

	REPUBLIQUE TUNISIENNE ***** MINISTÈRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE ***** DIRECTION GENERALE DES ETUDES TECHNOLOGIQUES ***** INSTITUT SUPERIEUR DES ETUDES TECHNOLOGIQUES DE CHARGUIA ***** Département Technologies de l'Informatique	
---	--	---

Rapport de Projet de Fin d'Etudes

Présenté en vue de l'obtention de :

Licence Appliquée en Technologies de l'Informatique

Parcours : Réseaux et Services Informatiques

Sujet :

IMPLEMENTATION D'UNE ARCHITECTURE RESEAU
AVEC SOLUTION DE CONTROLE D'ACCES,
MONITORING & AUTOMATISATION

Elaboré par

Farhat Hiba & El Ghoul Essia

Encadrant académique : Mr BOUZIRI Zied

Encadrante professionnelle : Mme BEN HAMZA Dhouha

Société d'accueil : GlobalNet

Année universitaire : 2019/2020

Dédicaces

A mon très cher père

Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit.

Tu as toujours été à mes côtés pour me soutenir et m'encourager.

Que ce travail traduit ma gratitude et mon affection.

A ma très chère mère

Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

A ma chère sœur et mes très chers frères

Pour votre soutien et encouragements, vous occupez une place particulière dans mon cœur.

A mes chères cousines

Pour leurs aides et supports dans les moments difficiles.

À mes amis proches, À tous ceux que j'aime et tous qui me sont chers...

HIBA FARHAT

Dédicaces

Au Dieu, tout puissant, mon créateur,
A la mémoire de mes grands-parents,
A mon père, pour ses sacrifices et sa patience,
A ma mère, ma raison d'être et ma raison de vivre,
A ma sœur pour son aide et ses encouragements,
A mes amis, à tous mes proches,
A tous mes enseignants qui ont contribué à ma formation,
Je leurs dédie ce modeste travail en espérant qu'il soit validé.

ESSIA EL GHOUЛ

Remerciements

Nous tenons à remercier tous les membres du jury pour l'honneur qu'ils nous ont accordé de vouloir juger et accepter d'évaluer notre travail.

Nous exprimons nos vifs remerciements également à Monsieur Zied BOUZIRI, notre tuteur pédagogique à ISET CHARGUIA, pour sa disponibilité, son aide, ses précieux conseils, ses critiques constructives, ses explications et suggestions pertinentes ainsi que pour ses qualités humaines et morales que nous avons toujours appréciées.

Nous adressons aussi nos remerciements à Madame Dhouha Ben Hamza d'avoir répondu favorablement pour nous encadrer durant toute la période du déroulement de notre Projet de Fin d'Etudes et de nous soutenir sur le plan scientifique par sa contribution et ses efforts considérables en nous fournissant les informations nécessaires à ce projet.

Nos sincères gratitude à tout le personnel de Globalnet pour les conditions favorables et l'ambiance de travail agréable créées au sein de leur société durant le déroulement de notre stage.

Sommaire

Introduction générale.....	1
Chapitre 1 : Présentation du cadre du stage.....	2
Introduction	2
1. Présentation de la société	2
2. Présentation du domaine de gestion de réseaux :	3
2.1 L'automatisation informatique	3
2.2 La supervision informatique :	3
2.3 La virtualisation :	3
2.4 La sécurité :	3
3. Etude de l'existant :	3
3.1 Description de l'existant :	4
3.2 Critique de l'existant	4
3.3 Solution proposé	4
4. Méthodologie adoptée et langage de modélisation	4
4.1 Méthode de réalisation.....	4
4.2 Présentation de Scrum	6
4.2.1 Les rôles	7
4.2.2 Les évènements	7
4.2.3 Les cycles de la méthode scrum.....	8
4.3 Langage de modélisation	9
Conclusion.....	10
Chapitre 2 : Etat de l'art	11
Introduction	11
1. La supervision	11
1.1 Les objectifs et intérêts de la supervision	11
1.2 Pourquoi superviser	11
2. La virtualisation.....	12
2.1 Fonctionnement	12
2.2 Types de ressources virtualisées	12
2.2.1 Virtualisation des données	13
2.2.2 Virtualisation des postes de travail.....	13
2.2.3 Virtualisation de serveurs.....	13

2.2.4	Virtualisation des systèmes d'exploitation	13
2.2.5	Virtualisation des fonctions réseau.....	13
3.	VPN.....	13
3.1	Utilisation de VPN.....	13
3.1.1	Accès d'utilisateur distant sur Internet	13
3.1.2	Connexion de réseaux sur Internet	14
3.1.3	Connexion d'ordinateurs sur un intranet.....	14
3.2	Caractéristiques de VPN.....	14
4.	VLAN	15
4.1	Utilité des vlans	15
5.	L'automatisation Informatique.....	15
5.1	Pourquoi automatiser	15
5.2	Avantages	16
5.3	Intérêt d'automatisation de la supervision.....	16
6.	Le protocole SNMP.....	17
6.1	Présentation	17
6.1.1	Fonctionnement.....	17
6.1.2	La MiB	18
7.	Protocole SSH	19
8.	Protocole AAA.....	19
8.1	Protocole RADIUS	20
8.1.1	Fonctionnement.....	20
8.2	Protocole TACACS+.....	21
8.2.1	Fonctionnement.....	21
8.3	Comparaison.....	22
8.4	Les outils de monitoring	22
8.4.1	Les plateformes éditeurs.....	22
8.4.2	Les plateformes libres	23
8.5	Les outils d'automatisation.....	27
Conclusion.....		27
Chapitre 3: Sprint 0 Spécification des besoins		28
Introduction		28
1. Spécification des besoins		28

1.1	Besoins fonctionnels.....	28
1.2	Besoins non fonctionnels.....	29
1.3	Backlog général du produit.....	29
1.4	Diagramme de cas d'utilisation général	32
1.4.1	Identification d'acteurs :.....	32
1.4.2	Diagramme de cas d'utilisation	32
1.5	Diagramme d'activités	34
1.5.1	Diagramme d'activité « Notification ».....	34
1.6	Environnement de travail.....	35
1.6.1	Environnement matériel :	35
1.6.2	Environnement logiciel	36
1.7	Architecture de projet	39
1.8	Planification de la release	41
	Conclusion.....	42
	Chapitre 4 : Sprint 1 mise en place de l'outil de supervision.....	43
	Introduction	43
1.	Spécification fonctionnelle.....	43
1.1	Le Backlog du sprint.....	43
1.2	Diagramme de cas d'utilisation du sprint 1	44
1.3	Réalisation	44
1.3.1	Installation.....	45
1.3.2	Installation et configuration de l'agent SNMP	46
1.3.3	Ajout des commandes	47
1.3.4	Ajout des hôtes à superviser	48
1.3.5	Création graphique avec cacti	50
1.3.6	Génération des rapports.....	57
1.3.7	Notifications par mail.....	61
1.4	Revue de sprint	61
1.5	Rétrospectives.....	62
1.6	Burndown chart	62
	Conclusion.....	62
	Chapitre 5 : Sprint 2 Implémentation d'une connexion VPN et serveur d'authentification	63
	Introduction	63

1.	Spécification fonctionnelle.....	63
1.1	Le Backlog du sprint.....	63
1.2	Diagramme de cas d'utilisation « Authentification »	64
2.	Réalisation	65
2.1	Mise en place d'un réseau privé virtuel :	65
2.1.1	Configuration du routeur.....	65
2.1.2	Test d'accès VPN à distance	67
3.	Configuration du AAA.....	72
3.1	Configuration de serveur FreeRADIUS	73
3.2	Configuration du routeur comme client.....	80
3.3	Revue de sprint	82
3.4	Rétrospective	82
3.5	Burndown chart	83
	Conclusion.....	83
	Chapitre 6 : sprint 3 automatisation de la supervision avec ansible	84
	Introduction	84
1.	Spécification fonctionnelle :.....	84
1.1	Backlog du sprint :.....	84
1.2	Diagramme de cas d'utilisation du sprint 3	85
2.	Réalisation.....	86
2.1	Configuration Ansible	86
2.1.1	Sécurisation des transferts	86
2.1.2	Configuration du fichier inventaire ansible.....	87
2.2	Automatiser la configuration snmp :	88
2.3	Automatisation de l'ajout des machines dans le serveur EON	89
2.3.1	Génération d'une clé API.....	89
2.3.2	Création d'une page web dynamique	90
2.3.3	Création de playbook ansible et script bash	91
2.3.4	Exécution de playbook	92
2.4	Revue de sprint	93
2.5	Rétrospectives.....	94
2.6	Burndown chart	94
	Conclusion.....	95

Annexe A: Installation VMware ESXi	96
1. Installation de VMware ESXi sur VMware Workstation	96
ANNEXE B : Configuration snmp.....	102
2. Configuration SNMP de VMware ESXi	102
3. Installation et configuration de l'agent SNMP de Windows.....	104
3.1 Installation et configuration de l'agent SNMP de CentOS 7.....	108
ANNEXE C : Installation FreeRADIUS sur Ubuntu 18.04	113
Conclusion générale	118

Liste des figures

Figure 1 : les cycles de méthode scrum.....	8
Figure 2 : structure de table MIB.....	19
Figure 3 : Les éléments de serveur RADIUS	21
Figure 4 : Fonctionnement du protocole TACACS+.....	22
Figure 5 : Diagramme de cas d'utilisation général	33
Figure 6 : Diagramme cas d'utilisation Gestion des services.....	33
Figure 7: Diagramme d'activités.....	35
Figure 8 : Composants d'Eyes-of-network.....	37
Figure 9 : Architecture VMware ESXi.....	38
Figure 10 : Architecture du projet	39
Figure 11: Diagramme de cas d'utilisation du sprint 1	44
Figure 12 : Interface web d'ESXi.....	45
Figure 13 : interface web eyes of network	46
Figure 14: Configuration de fichier /etc/snmp/snmpd.conf	46
Figure 15 : Configuration snmp routeur.....	47
Figure 16 : configuration web d'Eon	47
Figure 17 : éditeur de commandes	47
Figure 18: liste des équipements	48
Figure 19 : ajout d'un hôte.....	48
Figure 20 : Etat des hôtes	49
Figure 21 : Etats des hôtes et services supervisés	49
Figure 22 : Menu Cacti.....	50
Figure 23 : Importation des hôtes.....	50
Figure 24 : Interface Cacti.....	51
Figure 25 : Tableau de bord Cacti	51
Figure 26 : Liste des équipements importés	52
Figure 27 : Création d'un nouveau graphe.....	52
Figure 28 : Validation des choix de la création de graphe	53
Figure 29 : Création des graphes avec succès	53
Figure 30 : Accès à la liste des graphes.....	54
Figure 31 : Liste des graphes créés	54
Figure 32 : Graphe Memory Usage du serveur Freeradius en cours de création	55
Figure 33 : Accès à l'arborescence des graphes.....	55
Figure 34 : Création d'une nouvelle arborescence des graphes	55
Figure 35 : Ajout d'un nouveau graphe à l'arborescence	56
Figure 36 : Validation des choix du type d'arborescence et du graphe	56
Figure 37 : Liste des graphes ajoutés à l'arborescence.	56
Figure 38 : Schéma d'accès au rapport tendances.	57
Figure 39 : Choix du type d'hôte.....	57
Figure 40 : Choix de l'hôte.....	58
Figure 41 : Options du rapport	58
Figure 42 : Rapport tendances du serveur Freeradius	58

Figure 43 : Choix de la création du rapport SLA technique.....	59
Figure 44 : Rapport SLA du serveur Freeradius	59
Figure 45 : Schéma d'accès au 'performances'	60
Figure 46 : Rapport performances du serveur Freeradius	60
Figure 47 : notifications par mail	61
Figure 48: Burndown chart sprint 1	62
Figure 49 : Diagramme de cas d'utilisation « Authentification »	64
Figure 50 : Configuration VPN du routeur	65
Figure 51 : configuration mode tunnel et algorithmes.....	65
Figure 52: Configuration model aaa.....	66
Figure 53 : Configuration pool d'adresses et autorisation de trafic.....	66
Figure 54 : Configuration de carte de chiffrement	66
Figure 55 : liaison entre carte dynamique et carte statique.	67
Figure 56 : Lier la carte à une interface.....	67
Figure 57 : Liste des associations de sécurité ISAKMP	67
Figure 58 : Création d'une nouvelle entrée de connexion.....	68
Figure 59 : Les informations de l'entrée de connexion à créer	68
Figure 60 : Etablissement d'une connexion VPN	69
Figure 61 : Authentification de l'utilisateur pour l'entrée de connexion créé	69
Figure 62 : Sécurisation du canal de communication.....	70
Figure 63 : Etablissement de la connexion avec succès	70
Figure 64 : Accès aux statistiques de tunnel de VPN client.....	71
Figure 65 : Détails de tunnel	71
Figure 66 : Détails des routes sécurisées.....	72
Figure 67 : nouvelle associations ISAKMP ajoutée.....	72
Figure 68 : Edition du fichier sql.....	73
Figure 69 : Redémarrage du service Freeradius	73
Figure 70 : Edition du fichier clients.conf.....	74
Figure 71 : Edition du fichier users	75
Figure 72 : Test de l'authentification freeradius en local.....	75
Figure 73 : Authentification radius dans les routeurs R1 et R2	76
Figure 74: page d'accueil daloRADIUS	76
Figure 75 : ajout d'un user dans daloRADIUS	77
Figure 76 : Validation des données de l'utilisateur	77
Figure 77 : les privilèges d'un user	78
Figure 78 : Liste users	78
Figure 79 : ajout d'un NAS	79
Figure 80 : Liste NAS	79
Figure 81 : Déclaration des éléments de groupe radius.....	80
Figure 82 : Configuration de l'authentification au niveau du routeur.....	80
Figure 83 : Configuration de ligne vty	80
Figure 84 : Test d'authentification à distance d'user avec privilèges 15	81
Figure 85 : Accès à distance au mode de configuration du routeur	81
Figure 86 : Test d'authentification à distance d'user avec privilèges 3	81

Figure 87 : Burndown chart sprint3	83
Figure 88: Diagramme de cas d'utilisation du sprint 3.....	85
Figure 89 : Génération des clés.	86
Figure 90: copie de clé publique.	87
Figure 91: Configuration de fichier d'inventaires.....	87
Figure 92: Test de connectivité	88
Figure 93: automatisation de configuration du snmp	88
Figure 94 : exécution du playbook de configuration snmp	89
Figure 95 : Clé API	90
Figure 96 : création d'une page web dynamique addHost	91
Figure 97 : playbook d'ajout machine	92
Figure 98 : script bash addHost.sh	92
Figure 99 : Exécution de playbook d'ajout des hôtes	92
Figure 100 : machines ajoutées avec succès	93
Figure 101 : Burndown chart de sprint 3.....	94
Figure 102 : Ajout d'une nouvelle machine virtuelle.....	96
Figure 103 : Choix tu type de configuration de la machine	96
Figure 104 : Choix de l'emplacement de l'image iso.....	97
Figure 105 : Choix du nom et de l'emplacement de la machine virtuelle.....	97
Figure 106 : Choix de la capacité du disque de la machine virtuelle	98
Figure 107 : Validation de la création de la machine.....	98
Figure 108 : Liste des machines virtuelles de VMware Workstation	99
Figure 109 : Choix du disque pour l'installation.....	100
Figure 110 : Choix de la langue	100
Figure 111 : Definition du mot de passe	100
Figure 112 : Confirmation de l'installation	101
Figure 113 : Redémarrage du serveur	101
Figure 114 : Démarrage de la machine virtuelle VMware ESXi	101
Figure 115 : Démarrage du service SSH	102
Figure 116 :Accès à VMWARE ESXI à distance avec putty	102
Figure 117: Configuration SNMP de VMWARE ESXI	103
Figure 118 : Selection menu Programmes	104
Figure 119 : Selection menu Programmes et fonctionnalités.....	104
Figure 120 : Activation du protocole SNMP	105
Figure 121 : Accès aux services de Windows	105
Figure 122 : Liste des services Windows	106
Figure 123 : Les propriétés du service SNMP	106
Figure 124 : Les informations de sécurité du service SNMP	107
Figure 125 : Ajout du nom de la communauté	107
Figure 126 : Ajout de l'adresse IP du serveur	107
Figure 127 : Ajout de l'adresse du serveur avec succès.....	108
Figure 128 : Installation du service snmpd.....	108
Figure 129 : Démarrage et statut du service snmp	109
Figure 130 : Edition du fichier /etc/snmp/snmpd.conf	109

Figure 131 : Installation de l'agent snmp	111
Figure 132 : Le statut du service snmpd.....	111
Figure 133 : Installation des mibs.....	111
Figure 134 : Edition du fichier /etc/snmp/snmpd.conf 2	112
Figure 135 : Mise à jour de la cache des paquets.....	113
Figure 136 : Installation de freeradius et de la base de données mysql	113
Figure 137 : création d'une nouvelle base de données.....	113
Figure 138 : Attribution des privilèges.....	114
Figure 139 : Mise à jour et importation de la base de données	114
Figure 140 : Installation apache, php et d'autres packages	114
Figure 141 : Edition du fichier de configuration daloradius.conf.php	116
Figure 142 : Redémarrage des services freeradius et apache	116
Figure 143: Interface web daloradius	117

Liste des tableaux

Tableau 1 : Tableau comparatif entre les méthodes agiles.....	5
Tableau 2 : Comparaison entre les protocoles TACACS+ et RADIUS.....	22
Tableau 3 : Etude comparatif des outils d'automatisation.....	27
Tableau 4: Backlog général.....	30
Tableau 5 : Liste des équipements utilisés	40
Tableau 6: Les noms des VLANs.....	40
Tableau 7 : Vlans et adressage des PCs	41
Tableau 8 : Plannification de release	42
Tableau 9 : Backlog du sprint 1.....	43
Tableau 10 : liste des cartes réseau	45
Tableau 11 : backlog de sprint 2	63
Tableau 12 : Backlog du sprint 3	84
Tableau 13 : Description textuelle de cas d'utilisation "automatiser la configuration snmp" .	85
Tableau 14 : Description textuelle de cas d'utilisation "automatiser l'ajout d'une hôte au eyes of network "	85

Glossaire

A

AAA: Authentication, Authorization, Accounting

ACL: Access Control List

AES: Advanced Encryption Standard

C

CPU : Central Processing Unit

D

DES : Data Encryption Standard

F

FAI : Fournisseur d'accès à Internet

FTP: File Transfer Protocol

H

HMAC: keyed-hash message authentication code

I

ISAKMP: Internet Security Association and Key Management Protocol

IPSec: IP Security Protocol

IPX: Internet Packet Exchange

K

KVM: Kernel-Based Virtual Machine

L

L2TP: (Layer 2 Tunneling Protocol)

M

MIB: Management Information Base

N

NAS: Network Access Server

NAS: Network Attached Storage

NFV: Network Functions Virtualization

O

OID: Object IDentifier

P

PPP: Point-to-Point Protocol

PPTP: Point-to-Point Tunneling Protocol

R

RAM: Random Access Memory

S

SHA: Secure Hash Algorithm

SNMP: Simple Network Management Protocol

SMTP: Simple Mail Transfer Protocol

SSH: Secure Shell

SLA: Service Level Agreement

T

TCP: Transmission Control Protocol

U

UDP: User Datagram Protocol

UML: Unified Modeling Language

V

VLAN: Virtual LAN

VPN: Virtual Private Network

X

XML: Extensible Markup Language

Introduction générale

L'administration et la gestion des infrastructures informatiques deviennent de plus en plus complexes. Il y a plus de serveurs, plus d'appareils, plus de plateformes, plus d'applications et plus de données. Il n'est plus possible de les gérer manuellement. Les administrateurs qui doivent ajouter ou modifier des fichiers de configuration sur un ensemble de serveurs doivent se connecter à chaque équipement et effectuer les mêmes modifications plusieurs fois. Cela agrave l'erreur humaine et fait perdre du temps. Par conséquent, l'adoption de l'automatisation des processus informatiques est devenue indispensable pour les entreprises qui cherchent à gérer efficacement leurs systèmes informatiques et leurs ressources humaines dédiées, ainsi qu'à améliorer la productivité et la qualité des services informatiques. L'automatisation met fin aux processus informatiques inefficaces, accélère le déploiement de nouvelles configurations, les met en production et utilise l'infrastructure, et améliore sa qualité et sa fiabilité, réduisant ainsi les coûts tout en économisant du temps. La surveillance est l'un des processus de la chaîne de production informatique qui doit être automatisé.

C'est dans ce contexte que s'inscrit, essentiellement, notre projet intitulé «implémentation d'une architecture réseau avec solution de contrôle d'accès, monitoring et automatisation»

Tout au long de ce rapport, nous allons exposer les différentes étapes de réalisation de notre projet qui sera divisé en six chapitres.

Le premier chapitre « Présentation du cadre de stage » est un chapitre introductif dans lequel nous effectuerons une brève description de la société. Ensuite, nous exposerons le cadre général du projet et la solution proposée. Par la suite, nous procéderons d'une présentation de choix méthodologique que nous avons adoptés, une brève étude comparative et une présentation de Scrum.

Pour le deuxième chapitre nommé « Etat de l'art » qui sera consacré pour une profonde analyse afin de mieux cerner les besoins de GlobalNet.

Dans le troisième chapitre « Spécifications des besoins », nous spécifierons les besoins fonctionnels pour les illustrer par des diagrammes de cas d'utilisation, nous présenterons le backlog général le diagramme de cas d'utilisation général ainsi que le diagramme d'activité, l'environnement de travail, l'architecture de notre projet et nous clôturerons par la planification de la release.

Pour les trois derniers chapitres, mise en place de l'outil de supervision, implémentation d'une connexion VPN et serveur d'authentification et automatisation de la supervision avec ansible. Nous détaillerons trois sprints avec la présentation de backlog de chaque sprint et nous allons clôturer par la réalisation.

Enfin, nous achèverons par une conclusion générale, qui accorde une évaluation de notre travail et qui offre des perspectives mettant fin à notre rapport de fin d'études.

Chapitre 1 : Présentation du cadre du stage

Introduction

Ce chapitre se focalise sur la présentation de l'entreprise accueillante et l'étude détaillée de l'existant où nous cernerons la problématique de notre sujet et nous présenterons la solution adoptée pour ce dernier ainsi que la méthodologie adaptée tout au long de ce projet.

1. Présentation de la société

GlobalNet est un fournisseur de services Internet depuis 1997 et est affilié à Standard Sharing Software (3S), une organisation de partage de technologies. 3S opère dans le domaine de l'innovation et de la complémentarité avec le soutien d'un vaste réseau de partenaires bien connus (tels que Cisco, IBM, Novell et Tivoli).

GlobalNet fournit des services Internet pour les particuliers et les professionnels, des abonnements Internet personnels, un accès dédié aux professionnels (LS, Frame Relay, VSAT), plusieurs accès xDSL, des produits VPN complets et l'hébergement de serveurs Web.

- **Le groupe Standard Sharing Software (3S)**

Fondé en 1988, 3S est un groupe technologique tunisien avec de nombreuses filiales. Il existe trois activités principales de 3S: la libération de logiciels, l'intégration de systèmes et l'intégration de réseaux. Elle se spécialise également dans la formation aux nouvelles technologies, aux réseaux mobiles, aux logiciels de transaction, aux codes à barres, aux centres d'appels et au commerce électronique.

- **Garanties entreprises**

Maîtrise des solutions Internet puissantes et efficaces; technologie mise depuis 1991, GlobalNet prend en charge l'intégration des réseaux intelligents, de la voix et des données via 3S. De plus, l'Alliance stratégique des systèmes 3S / Cisco, un leader mondial dans le développement de réseaux IP, garantit également la qualité pour les clients. Avantages, faisant notamment de GlobalNet un partenaire idéal pour la réalisation de projets commerciaux complexes basés sur Internet.

- **Les différents départements de la société**

GlobalNet a bâti sa réputation grâce à son architecture en cascade qui s'appuie essentiellement sur ces trois services :

Département commercial ;

Département financier ;

Département technique.

GlobalNet propose des solutions internet aux particuliers et aux entreprises. En collaboration étroite entre les différents départements, les besoins sont évoqués afin de répertorier les solutions qui seront reproduits sous forme de packs à proposer aux abonnés.

Le département commercial gère la vente et la publicité des produits proposés. Quant au service financier, il est à la charge du suivi des factures et la fidélisation clientèle. Le département technique assure principalement le fonctionnement, la continuité des services et leurs qualités.

2. Présentation du domaine de gestion de réseaux :

Les domaines d'activité de notre projet comprennent trois concepts principaux: la supervision du réseau, l'automatisation informatique, la sécurité et la virtualisation.

2.1 L'automatisation informatique

L'automatisation informatique comprend l'utilisation de logiciels pour créer des instructions et des processus reproductibles pour remplacer ou réduire l'interaction humaine avec les systèmes informatiques. L'automatisation est un élément clé pour optimiser la mise en œuvre de ces systèmes. Il leur permettra donc de se développer rapidement. [1]

2.2 La supervision informatique :

La supervision est une technologie qui peut utiliser pleinement les ressources informatiques pour obtenir des informations sur l'état du réseau et de ses composants. Ces données seront ensuite traitées et affichées pour clarifier tout problème.

2.3 La virtualisation :

La virtualisation regroupe toutes les technologies matérielles et / ou logicielles qui permettent d'exécuter plusieurs systèmes d'exploitation sur le même ordinateur, plusieurs instances différentes et des instances distinctes du même système ou de plusieurs applications. Ils fonctionnent sur des machines physiques distinctes.

2.4 La sécurité :

La protection des flux réseaux, et notamment des flux point à point identifiables facilement, comme les transferts de fichiers entre entreprises ou les accès des ordinateurs portables des utilisateurs nomades vers le réseau interne d'une entreprise à partir d'Internet, peut bénéficier d'une technique de protection générique consistant à authentifier et chiffrer l'ensemble du flux réseau concerné. Les technologies permettant cette protection sont souvent regroupées sous la désignation de « VPN » pour Virtual Private Network (réseau privé virtuel). [2]

3. Etude de l'existant :

L'étude de l'existant est une étape importante dans la mise en pratique de tout projet informatique. Cela explique l'environnement d'exploitation et décrit le contenu principal de notre projet.

3.1 Description de l'existant :

Les systèmes d'information jouent un rôle essentiel dans le succès des organisations en assurant des opérations efficaces et une gestion efficace pour maintenir son avantage parmi les différents concurrents.

3.2 Critique de l'existant

L'échange d'informations et la diffusion en temps opportun sont les priorités de tout gestionnaire de système d'information. Ces systèmes sont sujets aux pannes, à la dégradation des performances et à d'autres problèmes de fonctionnement. Les systèmes d'information deviennent de plus en plus complexes, et les problèmes de surveillance et de localisation deviennent de plus en plus difficiles pour les administrateurs réseau et système. Le service informatique et les administrateurs doivent toujours comprendre l'état de chaque appareil et service sur le réseau pour obtenir une réponse rapide.

3.3 Solution proposé

Pour bien mener le projet tout en respectant les engagements contractuels, en tenant compte des délais et en produisant les résultats escomptés, le projet a été organisé de sorte que le service informatique et les administrateurs doivent toujours comprendre l'état de chaque équipement et services sur le réseau pour améliorer la vitesse de réponse.

L'automatisation de l'ensemble de la chaîne de production informatique est l'une des technologies qui permet aux administrateurs systèmes d'augmenter l'efficacité et d'améliorer la qualité, les performances et la résilience des systèmes d'information. Pour réaliser notre solution, nous devons respecter une méthode fiable.

Dans ce qui suit, nous présenterons la méthodologie utilisée et le langage de modélisation choisis.

4. Méthodologie adoptée et langage de modélisation

Tout au long de notre travail, nous suivrons une approche agile. Cette approche nous permettra de mieux gérer les différentes étapes de mise en œuvre. En effet, chaque étape sera vérifiée par notre encadrante professionnelle de la société. Les méthodes agiles permettent aux clients de mettre à jour ou de modifier les exigences en fonction de l'avancement du projet. Différente de la méthode classique de gestion de projet, tandis que la méthode classique de gestion de projet détermine les besoins du client au début et il est vérifiée à la fin du travail.

La méthodologie agile comprend plusieurs méthodes. Dans les sous-sections suivantes, nous effectuerons une étude comparative de certaines méthodes agiles afin de choisir la méthode la plus appropriée pour notre travail.

4.1 Méthode de réalisation

Avant d'adopter une méthode pour gérer nos projets agiles, nous réaliserons une étude comparative sur les méthodes les plus utilisées.

Cette recherche nous permettra de déterminer la méthode la plus adaptée à notre travail. Le tableau 1 décrit chacune des quatre méthodes et met en évidence ses avantages et ses inconvénients. [3]

Tableau 1 : Tableau comparatif entre les méthodes agiles

Méthode	Description	Points Forts	Points Faibles
Kanban	<ul style="list-style-type: none"> ▪ Impose un système déclenché par la consommation du client ▪ Se base sur l'approche Lean ▪ Contrôle visuellement le flux de travail 	<ul style="list-style-type: none"> ▪ Evite la surproduction ▪ Permet d'identifier rapidement les problèmes et d'agir rapidement ▪ Encourage la coopération au sein de l'équipe pour résoudre les problèmes 	<ul style="list-style-type: none"> ▪ Ne s'adapte pas à toutes les industries ▪ Des problèmes système peuvent entraîner l'arrêt de la chaîne de production ▪ Perte d'étiquette peut causer des difficultés ▪ Le système cesse de fonctionner lorsque la demande est trop irrégulière
ScrumBan	<ul style="list-style-type: none"> ▪ Méthode basée sur Scrum et Kanban ▪ Le travail est effectué en courte itérations et contrôlé à l'aide de supports visuels (comme tableau de Kanban) ▪ Ne nécessite aucun rôle d'équipe, ni un nombre spécifique de membres de l'équipe 	<ul style="list-style-type: none"> ▪ Effectuer des changements à chaque moment de manière immédiate puisqu'il n'y a pas de sprint à respecter ▪ Adapté à des projets mixtes cycle en V et agile 	<ul style="list-style-type: none"> ▪ Utilisé uniquement pour les startups et les projets qui nécessitent une fabrication de produit continu

eXtreme Programming (XP)	<ul style="list-style-type: none"> ▪ Développement guidé par les besoins du client ▪ Equipes réduites, centrées sur les développeurs 	<ul style="list-style-type: none"> ▪ Itératif et incrémentale ▪ Simple à mettre en Builds journaliers ▪ Amélioration constante et adaptations aux modifications 	<ul style="list-style-type: none"> ▪ Ne couvre pas les phases en amont et en aval du développement ▪ Focalisé sur l'aspect individuel du développement
Scrum	<ul style="list-style-type: none"> ▪ Approche itérative incrémentale ▪ Concerne des très grands projets ▪ Peut théoriquement s'appliquer à n'importe quel contexte ou à un groupe de personnes qui travaillent ensemble pour atteindre un but commun 	<ul style="list-style-type: none"> ▪ La participation active du client ▪ Qualité du produit mise en avant ▪ Simplicité des processus ▪ Augmentation de la productivité ▪ Chaque équipe a son lot de responsabilités ▪ Amélioration de la communication 	<ul style="list-style-type: none"> ▪ Peu de documentation écrite ▪ Violation de responsabilité

Comme le montre le tableau 1 ci-dessus, Scrum est la méthode de réalisation agile la plus adaptée à notre travail. En effet, cela permet de fournir des livrables à la fin de chaque phase d'exécution et de vérification au client. Il garantit également aux clients une meilleure visibilité pendant la phase de mise en œuvre. Les tests pouvant être effectués en continu (les problèmes sont rapidement découverts), un meilleur processus de contrôle qualité peut être assuré. Ensuite, nous continuons à introduire la méthode agile Scrum car nous l'adopterons dans la mise en œuvre du projet. [4]

4.2 Présentation de Scrum

La méthode SCRUM, utilisée dès 1993, est une des méthodes les plus utilisées et la plus populaire des méthodes agiles.

Elle est principalement utilisée lors de conférence, de réunion, dans des blogs, dans divers ouvrages, et même dans divers communautés.

Cette méthodologie a pour objectif de satisfaire le client en livrant rapidement et régulièrement des fonctionnalités à grande valeur ajoutée.

La mise en place d'un dialogue constant est établie avec le client afin de mettre en place le projet.

4.2.1 Les rôles

Dans le cadre de la méthode Scrum, nous pouvons constater la création de nombreux rôles dans l'entreprise. Ces rôles ont été créés dans le but de permettre l'intégrité, la bonne élaboration d'un projet. Chaque rôle est important.

Ces rôles sont :

- **Product owner** : Il s'agit du représentant du projet qui est en relation constante avec le client. Il est l'interlocuteur privilégié du Scrum Master et de la Team member. Il fait le lien entre l'équipe de développement, le Scrum Master et le client final. Il comprend les besoins et définit les problématiques, tout en élaborant diverses spécifications. Il a également pour but de prioriser les tâches attribuées à l'équipe.
- **Le Scrum master** : Le Scrum master quant à lui, il est chargé de veiller au bon respect et à l'application de la méthode Scrum..

Il a également pour but, lors de sprint de relever les éléments bloquant l'avancement du projet.

- **Team member** : Il s'agit d'un groupe formé de développeur, architecte, consultant... Ce sont les personnes chargées à l'élaboration du sprint, et à l'exécution des tests fonctionnels.

4.2.2 Les évènements

Nous pouvons distinguer plusieurs évènements possibles lors d'un projet Scrum.

Les évènements sont :

- **Sprint** : Un sprint est un délai de moins d'un mois, afin de faire un premier rendu du produit. Une fois en accord avec le client sur la durée des rendues, il faut que celui-ci devient constant pour le développement du produit.
- **La réunion de planning** : Il s'agit ici, d'une réunion auprès de toute l'équipe qui dure approximativement 3 à 4 heures. La priorité étant de définir l'objectif de l'itération, puis de produire le backlog de sprint connaître le périmètre de l'équipe et d'obtenir leurs engagements. Le product owner est en étroite collaboration avec l'équipe afin de découper les fonctionnalités à réaliser et à implémenter. Ce découpage se fait en tâche d'analyse, de développement, de tests, et faire une estimation de la charge à réaliser.
- **Scrum meeting** : Il s'agit d'une réunion, généralement matinale, qui aura lieu tous les jours. Elle dure approximativement 10 à 15 minutes et se fait généralement debout. La réunion a pour but de mettre à jour les tâches de chacun, de maintenir leurs engagements et d'identifier les éléments bloquants. Chaque membre doit annoncer ce qu'il a fait la veille, ce qu'il fera aujourd'hui et les éléments entravant son avancement.
- **La démonstration** : Il s'agit du dernier jour de l'itération. Cette réunion se fait avec l'équipe scrum et les clients. Chaque membre scrum présente les fonctionnalités ayant été élaborées durant cette itération. Cette réunion a pour but de livrer une version de démonstration auprès des clients.
- **La rétrospective** : A la fin de la "démonstration", l'équipe se réunit en interne afin d'analyser l'itération précédente. Il s'agit ici de l'améliorer et d'en déduire un plan d'action à

la réalisation d'une potentielle prochaine itération.

4.2.3 Les cycles de la méthode scrum



Figure 1 : les cycles de méthode scrum

Nous avons vu précédemment les différents rôles et évènements dans la méthode SCRUM, maintenant nous verrons les différents cycles utilisés par cette méthode. [4]

- Compréhension du besoin

L'équipe de développement à un rôle essentiel dans cette partie, il aura pour rôle de lister toutes les fonctionnalités qu'ils doivent juger utiles afin de permettre la réalisation du concept. L'ensemble des fonctionnalités devra être estimé d'une manière rapide, optimale et objective.

Le Product Owner, sera susceptible d'aider par ailleurs en cas de nécessité les équipes de développement à comprendre le besoin, à approfondir certaines notions.

Le but étant d'estimer le coût et la durée des fonctionnalités.

- Concertation

Pour démarrer le projet, l'équipe de développement et le product owner, peuvent commencer par déterminer la durée des "Sprint". La durée des itérations va en général de 2 à 4 semaines.

Cette durée devra être la même pour l'ensemble des itérations. Et ces itérations devront être suivis par des "réunions de planification".

- Réunion de planification

Le but des réunions de planification est de formaliser et de planifier les tâches à accomplir.

- Vision du projet

Dès que le product owner aura tous les éléments permettant de constituer le Product Backlog, on peut planifier le premier Sprint.

Le Product Owner voit alors l'équipe de développement de la route à suivre à travers un "Roadmap", la deadline, l'objectif du Sprint, mais surtout voir la vision du Produit.

- La Réalisation du projet

L'équipe de développement se concentre ensuite sur les tâches à accomplir. Ces tâches seront les exigences sélectionnées à accomplir. A la fin de chaque Sprint, ces tâches seront des fonctionnalités utilisables.

- Le Sprint

Lors de l'étape du "Sprint", l'ensemble de l'équipe se concentre sur les tâches effectuées du Sprint Backlog. En cas de retard, des tâches seront retirés afin de préserver l'objectif du sprint. Si par ailleurs, il y a de l'avance, des tâches y seront ajoutés.

- La Mêlée Quotidienne

Cette réunion, organisée par le Scrum Master, est une réunion où il est important de se tenir debout afin que la réunion ne dure pas dans le temps. L'équipe fait remonter les obstacles et permet une entraide sur les difficultés rencontrées. Cette réunion permet également de vérifier l'avancement d'un Sprint. La mêlée quotidienne se déroule généralement le matin à lieu et heure fixe. La durée de la réunion est de 15 minutes.

- La Revue du Sprint

La revue du Sprint est également une réunion, d'une durée approximative de 1 heure par semaine de Sprint. Elle permet d'inspecter et d'analyser le Sprint délivré. Elle permet de faire aussi un point sur l'avancement de la "Release" et d'adapter au besoin le plan et le product Backlog. L'équipe de développement est présente à la réunion pour exposer les fonctionnalités. Le product owner, lui, leur donne un Feedback afin d'avoir la validation de leurs fonctionnalités ou non.

- La Rétrospective

Cette réunion est généralement animée par le Scrum Master à son équipe, et elle est d'une durée de 45 minutes par semaine de Sprint elle a pour but d'améliorer en continue, le processus de développement de l'équipe en mettant les idées de chacun à contribution.

Elle a pour but d'identifier les éléments "positifs" au récent Sprint rencontré, de définir les éléments à améliorer et de définir un plan d'action pour l'amélioration.

Il est important d'identifier les points "négatifs" aussi, afin d'en réduire le plus possible. Il est important de définir un plan d'action afin de lutter contre ces éléments.

4.3 Langage de modélisation

Comme tout projet informatique l'étape de conception est primordiale c'est pour ça nous avons recourt au langage UML pour la modélisation de notre projet. Ce choix est du à le rôle du UML et son rôle dans la modélisation des diagrammes de notre projet.

Le langage UML (Unified Modeling Language, ou langage de modélisation unifié) a été pensé pour être un langage de modélisation visuelle commun, et riche sémantiquement et syntaxiquement. Il est destiné à l'architecture, la conception et la mise en œuvre de systèmes

logiciels complexes par leur structure aussi bien que leur comportement. L'UML a des applications qui vont au-delà du développement logiciel, notamment pour les flux de processus dans l'industrie.

Il ressemble aux plans utilisés dans d'autres domaines et se compose de différents types de diagrammes. Dans l'ensemble, les diagrammes UML décrivent la limite, la structure et le comportement du système et des objets qui s'y trouvent.

L'UML utilise les points forts de ces trois approches pour présenter une méthodologie plus cohérente et plus facile à utiliser. Il représente les meilleures pratiques de création et de documentation des différents aspects de la modélisation des systèmes logiciels et d'entreprise. [5]

Conclusion

Ce chapitre représente un point de départ pour effectuer notre projet. Nous avons présenté l'organisme d'accueil, déterminé le domaine métier, étudié l'existant et fixé les objectifs à atteindre. Par la suite, nous avons présenté la méthodologie et le langage de modélisation choisi pour réaliser notre projet. Le chapitre suivant comportera les détails des notions présentés dans le domaine métier.

Chapitre 2 : Etat de l'art

Introduction

Nous allons commencer par une présentation des concepts de base de notre projet, puis une étude de quelques solutions open source existant dans le marché en vue de les évoluer et choisir les mieux adoptées à utiliser pour le déroulement de projet.

1. La supervision

La supervision du réseau est un ensemble de protocoles, de matériels et de logiciels informatiques qui peuvent assurer les activités suivantes: surveillance, visualisation, analyse et action. Ceci est assuré en utilisant des ressources réseau appropriées (matériel ou logiciel) qui peuvent fournir des informations sur l'état du réseau et de ses ordinateurs distants. Par conséquent, il doit y avoir une console de supervision pour collecter et synthétiser toutes les informations avec la possibilité de surveillance de la visibilité des systèmes d'information. De cette façon, nous pouvons obtenir rapidement des informations pour comprendre l'état de santé et les performances du réseau et du système. Cela donne rapidement une image du système à l'étude. Grâce à ces informations, nous pouvons gérer automatiquement les défaillances et les surcharges sur le réseau.

1.1 Les objectifs et intérêts de la supervision

La supervision a pour but de contrôler l'infrastructure informatique (réseau, système, services applicatifs, etc.). L'ensemble de la flotte doit être clairement comprise pour gérer et collecter des informations sur le tableau de bord. La supervision est basée sur les points suivants, qui peuvent garantir la qualité de nos services:

- Etre proactif: les administrateurs doivent prendre des mesures proactives et prévoir les pannes.
- Etre réactif: prendre des décisions rapides en mesurant les problèmes et en limitant les risques lorsque des problèmes surviennent. Identifier les cibles avant les pannes et les problèmes pour effectuer une intervention à distance pour résoudre certains problèmes (redémarrer le serveur, le routeur, démarrer la mise à jour, etc.) ou en cas de panne, alerter l'administrateur réseau par SMS ou email.

La supervision informatique de l'entreprise vise à utiliser des systèmes de contrôle et de surveillance pour la maintenance préventive. Cela évite les incidents et prévient les arrêts ou interruptions d'activités dus à l'apparition de problèmes informatiques (plantages, intrusions, virus, etc.) ça résulte une surveillance continue des systèmes d'information (7j/24h) et donc ça permet gagner du temps dans le diagnostic et la résolution des incidents. [6]

1.2 Pourquoi superviser

Sans l'image de l'état de santé de la plateforme de production, il ne peut y avoir une. Nous sommes besoin d'une console de supervision pour collecter et synthétiser toutes les

informations. Nous surveillons la visibilité des systèmes d'information. Cela va permettre d'obtenir rapidement des informations et de comprendre l'intégrité du réseau, du système et des performances. La supervision permet également de prévenir les pannes et de prévoir les pannes. Grâce à la supervision, nous pouvons également comprendre rapidement l'impact des opérations (ajout de nouveaux clients, nouveaux ordinateurs, etc.) sur le système. Par conséquent, nous pouvons connaître et quantifier techniquement l'impact de telles modifications et réagir rapidement en cas de besoin.

Lorsqu'un échec se produit, cela affectera la productivité de l'entreprise. Par conséquent, il faut faire toujours attention à ce qui s'est passé.

Dans l'ensemble, nous avons la responsabilité de surveiller et de rappeler l'apparition de problèmes et de les prévoir lorsque cela est possible. Nous effectuerons un test et analyserons les résultats sous forme de graphiques ou d'autres formes, et nous mettrons en place pour agir face aux événements en fonction des conditions de déclenchement (redémarrage du service, alertes administrateur pour le comportement des processus, etc.). Par conséquent, nous aurons de la visibilité pour tout le contenu.

2. La virtualisation

La virtualisation est une technologie qui permet d'utiliser des ressources généralement liées au matériel pour créer des services informatiques utiles. Elle permet aussi d'utiliser sa pleine capacité en distribuant des ordinateurs physiques entre de nombreux utilisateurs ou différents environnements. [7]

2.1 Fonctionnement

Les logiciels appelés hyperviseurs peuvent isoler les ressources physiques de l'environnement virtuel. Ces hyperviseurs peuvent être basés sur un système d'exploitation (tel qu'un ordinateur portable) ou ils peuvent être installés directement sur un système physique (tel qu'un serveur). L'hyperviseur alloue des ressources physiques pour permettre à l'environnement virtuel de les utiliser.

Ces ressources sont divisées de l'environnement physique et distribuées dans différents environnements virtuels. Les utilisateurs interagissent avec ces environnements (également appelés machines virtuelles ou hôtes) et y effectuent des calculs.

Lorsque l'environnement virtuel est exécuté et que l'utilisateur ou le programme émet une instruction demandant plus de ressources à l'environnement physique, l'hyperviseur envoie cette demande au système physique et met en cache les modifications.

Le processus est presque aussi rapide que sur le système natif, surtout si la demande est envoyée via un hyperviseur open source basé sur une machine virtuelle basée sur le noyau (KVM). [7]

2.2 Types de ressources virtualisées

2.2.1 Virtualisation des données

Les données dispersées dans l'environnement peuvent être regroupées en une seule source. La virtualisation des données permet aux entreprises d'utiliser les données comme source dynamique. Par conséquent, ils profitent des capacités de traitement qui peuvent collecter des données à partir de plusieurs sources, héberger facilement de nouvelles sources de données et transformer les données pour répondre aux besoins des utilisateurs. [7]

2.2.2 Virtualisation des postes de travail

La virtualisation des postes de travail est souvent confondue avec la virtualisation des systèmes d'exploitation (qui permet de déployer plusieurs systèmes d'exploitation sur un seul ordinateur), tandis que la virtualisation des postes de travail permet à un administrateur central (ou un outil de gestion automatisé) de déployer l'environnement sur des centaines d'ordinateurs physiques simultanément Sur le poste de travail de simulation. [7]

2.2.3 Virtualisation de serveurs

La virtualisation de serveurs optimise l'exécution de ces fonctions spécifiques et implique leur partitionnement, de sorte que les composants peuvent être utilisés pour effectuer différentes fonctions. [7]

2.2.4 Virtualisation des systèmes d'exploitation

La virtualisation des systèmes d'exploitation se produit au niveau du noyau, ce qui correspond à leur gestionnaire de tâches central. Cette méthode permet notamment aux environnements Linux et Windows de s'exécuter en parallèle. Les entreprises peuvent également transférer des systèmes d'exploitation virtuels vers des ordinateurs, ce qui présente les avantages de réduire les coûts matériels, d'améliorer la sécurité et de réduire le temps de service informatique. [7]

2.2.5 Virtualisation des fonctions réseau

La virtualisation des fonctions réseau (NFV) sépare les fonctions réseau clés (telles que les services d'annuaire, le partage de fichiers et la configuration des adresses IP) pour les allouer dans différents environnements.

3. VPN

Le réseau privé virtuel est considéré comme une extension du réseau local et conserve la sécurité logique que peut avoir le réseau local. Il correspond en fait à l'interconnexion du réseau local via la technologie "tunnel". [8]

3.1 Utilisation de VPN

3.1.1 Accès d'utilisateur distant sur Internet

Un réseau privé virtuel permet d'accéder à distance aux ressources de l'entreprise via Internet, tout en préservant la confidentialité des informations

Les utilisateurs n'ont pas besoin de faire des appels longue distance à l'entreprise ou au serveur d'accès au réseau externe (NAS), mais appellent le fournisseur de services Internet local (ISP). En utilisant la connexion au fournisseur, le logiciel VPN peut créer un réseau privé virtuel entre l'utilisateur connecté à distance et le serveur VPN de l'entreprise sur Internet.

3.1.2 Connexion de réseaux sur Internet

Il existe deux façons de connecter un réseau local à un site distant à l'aide d'un VPN:

Utilisation des lignes dédiées pour connecter les succursales au réseau local de l'entreprise. Les succursales et les routeurs de concentrateurs d'entreprise peuvent utiliser des circuits privés locaux et des fournisseurs de services Internet locaux pour remplacer les circuits privés longue distance coûteux entre les succursales et les concentrateurs d'entreprise. Connecter à Internet. Le logiciel VPN utilise une connexion (FAI) locale et l'Internet public pour créer un réseau privé virtuel entre le routeur de la succursale et le routeur concentrateur de l'entreprise.

Utilisation des lignes d'accès à distance pour connecter les succursales au réseau local. Le routeur de la succursale peut appeler le FAI local au lieu d'utiliser le routeur de la succursale pour effectuer des appels longue distance avec l'entreprise ou le NAS externe. Le logiciel VPN utilise la connexion du fournisseur local au routeur de la succursale sur Internet et au routeur concentrateur de l'entreprise pour créer un réseau privé virtuel.

3.1.3 Connexion d'ordinateurs sur un intranet

Dans certains réseaux d'entreprise, les données du service sont si sensibles que le LAN est réellement déconnecté du reste du réseau de l'entreprise. Bien que cette configuration protège la confidentialité des informations dans le service, elle pose des problèmes d'accès aux informations aux utilisateurs qui ne sont pas physiquement connectés au réseau local séparé.

3.2 Caractéristiques de VPN

Une solution VPN doit, au minimum, mettre en œuvre un ensemble des fonctionnalités comme **l'authentification d'utilisateur** puisque la solution doit vérifier l'identité de l'utilisateur et permettre l'accès VPN uniquement aux personnes autorisées. En outre, elle doit fournir des informations d'audit et de comptabilisation permettant de savoir quelles personnes ont accédé à quelles données et à quel moment ainsi que **la gestion d'adresses** car la solution doit affecter une adresse de client sur le réseau privé, et doit garantir en permanence la confidentialité des adresses privées aussi le **cryptage des données** est une étape nécessaire afin que les données transportées sur le réseau public soient illisibles pour les clients non autorisés sur le réseau.

Gestion de clés est aussi une caractéristique de VPN la solution doit générer et régénérer des clés de cryptage pour le client et le serveur Et supporte la **prise en charge multi protocole** pour être en mesure de gérer les protocoles les plus fréquemment employés sur les réseaux publics. Cela inclut notamment le protocole Internet (IP, Internet Protocol), le protocole IPX (Internet Packet Exchange), etc. Une solution VPN Internet basée sur le protocole PPTP (Point-to-Point Tunneling Protocol) ou L2TP (Layer 2 Tunneling Protocol)

satisfait toutes ces exigences de base et bénéficie de la disponibilité mondiale d'Internet. D'autres solutions, notamment le nouveau protocole de sécurité Internet IPSec (IP Security Protocol), répondent à certaines de ces exigences, mais restent très utiles dans des situations spécifiques.

4. VLAN

VLAN pour réseau local virtuel décrit un réseau local. Les VLAN regroupent logiquement et indépendamment un groupe d'ordinateurs. Nous pouvons trouver plusieurs coexistences sur le même commutateur réseau en même temps. En termes d'avantages, les VLAN améliorent la gestion du réseau en apportant une plus grande flexibilité dans la gestion. Il offre une sécurité supérieure en exigeant à titre d'exemple le passage par un routeur pour communiquer entre deux machines. Enfin, il peut optimiser la bande passante, séparer les flux et réduire la propagation du trafic.

Il existe trois différents types de réseau local virtuel : de niveau 1 (aussi appelé VLAN par port), de niveau 2 (VLAN par adresse MAC) et de niveau 3 (VLAN par adresse IP). [9]

4.1 Utilité des vlans

Dans un réseau local la communication entre les différentes machines est régie par l'architecture physique.

Grâce aux réseaux virtuels (VLAN) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

5. L'automatisation Informatique

L'automatisation informatique fait référence à tous les outils et pratiques utilisés pour automatiser les tâches normalement effectuées par l'homme. Il vise à faire plus, mieux et plus rapidement avec une intervention manuelle minimale voire nulle. Pour y parvenir, nous utilisons des scripts et des planificateurs de mission pour créer des instructions et des processus reproductibles.

L'intelligence artificielle joue un rôle clé dans l'automatisation car elle peut utiliser des informations provenant de grandes quantités de données. [10]

5.1 Pourquoi automatiser

L'automatisation est non seulement un outil important pour la gestion, la transformation et l'adaptation de notre infrastructure informatique, mais également pour la gestion des fonctions métier à travers ses processus. Grâce à l'automatisation, nous pouvons investir dans l'innovation, le temps et les efforts qui n'ont plus besoin d'être effectués manuellement. Pour une entreprise d'automatisation, l'objectif est d'accélérer le travail de l'équipe informatique afin de gagner du temps pour gérer et résoudre les problèmes liés aux processus, et ces processus peuvent également être automatisés à long terme. Les opérations

informatiques ne sont pas faciles. La coexistence de systèmes et de processus nouveaux et anciens est très complexe, de sorte que le taux de croissance des exigences et des exigences dépasse de loin les fonctions informatiques et commerciales.

On trouve aussi l'avènement de nouvelles méthodes, telles que le DevOps, oblige le personnel à adopter une nouvelle culture. Ce qui implique l'évolution des technologies (virtualisation, cloud, conteneurs, etc.) est trop rapide pour être gérée manuellement.

5.2 Avantages

L'automatisation informatique augmente la productivité, ce qui permet aux employés de consacrer plus de temps à l'optimisation des activités. Le logiciel est responsable des tâches répétitives. En raison de moins d'intervention manuelle et moins d'erreurs, il est également plus fiable. Les tâches répétitives sont toujours effectuées de la même manière. Par conséquent, nous pouvons toujours connaître exactement à quel moment les processus, tests, mises à jour, workflows, etc. ont lieu et combien de temps ils prennent. Au final, le résultat sera toujours fiable.

On trouve aussi la gouvernance simplifiée plus nous avons de personnel, plus le risque de lacunes dans les compétences est élevé. Et en raison de ces différences, certains employés peuvent ne pas savoir ce que fait un autre employé. En codifiant nos processus, nous gagnerons un meilleur contrôle. [11]

5.3 Intérêt d'automatisation de la supervision

Automatiser son système d'information est l'une des tâches les plus importantes de l'administrateur système. Aujourd'hui, les outils de supervision comme les outils de gestion de configuration sont suffisamment matures pour automatiser efficacement la supervision. En passant un peu de temps sur les deux types d'outil, il est possible de faire en sorte qu'un serveur ajouté au système d'informations soit automatiquement ajouté à l'outil de supervision, sans que l'administrateur n'ait besoin de réaliser une tâche spécifique. Dès lors, il n'y aura plus d'oubli et l'administrateur système pourra se concentrer sur d'autres tâches.

Pour arriver à ce résultat, l'administrateur système doit maîtriser son outil de gestion de configuration comme son outil de supervision. La configuration de modèle de supervision comme les recettes de déploiement et de configuration doivent être poussées le plus loin possible. Cette tâche est nécessaire et un des facteurs clés de réussite du projet d'intégration. Les outils, si leur périmètre fonctionnel est bien évidemment à prendre en compte, ne sont qu'un point d'appui : la méthode de travail est l'élément le plus important.

Comme toujours, une amélioration continue doit être mise en place, pour améliorer l'utilisation des outils et faire évoluer la gestion de configuration.

6. Le protocole SNMP

6.1 Présentation

SNMP (Simple Network Management Protocol) est un protocole de gestion de réseau fourni par l'IETF. Il s'agit actuellement du protocole de gestion des équipements réseau le plus utilisé.

SNMP est un protocole relativement simple. Cependant, toutes ses fonctions sont suffisamment puissantes pour gérer des réseaux hétérogènes complexes. Il est également utilisé pour gérer à distance des applications: bases de données, serveurs, logiciels, etc.

L'environnement de gestion SNMP comprend les parties suivantes: station de surveillance, éléments actifs du réseau, variables MIB et protocoles. Les différents composants du protocole SNMP sont les suivants:

Les éléments actifs du réseau sont les appareils ou logiciels que nous essayons de gérer. Cela va des postes de travail aux concentrateurs, routeurs, ponts, etc. Chaque élément du réseau a une entité dite proxy qui répond aux demandes des stations de supervision. Les agents sont des modules qui résident dans des éléments de réseau. Ils rechercheront des informations de gestion, telles que le nombre de paquets reçus ou envoyés.

- La station de supervision (appelée aussi manager) exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail.
- La MIB (Management Information Base) est une collection d'objets résidant dans une base d'information virtuelle. Ces collections d'objets sont définies dans des modules MIB spécifiques.
- Le protocole, qui permet à la station de supervision d'aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments. [12]

6.1.1 Fonctionnement

Le protocole SNMP est basé sur un fonctionnement asymétrique. Il se compose d'un ensemble de demandes, de réponses et d'un nombre limité d'alertes. Le gestionnaire envoie la demande à l'agent, qui renvoie la réponse. Lorsqu'un événement anormal se produit sur l'élément de réseau, l'agent envoie une alerte (trap) au manager.

SNMP utilise le protocole UDP [RFC 768]. Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station de gestion. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents.

- Les requêtes SNMP

Il existe quatre types de requêtes: GetRequest, GetNextRequest, GetBulk, SetRequest.

- ✓ La requête GetRequest permet la recherche d'une variable sur un agent.
- ✓ La requête GetNextRequest permet la recherche de la variable suivante.
- ✓ La requête GetBulk permet la recherche d'un ensemble de variables regroupées.
- ✓ La requête SetRequest permet de changer la valeur d'une variable sur un agent.

- Les réponses de SNMP

À la suite de requêtes, l'agent répond toujours par GetResponse. Toutefois si la variable demandée n'est pas disponible, le GetResponse sera accompagné d'une erreur noSuchObject.

- Les alertes (Traps, Notifications)

Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informe la station de supervision via une trap. Les alertes possibles sont: ColdStart, WarmStart, LinkDown, LinkUp, AuthentificationFailure. [12]

6.1.2 La MiB

Chaque agent SNMP maintient une base de données décrivant les paramètres de l'appareil géré. Le Manager SNMP utilise cette base de données pour demander à l'agent des renseignements spécifiques. Cette base de données commune partagée entre l'agent et le Manager est appelée Management Information Base (MIB).

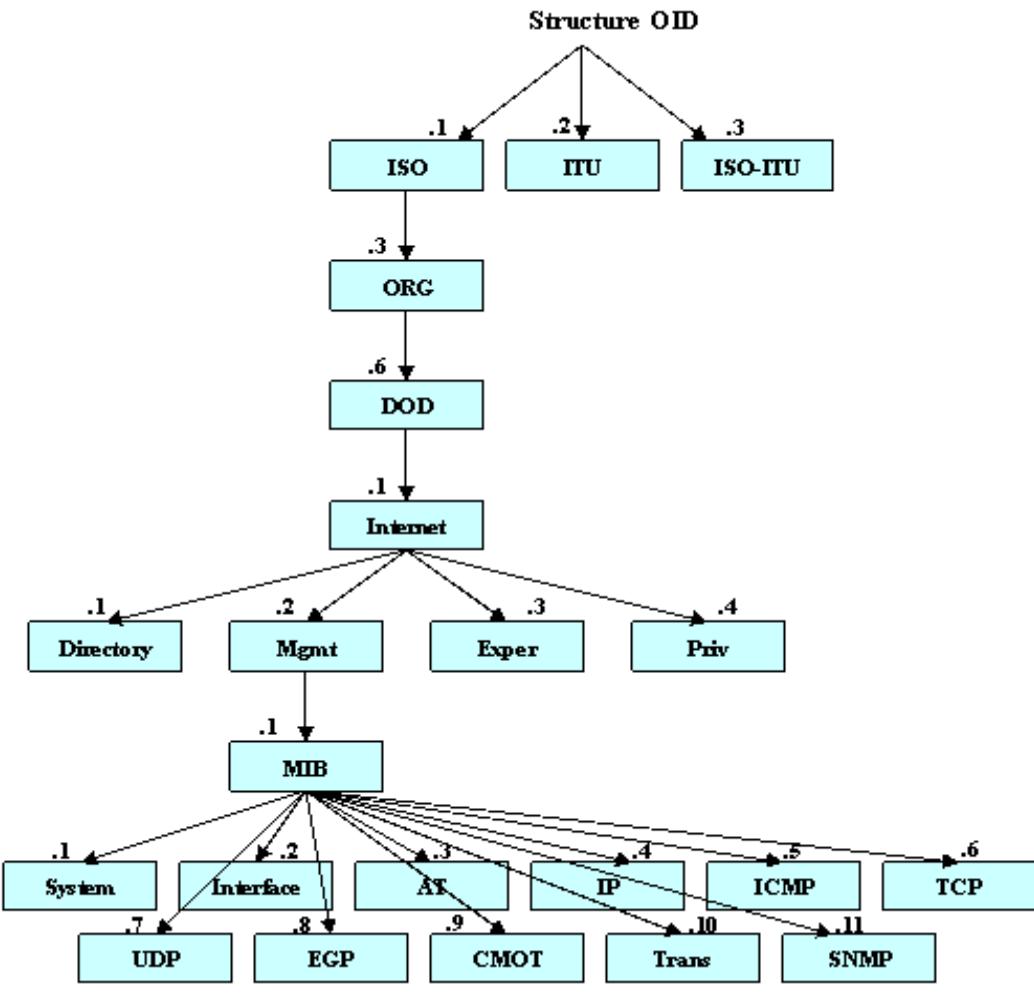
Généralement ces MIB contiennent l'ensemble des valeurs statistiques et de contrôle définis pour les éléments actif du réseau. SNMP permet également l'extension de ces valeurs standards avec des valeurs spécifiques à chaque agent, grâce à l'utilisation de MIB privées.

Un fichier MIB est écrit en utilisant une syntaxe particulière, cette syntaxe s'appelle SMI 3, basée sur ASN.1 tout comme SNMP lui-même.

En résumé, les fichiers MIB sont l'ensemble des requêtes que le Manager peut effectuer vers l'agent. L'agent collecte ces données localement et les stocke, tel que défini dans la MIB. Ainsi le Manager doit être conscient de la structure (que celle -ci soit de type standard ou privée) de la MIB afin d'interroger l'agent au bon endroit.

La structure d'une MIB est une arborescence hiérarchique dont chaque nœud est défini par un nombre ou un Object IDentifier (OID). Chaque identifiant est unique et représente les caractéristiques spécifiques du périphérique géré. Lorsqu'un OID est interrogé, la valeur de retour n'est pas un type unique (texte, entier, compteur, tableau...) Un OID est donc une séquence de chiffres séparés par des points.

Une MIB est un arbre très dense, il peut y avoir des milliers d'OID dans la MIB. [12]



[12]

Figure 2 : structure de table MIB

7. Protocole SSH

Secure Shell (SSH) Est un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

8. Protocole AAA

AAA est un protocole qui permet la sécurité des réseaux et des services réseaux avec le contrôle des accès non autorisés avec l'authentification, des utilisateurs ayant accès aux réseaux avec l'autorisation, des actions faites sur le réseau avec la traçabilité. [13]

Authentification

L'authentification est une procédure qui permet de vérifier l'identité de l'utilisateur afin de lui donner l'accès, en fonction de ses droits, aux réseaux ou aux différents équipements correspondants par le biais d'un nom utilisateur et un mot de passe.

Autorisation

Après l'authentification, l'utilisateur a besoin d'une autorisation afin d'accéder aux réseaux. Celle-ci permet de fournir des droits aux utilisateurs afin d'interdire ou accepter leurs actions comme l'utilisation de certaines commandes ou certaines ressources. Pendant l'authentification l'équipement demande les autorisations au serveur AAA.

La traçabilité

Permet de tracer les actions des utilisateurs authentifiés et autorisés à accéder aux équipements en collectant leurs données sous forme de logs

8.1 Protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial-In User Service), mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC.

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il s'agit du protocole de prédilection des fournisseurs d'accès à internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé.

Il est à noter que le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.

8.1.1 Fonctionnement

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;

Le NAS achemine la demande au serveur RADIUS ;

Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :

- ACCEPT : l'identification a réussi ;
- REJECT : l'identification a échoué ;
- CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge ») ;
- CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

Le schéma suivant récapitule les éléments entrant en jeu dans un système utilisant un serveur RADIUS : [14]

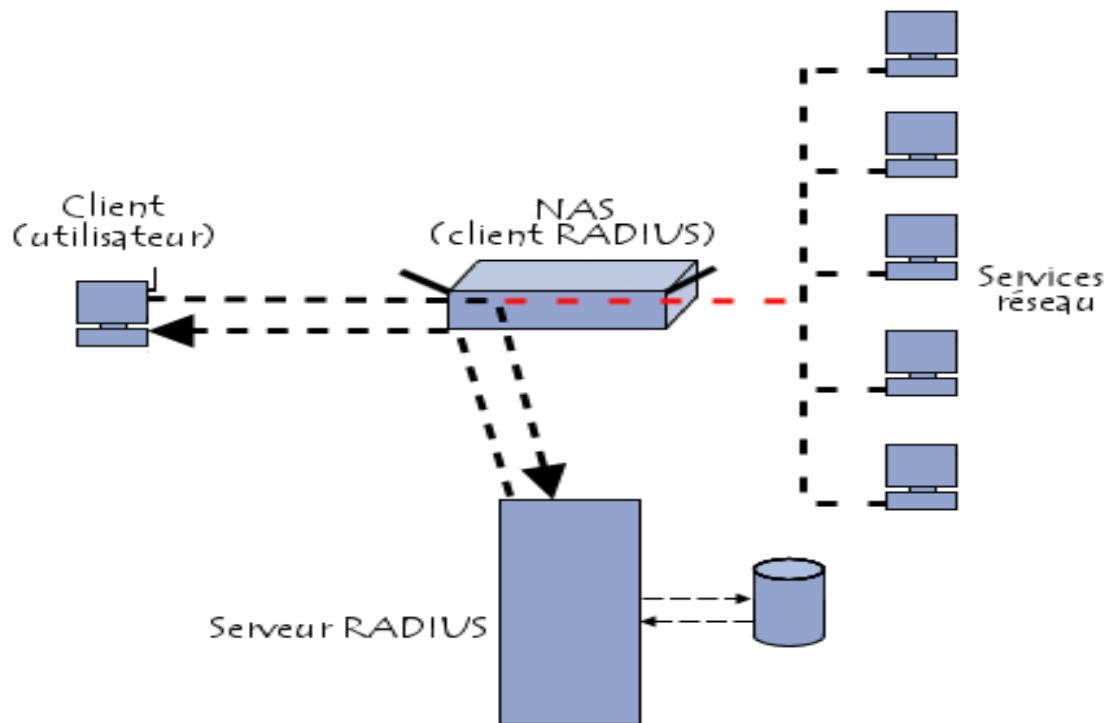


Figure 3 :Les éléments de serveur RADIUS

8.2 Protocole TACACS+

TACACS+ signifie Terminal Access Controller Access-Control System Plus et permet d'effectuer un contrôle d'accès pour les équipements réseau grâce à un équipement (serveur) qui centralise l'ensemble des informations liées à l'authentification des clients.

La communication entre le "suppliant", le client TACACS+ et le serveur TACACS+ ne se passe pas exactement de la même manière que pour le protocole RADIUS

8.2.1 Fonctionnement

Lorsque l'utilisateur cherche à se connecter au routeur, celui-ci va interroger le serveur TACACS+ pour savoir quelle action réaliser.

Le serveur TACACS+ répond qu'il faut demander le nom d'utilisateur.

Le routeur demande ensuite le nom d'utilisateur au client.

Ce nom d'utilisateur est transmis jusqu'au serveur TACACS+ qui va ensuite demander au routeur d'effectuer la demande du mot de passe.

De la même manière, le serveur TACACS+ demande au routeur d'effectuer la demande du mot de passe auprès du client.

Une fois les informations récupérées, le serveur décide de valider ou de rejeter la demande de connexion.

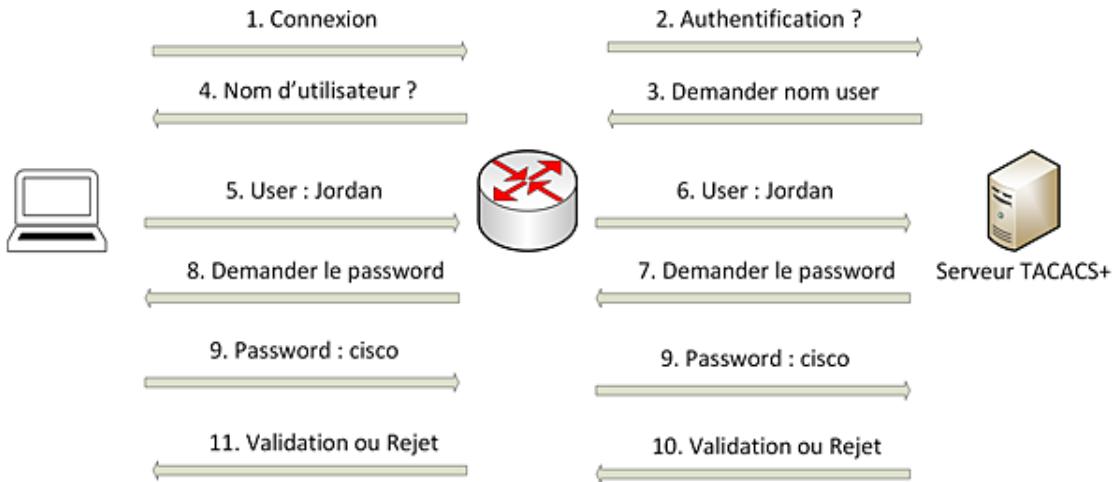


Figure 4 : Fonctionnement du protocole TACACS+

8.3 Comparaison

Tableau 2 : Comparaison entre les protocoles TACACS+ et RADIUS

TACACS+	RADIUS
Protocole propriétaire Cisco	Protocole standard ouvert
Utilise TCP comme protocole de transmission	Utilise UDP comme protocole de transmission
Traite l'authentification, l'autorisation et la responsabilité différemment	L'authentification et l'autorisation sont combinées
Utilisé pour l'administration des appareils	Utilisé pour l'accès au réseau
Utilise le numéro de port TCP 49	Utilise le numéro de port UDP 1812 pour l'authentification et l'autorisation et 1813 pour la traçabilité

8.4 Les outils de monitoring

Plusieurs outils de surveillance peuvent être utilisés. Ces outils peuvent être classés en fonction des attentes de l'administrateur et des objectifs spécifiés. Ils peuvent également être classés en fonction de la valeur et de l'impact économique des équipements à surveiller, car il existe toujours des outils gratuits et d'autres outils payants. Dans ce qui suit, nous proposons quelques solutions.

8.4.1 Les plateformes éditeurs

Depuis la naissance du terme de supervision, les grands éditeurs de logiciel ont rapidement compris que la supervision devient un besoin exigé par les entreprises qui essayent toujours

de garantir la disponibilité de leurs services, pour cela les éditeurs de logiciel ont commencé à développer des outils de surveillance payants au profit de ces entreprises.

Actuellement on retrouve des logiciels de supervision proposés par les plus populaires éditeurs de logiciel tel que Scom(Microsoft), HP OpenView(HP), IBM Trivoli Monitoring(IBM), BMC Patrol(BMC).

Dans ce qui va suivre, nous présenterons trois leaders des logiciels payants de supervision : Scom, HP OpenView et IBM Trivoli Netview

- **Scom**

Scom (System Center Operations Manager) autrefois connu sous le nom de MOM (Microsoft Operations Manager) est un programme de supervision réseau Microsoft développé par Microsoft qui permet le monitoring des différents équipements grâce à une interface logicielle, l'outil peut supporter seulement les matériaux et produits Microsoft (Switch, serveurs...)

- **HP OpenView**

HP OpenView est parmi les logiciels majeurs de la supervision. Il permet la supervision des équipements réseaux et l'affichage de l'état courant des équipements grâce à une interface graphique. Un système d'alarme intégré permet de synchroniser tous les équipements et de communiquer avec les machines par le protocole SNMP.

Le logiciel HP OpenView permet le contrôle d'un réseau distribué depuis un seul point. HP OpenView envoie des requêtes SNMP périodiques vers les agents, si un état change ou un périphérique devient inreachable, une alarme est directement déclenchée

- **IBM Trivoli Monitoring**

La solution IBM Tivoli Monitoring est conçue pour faciliter la gestion des applications critiques en surveillant de façon proactive les principales ressources informatiques IBM Tivoli Monitoring est capable d'apporter la réponse la plus adaptée aux différents événements et incidents survenant pendant une exploitation informatique, typiquement d'agir directement sur le composant logiciel ou sur le système (réseau, serveurs, ...) responsable d'un mauvais temps de réponse.

8.4.2 Les plateformes libres

Il existe des solutions de supervision libres et professionnelles. 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 des participations aux forums.

Parmi les plus répandues, reconnues du moment nous pouvons citer Nagios, ZABBIX, EYES-OF NETWORK et FAN

Nagios

Nagios est certainement le logiciel libre le plus connu dans le milieu de la supervision réseau. Appréciée des entreprises ainsi que des particuliers, cette application possède une

très grande communauté qui participent activement au développement. L'architecture logicielle est modulaire comme chez ses concurrents : Le moteur qui gère l'ordonnancement de la supervision, écrit en C en plus l'interface Web réalisé à l'aide des CGI

Aussi des greffons, ou plugins qui étendent les possibilités de Nagios (Plus de 1200 plugins existants sur nagiosexchange.org)

Il existe notamment des plugins Nagios nommée NRPE et NCSA c'est un agent esclave qui attend l'ordre du moteur Nagios (polling) et NCSA envoi de lui-même les données (trapping).

L'interface est divisée en trois :

- Partie monitoring, qui permet plusieurs vues : vue globale, vue précise, vue de la carte du réseau, vue des problèmes, ... même une vue "3D".
- Partie reporting regroupant les tendances des statistiques, les alertes et évènements ainsi qu'un rapport de disponibilités des services.
- Partie configuration classique permettant de tout configurer.

Avantages

Nagios est reconnu auprès des entreprises, grande communauté Il plétoire de plugins qui permettent d'étendre les possibilités C'est une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau et les performances du moteur, un autre avantage majeur c'est qu'il ya beaucoup de documentations sur le web.

Inconvénients

Nagios comprend une interface non ergonomique et peu intuitive qui limite son utilisation en plus sa configuration fastidieuse via beaucoup de fichiers et pour avoir toute les fonctionnalités il faut installer des plugins, de base c'est assez limité. [15]

Zabbix

Créé en 2001, puis donnant naissance à une entreprise nommée Zabbix SIA en 2005, Zabbix est une solution de supervision open-source de plus en plus prisée. L'entreprise vise à faire de Zabbix un logiciel reconnu dans le milieu de la supervision et créer une communauté autour de lui pour permettre une évolution plus rapide. A côté de cela, cette société propose un service de maintenance commercial.

L'architecture logicielle est découpée en composants dans le but de faciliter le monitoring distribué :

Serveur : Le serveur est le cœur de l'application Zabbix. Il centralise les données et permet de les attendre (trapping) ou d'aller les chercher (polling). Il centralise aussi toutes les informations de configuration et permet d'alerter les administrateurs en cas de problème.

Le proxy : Élément optionnel de l'architecture, il permet de bufférer les données reçus des différents sites dans le but d'alléger les traitements pour le serveur.

L'agent : Une fois installé sur un système, l'agent va collecter les données locales et les envoyer au serveur.

L'interface Web : Celle-ci est une partie du serveur bien qu'il n'est pas obligatoire qu'elle se trouve sur la même machine que le serveur. L'interface permet de configurer entièrement Zabbix, d'accéder aux statistiques ainsi qu'à d'autres informations

Avantages

Zabbix est une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statistiques et reporting aussi elle est menée d'une interface vaste mais claire permettant la gestion des templates poussée, avec import/export XML, modifications via l'interface aussi elle est compatible avec MySQL, PostgreSQL, Oracle, SQLite

Inconvénients

Son interface est un peu vaste, la mise en place des templates n'est pas évidente au début : petit temps de formation nécessaire en plus que l'agent zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données (via VPN par exemple). Cette solution commence à être connu, mais pas encore auprès des entreprises : Peu d'interfaçage avec d'autres solutions commerciales [15]

Check_MK

C'est une solution de supervision open source développée par Mathias KETTNER en 2008. En réalité c'est une extension de Nagios, qui est l'outil de monitoring le plus connu et le plus utilisé dans les entreprises.

Avantages

C'est une solution simple à installer et configurer aussi son interface Web est beaucoup plus intuitive et elle intègre des outils, comme PNP4Nagios et RRDTool. L'interface permet une configuration entièrement graphique. Aussi Check_MK est capable de réaliser un inventaire automatique des services disponibles sur un hôte à superviser. et pas besoin de développer des sondes.

Inconvénients

Offre plus de services sur l'environnement Unix [16]

Cacti

Cacti est un logiciel de supervision permettant de surveiller l'activité de son architecture informatique à partir de graphiques quotidiens, hebdomadaires, mensuels et annuels.

Cette solution n'est donc pas destinée à alerter en temps réel sur les dysfonctionnements d'un système mais bien de proposer une vision dans le temps de l'évolution d'indicateurs matériels et logiciels (trafic réseau, occupation des disques, temps de réponse, etc...).

Avantages

La configuration est trop simple avec l'utilisation des templates pour les machines, les graphiques, et la récupération des données tout se configure aisément et entièrement via l'interface web. Import/ Export très simple des templates au format XML

En plus avec le choix du moteur de récolte des données, On peut opter pour la performance ou la simplicité et donc gestion des utilisateurs

Elle présente aussi une communauté sur le web, qui résulte la présence d'une dizaine de plugins permettant d'étendre les fonctionnalités

Inconvénients

Cacti présente un développement lent et ne comporte pas la gestion d'alarmes, sauf avec un plugin nommé Thold ainsi il se limite dans la gestion de panne en plus que l'absence d'une cartographie de réseau. [17]

Eyes-Of-Network

Eyes Of Network « EON » est une solution complète de supervision, basée sur la distribution GNU/Linux CentOS, gérée et administrée via une interface web, qui est accessible par tous les acteurs d'un système d'informations avec une vue correspondant à chacun de leur métier.

EON est open source et sous licence GPL2, qui englobe plusieurs outils de supervision monitoring et de gestion, chacun d'eux est spécialisé pour effectuer une tâche spécifique de supervision :

- NAGIOS : gestion des incidents et des problèmes,
- THRUK : interface de supervision multibackend,
- NAGVIS : cartographie personnalisée de la disponibilité,
- CACTI et PNP4NAGIOS : gestion des performances,
- WEATHERMAP : cartographie de la bande passante,
- BACKUP MANAGER : Outil de sauvegarde de la solution,
- EONWEB : Interface Web unifiée de la solution,
- EZGRAPH : Librairie d'affichage des graphiques,
- SNMPTT : Traduction des traps snmp,
- GLPI / OCS / FUSION : Gestion de parc et inventaire.

Avantages

EON est managée avec une interface de configuration web qui permet de faciliter le déploiement des outils de supervision aussi cette solution regroupe tous les fonctionnalités de Nagios et Cacti.

Inconvénients

Une configuration en interface web qui ne supporte pas la navigation sécurisée (HTTPS)

8.5 Les outils d'automatisation

Ansible

Ansible est un logiciel libre qui permet, de façon automatique et simple, d'effectuer l'installation de paquets et de playbooks, de configurer les serveurs de production et de réaliser différentes tâches de paramétrage possibles en SSH. [18]

Puppet

Outil open source de gestion des configurations, Puppet automatise le packaging et le provisioning d'applications sur les serveurs de production. Développé en Ruby, il gère les déploiements logiciels sur les serveurs bare metal ou les machines virtuelles. [18]

Chef

Logiciel de gestion de configurations pour le développement informatique. Il permet d'automatiser des infrastructures serveur comme les systèmes d'exploitation. Elles entrent en ligne de compte pour le packaging et le provisioning. [18]

Tableau 3 : Etude comparatif des outils d'automatisation

Outil Critères			
Sans Agent	Oui	Non	Non
Langage	Python	Ruby	Ruby
Dépendance client	Python,sshd ;bash	Ruby,ssh,bash	Ruby
Mécanisme	Push	Pull	Pull
Approche	Procédural	Procédural	Déclarative
Installation	Facile	Peu facile	Difficile

Conclusion

Dans ce premier chapitre, nous avons présenté, d'abord, les intérêts des grands concepts de notre projet et nous avons étudié, les protocoles qui peuvent nous aider. Puis, nous avons fait une étude des solutions permettent d'accomplir ce sujet.

Dans le chapitre suivant nous allons citer les besoins de projet et les solutions optées.

Chapitre 3: Sprint 0 Spécification des besoins

Introduction

Un projet Scrum démarre généralement par la première phase «sprint 0 » dédié aux travaux préparatoires pour construire une bonne vision du produit. Durant ce chapitre, nous allons identifier les besoins que notre projet doit fournir et nous allons présenter un plan de la release afin de produire notre backlog du produit initial.

Nous allons également décrire l'environnement de réalisation, ainsi que l'architecture de notre projet.

1. Spécification des besoins

1.1 Besoins fonctionnels

Les besoins fonctionnels expriment une action que doit effectuer le système en réponse à une demande. Il ne devient opérationnel que s'il les satisfait. Dans le cas de notre projet, le travail est composé de trois grandes parties:

L'implémentation et la configuration d'une solution Open Source de supervision des différents équipements réseaux et serveurs

L'objectif dans cette partie est de mettre en place une solution de monitoring sur une plateforme virtuelle grâce à l'outil de virtualisation. Cette solution nous fournit un tableau de bord de management qui nous permet d'avoir une visibilité globale et instantanée sur l'état de santé du système informatique, elle permet de :

- Surveiller la disponibilité des équipements, de service sur la plupart des systèmes d'exploitation.
- Surveiller l'usage du CPU, de la RAM, du Disque Dur et/ou de quelques processus
- Être alerter en cas de problème (CPU et/ou RAM sur utilisé, hôtes et/ou services inaccessible...)
- Ressortir le comportement des ressources surveillées sur une période déterminée
- Ressortir une carte du réseau
- Tracer des graphes de performances.
- Collecter des données Dashboard et présenter des rapports.
- Réaliser l'interfaçage avec le protocole SNMP.
- Vérifier l'exécution des services machine.
- Acquitter des alertes par les administrateurs en cas de détection d'une panne.

L'implémentation d'une solution d'accès local ou distant sécurisé

La solution d'accès sécurisée et la solution de contrôle d'accès aux données est indispensable afin d'empêcher toute fraude et intrusion illégale donc toutes les tentatives d'accès doivent être validées, authentifiées et autorisées selon les priviléges octroyés par des

systèmes de sécurité et de protocole d'authentification qui assurent le contrôle de conformité, la traçabilité et la visibilité sur tous les accès.

De même elle assure la protection de transmission des données DATA dans le réseau WAN grâce à des protocoles de cryptage afin de garantir la mobilité des superviseurs qui peuvent accéder aux différentes ressources intérieures en toute sécurité indépendamment de leurs emplacement.

La mise en place de la solution d'automatisation

Automatiser la mise en supervision des équipements informatiques et servir de l'outil de gestion de configuration pour installer automatiquement les agents de supervision puis de déclarer les nouveaux éléments dans l'outil de supervision

1.2 Besoins non fonctionnels

Afin d'offrir une solution complète et performante à différents niveaux, nos plateformes doivent couvrir les besoins non fonctionnels suivants :

Facilité d'utilisation : Le système offre une interface simple facile à utiliser en donnant à l'administrateur la possibilité d'agir sur les ressources qu'il manipule.

Rapidité : Le logiciel de supervision prévient dès qu'un problème survient avant même que la plupart des utilisateurs en aient conscience.

Extensibilité: Le système doit être extensible et permet d'ajouter et de supporter d'autres fonctionnalités et d'intégrer tout type d'équipement réseau.

Performance : une application doit être avant tout performante c'est à dire à travers ses fonctionnalités, elle répond à toutes les exigences des usagers d'une manière optimale.

1.3 Backlog général du produit

Le backlog général permet de lister les grandes lignes expliquant les besoins de client que l'équipe projet doit réaliser. Il contient donc la liste des fonctionnalités intervenant dans la constitution d'un produit, ainsi que tous les éléments nécessitant l'intervention de l'équipe projet.

Tous les éléments inclus dans le backlog scrum sont classés par priorité indiquant l'ordre de leur réalisation.

Tableau 4: Backlog général

Tâche	ID	USER STORY	Priorité	Complexité	Sprint
Installation de l'environnement de travail	T1.U1	En Tant qu'Administrateur je veux installer un outil de virtualisation	1	1	
	T1.U2	En tant qu'Administrateur je veux installer un logiciel de simulation de réseaux informatiques	2	1	
	T1.U3	En tant qu'Administrateur je veux installer un hyperviseur	3	8	
	T1.U4	En tant qu'Administrateur je veux installer une machine virtuelle Ubuntu	4	1	1
	T1.U5	En tant qu'Administrateur je veux installer une machine virtuelle Windows 7	4	1	
	T1.U6	En tant qu'Administrateur je veux installer et configurer l'outil de supervision	5	20	
Installation d'un protocole de gestion des équipements réseaux	T2.U1	En tant qu'Administrateur je veux installer le protocole de gestion des équipements sur les machines à superviser	6	8	

Ajout des machines à superviser au niveau de l'outil de supervision	T3.U1	En tant qu'Administrateur je veux superviser des équipements et des services avec la génération des statistiques et rapports	7	20	
Mise en place d'un serveur d'authentification	T4.U1	En tant qu'Administrateur je veux installer un serveur d'authentification	8	20	
	T4.U2	En tant qu'Administrateur je veux configurer les routeurs comme clients	9	10	
Mise en place d'un VPN	T5.U1	En tant qu'Administrateur je veux mettre en place un VPN d'accès avec un VPN client mobile en mode léger au niveau de la machine virtuelle Windows	10	20	2
Mise en place d'un serveur de messagerie	T6.U1	En tant qu'Administrateur je veux mettre en place un serveur de messagerie électronique au niveau de l'hyperviseur	11	8	
Implémentation d'une solution d'automatisation	T7.U1	En tant qu'administrateur je veux mettre en place d'un serveur de transfert de fichiers	12	8	3

	T7.U2	En tant qu'administrateur je veux installer automatiquement les agents de supervision	13	20	
	T7.U3	En tant qu'un administrateur je veux déclarer les nouveaux éléments dans l'outil de supervision	14	20	
					Total : 164

Après avoir décrit le backlog de notre projet, il faut présenter le diagramme de cas d'utilisation générale de notre sujet.

1.4 Diagramme de cas d'utilisation général

Un diagramme de cas d'utilisation est un moyen simple d'exprimer des besoins. Il montre le comportement d'un composant, une classe ou un système, tel qu'un utilisateur extérieur le voit. Il correspond à un ensemble de transactions effectuées au cours de l'interaction entre le système et l'acteur (administrateur).

1.4.1 Identification d'acteurs :

Globalement, nous avons distingué un seul acteur: l'administrateur, celui qui aura la fonction de la supervision réseau. En fait son rôle consiste à superviser le réseau en récupérant des informations sur les équipements et réparer les pannes détectées. Cet acteur utilise le système à travers un ensemble d'interfaces bien définies. Il doit s'authentifier pour qu'il puisse utiliser le système.

1.4.2 Diagramme de cas d'utilisation

Afin de décrire les exigences fonctionnelles de notre système, voici une description du cas d'utilisation globale ainsi que d'autres qui sont les principaux.

Ce diagramme va nous permettre de décrire l'interaction entre le projet et les acteurs de notre projet en utilisant le diagramme de cas d'utilisation du langage de modélisation UML



Figure 5 : Diagramme de cas d'utilisation général

- **Diagramme de cas d'utilisation « Gestion des services »**

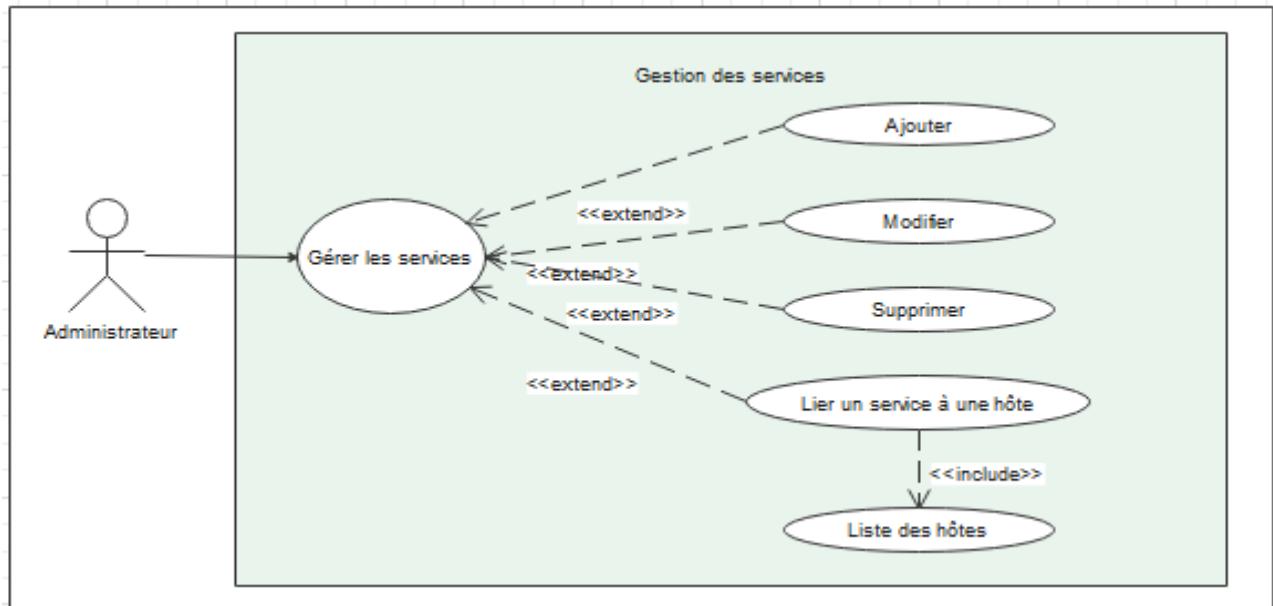


Figure 6 : Diagramme cas d'utilisation Gestion des services

Titre : Gestion des services

Objectif: ajouter, modifier, supprimer un service ou lier un service à une hôte parmi la liste des hôtes.

Acteurs: Administrateur.

Précondition: L'administrateur est déjà identifié.

Scénario nominal

- L'administrateur affiche la partie de gestion des services.
- L'administrateur choisit une opération à faire.
- L'administrateur effectue l'opération choisie précédemment.
- Le système enregistre les modifications effectuées.

Enchaînement d'exception

Un message d'erreur sera affiché si les informations introduites lors de l'opération sont incorrects ou si un champ obligatoire est vide.

1.5 Diagramme d'activités

Le Diagramme d'activités est un autre diagramme important dans UML pour décrire les aspects dynamiques du système. Il est essentiellement un organigramme pour représenter le flux d'une opération vers une autre opération.

La description d'un cas d'utilisation par un diagramme d'activités correspond à sa traduction algorithmique

1.5.1 Diagramme d'activité « Notification »

Ce diagramme décrit les différentes activités que prend le système lorsqu'il détecte un service ou équipement non fonctionnel. A ce stade le système commence par vérifier l'état du service correspondant à l'hôte jusqu'à la validation de l'état non-ok. Ensuite, il récupère la liste des contacts afin d'en choisir un et le notifier par un mail.

Si l'intervalle de temps de la prochaine notification est écoulé et que l'état du service est encore non-ok, le système recommence la vérification des services.

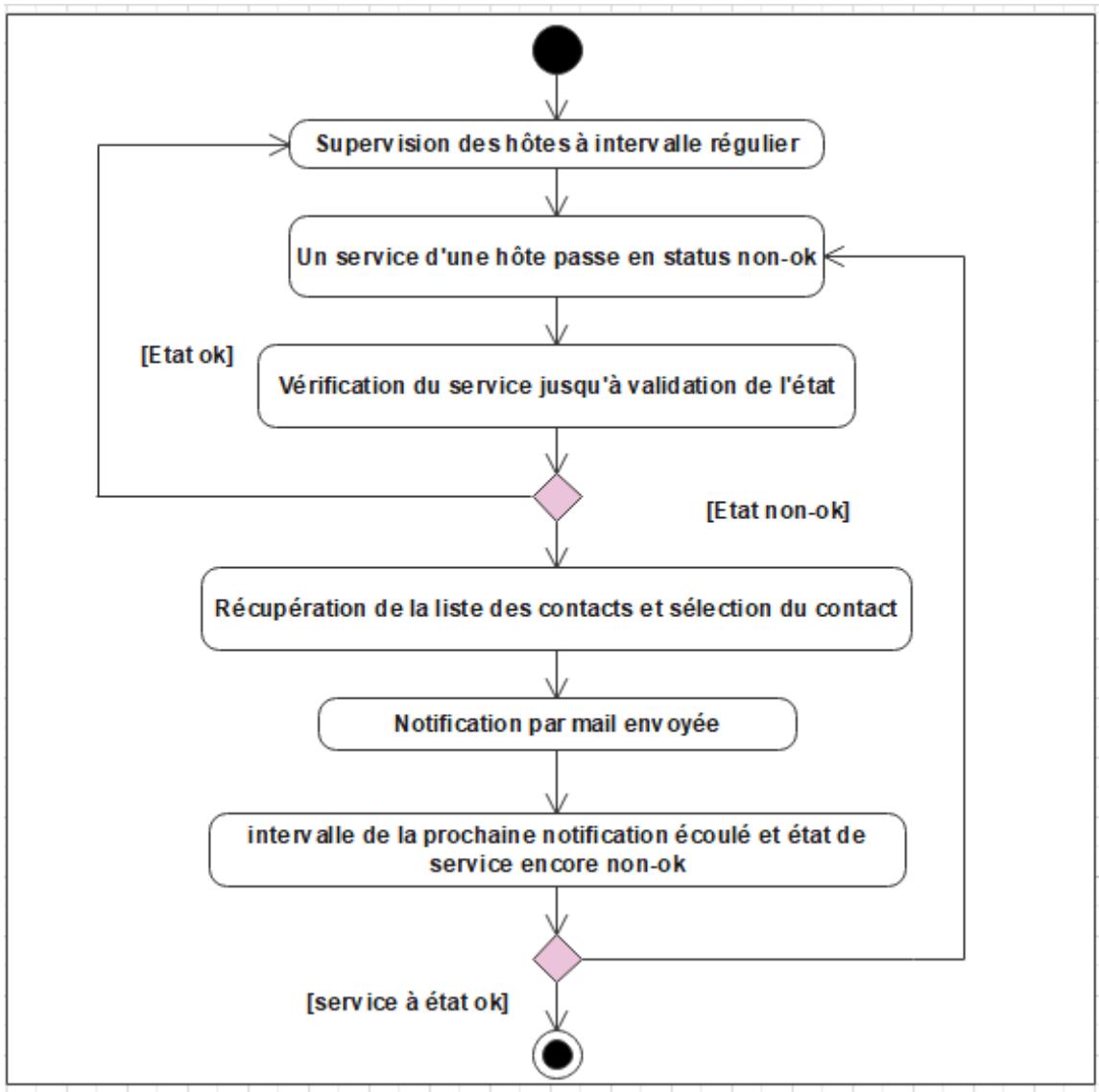


Figure 7: Diagramme d'activités

1.6 Environnement de travail

1.6.1 Environnement matériel :

Tout au long de notre projet, nous avons eu à notre disposition un ordinateur portable avec la configuration suivante :

- Intel(R) Core(TM) i3-5005U CPU (2.00GHz)
- 12 Go de RAM
- Disque dur de capacité 500 Go.
- Système d'exploitation Windows 10

1.6.2 Environnement logiciel

Pour permettre de mieux calibrer les solutions, les produits choisies, sont jugés selon Leurs simplification puisque les outils de supervision, authentification, automatisation et virtualisation doivent permettre le gain du temps à l'administrateur, afin de donner plus d'importance à d'autres tâches utiles plutôt que surveiller en permanence l'infrastructure et

Le choix dépend en général de la taille du réseau et des périphériques utilisés, en plus ces solutions doivent être Open source et simples dans l'installation et l'utilisation.

Pour ce fait on va citer brièvement les solutions retenues dans cette section ainsi que leur mode de fonctionnement. Certaine sont choisies après l'étude comparatif que nous avons fait dans le dernier chapitre et certaines sont imposé par la société.

- **Gns3**

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.

- **VMware Workstation**

VMware Workstation est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique. [19]

- **EyesOfNetwork (EON)**

En se basant, sur l'étude comparatif que nous avons présenté, on estime qu'Eyes-Of-Network est la solution la plus adaptée aux besoins de notre projet pour plusieurs raisons, En effet Eyes-Of network combine deux outils très efficaces et connus dans le domaine de monitoring, chacun d'eux est spécialisé pour effectuer une tache spécifique de supervision on parle ici de **Nagios** et **Cacti**, en revanche, il inclut d'autres applications intégrées de supervision répondant aux différents besoins de supervision, qu'on va les détailler plus tard.

Grâce à ses plugins, EON 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 Eyes-of-network 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. Aussi, utilisé surtout par plusieurs entreprises renommées, tels que Yahoo (100 000 serveurs), Yellow pipe Web Hosting (7000 serveurs) [20]

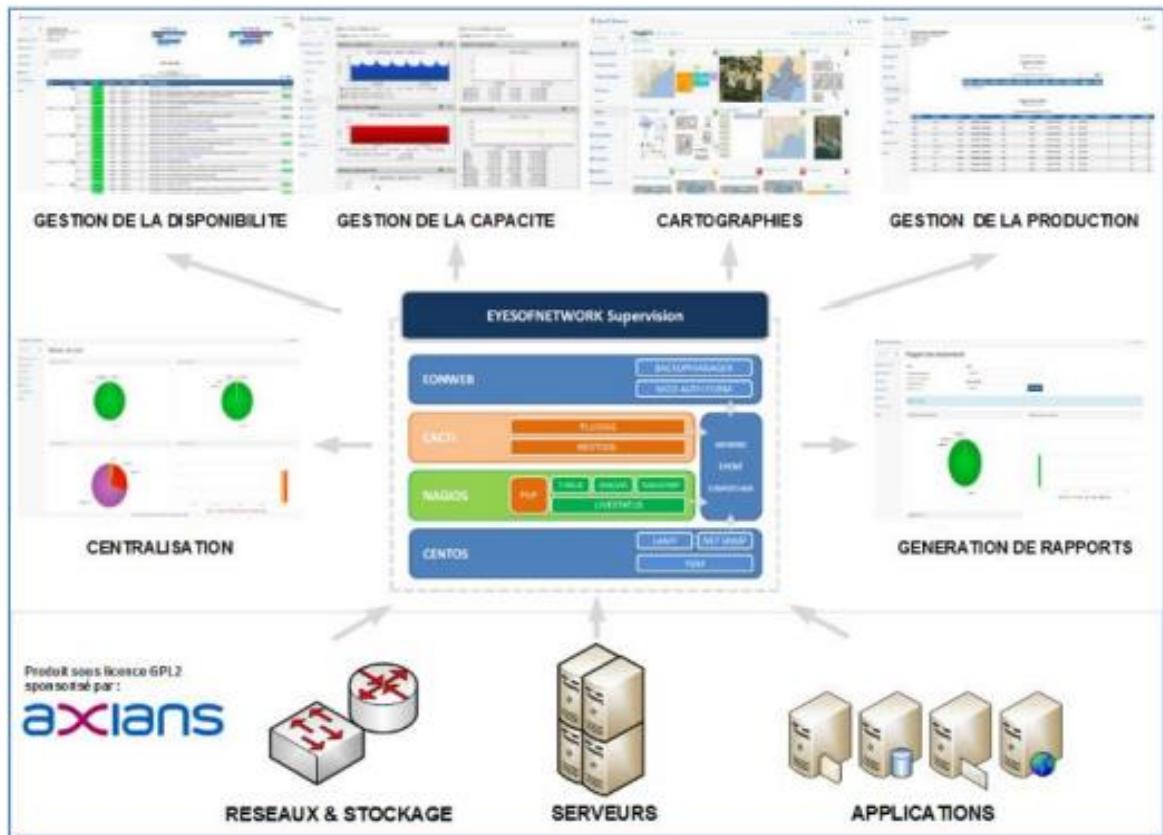


Figure 8 : Composants d’Eyes-of-network

- **Ansible**

Dans notre cas nous choisissons l’outil Ansible qui est reconnu pour la simplicité de son langage. Écrit dans le langage lisible par l’humain YAML, sa petite courbe d’apprentissage échappe à la complexité et aux connaissances exclusives associées à Chef, et à Puppet. Ansible est plus facile d’accès que les autres options et ses instructions s’écrivent et se comprennent plus aisément pour une organisation

L’avantage d’Ansible par rapport aux autres outils de gestion de configuration est son aspect sans agent, c’est-à-dire, il n’a pas besoin d’une configuration a priori pour contrôler une machine. De même, sa communauté est plus grande, et chaque mois de nouvelles options sont ajoutées. [21]

Donc, Ansible reste le plus adapté et facile à mettre en œuvre en comparaison avec Chef et Puppet.

- **FreeRADIUS**

Après avoir étudié, et comparé les protocoles mentionnés dans le chapitre 2 à savoir TACACS et RADIUS, nous avons choisi ce dernier, pour réaliser et atteindre un besoin de notre projet pour ce faire nous avons recourt à FreeRADIUS qui est un serveur RADIUS libre. Il offre une alternative aux autres serveurs d’entreprise RADIUS, en plus c’est un des serveurs RADIUS les plus modulaires et riches en fonctionnalités disponibles aujourd’hui

FreeRADIUS est, entre autres, utilisé par des fournisseurs d'accès à l'internet pour authentifier leurs clients et leur communiquer une configuration IP. Il est considéré comme le serveur le plus utilisé dans le monde

- **VMware ESXi**

VMware ESXi est un hyperviseur de type 1 indépendant des systèmes d'exploitation. Il repose lui-même sur le système d'exploitation VMkernel qui assure l'interface avec les agents dont il soutient l'exécution.

VMware décrit le système ESXi comme similaire à un nœud informatique sans état. Les informations d'état peuvent être téléchargées à partir d'un fichier de configuration enregistré. VMkernel – le système d'exploitation d'ESXi – assure directement l'interface avec les agents VMware et les modules tiers agréés. Les administrateurs chargés de la virtualisation peuvent configurer VMware ESXi via sa console ou le client VMware vSphere, et consulter la liste de compatibilité matérielle de VMware pour y trouver les équipements agréés et pris en charge sur lesquels installer ESXi.

Avant l'arrivée d'ESXi, VMware proposait l'hyperviseur ESX, qui comprenait davantage de composants, tels que le système d'exploitation de la console et un pare-feu. Des interfaces distantes de ligne de commande et des éléments normés de gestion des systèmes remplacent les fonctions de la console des services. L'hyperviseur prend en charge la fonction de déploiement automatisé Auto Deploy, la création d'images personnalisées, ainsi que d'autres outils que n'intégrait pas ESX. VMware indique que l'architecture d'ESXi occupe moins de 150 Mo d'espace – dont 32 Mo d'espace disque – à comparer aux près de 2 Go d'ESX. [22]

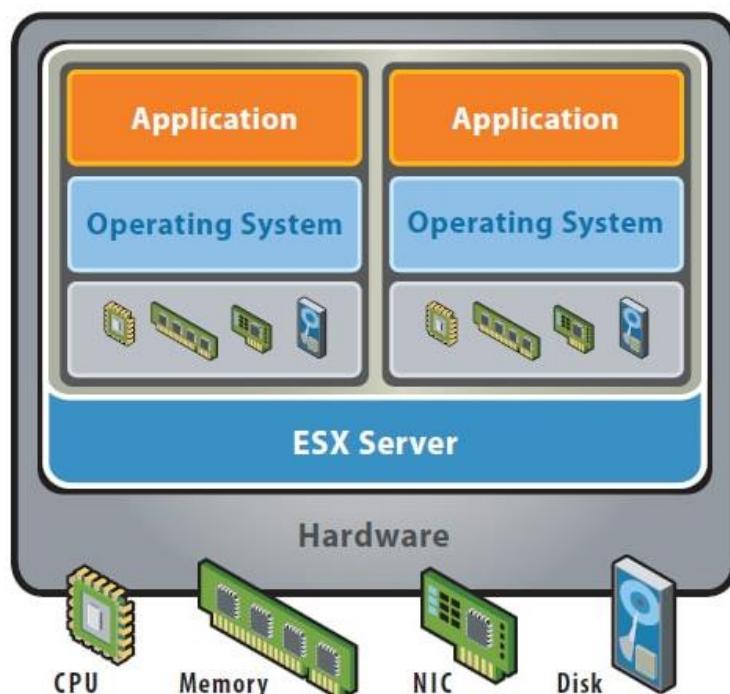


Figure 9 : Architecture VMware ESXi

- **PUTTY**

PuTTY est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin, et TCP brut. Il permet également d'établir des connexions directes par liaison série RS-232. À l'origine disponible uniquement pour Windows, il est à présent porté sur diverses plates-formes Unix (et non-officiellement sur d'autres plateformes). PuTTY est écrit et maintenu principalement par Simon Tatham. C'est un logiciel libre distribué selon les termes de la licence MIT.

- **Cisco VPN Client**

Cisco VPN Client est un client VPN propriétaire permettant de se connecter aux concentrateurs VPN Cisco. Il est utilisé dans le cadre d'infrastructures gérant des milliers de connexions, on le retrouve donc le plus souvent dans les grandes entreprises et de nombreuses universités.

1.7 Architecture de projet

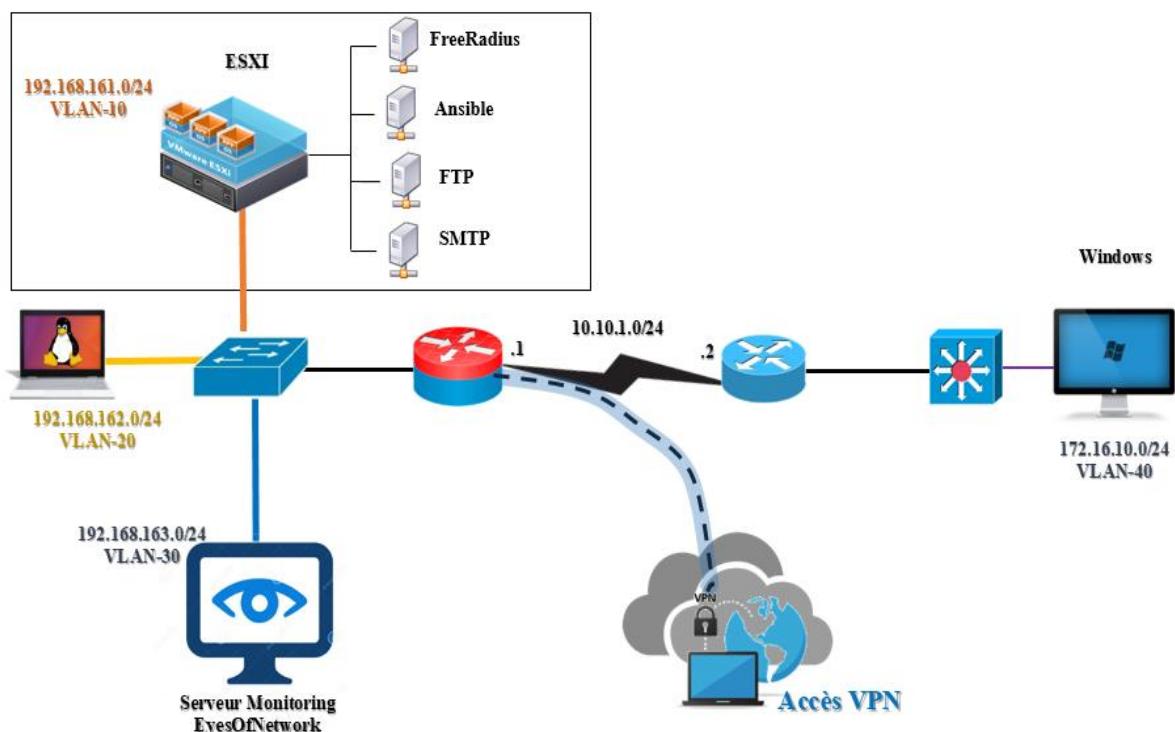


Figure 10 : Architecture du projet

Afin de mieux répondre aux besoins des entreprises clientes, la conception d'un réseau doit s'effectuer suivant un modèle hiérarchique.

Modèle de conception hiérarchique à trois couches

- **La couche d'accès (Access Layer) :**

Cette couche permet de constituer des périphériques finaux. Le rôle de cette couche est de connecter les périphériques finaux au reste du réseau et de vérifier s'ils sont autorisés.

- **La couche de distribution (Distribution Layer) :**

Cette couche contient essentiellement des commutateurs de niveau 3 (fonction de routage) et sert d'interconnexion entre la couche d'accès et la couche de cœur de réseau. Son rôle et de gérer le flux du trafic à l'aide de stratégies et de délimiter les domaines de diffusion via des fonctions de routage inter VLAN

- **La couche cœur de réseau (Core Layer) :**

La couche cœur et considérée comme étant le réseau fédérateur à haut débit de l'inter-réseau et assure la connexion aux ressources internet. Le trafic au niveau de cette couche est important et rapide.

- **La couche périphérique (Edge Layer) :**

Ce bloc représente l'interconnexion du réseau local avec les sites distants à travers deux réseaux étendus et un accès de tous les PCs via l'Internet. La haute disponibilité doit être présente à tous les niveaux et chaque bloc dans l'infrastructure doit respecter les principes de design d'un réseau d'entreprise modulaire. Cette architecture complètement modulaire offre une approche évolutive avec une simplicité d'exploitation, de gestion et de maintenance à tous les niveaux.

Les équipements réseau utilisées sont présentés dans le tableau ci-dessous :

Tableau 5 : Liste des équipements utilisés

Equipements	Type et marque d'équipement
SW1	Cisco c3745-adventerprise
SW2	Cisco c3745-adventerprise
R1	c3725-adventerprisek
R2	c3725-adventerprisek
VMwareESXi6.x-1	VMware VM template
Ubuntu-1	VMware VM template
EyesOfN-1	VMware VM template
Windows7-1	VMware VM template

Les Vlans seront nommées dans la configuration comme suit :

Tableau 6: Les noms des VLANs

Nom de vlan	ID vlan	Adresse Réseau
VLAN-10	10	192.168.161.0/24
VLAN-20	20	192.168.162.0/24
VLAN-30	30	192.168.163.0/24
VLAN-40	40	172.16.10.0/24

La liste illustrée dans le tableau ci-dessous présente les Vlans et les adresses IP employées:

Tableau 7 : Vlans et adressage des PCs

Nom de l'hôte	Vlan ID	Adresse IP	Passerelle
VMwareESXi6.x-1	10	192.168.161.139	192.168.161.254
Ubuntu-1	20	192.168.162.100	192.168.162.254
EyesOfN-1	30	192.168.163.130	192.168.163.254
Windows7-1	40	172.16.10.100	172.16.10.254

1.8 Planification de la release

Release est une série de sprints consécutifs qui peuvent aider à fournir des produits qui apportent de la valeur à ses utilisateurs. À la fin de chaque version, nous obtiendrons un livrable indépendant des autres versions du même projet. En ce qui nous concerne, nous avons découpé le projet en une version séparée qui commence le 3 mars 2020 et se termine le 30 mai 2020.

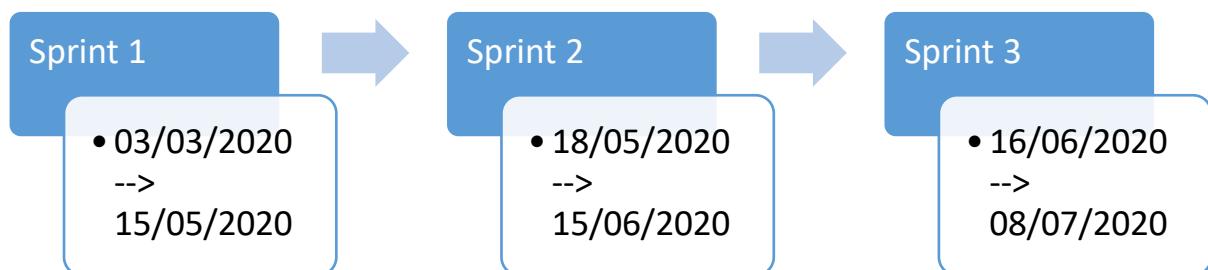
Le découpage était comme suit :

Sprint 1 : 03/03/2020 → 14/04/2020

Sprint 2 : 15/04/2020 → 07/05/2020

Sprint 3 : 18/05/2020 → 30/05/2020

Mais suite aux changements nous étions obligés de changer la planification des releases comme le montre le graphique ci-dessous :



Le tableau ci-dessous présente notre planification de release ainsi que les User Stories de chaque release :

Tableau 8 : Planification de release

Sprint	Estimation
Sprint 1	
Du 03/03/2020 jusqu'à 15/05/2020 T1.U1,T1.U2 ,T1.U3,T1.U4,T1.U5,T1.U6 ,T2.U1, T3.U1	60 Points
Sprint 2	
Du 18/05/2020 jusqu'à 15/06/2020 T4.U1,T4.U2,T5.U1,T6.U1	66 Points
Sprint 3	
Du 16/06/2020 jusqu'à 02/07/2020 T7.U1,T7.U2,T7.U3	48 Points

Conclusion

Dans ce chapitre, nous avons préparé notre plan de travail. Nous avons capturé les besoins fonctionnels de notre projet et présenté le backlog de produit. Nous avons par la suite exposé notre environnement de travail ainsi que l'architecture de notre solution. Nous avons également donné la planification des différents sprints à mettre en œuvre. Dans le chapitre qui suit nous allons entamer le premier sprint.

Chapitre 4 : Sprint 1 mise en place de l'outil de supervision

Introduction

Notre release sera composé de trois sprints. Dans ce chapitre nous allons présenter la mise en place de l'architecture à réaliser puisque c'est une étape essentielle permettant de prévoir de nombreux problèmes qui peuvent survenir.

1. Spécification fonctionnelle

1.1 Le Backlog du sprint

Avant de commencer le travail et après le choix des user stories à réaliser durant ce sprint, nous arrivons à l'étape de décomposition des user stories en tâches simples. Nous présentons à travers le tableau ci-dessous notre backlog de sprint détaillé avec l'estimation de chaque tâche en heure.

Tableau 9 : Backlog du sprint 1

ID	User story	Tâche	Estimation (h)
AAAA	Préparation de l'environnement de travail	Installation GNS3	0.5
		Installation et configuration de VMware Workstation	1
		Installation Windows 7	1
		Installation Ubuntu	1
		Installation et configuration de VMware ESXi	72
		Installation et configuration d'Eyes Of Network	6
		Configuration de la liaison GNS3 et machine physique	2
BBBB	Installation et configuration de l'agent de protocole simple de gestion de réseau (SNMP)	installation et configuration de l'agent SNMP sur les machines virtuelles	2
		Installation et configuration de l'agent SNMP sur les routeurs	2
		Création des plugins et commandes selon les besoins	26

CCCC	Ajout des hôtes à superviser au niveau de la solution de supervision	Ajout des hôtes	1
	Génération rapports et statistiques		72

Après avoir listé les tâches de ce sprint nous allons présenter son diagramme de cas d'utilisation.

1.2 Diagramme de cas d'utilisation du sprint 1

Ce cas d'utilisation offre à l'administrateur la possibilité de configuration et ajout des équipements à superviser dans le serveur de supervision

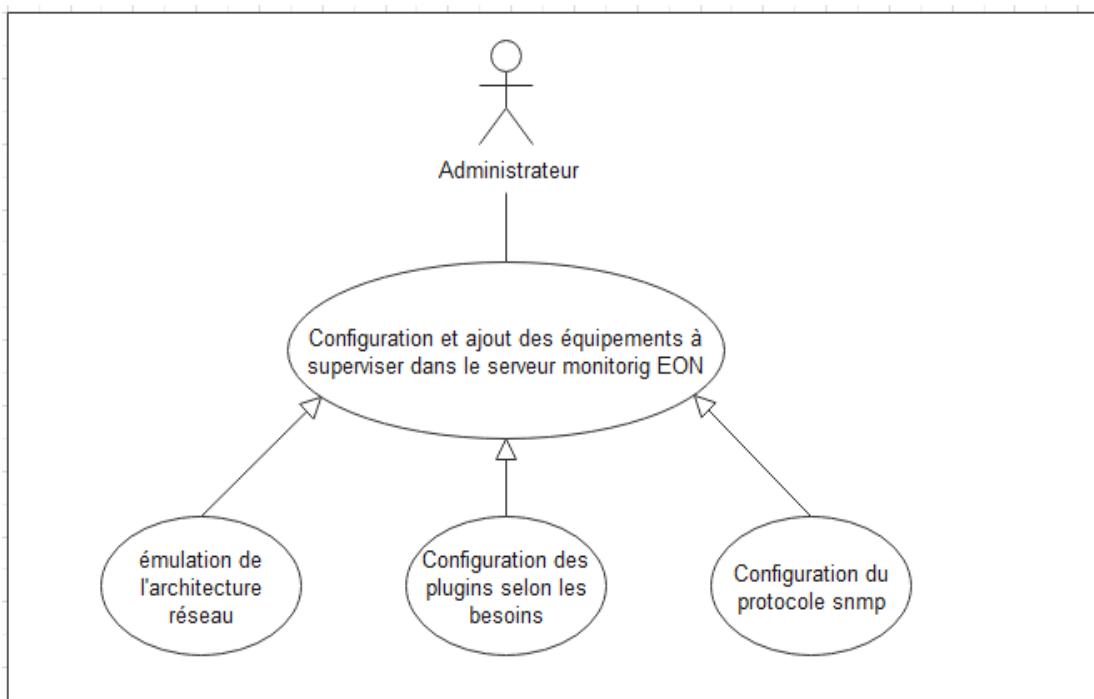


Figure 11: Diagramme de cas d'utilisation du sprint 1

1.3 Réalisation

- **Intégration GNS3 et VMware Workstation**

C'est un processus qui est particulièrement pratique pour les phases de test, car il permet de lier la partie système, désormais très répandue, dans la virtualisation au réseau lui aussi virtualisé.

- **Préparation des cartes réseau**

Dans le but d'avoir une mise en place simple, nous allons commencer par identifier les cartes réseau virtuelles.

Tableau 10 : liste des cartes réseau

Nom de carte	Adresse IP	Passerelle
VMware ESXi	192.168.161.10	192.168.161.254
VMware Ubuntu	192.168.162.10	192.168.162.254
VMware EON	192.168.163.10	192.168.163.254
VMware Windows	172.16.10.10	172.16.10.254

1.3.1 Installation

L'installation et la configuration de VMware ESXi est listée dans l'annexe A ainsi que les fichiers de configurations des routeurs

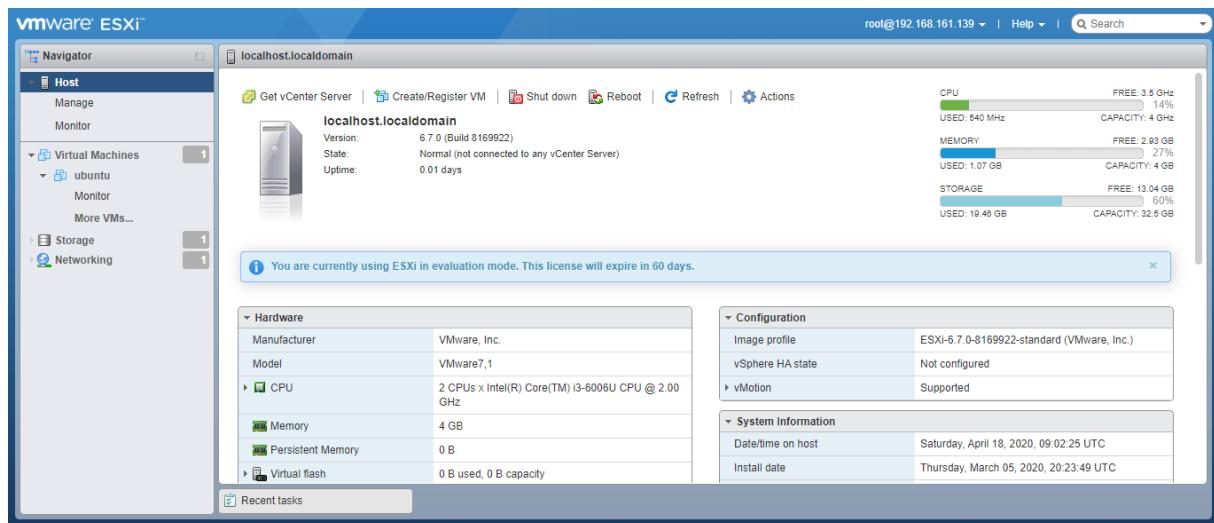


Figure 12 : Interface web d'ESXi

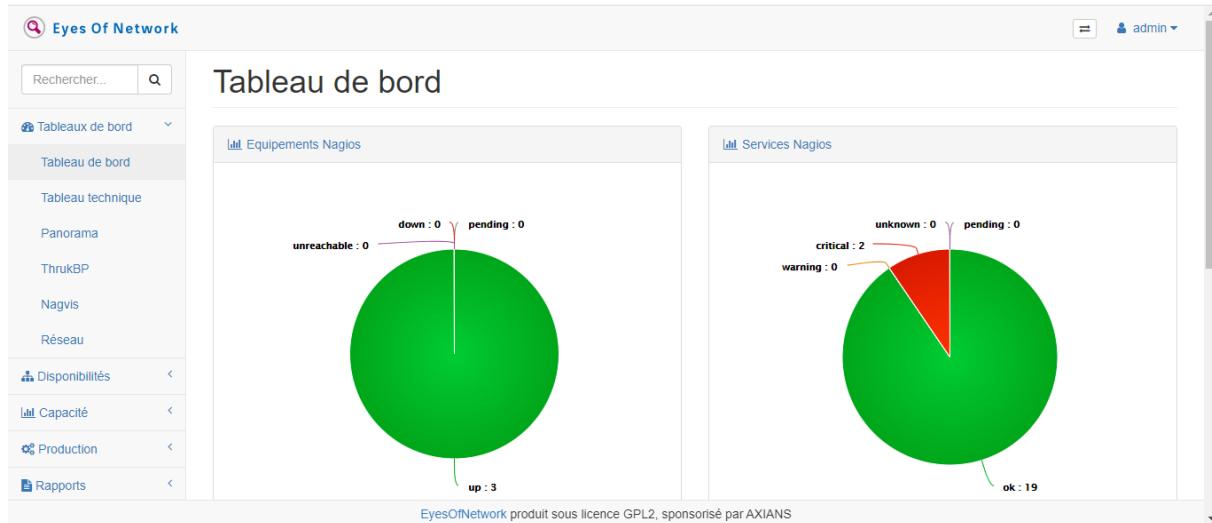


Figure 13 : interface web eyes of network

1.3.2 Installation et configuration de l'agent SNMP

- **Configuration snmp dans les machines**

Nous prenons l'exemple de configuration snmp sur un hôte Ubuntu

La configuration détaillée est citée dans l'<<Annexe B>>

- Il faut installer et activer le service SNMP dans l'hôte à superviser
- installation de MIB
- Configuration du fichier /etc/snmp/snmpd.conf

Autoriser l'accès en lecture des données SNMP à un hôte

```
#  
# ACCESS CONTROL  
#  
  
hrSystem groups only  
view systemonly included .1.3.6.1.2.1.1  
view systemonly included .1.3.6.1.2.1.25.1  
  
# system +  
  
from the local host  
rocommunity EyesOfNetwork 192.168.163.130| # Full access  
to basic system info  
#rocommunity public default -V systemonly # Default access
```

Figure 14: Configuration de fichier /etc/snmp/snmpd.conf

- **Configuration SNMP d'un routeur CISCO**

Pour configurer SNMP Il est indispensable de préciser le nom de communauté et l'adresse de notre serveur comme la montre la figure ci-dessous

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#snmp-server community EyesOfNetwork
R1(config)#snmp-server host 192.168.163.130 EyesOfNetwork
R1(config)#end

```

Figure 15 : Configuration snmp routeur

1.3.3 Ajout des commandes

Pour ajouter des commandes à notre serveur de supervision, il faut sélectionner le menu Administration, puis Configuration Nagios et finalement Nagios Commands.

The screenshot shows the Eonweb Configurator interface. On the left, there's a sidebar with navigation links: Tableaux de bord, Disponibilités, Capacité, Production, Rapports, Administration (selected), Configuration Nagios, and Applications. The main content area is titled "Eonweb Configurator" and shows a grid of configuration items. Under the "Administration" section, there are several categories: Nagios Daemon Configuration, Nagios Web Interface Configuration, Nagios Resources, Nagios Commands, Time Periods, Contacts, Contact Groups, Host Groups, Service Groups, and Host Groups. Each item has a brief description and a small icon. At the top right, there are links for Paramètres, Equipements, Modèles, and a search bar labeled "Search".

Figure 16 : configuration web d'Eon

Cliquer sur **Add A New Command**, puis remplir les différents champs :

- Command Name (nom de la commande),
- Command Line (la commande exécuté),
- Command Description (pour commenter la commande).

Puis cliquer sur **Create Command**.

The screenshot shows the "Nagios Command Editor" page. It has a similar header and sidebar as Figure 16. The main form contains three input fields: "Command Name" with the value "check_nt-nsclient_ram", "Command Line" with the value "\$USER1\$/check_nt -H SHOSTADDRESS\$ -p 12489 -s pass -v MEMUSE -w SARG1\$ -c \$ARG2\$", and "Command Description" with the value "Regarde le pourcentage d'utilisation de la RAM passe à Warning ARG1 et Critical ARG2". Below the form are two buttons: "Create Command" (highlighted in blue) and "Cancel".

Figure 17 : éditeur de commandes

Nous allons refaire la même procédure pour toutes les nouvelles commandes à ajouter d'autres commandes avec d'autres plugins seront configurées et citées dans l'**Annexe A**.

1.3.4 Ajout des hôtes à superviser

Nous allons ajouter les différents hôtes et équipements qui vont être supervisés. Donc on se rendre dans Administration puis Configurations Nagios puis dans Equipements et Lister

Host Browser

The screenshot shows the Nagios Host Browser interface. At the top, there is a green button labeled "Add A New Child Host". Below it, a toolbar with buttons for "Object to Add" (set to "HostGroup"), "Do it!", "Actions", "Delete", and "Submit". The main area displays a table of hosts:

Host Name	Address	Description
localhost	127.0.0.1	EyesOfNetwork Network Server
pc-ubuntu	192.168.162.100	pc-ubuntu
PC-windows	172.16.10.100	PC-windows

Figure 18: liste des équipements

Remplir les champs suivants :

- Host Name (nom de l'équipement),
- Host Description (description de l'équipement),
- Address (adresse IP de l'équipement),

Et enfin lui attribuer un Template la plus adaptée

Add New Host

The screenshot shows the "Add New Host" configuration form. It includes fields for Host Name (set to "windows"), Host Description (set to "PC-windows"), Address (set to "172.16.10.100"), Display Name (Optional) (set to "windows"), and a section for Host Templates To Inherit From (Top to Bottom). At the bottom, there is a dropdown for "Add Template To Inherit From" set to "GENERIC_HOST" and buttons for "Add Host" and "Cancel".

Figure 19 : ajout d'un hôte

Pour ajouter l'hôte dans un groupe, il faut retourner sur la page où tous les équipements sont listés dans Administration, Equipements et Lister.

Puis nous devons sélectionner les équipements souhaités pour les mettre dans le groupe. En choisissant les options dans Object to Add il faut laisser HostGroup puis mettre le nom du groupe dans le champ libre, et de Do It

Voilà le ou les équipements sont ajoutés au groupe.

Host Status Details For All Host Groups

select host with leftclick to send multiple commands. Select multiple with shift + mouse.
select all - unselect all - all problems - all with downtime

Host	Status	Last Check	Duration	Status Information
PC-windows	UP	16:05:44	0d 0h 41m 39s	PING OK - Paquets perdus = 0%, RTA = 18.72 ms
localhost	UP	16:04:18	12d 8h 16m 42s	PING OK - Paquets perdus = 0%, RTA = 0.04 ms
pc-ubuntu	UP	16:08:35	0d 0h 42m 15s	PING OK - Paquets perdus = 0%, RTA = 26.48 ms

select all - unselect all - all problems - all with downtime
3 of 3 Matching Host Entries Displayed

Figure 20 : Etat des hôtes

Current Network Status

Last Updated: Sat Apr 18 11:57:29 CEST 2020
Updated every 90 seconds
Thruk 2.20-2 - www.thruk.org
Logged in as admin

Host Status Totals

Up	Down	Unreachable	Pending
3	0	0	0

All Problems | **All Types**

0	3
---	---

Service Status Totals

OK	Warning	Unknown	Critical	Pending
19	0	0	2	0

All Problems | **All Types**

2	21
---	----

Service Status Details For All Host

Select hosts / services with leftclick to send multiple commands. Select multiple with shift + mouse.
select all (hosts) - unselect all - all problems - all with downtime

Host	Service	Status	Last Check	Duration	Attempt	Status Information
PC-windows	interfaces	OK	11:57:28	0d 0h 38m 1s	1/4	OK: Bluetooth Device (RFCOMM Protocol TDI)\notPresent Intel(R) PRO/1000 MT Network Connection #2\down Bluetooth Device (Personal Area Network)\down Intel(R) PRO/1000 MT Network Connection\up
	memory	OK	11:54:04	0d 0h 35m 27s	1/4	Physical Memory: 24%used(494MB/2047MB) Virtual Memory: 12%used(510MB/4095MB) (<80%) : OK
	partitions	OK	11:54:38	0d 0h 38m 63s	1/4	All selected storages (<90%) : OK
	processor	OK	11:55:11	0d 0h 38m 18s	1/4	1 CPU, load 0.0% < 80% : OK
	systme	CRITICAL	11:55:45	0d 0h 37m 44s	4/4#7	CRITICAL - System time is off by 3593 sec (04-18-2020, 10:55:52).
localhost	uptime	OK	11:58:19	0d 0h 26m 10s	1/4	OK: Hardware: Intel64 Family - up 38 minutes
	interfaces	OK	11:58:54	12d 4h 51m 50s	1/4	OK: ens33\up\ens37\down
	memory	OK	11:53:43	12d 4h 51m 31s	1/4	Ram : 40%, Swap : 0% : OK
	mysql	OK	11:54:14	12d 4h 51m 4s	1/4	Uptime: 3892 Threads: 2 Questions: 10235 Slow queries: 0 Opens: 138 Flush tables: 2 Open tables: 149 Queries per second avg: 2.629
	partitions	OK	11:54:48	11d 3h 18m 23s	1/4	All selected storages (<90%) : OK
pc-ubuntu	process_ged	OK	11:55:22	3d 1h 39m 22s	1/4	1 process named ged (> 0)
	processor	OK	11:55:58	12d 2h 42m 28s	1/4	CPU used 7.0%(<80%) : OK
	ssh	OK	11:58:31	10d 7h 38m 58s	1/4	SSH OK - OpenSSH_7.4 (protocol 2.0)
	systme	OK	11:55:58	12d 2h 41m 33s	1/4	System Time OK - 04-18-2020, 11:55:58
	uptime	OK	11:53:52	0d 0h 57m 41s	1/4	OK: Linux localhost.localdomain 3.10.0-382.3.2.el7.x86_64 - up 1 hours 5 minutes

Figure 21 : Etats des hôtes et services supervisés

1.3.5 Crédation graphique avec cacti

Afin de bien modéliser le concept de supervision de nos équipements nous avons eu recourt à la schématisation de ces états sous forme de graphes personnalisés et adaptés aux besoins de l'administrateur.

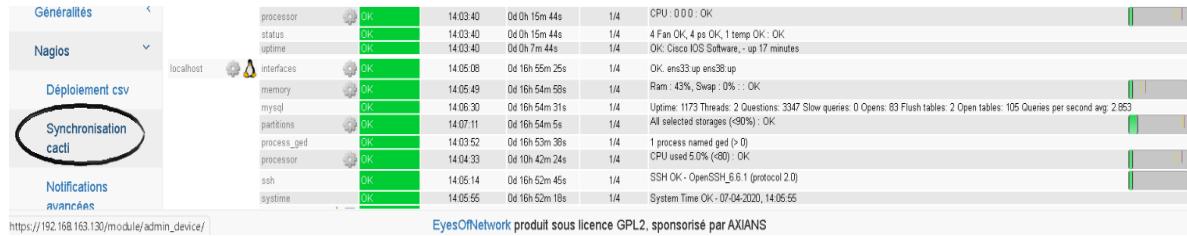


Figure 22 : Menu Cacti

Nous allons donc utiliser cacti pour la création de ces graphes

Nous devons tout d'abord faire la synchronisation avec cacti en sélectionnant le menu administration > Nagios > Synchronisation cacti dans le menu d'Eyes Of Network à gauche

Une nouvelle page s'affiche qui nous indique de choisir les paramètres d'imports ainsi que les hôtes Nagios à importer.

Nous devons cliquer sur le nom de l'hôte dans la liste affichée puis sur importer.

Figure 23 : Importation des hôtes

Nous avons importé tous les hôtes supervisés.

Après avoir importé les hôtes nécessaires, nous accédons à l'interface graphique de Cacti en sélectionnant le menu administration > liens externes > Cacti dans le menu d'EON à gauche.

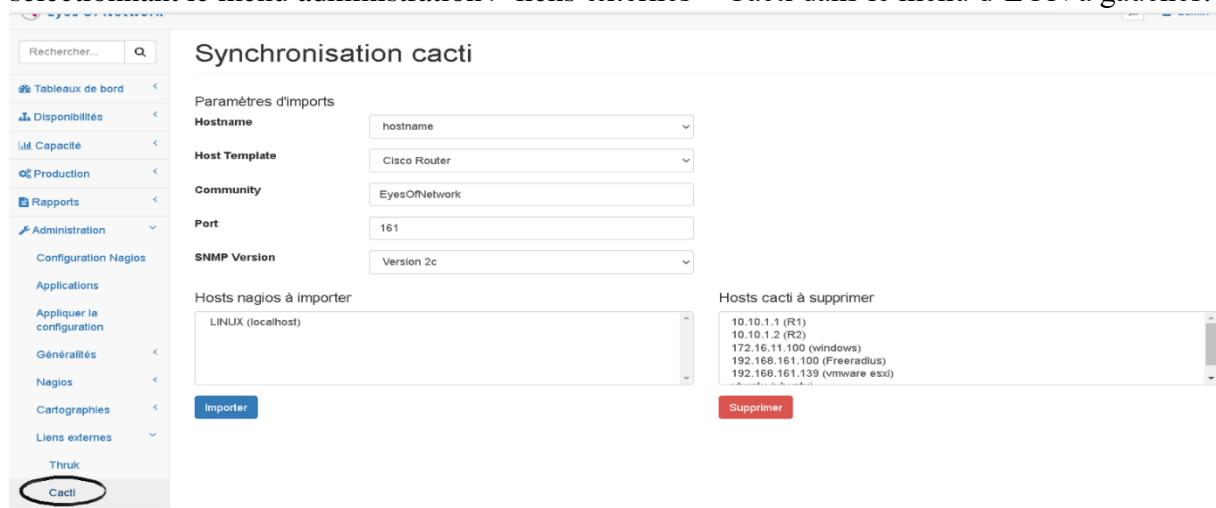


Figure 24 : Interface Cacti

Une nouvelle fenêtre s'ouvre, il s'agit de la page d'accueil de Cacti comme le montre la figure ci-dessous.



Figure 25 : Tableau de bord Cacti

Pour voir la liste des équipements importés précédemment, nous devons sélectionner **Devices** dans le menu à gauche .

Description**	ID	Graphs	Data Sources	Status	In State	Hostname	Current (ms)	Average (ms)	Availability	
Freeradius	5	0	0	Up	-	192.168.161.100	158.71	158.71	100	<input checked="" type="checkbox"/>
R1	3	0	0	Up	-	10.10.1.1	53.44	53.44	100	<input checked="" type="checkbox"/>
R2	4	0	0	Up	-	10.10.1.2	159.15	159.15	100	<input checked="" type="checkbox"/>
ubuntu	7	0	0	Up	-	ubuntu	131.65	131.65	100	<input checked="" type="checkbox"/>
vmware esxi	6	0	0	Up	-	192.168.161.139	158.2	158.2	100	<input checked="" type="checkbox"/>
windows	8	0	0	Up	-	172.16.11.100	131.46	131.46	100	<input type="checkbox"/>

Figure 26 : Liste des équipements importés

Comme le montre la figure ci-dessus les équipements sont importés avec succès, à partir de la liste ci-dessus nous pouvons savoir le nombre de graphes de chaque équipement, son statut (Up / Down / Unknown), le nom d'hôte qui peut être défini par son adresse IP, sa disponibilité et sa connectivité.

Pour créer un nouveau graphe nous devons sélectionner **New Graphs** dans le menu à gauche. Une nouvelle page apparaît qui nous indique de choisir l'hôte concerné, le type de graphe ainsi son modèle.

Dans notre cas nous avons choisi de commencer avec le serveur Freeradius avec un type de graphe en bits et le modèle **Linux-Memory Usage**.

Index	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address	
1	Netware - File System Activity	lo	softwareLoopback(24)	1000000	10		127.0.0.1	<input type="checkbox"/>
2	Netware - File System Cache	ether Controller	ethernetCsmacd(6)	4294967295	10000	00:0C:29:2A:2F:D8	192.168.161.100	<input type="checkbox"/>
3	Netware - Logged In Users	ether Controller	ethernetCsmacd(6)	4294967295	10000	00:0C:29:2A:2F:E5		<input type="checkbox"/>
	SNMP - Generic OID Template							
	ucdnet - CPU Usage							

Figure 27 : Crédit d'un nouveau graphe.

Si nous voulons créer des graphiques à partir d'une requête de données, il est indispensable de sélectionner l'interface pour laquelle nous souhaitons créer un graphique.

Ça nous permet de visionner le trafic généré au niveau des interfaces des hôtes supervisés.

Après avoir choisi les informations nécessaires, nous cliquons sur **Create** en bas de la page à droite.

The screenshot shows the 'New Graphs for [Freeradius (192.168.161.100) Cisco Router]' interface. At the top, there are fields for 'Host' (Freeradius (192.168.161.100)), 'Graph Types' (All), and buttons for 'Go' and 'Clear'. To the right are links for '*Edit this Host' and '*Create New Host'. Below this is a 'Graph Templates' section with a dropdown menu set to 'Create: Cisco - CPU Usage' and another dropdown set to 'Create: Linux - Memory Usage'. The main area is titled 'Data Query [SNMP - Interface Statistics]' and shows a table of network interfaces:

Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address
1	Up	lo	lo		softwareLoopback(24)	10000000	10		127.0.0.1
2	Up	VMware VMXNET3 Ethernet Controller	ens160		ethernetCsmacd(6)	4294967295	10000	00:0C:29:2A:2F:D8	192.168.161.100
3	Up	VMware VMXNET3 Ethernet Controller	ens192		ethernetCsmacd(6)	4294967295	10000	00:0C:29:2A:2F:E5	

At the bottom right, there is a 'Select a graph type:' dropdown set to 'In/Out Bits', a 'Cancel' button, and a 'Create' button, which is highlighted with a red box.

Figure 28 : Validation des choix de la création de graphe

Une nouvelle page s'affiche qui nous indique que les graphes ont été créés avec succès.

The screenshot shows the same interface as Figure 28, but now with a success message at the top: 'Created graph: Freeradius - Memory Usage' and 'Created graph: Freeradius - Traffic - ens160'. The 'Create' button at the bottom right is highlighted with a red box.

Figure 29 : Crédit des graphes avec succès

Pour voir la liste des graphes de chaque hôte nous devons sélectionner **Devices** dans le menu à gauche qui permet de visualiser la liste des hôtes importés précédemment, sélectionner l'hôte concerné, une nouvelle page s'ouvre qui contient des informations sur l'hôte (son adresse, son modèle etc.) puis sélectionner **Graph List** à droite en haut de la page.

Freeradius (192.168.161.100)

SNMP Information

System: Linux freeradius-virtual-machine 5.3.0-28-generic #30~18.04.1~Ubuntu~bionic

Uptime: 48d18 (0 days, 0 hours, 6 minutes)

Hostname: freeradius-virtual-machine

Location: sitting on the back of the Bay

Contact: nc.megaparle.org

Device (edit: Freeradius)

General Host Options

Description: Give this host a meaningful description.

Hostname: 192.168.161.100

Host Template: Cisco Router

Number of Collection Threads: 1 Thread (default)

Disable Host:

Availability/Reachability Options

Default Device Detection: SNMP Uptime

Ping Timeout Value: 400

Ping Retry Count: 1

SNMP Options

SNMP Version: Version 2

SNMP Community: EyesONNetwork

SNMP Port: 161

SNMP Timeout: 1000

Maximum OID's Per Get Request: 10

Figure 30 : Accès à la liste des graphes.

Graph Management

Host: Freeradius (192.168.161.100) Template: Any Go Clear

Search: Rows per Page: 30

Showing All Rows			
Graph Title**	ID	Template Name	Size
Freeradius - Memory Usage	5	Linux - Memory Usage	120x500
Freeradius - Traffic - ens160	6	Interface - Traffic (bits/sec)	120x500

Choose an action:

Figure 31 : Liste des graphes créés

Une nouvelle page s'affiche qui contient une liste des graphes de cet hôte, les graphes créés précédemment ont été ajoutées à la liste avec succès. Nous pouvons sélectionner le titre du graphe pour le voir.

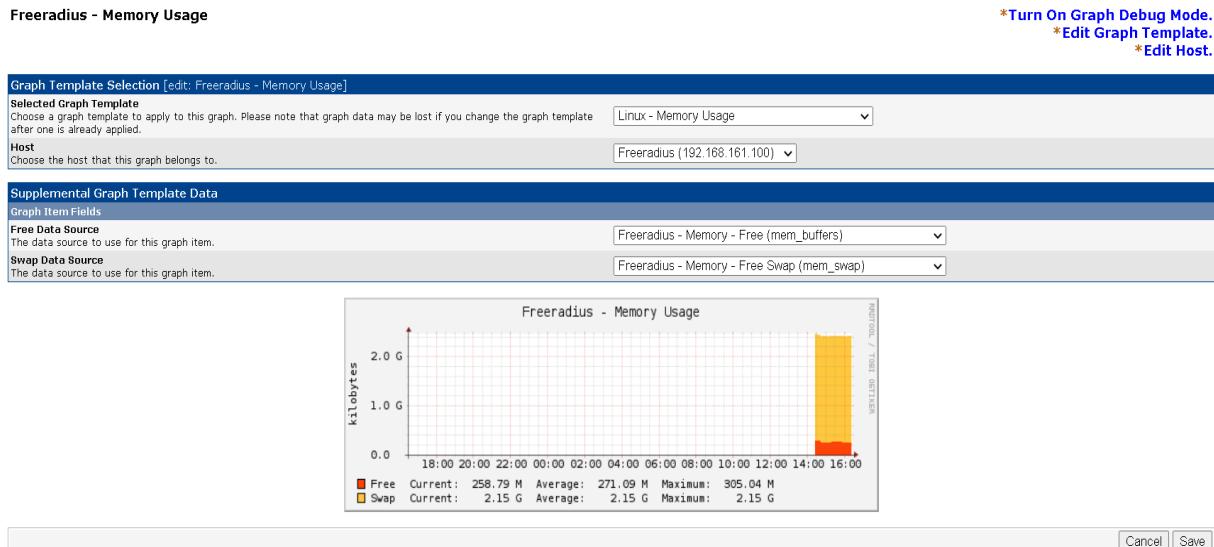


Figure 32 : Graphe Memory Usage du serveur Freeradius en cours de création

Nous remarquons que le graphe est en cours de création.

Nous avons répété les mêmes étapes citées précédemment pour créer d'autres graphes dédiés aux autres machines supervisées.

Il est indispensable de créer une arborescence de graphe afin d'ajouter les graphes créés précédemment.

Pour créer cette arborescence, nous devons cliquer sur **Graph Trees** dans le menu de Cacti à gauche puis sur **Add** en haut à droite.

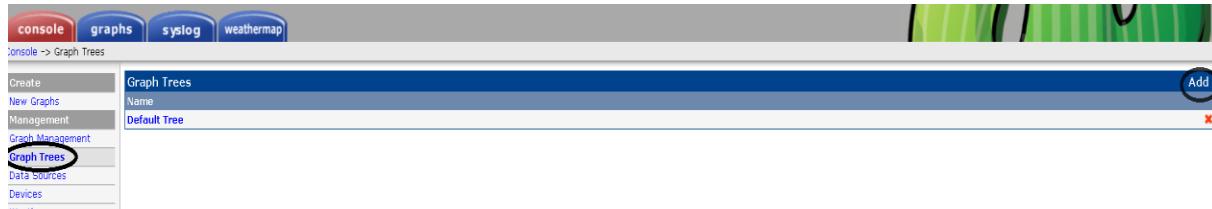


Figure 33 : Accès à l'arborescence des graphes

Et pour finir, il faut choisir le nom de l'arborescence de graphe et choisir le type de tri correspondant puis cliquer sur **Create** pour valider.

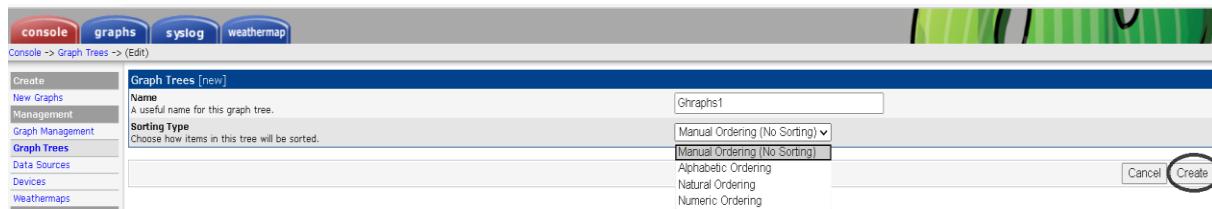


Figure 34 : Crédit d'une nouvelle arborescence des graphes

Pour commencer à ajouter des éléments à notre arborescence, nous devons cliquer sur **Add**.

The screenshot shows the 'Graph Trees [edit: Graph1]' configuration page. At the top, there are fields for 'Name' (set to 'Graph1') and 'Sorting Type' (set to 'Manual Ordering (No Sorting)'). Below these are sections for 'Tree Items' and 'Value'. A large 'Add' button is visible at the top right of the main content area.

Figure 35 : Ajout d'un nouveau graphe à l'arborescence

La page suivante nous indique de choisir le type de l'arborescence, dans notre cas nous avons choisi le graphe que nous souhaitons ajouter.

Et pour valider nos choix, nous devons cliquer sur **Create**.

The screenshot shows a 'Create' dialog box. It has fields for 'Parent Item' (set to 'root'), 'Tree Item Type' (set to 'Graph'), and 'Tree Item Value' (a dropdown menu showing 'Freeradius - Memory Usage', 'Freeradius - Traffic - ens160', 'R1 - CPU Usage', 'R1 - Traffic - Fa0/0', 'R1 - Traffic - Fa0/0.10', 'R1 - Traffic - Fa0/0.20', and 'R1 - Traffic - Se0/0'). At the bottom right, there are 'Cancel' and 'Create' buttons, with 'Create' being circled.

Figure 36 : Validation des choix du type d'arborescence et du graphe

Nous avons répété le même processus pour ajouter nos graphes créés.

La figure ci-dessous nous montre la liste des graphes qui font partie de notre l'arborescence créé précédemment.

The screenshot shows the 'Graph Trees [edit: Graph1]' configuration page again. It displays a table of 'Tree Items' and 'Value' pairs. The items listed are 'Freeradius - Memory Usage', 'Freeradius - Traffic - ens160', 'R1 - CPU Usage', 'R1 - Traffic - Fa0/0', 'R1 - Traffic - Fa0/0.10', 'R1 - Traffic - Fa0/0.20', 'R1 - Traffic - Se0/0', and 'R1 - Traffic - Fa0/0.30'. Each item is associated with a 'Graph' value. At the bottom right, there are 'Return' and 'Save' buttons.

Figure 37 : Liste des graphes ajoutés à l'arborescence.

1.3.6 Génération des rapports

Grâce à EYES OF NETWORK nous avons aussi la possibilité de générer des rapports afin faire l'évaluation de la disponibilité de nos applications et connaître la qualité de nos services

Nous allons donc faire la représentation de ces rapports afin de faire un résumé de l'état de nos équipements supervisés.

- **Rapport Tendances**

Le rapport disponibilité / tendance, permet d'avoir la disponibilité d'un hôte ou service durant une période donnée. L'exemple présenté par la figure ci-dessous, c'est la vue de disponibilité du serveur Freeradius.

Pour générer ce rapport, il faut cliquer sur **Rapports > Disponibilités > Tendances**



Figure 38 : Schéma d'accès au rapport tendances.

Pour créer ce rapport il est indispensable de passer par 3 étapes :

La sélection du type de rapport (un service ou un hôte)

Step 1: Select Report Type

Type:

Figure 39 : Choix du type d'hôte

Choisir un hôte parmi les hôtes supervisés

Step 2: Select Host

Host: Freeradius ▾

[Continue to Step 3](#)

Figure 40 : Choix de l'hôte

Et la dernière étape c'est le choix de la période souhaité, la date de début, la date de fin etc.

Step 3: Select Report Options

Report period: Last 24 Hours ▾

If Custom Report Period...

Start Date (Inclusive): July 03 2020

End Date (Inclusive): July 04 2020

Report time Period: None ▾

Assume Initial States: Yes ▾

Assume State Retention: Yes ▾

Assume States During Program Downtime: Yes ▾

Include Soft States: No ▾

First Assumed Service State: Unspecified ▾

Backtracked Archives (To Scan For Initial States): 4

Suppress image map:

[Create Report](#)

Figure 41 : Options du rapport

Et pour valider nos choix nous devons cliquer sur **Create Report**

La figure ci-dessous nous montre le résultat du rapport obtenu qui a été créé avec succès.

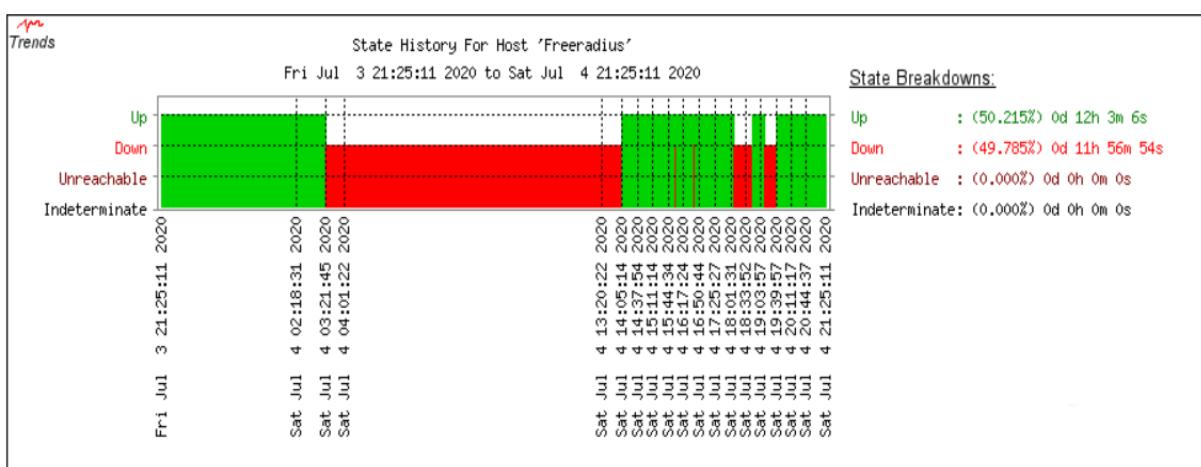


Figure 42 : Rapport tendances du serveur Freeradius

- **Rapport SLA technique**

Pour la génération d'un rapport SLA technique, nous devons cliquer sur **Rapports > évènements > SLA techniques** dans le menu d'EON à gauche.

Une nouvelle page s'affiche qui nous indique de spécifier la période (une journée, une semaine, un mois etc.) de choisir sur quel type d'élément nous souhaitons générer un rapport (sur les hôtes, les services etc.) et de faire une recherche sur cet élément et pour valider nous cliquons sur **Rechercher**.

Figure 43 : Choix de la création du rapport SLA technique



Figure 44 : Rapport SLA du serveur Freeradius

Le rapport d'évènement SLA technique nous a permis de résumer le temps moyen de résolution de panne datant d'une période donnée. L'exemple de la figure ci-dessus montre la vue de notre serveur Freeradius datant d'une journée.

• Rapport performances

Ce rapport mesure la capacité, permet d'afficher les graphes de Cacti créés sur durant une période donnée.

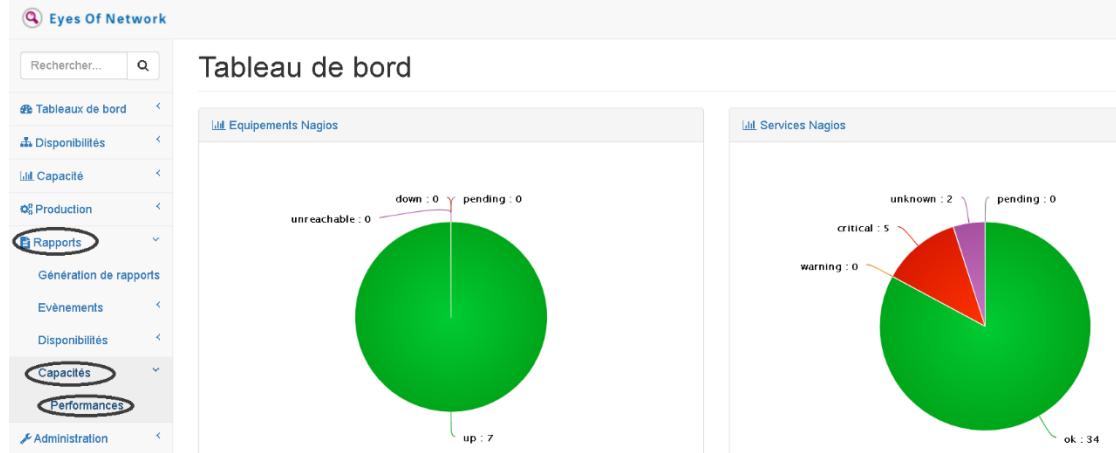


Figure 45 : Schéma d'accès au ‘performances’

Pour créer ce rapport il faut cliquer sur **Rapports > Capacités > Performances** à gauche dans le menu d'EON.

Nous devons par la suite choisir une période et spécifier le titre du graphe (dans notre cas nous avons choisi l'hôte freeradius et le trafic comme titre).

Les figures ci-dessous nous montrent les résultats obtenus.

Rapport de capacités

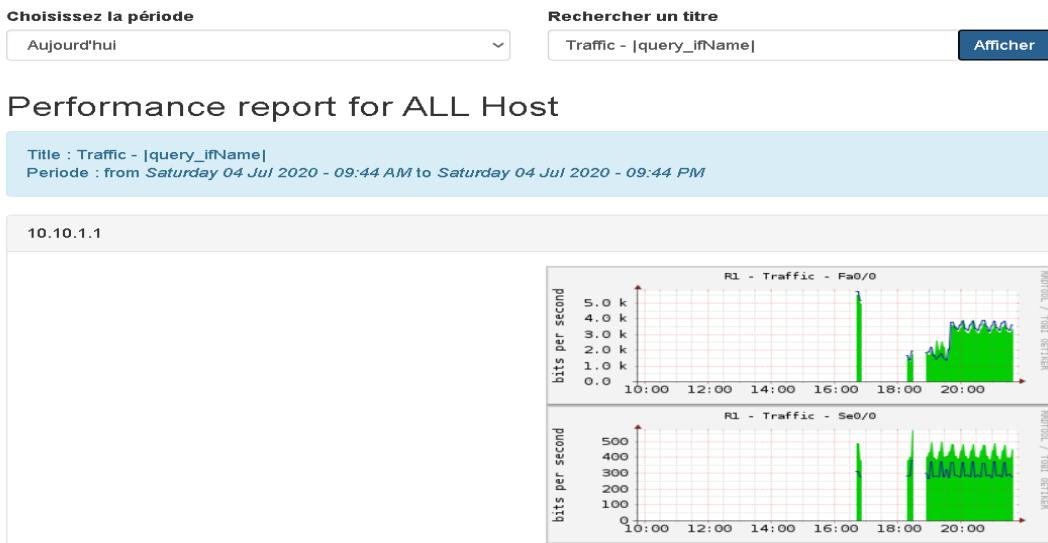


Figure 46 : Rapport performances du serveur Freeradius

1.3.7 Notifications par mail

Pour recevoir des notifications par email nous devons spécifier l'adresse mail de l'administrateur au niveau de la liste des contacts du serveur EON puis enregistrer la configuration effectuée en redémarrant Nagios.

Suite à cette configuration, nous devons voir les messages apparaître lorsque nous saisissons la commande mail au niveau de la ligne de commande de EON comme le montre la figure ci-dessous.

```
[root@localhost ~]# mail
Heirloom Mail version 12.5 7/5/10. Type ? for help.
"/var/spool/mail/root": 19 messages 19 new
>N 1 Anacron      Thu Jul  2 00:25 18/1143 "Anacron job 'cron.daily' on localhost.loc"
>N 2 Anacron      Sat Jul  4 14:43 18/1143 "Anacron job 'cron.daily' on localhost.loc"
>N 3 nagios       Sat Jul  4 17:19 26/827 "Host UP alert for Freeradius!"
>N 4 nagios       Sat Jul  4 17:19 32/932 "Services UNKNOWN alert for Freeradius/pro"
>N 5 nagios       Sat Jul  4 17:20 31/896 "Services UNKNOWN alert for Freeradius/sys"
>N 6 nagios       Sat Jul  4 17:21 31/879 "Services CRITICAL alert for Freeradius/up"
>N 7 nagios       Sat Jul  4 17:21 31/887 "Services CRITICAL alert for Freeradius/in"
>N 8 Mail Delivery System Sat Jul  4 17:22 86/3039 "Undelivered Mail Returned to Sender"
>N 9 nagios       Sat Jul  4 17:22 31/914 "Services UNKNOWN alert for Freeradius/mem"
>N 10 Mail Delivery System Sat Jul  4 17:22 81/3025 "Undelivered Mail Returned to Sender"
>N 11 nagios      Sat Jul  4 17:28 26/789 "Host DOWN alert for R1!"
>N 12 nagios      Sat Jul  4 17:29 26/789 "Host DOWN alert for R2!"
>N 13 Anacron     Sun Jul  5 12:35 18/1143 "Anacron job 'cron.daily' on localhost.loc"
>N 14 Anacron     Mon Jul  6 14:24 18/1143 "Anacron job 'cron.daily' on localhost.loc"
>N 15 Anacron     Tue Jul  7 11:48 18/1143 "Anacron job 'cron.daily' on localhost.loc"
>N 16 Anacron     Wed Jul  8 10:43 18/1145 "Anacron job 'cron.daily' on localhost.loc"
>N 17 Anacron     Thu Jul  9 13:30 18/1145 "Anacron job 'cron.daily' on localhost.loc"
>N 18 Anacron     Sat Jul 11 15:49 18/1145 "Anacron job 'cron.daily' on localhost.loc"
>N 19 Anacron     Sun Jul 12 14:17 18/1145 "Anacron job 'cron.daily' on localhost.loc"
&
```

Figure 47 : notifications par mail

1.4 Revue de sprint

Pendant ce sprint, nous avons réussi à terminer toutes les user stories et leurs tâches planifiées.

La réunion de validation du sprint 1 s'est tenu à distance le 16/05/2020 à 10h.

En présence de :

Product owner: Mme Ben hamza Dhouha ;

Scrum team: Farhat Hiba et El Ghoul Essia

Les fonctionnalités de Sprint 1:

Fonctionnalités	Validation
mise en place de l'outil de supervision : <ul style="list-style-type: none">✓ Installation et configuration de l'agent de protocole simple de gestion de réseau (SNMP).✓ Ajout des hôtes à superviser au niveau de la solution de supervision.✓ Génération rapports et statistiques.	OUI

1.5 Rétrospectives

Au niveau de ce sprint nous avons rencontré un problème au niveau de la supervision des machines, nous l'avons résolu en ajoutant des adaptateurs réseau avec les adresses réseau des machines et du serveur au niveau de l'éditeur de réseau virtuel de VMware Workstation.

Nous avons rencontré des problèmes au niveau de la connectivité des machines virtuelles celle-ci a été résolu avec la création des vlans.

1.6 Burndown chart

Le burndown chart est un graphique qui reflète l'avancement de notre travail.

Il est formé de deux axes :

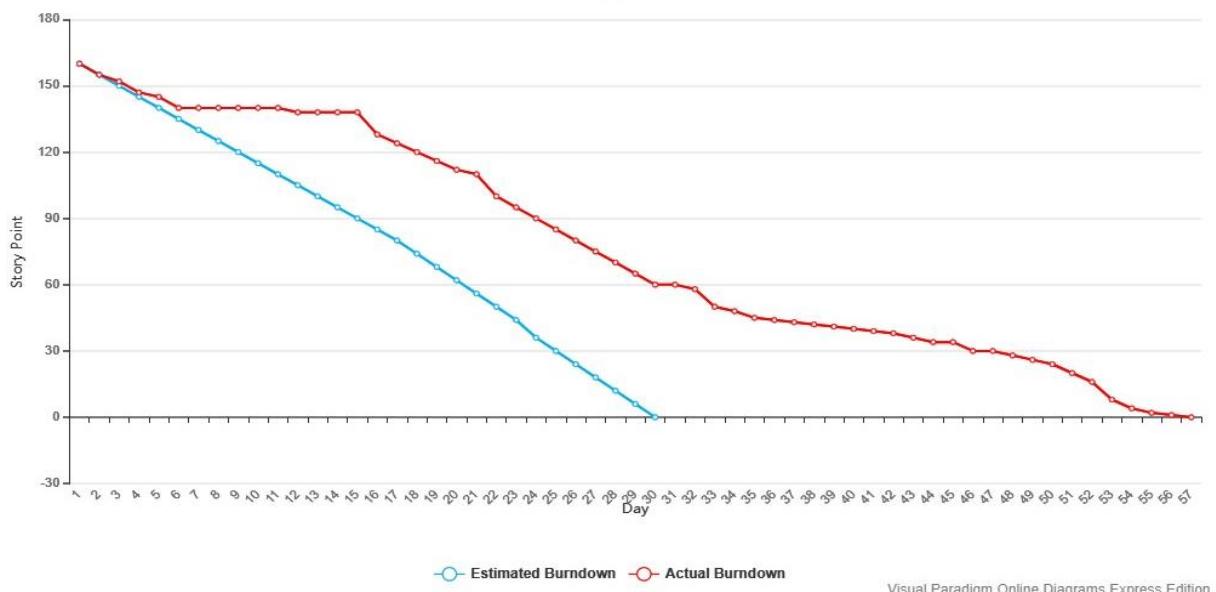


Figure 48: Burndown chart sprint 1

Visual Paradigm Online Diagrams Express Edition

- L'axe vertical indique la charge totale du sprint (La vélocité),
- L'axe horizontal représente les jours de du sprint.

Au niveau de la courbe, nous remarquons un avancement pendant la première semaine après avec l'arrêt de stage il y a eu un retard pendant quelques jours.

Conclusion

Au cours de ce sprint, nous avons implémenté un ensemble d'outils de supervision offert par Eyes-of-network permettant à l'administrateur de gérer les équipements réseaux l'état d'interface et l'état d'application.

Ainsi, nous avons essayé au maximum d'enrichir cette partie de monitoring, par des outils supplémentaires offerts par EON qui fournissent une importance robuste à notre solution de supervision, tel que la gestion des rapports et la gestion des notifications.

Chapitre 5 : Sprint 2 Implémentation d'une connexion VPN et serveur d'authentification

Introduction

Après avoir mis en place notre solution de supervision Eyes of network, nous passons maintenant à la mise en place du serveur d'authentification et un accès sécurisé. L'objectif est d'assurer un accès aux données de réseau sécurisée et mobile tout en assurant la confidentialité, l'intégrité et l'authenticité.

1. Spécification fonctionnelle

1.1 Le Backlog du sprint

Tableau 11 : backlog de sprint 2

ID	User story	Tâche	Estimation (h)
AAAA	En tant qu'un administrateur je vais mettre en place d'un réseau privé virtuel	Configuration du routeur avec le contrôle d'accès	72
		Mise en place de Cisco VPN client	1
BBBB	En tant qu'un administrateur je vais configuration de l'AAA	installation et configuration de serveur Freeradius	90
		Installation daloradius	3
		Configuration des utilisateurs	0.5
		Configuration NAS	0.5

1.2 Diagramme de cas d'utilisation « Authentification »

Avant d'effectuer toute action, les utilisateurs du système doivent tout d'abord s'authentifier en saisissant leur login et leur mot de passe.

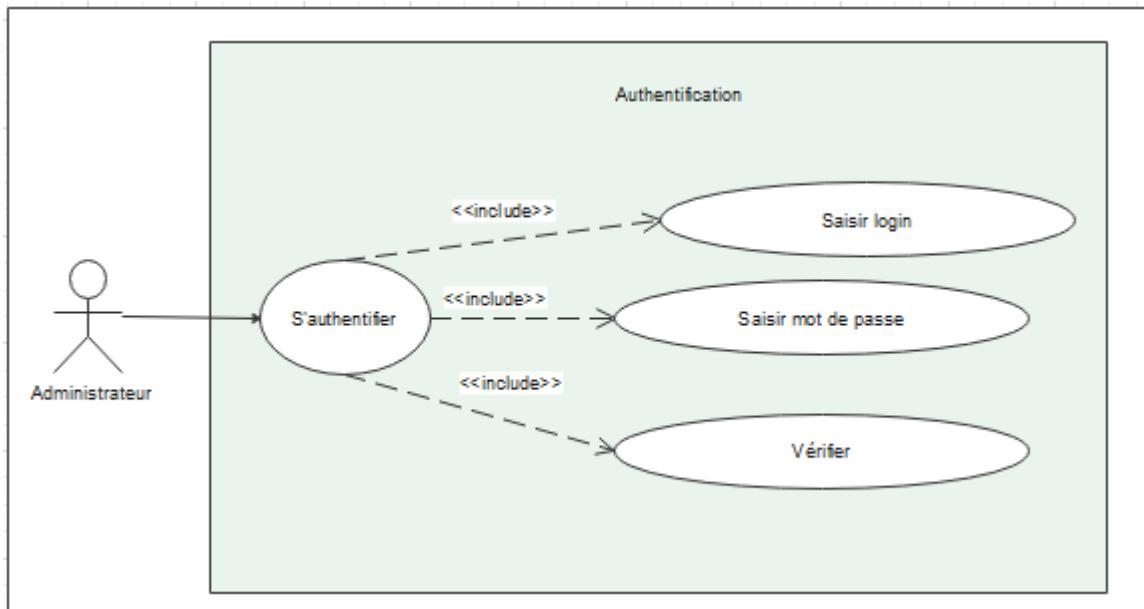


Figure 49 : Diagramme de cas d'utilisation « Authentification »

Titre : Authentification

Objectif: se connecter au système.

Acteurs: Administrateur.

Précondition: Serveur disponible

Scénario nominal

- L'administrateur demande à s'authentifier.
- L'administrateur fournit son login et son mot de passe.
- L'administrateur est authentifié et à la main d'y accéder.

Finis : quand L'utilisateur termine la session et se déconnecte

Enchaînement d'exception

Un message d'erreur sera affiché si le login et/ou le mot de passe sont incorrects, Serveur introuvable ou bien compte utilisateur bloqué

Post-condition

L'administrateur peut accéder aux différentes fonctionnalités du système.

2. Réalisation

Ce sprint va permettre la réalisation d'un accès crypté, authentifié et mobile des administrateurs aux services de réseau pour ce faire on va :

- Installer et configurer FreeRADIUS
- Créer un vpn "site to site" entre les routeurs R1 et R2

2.1 Mise en place d'un réseau privé virtuel :

2.1.1 Configuration du routeur

Pour configurer un réseau privé virtuel, nous devons tout d'abord spécification de l'identificateur de groupe de Diffie-Hellman, que les deux paires IPsec utilisent pour calculer un secret partagé sans le transmettre à l'autre.

Chaque stratégie est identifiée par un numéro de priorité.

Par la suite, il faut spécifier l'algorithme de cryptage à utiliser avec la commande de encryption 3des afin d'assurer la confidentialité des données ainsi que l'algorithme de hachage avec la commande hash SHA

Puis configurer le type d'authentification par clé pré-partagé avec la commande authentication pre-share et nous définissons le groupe Diffie-Hellman à utiliser, dans notre cas nous utilisons le groupe 2 utilisant 1024 bits

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
```

Figure 50 : Configuration VPN du routeur

Nous avons défini un ensemble de transformations IPSec afin d'indiquer comment protéger le trafic avec la spécification des algorithmes utilisés pour les protocoles AH et ESP et le mode (tunnel ou transport) nous avons utilisé la commande :

```
R1(config)#crypto ipsec transform-set transfr esp-3des esp-sha-hmac
```

Figure 51 : configuration mode tunnel et algorithmes

```
(crypto ipsec transform-set <transform-set-name> < transform1> [< transform2>][<transform3>])
```

Dans notre cas nous avons utilisé :

- Le mode tunnel qui est par défaut ,
- esp-3des : l'algorithme de chiffrement triple DES pour le protocole ESP,
- esp-sha-hmac : l'algorithme d'authentification SHA-HMAC pour le protocole ESP.

Maintenant il faut configurer la méthode de l'authentification des utilisateurs, nous avons choisi le mode local afin d'utiliser la base de données locale du routeur.

Une fois qu'un utilisateur est authentifié, nous pouvons définir des paramètres qui limitent l'accès de l'utilisateur sur le réseau à l'aide de la commande aaa authorization.

Les commandes d'autorisation ont le même aspect que la commande d'authentification :

Dans notre cas nous avons utilisé la commande aaa authorization network groups local qui permet de démarrer l'autorisation pour tous les services liés au réseau tels que le protocole Internet en ligne de série (SLIP) et le protocole point à point (PPP) en utilisant la base de données locale .

```
R1(config)#aaa new-model  
R1(config)#aaa authentication login users local  
R1(config)#aaa authorization network groups local
```

Figure 52: Configuration model aaa

Passons à définir un pool d'adresses IP, autoriser un trafic IP venant d'un réseau spécifique et la définition d'un groupe de stratégies avec un mot de passe

```
R1(config-isakmp-group)#ip local pool vpnpool 192.168.100.32 192.168.100.63  
R1(config)#access-list 101 permit ip 192.168.161.0 0.0.0.255 any  
R1(config)#access-list 101 permit ip 192.168.162.0 0.0.0.255 any  
R1(config)#access-list 101 permit ip 192.168.163.0 0.0.0.255 any  
R1(config)#crypto isakmp client configuration group globalnet  
R1(config-isakmp-group)#key cisco  
R1(config-isakmp-group)#pool vpnpool  
R1(config-isakmp-group)#acl 101  
R1(config-isakmp-group)#exit
```

Figure 53 : Configuration pool d'adresses et autorisation de trafic

Après la définition de pool d'adresses et le groupe de stratégies nous allons configurer une carte de chiffrement dynamique nommé d-map avec le numéro de séquence 1 afin d'indiquer quel transform-set à utiliser.

```
R1(config)#crypto dynamic-map dmap 1  
R1(config-crypto-map)#set transform-set transfr  
R1(config-crypto-map)#reverse-route  
R1(config-crypto-map)#exit
```

Figure 54 : Configuration de carte de chiffrement.

Ensuite nous avons fait la liaison entre la carte de chiffrement dynamique et la carte crypto statique et configurer le routeur pour répondre aux demandes de configuration de mode des clients distants.

```
R1(config)#crypto map pfe 1 ipsec-isakmp dynamic dmap  
R1(config)#crypto map pfe client configuration address respond  
R1(config)#crypto map pfe isakmp authorization list groups  
R1(config)#crypto map pfe client authentication list users
```

Figure 55 : liaison entre carte dynamique et carte statique.

Maintenant il nous reste que la définition d'un compte utilisateur avec un login et un mot de passe et appliquer la carte cryptographique précédemment définie sur une interface en utilisant la commande crypto map en mode configuration de l'interface.

```
R1(config)#username test password test  
R1(config)#int s0/0  
R1(config-if)#crypto map pfe  
R1(config-if)#  
*Mar 1 01:12:47.555: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON  
R1(config-if)#end
```

Figure 56 : Lier la carte à une interface.

Après avoir terminé la configuration nécessaire de notre routeur nous pouvons taper la commande ci-dessous pour afficher les associations de sécurité ISAKMP

```
R1#sh crypto isakmp sa  
IPv4 Crypto ISAKMP SA  
dst             src             state             conn-id slot status  
  
IPv6 Crypto ISAKMP SA
```

Figure 57 : Liste des associations de sécurité ISAKMP

Nous remarquons qu'il n'y'a aucune association puisqu'il n'existe aucun client VPN configuré

2.1.2 Test d'accès VPN à distance

Pour tester l'accès VPN à distance nous avons utilisé Cisco VPN client.

Après le démarrage du client nous devons cliquer sur Connection Entries puis sur l'icône New comme le montre la figure de la page suivante

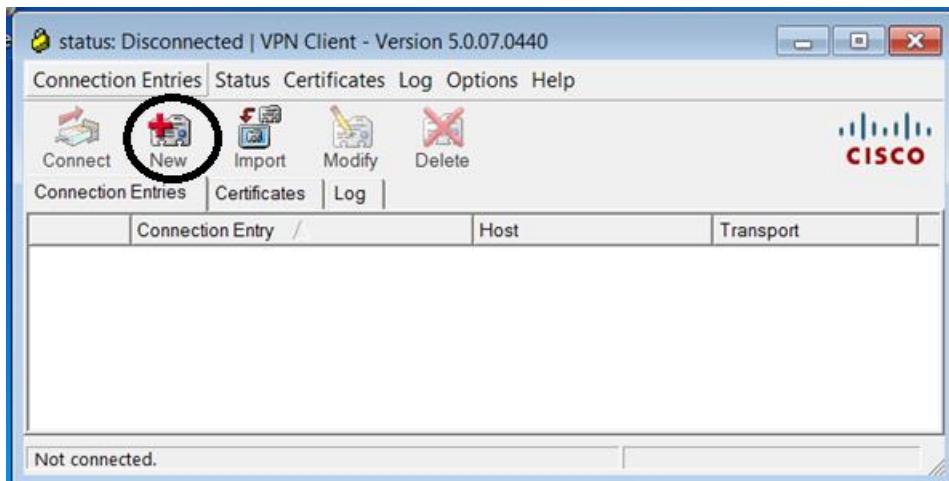


Figure 58 : Création d'une nouvelle entrée de connexion

Une nouvelle fenêtre s'affiche qui nous indique d'entrer les informations nécessaires afin de définir une nouvelle entrée de connexion.

- L'entrée de connexion = R1,
- L'adresse IP de l'interface s0/0 du routeur R1,
- Le nom du groupe d'authentification qui définit le pool d'adresses : globalnet,
- La clé pré-partagée configurée dans le routeur précédemment : Cisco.

Pour valider ces informations nous devons les enregistrer en cliquant sur Save.

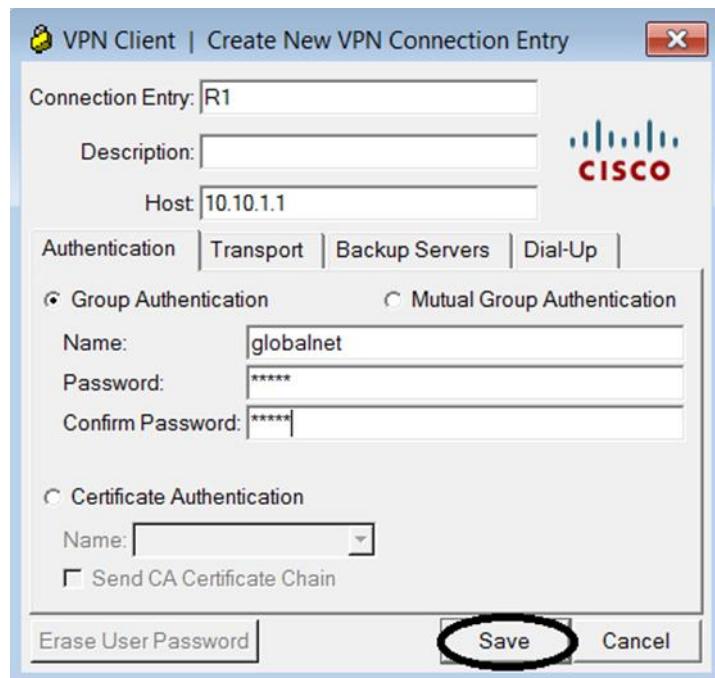


Figure 59 : Les informations de l'entrée de connexion à créer

Après avoir terminé la configuration du VPN client, nous devons à présent établir la connexion VPN

Pour l'établissement de la connexion VPN nous devons sélectionner la connexion créée précédemment (R1) puis cliquer sur l'icône Connect

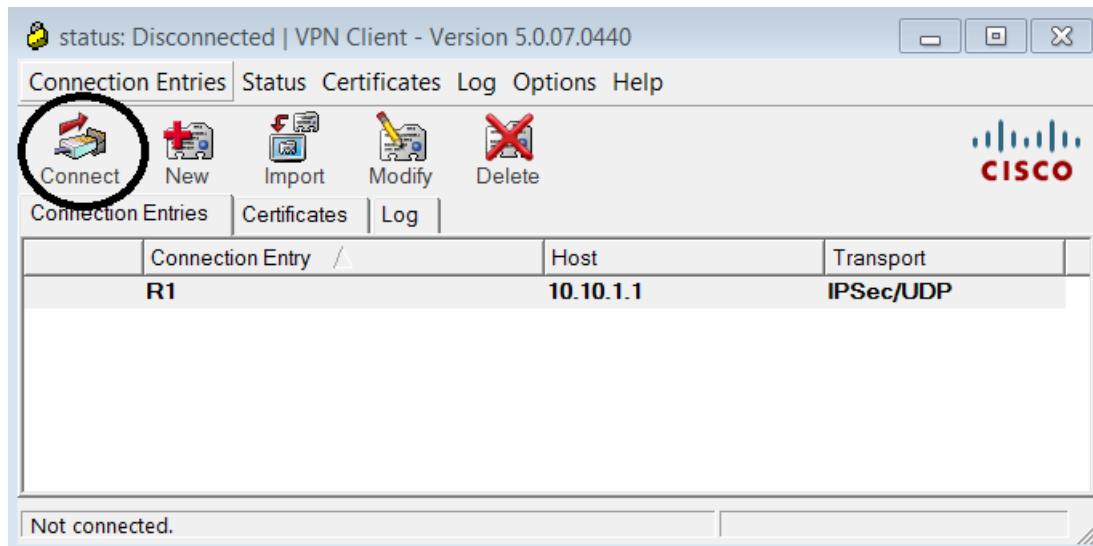


Figure 60 : Etablissement d'une connexion VPN

Une nouvelle fenêtre d'authentification d'utilisateur apparaît qui nous indique de taper le nom de l'utilisateur (test) et le mot de passe (test) précédemment configurés sur le routeur puis cliquer sur OK pour confirmer.

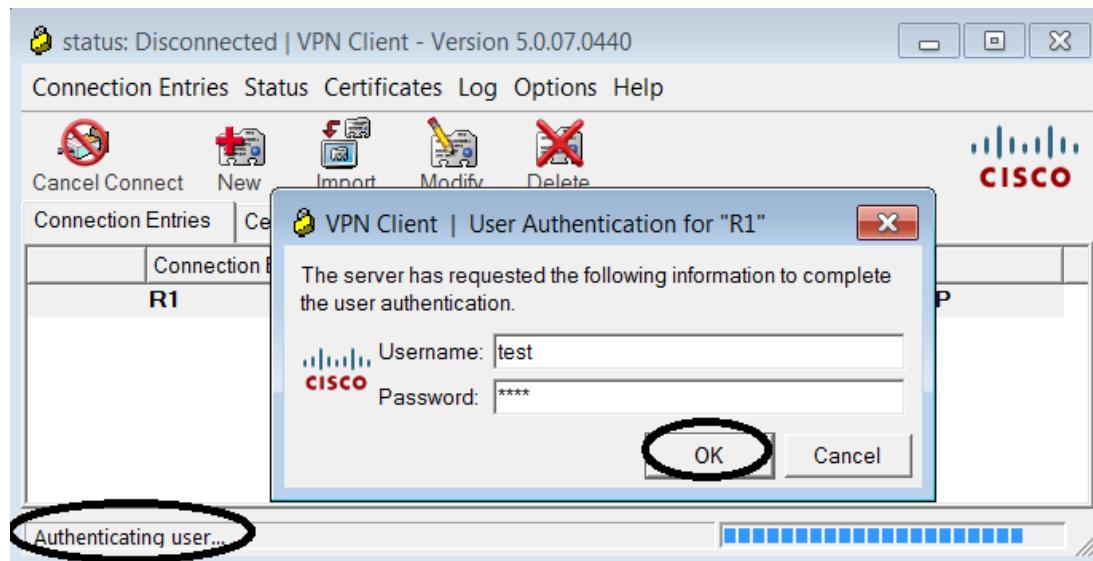


Figure 61 : Authentification de l'utilisateur pour l'entrée de connexion créée

La sécurisation du canal de communication est en cours

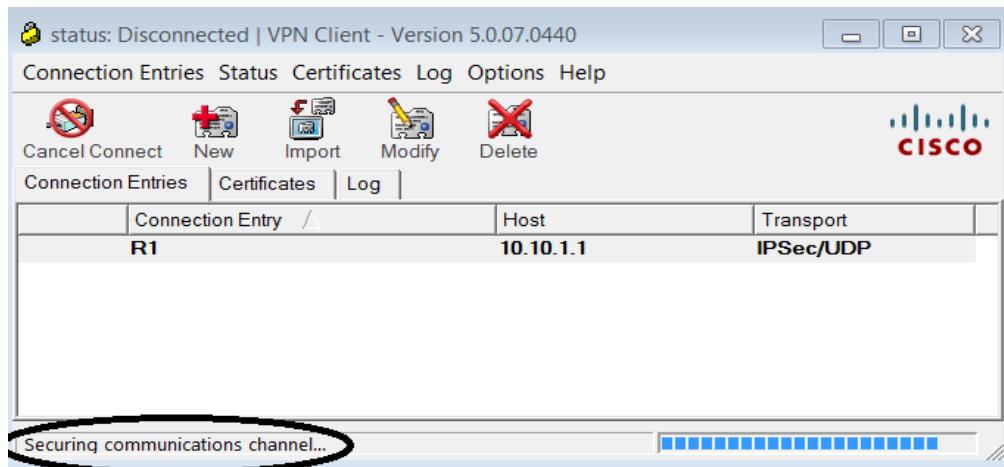


Figure 62 : Sécurisation du canal de communication

Après quelques temps la connexion du VPN client avec le routeur R1 s'établie avec succès comme le montre la figure ci-dessous

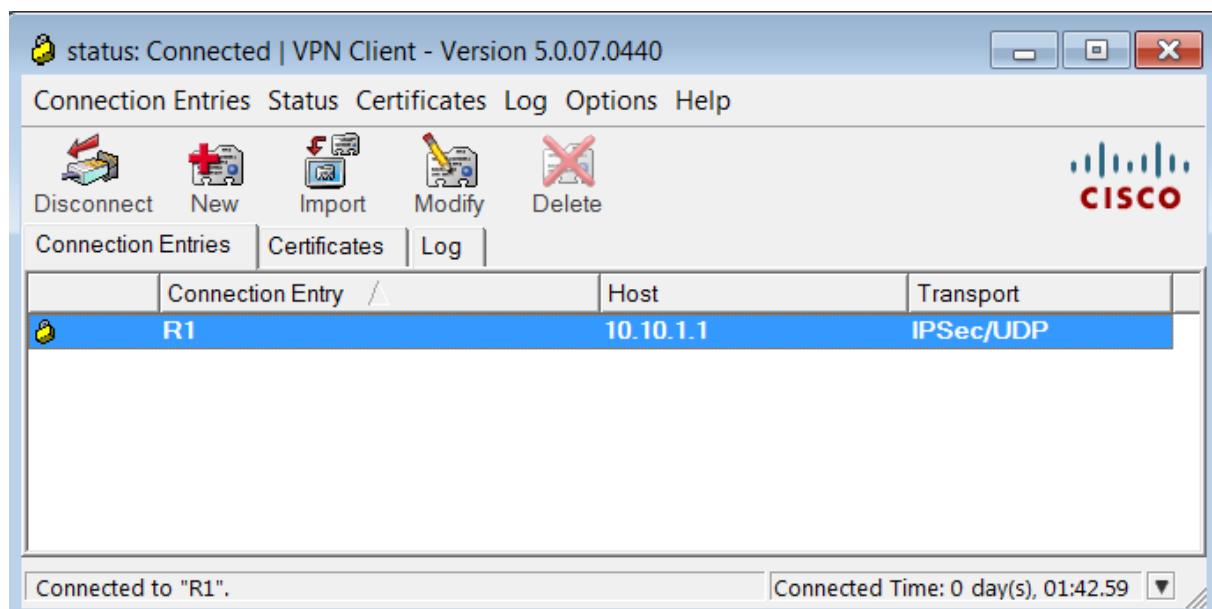


Figure 63 : Etablissement de la connexion avec succès

Nous avons donc la possibilité de consulter les statistiques de tunnel VPN client en choisissant Statistics après un clic droit sur l'icône du VPN client qui se trouve au niveau des icônes masqués de la barre des tâches

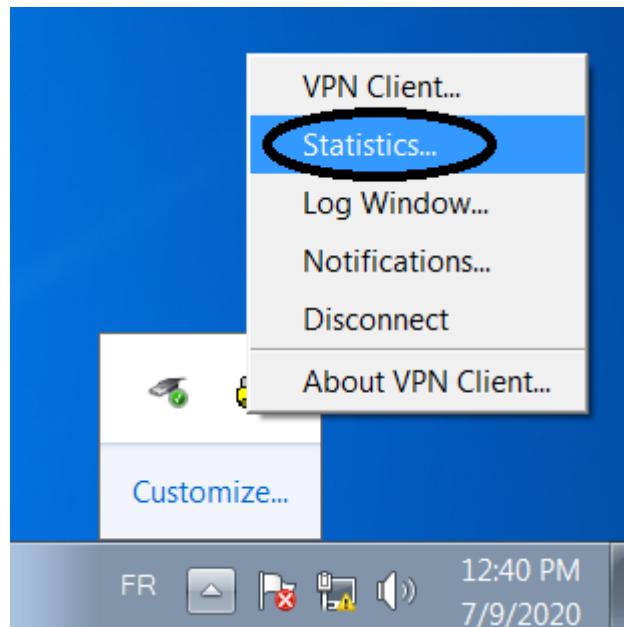


Figure 64 : Accès aux statistiques de tunnel de VPN client

La fenêtre des statistiques s'affiche qui contient un onglet des détails sur le tunnel à propos l'adresse du client et du serveur VPN, le nombre des paquets cryptés, décryptés jetés et bipassés, la méthode de cryptage utilisée, la méthode d'authentification utilisée etc.

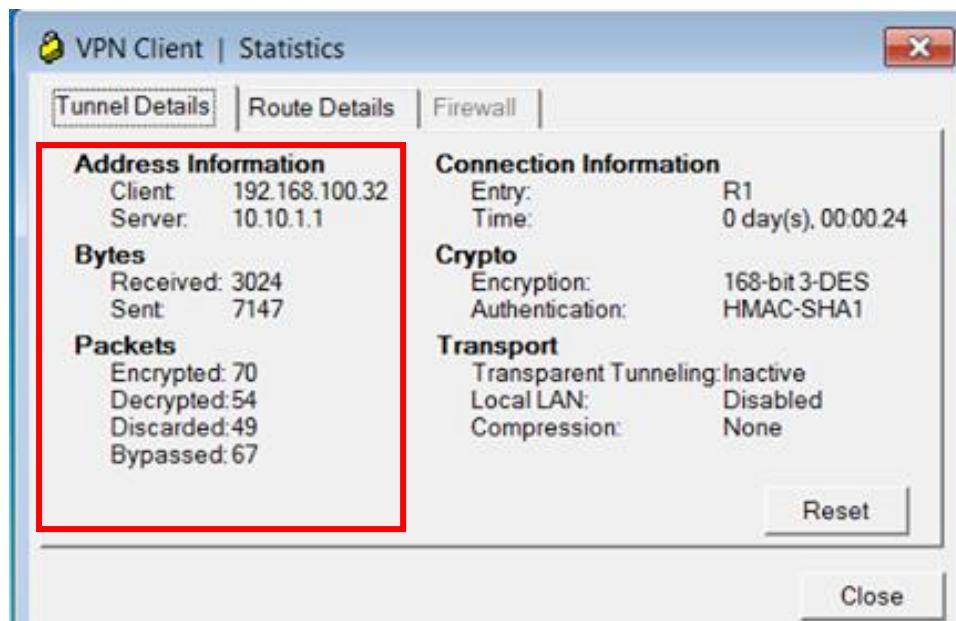


Figure 65 : Détails de tunnel

L'onglet Détails des routes permet d'afficher les routes que le client VPN sécurise vers le routeur.

Dans cet exemple, le client VPN sécurise l'accès aux réseaux 192.168.161.0/24, 192.168.162.0/24 et 192.168.163.0/24 alors que tout autre trafic n'est pas chiffré et n'est pas

envoyé à travers le tunnel. Le réseau sécurisé est téléchargé à partir d'ACL 101 qui est configuré dans le routeur R1.

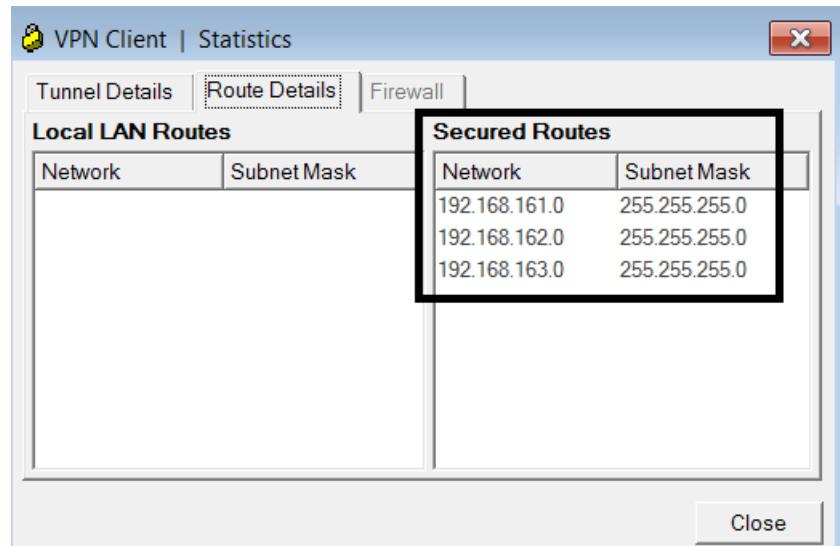


Figure 66 : Détails des routes sécurisés

Après avoir terminé la configuration nécessaire de notre VPN client nous pouvons vérifier les associations de sécurité ISAKMP

```
R1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id slot status
10.10.1.1    172.16.11.100  QM_IDLE   1002     0 ACTIVE
```

Figure 67 : nouvelle associations ISAKMP ajoutée.

Nous pouvons remarquer que l'adresse source affichée dans la figure ci-dessus est l'adresse de notre machine Windows dans laquelle nous avons installé et configuré le Cisco client VPN.

3. Configuration du AAA

Pour la configuration de l'AAA (authentication authorization and accounting) nous avons utilisé FreeRADIUS comme serveur d'authentification.

L'installation détailler de serveur est citée dans l'Annexe C.

Authentification RADIUS (Sécuriser l'accès à l'équipement)

Lorsqu'un utilisateur souhaite se connecter à son équipement réseau, Switch ou Routeur Cisco en Telnet ou ssh il doit spécifier un login et un mot de passe pour être autoriser à "entrer".

En règle générale ce couple login/mot de passe est stocké en local sur l'équipement. Le compte utilisateur est créé à l'aide de la commande suivante :

« ClientRADIUS (config) username nom secret password. »

Nous avons utilisé le mot clef secret au lieu de password, pour chiffrer le mot de passe en MD5 (cypher 5) et non avec l'algorithme de chiffrement de Cisco (cypher 7) qui est beaucoup plus faible et facilement crackable. Cette méthode à l'avantage d'être simple et rapide à mettre en place. Mais lorsque plusieurs personnes susceptibles de se connectent aux équipements réseaux, devoir créer un compte pour chacun serait très contraignant. Sinon on peut mettre en place un login et un mot de passe unique pour tout le monde, mais c'est au niveau de la sécurité que ça craint.

Pour remédier à cela, nous avons utilisé un serveur RADIUS qui sera chargé de valider l'authentification des utilisateurs qui souhaitent se connecter aux équipements réseaux.

3.1 Configuration de serveur FreeRADIUS

Après l'installation, nous devons configurer free radius pour l'authentification MySQL.

Pour ce faire, il faut éditer le fichier de configuration du serveur de base de données MySQL situé sous le répertoire /etc/freeradius/3.0/mods-enabled afin d'ajouter et modifier les informations nécessaires de notre base de données radius MySQL précédemment créé.

```
root@freeradius-virtual-machine:~# vim /etc/freeradius/3.0/mods-enabled/sql

dialect = "mysql"

# Connection info:
#
server = "localhost"
port = 3306
login = "radius"
password = "rsi3"

# Database table configuration for everything except Oracle
radius_db = "radius"

#
driver = "rlm_sql_mysql"

read_clients = yes
```

Figure 68 : Edition du fichier sql

Après avoir édité le fichier de configuration, nous devons redémarrer le service freeradius comme la montre la figure ci-dessous

```
root@freeradius-virtual-machine:~# service freeradius restart
root@freeradius-virtual-machine:~#
```

Figure 69 : Redémarrage du service Freeradius

- **Edition du fichier clients.conf : ajout du client au serveur radius**

Nous allons maintenant réaliser la configuration nécessaire pour l'authentification des routeurs R1 et R2.

Nous commençons par la configuration du fichier clients.conf qui contient une liste des clients qui peuvent être un équipement réseaux (commutateur, routeur) identifiés par un shortname qui est le nom du client ou de l'équipement, une adresse IP, un mot de passe secret et un nastype qui est le type de NAS.

La figure ci-dessous montre la configuration nécessaire pour déclarer les routeurs R1 et R2 comme clients.

```
root@freeradius-virtual-machine:~# vim /etc/freeradius/3.0/clients.conf
```

```
client 10.10.1.1 {
    secret = secretkey
    nastype = cisco
    shortname = R1
}
client 192.168.160.254 {
    secret = secretkey
    nastype = cisco
    shortname = R1
}
client 192.168.161.254 {
    secret = secretkey
    nastype = cisco
    shortname = Gateway
}
client 10.10.1.2 {
    secret = secretkey
    nastype = cisco
    shortname = R2
}
client 172.16.11.254 {
    secret = secretkey
    nastype = cisco
    shortname = R2
}
```

Figure 70 : Edition du fichier clients.conf

- **Ajout d'un nouvel utilisateur au serveur freeradius : éditer le fichier users**

Nous devons aussi éditer le fichier users afin d'ajouter deux utilisateurs nommés essia et hiba à notre serveur radius avec les mots de passes essiapass et hibapass et leurs donner les niveaux 15 et 3 comme privilège.

```
root@freeradius-virtual-machine:/etc/freeradius# vi users

essia Cleartext-Password := "essiapass"
    Service-Type = NAS-Prompt-User,
    Cisco-AVPair ="shell:priv-lvl=15"
hiba Cleartext-Password := "hibapass"
    Service-Type = Nas-Prompt-User,
    Cisco-AVPair ="shell:priv-lvl=3"
```

Figure 71 : Edition du fichier users

Après avoir configuré ces deux fichiers, nous devons redémarrer le service pour enregistrer les modifications .

```
root@freeradius-virtual-machine:~# service freeradius restart
```

Les utilisateurs ont été ajoutés avec succès, nous pouvons donc tester l’authentification radius avec ces utilisateurs localement sur le serveur à l’aide de la commande ci-dessous :

```
root@freeradius-virtual-machine:~# radtest essia essiapass localhost 0 testing1
23
Sent Access-Request Id 195 from 0.0.0.0:59858 to 127.0.0.1:1812 length 75
    User-Name = "essia"
    User-Password = "essiapass"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 0
    Message-Authenticator = 0x00
    Cleartext-Password = "essiapass"
Received Access-Accept Id 195 from 127.0.0.1:1812 to 0.0.0.0:0 length 51
    Service-Type = NAS-Prompt-User
    Cisco-AVPair = "shell:priv-lvl=15"
root@freeradius-virtual-machine:~# radtest hiba hibapass localhost 0 testing123

Sent Access-Request Id 99 from 0.0.0.0:55755 to 127.0.0.1:1812 length 74
    User-Name = "hiba"
    User-Password = "hibapass"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 0
    Message-Authenticator = 0x00
    Cleartext-Password = "hibapass"
Received Access-Accept Id 99 from 127.0.0.1:1812 to 0.0.0.0:0 length 50
    Service-Type = NAS-Prompt-User
    Cisco-AVPair = "shell:priv-lvl=3"
```

Figure 72 : Test de l’authentification freeradius en local

Testing123 est un mot de passe par défaut dans le fichier clients.conf pour tester localement.

Une vérification de l’accès des utilisateurs devient obligatoire avant de pouvoir accéder à la ligne de commande des routeurs.

Nous devons s'authentifier avec le nom d'utilisateur et le mot de passe définis dans le serveur radius.



Figure 73 : Authentification radius dans les routeurs R1 et R2

Comme cette configuration est un peu sensible et peu amener à une perte de temps nous avons installé une interface graphique dalaradius .



Figure 74: page d'accueil daloRADUIS

Cette solution va faciliter le management des utilisateurs comme suit :

- **Ajout d'un utilisateur**

Pour ajouter un nouvel utilisateur nous devons accéder au menu de gestion et cliquer sur nouvel utilisateur.

The screenshot shows the daloRADIUS Management interface. At the top, there's a header with the daloRADIUS logo, the text "RADIUS Management, Reporting, Accounting and Billing by Liran Tal", and a search bar labeled "Search Users". To the right, it says "Welcome, administrator. Location: default". Below the header is a navigation menu with links like Home, Management (which is highlighted), Reports, Accounting, Billing, GIS, Graphs, Config, and Help. Under the Management link, there's a sub-menu with options: List Users, New User (circled in red), New User - Quick Add, Edit User, Search Users, Remove Users, Import Users. To the right of the sub-menu, there's a chart titled "Total Users" showing one user. The main title "Users and Hotspots Management" is displayed above the chart.

Figure 75 : ajout d'un user dans daloRADIUS

Une nouvelle page s'affiche qui indique de taper un nom d'utilisateur, un mot de passe et choisir le type de mot de passe à partir d'une liste déroulante, dans notre cas nous avons choisi le type Cleartext.

New User | ?

The screenshot shows the "New User" configuration page. At the top, there are tabs for Account Info, User Info, Billing Info, and Attributes. The "Account Info" tab is selected. Below the tabs, there's a section titled "Username Authentication" with the following fields: "Username" (essia), "Password" (essiapass), "Password Type" (Cleartext-Password), and "Group" (Select Groups). There are also "Random" and "Add" buttons next to the password and group fields. At the bottom of the form, there's a "Save" button.

Figure 76 : Validation des données de l'utilisateur

L'une des caractéristiques les plus importantes de FreeRADIUS est l'attribut, nous pouvons utiliser des attributs pour définir ce qu'un utilisateur peut ou ne peut pas faire, créer des règles dynamiques pour décider si un utilisateur peut être authentifié.

Dans notre cas nous avons choisi le fournisseur cisco, l'attribut Cisco-AVPair et un niveau de privilège égale à 15.

New User | ?

Account Info User Info Billing Info **Attributes**

Locate Attribute via Vendor/Attribute

Vendor: Cisco

Attribute: Cisco-AVPair

Quickly Locate attribute with autocomplete input

Custom Attribute:

Attribute: Cisco-AVPair
Value: shell:priv-lvl=15 Op: = Target: reply

Figure 77 : les privilèges d'un user

L'utilisateur a été créé avec succès, nous pouvons afficher la liste des utilisateurs créés en cliquant sur List Users dans le menu de gestion.

Users Listing | ?

SELECT: [ALL](#) [NONE](#)

1

ID	Name	Username	Password
<input type="checkbox"/> 17		admin	radius
<input type="checkbox"/> 21		user1	cisco
<input type="checkbox"/> 22		root	root
<input type="checkbox"/> 23		essia	essiapass
<input type="checkbox"/> 24		hiba	hibapass

PAGE 1 OF 1

Figure 78 : Liste users

- **Ajout d'un client et un utilisateur NAS**

Pour qu'un autre équipement se connecte à notre serveur il doit être ajouté à la table client NAS de la base de données RADIUS.

Pour ajouter un nouveau NAS, il faut cliquer sur Gestion > NAS > Nouveau NAS.

The screenshot shows the dalo RADIUS Management interface. The top navigation bar includes Home, Management, Reports, Accounting, Billing, GIS, Graphs, Config, Help, Users, Batch Users, Hotspots, Nas, User-Groups, Profiles, HuntGroups, Attributes, Realms/Proxys, and IP-Pool. The 'Nas' menu item is highlighted with a red oval. The main content area is titled 'New NAS Record'. It contains a 'NAS Info' section with tabs for 'NAS Info' and 'NAS Advanced'. The 'NAS Info' tab is selected. The form fields are: NAS IP/Host (10.10.1.1), NAS Secret (secretkey), NAS Type (cisco, dropdown menu), and NAS Shortname (R1). An 'Apply' button is at the bottom. The right side of the interface shows a 'NAS Info' panel.

Figure 79 : ajout d'un NAS

Nous pouvons maintenant ajouter notre client en précisant son adresse, son mot secret, son type et son nom.

Dans notre cas nous avons ajouté la passerelle et l'adresse du routeur R1 et R2 la figure ci-dessous montre la liste des clients NAS ajoutés.

NAS Listing in Database

The screenshot shows the 'NAS Listing in Database' page. At the top, there is a 'SELECT: ALL NONE' button and a 'Delete' button. Below this, a table displays the following data:

NAS ID	NAS IP/Host	NAS Shortname	NAS Type	NAS Ports	NAS Secret	NAS Virtual Server
5	10.10.1.1	R1	cisco	0	Str0ngR@diusPass	
6	10.10.1.2	R2	cisco	0	Str0ngR@diusPass	
8	192.168.161.254	monPC	cisco	0	Str0ngR@diusPass	
9	172.16.10.254	passerelle	cisco	0	Str0ngR@diusPass	
10	192.168.161.105	ansible	other	0	Str0ngR@diusPass	

At the bottom, it says 'PAGE 1 OF 1' with navigation icons.

Figure 80 : Liste NAS

3.2 Configuration du routeur comme client

Premièrement, il faut activer le protocole AAA avec la commande « aaa new-model » pour pouvoir commencer la configuration radius.

Ensuite, nous devons définir un groupe de serveurs de type RADIUS.

Puis indiquer l'adresse IP du serveur RADIUS ainsi que la clé secrète et les ports par défaut à utiliser (le port 1812 pour l'authentification et le port 1813 pour la traçabilité).

```
R1(config)#aaa new-model
R1(config)#aaa group server radius RadiusGrp
R1(config-sg-radius)#server-private 192.168.161.100 auth-port 1812 acct-port 1$
```

Figure 81 : Déclaration des éléments de groupe radius

Dans notre cas nous avons l'adresse 192.168.161.100 qui est celle de notre serveur, RadiusGrp qui est le nom du groupe choisi et le mot secretkey comme clé secrète.

Nous passons maintenant à la configuration de l'authentification, l'autorisation et la traçabilité.

```
R1(config-sg-radius)#aaa authentication login default group RadiusGrp
R1(config)#aaa authorization exec default group RadiusGrp
R1(config)#aaa accounting exec default start-stop group RadiusGrp
R1(config)#aaa accounting system default start-stop group RadiusGrp
R1(config)#radius-server vsa send accounting
R1(config)#radius-server vsa send authentication
```

Figure 82 : Configuration de l'authentification au niveau du routeur

Puis configurer l'authentification sur les lignes vty.

```
R1(config)#line vty 0 4
R1(config-line)#transport input telnet ssh
R1(config-line)#login authentication default
```

Figure 83 : Configuration de ligne vty

Nous pouvons aussi accéder à la ligne de commande des routeurs à distance via Telnet en utilisant le programme PuTTY par exemple.

Nous utilisons le même nom d'utilisateur ainsi que le même mot de passe configurés et définis au niveau du serveur freeradius précédemment.

Pour afficher le niveau de privilège définis dans le serveur nous utilisons la commande : **show privilege**

Cet utilisateur a un niveau de privilège égale à 15, il a la possibilité d'accéder au mode de configuration du routeur, d'afficher la configuration actuelle avec la commande show running-config view full et d'utiliser toutes les commandes liées à l'interface.

```
User Access Verification  
Username: essia  
Password:  
  
R1#show privilege  
Current privilege level is 15  
R1#show running-config view full  
Building configuration...  
  
Current configuration : 3406 bytes  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R1  
!  
boot-start-marker  
boot-end-marker  
!
```

Figure 84 : Test d'authentification à distance d'user avec privilèges 15

```
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#[redacted]
```

Figure 85 : Accès à distance au mode de configuration du routeur

Contrairement à cet utilisateur qui a un niveau du privilège égal à 3, il n'a pas le droit d'accéder au mode de configuration ou même d'afficher la configuration du routeur comme le montre la figure ci-dessous.

```
User Access Verification  
Username: hiba  
Password:  
  
% Authentication failed  
  
Username: hiba  
Password:  
  
R2#show privilege  
Current privilege level is 3  
R2#conf t  
^  
% Invalid input detected at '^' marker.  
  
R2#show running-config view full  
^  
% Invalid input detected at '^' marker.
```

Figure 86 : Test d'authentification à distance d'user avec privilèges 3

3.3 Revue de sprint

Pendant ce sprint, nous avons réussi à terminer toutes les user stories et leurs tâches planifiées.

La réunion de validation du sprint 2 s'est tenu à distance le 15/06/2020 à 14h.

En présence de :

Product owner: Mme Ben hamza Dhouha

Scrum team: Farhat Hiba et El Ghoul Essia

Les fonctionnalités de Sprint 2:

Fonctionnalités	Validation
Mise en place d'un réseau privé virtuel <ul style="list-style-type: none">✓ Configuration du routeur avec les contrôle d'accés✓ Mise en place de cisco VPN client	OUI
Configuration de l'AAA <ul style="list-style-type: none">✓ installation et configuration de serveur FreeRADIUS✓ Installation dalaradius✓ Configuration des utilisateurs✓ Configuration NAS	

3.4 Rétrospective

Au niveau de ce sprint nous avons rencontré des problèmes au niveau de la configuration VPN .nous l'avons résolu en changeant une autre méthode.

Aussi nous sommes encerclés au niveau de la configuration du serveur freeradius, l'authentification se bloque suite à la saisie du nom d'utilisateur et du mot de passe.

Nous avons rencontré aussi un problème au niveau de dalaradius. Nous l'avons résolu avec le changement de la cible du privilège en mode réponse au lieu de la vérification.

3.5 Burndown chart

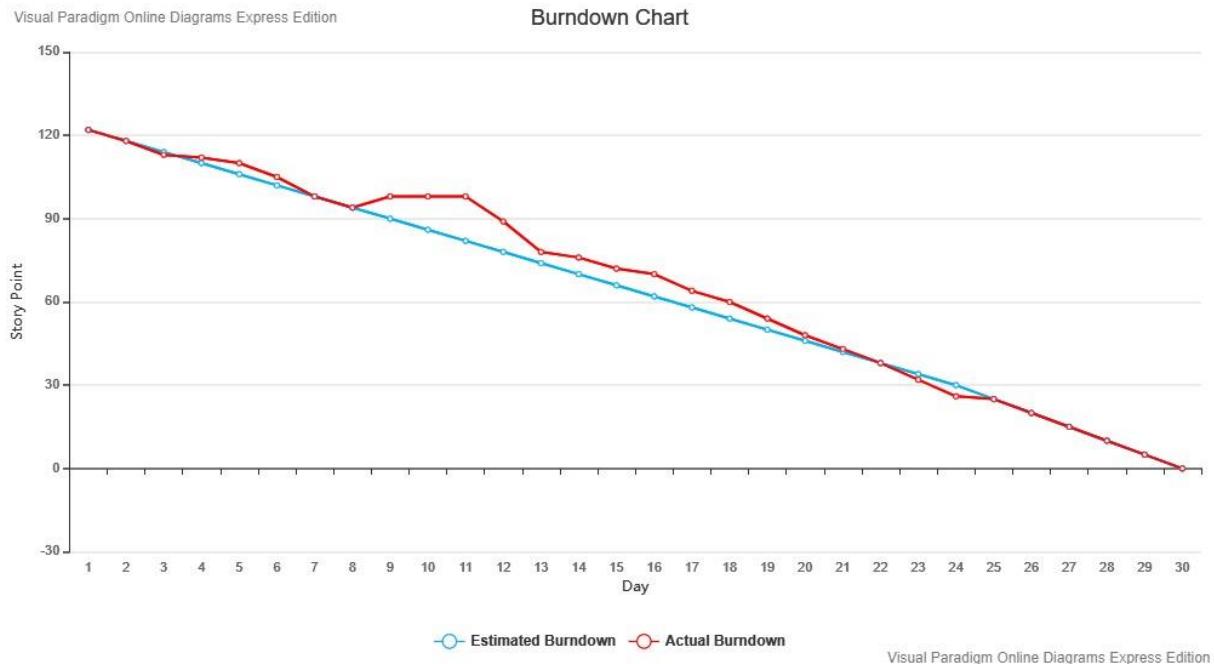


Figure 87 : Burndown chart sprint3

Comme la montre la figure 87, nous avons rencontré des problèmes la deuxième semaine, puis une coïncidence durant la dernière période de sprint.

Conclusion

Au cours de ce sprint, nous avons mis en place un réseau privé virtuel d'accès et un serveur d'authentification pour le contrôle des accès en local et à distance afin de fournir une solution sécurisée.

Chapitre 6 : sprint 3 automatisation de la supervision avec ansible

Introduction

Après avoir mis en place nos solutions de supervision et d'authentification, nous passons maintenant à l'automatisation de la supervision des machines. Ce chapitre illustre le cycle de vie du troisième sprint à savoir la spécification fonctionnelle et la réalisation.

1. Spécification fonctionnelle :

La spécification fonctionnelle comporte trois parties :

Le backlog du sprint qui présente les différents user stories concernant ce sprint, le diagramme de cas d'utilisation et la configuration de serveur pour gérer les machines.

1.1 Backlog du sprint :

Tableau 12 : Backlog du sprint 3

ID	User Story	Tâche	Estimation
AAAA	En tant qu'Administrateur je veux installer automatiquement les agents de supervision puis déclarer les nouveaux éléments dans l'outil de supervision	Installation et configuration ansible	2
		Installation des API d'eyes of network	0.5
		Sécurisation de transfert des clés	4
		Ecrire un playbook permettant la configuration automatique de protocole snmp	10
		Ecrire un script php permettant l'ajout de machines	20
		Ecrire le fichier playbook contenant le script de l'ajout des machines	10

Après avoir présenté la liste des tâches, nous allons passer à la présentation du cas d'utilisation de ce sprint.

1.2 Diagramme de cas d'utilisation du sprint 3

Ce cas d'utilisation offre à l'administrateur la possibilité d'automatiser la configuration et d'ajouter des machines dans le serveur monitoring

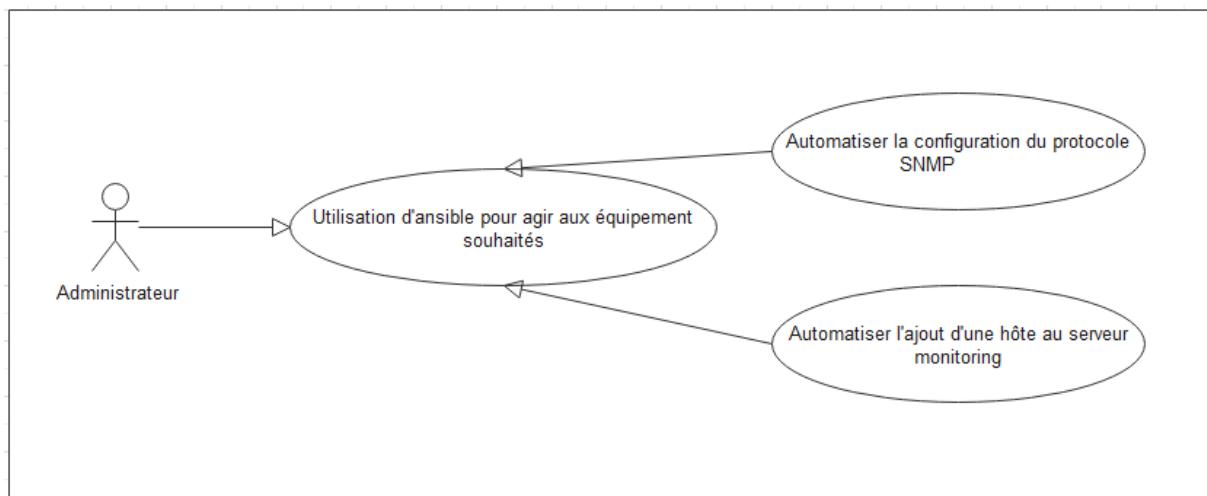


Figure 88: Diagramme de cas d'utilisation du sprint 3.

Maintenant nous allons donner une description textuelle des cas d'utilisation de sprint 3.

Tableau 13 : Description textuelle de cas d'utilisation "automatiser la configuration snmp"

Cas d'utilisation	Automatiser la configuration du protocole snmp
Acteur	Administrateur
Pré condition	La machine cible est accessible via SSH
Scénario Principal	L'administrateur exécute le script qui automatise l'installation du protocole snmp et la configuration distante de fichier /etc/snmp/snmpd.conf
Post Condition	Le fichier de configuration du snmp est configuré

Tableau 14 : Description textuelle de cas d'utilisation "automatiser l'ajout d'une hôte au eyes of network "

Cas d'utilisation	Automatiser l'ajout d'une hôte au serveur monitoring
Acteur	Administrateur
Pré condition	La machine cible est accessible via SSH
Scénario Principal	L'administrateur exécute le script qui automatise l'ajout d'hôte dans eyes of network
Post Condition	La machine est ajoutée dans le serveur

Après l'explication et la description textuelle de chaque cas d'utilisation, nous passons aux détails des étapes de réalisation de ce sprint.

2. Réalisation

Dans cette section, nous présentons les différentes tâches réalisées durant ce sprint, elle comporte deux parties :

- Sécurisation des transferts de clé et configuration des fichiers de base d'ansible
- Automatisation de l'ajout des machines dans le serveur EON

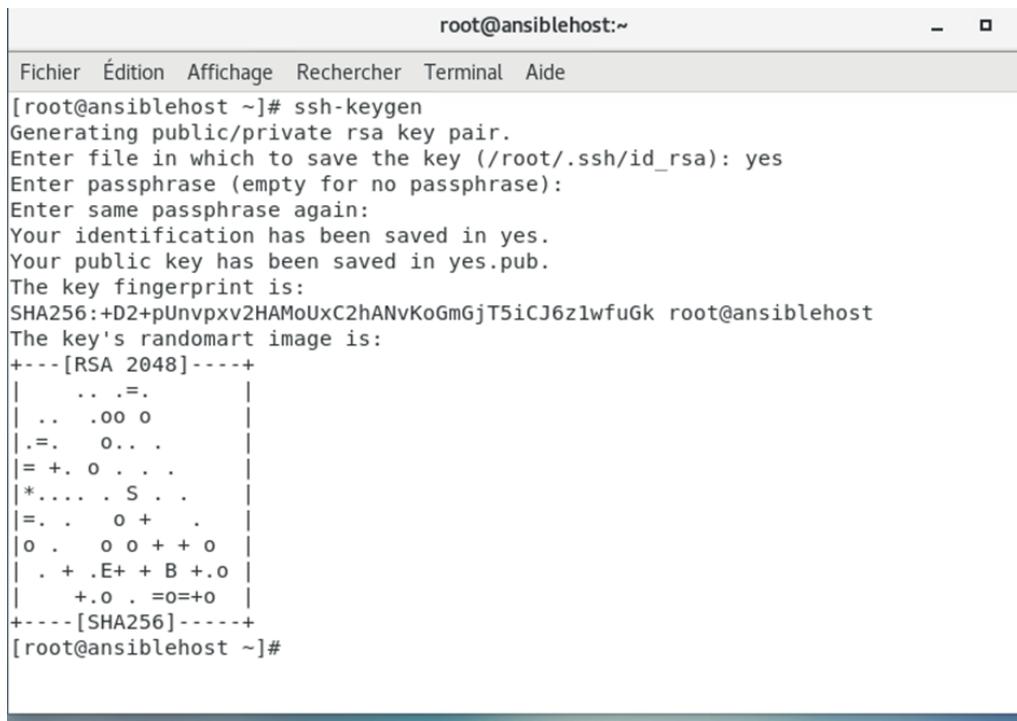
D'abord nous allons installer et configurer Ansible (Annexe D)

2.1 Configuration Ansible

Pour assurer un transfert sécurisé des configurations sur le réseau, nous avons utilisé le protocole SSH afin de garantir une confidentialité

2.1.1 Sécurisation des transferts

La figure ci-dessous présente la génération d'un couple clé SSH (publique/privé) qui assurent l'authentification mutuelle. Lors de sa production, nous saisissons une « passphrase » qui est un mot de passe servant à chiffrer le fichier contenant la clé privée. Cette protection permet d'éviter à quiconque d'accéder au fichier d'en extraire le contenu.



```
root@ansiblehost:~ - □
Fichier Édition Affichage Rechercher Terminal Aide
[ root@ansiblehost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): yes
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in yes.
Your public key has been saved in yes.pub.
The key fingerprint is:
SHA256:+D2+pUnpxv2HAMoUxC2hANvKoGmGjT5iCJ6zlwfuGk root@ansiblehost
The key's randomart image is:
+---[RSA 2048]---+
|   ...=.
| .. .oo o
|.=. o...
|=+. o ...
|*.... S ..
|=.. o +
|o . o o + + o
| . + .E+ + B +.o
| +.o . =o=+o
+---[SHA256]---+
[ root@ansiblehost ~]#
```

Figure 89 : Génération des clés.

Dans l'étape suivante, nous copions la clé publique sur la machine destination dans le fichier `authorized_keys` en indiquant le mot de passe de l'utilisateur de cette machine

```
[root@ansiblehost ~]# ssh-copy-id root@192.168.161.200
/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that
are already installed
/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is
to install the new keys
root@192.168.161.200's password:

Number of key(s) added: 1

Now try logging into the machine, with:    "ssh 'root@192.168.161.200'"
and check to make sure that only the key(s) you wanted were added.

[root@ansiblehost ~]#
```

Figure 90: copie de clé publique.

2.1.2 Configuration du fichier inventaire ansible

Le fichier inventaire par défaut est `/etc/ansible/hosts` mais pour des raisons de sécurité nous allons créer un fichier à part pour ne pas l'endommager.

Ceci doit être configuré avant de pouvoir commencer la communication avec la machine distante.

Les crochets permettent de définir des groupes, nous avons défini un groupe machines qui regroupe les nouveaux hôtes que nous allons automatiser leur supervision.

```
[root@ansiblehost ~]# cat /home/admin/inventory
[machines]
ftp ansible_ssh_host=192.168.161.200
smtp ansible_ssh_host=192.168.161.201
```

Figure 91: Configuration de fichier d'inventaires

Après avoir configuré l'accès ssh et le fichier d'inventaire nous pouvons maintenant tester la connectivité avec les machines distantes ajoutées dans le fichier inventaire.

- **Test de connectivité**

La figure ci-dessous montre le test de base pour s'assurer que les machines déclarées précédemment dans le fichier « inventory » disposent d'une connexion à l'hôte.

```

root@ansiblehost:~# ansible machines -m ping
[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 192.168.161.200 should
use /usr/bin/python3, but is using /usr/bin/python for backward compatibility
with prior Ansible releases. A future Ansible release will default to using the
discovered platform python for this host. See https://docs.ansible.com/ansible
/2.9/reference_appendices/interpreter_discovery.html for more information. This
feature will be removed in version 2.12. Deprecation warnings can be disabled
by setting deprecation_warnings=False in ansible.cfg.

192.168.161.200 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python"
    },
    "changed": false,
    "ping": "pong"
}
192.168.161.201 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
[root@ansiblehost:~]#

```

Figure 92: Test de connectivité

2.2 Automatiser la configuration snmp :

Tout contact répété avec les fichiers de configurations se considère comme une perte de temps, ainsi il risque d'endommager ces derniers si une action est mal faite principalement au cas où nous allons gérer un grand réseau disposant un nombre important d'hôtes.

Pour remédier à ces problèmes nous avons créé un playbook ansible comme le montre la figure ci-dessous pour l'installation du le protocole snmp et la modification de fichier /etc/snmp/snmpd.conf

```

Ouvrir ▾  test.yml /home/admin Enregistrer  - □ ×
hosts: machines
remote_user: root
tasks:
- name: update Debian packages cache
  apt: update_cache=yes cache_valid_time=3600
- name: PKG debian-keyring is at the latest version
  apt: pkg=debian-keyring state=latest
- name: PKG snmpd is at the latest version
  apt: pkg=snmpd state=latest
- name: snmpd.conf file configuration
  copy: content='rocommunity public <192.168.163.130>' dest=/etc/snmp/snmpd.conf
- name: restart snmpd
  service: name=snmpd state=restarted

```

Figure 93: automatisation de configuration du snmp

Maintenant nous allons exécuter le playbook pour vérifier son bon fonctionnement.

```
[root@ansiblehost admin]# ansible-playbook -i /home/admin/inventory /home/admin/test.yml

PLAY [machines] *****

TASK [Gathering Facts] *****
[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 192.168.161.200 should
use /usr/bin/python3, but is using /usr/bin/python for backward compatibility
with prior Ansible releases. A future Ansible release will default to using the
discovered platform python for this host. See https://docs.ansible.com/ansible
/2.9/reference_appendices/interpreter_discovery.html for more information. This
feature will be removed in version 2.12. Deprecation warnings can be disabled
by setting deprecation_warnings=False in ansible.cfg.
ok: [192.168.161.200]
ok: [192.168.161.201]

TASK [update Debian packages cache] *****
ok: [192.168.161.200]
ok: [192.168.161.201]

TASK [PKG debian-keyring is at the latest version] *****
ok: [192.168.161.200]
ok: [192.168.161.201]

TASK [PKG snmpd is at the latest version] *****
ok: [192.168.161.200]
ok: [192.168.161.201]

TASK [snmpd.conf file configuration] *****
ok: [192.168.161.200]
ok: [192.168.161.201]

TASK [restart snmpd] *****
changed: [192.168.161.200]
changed: [192.168.161.201]

PLAY RECAP *****
192.168.161.200      : ok=6    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
192.168.161.201      : ok=6    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

[root@ansiblehost admin]#
```

Figure 94 : exécution du playbook de configuration snmp

2.3 Automatisation de l'ajout des machines dans le serveur EON

Eyes Of Network comprend une API "Restful" appelée EONAPI qui permet aux programmes externes d'accéder aux informations de la base de données de surveillance et de manipuler des objets à l'intérieur des bases de données de la suite EON.

Dans le contexte de l'API HTTP EON, l'attribut "Restful" signifie essentiellement qu'il est basé sur HTTP/HTTPS et qu'il utilise un ensemble d'URL "HTTP GET/POST" pour accéder et manipuler les données et que nous obtiendrons un document JSON en retour (pour la plupart des appels).

L'API HTTP EON offre des fonctions de manipulation d'objets (p. ex., édition, ajout, suppression)

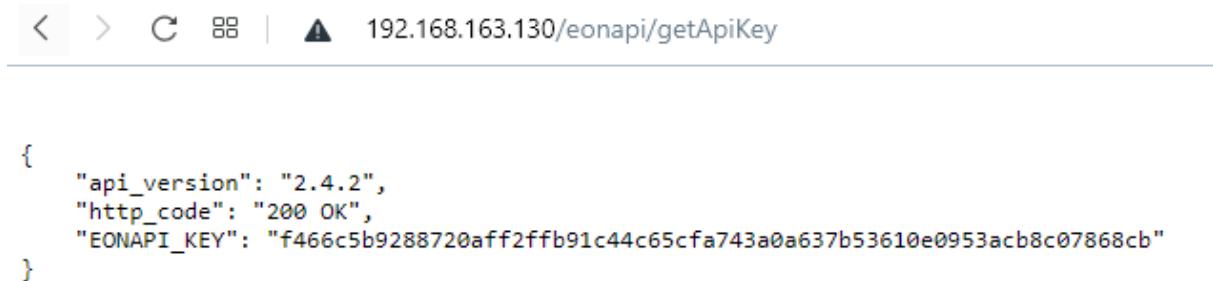
2.3.1 Génération d'une clé API

Certains appels à l'API sont protégés par la clé API. Nous devons présenter une clé valide dans notre demande. Chaque utilisateur EON dispose d'une APIKEY privée qui permet d'authentifier et valider les priviléges.

Il faut générer notre APIKEY avec l'EONAPI en suivant cette URI dans notre appel d'API de navigateur ou d'application :

[https://\[EON_IP\]/eonapi/getAuthenticationStatus?&username=\[username\]&apiKey=\[apiKey\]](https://[EON_IP]/eonapi/getAuthenticationStatus?&username=[username]&apiKey=[apiKey])

La figure ci-dessous affiche le résultat obtenu :



A screenshot of a web browser window. The address bar shows the URL: 192.168.163.130/eonapi/getApiKey. The page content displays a JSON object:

```
{  
    "api_version": "2.4.2",  
    "http_code": "200 OK",  
    "EONAPI_KEY": "f466c5b9288720aff2ff91c44c65cfa743a0a637b53610e0953acb8c07868cb"  
}
```

Figure 95 : Clé API

Nous allons utiliser cette clé dans les étapes qui suivent.

2.3.2 Crédation d'une page web dynamique

Cette page est implémenté en utilisant les deux langages web PHP et JavaScript, et grâce à la bibliothèque Ajax du JavaScript, les paramètres qui sont reçus à travers la méthode GET seront envoyés au API à travers la méthode POST afin de mettre à jour la base de donnée.

La fonction CreateHost de l'API (EONAPI) est responsable de réaliser l'ajout de la machine dans la base de données d'Eyeofnetwork à condition qu'elle reçoive les informations de la machine à ajouter à travers des variables de la méthode POST.

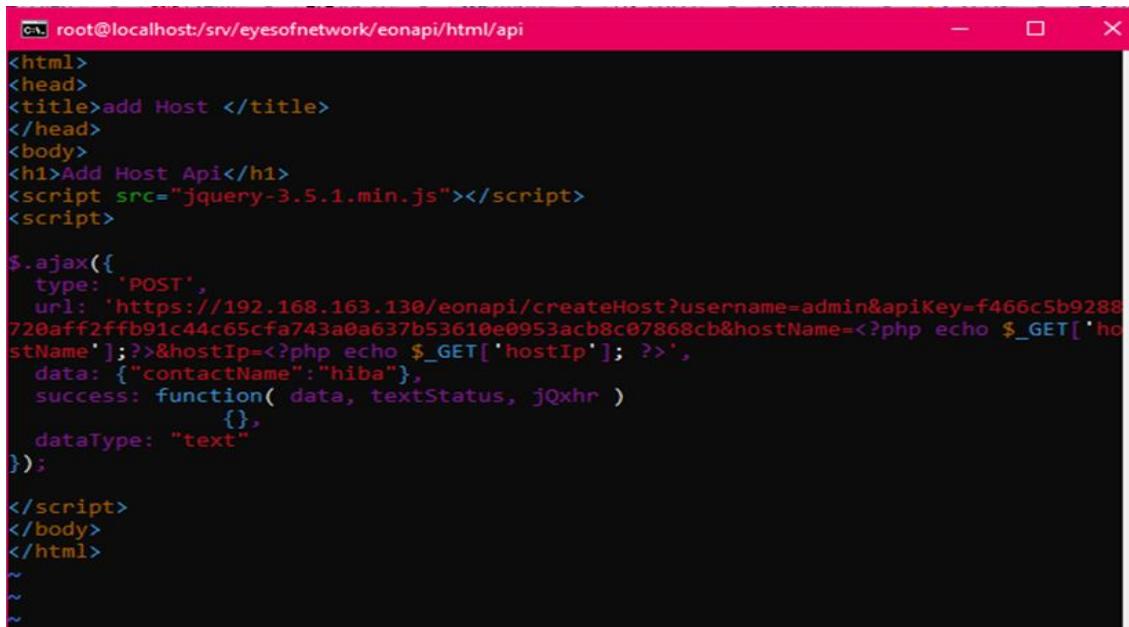
En cas de réussite d'ajout, l'api renvoie une réponse JSON, sinon un message d'erreur ou une exception ou cas où il y a des informations manquantes lors de l'appel.

Un appel API de base ressemblera à cela :

[https://\[EON_IP\]/eonapi/\[API_function\]?&username=\[username\]&apiKey=\[apiKey\]](https://[EON_IP]/eonapi/[API_function]?&username=[username]&apiKey=[apiKey])

Cette page web joue le rôle d'intermédiaire entre le script bash (qui est appelé à travers ansible) et l'API

Comme la montre la figure ci-dessous.



```
root@localhost:/srv/eyesofnetwork/eonapi/html/api
<html>
<head>
<title>add Host </title>
</head>
<body>
<h1>Add Host Api</h1>
<script src="jquery-3.5.1.min.js"></script>
<script>

$.ajax({
  type: 'POST',
  url: 'https://192.168.163.130/eonapi/createHost?username=admin&apiKey=f466c5b9288720aff2fffb91c44c65cfa743a0a637b53610e0953acb8c07868cb&hostName=<?php echo $_GET['hostName']; ?>&hostIp=<?php echo $_GET['hostIp']; ?>',
  data: {"contactName": "hiba"},
  success: function( data, textStatus, jqxhr )
  {
    console.log(data);
  },
  dataType: "text"
});

</script>
</body>
</html>
~
```

Figure 96 : création d'une page web dynamique addHost

En effet, cette page est créée afin d'assurer le transfert des deux variable hostName et hostIp à l'api.

Après la réussite de la création de la page web intermédiaire, nous allons passer à l'étape suivante qui permet de créer un script bash qui fait l'appel à cette page par la méthode GET.

2.3.3 Cr éation de playbook ansible et script bash

Ce playbook va se lancer sur les machines déclarées dans le fichier d'inventaires comme nous l'avons mentionné précédemment. Ce qui permettra leurs configuration snmp, puis il passe à l'ajout des machines avec l'exécution locale pour chaque hôte séparé à l'aide d'un script bash nommé addHost.sh qui prend en paramètres le nom et l'adresse IP déclarés précédemment dans le fichier d'inventaires.



```
Ouvrir
test.yml
/home/admin
Enregistrer
hosts: machines
remote_user: root
tasks:
- name: update Debian packages cache
  apt: update_cache=yes cache_valid_time=3600
- name: PKG debian-keyring is at the latest version
  apt: pkg=debian-keyring state=latest
- name: PKG snmpd is at the latest version
  apt: pkg=snmpd state=latest
- name: snmpd.conf file configuration
  copy: content='rocommunity public <192.168.163.130>' dest=/etc/snmp/snmpd.conf
- name: restart snmpd
  service: name=snmpd state=restarted
- name: ajout machine dans EyesOfNetwork
  local_action: command sh /home/admin/addHost.sh {{ inventory_hostname }}
{{ ansible_ssh_host }}
```

Figure 97 : playbook d'ajout machine



The screenshot shows a terminal window with the title "addHost.sh" and the path "/home/admin". In the top left corner, there are buttons for "Ouvrir" and a dropdown menu. The main area contains the following command:

```
#!/bin/bash
curl -k -X POST "https://192.168.163.130/eonapi/addHost.php?&hostName=$1&hostIp=$2"
```

Figure 98 : script bash addHost.sh

Curl est un utilitaire en ligne de commande qui permet aux utilisateurs de créer des requêtes HTTP.

-k : cette option spécifie un fichier texte qui permet de lire les arguments curl.

Les arguments en ligne de commande trouvés dans le fichier texte seront utilisés comme s'ils étaient fournis sur la ligne de commande.

-x : Spécifie une méthode de requête personnalisée à utiliser lors de la communication avec le serveur HTTP. La méthode de requête spécifiée sera utilisée à la place de la méthode utilisée autrement (par défaut GET)

2.3.4 Exécution de playbook

Après la préparation et la création des fichiers nécessaires nous allons maintenant lancer le playbook d'ajout des machines.



```
[root@ansiblehost ~]# ansible-playbook -i /home/admin/inventory /home/admin/test.yml
PLAY [machines] ****
TASK [Gathering Facts] ****
[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host ftp should use
/usr/bin/python3, but is using /usr/bin/python for backward compatibility with
prior Ansible releases. A future Ansible release will default to using the
discovered platform python for this host. See https://docs.ansible.com/ansible/
2.9/reference_appendices/interpreter_discovery.html for more information. This
feature will be removed in version 2.12. Deprecation warnings can be disabled
by setting deprecation_warnings=False in ansible.cfg.
ok: [ftp]
ok: [smtp]

TASK [ajout machine dans EyesOfNetwork] ****
changed: [smtp]
changed: [ftp]

PLAY RECAP ****
ftp                  : ok=2    changed=1    unreachable=0    failed=0    skipped=
0      rescued=0   ignored=0
smtp                : ok=2    changed=1    unreachable=0    failed=0    skipped=
0      rescued=0   ignored=0

[root@ansiblehost ~]#
```

Figure 99 : Exécution de playbook d'ajout des hôtes

192.168.163.130/module/module_frame/index.php

k Paramètres Ec

Host Browser

Add A New Child Host

Object to : | Actions :

Host Name	Address	Description
ESXI	192.168.161.139	ESXI
FreeRADIUS	192.168.161.100	FreeRADIUS
ftp	192.168.161.200	
localhost	127.0.0.1	EyesOfNetwork Network Server
pc-ubuntu	192.168.162.100	pc-ubuntu
PC-WIN	172.16.10.100	PC-WIN
R1 s0/0	10.10.1.1	R1 s0/0
R2 s0/0	10.10.1.2	R2 s0/0
smtp	192.168.161.201	

Figure 100 : machines ajoutées avec succès

Les figures ci-dessus montrent bien l'ajout des machines avec succès.

2.4 Revue de sprint

Pendant ce sprint, nous avons réussi à terminer toutes les user stories et leurs tâches planifiées.

La réunion de validation du sprint 3 s'est tenue au local de l'entreprise GLOBALNET le 0/07/2020 à 9h.

En présence de :

Product owner: Mme Ben hamza Dhouha

Scrum team: Farhat Hiba et El Ghoul Essia

Les fonctionnalités de Sprint 3 :

Fonctionnalités	Validation
Installation automatique des agents de supervision et déclaration des nouveaux éléments dans l'outil de supervision ✓ Installation et configuration ansible ✓ Installation des API d'eyes of network ✓ Sécurisation de transfert des clés ✓ Ecrire un playbook permettant la configuration automatique de protocole snmp ✓ Ecrire un script php permettant l'ajout de machines ✓ Ecrire le fichier playbook contenant le script de l'ajout des machines	OUI

2.5 Rétrospectives

Durant notre dernière réunion de rétrospectives, nous avons cité les problèmes rencontrés
Nous sommes bloqués au niveau automatisation d'ajout de machines et nous avons résolu le problème avec la création de la page web dynamique et le script bash.

2.6 Burndown chart

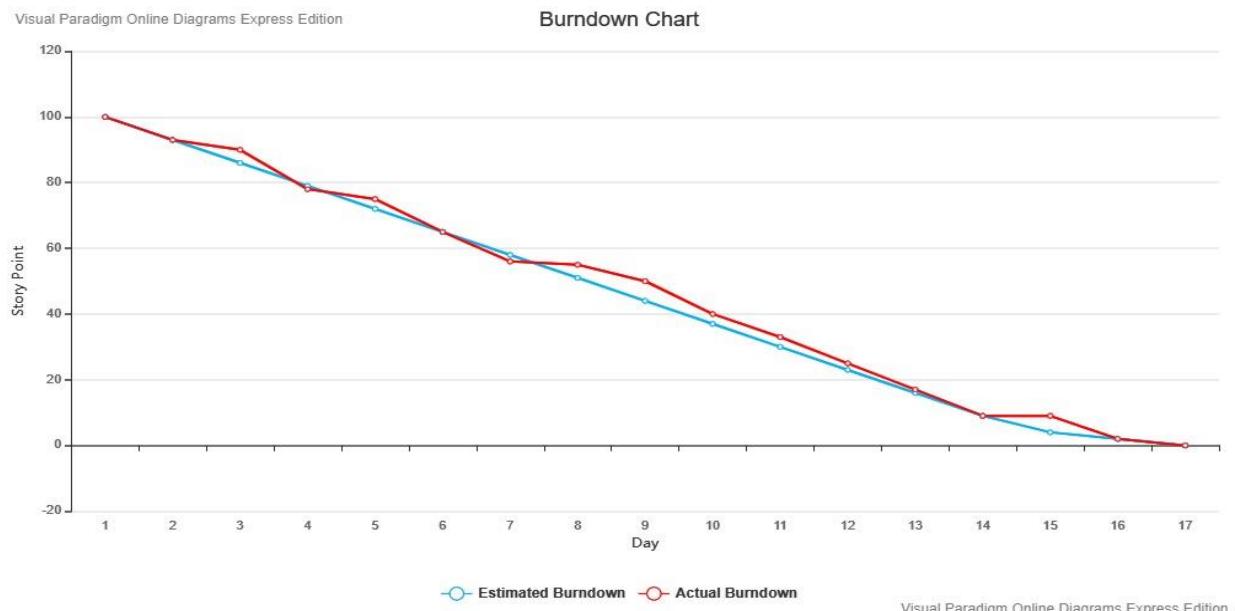


Figure 101 : Burndown chart de sprint 3

Au niveau de la courbe, nous remarquons un avancement dans la première semaine puis un peu de retard la deuxième. Finalement nous avons passé les problèmes rencontrés au niveau d'automatisation d'ajout des machines.

Conclusion

Dans ce dernier chapitre, nous avons installé ansible pour l'automatisation de la configuration du protocole smtp et de la supervision des deux serveurs FTP et SMTP.

Annexe A: Installation VMware ESXi

1. Installation de VMware ESXi sur VMware Workstation

Pour créer une nouvelle machine, dans le menu supérieur sous « File » il faut sélectionner « New Virtual Machine... »

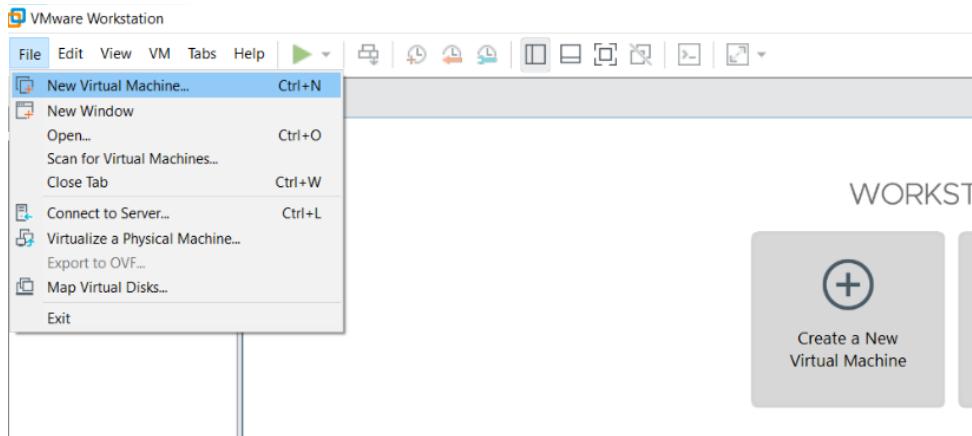


Figure 102 : Ajout d'une nouvelle machine virtuelle

Sur la première page, nous laissons « Typical » coché puis nous cliquons sur « Next »



Figure 103 : Choix du type de configuration de la machine

Sur la page suivante, nous devons cocher « Installer disc image file (iso) ». Ensuite il faut choisir l'emplacement de l'image de la machine virtuelle

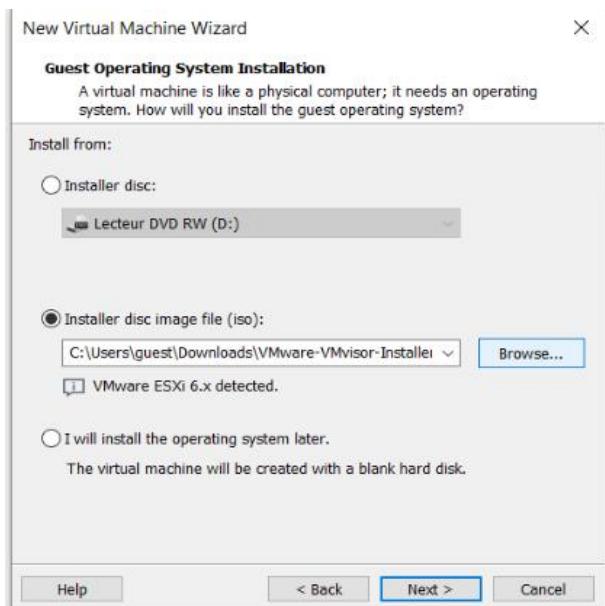


Figure 104 : Choix de l'emplacement de l'image iso

Maintenant il faut donner un nom pour la machine virtuelle ajoutée

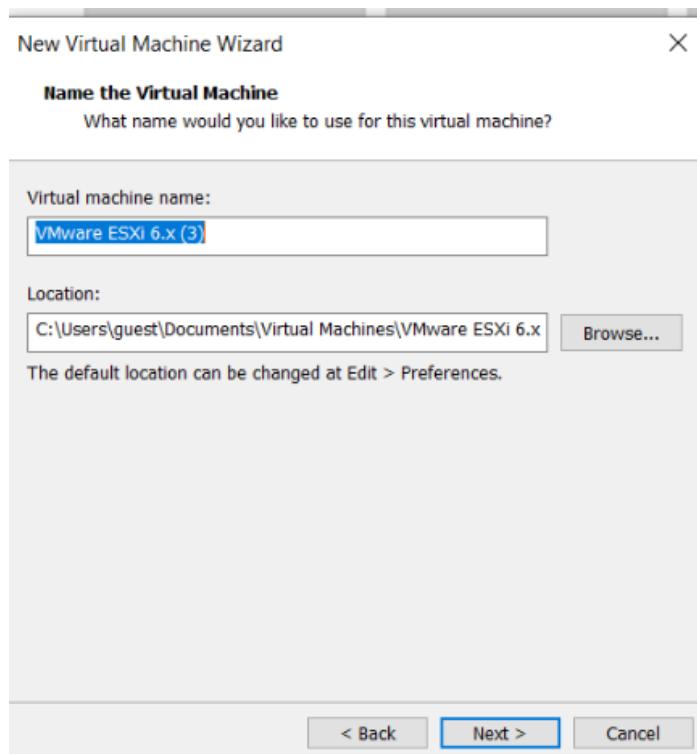


Figure 105 : Choix du nom et de l'emplacement de la machine virtuelle

Ensuite nous spécifions la capacité du disque de la machine virtuelle

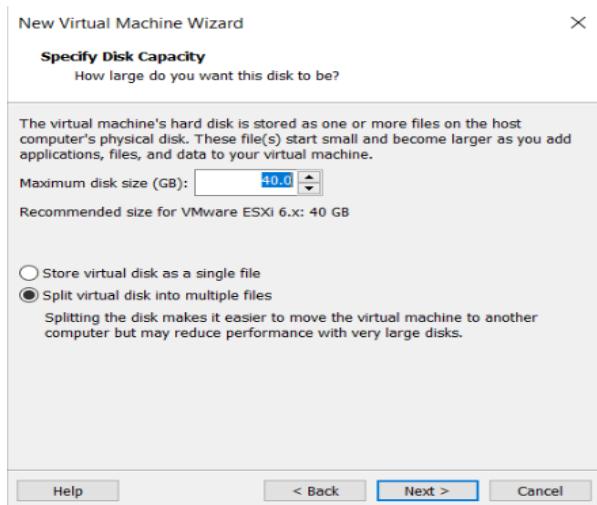


Figure 106 : Choix de la capacité du disque de la machine virtuelle

Nous arrivons sur un récapitulatif de notre machine. Pour terminer la création de VM nous devons cliquez sur « Finish »

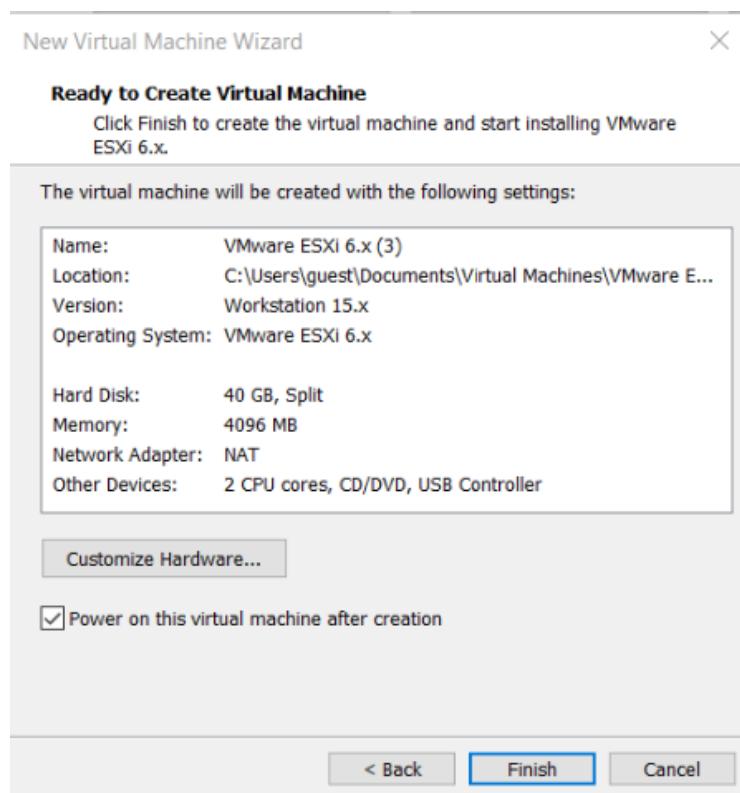


Figure 107 : Validation de la création de la machine

Ensuite nous devons démarrer la machine virtuelle ajoutée

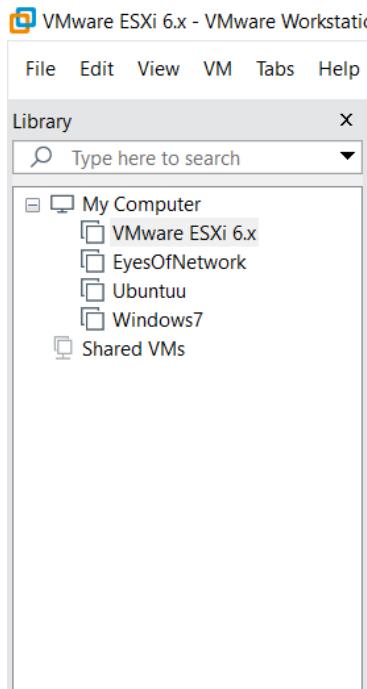
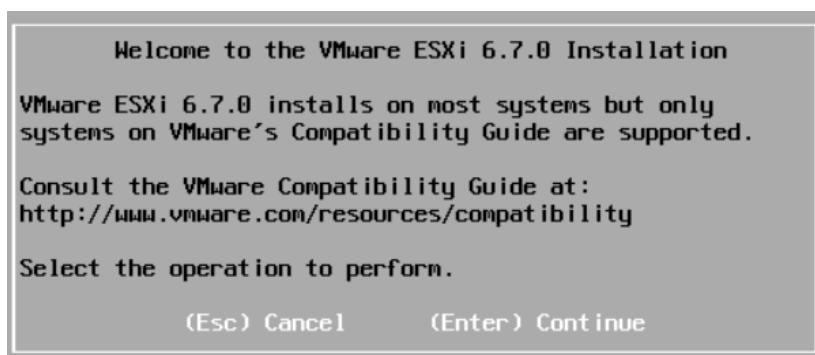


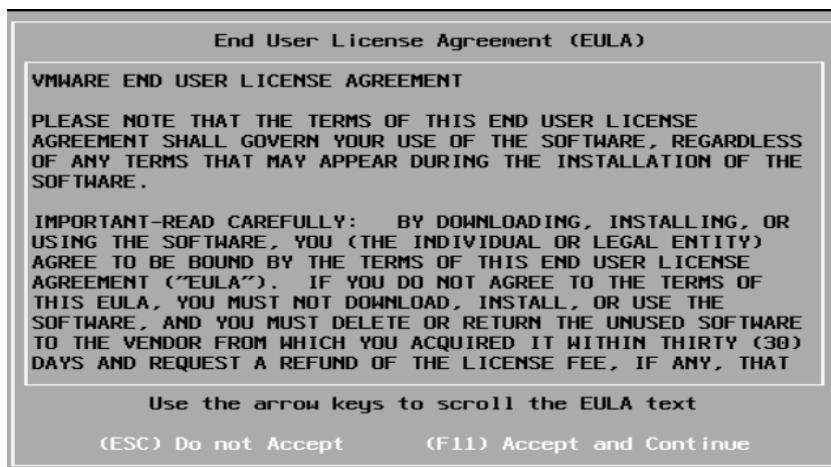
Figure 108 : Liste des machines virtuelles de VMware Workstation

Après le chargement de l'ISO, nous arrivons à cette page

Pour continuer, nous cliquons sur « Continue »



Ensuite nous cliquons sur F11 pour accepter les termes du contrat de licence



Le disque de 40 GB renseignée lors de la configuration de la VM apparaît.
Pour continuer il faut cliquer sur Enter

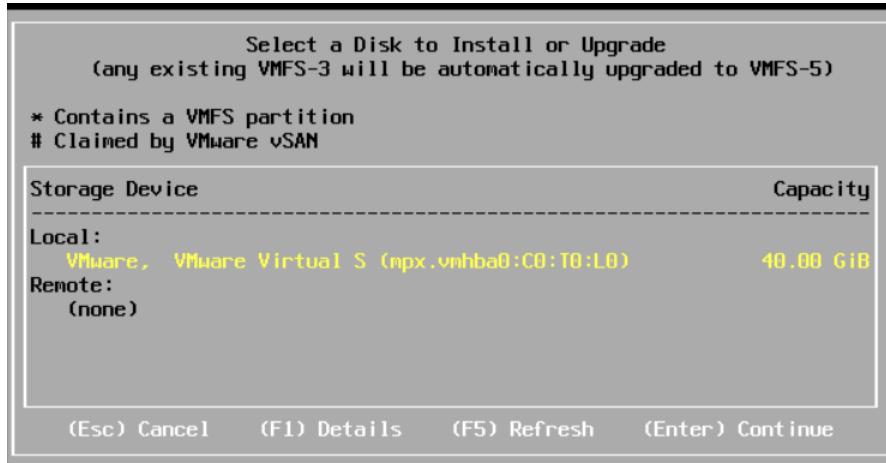


Figure 109 : Choix du disque pour l'installation

Une nouvelle fenêtre s'affiche, nous indique de sélectionner la langue du clavier souhaitée

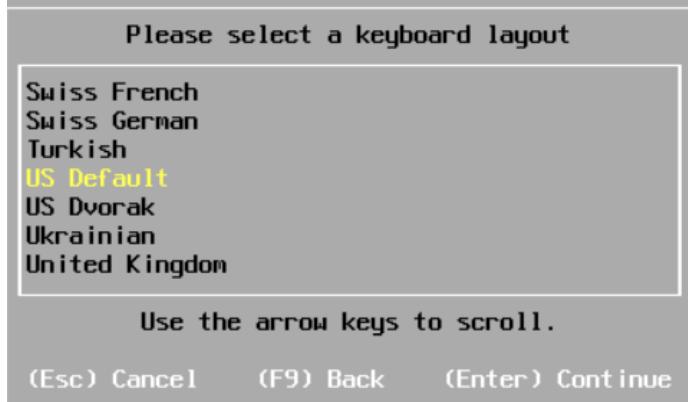


Figure 110 : Choix de la langue

Nous choisissons un mot de passe root



Figure 111 : Definition du mot de passe

Nous devons cliquer sur F11 pour démarrer l'installation

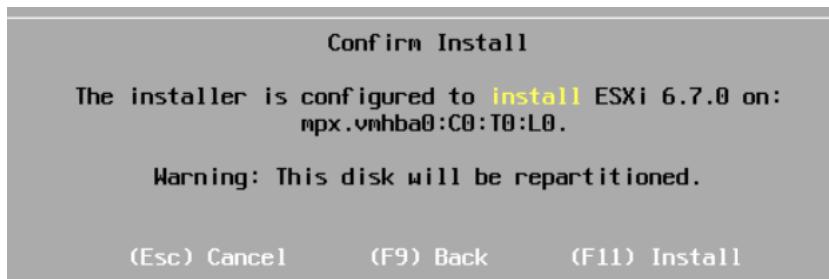


Figure 112 : Confirmation de l'installation

Une fois l'installation est terminée, nous devons redémarrer, donc il faut cliquer sur Reboot



Figure 113 : Redémarrage du serveur

Après le redémarrage, la machine virtuelle VMware ESXI démarre et nous pouvons l'utiliser



Figure 114 : Démarrage de la machine virtuelle VMware ESXi

ANNEXE B : Configuration snmp

2. Configuration SNMP de VMware ESXi

Pour pouvoir configurer SNMP sur le serveur VMWare ESXi nous devons tout d'abord activer le service SSH

Pour cela il faut accéder au menu de gestion puis l'onglet services, faire un clic droit sur le service TSM-SSH et cliquer sur démarrer

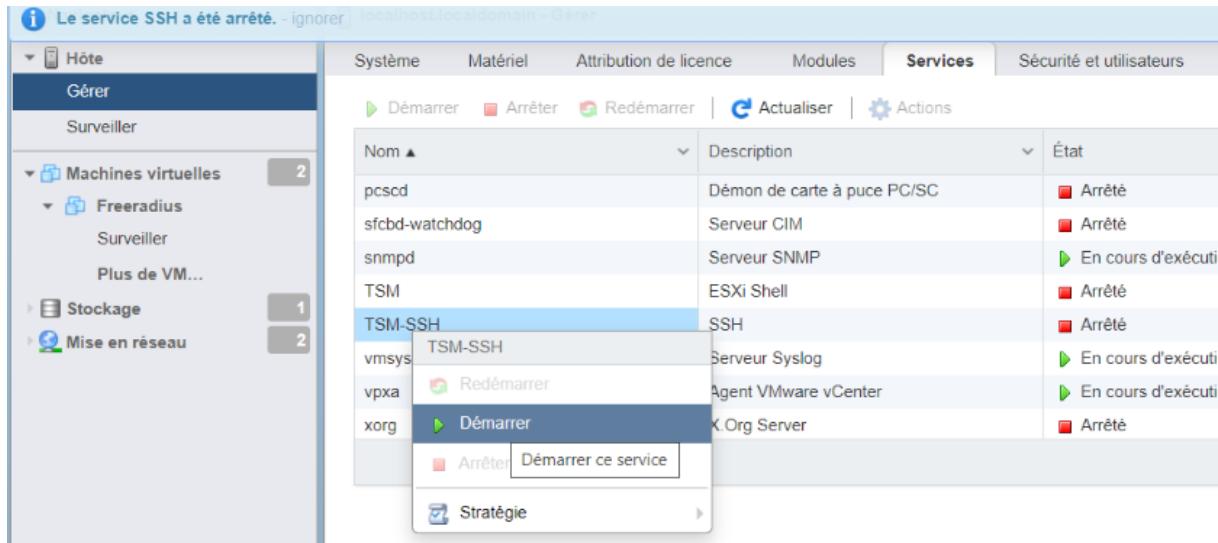


Figure 115 : Démarrage du service SSH

Nous pouvons maintenant accéder à ce serveur par le biais de SSH en utilisant le logiciel open source PuTTY sur notre machine Windows.

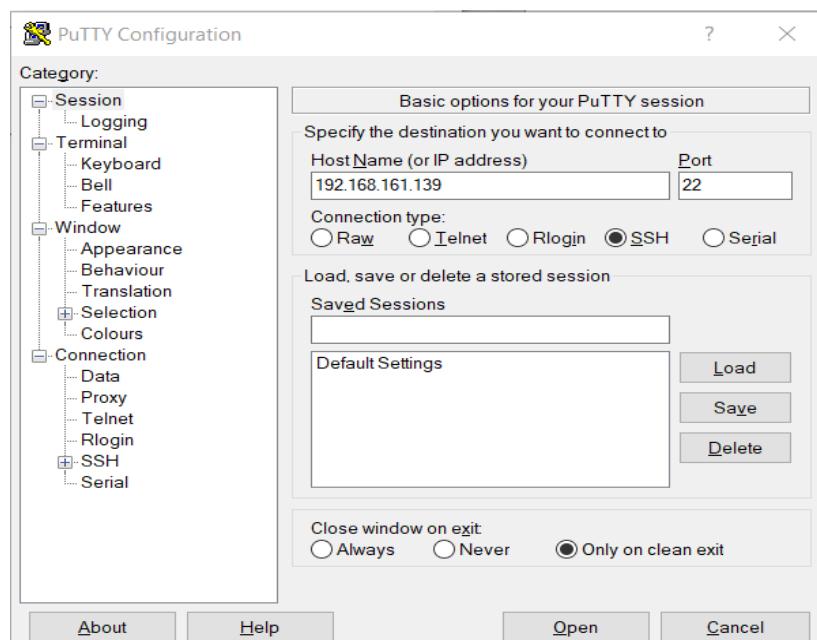
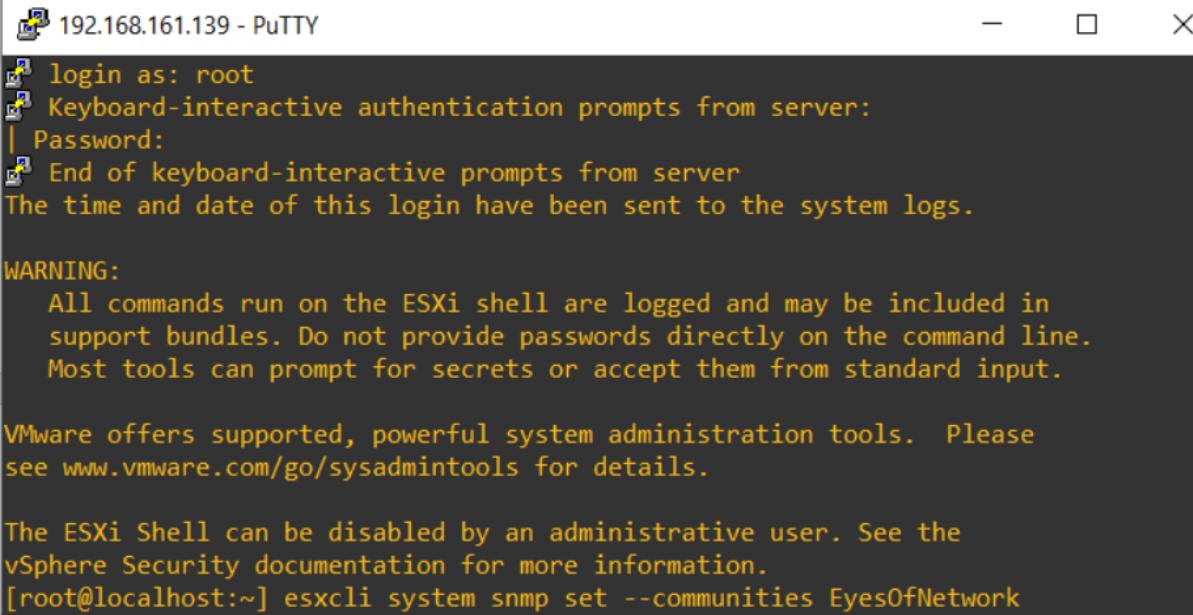


Figure 116 : Accès à VMWARE ESXI à distance avec putty

Une nouvelle fenêtre apparaît qui nous indique de taper le nom d'utilisateur et le mot de passe pour avoir l'accès à la ligne de commande de la console

Après une connexion réussie nous utilisons les commandes ci-dessous pour la configuration nécessaire



```
192.168.161.139 - PuTTY

login as: root
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
The time and date of this login have been sent to the system logs.

WARNING:
All commands run on the ESXi shell are logged and may be included in
support bundles. Do not provide passwords directly on the command line.
Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~] esxcli system snmp set --communities EyesOfNetwork
```

Figure 117: Configuration SNMP de VMWARE ESXI

La communauté EyesOfNetwork dispose une autorisation en lecture seule sur le serveur VMware ESXi

Et enfin nous devons activer SNMP

```
[root@localhost:~] esxcli system snmp set --enable true
```

3. Installation et configuration de l'agent SNMP de Windows

Pour installer l'agent Microsoft SNMP sur Windows 7, nous devons accéder au panneau de contrôle et cliquer sur Programmes

Une nouvelle liste s'affiche, nous devons choisir programmes et fonctionnalités

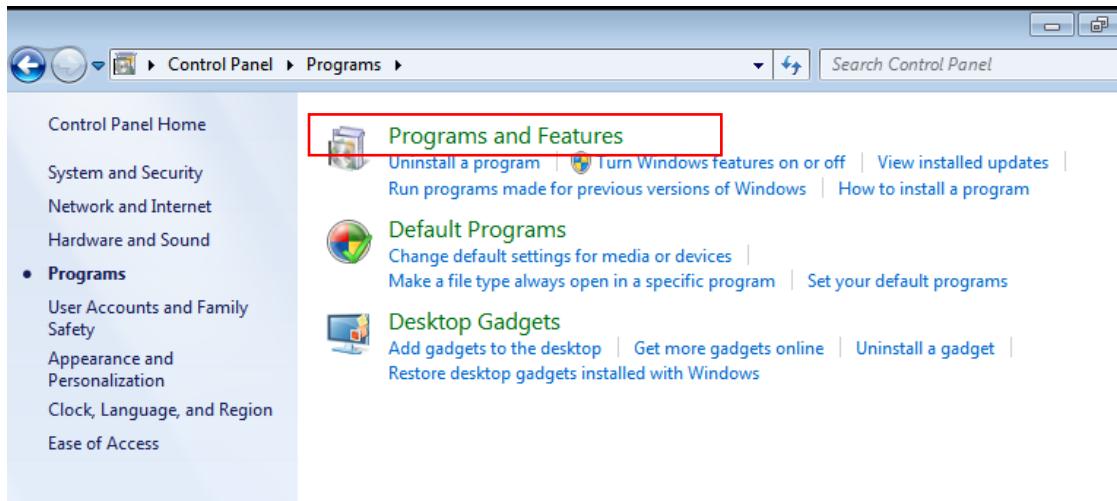


Figure 118 : Selection menu Programmes

Puis cliquer sur Activer ou désactiver des fonctionnalités Windows situé dans la liste à gauche

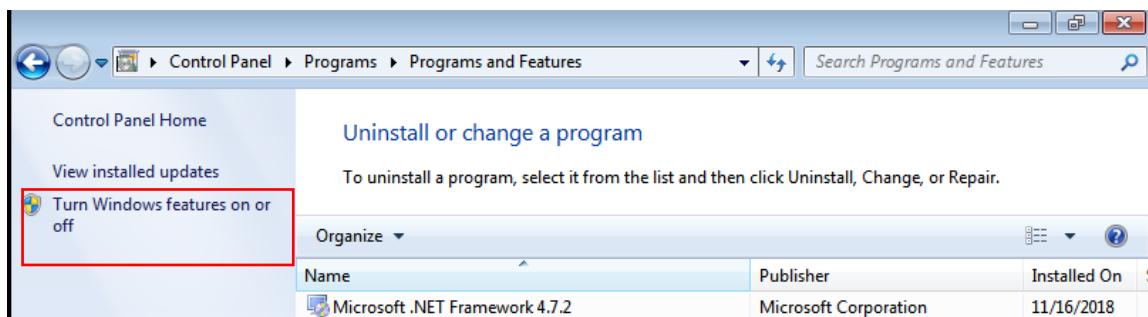


Figure 119 : Selection menu Programmes et fonctionnalités

Dans la liste des fonctionnalités affichée, il faut cocher la case Protocole SNMP, ceci est nécessaire pour installer l'agent SNMP et d'autres services SNMP.

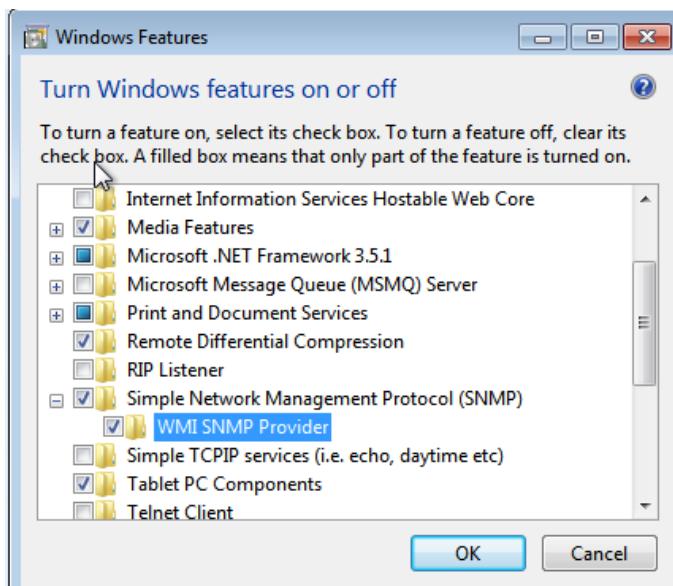


Figure 120 : Activation du protocole SNMP

Il est normalement inutile d'avoir le fournisseur SNMP WMI. Le composant fournisseur de SNMP WMI permet aux applications WMI d'accéder aux informations SNMP (Simple Network Management) à travers WMI (Windows Management Instrumentation).

Pour modifier la communauté SNMP sur un hôte Windows il faut se rendre sur la page des services Windows. Pour ce faire nous devons taper « service » dans le menu démarré.

D'où Le programme « services » devrait apparaître.

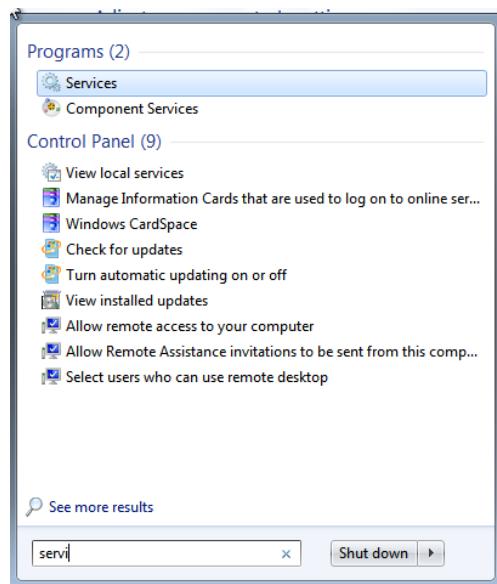


Figure 121 : Accès aux services de Windows

Finalement, nous devons sélectionner l'icône des Services puis double cliquer sur le service SNMP dans la liste des services

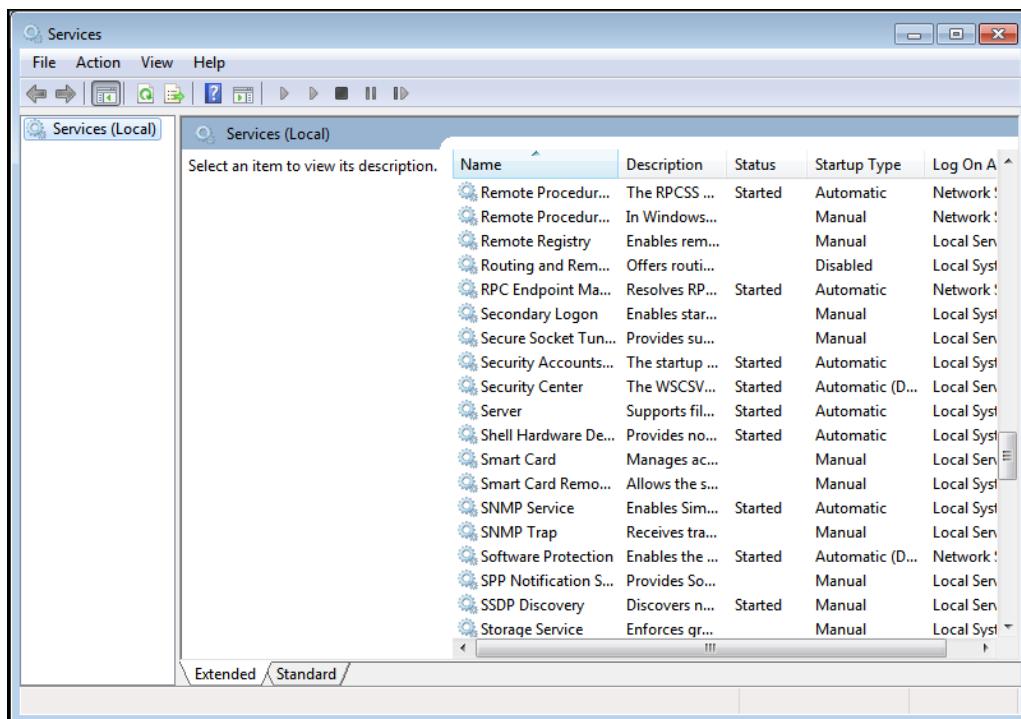


Figure 122 : Liste des services Windows

La fenêtre de propriétés de service SNMP est affichée

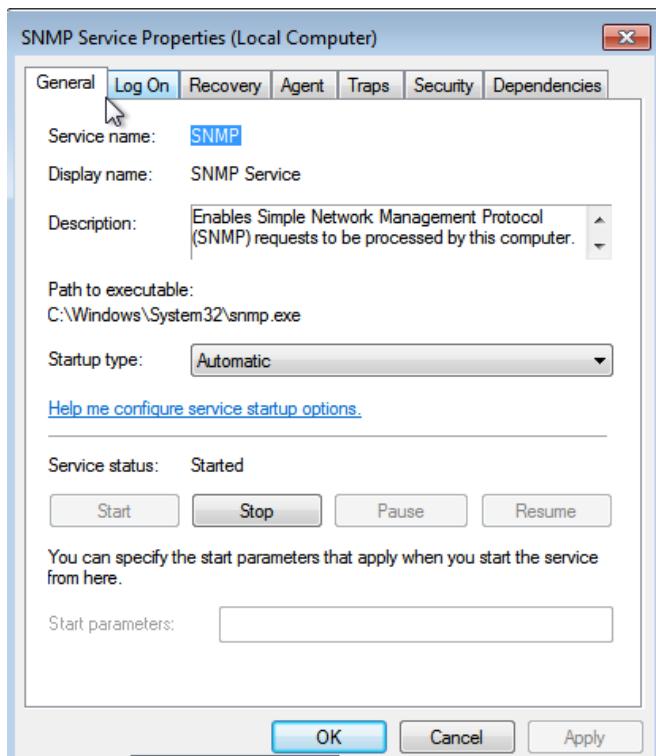


Figure 123 : Les propriétés du service SNMP

Ensuite, nous allons accéder à l'onglet sécurité « Sécurité »

Normalement, il ne devrait y avoir qu'un seul hôte SNMP de configuré (le localhost).

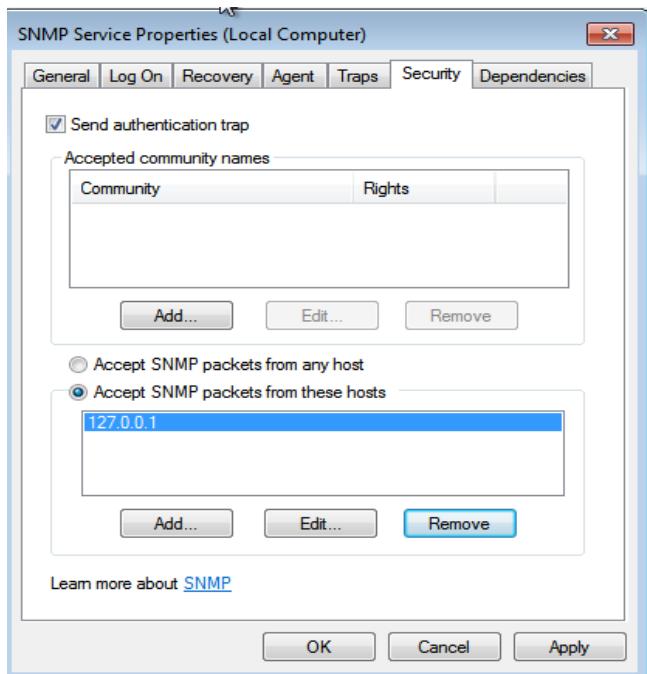


Figure 124 : Les informations de sécurité du service SNMP

Pour configurer la communauté SNMP, il faut cliquer sur « Ajouter... », La fenêtre de « Configuration de service SNMP » va s'ouvrir. C'est là que nous allons renseigner le nom de communauté SNMP souhaité, ainsi que les « Droits de communauté » qu'il faudra configurer en « LECTURE CREATION »

- . Une fois, la configuration terminée, cliquez sur « Ajouter ».

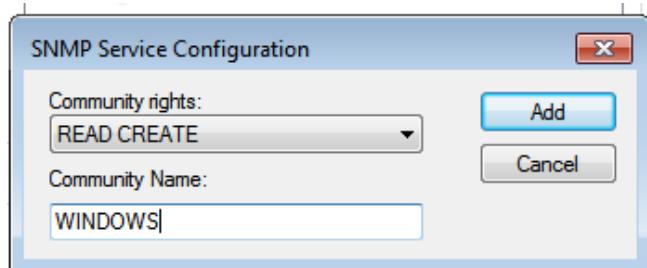


Figure 125 : Ajout du nom de la communauté

Puis nous devons cliquer sur le second bouton « Ajouter... » Qui va nous ouvrir à nouveau la fenêtre « Configuration du service SNMP » mais cette fois pour configurer l'adresse du serveur Nagios. Une fois, l'adresse de notre serveur Nagios saisie, il faut cliquer sur « Ajouter ».

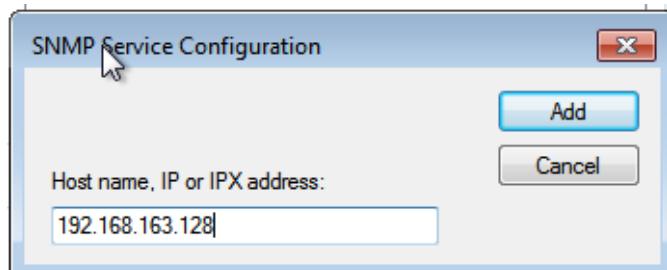


Figure 126 : Ajout de l'adresse IP du serveur

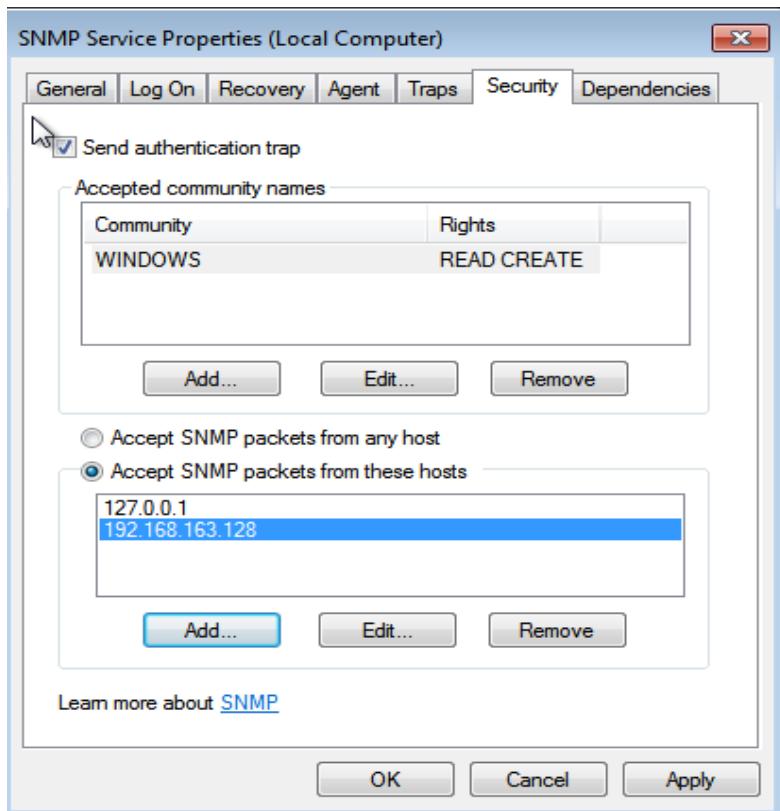


Figure 127 : Ajout de l'adresse du serveur avec succès

Pour terminer, nous devons cliquer sur « Appliquer » puis « OK ».

Le service SNMP de notre hôte Windows est maintenant configuré, il va à présent pouvoir être supervisé par Nagios.

3.1 Installation et configuration de l'agent SNMP de CentOS 7

Pour installer le service SNMPPD nous devons exécuter la commande ci-dessous

```
[root@localhost ~]# yum install net-snmp net-snmpd-utils
Loaded plugins: fastestmirror, langpacks,
               : priorities
Loading mirror speeds from cached hostfile
 * base: centos.mirror.garr.it
 * epel: mirrors.n-ix.net
 * extras: centos.mirror.fr.planethoster.net
 * remi-php70: fr2.rpmfind.net
 * remi-php71: fr2.rpmfind.net
 * remi-php72: fr2.rpmfind.net
 * remi-php73: fr2.rpmfind.net
 * remi-safe: fr2.rpmfind.net
 * updates: centos.mirror.ate.info
 * webstatic: uk.repo.webstatic.com
No package net-snmpd-utils available.
Resolving Dependencies
--> Running transaction check
--> Package net-snmp.x86_64 1:5.7.2-43.el7_7.3 will be installed
--> Processing Dependency: net-snmp-libs = 1:5.7.2-43.el7_7.3 for package: 1:net-snmp-5.7.2-43.el7_7.3.x86_64
--> Processing Dependency: net-snmp-agent-libs = 1:5.7.2-43.el7_7.3 for package: 1:net-snmp-5.7.2-43.el7_7.3.x86_64
--> Processing Dependency: libnetsnmptrapd.so.31()(64bit) for package: 1:net-snmp-5.7.2-43.el7_7.3.x86_64
--> Processing Dependency: libnetsnmpmibs.so.31()(64bit) for package: 1:net-snmp-5.7.2-43.el7_7.3.x86_64
--> Processing Dependency: libnetsnmpagent.so.31()(64bit) for package: 1:net-snmp-5.7.2-43.el7_7.3.x86_64
--> Running transaction check
--> Package net-snmp-agent-libs.x86_64 1:5.7.2-43.el7_7.3 will be installed
--> Package net-snmp-libs.x86_64 1:5.7.2-43.el7 will be updated
```

Figure 128 : Installation du service snmpd

Nous devons également démarrer le service SNMP manuellement et vérifier son état

```
[root@localhost ~]# systemctl start snmpd
[root@localhost ~]# systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset: disabled)
     Active: active (running) since Wed 2020-03-25 02:38:37 CET; 2s ago
       Main PID: 3863 (snmpd)
          Tasks: 1
         CGroup: /system.slice/snmpd.service
             └─3863 /usr/sbin/snmpd -L$0-6d -f

Mar 25 02:38:36 localhost.localdomain systemd[1]: ...
Mar 25 02:38:37 localhost.localdomain snmpd[3863]: ...
Mar 25 02:38:37 localhost.localdomain systemd[1]: ...
Hint: Some lines were ellipsized, use -l to show in full.
```

Figure 129 : Démarrage et statut du service snmp

Et maintenant, nous allons accéder au fichier de configuration /etc/snmp/snmpd.conf

```
# By default, the agent responds to the "public" community for read
# only access, if run out of the box without any configuration file in
# place. The following examples show you other ways of configuring
# the agent so that you can change the community names, and give
# yourself write access to the mib tree as well.
#
# For more information, read the FAQ as well as the snmpd.conf(5)
# manual page.

#####
# First, map the community name "public" into a "security name"

#      sec.name    source        community
com2sec notConfigUser  default      public

#####
# Second, map the security name into a group name:

#      groupName    securityModel securityName
group    notConfigGroup v1           notConfigUser
group    notConfigGroup v2c          notConfigUser

#####
# Third, create a view for us to let the group have rights to:

-- INSERT --
```

41,44

5%

Figure 130 : Edition du fichier /etc/snmp/snmpd.conf

Nous allons changer la "communauté". La communauté est une sorte de "mot de passe" qui va permettre de restreindre l'accès aux informations fournis par le serveur SNMP. Par défaut, cette communauté est généralement "public", c'est pourquoi il est recommandé de changer, autrement, n'importe qui dans notre réseau pourra alors questionner notre serveur sur leurs

états de santé, nous avons donc remplacé "public", par "EyesOfNetwork" comme le montre la figure ci-dessous :

```
# By far, the most common question I get about the agent is "why won't
# it work?", when really it should be "how do I configure the agent to
# allow me to access it?"
#
# By default, the agent responds to the "public" community for read
# only access, if run out of the box without any configuration file in
# place. The following examples show you other ways of configuring
# the agent so that you can change the community names, and give
# yourself write access to the mib tree as well.
#
# For more information, read the FAQ as well as the snmpd.conf(5)
# manual page.

#####
# First, map the community name "public" into a "security name"

#      sec.name    source        community
com2sec notConfigUser  default      EyesOfNetwork

#####
# Second, map the security name into a group name:

#      groupName      securityModel securityName
group   notConfigGroup v1            notConfigUser
group   notConfigGroup v2c           notConfigUser
```

Il est également nécessaire de corriger les lignes 55 et 56 pour qu'elles ressemblent à cela :

```
# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#      name          incl/excl    subtree        mask(optional)
view   systemview   included     .1.3.6.1.2.1
view   systemview   included     .1.3.6.1.2.1.25.1

#####
```

Le texte ci-dessus est noté avec des informations de base sur la fonction de chaque ligne de configuration. En bref, nous créons ces scénarios pour l'interrogation.

AllUser est affecté à AllGroup et ne peut utiliser que le modèle de sécurité SNMP 2c. AllGroup peut utiliser AllView. AllView est affecté à l'arborescence OID entière, et tout cela est référencé dans un sondage SNMP par la chaîne de communauté secrète et unique EyesOfNetwork.

Après avoir terminé les modifications nécessaires au niveau du fichier de configurations, nous devons redémarrer le service SNMP pour recharger le nouveau fichier de configuration.

7.1 Installation et configuration de l'agent SNMP d'Ubuntu

Sur la console Linux, nous devons utiliser la commande suivante pour installer les services requis.

```
root@ubuntu:~# apt-get install snmp snmpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 131 : Installation de l'agent snmp

Pour connaître l'état du service snmpd nous pouvons utiliser la commande ci-dessous :

```
root@ubuntu:~# systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon
  Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; ven
  Active: active (running) since Sat 2020-03-28 18:50:00 PDT; 25m
    Main PID: 3092 (snmpd)
      Tasks: 1 (limit: 2293)
     CGroup: /system.slice/snmpd.service
             └─3092 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmpd
```

Figure 132 : Le statut du service snmpd

Le service est lancé et fonctionnel

Nous allons maintenant faire l'installation de MIB

Pour des raisons de licence, le package net-snmp installe uniquement un petit nombre de MIB dans le répertoire

/usr/share/mibs. Un grand nombre de MIB standard peut être installé à l'aide du package snmp-mibs-downloader, d'où nous allons utiliser la commande ci-dessous :

```
root@ubuntu:~# sudo apt-get install snmp-mibs-downloader
Reading package lists... Done
```

Figure 133 : Installation des mibs

Ensuite, il faut accéder au fichier de configuration /etc/snmp/snmpd.conf en tapant la commande suivante :

```
root@ubuntu:~# nano /etc/snmp/snmpd.conf
u:~# gedit /etc/snmp/snmpd.conf
```

Actuellement, le Snmpd est configuré pour n'autoriser que les connexions provenant de l'ordinateur local.

Nous devons commenter la ligne actuelle et dés commenter la ligne en dessous pour autoriser toutes les connexions.

```

# Listen for connections from the local system only
#agentAddress udp:127.0.0.1:161
# Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161

```

Figure 134 : Edition du fichier /etc/snmp/snmpd.conf 2

Et enfin, pour autoriser l'accès en lecture des données SNMP à un hôte spécifique nous devons taper la chaîne communauté dans notre cas nous avons choisi « EyesOfNetwork » suivie de l'adresse de notre serveur :

```

#
# ACCESS CONTROL
#
#                                     # system +
hrSystem groups only
view    systemonly included     .1.3.6.1.2.1.1
view    systemonly included     .1.3.6.1.2.1.25.1
                                         # Full access
from the local host
rocommunity EyesOfNetwork  192.168.163.130|          # Default access
to basic system info
#rocommunity public default      -V systemonly
.. . .

```

Puis, pour enregistrer les modifications, il faut redémarrer le service « snmpd » grâce à la commande :

Service snmpd restart.

ANNEXE C : Installation FreeRADIUS sur Ubuntu 18.04

Tout d'abord, nous devons mettre à jour notre cache :

```
root@freeradius-virtual-machine:~# apt-get update
Atteint :1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Atteint :2 http://tn.archive.ubuntu.com/ubuntu bionic InRelease
Atteint :3 http://tn.archive.ubuntu.com/ubuntu bionic-updates InRelease
Atteint :4 http://tn.archive.ubuntu.com/ubuntu bionic-backports InRelease
Lecture des listes de paquets... Fait
```

Figure 135 : Mise à jour de la cache des paquets

, il faut installer FreeRADIUS et le service MySQL :

```
root@freeradius-virtual-machine:~# apt-get install freeradius freeradius-mysql
mysql-server mysql-client
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  freeradius-common freeradius-config freeradius-utils freetds-common libaio1
  libct4 libdbi-perl libevent-core-2.1-6 libfreeradius3 libhtml-template-perl
  libmysqlclient20 make mysql-client-5.7 mysql-client-core-5.7 mysql-common
  mysql-server-5.7 mysql-server-core-5.7
Paquets suggérés :
  freeradius-ldap freeradius-postgresql freeradius-krbs snmp libmldb perl
  libnet-daemon-perl libsql-statement-perl libipc-sharedcache-perl make-doc
  mailx tinyca
Les NOUVEAUX paquets suivants seront installés :
  freeradius freeradius-common freeradius-config freeradius-mysql
  freeradius-utils freetds-common libaio1 libct4 libdbi-perl
  libevent-core-2.1-6 libfreeradius3 libhtml-template-perl libmysqlclient20
  make mysql-client mysql-client-5.7 mysql-client-core-5.7 mysql-common
  mysql-server mysql-server-5.7 mysql-server-core-5.7
0 mis à jour, 21 nouvellement installés, 0 à enlever et 212 non mis à jour.
Il est nécessaire de prendre 22.0 Mo dans les archives.
Après cette opération, 167 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://tn.archive.ubuntu.com/ubuntu bionic/main amd64 mysql-com
mon all 5.8+1.0.4 [7,308 B]
Réception de :2 http://tn.archive.ubuntu.com/ubuntu bionic-updates/main amd64 l
ibaio1 amd64 0.3.110-5ubuntu0.1 [6,476 B]
```

Figure 136 : Installation de freeradius et de la base de données mysql

Après avoir terminée l'installation, nous devons accéder au serveur de base de données MySQL afin de créer une base de données radius :

```
root@freeradius-virtual-machine:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.30-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE radius CHARACTER SET UTF8 COLLATE UTF8_BIN;
Query OK, 1 row affected (0.30 sec)
```

Figure 137 : création d'une nouvelle base de données

Ainsi qu'un utilisateur MySQL nommé radius et lui accorder tous les priviléges pour la base données radius récemment créée.

```

mysql> CREATE USER 'radius'@'%' IDENTIFIED BY 'kamisama123';
Query OK, 0 rows affected (0.54 sec)

mysql> GRANT ALL PRIVILEGES ON radius.* TO 'radius'@'%';
Query OK, 0 rows affected (0.05 sec)

mysql> QUIT;
Bye
root@freeradius-virtual-machine:~# 

```

Figure 138 : Attribution des privilèges

Nous devons par la suite mettre à jour la base de données par défaut, chercher l'emplacement du fichier schema.sql et importer le modèle de base de données radius dans le système de gestion de base de données MySQL, le système nous indique qu'il faut taper un mot de passe, il s'agit du mot de passe de l'utilisateur radius SQL.

```

root@freeradius-virtual-machine:~# updatedb
root@freeradius-virtual-machine:~# locate main/mysql/schema.sql | grep freeradius
/etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql
root@freeradius-virtual-machine:~# mysql -u radius -p radius < /etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql
Enter password: 

```

Figure 139 : Mise à jour et importation de la base de données

Et enfin pour terminer l'installation, il faut créer un lien symbolique afin d'activer le module freeradius MySQL :

```

root@freeradius-virtual-machine:~# ln -s /etc/freeradius/3.0/mods-available/sql
/etc/freeradius/3.0/mods-enabled/

```

- Installation de Dalaradius**

Pour gérer le serveur radius à partir d'une interface web, nous allons installer l'outil d'administration web Dalaradius, nous commençons donc par l'installation du serveur web apache, PHP et d'autres packages requis à notre système en utilisant les commandes ci-dessous :

```

root@freeradius-virtual-machine:~# apt-get install apache2 php libapache2-mod-php5
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
unzip est déjà la version la plus récente (6.0-21ubuntu1).
unzip passé en « installé manuellement ».
Les paquets supplémentaires suivants seront installés :
  apache2-bin apache2-data apache2-utils libapache2-mod-php7.2 libapr1
  libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 php-common
  php7.2 php7.2-cli php7.2-common php7.2-json php7.2-mysql php7.2-opcache
  php7.2-readline
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php
  libapache2-mod-php7.2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.2-0 php php-common php-mysql php7.2 php7.2-cli
  php7.2-common php7.2-json php7.2-mysql php7.2-opcache php7.2-readline
0 mis à jour, 21 nouvellement installés, 0 à enlever et 210 non mis à jour.
Il est nécessaire de prendre 5,702 ko dans les archives.
Après cette opération, 24.6 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://tn.archive.ubuntu.com/ubuntu/bionic/main amd64 libapr1
md64 1.6.3-2 [90.9 kB]
Réception de :2 http://tn.archive.ubuntu.com/ubuntu/bionic/main amd64 libaprutil1

```

Figure 140 : Installation apache, php et d'autres packages

```

root@freeradius-virtual-machine:~# apt-get install php-pear php-db php-mail php
-gd php-common php-mail-mime
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
php-common est déjà la version la plus récente (1:60ubuntu1).
php-common passé en « installé manuellement ».
Les paquets supplémentaires suivants seront installés :
  php-auth-sasl php-mbstring php-net-smtp php-net-socket php-xml php7.2-gd
  php7.2-mbstring php7.2-xml
Les NOUVEAUX paquets suivants seront installés :
  php-auth-sasl php-db php-gd php-mail php-mail-mime php-mbstring
  php-net-smtp php-net-socket php-pear php-xml php7.2-gd php7.2-mbstring
  php7.2-xml
0 mis à jour, 13 nouvellement installés, 0 à enlever et 210 non mis à jour.
Il est nécessaire de prendre 1,074 ko dans les archives.
Après cette opération, 5,531 ko d'espace disque supplémentaires seront utilisés
.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://tn.archive.ubuntu.com/ubuntu bionic-updates/main amd64 p
hp7.2-xml amd64 7.2.24-0ubuntu0.18.04.6 [107 kB]
Réception de :2 http://tn.archive.ubuntu.com/ubuntu bionic/universe amd64 php-x
ml all 1:7.2+60ubuntu1 [2,024 B]
Réception de :3 http://tn.archive.ubuntu.com/ubuntu bionic-updates/main amd64 p
hp-pear all 1:1.10.5+submodules+notgz-1ubuntu1.18.04.1 [284 kB]
Réception de :4 http://tn.archive.ubuntu.com/ubuntu bionic/universe amd64 php-a ..
```

Par ailleurs il faut télécharger, extraire daloradius et l'enregistrer dans un dossier nouvellement créé :

```

root@freeradius-virtual-machine:~# mkdir /downloads/daloradius -p
root@freeradius-virtual-machine:~# cd /downloads/daloradius
root@freeradius-virtual-machine:/downloads/daloradius# wget https://github.com/
lirantal/daloradius/archive/master.zip
--2020-06-12 15:07:05-- https://github.com/lirantal/daloradius/archive/master.
zip
Résolution de github.com (github.com)... 140.82.118.3
Connexion à github.com (github.com)|140.82.118.3|:443... connecté.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://codeload.github.com/lirantal/daloradius/zip/master [suiva
nt]
--2020-06-12 15:07:06-- https://codeload.github.com/lirantal/daloradius/zip/ma
ster
Résolution de codeload.github.com (codeload.github.com)... 140.82.114.9
Connexion à codeload.github.com (codeload.github.com)|140.82.114.9|:443... connec
té.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : non indiqué [application/zip]
Enregistre : «master.zip»
master.zip          [          =>          ]  4.47M  287KB/s
```



```

root@freeradius-virtual-machine:/downloads/daloradius# unzip master.zip
Archive: master.zip
909ec0ac3271f58e36847ef4d176b5c17416a43e
  creating: daloradius-master/
  extracting: daloradius-master/.gitignore
  inflating: daloradius-master/.htaccess
  inflating: daloradius-master/.htpasswd
  inflating: daloradius-master/ChangeLog
  inflating: daloradius-master/Dockerfile
  inflating: daloradius-master/Dockerfile-freeradius
  inflating: daloradius-master/FAQS
  inflating: daloradius-master/INSTALL
  inflating: daloradius-master/INSTALL.opensUSE
  inflating: daloradius-master/INSTALL.quick
  inflating: daloradius-master/INSTALL.win
  inflating: daloradius-master/LICENSE
  inflating: daloradius-master/README.md
  inflating: daloradius-master/acct-active.php
  inflating: daloradius-master/acct-all.php
  inflating: daloradius-master/acct-custom-query.php
  inflating: daloradius-master/acct-custom.php
```

Puis déplacer le répertoire nouvellement décompressé sous le répertoire du serveur web apache :

```
root@freeradius-virtual-machine:/downloads/daloradius# mv daloradius-master /var/www/html/daloradius  
root@freeradius-virtual-machine:/downloads/daloradius#
```

En outre, nous utilisons les commandes ci-dessous pour importer les tables MySQL daloradius dans la base de données MySQL freeradius.

Le système demande d'entrer un mot de passe, il s'agit de celui de l'utilisateur récemment créé :

```
root@freeradius-virtual-machine:/var/www/html/daloradius/contrib/db# mysql -u r  
adius -p radius < fr2-mysql-daloradius-and-freeradius.sql  
Enter password:
```

```
root@freeradius-virtual-machine:/downloads/daloradius# cd /var/www/html/daloradius/contrib/db
```

Nous devons par la suite éditer le fichier de configuration daloradius.conf.php en ajoutant l'utilisateur, le mot de passe et le nom de la base de données radius récemment créé.

```
root@freeradius-virtual-machine:/var/www/html/daloradius/contrib/db# mysql -u r  
adius -p radius < mysql-daloradius.sql  
Enter password:
```

```
lus.comn.php  
root@freeradius-virtual-machine:~# vim /var/www/html/daloradius/library/dalorad  
ius.conf.php  
root@freeradius-virtual-machine:~#  
  
$configValues['CONFIG_DB_HOST'] = 'localhost';  
$configValues['CONFIG_DB_PORT'] = '3306';  
$configValues['CONFIG_DB_USER'] = 'radius';  
$configValues['CONFIG_DB_PASS'] = 'rsi3';  
$configValues['CONFIG_DB_NAME'] = 'radius';  
$configValues['CONFIG_DB_CHARSET'] = 'utf8';  
$configValues['CONFIG_DB_COLLATION'] = 'utf8_general_ci';  
$configValues['CONFIG_DB_SOCKET'] = '';
```

Figure 141 : Edition du fichier de configuration daloradius.conf.php

Ensuite, nous devons définir le propriétaire / le groupe de la racine web d'une manière récursive sur tous les fichiers et répertoires sous le répertoire donné et pour s'assurer que tout fonctionne il faut redémarrer les services apache et freeradius.

```
root@freeradius-virtual-machine:~# chown www-data.www-data /var/www/html/dalora  
dius/* -R  
root@freeradius-virtual-machine:~# service freeradius restart  
root@freeradius-virtual-machine:~# service apache2 restart  
root@freeradius-virtual-machine:~#
```

Figure 142 : Redémarrage des services freeradius et apache

L'installation est terminée, nous pouvons maintenant taper dans la barre d'adresse de notre navigateur : l'adresse IP de notre serveur web/daloradius.

L'interface web de dalaradius s'affiche, pour se connecter il faut taper le nom d'utilisateur administrator et le mot **passe radius qui sont par défaut.**

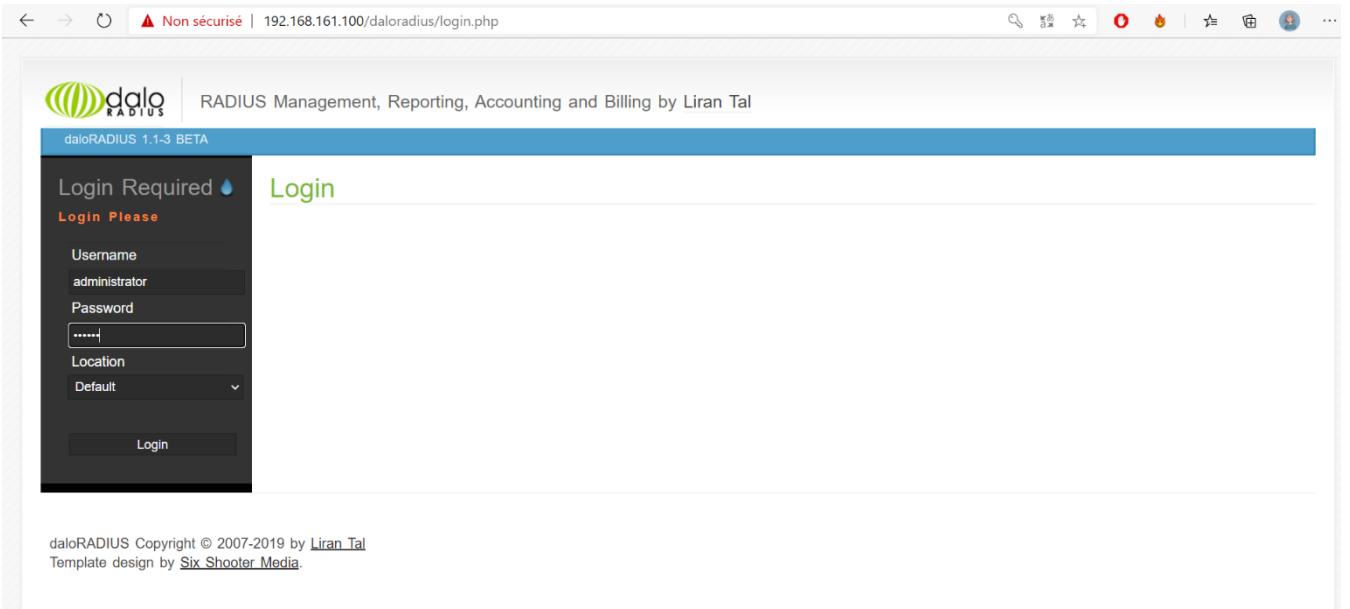


Figure 143: Interface web dalaradius

Après une connexion réussie le tableau de bord dalaradius s'affiche.

Conclusion générale

Ce présent rapport a été élaboré pour la validation de stage de fin d'études. Notre projet est réalisé à GlobalNet et qui consiste à implémenter une solution de supervision réseau avec automatisation.

L'objectif de notre travail est la surveillance en continue des systèmes d'information, l'optimisation de la disponibilité et la performance des équipements réseau, le gain du temps dans le diagnostic et la résolution des incidents et des pannes, la gestion des accès à un réseau grâce à l'authentification, la sécurité grâce à un réseau privé virtuel et la simplification d'effectuer des tâches répétitives grâce à l'automatisation.

Les étapes de la réalisation de notre projet ont porté sur l'étude et l'analyse de l'existant, l'état de l'art, la spécification des besoins des acteurs, la mise en place de l'outil de supervision Eyes Of Network, l'implémentation d'un réseau privé virtuel et d'un serveur d'authentification FreeRadius ainsi que l'automatisation de la supervision avec ansible.

Notre rapport de fin d'études s'est articulé en six chapitres.

Dans le premier chapitre, nous avons présenté l'organisme d'accueil, le contexte de notre projet ainsi que l'étude et la critique de l'existant dans GlobalNet.

Par la suite, nous avons annoncé la solution sur laquelle notre projet s'est basé. Ensuite, nous avons élaboré une étude comparative afin de mieux mettre en valeur notre projet. A la fin, nous avons clôturé par le choix méthodologique SCRUM que nous avons adopté.

Dans le deuxième chapitre, nous avons élaboré une analyse profonde afin de mieux cerner les besoins de GlobalNet. Au cours de ce chapitre, nous avons présenté les outils utilisés et des études comparatives pour mieux choisir.

Dans le troisième chapitre, nous avons présenté les spécifications des besoins. Au cours de ce chapitre nous avons commencé par une capture des besoins fonctionnels et non fonctionnels. Par la suite, nous avons présenté le backlog général, le diagramme de cas d'utilisation général ainsi que le diagramme d'activité et l'environnement de travail.

Et pour les trois derniers chapitres, mise en place de l'outil de supervision, Implémentation d'une connexion VPN et serveur d'authentification et automatisation de la supervision avec ansible, nous avons mis en valeur notre travail en détaillant les trois sprints, nous avons présenté les backlog des sprints correspondants, et nous avons clôturé par la réalisation.

De point de vue technique, ce stage nous a aidés à approfondir nos connaissances en informatique et de mettre dans ce projet nos acquis théoriques que nous avons appris durant les années d'études à l'Institut Supérieur Des Etudes Technologiques de Charguia.

En plus, cette expérience nous a permis de découvrir et de se familiariser avec l'environnement professionnel et nous a offert la possibilité de collaborer à l'égard du secteur de la technologie de l'information et approfondir nos connaissances.

En termes de perspectives, notre projet pourrait être amélioré en ajoutant l'automatisation de l'enregistrement de la configuration des routeurs (backup) au niveau du serveur FTP pour faire face aux pannes inattendues.

Nétographie

- [1] [En ligne]. Available: <https://www.redhat.com/fr/topics/automation/whats-it-automation>.
- [2] [En ligne]. Available: https://fr.wikibooks.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_informatiques/S%C3%A9curit%C3%A9_informatique/Chiffrement_de_flux_et_VPN.
- [3] [En ligne]. Available: <https://www.blogdumoderateur.com/scrum-kanban-scrumban-methode/>.
- [4] [En ligne]. Available: <https://www.supinfo.com/articles/single/2780-presentation-methode-scrum>.
- [5] [En ligne]. Available: <https://www.lucidchart.com/pages/fr/langage-uml>.
- [6] [En ligne]. Available: <https://www.nowteam.net/supervision-informatique-entreprise/>.
- [7] [En ligne]. Available: http://www-igm.univ-mlv.fr/~dr/XPOSE2007/dmichau_supervision/supervision.html.
- [8] [En ligne]. Available: <https://www.le-vpn.com/fr/cest-quoi-le-vpn-ou-reseau-prive-virtuel/>.
- [9] [En ligne]. Available: <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203415-vlan-virtual-local-area-network-definition-traduction/>.
- [10] [En ligne]. Available: <https://www.ipe.fr/quest-ce-que-lautomatisation-informatique/>.
- [11] [En ligne]. Available: <https://www.redhat.com/fr/topics/automation>.
- [12] [En ligne]. Available: <https://www.frameip.com/snmp/>.
- [13] [En ligne]. Available: <https://www.supinfo.com/articles/single/10150-protocole-securite-aaa>.
- [14] [En ligne]. Available: <https://web.maths.unsw.edu.au/~lafaye/CCM/authentification/radius.htm>.
- [15] [En ligne]. Available: <http://www.o00o.org/monitoring/solutions.html>.
- [16] [En ligne]. Available: <https://www.supinfo.com/articles/single/3124-comparaison-outils-supervison>.
- [17] [En ligne]. Available: <https://wiki.monitoring-fr.org/cacti/start>.
- [18] [En ligne]. Available: <https://www.journaldunet.fr/web-tech/guide-de-l-entreprise-collaborative/devops/>.
- [19] [En ligne]. Available: https://fr.wikipedia.org/wiki/VMware_Workstation_Pro.

- [20] [En ligne]. Available: <https://sites.google.com/site/plecorentin/portefeuille-de-competence/travaux-menes-au-cfai84/serveur>.
- [21] [En ligne]. Available: <https://www.lemagit.fr/tip/Puppet-contre-Ansible-le-face-a-face-de-la-gestion-des-configurations-et-de-DevOps>.
- [22] [En ligne]. Available: <https://whatis.techtarget.com/fr/definition/ESXi-VMware>.
- [23] [En ligne]. Available: <https://www.redhat.com/fr/topics/virtualization/what-is-virtualization>.
- [24] [En ligne]. Available: <https://www.educba.com/what-is-ansible/>.

ملخص

يندرج هذا العمل ضمن إطار نهاية الدراسات الذي تم في غلوبالنات للحصول على شهادة الإجازة التطبيقية في تكنولوجيات الإعلامية

يتتألف مشروعنا من تنفيذ بنية شبكة مع تنفيذ أداة مراقبة من أجل التدخل السريع لتصحيح الأعطال التي ووجهت، والتشغيل الآلي لزيادة الإنتاجية وتقليل تكاليف التشغيل، خاصة فيما يتعلق بالمهام المتكررة، التحكم في الوصول من خلال إنشاء شبكة ظاهرية خاصة وخادم مصادقة لتمثيل حل آمن

يعرض هذا التقرير المراحل المختلفة لهذا التنفيذ باستخدام طريقة سكروم

كلمات مفاتيح: الافتراضية ، الإشراف ، التشغيل التلقائي ، الأمان ، المصادقة

Résumé

Ce travail s'inscrit dans le cadre du projet de fin d'études pour l'obtention du diplôme de Licence Appliquée en Technologies de l'Informatique. Il a été réalisé au sein de GlobalNet.

Notre projet consiste à implémenter une architecture réseau avec la mise en place d'un outil de supervision afin d'intervenir rapidement pour corriger les pannes rencontrées, l'automatisation pour renforcer la productivité et réduire les coûts d'exploitation surtout en ce qui concerne les tâches répétitives, le contrôle d'accès avec la mise en place d'un réseau privé virtuel et d'un serveur d'authentification pour représenter une solution sécurisée.

Ce rapport présente les différentes phases de cette implémentation en utilisant la méthode SCRUM.

Mots clés : virtualisation, supervision, automatisation, sécurité, authentification.

Abstract

This work is part of the graduation project for the diploma of Applied License in Computer Technologies. It was realized within Globalnet.

Our project consists in implementing a network architecture with the implementation of a monitoring tool in order to intervene quickly to correct the failures encountered, automation to increase productivity and reduce operating costs, especially with respect to repetitive tasks, access control with the establishment of a virtual private network and an authentication server to represent a secure solution.

This report presents the different phases of this implementation using the SCRUM method.

Keywords: virtualization, monitoring, automation, security, authentication.

