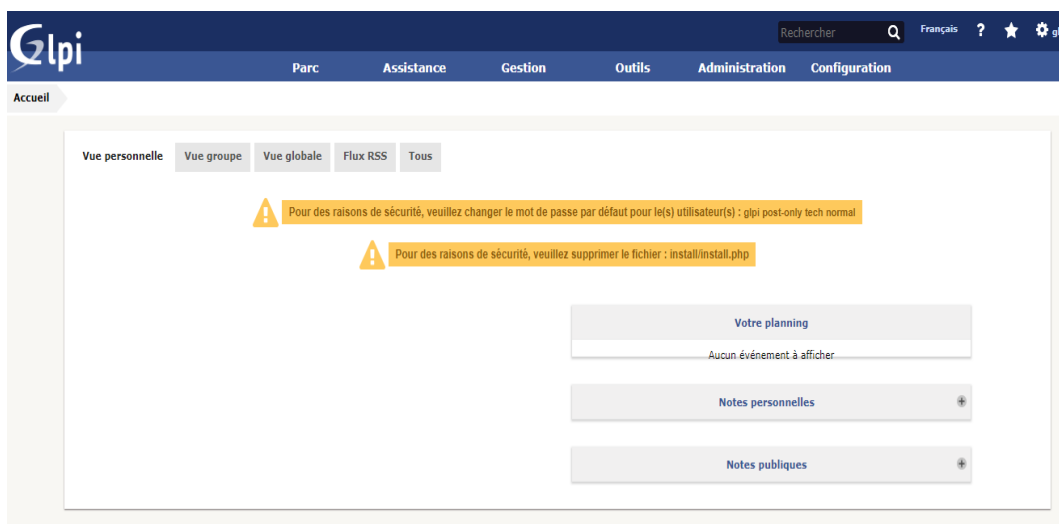
L'installation est terminée

Les identifiants et mots de passe par défaut sont :

- glpi/glpi pour le compte administrateur
- tech/tech pour le compte technicien
- normal/normal pour le compte normal
- post-only/postonly pour le compte postonly

Vous pouvez supprimer ou modifier ces comptes ainsi que les données initiales.

Utiliser GLPI



Pour supprimer l'erreur il faut renommer le dossier /var/www/html/glpi/install et changer le mot de passe par défaut des utilisateurs.

Annexe E : d'installation et de configuration des agents d'inventaire et supervision

Annexe E : installation des agents d'inventaire et supervision

1) Installation des agents SNMP

✓ Equipement réseaux « Switch Cisco »

Pour réussir l'inventaire ET la supervision de nos switch Cisco j'ai décidé de lui.

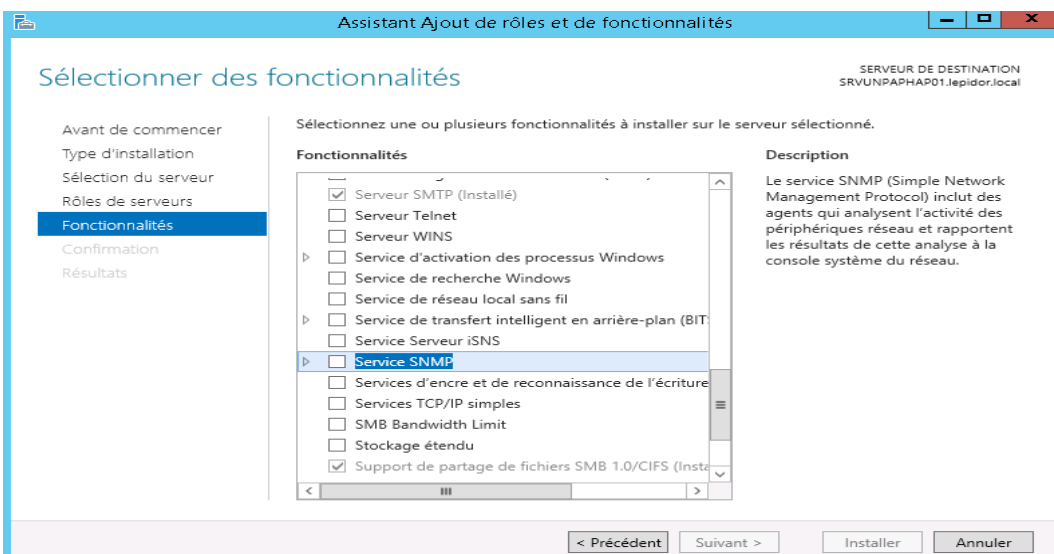
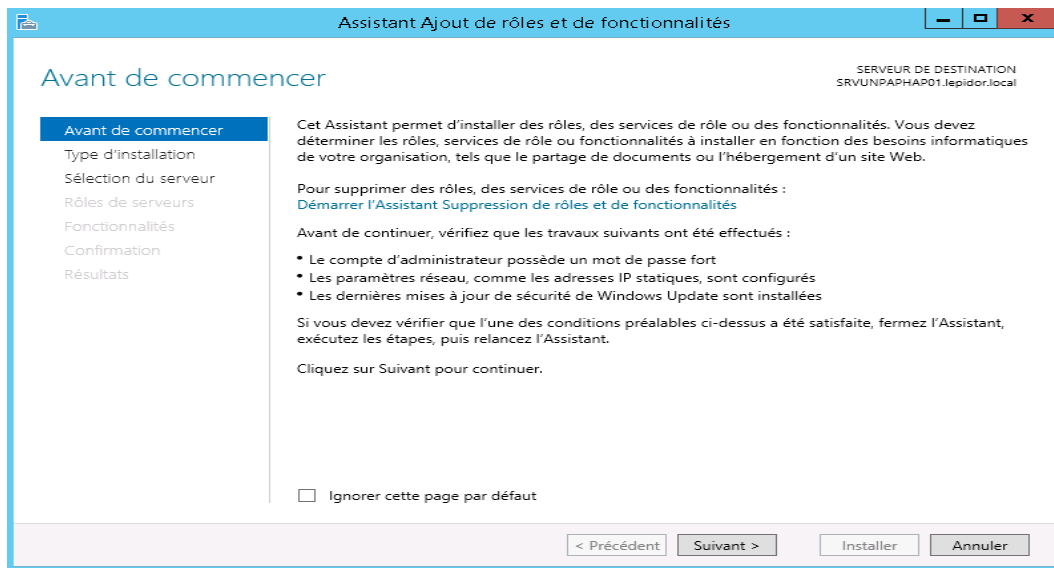
Attribuer une adresse IP

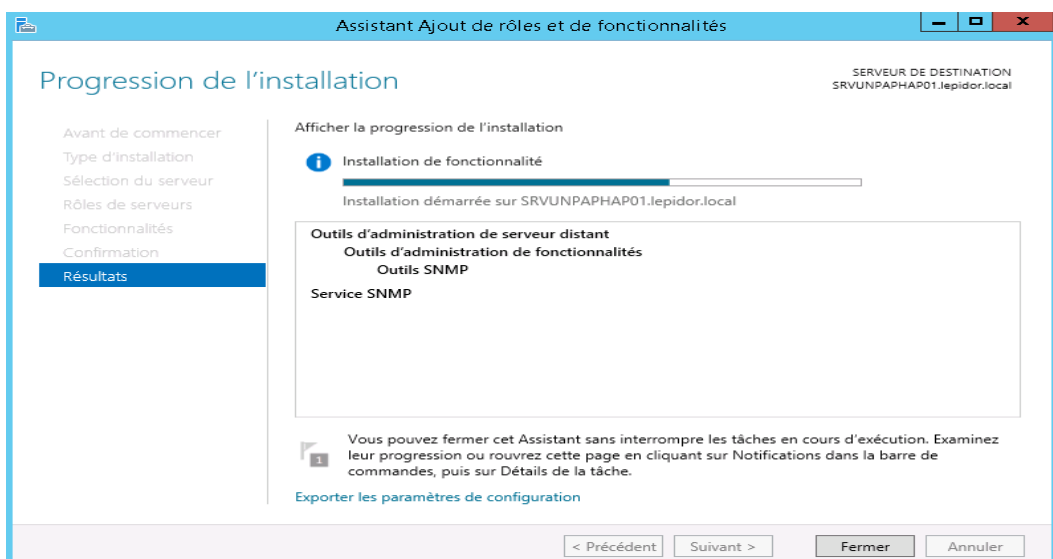
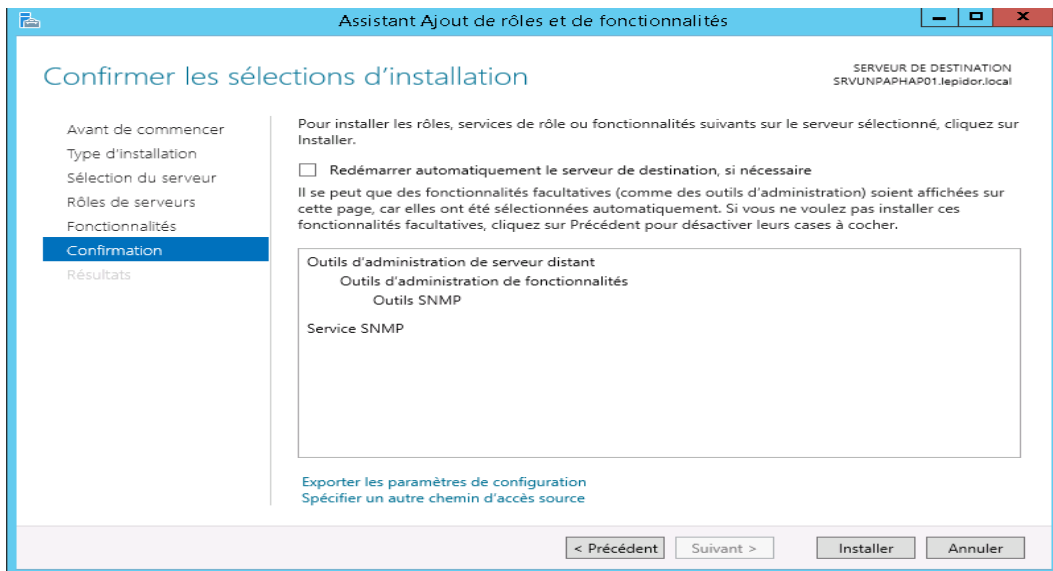
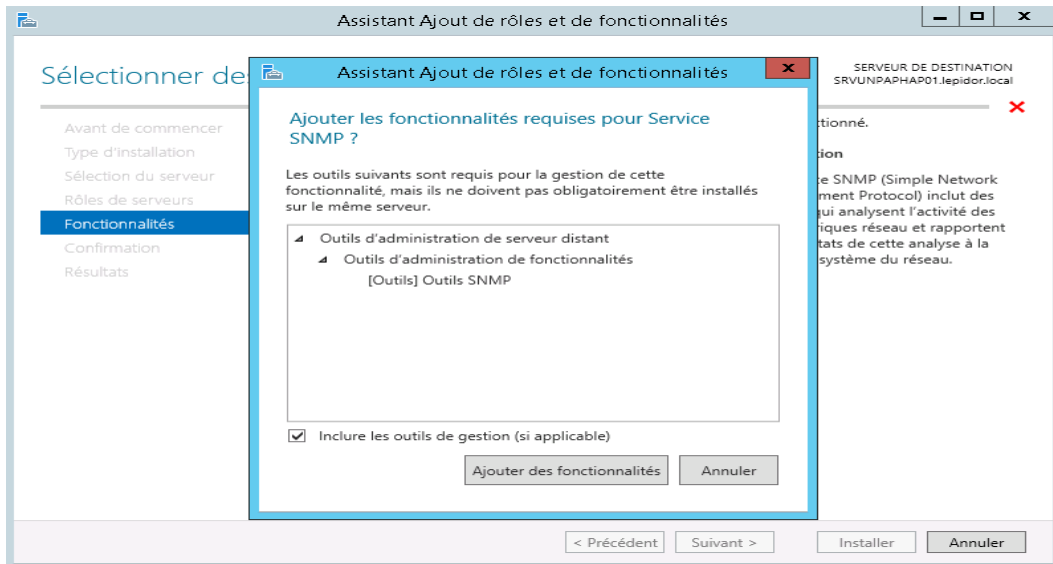
```
SW-GMA(config)#interface vlan 101
SW-GMA(config-if)#ip
SW-GMA(config-if)#ip add
SW-GMA(config-if)#ip address 255.255.255.0
SW-GMA(config-if)#
```

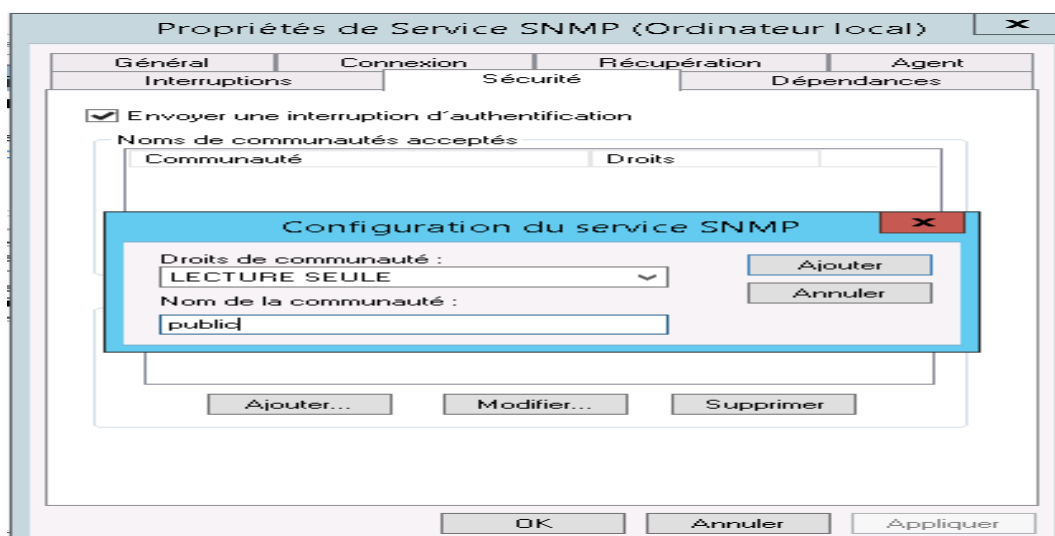
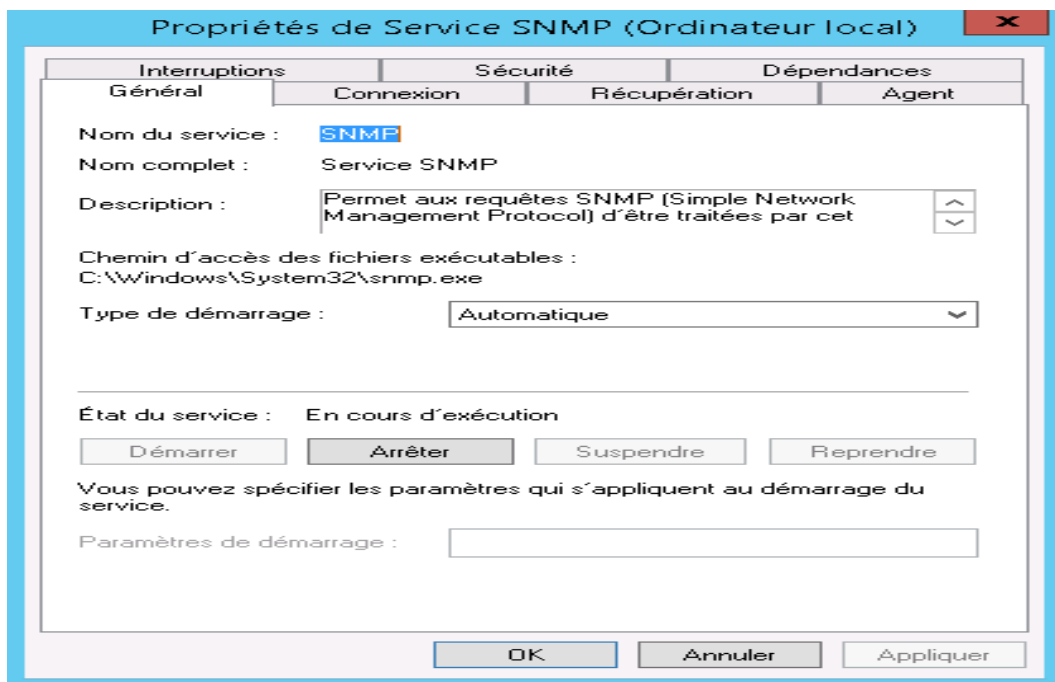
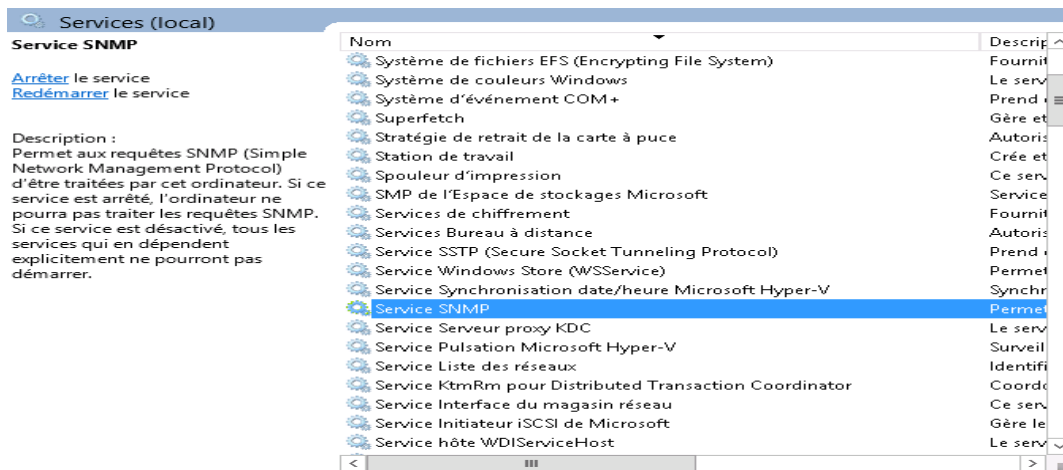
Activer le service SNMP en appliquant les règles de sécurité qui exigent la suppression de communauté SNMP par défaut PUBLIC et de créer une communauté SNMP propriétaire.

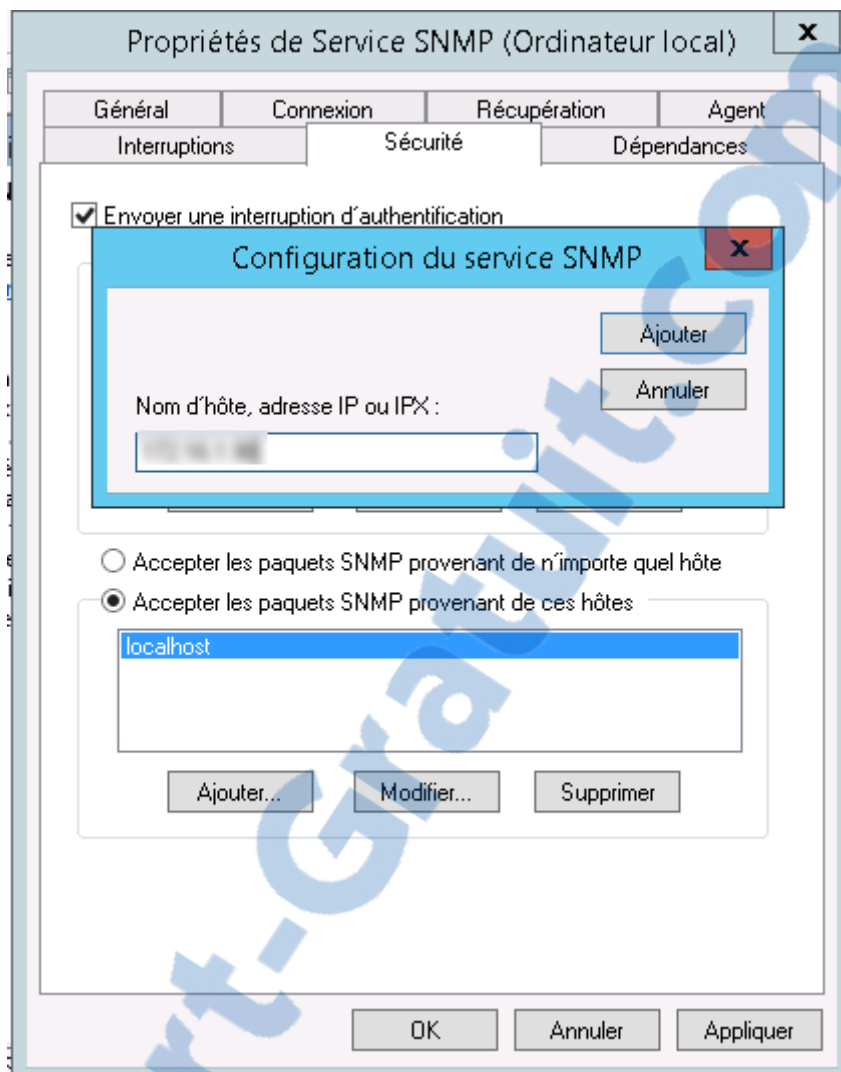
```
SW-GMA(config)#no snmp-server community public RO
SW-GMA(config)#snmp-server community RO
SW-GMA(config)#snmp-server host
```

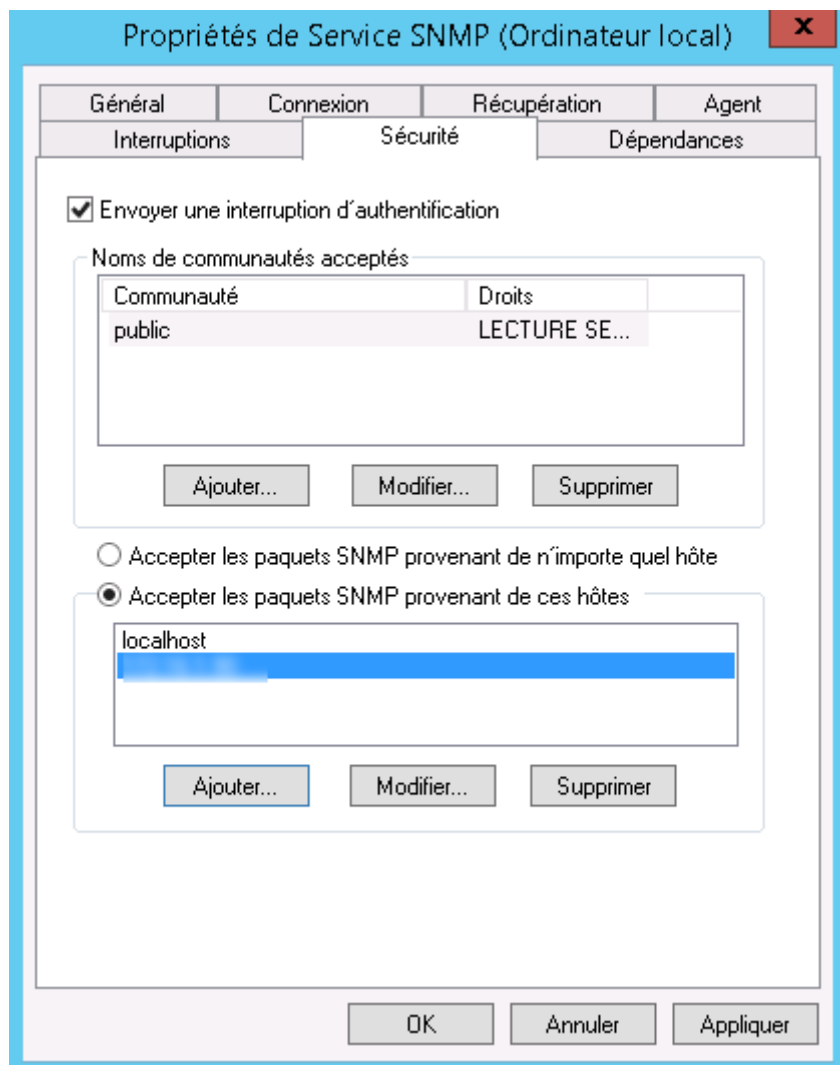
✓ Serveur Windows:



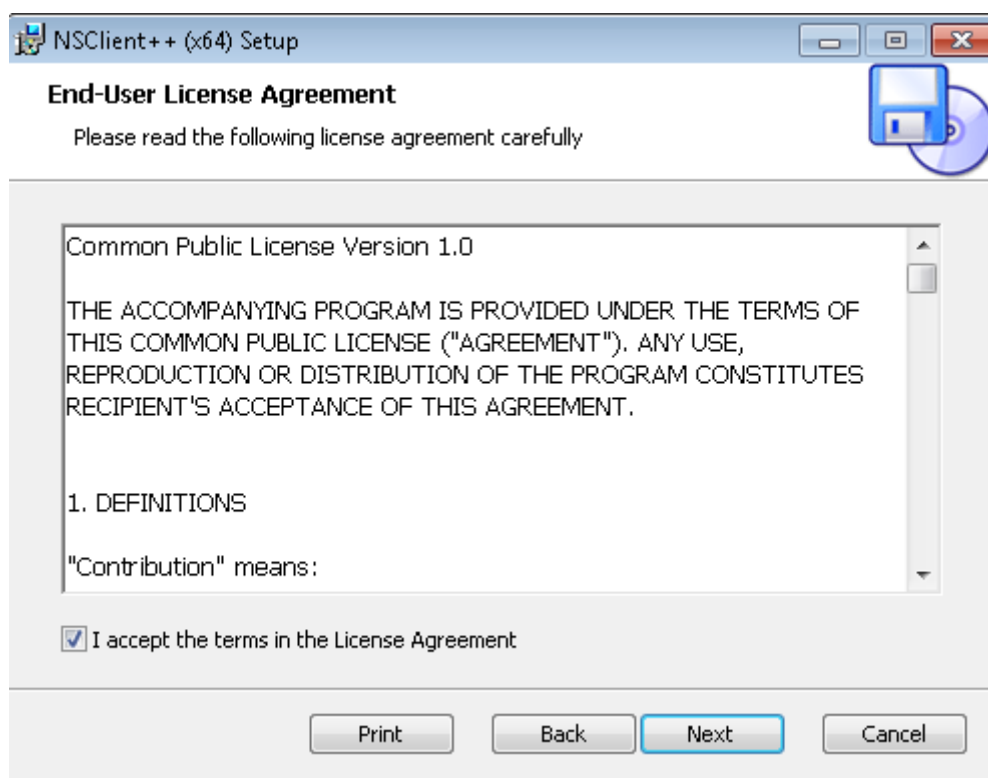
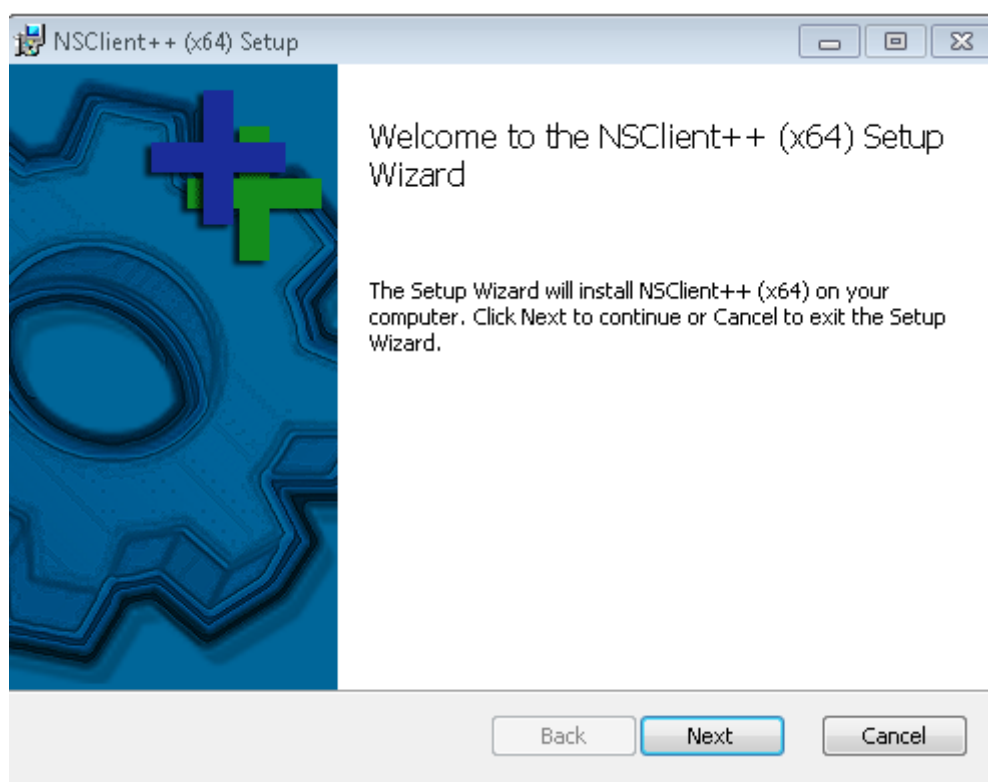








2) Installation de NS client



```

; ALLOWED HOSTS - A comaseparated list of allowed hosts. You can use netmasks (/ syntax) or * to create ranges.
allowed hosts = 172.16.1.0/24,172.16.1.0

; PASSWORD - Password used to authenticate against server
password = admin*789

; A list of aliases available. An alias is an internal command that has been "wrapped" (to add arguments). Be careful so you don't create loops.
[[/settings/external scripts/alias]

; alias_cpu - Alias for alias_cpu. To configure this item add a section called: /settings/external scripts/alias/alias_cpu
alias_cpu = checkCPU warn=80 crit=90 time=5m time=1m time=30s

; alias_cpu_ex - Alias for alias_cpu_ex. To configure this item add a section called: /settings/external scripts/alias/alias_cpu_ex
alias_cpu_ex = checkCPU warn=$ARG1$ crit=$ARG2$ time=5m time=1m time=30s

; alias_disk - Alias for alias_disk. To configure this item add a section called: /settings/external scripts/alias/alias_disk
alias_disk = CheckDriveSize MinWarn=10% MinCrit=5% CheckAll FilterType=FIXED

; alias_disk_loose - Alias for alias_disk_loose. To configure this item add a section called: /settings/external scripts/alias/alias_disk_loose
alias_disk_loose = CheckDriveSize MinWarn=10% MinCrit=5% CheckAll FilterType=FIXED ignore-unreadable

; alias_event_log - Alias for alias_event_log. To configure this item add a section called: /settings/external scripts/alias/alias_event_log
alias_event_log = CheckEventLog file=application file=system MaxWarn=1 MaxCrit=1 "filter=generated gt -2d AND severity NOT IN ('success', 'in

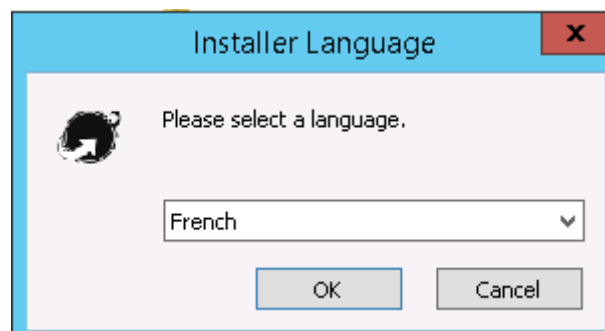
; alias_file_age - Alias for alias_file_age. To configure this item add a section called: /settings/external scripts/alias/alias_file_age
alias_file_age = checkFile2 filter=out "file=$ARG1$" filter-written=>1d MaxWarn=1 MaxCrit=1 "syntax=%filename% %size%"

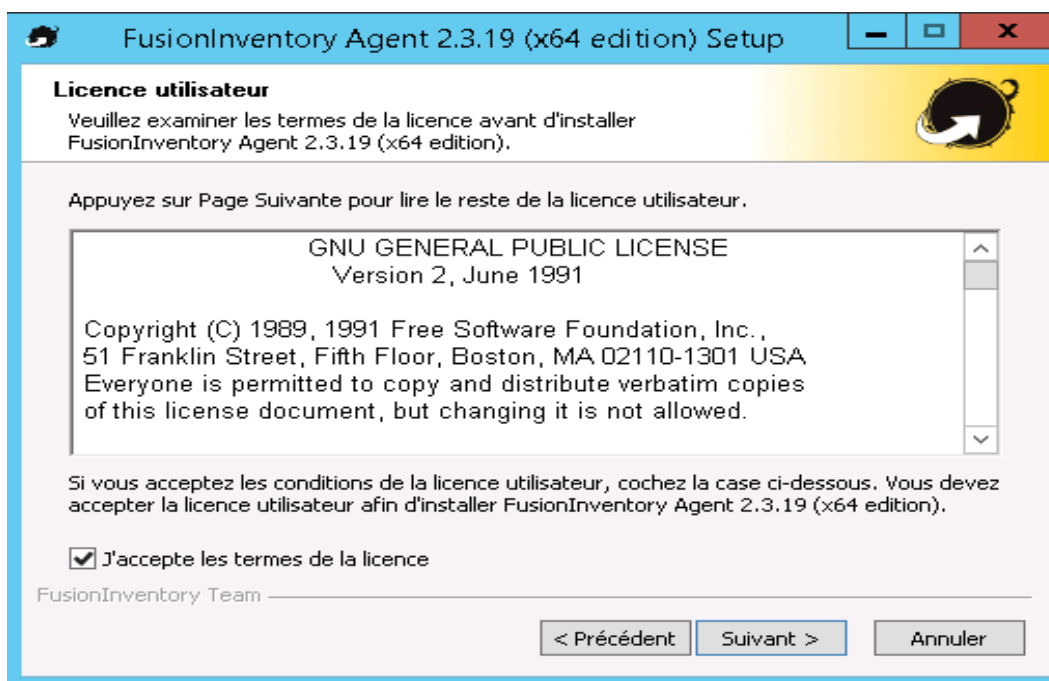
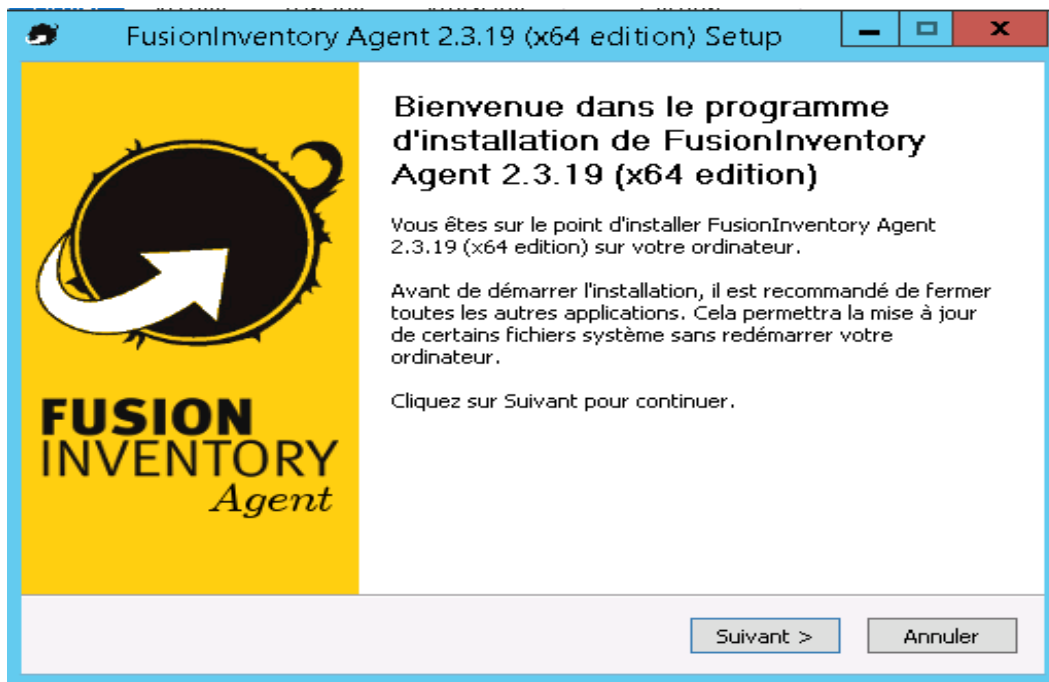
; alias_file_size - Alias for alias_file_size. To configure this item add a section called: /settings/external scripts/alias/alias_file_size
alias_file_size = CheckFiles "filter=size > $ARG2$" "path=$ARG1$" MaxWarn=1 MaxCrit=1 "syntax=%filename% %size%" max-dir-depth=10

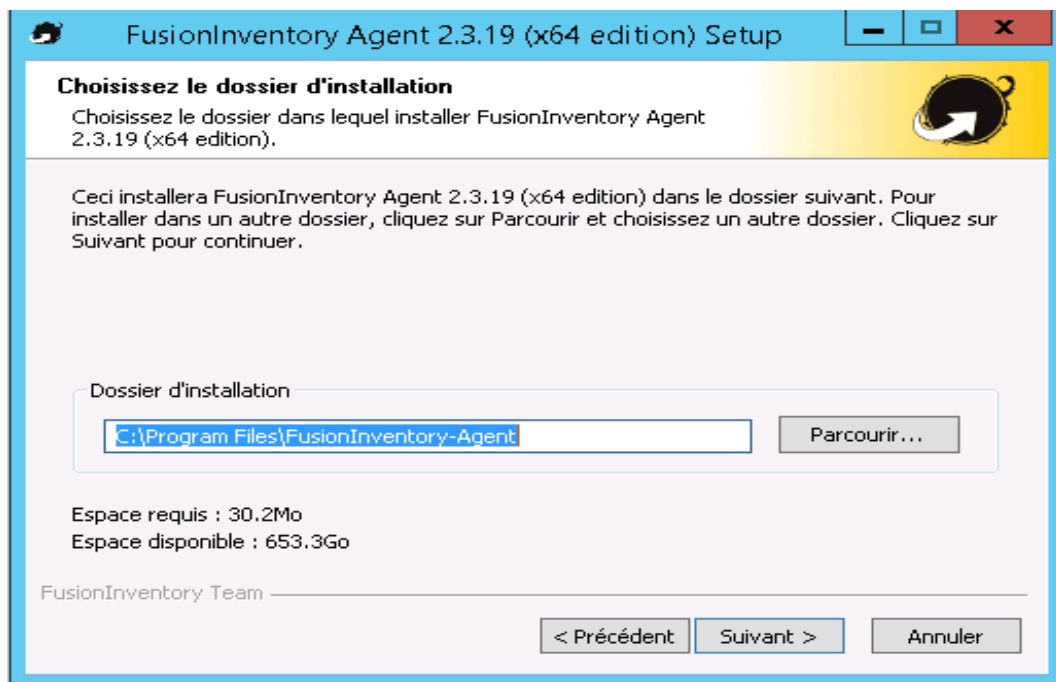
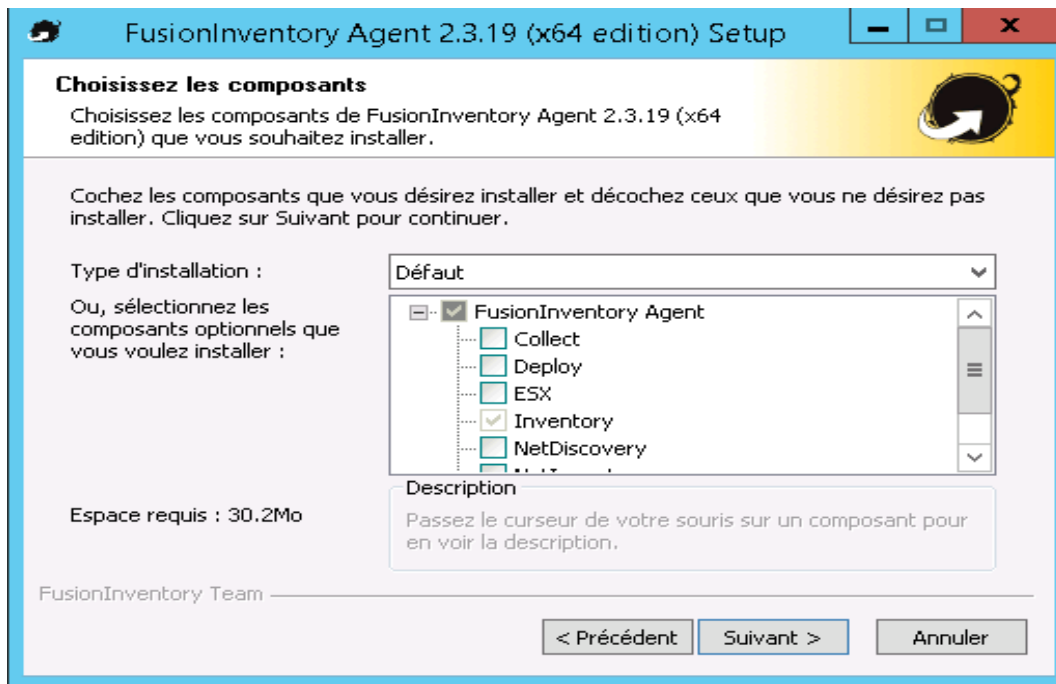
; alias_mem - Alias for alias_mem. To configure this item add a section called: /settings/external scripts/alias/alias_mem

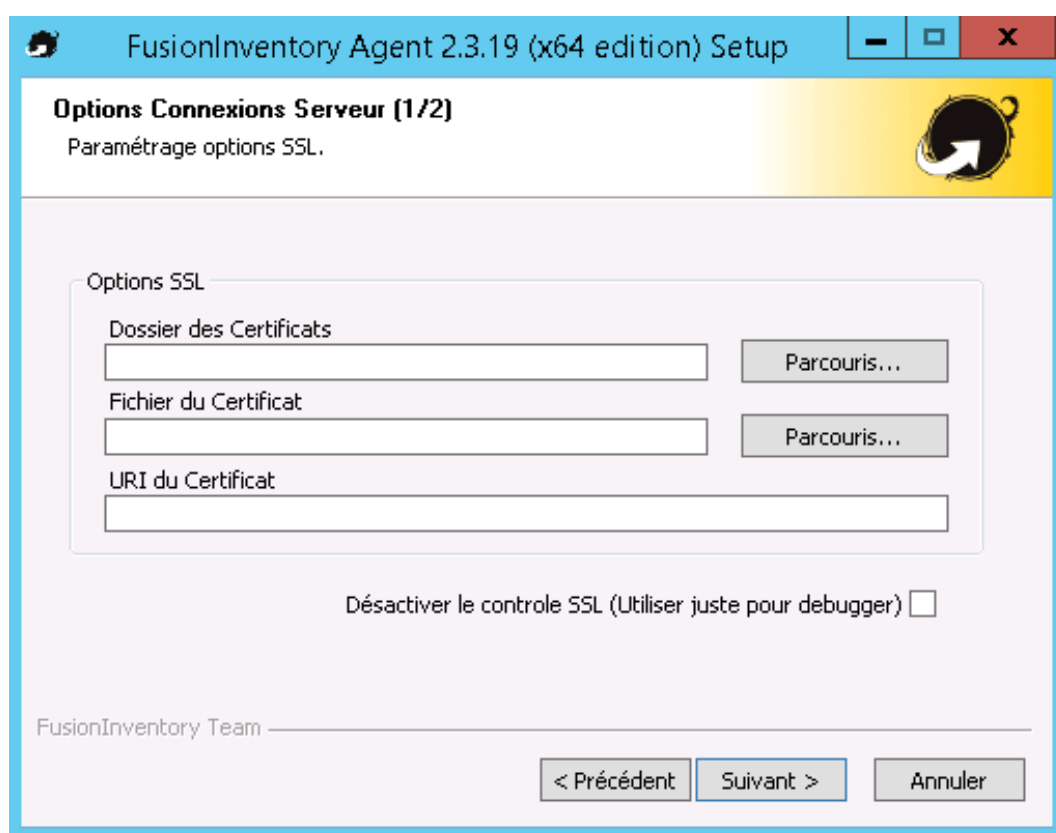
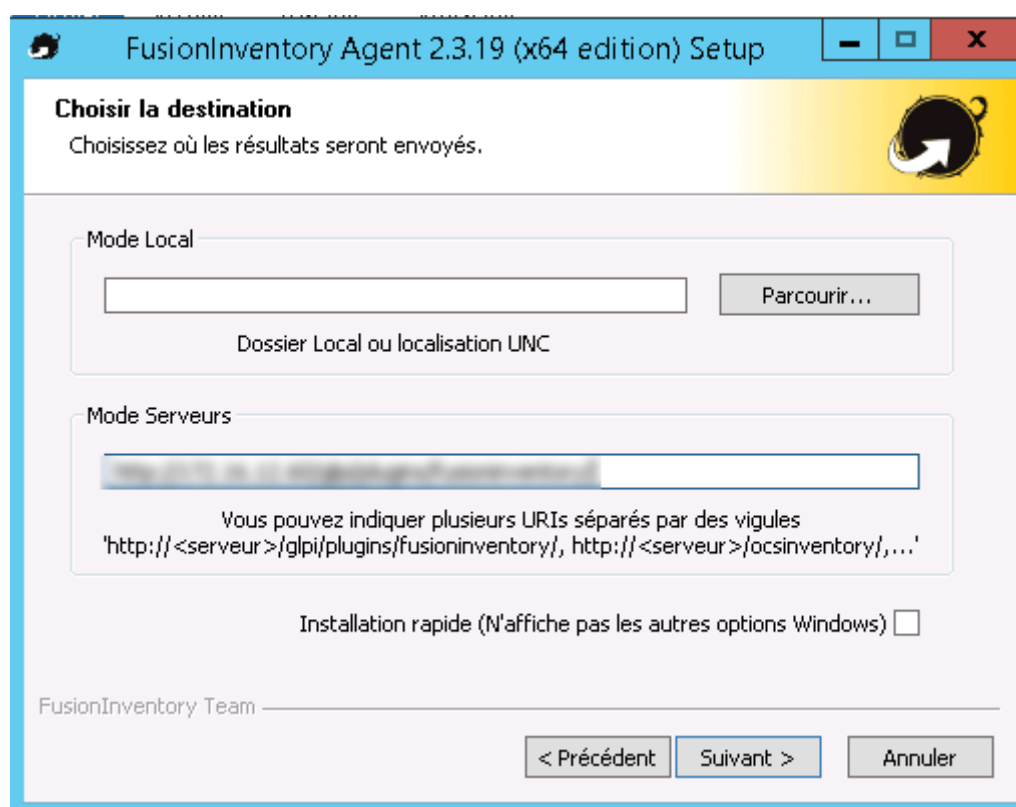
```

3) Installation de FusionInventory agent









FusionInventory Agent 2.3.19 (x64 edition) Setup

Options Connexions Serveurs (2/2)
Paramétrage options du proxy.

Options Proxy

Serveur

Utilisateur

Mot de Passe

FusionInventory Team

< Précédent Suivant > Annuler

FusionInventory Agent 2.3.19 (x64 edition) Setup

Choisir le mode d'Exécution
Choisissez la façon dont vous voulez que FusionInventory Agent soit exécuté.

Mode d'Exécution

☒ Comme un Service Windows

☐ Comme une Tâche Windows

☐ Manuellement

FusionInventory Team

< Précédent Suivant > Annuler

FusionInventory Agent 2.3.19 (x64 edition) Setup

Options du serveur HTTP
Paramétrage des options du serveur HTTP intégré.

Options du Serveur HTTP Intégré

IP Port

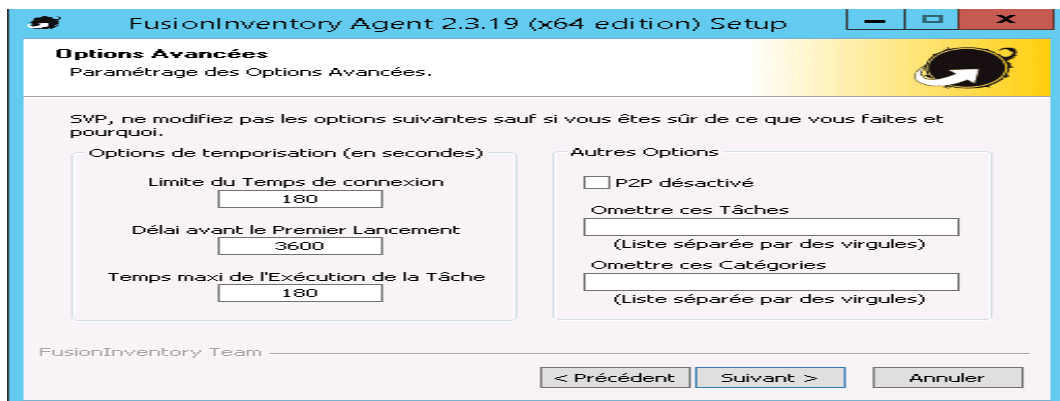
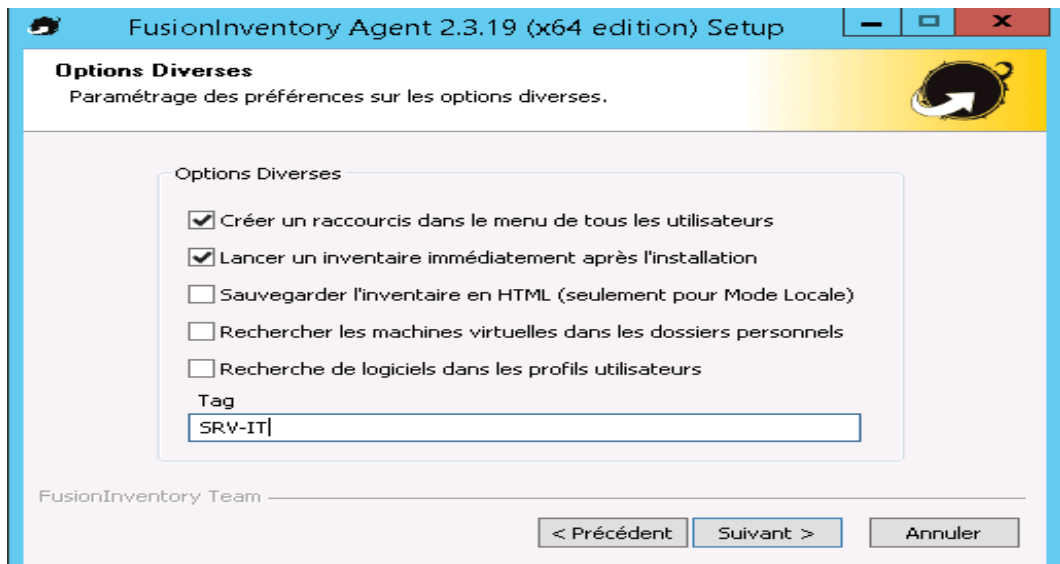
IPs de Confiance

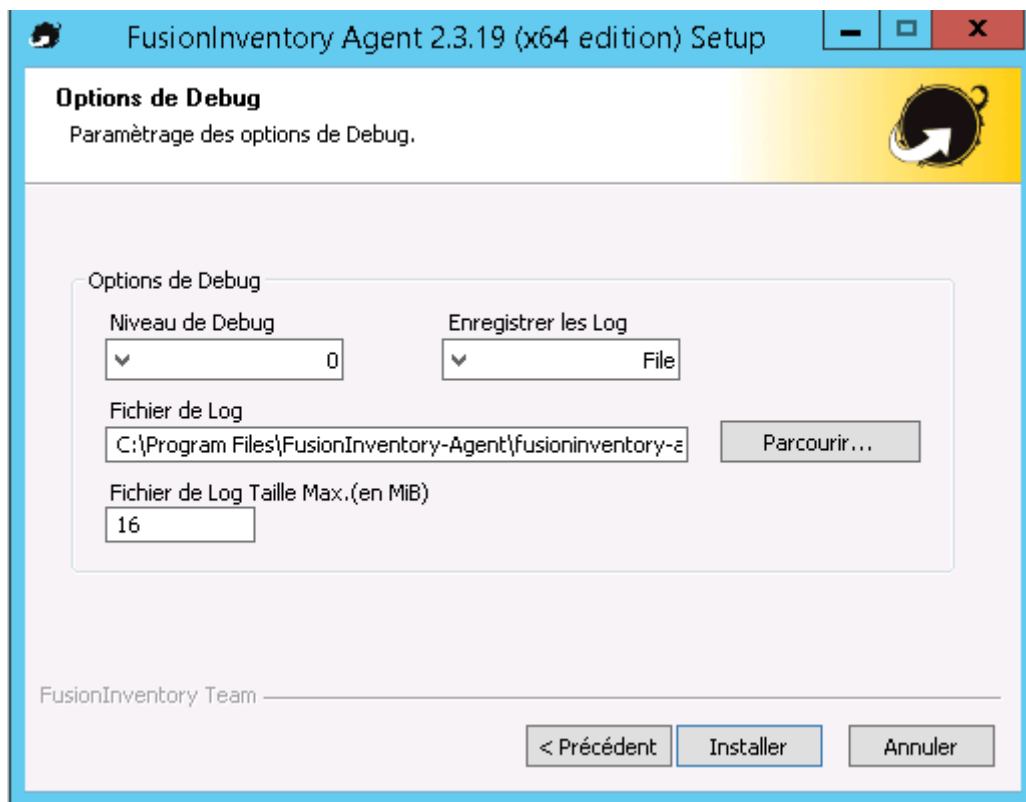
Ajouter une exception dans le Firewall de Windows ☒

Activer le serveur HTTP intégré ☒

FusionInventory Team

< Précédent Suivant > Annuler





Annexe F : Configuration Nagios avec Centreon

Il faut bien noter que pour toute modification (ajouté un groupe de périphériques, une ou plusieurs machines dans centreon) il faut faire la manipulation suivante pour envoyer les modifications vers nagios

Aller dans Configuration/Monitoring Engine (1) et cocher toutes les cases comme suit (2) et cliquer sur « **export** » (2)

➤ Ajouter un utilisateur

Pour créer un utilisateur. Il suffit de se connecter sur l'interface Centreon puis dans configuration(1)/utilisateurs(2)/ajouter(3)

Alias / Login	Full Name	Email	Host Notification Period	Services Notification Period	Language	Access	Admin	Status	Options
sbahri	Bahri_SAMI	sami.bahri@lepidor.com.tn	24x7 (d,u,r,f,s)	24x7 (w,u,c,r,f,s)	en_US	Enabled	No	Enabled	
guest	Guest	guest@localhost	24x7 (n)	24x7 (n)	en_US	Disabled	No	Enabled	
nagiosadmin	nagiosadmin_nagiosadmin	mehdi.hattab@lepidor.com.tn	24x7 (d,u,r)	24x7 (w,u,c)	en_US	Enabled	Yes	Enabled	
admin	Supervisor	root@localhost	24x7 (n)	24x7 (n)	en_US	Enabled	Yes	Enabled	
user	User	user@localhost	24x7 (n)	24x7 (n)	en_US	Enabled	No	Enabled	

1-Nom de session :

General Information | Centreon Authentication | Additional Information

Save Res

Modify a User

General Information

Alias / Login * sbahri 1

Full Name * Bahri_SAMI 2

Email * sami.bahri@lepidor.com.tn 3

Pager

Contact template used

Group Relations

Linked to Contact Groups

Guest Available

Supervisors Selected

Add Remove 4

Notification

Enable Notifications ☒ Yes ☐ No ☐ Default 5

Host

Host Notification Options ☒ Down ☒ Unreachable ☒ Recovery ☒ Flapping ☒ Downtime Scheduled ☐ None

Host Notification Period 24x7

Host Notification Commands

host-notify-by-email
host-notify-by-epager
host-notify-by-jabber
notify-by-email
notify-by-epager
notify-by-jabber
notify-by-sendmailservices

host-notify-by-sendmailhost Selected

Add Remove 6

Service

Service Notification Options ☒ Warning ☒ Unknown ☒ Critical ☒ Recovery ☒ Flapping ☒ Downtime Scheduled ☐ None 7

Service Notification Period 24x7 8

Service Notification Commands

host-notify-by-email
host-notify-by-epager
host-notify-by-jabber
notify-by-email
notify-by-epager
notify-by-jabber
notify-by-sendmailservices

host-notify-by-sendmailhost Selected

2-Nom complet

3-Email de notification

4-Groupe Utilisateur

5-Activation de Notification

6-Commande de Notification

7-Type de Notification

8-Periode de Notification

➤ Ajouter un Host

Aller dans configuration/host/ajouter

The screenshot shows the Nagios Core web interface for configuring a host. The main content area is titled 'Modify a Host' and contains several sections:

- General Information:** Fields for Host Name (Assabil), Alias (Assabil), IP Address / DNS (172.16.12.52), and SNMP Community & Version. A 'Resolve' button is next to the IP field.
- Host Check Properties:** Fields for Check Period (24x7), Check Command, Args, Max Check Attempts (5), Normal Check Interval (2 * 60 seconds), and Retry Check Interval (1 * 60 seconds). There are also radio buttons for Active Checks Enabled and Passive Checks Enabled.
- Macros:** A table for Custom macros with columns for Macro name and Macro value.
- Notification:** A section for Notification Enabled (radio buttons for Yes, No, Default) and Linked Contacts. It shows a list of Available contacts (Guest, User) and a list of Selected contacts (Bahri_SAMI, nagiosadmin_nagiosadmin, Supervisor).

1-Nom de Machine

2-Description de l'ordinateur

3-Adresse IP de la machine

4-Communauté SNMP, par défaut Public

5-Template de Machine

6-Période de vérification

7-Nombre d'essais maximum avant l'envoi de mail en cas d'échec

8-Lorsque le statut est OK, le service est vérifié toutes les x minutes

9-intervalle de vérification

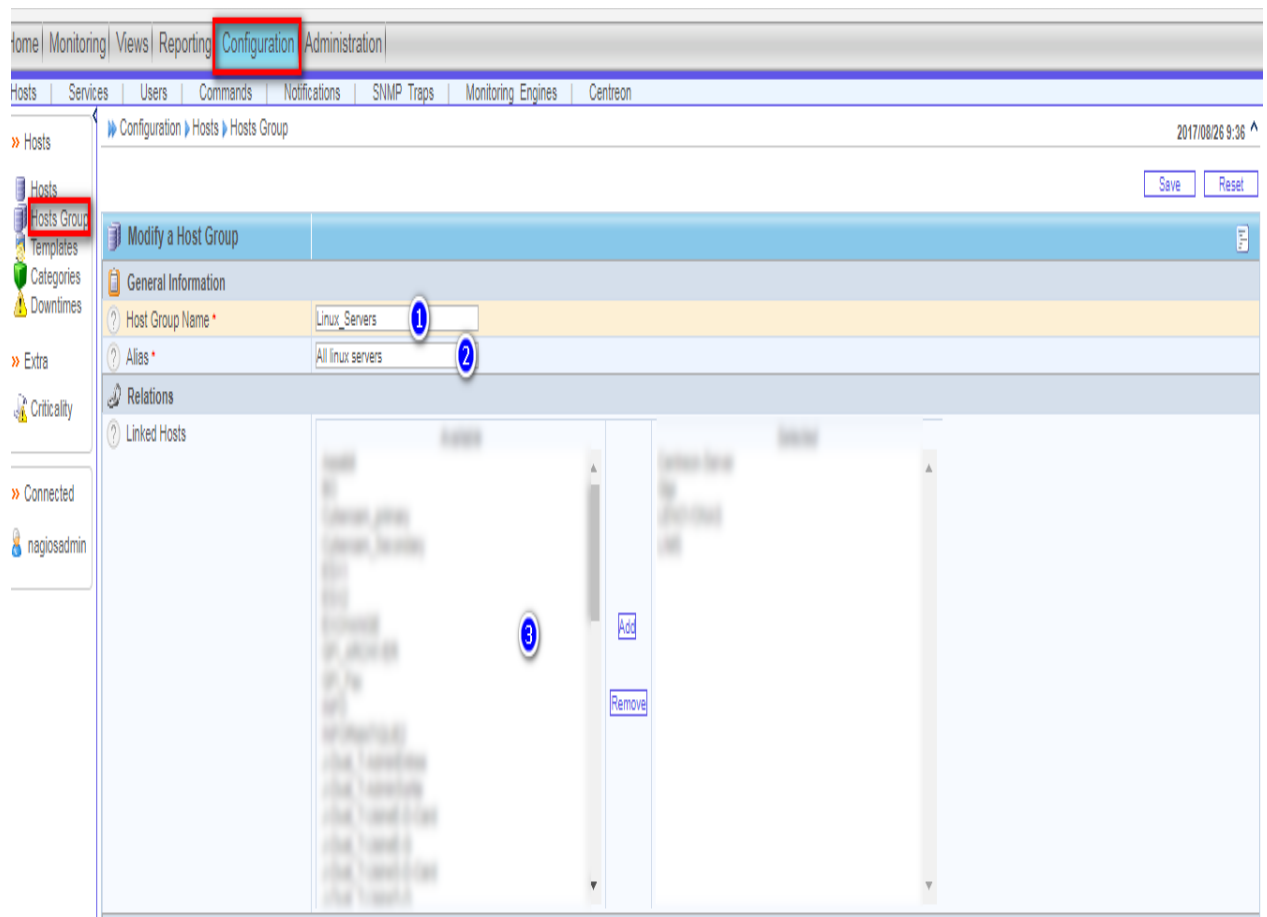


10-Activation désactivation de notification

11-Groupe de notification

➤ Création des hosts groups

Aller dans configuration/host/ajouter



1-Nom de Groupe

2-Description de Groupe

3-Host attribué au groupe

➤ Ajouter un service

Aller dans configuration/service/ajouter

The screenshot shows the Nagios service configuration page. The left sidebar contains navigation links: Templates, Categories, Downtimes, Meta Services, Extra, Criticality, and Connected (nagiosadmin). The main form is divided into sections: General Information, Service State, Macros, and Notification. Numbered annotations (1-10) point to specific fields: 1. Description field (value: check_fip); 2. Check Period dropdown (value: 24x7); 3. Check Command dropdown (value: check_fip); 4. Max Check Attempts input (value: 5); 5. Normal Check Interval input (value: 1) with a unit dropdown (value: 60 seconds); 6. Retry Check Interval input (value: 1) with a unit dropdown (value: 60 seconds); 7. Active Checks Enabled radio button (selected: Yes); 8. Implied Contacts 'Selected' list (values: Bahri_SAMI, nagiosadmin_nagiosadmin); 9. Notification Interval input (value: 1) with a unit dropdown (value: 60 seconds); 10. Notification Type checkboxes (Warning, Unknown, Critical, Recovery, Flapping, Downtime Scheduled).

1-Nom de service

2-Periode de vérification

3-commande exécuté

4- Nombre d'essais maximum avant l'envoi de mail en cas d'échec

Annexe G : Configuration GLPI

➤ Activation authentification LDAP

Aller dans configuration/Authentification/Annuaire LDAP /Ajouter

Remplir les informations de connexion au serveur AD

Glpi Parc Assistance Gestion Outils Plugins Administration **Configuration**

Accueil Configuration **Authentification** **Annuaire LDAP** + Q

Annuaire LDAP - glpi 1/1

Annuaire LDAP

Tester
Utilisateurs
Groupes
Informations avancées
Réplicats
Historique
Tous

Annuaire LDAP

Nom: glpi Dernière modification: 2016-04-28 16:06

Serveur par défaut: Oui Actif: Oui

Serveur: Port (par défaut 389): 389

Filtre de connexion: (&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

BaseDN: DC=lepidor,DC=local

DN du compte (pour les connexions non anonymes): cn=administreur,cn=users,dc=lepidor,dc=local

Mot de passe du compte (pour les connexions non anonymes): Effacer Champ de l'identifiant: samaccountname

Commentaires:

Créé le Dernière mise à jour le 2016-04-28 16:06

Sauvegarder Supprimer définitivement

➤ Configuration de collecteur Mail

Collecteur - support@lepidor.com.tn 1/1

Collecteur

Actions
Historique
Tous

Nom (Courriel): support@lepidor.com.tn

Actif: Oui

Serveur: **Serveur Exchange**

Options de connexion: IMAP SSL NO-TLS NO-VALIDATE-CERT

Dossier des messages entrants (optionnel, souvent INBOX): inbox

Port (optionnel):

Chaine de connexion: { /imap/ssl/nowalidate-cert/notls}inbox

Identifiant: support@lepidor.local

Mot de passe: Effacer

Utiliser une authentification Kerberos: Non

Dossier d'archivage des courriels acceptés (optionnel):

Dossier d'archivage des courriels refusés (optionnel):

Taille maximale des fichiers importés par le collecteur: 10 Mio

Utiliser la date du courriel au lieu de celle de la collecte: Oui

➤ Tache de découverte réseaux avec fusion inventory

En cours

0

Succès

1

Annulé

1

En erreur

0

UNPAINFPC04.lepidor.local-2017-09-04-11-15-05

2017-09-04 16:12:50

Total Found:85 Created:1 Updated:84

59ad77aeab50a

2017-09-04 16:12:50

Ok

Total Found:85 Created:1 Updated:84

2017-09-04 16:12:23

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:12:23

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:12:17

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:12:17

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:10:09

En cours d'exécution

[Détail] Mise à jour de l'objet Imprimante

2017-09-04 16:10:09

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:10:04

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:10:04

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:54

En cours d'exécution

[Détail] Mise à jour de l'objet Equipement

2017-09-04 16:09:53

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:50

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:09:50

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:30

En cours d'exécution

Import refusé [ip]:172.16.12.210, [name]

2017-09-04 16:09:30

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:28

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:09:28

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:28

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:09:28

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:20

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:09:20

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:10

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:09:09

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:09:09

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:09:09

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:59

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:59

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:52

En cours d'exécution

Import refusé [ip]:172.16.12.50, [name]

2017-09-04 16:08:52

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:48

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:47

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:47

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:47

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:46

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:46

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:46

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:46

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:45

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:45

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:45

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:45

En cours d'exécution

1 périphériques trouvés

2017-09-04 16:08:44

En cours d'exécution

[Détail] Mise à jour de l'objet Ordinateur

2017-09-04 16:08:44

En cours d'exécution

1 périphériques trouvés



GLOSSAIRE

UNPA : Usine Nouvelle des Pattes Alimentaires

RSSI : Responsable de la sécurité des systèmes d'information

FO : Fibre optique

FH : Faisceau hertzien

SMS: Short Message Service

ITIL: Information Technology Infrastructure Library

SLA: Service-level agreement

CI: configuration item

ISO: Organization international de normalization

GLPI : Gestion Libre de Parc Informatiques

FAN: Fully Automated Nagios

PHP: Hypertext Preprocessor

CPU: Central Processing Unit

HA: High Availability

VLAN: Virtual local Area Network

VPN: Virtual Private Network

FTP: File Transfer Protocol

DHCP: Dynamic Host Configuration Protocol

SMTP: Simple Mail Transfer Protocol

DNS: Domain Name System

SSH: Secure Shell

SNMP: Simple Network Management Protocol

HTTP: Hypertext Transfer Protocol

GSM: Global System for Mobile Communications

TCP: Transmission Control Protocol

IP: Internet Protocol

Webographie

<http://www.fullyautomatednagios.org/>

<https://www.nagios.org/>

<http://glpi-project.org/>

<https://www.centreon.com/solutions/>

<https://github.com>

<http://www.iti-france.com/>

<https://www.memoireonline.com/>