الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة

Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière Télécommunications
Spécialité Réseaux & Télécommunications

présenté par

HIFI Ouassim

&

SEFOUANE Slimane

Installation et test d'un système de monitoring d'infrastructure réseaux (Op manager)

Proposé par : Dr. MEHDI Merouane et M.YALAOUI Moussa

Année Universitaire 2019-2020

Avant tout on remercie Dieu « ALLAH » le tout puissant de nous avoir accordé la force, le courage et la patience pour terminer ce travail.

On tient à faire part de notre reconnaissance particulière et de notre respect profond aux membres composant le jury :

On exprime notre profonde gratitude à Mr Habib Docteure à l'Université de Blida 1 d'avoir accepté de présider le jury.

Un grand merci à Mr Zair pour avoir accepté d'examiner notre mémoire.

On adresse nos sincères remerciements à Mr Yalaoui moussa qui nous a fait l'honneur d'avoir encadré et dirigé ce travail.

Ses conseils pertinents nous ont permis de mener à terme ce travail.

Notre gratitude est exprimée à tous nos enseignants, qui nous ont donné les bases de la science.

Ouassim et Slimane

Nos grands remerciements sont pour notre Dieu qui nous a aidé et nous a donné le pouvoir, la patience et la volonté d'avoir réalisé ce modeste travail.

Nous dédions ce travail a notre raison de vie nos parents, nos joies de vivre et source de réussite.

Tout La famille Hifi et Choubane en particulier mes frères et ma sœur, c'est difficile d'exprimer mes sentiments envers eux par de simples mots ; Merci pour votre amour, votre affection, votre attention, vos encouragements, vos sacrifices merci pour tout. Que Dieu vous garde pour moi.

Dédicace à mon meilleures ami betina Mohamed Toufik pour l'aide précise et pour ces magnifiques gestes tout en coure de notre cycle universitaire.

Dédicace a tout la famille Sefouane en particulier mes frères et sœurs, c'est difficile d'exprimer mes sentiments envers eux par de simples mots ; Merci pour votre amour, votre affection, votre attention, vos encouragements, vos sacrifices merci pour tout. Que Dieu vous garde pour moi.

Sans oublier mes amis rida, Monime, Oussama, Oussama, Abderrahmane et

Lounis merci pour vos meilleurs soutiens et les moments joyeux partager entre nous.

À tous les enseignants pendant notre carrière pour nous avoir poussé à continuer.

Ainsi que tous ceux qui nous ont aidé de près ou de loin.

Ouassim et Slimane

ملخص:

في الوقت الذي تكنولوجيا المعلومات هي العمود الفقري لأي شركة، والإشراف هي واحدة من الأدوات الحيوية التي لا غنى عنها لحسن سير العمل، لذلك يجب أن تعمل هذه الأداة العمل على النحو الأمثل لتكون قادرة على تحقيق نتائج جيدة .

Op Manager، وهو حل مراقبة شبكة مثل أجهزة التوجيه، ومفاتيح، وجدران الحماية، وميزانيات التحميل، ووحدات تحكم الشبكة المحلية اللاسلكية، والخوادم، والأجهزة الظاهرية، والطابعات، وأجهزة التخزين وأي شيء آخر يحتوي على عنوان IP ومتصل بالشبكة ويستخدم بروتوكولات SNMP و WMI .

في موجزنا، حددنا المعدات التي يجب الاشراف عليها، وأي بروتوكول للأشراف وتطبيق مدير العمليات على هاده المعلومات المختلفة.

.

كلمات المفاتيح: علوم الكمبيوتر، الإشراف، op manager، SNMP، WMI

Résumé :

A l'heure ou l'informatique constitue l'épine dorsale des SI de toute entreprise, la supervision est l'un des outils indispensable et vital pour le bon fonctionnement de celle-ci, Donc cet outil de travail doit fonctionner de manière optimale pour pouvoir permettre de bons résultats.

Op Manager, une solution de surveillance réseau tels que les routeurs, les commutateurs, les pare-feu, les équilibreurs de charge, les contrôleurs LAN sans fil, les serveurs, les machines virtuelles, les imprimantes, les périphériques de stockage et tout ce qui a une adresse IP et est connecté au réseau et utilise les protocole SNMP et WMI.

Dans notre mémoire on a défini quel équipement superviser, avec quel protocole superviser et appliquer op manager sur ces différents équipements.

Mots clés : Informatique, supervision, op manager, SNMP, WMI.

Abstract:

At a time when IT is the backbone of the IS of any company, supervision is one of the indispensable and vital tools for the proper functioning of it, so this working tool must function optimally to be able to achieve good results.

Op Manager, a network monitoring solution such as routers, switches, firewalls, load balancers, wireless LAN controllers, servers, virtual machines, printers, storage devices and anything else that has an IP address and is connected to the network and uses the SNMP and WMI protocols.

In our brief we have defined which equipment to supervise, with which protocol to supervise and apply op manager on this different equipment

Keywords: Informatique, supervision, op manager, SNMP, WMI.

ATM *: Asynchronous Transfer Mode*
CIFS *: Common Internet File System*
CIM *: Common Information Model*
CIR *: Committed Information Rate*
CPU *: Central Processing Unit*
CRM *: Customer Relationship Management*
CSMA/CD *: accès multiple avec écoute de porteuse et détection de collision*
CSS *: Cascading Style Sheets*
DHCP *: protocole de configuration dynamique des hôtes*
DMZ *: Demilitarized Zone*
DNS *: Domain Name System*
DR *: Designated Router*
EIGRP : Enhanced Interior Gateway Routing Protocol
ESX *: Elastic Sky X.*
FAI *: fournisseurs d'accès Internet*
FTP *: File Transfer Protocol*
GAN generative adversarial networks
HDLC *: High-Level Data Link Control*
HTML *: HyperText Markup Language*
ICANN *: Internet Corporation for Assigned Names and Numbers*
ICMP *: Internet Control Message Protocol*
IGP *: Interior Gateway Protocol*
IIS *: Internet Information Services*
IMAP *: Internet Message Access Protocol*
IP/MPLS *: Internet Protocol/Multi-Protocol Label Switching*
IPX *: Internetwork packet exchange*
ISA *: Intelligent System Architecture*
LAN *: Local Area Network*
LDAP *: Lightweight Directory Access Protocol*
MAN *: Metropolitan Area Network*
MIB *: Management Information Base*
MPLS : MultiProtocol Label Switching
NCP *: Netware Core Protocol*
NFS *: Network File System*
NMS *: Network Management System, : Network Management System*
NOC *: Network Operations Center*
NRPE *: Nagios Remote Plugin Executor*
NTLM *: NT Lan Manager*
OEM *: Original Equipment Manufacturer*
OS *: Operating System*
OSI *: Open Systems Interconnection*
OSPF : Open Shortest Path First
PDH *: Plesiochrone Digitale Hierarchie*
POP *: Point of Presence*
PPP *: protocole point à point*
PRTG *: Passeler routing traffic grapher*
QOS *: Quality of service .*
RAM Random Access Memory
RIP : Routing Information Protocol
SDLC *: Synchronous Data Link Control*
SFF *: Small form factor*

Listes des abréviations

SFP : Small form-factor
SGBD *: Système de gestion de base de données*
SI *: Science information*
SLA *: Service Level Agreement*, *: Service Level Agreement*
SMB *: Server Message Block*
SMTP *: Simple Mail Transfer Protocol*
SNMP *: Simple Network Management Protocol*
SONET *: Synchronous Optical Network*
SSH *: Secure Shell*
TCP *: Transfer Control Protocol*
TELNET *: terminal network*
TTL *: Time To Live*
UI *: l'interface utilisateur*
URL *: Uniform Resource Locator*
VLAN *: Virtual Local Area Network*
VM *: machines virtuelles*
VoIP *: Voice Over Internet Protocol*
VPN *: Virtual Private Network*
WBEM *: Web-Based Enterprise Management*
WinRM *: Windows Remote Gestion*
WLAN *: Wireless Fidelity*
WMAN : Wireless Metropolitan Area Network
WMI *: Windows Management Instrumentation*, *: Windows Management Instrumentation*

Table des matières

Table des matières

Table des matières

Table des matières

Table des matières

Table des matières

Liste des figures

Liste des figures

Liste des figures

Liste des tableaux

De nos jours, l'informatique est devenu indispensable au sein d'une entreprise quel que soit son secteur d'activité. On compte désormais sur les services offerts par les réseaux pour le fonctionnement des entreprises, (transactions bancaires, téléconférences). Les systèmes d'information sont au centre des différentes entités métiers et doivent fonctionner pleinement et en permanence pour garantir l'efficacité de l'entreprise. A tous les niveaux les système informatique (les réseaux, les terminaux utilisateurs, les serveurs d'application, les données), constituent autant de maillons sensibles dont la disponibilité et la qualité de service conditionnent le bon fonctionnement de l'entreprise.

Les problèmes liés à l'informatique doivent donc être réduits au minimum, car une indisponibilité ou une baisse de QOS des systèmes d'information conduirait à des impacts très préjudiciables sur l'activité, l'économie et sur la notoriété d'une entreprise, ce qui rend les logiciels de la supervision indispensable. Ainsi, la supervision des système informations s'avère nécessaire. Elle permet d'avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau et d'avoir des indicateurs sur la performance de son architecture.

L'objectif de notre projet est d'essayé de diminué ces problèmes, en appliquons une solution de supervision, la méthode qu'on a utilisée dans ce mémoire, et avant tout définir une infrastructure réseau et définir ces équipements, savoir parmi ces équipements les quelles est mieux placé pour être superviser, quel protocole utiliser pour les superviser ? Et enfin appliquer une solution de supervision qui est un logiciel et voir les résultats obtenus.

Le premier chapitre, nous présenterons, L'infrastructure du réseau informatique ensuite dans le deuxième chapitre, nous ferons part des protocoles de supervision réseau et de monitoring et quelque logiciel de supervision. Dans le troisième chapitre nous présenterons le Logiciel utilisé Op manager et le quatrième chapitre ressortira la mise en œuvre de la solution et les résultats que nous avons obtenus ainsi qu'un bref état de ce qui a été réalisé.

1 Chapitre 1 : Infrastructure du réseau informatique

1.1 Introduction :

Une infrastructure réseau constitue une obligation pour toute société moderne et ambitieuse. Celle-ci s'apparente à la charpente de votre organisation informatique. Le bon fonctionnement de vos équipements et logiciels en dépend. Elle favorise une transmission rapide et sécurisée de vos données. Découvrez le rôle et l'importance d'une infrastructure informatique ainsi que ses exigences en matière de performance [1].

1.2 C'est quoi une Infrastructure Réseau ?

Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations. Par analogie avec un filet (un réseau est un « petit rets », c'est-à-dire un petit filet, on appelle nœud l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions ou équipements (un ordinateur, un routeur, un concentrateur, un commutateur).

Indépendamment de la technologie sous-jacente, on porte généralement une vue matricielle sur ce qu'est un réseau.

De façon horizontale, un réseau est une strate de trois couches : les infrastructures, les fonctions de contrôle et de commande, les services rendus à l'utilisateur. De façon verticale, on utilise souvent un découpage géographique : réseau local, réseau d'accès et réseau d'interconnexion. Les infrastructures ou supports peuvent être sur des câbles dans lesquels circulent des signaux électriques, circulent des ondes radio, ou des fibres optiques qui propagent des ondes lumineuses. Elles permettent de relier « physiquement » des équipements assurant l'interconnexion des moyens physiques qui sont définis par des protocoles. Les équipements d'un réseau sont connectés directement ou non entre eux, conformément à quelques organisations types connues sous le nom de topologie de réseau. Les principaux types de réseaux filaires pour les réseaux informatiques d'entreprises ou de particuliers utilisent les protocoles qui proviennent du standard Ethernet , d'où une infrastructure c'est l'ensemble de logiciel et matériel existant dans une entreprise [1].

1.3 Définition d'une infrastructure réseau :

Le réseau informatique représente l'ensemble des équipements et périphériques reliés physiquement ou virtuellement entre eux au sein d'une entreprise dans le but de partager des ressources ou des informations. Il constitue une succession de nœuds interconnectés via des

chemins de communication. Les infrastructures réseau se démarquent généralement par leur portée géographique, la technologie exploitée pour le transfert des fichiers, les types de signaux ainsi que les connexions et les liaisons physiques utilisées. Pour installer une infrastructure performante [1].

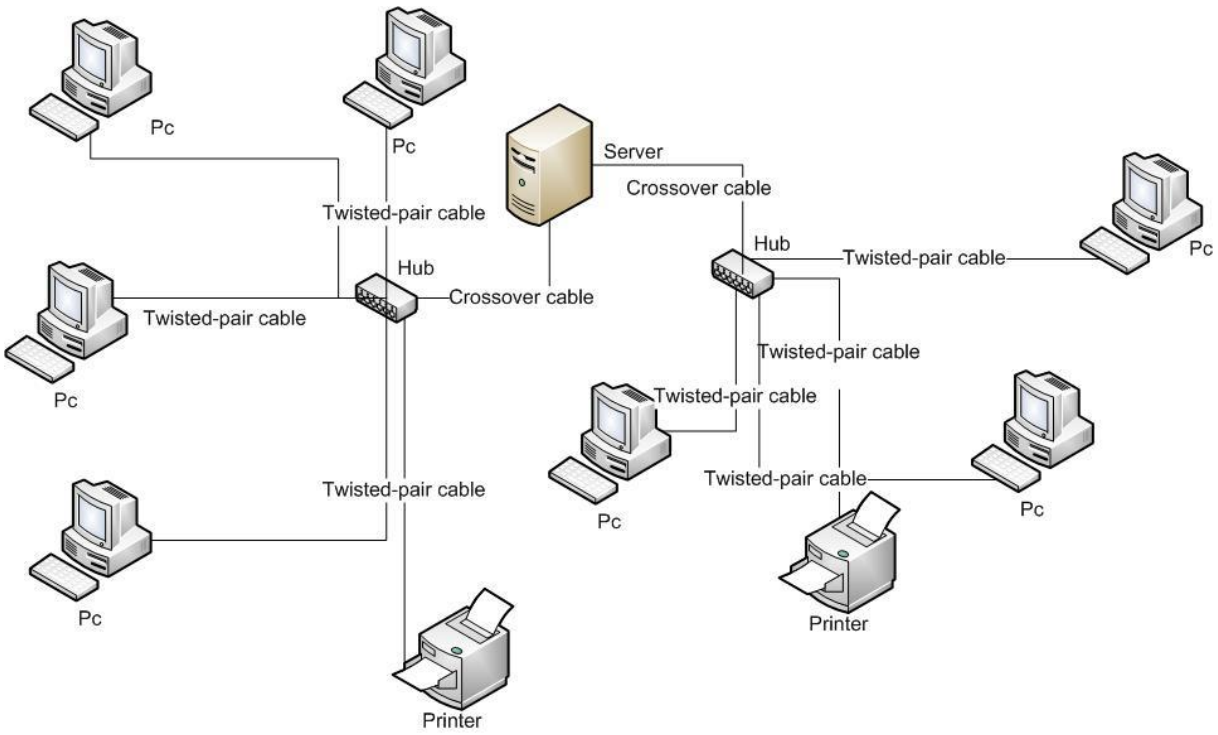


Figure 1.1 : quelques équipements d'une infrastructure réseau [2].

1.4 Les différents types d'infrastructure réseau :

La solution informatique propose une multitude de réseaux. Ils se démarquent par des avantages et des inconvénients spécifiques.

1.4.1 Local Area Network(LAN)

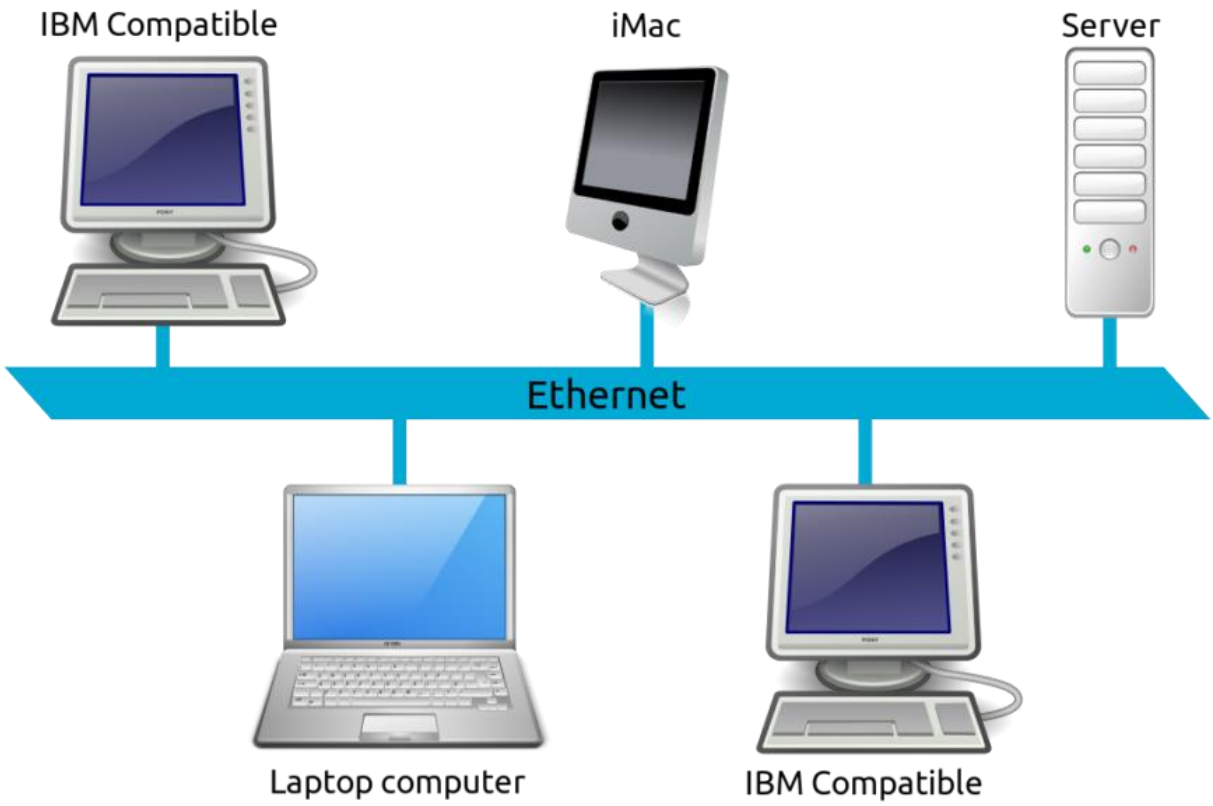


Figure 1.2 : Infrastructure réseau local.

Le LAN permet de réunir sur un réseau au moins deux ordinateurs. Il autorise le partage des serveurs de fichiers, des imprimantes ou des applications entre de nombreux postes d'une entreprise. Il assure un échange confortable et sécurisé d'informations entre les périphériques connectés au réseau. Le LAN reste prisé par les sociétés qui souhaitent transférer rapidement d'importantes données. Son débit peut atteindre 10 à 1000 Mbit/s selon la structure du réseau et le moyen de transmission exploité. Sa mise en place repose généralement sur le protocole Ethernet. Avec un LAN, la communication des informations s'effectue via des câbles de cuivre ou de fibre optique. L'intégrateur doit recourir à des éléments de couplages et des nœuds de distribution comme les concentrateurs (hub), les commutateurs réseau (switch) ou des ponts (bridge) [2].

1.4.2 Métropolitain Area Network (MAN)

Le MAN convient aux grandes entreprises qui disposent de succursales dans de nombreuses villes à proximité l'une de l'autre. Le MAN constitue donc une infrastructure réseau à large bande qui connecte divers LAN géographiquement proches. Pour

implémenter cette solution, elle exploite des routeurs et des fibres optiques de haute performance qui garantissent un débit de transfert plus élevé que celui fourni par Internet. Les entreprises peuvent aussi opter pour le Wireless Métropolitain Area Network (WMAN). Ces grands réseaux de radio régionaux reposent sur la technologie WiMax et les normes IEEE 802.16. Grâce au WMAN, une société peut installer des bornes Wifi ou des WLAN hots pots dans ses agences et succursales [2].

1.4.3 Wide Area Network (WAN)

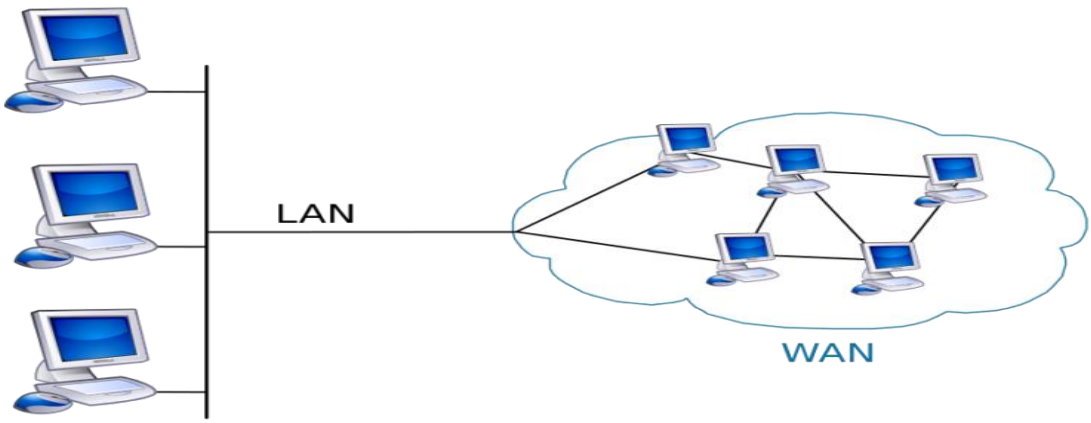


Figure 1.3 : Infrastructure réseau WAN.

Le WAN représente une infrastructure réseau qui couvre des zones géographiques assez vastes comme des pays et des continents. Il permet de relier un nombre illimité d'ordinateurs. Contrairement au LAN et au MAN, le WAN n'utilise pas l'Ethernet. Il exploite plutôt des techniques spécifiques comme IP/MPLS (Multi Protocol Label Switching), ATM (Asynchronous Transfer Mode), PDH (Plesiochrone Digitale Hiérarchie), SONET (Synchronous Optical Network) ou SDH (Synchrone Digitale Hiérarchie). Les réseaux étendus de type WAN appartiennent généralement à une organisation qui peut les exploiter en privé ou les louer. Les fournisseurs d'accès Internet recourent souvent à des WAN dans le cadre de leurs prestations [2].

1.4.4 Global Area Network (GAN)

Le GAN s'assimile à une infrastructure d'envergure planétaire comme Internet. Certaines entreprises peuvent mettre en place des réseaux isolés qui interconnectent une multitude de WAN à travers le monde. L'installation d'un GAN exige l'exploitation de fibre optique des

réseaux étendus ainsi que la pose de câbles sous-marins internationaux ou des transmissions par satellite [2].

1.4.5 Virtual Privat Network (VPN)

Un VPN exploite une infrastructure physique pour connecter virtuellement des systèmes informatiques. Il peut prendre la forme de l'un ou l'autre des réseaux énumérés ci-dessus. La transmission des données se réalise essentiellement par le biais d'Internet. Le transfert des informations s'effectue via un tunnel virtuel qui s'établit entre le serveur VPN et le VPN client. Les VPN recourent à un système de cryptage assez performant pour garantir la confidentialité des données [3].

1.4.6 Le réseau MPLS

Le Multi Protocol Label Switching repose sur un système assez innovant de commutation d'étiquettes. Il s'utilise essentiellement au niveau des réseaux informatiques étendus qui transmettent des données importantes. L'attribution des labels aux paquets intervient à l'entrée du réseau. Le retrait s'effectue à la sortie [4].

1.5 Equipement physique d'une infrastructure réseau :

1.5.1 Répéteur :

Un répéteur (en anglais repeater) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.

D'autre part, un répéteur peut permettre de constituer une interface entre deux supports physiques de types différents, c'est-à-dire qu'il peut par exemple permettre de relier un segment de pair torsadé à un brin de fibre optique [5].

1.5.2 Concentrateur (Hub) :

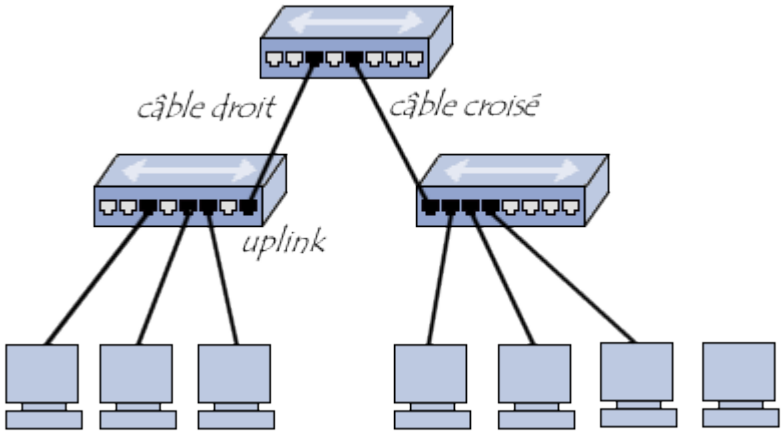


Figure 1.4 : implémentation d'un concentrateur dans un réseau.

Un concentrateur est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Le concentrateur est ainsi une entité possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports. Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports [6].

La figure 1.4 nous montre l'implémentation d'un concentrateur dans un réseau.

1.5.3 Les différents types de concentrateurs

On distingue plusieurs catégories de concentrateurs [6]:

- Les concentrateurs dits "actifs" : ils sont alimentés électriquement et permettent de régénérer le signal sur les différents ports.
- Les concentrateurs dits "passifs" : ils ne permettent que de diffuser le signal à tous les hôtes connectés sans amplification.

1.5.3.1 Les ponts (bridge)

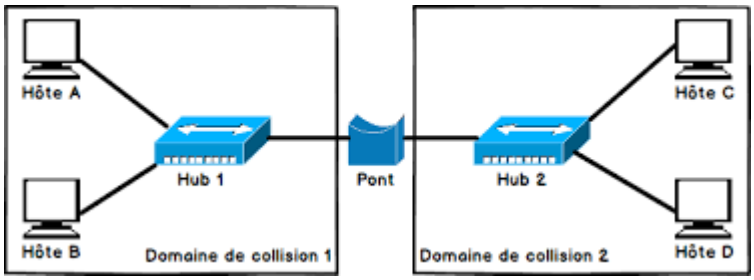


Figure 1.5 : Implémentation d'un pont sur un réseau.

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (au niveau de la couche 2 du modèle OSI), c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont.

Ainsi, le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées au niveau local et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (notamment les collisions) sur chacun des réseaux et d'augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre brin [5].

La figure 1.5 nous montre une implémentation d'un pont dans un réseau.

1.5.4 Les commutateurs (switches)

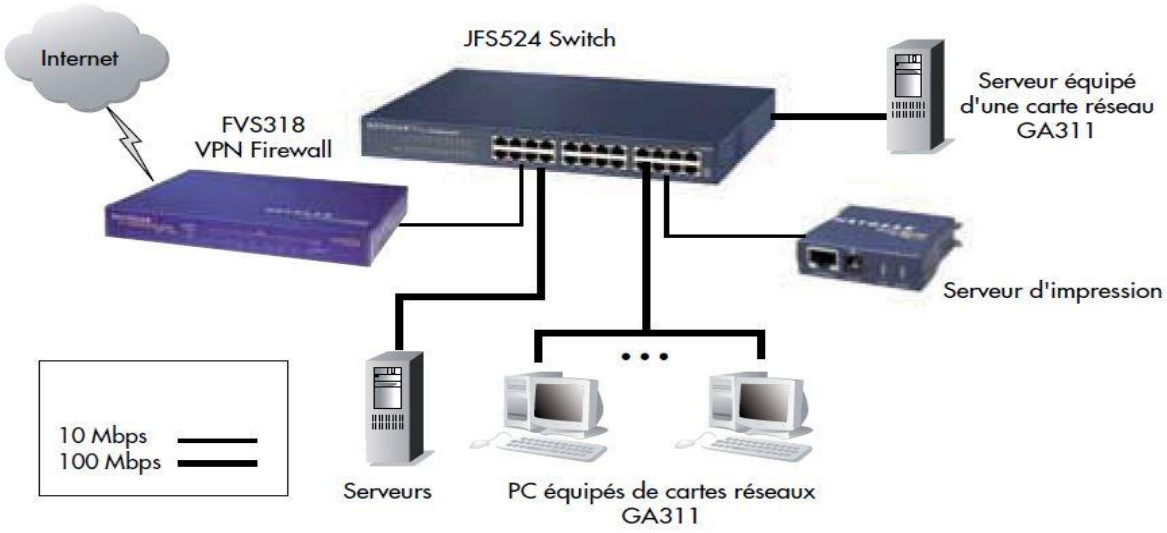


Figure 1.6 : l'ensemble des périphériques réseaux connecté à un switch.

En informatique, un switch est un boitier doté de quatre à plusieurs centaines de ports Ethernet, et qui sert à relier en réseau différents éléments du système informatique. Il permet notamment de créer différents circuits au sein d'un même réseau, de recevoir des informations et d'envoyer des données vers un destinataire précis en les transportant via le port adéquat. Le switch présente plusieurs avantages dans la gestion de votre parc informatique. Il contribue à la sécurité du réseau et à la protection des données échangées via le réseau. D'autre part, il permet de connecter davantage de postes de travail sur le même réseau Ethernet. Le switch permet avant tout de répartir l'information de manière « intelligente » au sein de l'entreprise. Il contrôle et sécurise au maximum votre réseau pour vous éviter les intrusions. Une fois paramétré par un technicien informatique, le switch distribue l'information seulement aux utilisateurs prédéfinis en fonction de la typologie de collaborateurs (pôle finance, direction, markéting…) et/ou de certaines restrictions, améliorant ainsi la confidentialité des données d'entreprise [7].

1.5.5 Les différents types de switches

Les switches non-paramétrables : Ce type de switch ne dispose pas d'interface de paramétrage. Ils se branchent simplement sur le réseau d'entreprise pour diffuser les données sur les différents ports en fonction de la configuration initiale.

Les switches Layer 2 : Ces switches peuvent être paramétrés par un technicien informatique grâce à une interface web ou une interface interne.

Les switches Layer 2+3 : Ils sont également paramétrables et permettent de mettre en œuvre un routage interne selon les adresses IP et adresses mac.

Les switches Cloud : Ces switches viennent de faire leur entrée sur le marché. Ils permettent de réaliser les mêmes actions que les autres switches mais leur interface est

Consultable à distance sur tous types d'appareil (tablette, Smartphone, ordinateur portable…). Ce switch fonctionne grâce à un système de Cloud sécurisé [7]**.**

1.5.6 Les ports

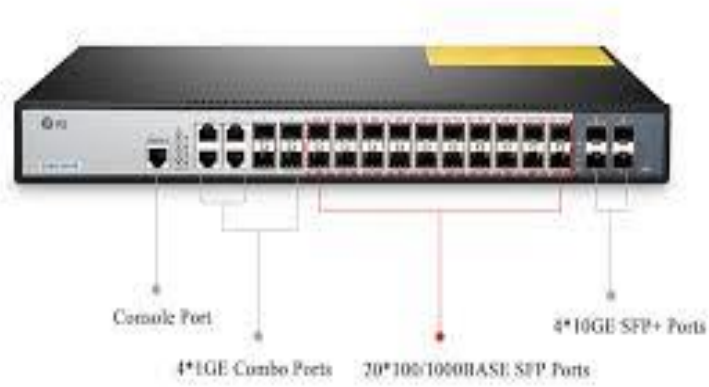


Figure 1.7 : différentes types des ports de switch.

La figure 1.7 nous montre les différents types des ports d'un switch.

1.5.6.1 Le port console

La première connexion s'effectue via le port console du switch. On utilisera pour cela un câble série fourni en général avec le switch [8]**.**

1.5.6.2 Le port Rj45

C'est une infrastructure physique qui utilise le câble a une sortie rj45 il permet d'interconnecter les équipements du réseau à l'aide d'un câble a paire torsadé [8]**.**

1.5.6.3 Port SFP

Le port SFP est conçu pour être utilisé avec des concentrateurs FF (Small form factor)il permet à un switch d'autoriser des liaisons optiques ou en cuivre en insérant le module SFP correspondant (le SFP de fibre ou de cuivre) [8].

1.5.6.4 Le protocole de communication avec l'extérieur

Le switch utilise le protocole Ethernet pour communiquer avec le monde extérieur, le protocole Ethernet est un protocole de réseau local a communication de paquet c'est une norme internationale ISO/IEC802.3 le protocole est classé dans la couche 2(liaison de donnée).

Et la couche 1 (physique) du modèle OSI il utilise la technologie CSMA/CD, comme le routeur le switch utilise aussi le protocole SNMP : SNMP (Simple Network Management Protocol) est un protocole Internet dédié à la gestion des périphériques sur les réseaux SNMP est principalement utilisé dans NMS (Network Management System) pour surveiller diverses conditions sur les périphériques qui nécessitent l'attention de l'administrateur réseau [8].

1.5.7 Passerelle (Gateway)

Une passerelle (en anglais, Gateway) est un dispositif permettant de relier deux réseaux informatiques différents, comme par exemple un réseau local et l'Internet. Ainsi, plusieurs ordinateurs ou l'ensemble du réseau local peuvent accéder à l'Internet par l'intermédiaire de la passerelle. Ainsi, plusieurs équipements peuvent accéder à l'autre réseau par l'intermédiaire de la passerelle. Ce processus intervient à partir de la couche 4 (couche transport) du modèle OSI et peut modifier la trame jusqu'à la couche 6 [5].

Cette différence est très importante quand on interconnecte des réseaux de nature différente. Une passerelle permet de faire communiquer des réseaux hétérogènes. Cette notion est très importante en réseaux de terrain.

Cependant, le terme passerelle (sans autre précision) est couramment employé comme exact synonyme du terme routeur, par exemple dans le routage on parle de passerelle par défaut (default Gateway) ou dans Interior Gateway Protocol, Border Gateway Protocol alors qu'il ne s'agit clairement que de routage au niveau IP, il est donc utile de préciser que l'on parle de passerelle applicative par exemple pour éviter toute ambigüité.

D'où Coute plus cher qu'un routeur : plus de capacité, spécifique à une application plus lente qu'un pont ou un routeur : exécutées conversions complexes [5].

Passerelle de transport : met en relation les flux de données d'UN protocole de couche transport.

Passerelle d'application : réalise l'interconnexion entre applications de couches supérieures.

Avantages : incontournables dans les grandes organisations

Inconvénients : nécessite souvent une gestion importante.

La figure 1.8 nous montre le principe d'une passerelle.

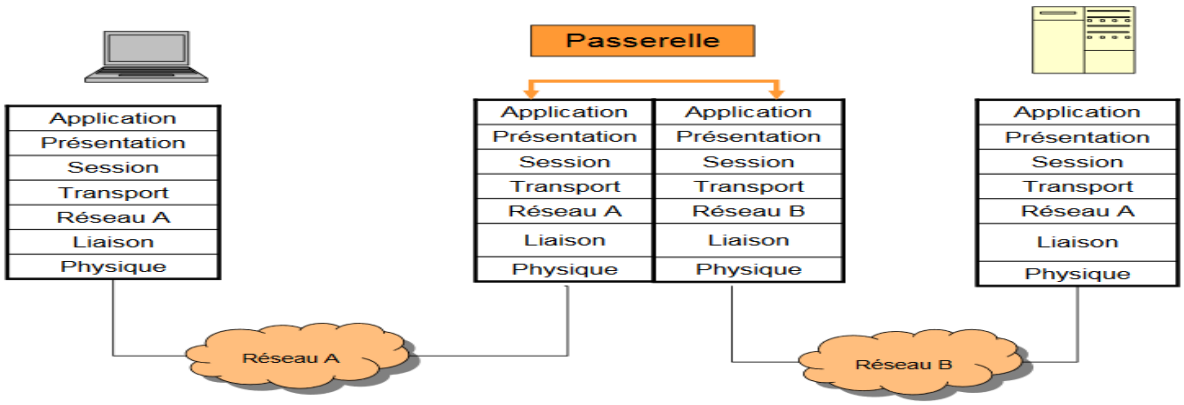


Figure 1.8 : Principe de passerelle.

1.5.8 Routeur

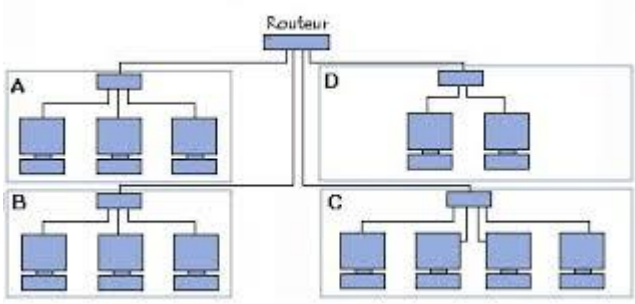


Figure 1.9 : routeur dans un réseau.

Le routeur est un périphérique réseau qui dirige les paquets de données sur un réseau. Il est également utilisé pour connecter différents réseaux. Et il peut connecter deux LAN ou deux WAN ensemble ou LAN et WAN ensemble. Il n'est pas essentiel pour connecter un réseau informatique à Internet alors qu'il est uniquement destiné à distribuer les données d'un réseau à un autre. Ainsi il filtre les paquets de données qui y arrivent et analyse ensuite le paquet de données pour déterminer l'adresse physique dans son champ de destination et

acheminer ce paquet jusqu'à sa destination. Il utilise RJ45 pour se connecter à un réseau informatique, la figure 1.9 nous montre un routeur dans un réseau [9].

1.5.8.1 Les ports

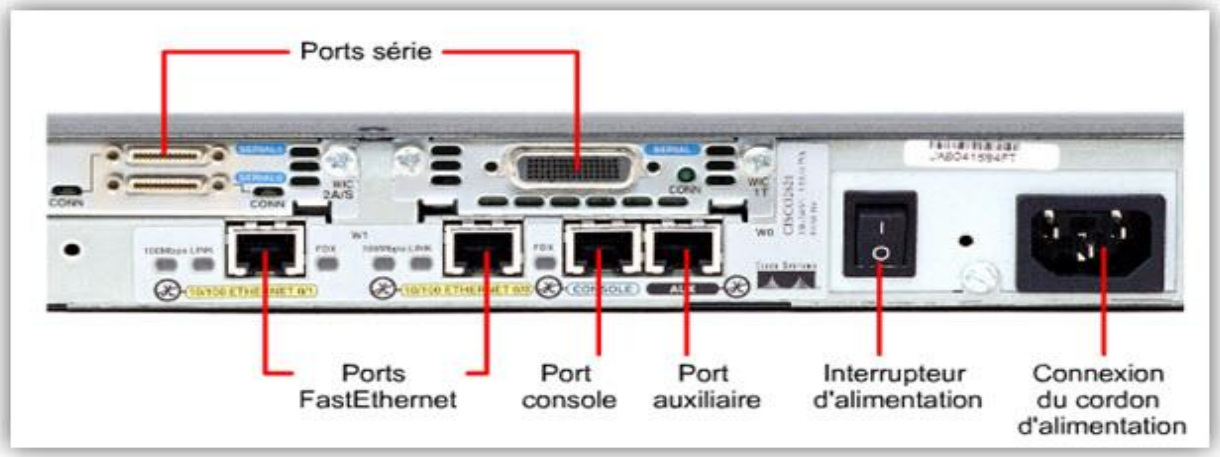


Figure 1.10: Les ports d'un routeur.

Cette figure 1.10 nous montre les différents ports dans un routeur.

1.5.8.1.1 Port Ethernet

Un port Ethernet ou socket est une ouverture sur un équipement de réseau dans lequel les câbles Ethernet se branchent. Leur but est de connecter du matériel de réseau câblé dans un réseau local Ethernet, un réseau métropolitain (MAN) ou un réseau étendu (WAN). Un routeur possède généralement plusieurs ports Ethernet pour accueillir plusieurs périphériques câbles sur un port Ethernet accepte un câble doté d'un concentrateur RJ-45 le port Ethernet permet de relier deux réseaux différents [10].

1.5.8.1.2 Les ports de gestions

En dehors des interfaces réseau, le routeur est pourvu de deux interfaces de type série asynchrone, nommées port console et port auxiliaire et dédiées à l'administration du système. Le port console autorise un accès local et l'administrateur l'utilisera plutôt pour réaliser la configuration initiale du routeur. En effet, une fois configuré et en exploitation, le routeur est accessible par le réseau et l'administrateur peut en assurer la gestion à l'aide d'une session TELNET ou SSH (Secure Shell, version sécurisée destinée à remplacer TELNET). La seconde interface série, nommée port auxiliaire permet un accès de l'administrateur à distance. Un scénario possible est de reprendre la main sur l'équipement distant quand l'administrateur n'y parvient plus par le réseau. Pour profiter de cette possibilité, il faut avoir été prévoyant,

c'est-à-dire avoir installé un modem au voisinage du routeur et avoir amené une ligne du réseau téléphonique commuté sur ce modem, ce qui revient à attribuer un numéro de téléphone au routeur. Une exception cependant : les routeurs de la gamme 800 ne disposent que d'un seul port série asynchrone destiné à l'administration. Appelé console [10].

1.5.8.1.3 Les ports série

Ce sont des ports dont l'interface est propriétaire Cisco en face arrière des routeurs. Il y a soit des ports 60 points (standard) soit des interfaces 50 points (pour des cartes filles sur des gammes supérieures ou égales à 4000). Les jonctions sont donc les mêmes que l'on veuille faire du RS232, du V11, du V35. Ce sont des câbles adaptateurs qui feront la conversion de signaux et de jonction. Ces interfaces permettent, suivants les versions logicielles que l'on charge sur le routeur, de travailler avec nombre de protocoles différents. On y implémente des protocoles WAN en couche basse : Frame Relay, X25, PPP, HDLC, SDLC. Au-dessus on retrouve des protocoles tels que : IP, IPX . Pour configurer une interface serial on utilise la commande : « interface serial X ». Attention, la connexion d'un PC ou Terminal sur un port Serial nécessite un câble croisé en direct (contrairement au port console) [10].

1.5.9 Les protocoles de communication avec le monde extérieur

1.5.9.1 RIP

Le protocole RIP (Routing Information Protocol) permet aux routeurs qui interconnectent des réseaux via le protocole IP (Internet Protocol) de partager des informations relatives à l'acheminement du trafic entre ces différents réseaux. Chaque routeur RIP gère une table de routage. Celle-ci contient une liste répertoriant toutes les destinations (ou réseaux) connues du routeur, ainsi que l'itinéraire qui y mène et la distance qui l'en sépare.

Ce protocole est classifié par l'IETF (Internet Engineering Task Force) comme protocole de passerelle intérieure (IGP, Interior Gateway Protocol). L'IGP est l'un des protocoles destinés au transfert de données dans un réseau de systèmes autonomes plus vaste [11].

1.5.9.2 EIGRP

EIGRP est un protocole de routage dynamique intérieur hautement fonctionnel de type « distance vector » (vecteur de distance) avancé. Il converge très rapidement et il est multi-

protocoles IPv4/IPv6. Il permet de contrôler finement la métrique de manière à influencer les entrées de la table de routage. EIGRP est alors capable de répartir la charge de trafic sur des liaisons à couts inégaux [11].

1.5.9.3 OSPF

Open Shortest Path First (OSPF) est un protocole de routage à état de liaison qui est utilisé pour trouver le meilleur chemin entre la source et le routeur de destination en utilisant son propre Shortest Path First). OSPF est développé par Internet Engineering Task Force (IETF) comme l'un des protocoles IGP (Interior Gateway Protocol), c'est-à-dire le protocole qui vise à déplacer le paquet dans un grand système autonome ou domaine de routage. Il s'agit d'un protocole de couche réseau qui fonctionne sur le numéro de protocole 89 et utilise la valeur AD 110. OSPF utilise l'adresse de multidiffusion 224.0.0.5 pour la communication normale et 224.0.0.6 pour la mise à jour vers le routeur désigné (DR) / le routeur désigné de sauvegarde (BDR) [11].

1.5.9.4 SNMP

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux.

SNMP est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications : les bases de données, les serveurs, les logiciels, etc.

L'environnement de gestion SNMP est constitué de plusieurs composantes : la station de supervision, les éléments actifs du réseau, les variables MIB et un protocole. Les différentes composantes du protocole SNMP sont les suivantes :

Les éléments actifs du réseau sont les équipements ou les logiciels que l'on cherche à gérer. Cela va d'une station de travail à un concentrateur, un routeur, un pont, etc. Chaque élément du réseau dispose d'une entité dite agent qui répond aux requêtes de la station de supervision. Les agents sont des modules qui résident dans les éléments réseau. Ils vont chercher l'information de gestion comme par exemple le nombre de paquets en reçus ou transmis [12].

1.6 Les serveurs

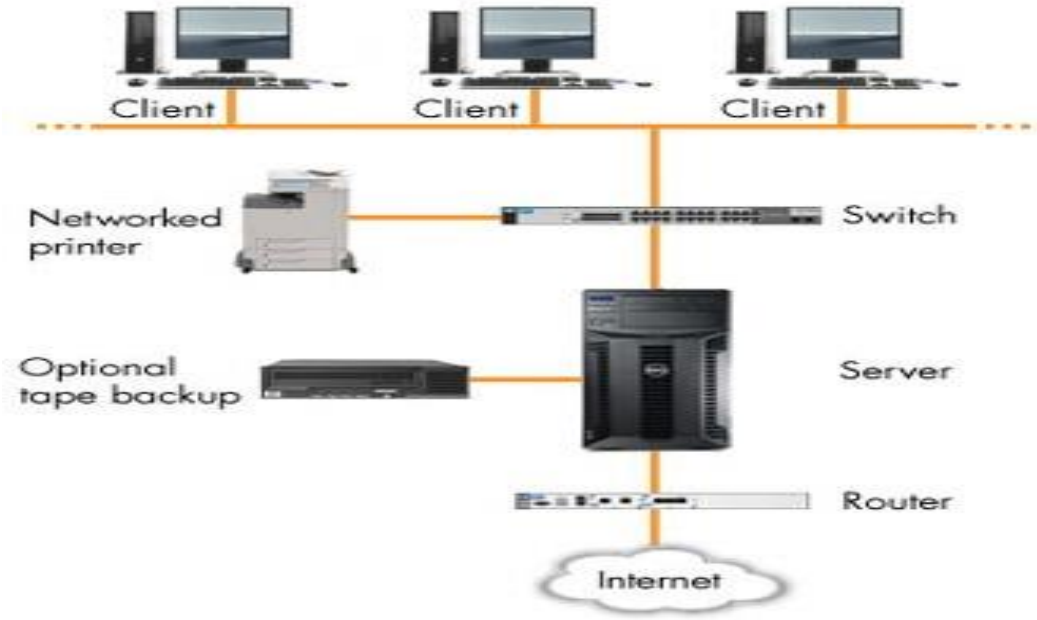


Figure 1.11 : emplacement d'un serveur dans une architecture réseau.

Le terme serveur désigne le rôle joué par un appareil matériel destiné à offrir des services à des clients en réseau Internet ou intranet. La taille du support physique d'un serveur varie d'un simple boitier à une ferme de calcul, selon le nombre d'utilisateurs susceptibles de le solliciter simultanément. Le serveur en entreprise est un ordinateur plus puissant qui va s'occuper du partage des fichiers, de faire des sauvegardes des données régulièrement, d'autoriser ou non l'accès à un ordinateur au réseau d'entreprise, gérer les e-mails, la connexion Internet et la sécurité informatique. Les serveurs sont souvent stockés dans une pièce dédiée et ventilée, dont l'accès est restreint à l'administrateur. On peut considérer le serveur comme le patron des ordinateurs de l'entreprise, un serveur on peut le caractériser avec ces composants physiques avec les différents types de système d'exploitation installé et sont différents types et rôles [13]**.**

La figure 1.11 nous montre l'emplacement d'un serveur dans une architecture réseau.

1.6.1 Les différents types des serveurs

1.6.1.1 Serveurs dédiés

Le serveur dédié ordinateur situé à distance mis à la disposition d'un seul client par un prestataire. Le client pourra bénéficier pleinement des capacités et des ressources de la machine

Dédiés « réels » : serveur dédié entièrement administré à distance par le client/Serveurs « info gérés » : L'administration du serveur est réalisée par le prestataire [14].

1.6.1.2 Serveurs mutualisés

Un hébergement mutualisé est un concept d'hébergement internet destiné principalement à des sites web. Ce type de serveur va donc héberger plusieurs sites internet sur un seul et même serveur. Il repose sur le partage équitable des ressources, à savoir la mémoire RAM, le CPU, les espaces disques et la bande passante [14].

1.6.1.3 Serveurs virtuels

Un serveur virtuel se comporte comme un serveur dédié, mais le dispositif qui l'héberge est mutualisé. La machine physique héberge plusieurs 4 mutualisé. La machine physique héberge plusieurs serveurs virtuels simultanément, d'où son caractère mutualisé [14].

1.6.2 Les caractéristiques physiques des serveurs

1.6.2.1 Le processeur

Le processeur est le cerveau de l'ordinateur, c'est lui qui organise les échanges de données entre les différents composants (disque dur, mémoire RAM, carte graphique) et qui fait les calculs qui font que l'ordinateur interagit avec vous et affiche votre système à l'écran. Sa puissance est exprimée en Hz. Aujourd'hui, un processeur atteint les 3Ghz (Giga, milliards) et certains ordinateurs sont équipés de plusieurs processeurs.

Les processeurs d'aujourd'hui sont capables de traiter des milliards d'informations par seconde, et accomplir des calculs immenses, qui permettent à la science, la médecine… de progresser rapidement. C'est là-dedans que réside le secret de la puissance informatique. La société Intel est la firme qui fabrique le plus de processeurs au monde [14].

1.6.2.2 CPU

L'unité centrale (CPU) de votre serveur (aussi appelée processeur) interprète et exécute les instructions, traite les données et effectue des tâches comme la diffusion de pages Web, le lancement de requêtes dans une base de données et l'exécution d'autres programmes et

commandes informatiques. Un nombre élevé de processeurs augmente la rapidité et l'efficacité du serveur, qui peut ainsi exécuter plus d'instructions dans un délai plus court.

La rapidité d'un processeur dépend en partie de la fréquence d'horloge, qui consiste en la vitesse d'exécution des instructions. Une fréquence d'horloge supérieure signifie un nombre élevé d'instructions exécutées par seconde. Il s'agit de la vitesse du processeur, que l'on mesure en hertz (GHz) [14].

1.6.2.3 Mémoire cache

La mémoire cache est une mémoire plus rapide et plus proche du matériel informatique (processeur, disque dur) auquel elle sert des données et des instructions. Son rôle est de stocker les informations les plus fréquemment utilisées par les logiciels et applications lorsqu'ils sont actifs. C'est cet accès direct qui détermine les performances d'un programme car il économise des échanges incessants entre le processeur et la mémoire vive, la RAM (Radom Access memory) [14].

1.6.2.4 Le nombre de cœur

Un cœur physique est un ensemble de circuits capables d'exécuter des programmes de façon autonome. Toutes les fonctionnalités nécessaires à l'exécution d'un programme sont présentes dans ces cœurs : compteur ordinal, registres, unités de calcul, etc. Des caches sont définis pour chaque processeur ou partagés entre eux [14].

1.6.2.5 La ram

La RAM est un type de mémoire qui équipe tout ordinateur et qui permet de stocker des informations provisoires. Son avantage majeur est sa capacité de lecture très rapide par rapport au disque dur et qui permet une utilisation fluide de votre ordinateur. RAM veut dire en anglais Random Access Memory : mémoire à accès aléatoire (son but n'étant pas de ranger de l'information mais d'y accéder rapidement et provisoirement).

La RAM ou mémoire vive est la ressource qui stocke temporairement ces données et ces instructions. Elle sert également à transmettre ces ordres à des fins de calcul notamment. Cette mémoire est l'intermédiaire de ces processus car une grande partie du traitement de données requis pour exécuter un site Web est extrêmement répétitive. La RAM stocke donc ces données répétitives de manière à pouvoir les livrer à des vitesses très élevées lorsque nécessaire [14].

1.6.2.6 Disque dur

IDE, SATA SSD, SAS : les différents disques durs

Les différences entre les disques durs en IDE, SATA et SSD.

Tout d'abord, pour ceux qui ne savent pas, les disques durs souvent dans votre ordinateur à stocker les données (système d'exploitation, vos musiques, films, photos).

SAS, IDE et SATA sont des systèmes de connexion entre le disque et carte mère. Le SSD est un « nouveau » type de disque dur utilisant la connexion en SATA Mais pour faire simple, SATA pour les « ancien » disques durs en SATA et SSD pour les « nouveaux ».

Les différences entre les trois types de disques durs, à part le prix bien entendu !

Le disque dur en IDE permet un transfert d'environ 10Mo/s, le SATA 35Mo/s environ, Cette multiplication par trois était une révolution quand les SATA sont sortis. Les SSD permettent une vitesse de transfert bien plus supérieur, environ 150Mo/s. Les tests effectués sur les disques durs SSD permettent un démarrage de Windows 7 en 8 secondes contre 18 pour un SATA normal.

Les disques durs SATA et SSD ont une meilleure durée de vie que les disques en IDE. Ceux en SSD sont réputés pour être plus fiables que les autres.

Point négatif pour les SSD, le prix est plus cher que les autres.

En conclusion, Les disques durs **SSD** utilisent une mémoire flash (et non mécanique comme les **HDD**) pour stocker l'information. Ils offrent une durabilité améliorée et une performance supérieure aux disques durs **HDD**. Néanmoins, ces derniers présentent une capacité de stockage généralement plus élevée pour un coup moindre. [15]**.**

1.7 Le rôle D’un serveur

En deux mots, un serveur est généralement un ordinateur plus puissant que votre ordinateur de bureau habituel. Il est spécialement conçu pour fournir des informations et des logiciels à d'autres ordinateurs qui lui sont reliés via un réseau. Les serveurs sont dotés de composants matériels qui gèrent la mise en réseau par câble Ethernet ou sans fil, généralement via un routeur.

Capables de traiter des charges de travail plus importantes et d'exécuter davantage d'applications, les serveurs tirent parti de leurs composants matériels spécifiques pour augmenter la productivité et réduire les temps d'inactivité.

Les serveurs offrent également des outils de gestion à distance qui permettent à un technicien informatique de vérifier l'utilisation et de diagnostiquer les problèmes depuis un autre site. Vous pouvez également utiliser ces outils pour exécuter des tâches de maintenance régulière, telles que l'ajout de nouveaux utilisateurs ou la modification de mots de passes. Parmi ces rôles il Ya des rôles qui sont implémenté avec le système d'exploitation comme un service [16].

1.8 Les services offerts par les serveurs

1.8.1 Service de fichier

Un serveur de fichiers permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur (serveur) hébergeant le service applicatif. Il possède généralement une grande quantité d'espace disque où sont déposés des fichiers. Les utilisateurs peuvent ensuite les récupérer au moyen d'un protocole de partage de fichier.

On utilise généralement l'un des cinq protocoles suivants [16]:

- FTP (File Transfer Protocol).
- SMB (Server Message Block) sur un réseau local.
- CIFS (Common Internet File System).
- NFS (Network File System).
- NCP (Netware Core Protocol).

Le choix du protocole dépend principalement de la méthode d'accès des utilisateurs. CIFS est utilisé par les systèmes d'exploitation Microsoft Windows, NFS est répandu dans le milieu UNIX. Toutefois des implémentations de ces protocoles sont disponibles pour tout type de système. Ces deux protocoles permettent d'établir des liaisons permanentes entre le client et le serveur [16].

FTP est utilisé pour des connexions ponctuelles lorsque le client n'a pas besoin d'être connecté en permanence au serveur de fichier [16].

1.8.2 Service de d'application

Un serveur d'applications est un logiciel d'infrastructure offrant un contexte d'exécution pour des composants applicatifs. Le terme est apparu dans le domaine des applications web. Au sens strict les composants hébergés par le serveur d'applications ne sont pas de simples procédures ou scripts mais de réels composants logiciels conformes à un modèle de composants (EJB, COM, Fractal, etc.).

Les clients des serveurs d'application sont : des programmes autonomes (standalone application), des applets ou d'autres composants.

La structuration en couches des différents composants mis à disposition par le serveur d'application permet une prise en compte des besoins métier, des interactions avec les utilisateurs, des connexions avec les bases de données, etc.

Les serveurs d'applications sont des logiciels occupant la couche centrale dans une architecture multicouche, qu'elle soit classique trois tiers (postes clients, serveur d'applications, serveur de données) ou étendue N tiers lorsqu'elle intègre par exemple des serveurs d'acquisition (données de terrain, données de processus, de back-office, etc.) ou des serveurs d'interface (Gateway, systèmes coopérants externes, etc.).

Dans un sens plus large, un serveur d'applications peut être une machine servant à héberger des applications, soit pour permettre leur exécution depuis un poste client (mode client-serveur de données, généralement partage de fichiers et politiques de gestion des accès), soit pour déporter l'affichage sur le poste client (mode client-serveur d'affichage) [16].

1.8.3 Service web

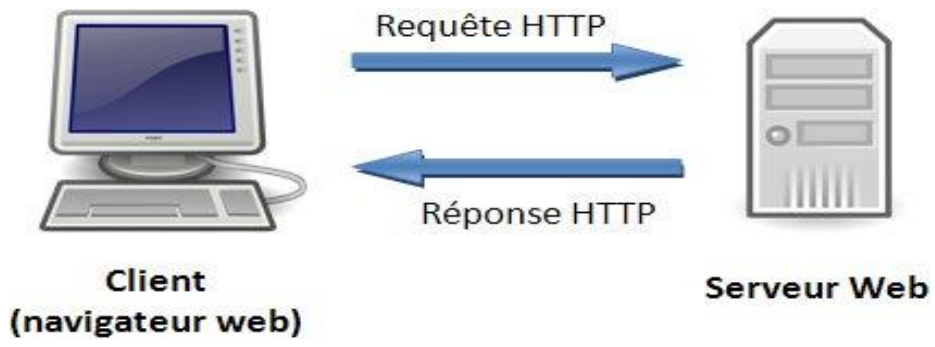


Figure 1.12 : Echange de requête entre client-serveur.

Un « serveur web » peut faire référence à des composants logiciels (software) ou à des composants matériels (hardware) ou à des composants logiciels et matériels qui fonctionnent ensemble.

1. Au niveau des composants matériels, un serveur web est un ordinateur qui stocke les fichiers qui composent un site web (par exemple les documents HTML, les images, les feuilles de style CSS, les fichiers JavaScript) et qui les envoie à l'appareil de l'utilisateur qui visite le site. Cet ordinateur est connecté à Internet et est généralement accessible via un nom de domaine tel que mozilla.org.
2. Au niveau des composants logiciels, un serveur web contient différents fragments qui contrôlent la façon dont les utilisateurs peuvent accéder aux fichiers hébergés. On trouvera à minimal un serveur HTTP. Un serveur HTTP est un logiciel qui comprend les URL et le protocole HTTP (le protocole utilisé par le navigateur pour afficher les pages web).

Au niveau le plus simple, à chaque fois qu'un navigateur a besoin d'un fichier hébergé sur un serveur web, le navigateur demande (on dit qu'il envoie une requête) le fichier via HTTP. Quand la requête atteint le bon serveur web (matériel), le serveur HTTP (logiciel) renvoie le document demandé, également grâce à HTTP [16]**.**

1.8.4 Service DHCP

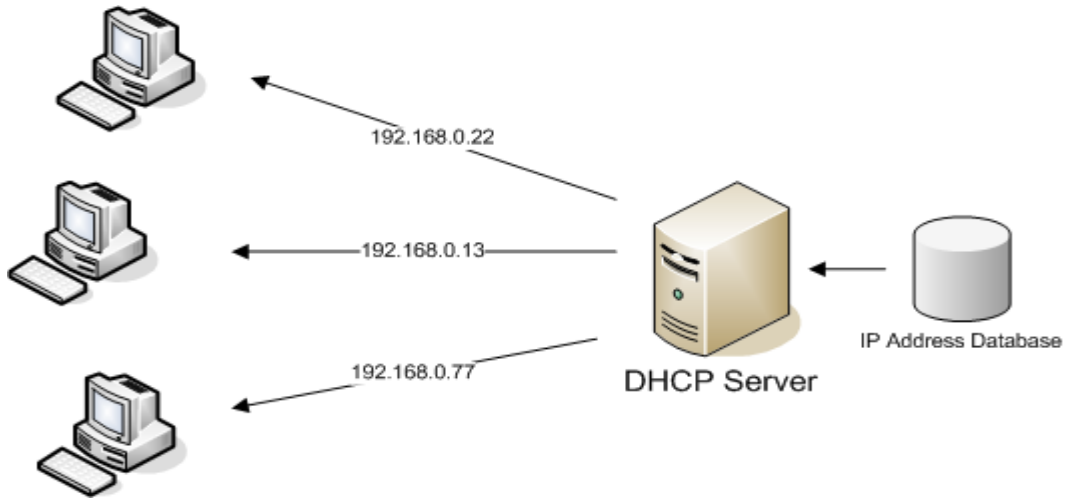


Figure 1.13 : principe de diffusion des adresses IP par le serveur DHCP.

Il existe donc deux méthodes pour obtenir une adresse IP. Soit c'est vous qui la configurez (méthode manuelle), soit c'est un serveur qui vous la donne (méthode dynamique). La méthode manuelle pose quelques problèmes de prime abord. En effet, vous avez vu que pour qu'une machine puisse communiquer avec ses voisines, son adresse IP devait se trouver

dans le même réseau que les autres machines. Pour sortir du réseau local, il faut que notre machine connaisse l'adresse de la passerelle. Cela fait déjà quelques informations dont il faut avoir connaissance quand vous branchez votre ordinateur à un réseau local.

On se rend donc bien compte qu'il serait bien d'avoir un mécanisme rapide et fiable pour adresser les machines d'un réseau. C'est là qu'entre en jeu le protocole DHCP, d'où c'est Un protocole pour distribuer des adresses IP

La première fonction d'un serveur DHCP (Dynamics Host Configuration Protocol) est de fournir des adresses IP (associées à un masque, bien évidemment) aux machines en faisant la demande.

Si vous avez configuré votre carte réseau pour récupérer son adresse IP automatiquement, votre machine va chercher à contacter un serveur DHCP susceptible d'être présent sur votre réseau local [17].

La figure 1.13 nous montre le principe de diffusion des adresse IP par un serveur DHCP.

1.8.5 Service DNS

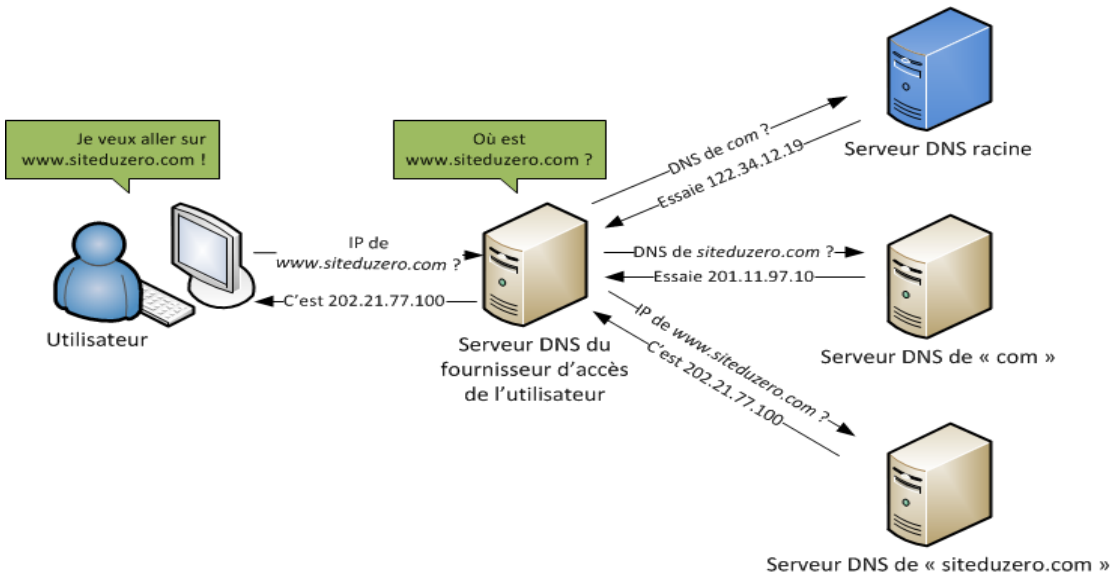


Figure 1.14 : principe de fonctionnement de serveur DNS.

Le serveur DNS (Domain Name System, ou Système de noms de domaine en français) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Pour simplifier, le serveur DNS agit comme un annuaire que consulte un ordinateur au moment d'accéder à un autre ordinateur via un réseau. Autrement dit, le serveur DNS est ce service qui permet d'associer à site web (ou un ordinateur connecté ou un serveur) une adresse IP,

comme un annuaire téléphonique permet d'associer un numéro de téléphone à un nom d'abonné.

Conçu en 1983 par Jon Postel et Paul Mockapetris, le DNS est aujourd'hui donc incontournable dans l'univers de la navigation sur le Web. Chaque fournisseur d'accès à Internet dispose notamment de ses propres serveurs DNS, avec des adresses IP qui prennent souvent la forme d'une succession de nombres de chiffres (194.158.122.10 par exemple).

Le dépôt d'un nom de domaine (du type "mondomaine.com") s'effectue auprès d'un "bureau d'enregistrement" ("registrar" en anglais), organisme intermédiaire entre les demandeurs (ou titulaires) de noms de domaine, et l'ICANN (Internet Corporation for AssignedNames and Numbers), société à but non lucratif responsable de l'allocation des adresses IP dans le monde via le système des noms de domaine [16].

La figure 1.14 nous montre le principe de fonctionnement de serveur DNS.

1.8.6 Service de messagerie

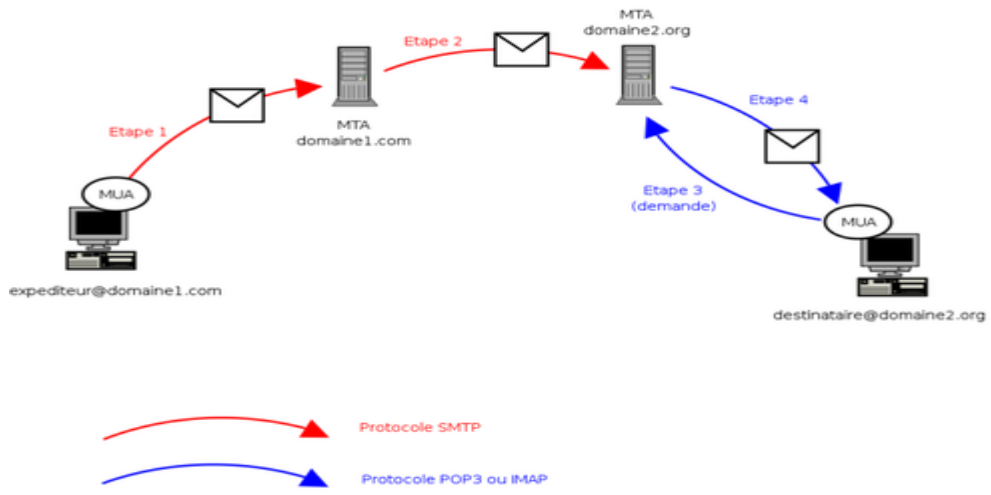


Figure 1.15: principe de fonctionnement de serveur de messagerie.

Un service de messagerie électronique, un logiciel serveur s'occupe alors de la gestion des transferts des messages. L'utilisateur final que vous êtes n'est jamais directement en contact avec ce serveur. Découvrez comment, en interne, le serveur de votre système informatique procède lors d'un envoi de mail [16].

SMTP, POP et IMAP sont les protocoles de messagerie qui définissent le moyen de transfert et de réception d'un mail. En un mot, vous pouvez envoyer un courrier électronique grâce au

protocole SMTP et vous pouvez le réceptionner sur votre ordinateur grâce au protocole POP ou au protocole IMAP [16].

Il existe deux types de serveur de messagerie : un serveur sortant, le serveur SMTP et serveur entrant, le serveur POP/IMAP [16].

La figure 1.15 nous montre le principe de fonctionnement de serveur de messagerie.

1.9 L'application propriétaire

1.9.1 Système de gestion de base de données

En informatique, un système de gestion de base de données est un logiciel système servant à stocker, à manipuler ou gérer, et à partager des informations dans une base de données, en garantissant la qualité, la pérennité et la confidentialité des informations, tout en cachant la complexité des opérations.

Un SGBD permet d'inscrire, de retrouver, de modifier, de trier, de transformer ou d'imprimer les informations de la base de données. Il permet d'effectuer des comptes rendus des informations enregistrées et comporte des mécanismes pour assurer la cohérence des informations, éviter des pertes d'informations dues à des pannes, assurer la confidentialité et permettre son utilisation par d'autres logiciels. Selon le modèle, le SGBD peut comporter une simple interface graphique jusqu'à des langages de programmation sophistiqués.

Les systèmes de gestion de base de données sont des logiciels universels, indépendants de l'usage qui est fait des bases de données. Ils sont utilisés pour de nombreuses applications informatiques, notamment les guichets automatiques bancaires, les logiciels de réservation, les bibliothèques numériques, les logiciels d'inventaire, les progiciels de gestion intégrés ou la plupart des blogs et sites web. Il existe de nombreux systèmes de gestion de base de données. En 2008, Oracle détenait près de la moitié du marché des SGBD avec MySQL et Oracle Data base. Vient ensuite IBM avec près de 20 %, laissant peu de place pour les autres acteurs.

Les SGBD sont souvent utilisés par d'autres logiciels ainsi que les administrateurs ou les développeurs. Ils peuvent être sous forme de composant logiciel, de serveur, de logiciel applicatif ou d'environnement de programmation [18].

1.10 Post Clients

Dans un réseau informatique, un client est le logiciel qui envoie des demandes à un serveur. Il peut s'agir d'un logiciel manipulé par une personne, ou d'un bot. Est

appelé client aussi bien l'ordinateur depuis lequel les demandes sont envoyées que le logiciel qui contient les instructions relatives à la formulation des demandes et la personne qui opère les demandes.

L'ordinateur client est généralement un ordinateur personnel ordinaire, équipés de logiciels relatifs aux différents types de demandes qui vont être envoyées, comme un navigateur web, un logiciel client pour le World wide web.

1.10.1 Les caractéristiques techniques d'un poste client

1.10.1.1 Processeur

Le processeur est un peu le cerveau de votre ordinateur. La vitesse et la rapidité de ce dernier dépendent en grande partie de lui. Il est composé de :

- **Cœur** : il s'agit du nombre de puces incluses dans le processeur. Le nombre de cœurs est très important, puisqu'il détermine le nombre de tâches que vous pourrez réaliser simultanément. Attention, le nombre de cœurs indiqué sur les fiches produits peut être soit physique, soit logique (séparation virtuelle que l'on appelle **Hyper-Threading**). Si vous êtes un gamer, nous vous conseillons de choisir un ordinateur comportant un processeur avec des cœurs uniquement physiques. Pour le multitâche classique en bureautique, l'hyper-threading est très adapté.
- **Fréquence** : il s'agit tout simplement de la vitesse de votre ordinateur. Plus elle est élevée, plus votre ordinateur ira vite. La fréquence est exprimée en Hz et correspond au nombre d'opérations par seconde que votre ordinateur va pouvoir faire. Un processeur avec une fréquence de 2GHz, pourra réaliser 2 milliards d'opérations à la seconde. Mais la fréquence donnée correspond à la somme des cœurs de votre processeur. Si vous avez un processeur 4 cœurs physiques cadencés à 2,5Ghz, vous aurez en réalité 2,5/4 = 625Mhz. Si vous avez 2 cœurs cadencés à 2,5Ghz, la fréquence de chaque cœur sera de 1,25Ghz. Un processeur 2 cœurs à 2.5Ghz ira donc plus vite pour une seule tâche qu'un 4 cœur de même fréquence. En revanche, si vous avez plusieurs petites tâches à effectuer, le 4 cœurs ira plus vite.
- **Mémoire cache** : c'est une mémoire tampon qui permet de stocker temporairement les données qui devant être traitées par le processeur. Ce procédé permet de réduire le temps d'attente et augmente donc la rapidité de votre processeur. La mémoire cache augmente ainsi la fréquence d'horloge d'un processeur.

1.10.1.2 La RAM

Quand vous voulez utiliser un logiciel, votre processeur récupère les données sur le disque dur et les charges sur la mémoire vive, il va ensuite principalement travailler avec la mémoire (la RAM) car elle travaille beaucoup, beaucoup plus vite, des milliers de fois plus vite, qu'un disque dur ou qu'un SSD.

C'est donc elle que le système utilise pour stocker ses tâches en cours. Plus on utilise de ressources sur son ordinateur, plus on va avoir d'une mémoire PC performante en vitesse, en volume de traitement et surtout en capacité.

1.11 System d'exploitation

Figure 1.16: les systèmes d'exploitation les plus utilisables.

En informatique, un système d'exploitation (souvent appelé OS de l'anglais Operating System) est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs. Il reçoit des demandes d'utilisation des ressources de l'ordinateur ressources de stockage des mémoires (par exemple des accès à la mémoire vive, aux disques durs), ressources de calcul du processeur central, ressources de communication vers des périphériques (pour parfois demander des ressources de calcul au GPU par exemple ou tout autre carte d'extension) ou via le réseau de la part des logiciels applicatifs. Le système d'exploitation gère les demandes ainsi que les ressources nécessaires, évitant les interférences entre les logiciels.

Le système d'exploitation est un logiciel, le deuxième après le firmware et le principal programme exécuté lors de la mise en marche de l'ordinateur, le premier étant le programme d'amorçage .Il offre une suite de services généraux facilitant la création de logiciels applicatifs et sert d'intermédiaire entre ces logiciels et le matériel informatique. Un système

d'exploitation apporte commodité, efficacité et capacité d'évolution, permettant d'introduire de nouvelles fonctions et du nouveau matériel sans remettre en cause les logiciels.

Il existe sur le marché des dizaines de systèmes d'exploitation différents, très souvent livrés avec l'appareil informatique. C'est le cas de Windows, Mac OS, Irix, Symbian OS, GNU/Linux, (pour lequel il existe de nombreuses distributions) ou Android. Les fonctionnalités offertes diffèrent d'un système à l'autre et sont typiquement en rapport avec l'exécution des programmes, l'utilisation de la mémoire centrale ou des périphériques, la manipulation des systèmes de fichiers, la communication, ou la détection et la gestion d'erreurs. Toutefois, la modélisation CIM attribue à ce concept une classe de base CIM_OperatingSystem, éventuellement dérivée sous Windows, Linux ou z/OS [19].

1.11.1Windows

Gamme de systèmes d'exploitation développés par Microsoft et destinés aux ordinateurs compatibles PC.

La caractéristique principale de Windows est une gestion cohérente, normalisée, à l'aide de symboles, menus et champs de dialogue graphiques que l'on active généralement par un clic de la souris. Il n'est donc plus nécessaire de saisir les commandes manuellement, comme c'était le cas avec MS-DOS.

Le nom "Windows" provient du fait que l'on utilise des fenêtres pour représenter la surface de travail sur laquelle on exploite les programmes d'application et les documents. Les tâches générales, telles que l'impression et la gestion des éléments du système (disque dur, carte graphique, etc.), sont gérées centralement par Windows et mises à la disposition de tous les programmes d'application [19].

1.11.2Linux

Linux est un système d'exploitation complet et libre, qui peut être utilisé en lieu et place de systèmes d'exploitation commercialisés, tels que Windows, de Microsoft. Il est accompagné de nombreux logiciels libres complémentaires, offrant un système complet aux utilisateurs.

Le système peut être utilisé sur des serveurs (LAN ou serveurs web), sur des PC ou encore sur des smartphones.

Linux est disponible en plusieurs versions, téléchargeables gratuitement sur le net, et nommées "distributions", telles que Debian ou Ubuntu [19].

1.11.3Mac Os

Mac OS est le système d'exploitation des postes de travail d'Apple , Mac OS X, propose notamment une interface de bureau dotée de caractéristiques tridimensionnelles. OS X est doté d'une conception modulaire qui facilite l'ajout de nouvelles fonctions au système d'exploitation à mesure qu'elles sont disponibles. Il est possible d'y exécuter des applications UNIX ainsi que d'anciennes applications Mac [19].

1.12 La virtualisation

Le concept de "virtualisation" est fortement présent dans les entreprises. Il a pour objectif principal de diminuer les contraintes physique tout en augmentant la flexibilité.

La virtualisation couvre l'ensemble des techniques permettant de dissocier les caractéristiques physiques d'un système matériel ou logiciel des applications orientées utilisateurs. Elle est utilisée pour permettre le fonctionnement de plusieurs machines virtuelles disposant chacune de leur système d'exploitation spécifique partageant la même infrastructure physique [20].

Ce concept offre beaucoup d'avantages pour votre entreprise [20] :

- Economique et écologique : utiliser plusieurs serveurs sur une seule machine.
- Gestion : bonne répartition des charges et reconfiguration des serveurs en cas d'évolution ou de panne.
- Assistance : très efficace.
- Portabilité & migration.

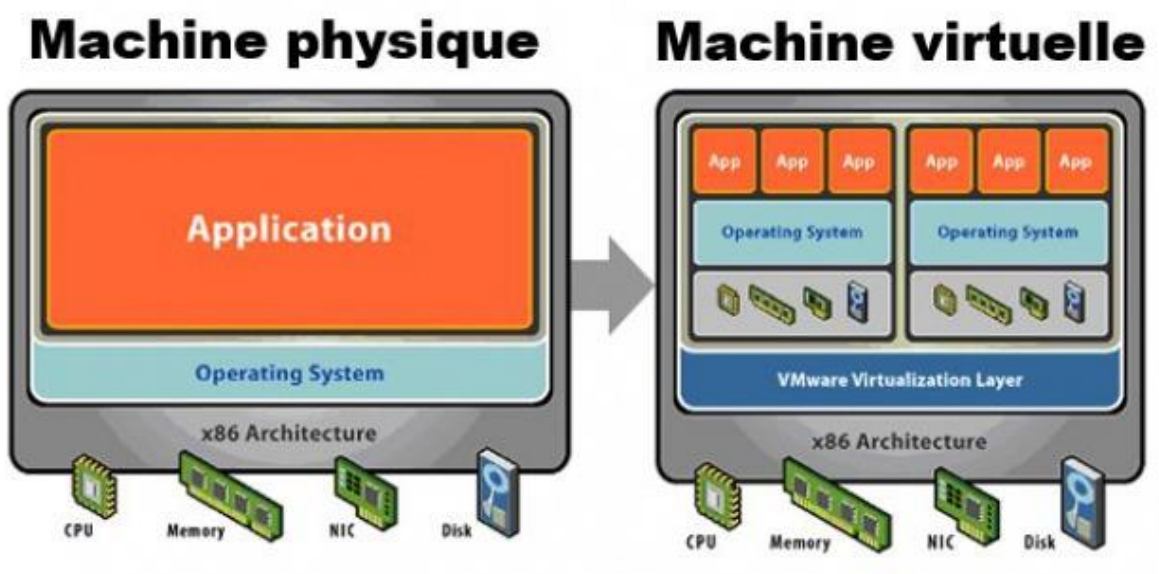


Figure 1.17 : principe de la virtualisation.

Dans la figure 1.17 on peut remarquer la différence entre une machine physique et virtuelle d'où la machine virtuelle peut avoir d'autre système d'exploitation qui s'exécute au même temps et qui auront donc a partagé les outils physiques comme la RAM le cpu [20]**.**

1.12.1La virtualisation de l'application

Dissocier l'application du système d'exploitation hôte, des autres applications présentes afin d'éviter les conflits.

Les applications sont transformées en services virtuels, administrés de façon centralisée, sans nécessiter d'installation sur le PC. Elles restent exécutées en local sur des postes de travail traditionnels dont elles exploitent les ressources [21]**.**

Les avantages sont [21] **:**

- Simplification de l'administration et du déploiement du parc informatique notamment lors de l'installation des nouvelles versions.
- Isolement des applications permettant de pallier les incompatibilités.
- Créer, pour chaque application, des copies des ressources partagées.

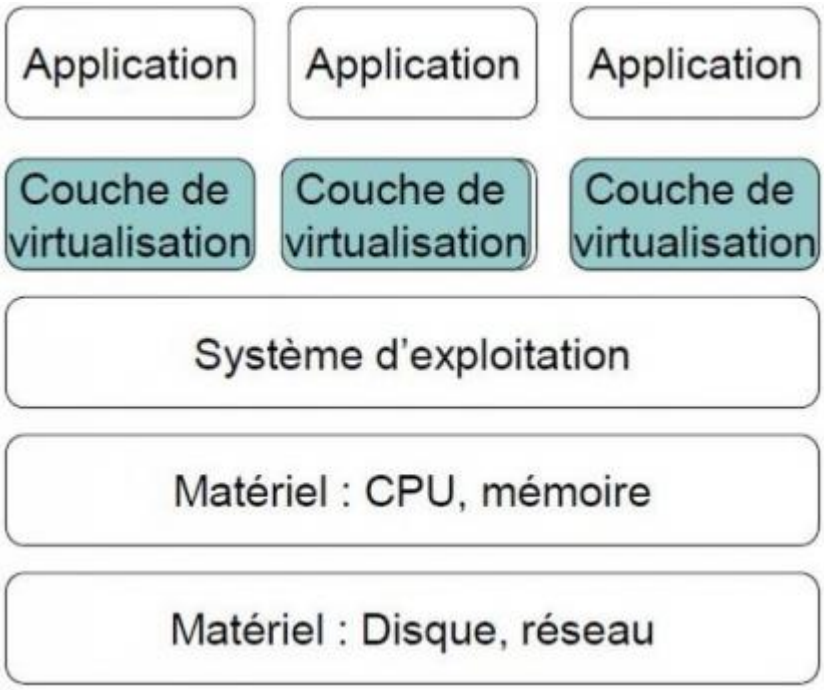


Figure 1.18 : la virtualisation de l'application.

La figure 1.18 nous montre la virtualisation de l'application.

1.12.2La virtualisation de session Windows

Délivrer des applications aux utilisateurs de façon centralisée.

Les applications sont alors directement installées dans des « sessions Windows virtuelles » sur un serveur dédié. Les utilisateurs accèdent à leurs sessions depuis des postes traditionnels ou des clients légers. Les applications étant exécutées sur les serveurs, le niveau de performance des terminaux n'a que peu d'importance [21]**.**

Les avantages sont [21]**:**

- Réductions des couts de déploiement, de mise à jour, de configuration.
- Augmentation de la durée de vie des postes de travail.
- Accès distants aux applications ou à utilisateurs tiers.
- Offrir une plus grande mobilité aux utilisateurs. Les applications sont accessibles depuis n'importe quel poste, n'importe quel OS (utilisateur nomade, poste en libre accès, télétravail...).

1.12.3La virtualisation du système d'exploitation

Exécuter sur une même plateforme matériel plusieurs environnements (systèmes d'exploitation) afin d'optimiser et de consolider les ressources physiques des infrastructures informatiques [21].

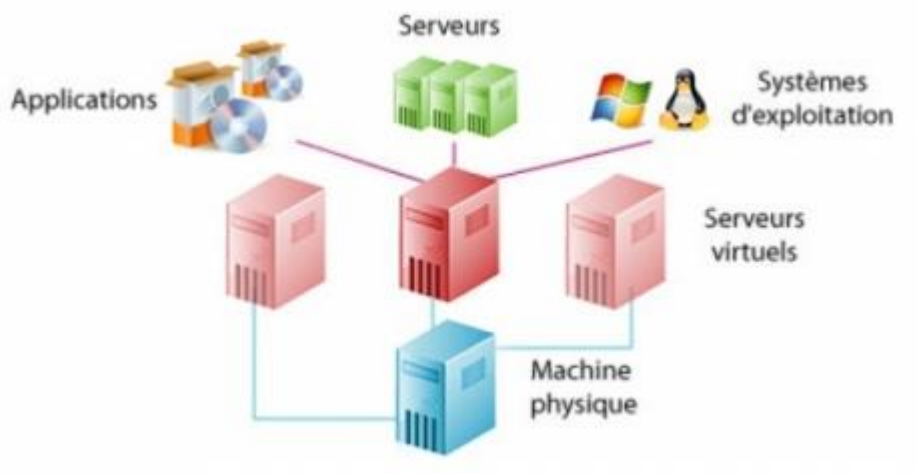


Figure 1.19 : la virtualisation du système d'exploitation.

La figure 1.19 nous montre la virtualisation d'un système d'exploitation.

1.13 Virtualisation des serveurs

Rentabiliser son parc informatique et utiliser efficacement les ressources des serveurs disponibles.

Pour cela, par un principe d'émulation, une couche logicielle, l'hyperviseur, isole les ressources physiques des systèmes d'exploitation. Ceux-ci s'exécutent alors sur des "machines virtuelles". Par ce principe plusieurs systèmes d'exploitation peuvent cohabiter sur une même machine, indépendamment l'un de l'autre [21].

Les avantages sont [21]:

- Consolidation des serveurs et optimisation de l'infrastructure : accroissement du taux d'utilisation des ressources en sortant du schéma « une application = un serveur ».
- Réduction des couts de l'infrastructure physique : réduction du nombre de serveurs et réduction de la quantité de matériel informatique.
- Augmentation de la flexibilité et de l'efficacité opérationnelle : nouvelle manière de gérer l'infrastructure informatique et gain de temps pour les administrateurs.

- Disponibilité accrue des applications et amélioration de la continuité d'activité : élimination des interruptions de service programmées et rétablissement rapide du service en cas d'interruptions non programmées.

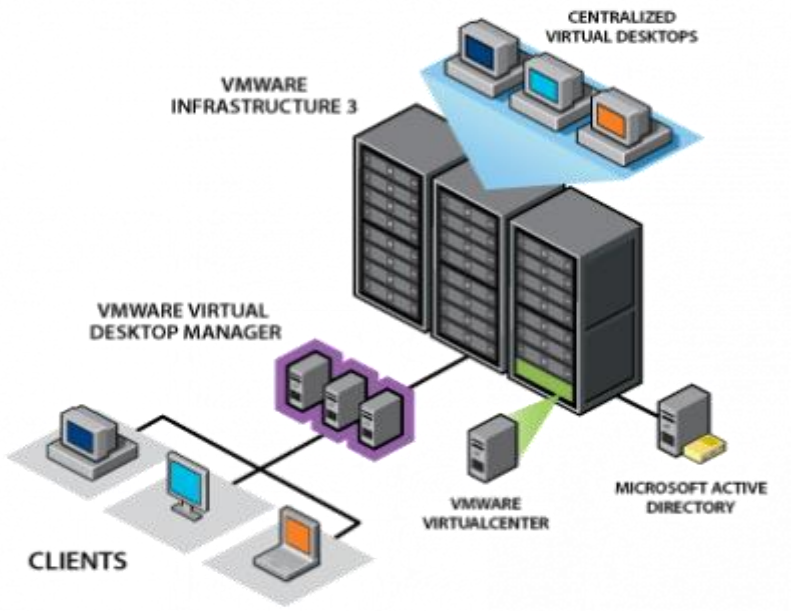


Figure 1.20 : la virtualisation d'un serveur.

La figure 1.20 nous montre la virtualisation d'un serveur.

1.13.1Virtualisation du poste de travail

Gérer beaucoup plus facilement les postes de travail des entreprises et de répondre plus simplement aux demandes des utilisateurs.

L'ensemble des ressources du poste client, données et logiciel, sont sur le serveur. L'administration est très nettement simplifiée tout comme la mobilité des utilisateurs (bureau virtuel). La virtualisation du poste client est un moyen radical mais efficace pour maitriser le cout de possession TCO. Les environnements (système d'exploitation et applications) sont intégralement exécutés sur les serveurs.

Déployez, gérez et surveillez des environnements de postes de travail sécurisés auxquels les utilisateurs finaux peuvent accéder localement ou à distance, avec ou sans connexion réseau, à partir de presque tous les ordinateurs de bureau, portables ou de poche [21]**.**

Les avantages sont [21] **:**

- Amélioration de la gestion et de la sécurité des postes de travail.
- Prolongement du cycle de vie des terminaux.

Figure 1.21 : virtualisation du poste de travail.

Ma figure 1.21 nous montre la virtualisation du poste de travail.

1.13.2Virtualisation du stockage

Masquer les spécificités physiques des unités de stockage.

Elle forme une couche de virtualisation active et transparente entre les périphériques de stockage sur disque afin d'optimiser la disponibilité, les performances et l'utilisation des petits et grands Datacenter. L'ensemble intègre des fonctions gérées de manière centralisée de protection des données, de provisionnement, de mise en cache, de réplication et de migration [22]**.**

Les avantages sont [22]**:**

- Prolongement du cycle de vie de vos investissements en matière de stockage et ce de manière rentable.
- Bénéficie d'un premier niveau de Plan de Reprise d'Activité.

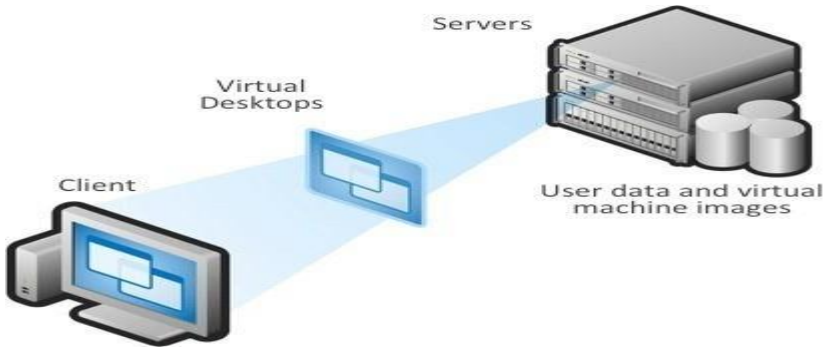


Figure 1.22 : virtualisation du stockage

1.13.3Les avantages de la virtualisation

- **Migration en direct** : des bases de données virtuelles peuvent être déplacées d'un serveur physique vers un autre sans interruption de fonctionnement [22]**.**

- **Déploiement simple et rentable de solutions à disponibilité élevée.**

- **Déploiement flexible, dynamique et automatisé** de nouvelles instances et ressources de système lorsque cela est nécessaire (extensibilité) [22]**.**

- **Possibilité d'un développement de base de données souple** : utiliser des appareils virtuels différents avec des systèmes ou des versions de bases de données différentes permet le développement ou la réalisation de tests dans le cadre du principe essais et erreurs du développement du logiciel souple. Différents supports de système peuvent être ajustés, modifiés ou supprimés sans trop de difficultés et sans le risque d'altérer les bases de données « achevées » dans certaines circonstances [22]**.**

- **Disponibilité améliorée** : en séparant les appareils virtuels les uns des autres, le système complet peut continuer de fonctionner correctement sans sacrifier le rendement lorsque des problèmes surviennent sur un seul appareil virtuel [22]**.**

Il n'est pas étonnant que la virtualisation des bases de données augmente aussi de plus en plus. Mais malgré ces avantages, elle peut également avoir des inconvénients si l'application est menée trop rapidement et sans préparation suffisante. Car il y a plusieurs éléments à considérer lorsque vous mettez en place la virtualisation d'une base de données. Des problèmes peuvent survenir en particulier dans certains cas [22]**.**

1.13.4Les inconvénients de la virtualisation

- **Virtualisation avec deux appareils informatiques de petite taille** : les bases de données ont généralement besoin de nombreuses ressources, que ce soit dans un système réel ou virtuel. Les systèmes de bases de données virtualités basés sur Microsoft SQL Server, ainsi que sur Oracle et d'autres, ont besoin, tout comme les « vraies » bases de données, de processeurs puissants et surtout d'une mémoire importante pour que toutes les données soient traitées de manière rapide par le système. Si ces critères ne sont pas fournis par l'appareil virtuel, cela peut entrainer une dégradation du rendement significative [23]**.**

- **Licences** : dans certains cas, comme avec des bases de données Oracle plus anciennes, les licences des bases de données précédentes ne peuvent pas être transférées vers un système virtualité, étant donné que les charges sont liées au rendement (potentiel) du système et non à ce qui est réellement utilisé. Il est alors important avant une transition de considérer en premier lieu le nombre d'instances et de processeurs qui vont être utilisés pour obtenir une comparaison entre le cout d'un serveur de base de données physique et ses homologues virtuels [23]**.**

- **Expertise de l'équipe insuffisante ou inexistante** : les bases de données sont par nature complexes, la virtualisation ne change rien à ce fait. La nouvelle technologie est associée à une couche de virtualisation supplémentaire qui ajoute une certaine complexité pour les administrateurs de bases de données. Si, dans l'entreprise, aucune différenciation n'est faite entre les administrateurs de virtualisation et les administrateurs de bases de données, alors l'employé doit acquérir des connaissances poussées en virtualisation de bases de données en plus de son savoir-faire « habituel » [23]**.**

- **Manque d'échange ou de coopération entre les administrateurs informatiques et les administrateurs de bases de données** : beaucoup d'administrateurs de bases de données n'ont pas de véritable accès aux profondeurs de la couche de virtualisation, étant donné qu'elle est gérée par les administrateurs informatiques. Lorsque des problèmes liés à une base de données virtuelle surviennent, causés par une anomalie dans l'appareil virtuel ou le système virtuel, cela entraine souvent de longs retards dans la résolution du problème [23]**.**

1.14 Conclusion

Actuellement, l'infrastructure réseau occupent le cœur des systèmes d'information dans les entreprises, les industries ou les institutions, dans ce chapitre on s'est base sur la question ' on supervision quoi ' pour l'application de notre sujet, Le chapitre suivant donnera une vue détaillée sur la supervision informatique et comment super visionne.

2 Chapitre 2 : Supervision Informatique

2.1 Introduction

La gestion d'un parc de serveurs est un travail à temps réel. Un bon administrateur réseau doit savoir à tout moment l'état des différentes machines et des différents services.

Cependant, l'administrateur ne peut pas se permettre de passer son temps devant un tableau avec des voyants verts en attendant qu'un voyant passe au rouge pour agir, son temps est occupé à d'autres tâches, donc il ne peut pas surveiller les statuts des machines en permanence. L'examen quotidien des logs systèmes est un bon début, mais, si un problème survient, on s'en rend compte seulement le lendemain, ce qui peut être trop tard.

Pour simplifier leur travail, les administrateurs utilisent généralement ce qu'on appelle un moniteur de supervision informatique'', un tel moniteur permet d'avoir une vue globale du fonctionnement de réseau ainsi que du niveau de performances des systèmes, et d'alerter par différents moyens l'apparition d'une anomalie.

Dans ce chapitre, nous allons présenter les notions de base concernant la supervision informatique [24]**.**

2.2 Définition de la supervision informatique

En informatique, la supervision est une technique de suivi, qui permet de surveiller, analyser, rapporter et d'alerter les fonctionnements anormaux des systèmes informatiques.

Le Monitoring s'agit de répéter de manière régulière un processus de test ou de surveillance d'une personne ou d'un bien. Le but étant d'obtenir très rapidement et simplement une vision précise des évènements ou anomalies sur la période analysée.

Entre outre, La supervision informatique consiste à indiquer et/ou commander l'état d'un serveur, d'un équipement réseau ou d'un service software pour anticiper les plantages ou diagnostiquer rapidement une panne [24]**.**

2.3 Que peut-on superviser ?

La supervision est un vaste domaine de l'informatique qui reprend plusieurs activités dont les principales sont :

Surveiller, Visualiser, Analyser, Piloter, Alerter.

La véritable question à se poser serait " est-ce qu'un système d'information peut ne pas avoir de faille ? " Concrètement an de maintenir un fonctionnement optimal, tout devrait être supervisé, ou du moins peut-être supervisé du moment que l'on peut déterminer son état :

(Réseau, Serveurs, Périphériques, Postes, Clients, Applications...)

Libre à l'administrateur de placer des niveaux de priorités entre plusieurs éléments pour dénir ce qui doit ou ce qui ne doit pas être supervisé selon plusieurs critères (charge du réseau, manque de moyens...). Actuellement à la L'université Saad dahleb, ne sont supervisés que les switch, serveurs et tout ce qui touche à l'état du réseau en lui-même. Il sera important de rajouter les diérentes imprimantes et multifonctions en réseau parmi les périphériques à superviser.

Concernant les postes de travail, ils sont trop nombreux et les remontées d'informations sur ceux-ci ne seraient pas assez pertinentes pour évaluer les problèmes. Des outils d'administration plutôt que de supervision seront à adopter pour ce type de matériel [25].

2.4 Comment superviser ?

2.4.1 La supervision ne se limite plus à l'infrastructure

Si l'infrastructure informatique reste le domaine privilégié de la supervision, il n'est plus le seul à pouvoir être supervisé : applications, respect des SLA ou encore processus informatisés sont les cibles des outils de supervision actuels [26].

Quel que soit le domaine, les catégories de points de contrôle sont les mêmes [26]**:**

- Contrôle de disponibilité

Il s'agit de vérifier la présence d'un serveur, d'un switch ou encore d'une application sur le réseau. Une requête Ping sera généralement utilisée.

Un contrôle de disponibilité est souvent combiné avec un contrôle de performance permettant par exemple de remonter une information sur la latence réseau.

- Contrôle de performance

Il s'agit d'effectuer une mesure et de la comparer à des seuils de criticité. Par exemple : performance d'un CPU, taux d'occupation d'un disque dur mais aussi nombre de commandes sur un site de e-commerce, durée moyenne d'un processus, etc.

- Contrôle d'intégrité

Les contrôles de cette catégorie servent à vérifier l'intégrité de l'élément supervisé. Par exemple : présence d'alertes dans un fichier journal, format incorrect d'un fichier d'échange, commandes passées hors horaire de bureau, incohérence de données entre deux applications, etc.

Cette liste est loin d'être exhaustive, chaque société possède ses propres spécificités et ses indicateurs de performance.

2.4.1.1 Supervision de l'infrastructure

La supervision de l'infrastructure est de loin la plus implémentée dans les entreprises. Elle couvre toutes les couches matérielles et logicielles du réseau au système d'exploitation en passant par les serveurs et les middlewares [26]**.**

Ci-dessous quelques exemples non exhaustifs de ce qu'il est possible de superviser [26] **:**

- Supervision du réseau

Disponibilité des switches et routeurs.

Mesure de la latence et du taux d'erreurs d'une liaison.

Mesure de la bande passante.

Contrôle de cohérence des routes et VLAN (Virtual Local Area Network).

- Supervision matérielle et environnementale

Mesure de température et d'humidité (à l'aide des sondes adéquates).

Mesure des IO disque ou réseau.

Mesure du taux de charge d'un onduleur.

Surveillance d'une panne de lecteur de cassette de sauvegarde.

Surveillance de l'état du RAID, des alimentations redondantes, des ventilateurs, etc.

- Supervision système

Mesure de la fréquence processeur et de l'utilisation de la mémoire vive.

Mesure du taux de remplissage des disques.

Surveillance du journal d'évènements système.

- Supervision des middlewares

Vérification du démarrage des services.

Mesure du temps de traitement d'une requête SQL.

Mesure et suivi du nombre de machines virtuelles sur un hyperviseur.

2.4.1.2 Supervision applicative

La majorité des implémentations de supervision applicative dans les entreprises se limitent à superviser la disponibilité des ports applicatifs et des processus. C'est bien sûr nécessaire mais pas suffisant pour une supervision efficace des applications. Il est conseillé de vérifier le fonctionnel de l'application grâce à des tests spécifiques.

En général, le test consiste à jouer un scénario fonctionnel sur l'application, en vérifiant un résultat prédictif : recherche d'un fournisseur, création d'une commande et annulation, etc. Sur des applications développées par l'entreprise, il est aussi possible d'implémenter un autotest qui sera simplement appelé par la solution de supervision via une requête HTTP ou un appel de Web Service par exemple. La connaissance fonctionnelle est ainsi conservée par l'application elle-même.

Bien entendu, une attention particulière doit être apportée à la sécurité. Les comptes utilisés pour la supervision doivent être bien identifiés et avec des droits très limités [26]**.**

2.4.1.3 Supervision des SLA

Un SLA est défini entre autres par plusieurs points de contrôle mesurables avec des seuils à ne pas dépasser pour une période donnée. Par exemple, le SLA Disponibilité du site Internet sur le mois peut être défini par les points de contrôle suivants [26] **:**

- Le temps moyen de téléchargement d'une page ne dépasse pas 2 secondes
- La page d'accueil s'affiche correctement
- La page contact fonctionne
- Le processus de commande fonctionne

Ces indicateurs sont agrégés dans une métrique commune représentant le SLA.

2.4.1.4 Supervision des processus informatisés

Superviser un processus informatisé signifie superviser tous les éléments de la chaine composant ce processus. Tout comme la supervision des SLA, les points de contrôle sont ensuite agrégés pour construire un indicateur global sur l'état du processus [26]**.**

Une bonne représentation graphique du processus est primordiale pour une implémentation efficace.

Par exemple, un processus de commande sur Internet peut être supervisé grâce aux points de contrôle suivants [26] **:**

- Disponibilité du site et de la page de commande.
- Nombre de commandes sur le site.
- Cohérence entre le nombre de commandes enregistrées sur le site et dans l'ERP (Enterprise Resource Planning).
- Nombre de commandes "en préparation".
- Ancienneté moyenne des commandes.

Il existe des logiciels spécialisés en supervision des processus. Cependant, les outils de supervision classiques tendent à s'approprier ce domaine.

2.4.2 Quels moyens pour la supervision ?

2.4.2.1 Grands principes

Les deux règles d'or de la supervision sont d'être le moins intrusif possible et le plus indépendant possible des éléments supervisés afin de garantir un regard extérieur non biaisé [26].

Il n'est pas pertinent par exemple de superviser une infrastructure virtualisée si le serveur de supervision se situe lui-même dessus. De même il est préférable d'éviter au maximum d'installer des logiciels ou des scripts sur les éléments supervisés [26].

Centre on respecte ce principe en ne requérant pas d'agent spécifique sur les ressources supervisées. Il s'appuie de préférence uniquement sur le protocole SNMP (Simple Network Management Protocol), largement disponible aujourd'hui en standard sur les ressources.

Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes : les méthodes active et passive, détaillées dans les paragraphes suivants [26].

2.4.2.1.1 Supervision passive

La supervision passive l'est du point de vue du serveur de supervision : ce sont les ressources supervisées qui transmettent des alertes au serveur de supervision [26] :

- La ressource supervisée vérifie son état et transmet de manière autonome le résultat au serveur de supervision.
- Le serveur de supervision reçoit l'alerte et la traite.
- L'échange est unidirectionnel.

Figure 2.1: les échanges unidirectionnels des ressources vers le serveur de supervision.

La méthode passive présente plusieurs intérêts. D'abord elle est moins consommatrice de ressources du point de vue serveur de supervision et réseau. Ensuite, elle est utile dans le cas où l'accès aux ressources est difficile (DMZ (Démilitarise Zone), matériel propriétaire, etc.) [26]**.**

Ce mode de supervision ne souffre pas de la latence due aux vérifications périodiques, l'alerte arrive en véritable temps réel sur l'interface de Centreon [26]**.**

Le principal point noir de la supervision passive concerne la fraicheur des informations : rien ne permet de garantir que la ressource supervisée est dans un état correct si aucune n'alerte N'est reçue. Les ressources n'envoient que très rarement des messages pour signaler un état correct A cause de sa non-fiabilité, la supervision passive, en pratique, est surtout utilisée en complément de la supervision active pour la réception des trappes SNMP [26]**.**

Le protocole standardisé et privilégié pour la supervision passive est SNMP avec le mécanisme de trappes [26]**.**

2.4.2.1.2 Supervision active

La supervision active est la plus classique. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision. Cette méthode est composée de trois étapes [26] **:**

- Le serveur envoie une requête vers la ressource supervisée.
- La ressource répond à la requête du serveur.
- Le serveur analyse l'information et détermine un état pour la ressource.

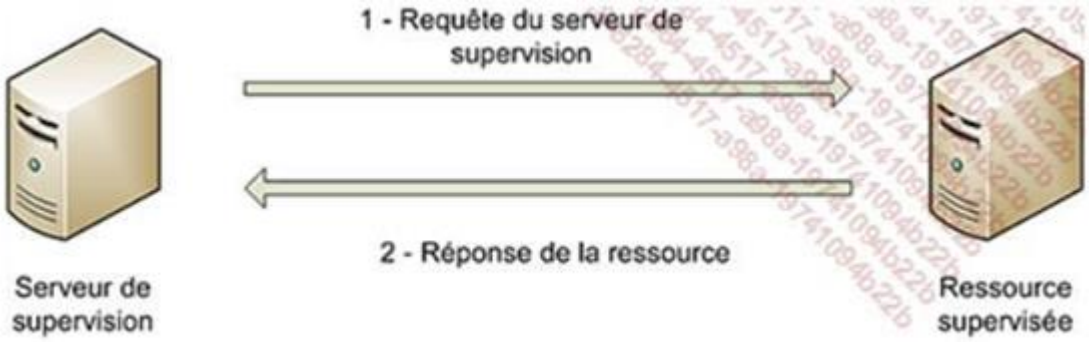


Figure 2.2 : les échanges entre serveur de supervision et les ressources de supervisions.

Cette méthode est la plus utilisée. Elle a l'avantage d'être fiable : les vérifications se font de manière régulière et en mode question-réponse [26]**.**

Les deux principaux protocoles de supervision active sont [26] **:**

- Le protocole SNMP (Simple Network Management Protocol) est le standard en matière de supervision active. Il est largement adopté et utilisé.
- Le protocole WMI (Windows Management Instrumentation) est un standard de supervision pour les systèmes Microsoft Windows.

Ces deux protocoles sont à privilégier car non intrusifs : les agents sont natifs aux systèmes supervisés.

Pour les systèmes fermés ou très isolés, la communauté Nagios propose le protocole NRPE (Nagios Remote Plugin Executor) qui demande l'installation d'un agent spécifique sur les systèmes supervisés. Il est compatible avec Centreon.

Certains protocoles d'administration peuvent également être utilisés pour la supervision : IPMI (Intelligent Platform Management Interface) pour la supervision de composants matériels, JMX (Java Management Extensions) pour les applications Java, etc.

Les protocoles systèmes SSH (Secure Shell) et Telnet sont également très utilisés. Ils permettent d'exécuter des commandes après connexion sur les systèmes supervisés.

Enfin, certains systèmes proposent des API propriétaires permettant de récupérer des états ou mesures [26]**.**

2.5 Les Protocoles nécessaire dans La supervision

2.5.1 Le protocole SNMP

2.5.1.1 C'est quoi SNMP ?

SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). C'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques. Ce protocole est donc utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau. Chaque machine, que ce soit sous Windows ou sous Linux possède de nombreuses informations capitales pour l'administrateur réseaux. On retrouve des informations comme la quantité de RAM utilisé, l'utilisation du CPU, l'espace disque et encore bien d'autre indicateurs. SNMP va permettre de remonter ces informations à l'administrateur de façon centralisé pour pouvoir réagir au plus vite aux pannes éventuelles [27].

2.5.1.2 Composants de base SNMP et leurs fonctionnalités

SNMP se compose de [28] **:**

- Gestionnaire SNMP.
- Appareils gérés.
- Agent SNMP.
- Base de données d'informations de gestion, autrement appelée base de données de gestion (MIB).

2.5.1.2.1 Gestionnaire SNMP

Un gestionnaire ou système de gestion est une entité distincte chargée de communiquer avec les périphériques réseau mis en œuvre par l'agent SNMP. Il s'agit généralement d'un ordinateur utilisé pour exécuter un ou plusieurs systèmes de gestion de réseau.

Fonctions clés du gestionnaire SNMP :

- Agents de requêtes.
- Obtient les réponses des agents.
- Définit les variables dans les agents.
- Reconnait les évènements asynchrones des agents [28]**.**

2.5.1.2.2 Périphériques gérés :

Un périphérique géré ou l'élément de réseau est une partie du réseau qui nécessite une certaine forme de surveillance et de gestion, par exemple routeurs, commutateurs, serveurs, postes de travail, imprimantes, onduleurs, etc [28].

2.5.1.2.3 Agent SNMP :

L'agent est un programme intégré à l'élément de réseau. L'activation de l'agent lui permet de collecter la base de données d'informations de gestion à partir du périphérique localement et la met à la disposition du gestionnaire SNMP, lorsqu'il est interrogé. Ces agents peuvent être standard (par exemple Net-SNMP) ou spécifiques à un fournisseur (par exemple, l'agent HP Insight) [28].

Fonctions clés de l'agent SNMP [28] :

- Collecte des informations de gestion sur son environnement local
- Stocke et récupère les informations de gestion telles que définies dans la MIB.
- Signale un évènement au gestionnaire.
- Agit en tant que proxy pour certains nœuds de réseau non SNMP gérables.

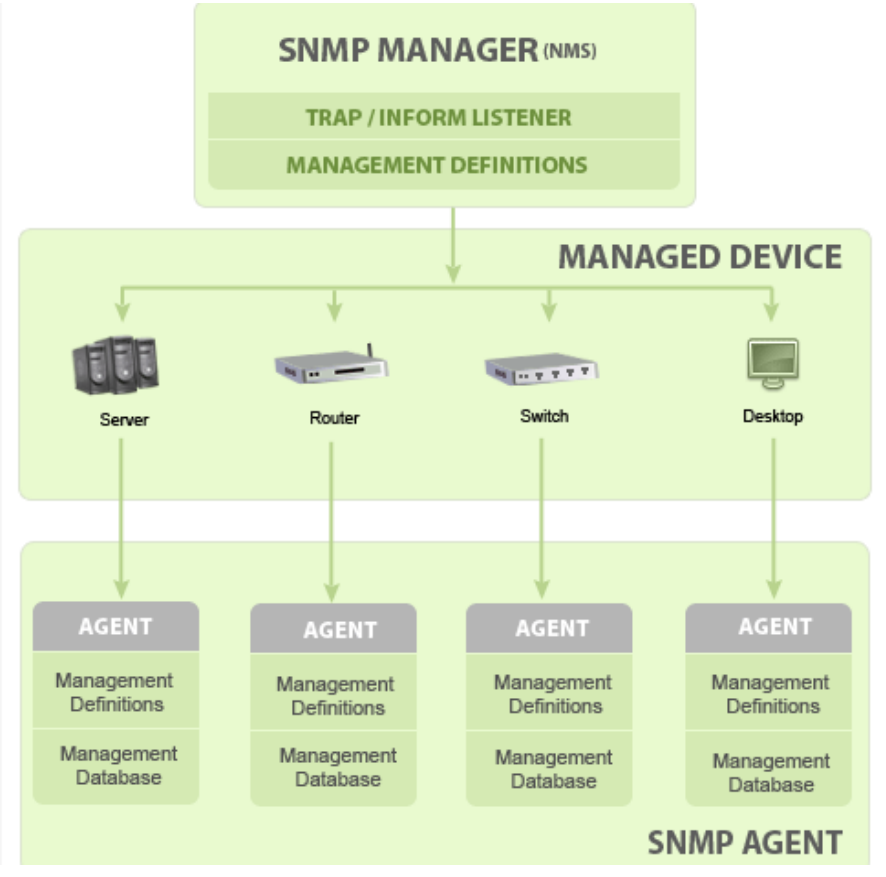


Figure 2.3: Basic SNMP Communication Diagramme.

2.5.1.2.4 Base de données d'informations de gestion ou base d'informations de gestion (MIB)

Chaque agent SNMP gère une base de données d'informations décrivant les paramètres du périphérique géré. Le gestionnaire SNMP utilise cette base de données pour demander à l'agent des informations spécifiques et traduit les informations selon les besoins du système de gestion de réseau (NMS). Cette base de données communément partagée entre l'agent et le gestionnaire s'appelle Management Information Base (MIB) [28].

En règle générale, ces MIB contiennent un ensemble standard de valeurs statistiques et de contrôle définies pour les nœuds matériels d'un réseau. SNMP permet également l'extension de ces valeurs standard avec des valeurs spécifiques à un agent particulier grâce à l'utilisation de MIB privées [28].

En bref, les fichiers MIB sont l'ensemble des questions qu'un gestionnaire SNMP peut poser à l'agent. L'agent collecte ces données localement et les stocke, comme défini dans la MIB. Ainsi, le gestionnaire SNMP doit être conscient de ces questions standard et privées pour chaque type d'agent [28].

2.5.1.3 Commandes de base de SNMP

La simplicité de l'échange d'informations a fait du SNMP un protocole largement accepté. La raison principale étant un ensemble concis de commandes, les voici ci-dessous :

- **GET** : l'opération GET est une demande envoyée par le gestionnaire au périphérique géré. Elle est effectuée pour récupérer une ou plusieurs valeurs du périphérique géré.
- **GET NEXT** : Cette opération est similaire à GET. La différence significative est que l'opération GET NEXT récupère la valeur du prochain OID dans l'arborescence MIB.
- **GET BULK** : l'opération GETBULK est utilisée pour récupérer des données volumineuses à partir d'une grande table MIB.
- **SET** : Cette opération est utilisée par les gestionnaires pour modifier ou affecter la valeur du périphérique géré.
- **TRAPS** : Contrairement aux commandes ci-dessus qui sont lancées à partir du gestionnaire SNMP, les TRAPS sont lancés par les agents. Il s'agit d'un signal adressé au gestionnaire SNMP par l'agent lors de la survenance d'un évènement.

- **INFORM** : Cette commande est similaire au TRAP initié par l'agent, INFORM comprend en outre une confirmation du gestionnaire SNMP à la réception du message.
- **RÉPONSE** : Il s'agit de la commande utilisée pour récupérer la ou les valeurs ou le signal des actions dirigées par le gestionnaire SNMP [28]**.**

2.5.1.4 Versions SNMP

Depuis sa création, SNMP a subi d'importantes mises à niveau. Cependant, le protocole SNMP v1 et v2c sont les versions les plus implémentées de SNMP. La prise en charge du protocole SNMP v3 a récemment commencé à rattraper son retard car il est plus sécurisé par rapport à ses anciennes versions, mais il n'a toujours pas atteint une part de marché considérable, plus de détail comme suivant : [29]**.**

SNMPv1 :

Il s'agit de la première version du protocole SNMP, qui est définie dans les RFC 1155 et 1157.

SNMPv2c :

Il s'agit du protocole révisé, qui comprend des améliorations de SNMPv1 dans les domaines des types de paquets de protocole, des mappages de transport, des éléments de structure MIB mais en utilisant la structure d'administration SNMPv1 existante ("basée sur la communauté" et donc SNMPv2c). Elle est définie dans RFC 1901, RFC 1905, RFC 1906, RFC 2578.

SNMPv3 :

SNMPv3 définit la version sécurisée du SNMP. Le protocole SNMPv3 facilite également la configuration à distance des entités SNMP. Il est défini par RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415.

Bien que chaque version ait évolué vers de riches fonctionnalités, l'accent a été mis sur l'aspect sécurité de chaque mise à niveau. Voici un petit clip sur chaque aspect de sécurité des éditions.

SNMP v1	Community-based security
SNMP v2c	Community-based security
SNMP v2u	User-based security
SNMP v2	Party-based security
SNMP v3	User-based security

Tableau 2.1 : Représentation des différentes versions du SNMP.

2.5.2 Le protocole WMI

WMI est l'implémentation Microsoft du Web-Based Enterprise Management (WBEM) et Modèle commun d'information (CIM) normes publiées par le Groupe de travail sur la gestion distribuée (DMTF) , Les deux normes visent à fournir un moyen indépendant de l'industrie de collecter et de transmettre informations relatives à tout composant géré dans une entreprise. Un exemple de composant géré dans WMI serait un processus en cours, une clé de registre, un service installé, des informations sur les fichiers, etc. Ces normes communiquent les moyens par lesquels les implémenter devraient interroger, remplir, structurer, transmettre, exécuter actions et consommer des données [30]**.**

À un niveau élevé, la mise en œuvre par Microsoft de ces normes peut être résumée comme suit [30] **:**

Composants gérés

Les composants gérés sont représentés comme des objets WMI - des instances de classe représentant des éléments hautement structurés

Données du système d'exploitation. Microsoft fournit une multitude d'objets WMI qui communiquent des informations liées au système d'exploitation. Par exemple. Win32_Process, Win32_Service, Antivirus Product Win32_StartupCommand, etc.

Consommer des données

Microsoft fournit plusieurs moyens pour consommer des données WMI et exécuter des méthodes WMI. Par exemple, PowerShell fournit un moyen très simple d'interagir avec PowerShell.

Requête de données

Tous les objets WMI sont interrogés à l'aide d'un langage de type SQL appelé WMI Query Langage (WQL). WQL permet contrôle fin sur lequel les objets WMI sont retournés à un utilisateur.

Remplissage des données

Lorsqu'un utilisateur demande des objets WMI spécifiques, le service WMI (Winmgmt) doit connaitre les moyens en pour remplir les objets WMI demandés. Ceci est accompli avec les fournisseurs WMI.

Un WMI fournisseur est une DLL basée sur COM qui contient un GUID associé qui est enregistré dans le Registre. WMI les fournisseurs font le gros du travail pour remplir les données - par exemple interrogation de tous les processus en cours d'exécution, énumération clés de registre, etc.

Lorsque le service WMI remplit les objets WMI, il existe deux types d'instances de classe : dynamique et objets persistants. Les objets dynamiques sont générés à la volée lorsqu'une requête spécifique est effectuée. Pour Par exemple, les objets Win32_Process sont générés à la volée. Les objets persistants sont stockés dans le CIM.

Structuration des données

La structure / le schéma de la grande majorité des objets WMI est décrit dans Managed Object Format (MOF) des dossiers. Les fichiers MOF utilisent une syntaxe similaire à C ++ et fournissent le schéma d'un objet WMI. Ainsi, alors que les fournisseurs WMI générer des données brutes, les fichiers MOF fournissent le schéma dans lequel les données générées sont formatées. De perspective des défenseurs, il convient de noter que les définitions d'objets WMI peuvent être créées sans fichier MOF.

Au lieu de cela, ils peuvent être insérés directement dans le référentiel CIM en utilisant du code .NET de base.

Transmission de données

Microsoft fournit deux protocoles pour la transmission de données WMI à distance : DCOM et Windows Remote Gestion (Win RM).

Exécution d'actions

Certains objets WMI incluent des méthodes qui peuvent être exécutées. Par exemple, une méthode courante exécutée par les attaquants pour effectuer un mouvement latéral est la méthode Create statique dans la classe Win32_Process. WMI fournit également un système d'évènementiel par lequel les utilisateurs peuvent enregistrer des gestionnaires d'évènements lors de la création, modification ou suppression de toute instance d'objet WMI.

La figure suivante fournit un aperçu de haut niveau de l'implémentation Microsoft de WMI et de la relation entre ses composants mis en œuvre et les normes qu'ils mettent en œuvre.

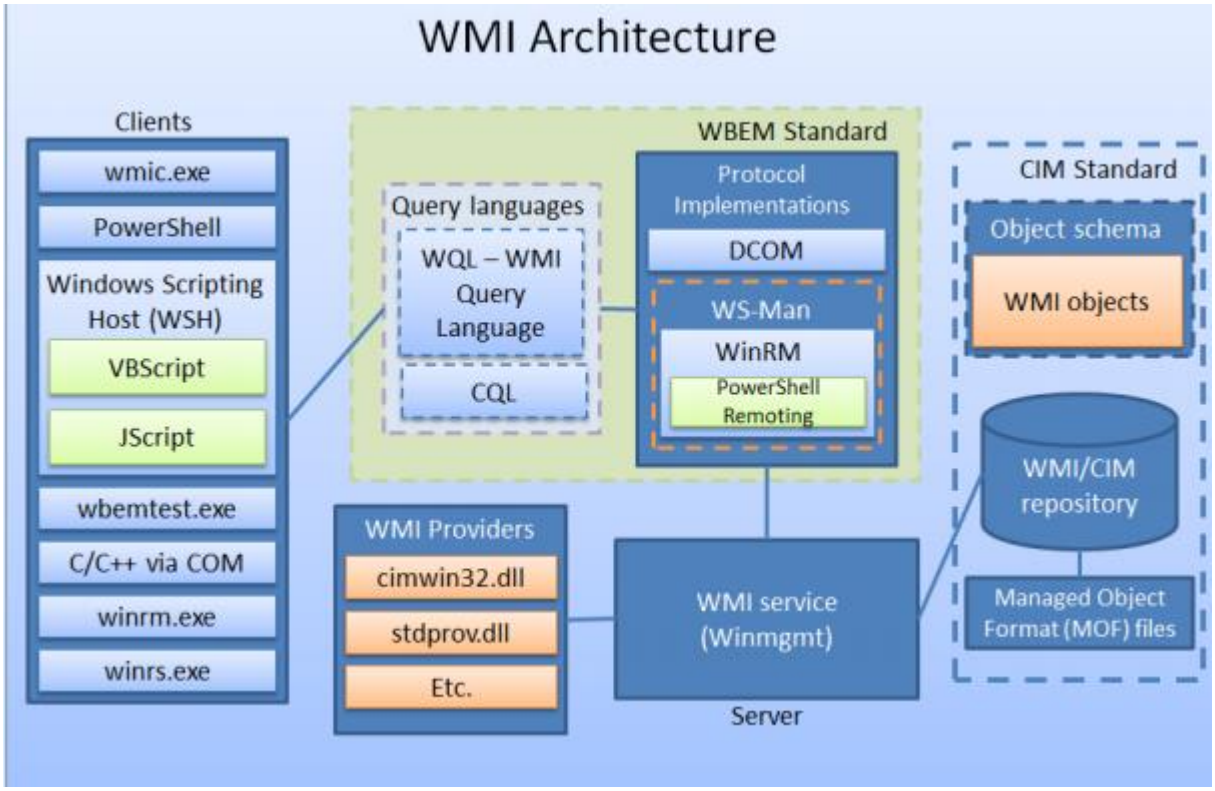


Figure 2.4 : Architecture WMI.

2.6 Évaluation du besoin en supervision

On vient de le voir, les solutions et protocoles de supervision sont nombreux. La DSI dispose donc d'un large choix d'outils lorsqu'elle souhaite mettre en place une supervision de son SI. Les besoins en supervision du SI du groupe Power flute requiert l'installation et la configuration d'un outil NMS. Ce type d'outil possède un coût, que ce soit en termes de licence ou de temps. Il est donc important de choisir la solution qui répond aux besoins actuels et futurs car elle accompagnera le SI pendant de nombreuses années.

En dehors de l'investissement que cela nécessite, il faut considérer la solution dans sa globalité et s'assurer qu'elle réponde correctement à chacun des besoins formulés par Power flute. Il faut donc se poser les bonnes questions dès le départ car c'est une étape importante pour la DSI mais également pour l'entreprise qui l'accompagne [31]**.**

Dans un premier temps, il est important de savoir [31]**:**

- Ce que l'on souhaite superviser. Quel est le périmètre présent et à venir ?
- Pourquoi superviser. Quels sont les problèmes déjà rencontrés ou possibles ?
- Pour qui superviser. Qui va devoir gérer et utiliser la supervision ?

Dans un second temps il faudra savoir comment nous souhaitons superviser.

D'où la solution doit proposer la possibilité de superviser les éléments essentiels au fonctionnement du réseau qui est le support indispensable à la bonne marche des unités du groupe Power flute. L'infrastructure réseau est récente, il y a donc peu de changements majeurs à envisager dans les quelques années à venir. Cependant la supervision Doit déjà être conçue avec assez de flexibilité pour s'adapter aux évolutions techniques futures [31]**.**

La mise en place d'un tel outil doit commencer par une analyse des chaines de liaisons qui composent le SI sur chaque site. Ces liaisons doivent-être décrites avec une granularité Suffisante pour identifier les points de contrôle essentiels, ainsi que leurs métriques. Il faut également recenser les applications et définir leur importance dans les processus métier. Il convient ensuite de représenter les différentes interactions entre ces applications pour définir les points critiques et les données à récolter [31]**.**

De cette première analyse, doivent ressortir des exigences précises que l'outil devra pouvoir accomplir. Il faut également définir les métriques réseaux utiles pour comprendre, contrôler et prédire le déroulement des applications. Afin d'être pertinentes pour les informaticiens et les utilisateurs des applications, ces métriques doivent avoir un sens du point de vue de l'application et pas seulement de l'infrastructure. Durant la phase de test on validera chacune de ces exigences pour être en mesure d'évaluer la pertinence de chaque outil [31]**.**

On en déduit alors plusieurs étapes [31]**:**

L'observation : consiste à regarder les applications métier dans leur ensemble et à comprendre le comportement et les exigences en termes de performance des applications, ceci afin de définir les sondes devant être utilisées.

La modélisation : il faut construire des modèles pour mieux comprendre l'utilisation du réseau faite par les applications.

Le déploiement : consiste à programmer la solution afin qu'elle réponde aux modèles préalablement définis.

La validation : c'est la phase durant laquelle l'équipe technique et les responsables métiers accordent sur les résultats obtenus durant les tests. Ces tests doivent satisfaire les exigences émises par les techniciens et les responsables métier.

Durant le déploiement de la solution, chaque sonde doit être paramétrée avec précision afin d'être à même de retourner un défaut uniquement quand il y a une situation réellement anormale. L'observation du comportement des sondes et des premiers graphiques générés par la supervision doit conduire à un ajustement du réglage de la solution [31]**.**

2.7 Quelque Logiciels de supervisions

NAGIOS

Créé en 1999 par Ethan Galstad, Nagios est un logiciel qui permet de superviser un système d'information. Il est considéré comme étant la référence des solutions de supervision open source. Il dispose de nombreuses fonctions telles que l'héritage multiple, les dépendances, l'escalade de notifications, les Template de services et d'hôtes, le support des surveillances actives et passives, etc. L'interface web est la partie graphique, via un serveur web tel que Apache, et qui va permettre à l'administrateur d'avoir une vue d'ensemble de son réseau, de visualiser la supervision des équipements et de produire des rapports d'activités [32]**.**

ZABBIX

Zabbix est un logiciel libre qui permet de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources. Le « serveur ZABBIX » peut être décomposé en trois parties séparées : Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être

disposée sur une machine différente pour répartir la charge et optimiser les performances. Il repose sur du C/C++, PHP pour la partie front end et MySQL / PostgreSQL / Oracle pour la partie base de données [32].

Vigilo NMS

Vigilo NMS est un logiciel publié sous licence GNU GPL version 2, destiné à la surveillance des systèmes, réseaux et applications informatiques. Il est écrit en Python, s'appuie sur le moteur de supervision Nagios et est compatible avec les greffons de celui-ci. Dans sa version communautaire, Vigilo NMS fournit un bac à alarmes ainsi qu'une interface de suivi des performances (métrologie). Les autres versions intègrent également le support de la haute-disponibilité, la répartition de charge, la corrélation des alarmes, la cartographie du parc et la génération automatique de rapports [32].

Solarwinds

Solarwinds propose aux professionnels de l'informatique une suite de logiciels de gestion des périphériques, systèmes et applications. De la défaillance et la performance à la configuration, en passant par la performance des applications et la gestion d'adresses IP, les utilisateurs peuvent consulter les statistiques en temps réel et la disponibilité de leur environnement informatique à partir de n'importe quel navigateur Web [33].

PRTG

Supervisez tous les systèmes et appareils, tout le trafic et toutes les applications de votre infrastructure IT, Avec PRTG, tout est compris. Pas besoin d'installer de plug-ins supplémentaires ou de télécharger quoi que ce soit, PRTG est une solution puissante et intuitive convenant aux entreprises de toute taille [34].

Op Manager Monitoring

Op Manager est un logiciel de gestion de réseau de bout en bout pour les réseaux informatiques d'entreprise hétérogènes et multifournisseurs. Il offre une approche unifiée pour faire évoluer et gérer l'infrastructure informatique distribuée, une fonctionnalité avancée de gestion des pannes et des performances sur l'ensemble des ressources informatiques critiques, à savoir. Périphériques réseau, liaisons WAN ou VoIP, serveurs, serveurs virtuels (VMware et Hyper-V), contrôleurs de domaine, MS Exchange, MS SQL et autres composants de l'infrastructure informatique.

Applications Manager fournit des informations critiques (telles que l'utilisation du processeur et de la mémoire, le nombre de threads et les détails de la base de données PGSQL) essentielles pour suivre les performances d'Op Manager, c'est ce logiciel que nous avons utilisé dans notre pratique [35]**.**

Pourquoi choisir OPMANAGER ?

On a choisi OpManager, car :

Il est facile a installé et à adapter, op manager contient une grande maps qui nous montre comme un résumé d'une architecture qui nous montre des différents équipements qu'on trouve dans notre entreprise, avec leur état, il suffit de cliquer sur l'un de nos périphériques est-il nous affiche des différents résultats comme son état, sa disponibilité son adresse IP ...

2.8 Conclusion

La supervision informatique est indispensable pour une entreprise qui a des défaillances d'un quelconque de ses services informatique et d'indispensabilité de son système d'information ces défaillance influent sur le rendement global de sa productivité, d'où l'application du système de supervision feront l'objectif de notre étude, le chapitre suivant donnera une vue détaillée sur le logiciel utilisé, dans le chapitre 3 on trouve plus de détails sur OpManager.

3 Chapitre 3 : Op Manager – Logiciel de surveillance réseau

3.1 Introduction

Les entreprises comptent sur les réseaux pour toutes les opérations. Par conséquent, la surveillance du réseau est très cruciale pour toute entreprise. Aujourd'hui, les réseaux s'étendent à l'échelle mondiale, ayant plusieurs liens établis entre des centres de données géographiquement séparés, des cloud publics et privés. Cela crée de multiples défis dans la gestion du réseau. Les administrateurs réseau doivent être plus proactifs et plus agiles dans la surveillance des performances du réseau. Cependant, cela est plus facile à dire qu'à faire.

Op Manager, une solution de surveillance réseau facile à utiliser et abordable. Il surveille les périphériques réseau tels que les routeurs, les commutateurs, les pare-feu, les équilibreurs de charge, les contrôleurs LAN sans fil, les serveurs, les machines virtuelles, les imprimantes, les périphériques de stockage et tout ce qui a une adresse IP et est connecté au réseau. Op Manager surveille en permanence le réseau et offre une visibilité et un contrôle approfondis sur celui-ci. En cas de panne, vous pouvez facilement explorer la cause première et l'éliminer avant que les opérations ne soient affectées [36].

3.2 Architecture OP Manager

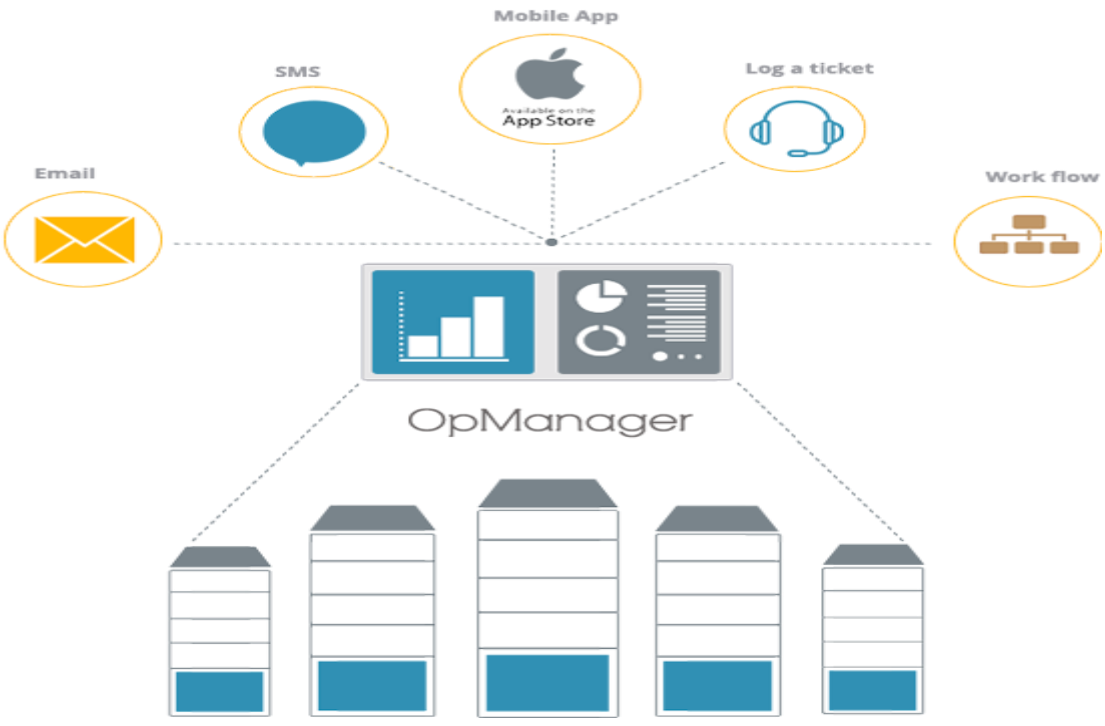


Figure 3.1 : Architecture op manager.

Op manager peut-être résumer dans une petite architecture avec ces différents caractères parmi eux [36] **:**

- Analyse en temps réel.
- Analyse des serveurs physique et virtuelle.
- Analyse base sur le seuil.
- Tableaux de bord personnalisable.
- Analyse des liaison Wan.
- Facile à configurer et abordable.

3.3 Console de gestion de réseau personnalisable

Op Manager dispose d'un tableau de bord largement personnalisable qui aide à transformer les données surveillées en intelligence exploitable pour le service informatique de l'entreprise. Avec plus de 90 widgets, le tableau de bord peut être modelé pour les besoins de chaque administrateur ainsi que dimensionné pour répondre à l'ensemble des besoins de gestion informatique [36]**.**

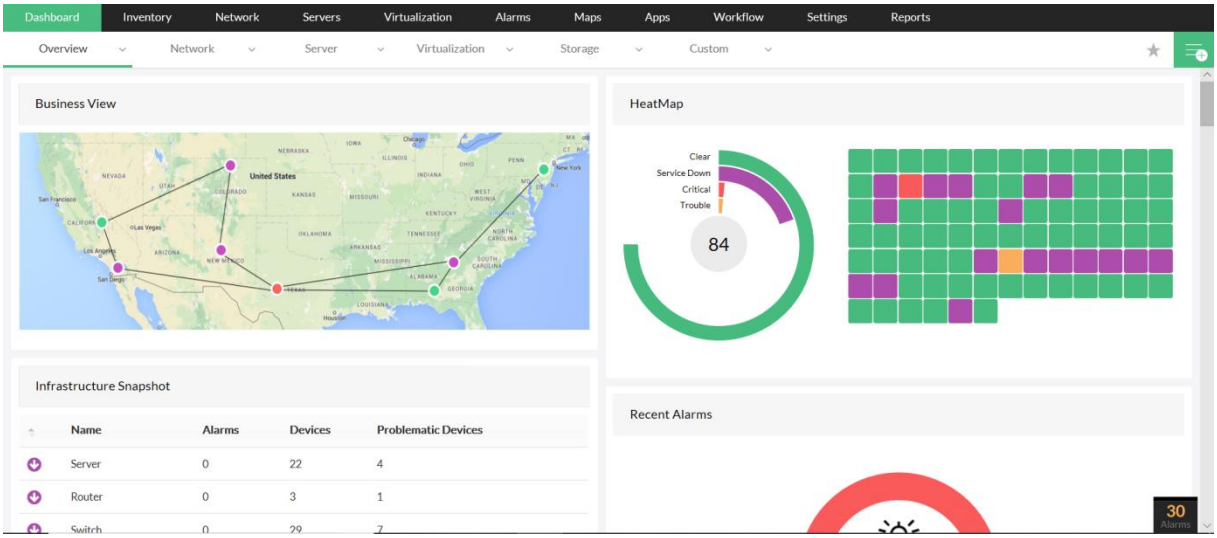


Figure 3.2 : vue d'entreprise de tableau d'bord afficher un groupe d'appareils et les liens.

Le tableau de bord fournit un aperçu en un coup d'œil de l'état actuel de votre réseau, avec des mesures critiques des routeurs, commutateurs, pare-feu, serveurs, services, application, URL, imprimante, onduleur et autres périphériques d'infrastructure. L'actualisation des données en un clic garantit que vous travaillez toujours avec les informations les plus à jour. Avec des graphiques de performances en temps réel facilement disponibles, les

administrateurs peuvent également dépanner rapidement et à distance les périphériques problématiques [36].

3.3.1 Le tableau de bord personnalisé fournit une puissante console de gestion de réseau contenant [37]

- Alarmes et évènements du réseau afin de mettre en évidence l'appareil qui nécessite une attention immédiate.
- Disponibilité et temps de réponse sur les appareils, URL, liaisons WAN et services.
- Statistiques de santé et de performance.
- Périphériques réseau.
- Serveurs, services et applications.
- Disponibilité et performances des interfaces / ports.
- Graphiques en temps réel pour les ressources et liens réseau critiques.
- Cartes regroupées par fournisseurs ou par types d'appareils (instantané d'infrastructure).
- Vues d'entreprise (regroupement d'appareils personnalisé en fonction de l'emplacement géographique ou des services d'entreprise ou d'un mappage logique).
- Widgets SLA.
- Autres liens texte ou HTML personnalisés.
- Vues plasma exclusives qui déploient le tableau de bord pour le projeter sur des fenêtres séparées, avec la possibilité de faire pivoter les tableaux de bord préférés sur des intervalles de temps égaux.

3.4 Surveillance du réseau en temps réel

Des bilans de santé et des audits de performance périodiques sont essentiels, mais lors de problèmes techniques, il devient très nécessaire d'analyser les données en temps réel. Par exemple, si un port de commutateur signale une utilisation de bande passante élevée, l'ingénieur réseau devra vérifier les statistiques d'utilisation en direct / les plus récentes de ce port particulier pour savoir si le problème persiste.

La plupart des administrateurs réseau exécutent de manière incommode des commandes via l'interface de ligne de commande sur leurs périphériques réseau ou à distance sur leurs serveurs pour vérifier les performances actuelles. Op Manager permet de signaler instantanément les performances de l'appareil en temps réel sans avoir à utiliser un autre outil pour accéder à distance à l'appareil problématique. Pendant les dégradations des performances du réseau, il suffit de lancer les graphiques en temps réel et d'obtenir à distance des informations actualisées sur les performances de l'appareil et son intégrité [38].

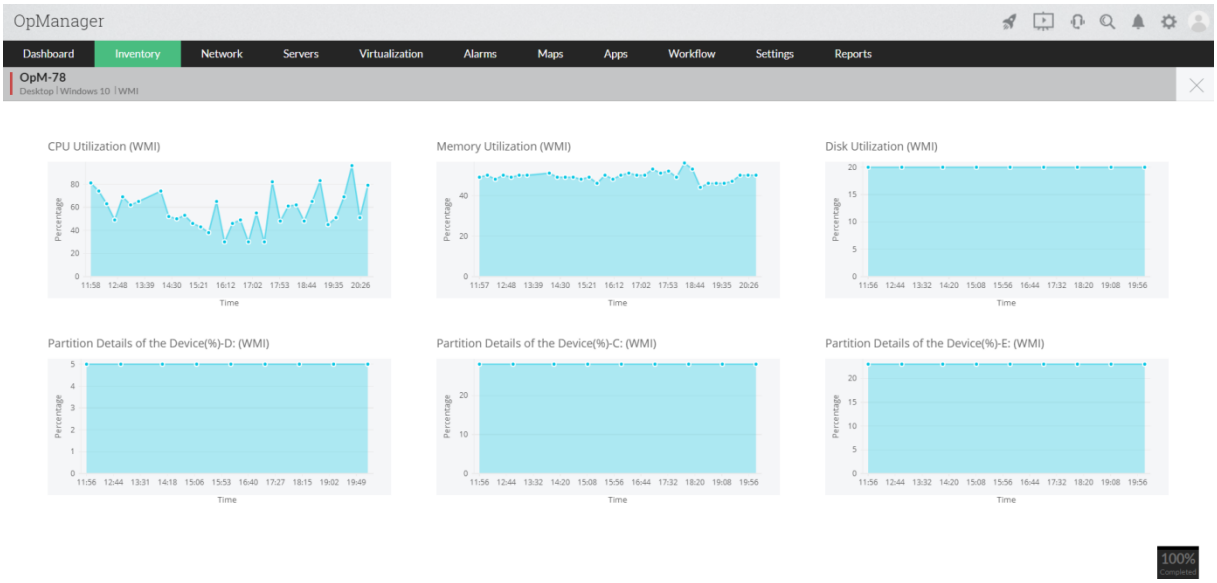


Figure 3.3 : Trafic d'interface en temps réel.

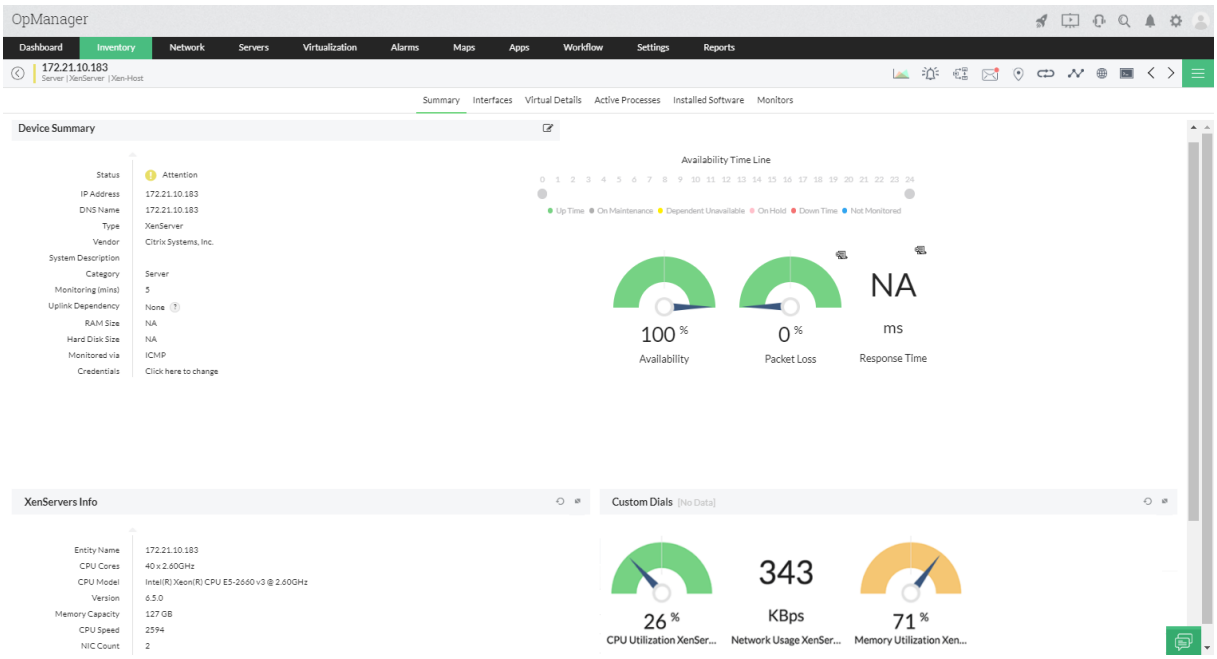


Figure 3.4 : Performances du serveur en temps réel.

3.4.1 Les graphiques en temps réel d'OpManager

- Statistiques en temps réel sur le processeur de l'appareil et l'utilisation de la mémoire.
- Informations actualisées sur toute mesure de performance d'un appareil.
- Trafic en temps réel / utilisation de la bande passante d'une interface / d'un port.

Les graphiques de performances en temps réel peuvent également être configurés en tant que widgets de tableau de bord pour permettre aux administrateurs de voir les tendances des performances en direct dès leur connexion [38].

3.5 Surveillance des performances du réseau

Les réseaux sont l'épine dorsale de chaque entreprise. Même dans les petites entreprises ou les entreprises, la perte de productivité lors d'une panne de réseau peut entrainer de lourds dommages. La surveillance du réseau vous aide à anticiper les pannes potentielles et à résoudre les problèmes de réseau de manière proactive. Cela aide à maintenir un réseau sans congestion qui maintient votre entreprise opérationnelle. Alors on a besoin d'un logiciel surveillance réseau pour surveiller les performances de tout appareil IP et aide les entreprises à visualiser à distance les performances de leur système et à surveiller les services réseau, l'utilisation de la bande passante, les commutateurs, les routeurs et le flux de trafic [37].

3.5.1 Facteurs ayant un impact sur les performances du réseau [39]

- Disponibilité
- CPU et mémoire
- Trafic
- Erreurs et rejets
- Performances WAN

3.5.1.1 Disponibilité

OpManager envoie un Ping à tous les appareils surveillés à des intervalles de surveillance définis, et si un appareil est en panne ou si le temps de réponse ou la perte de paquets est énorme, OpManager vous avertit immédiatement en envoyant un e-mail ou un SMS [39].

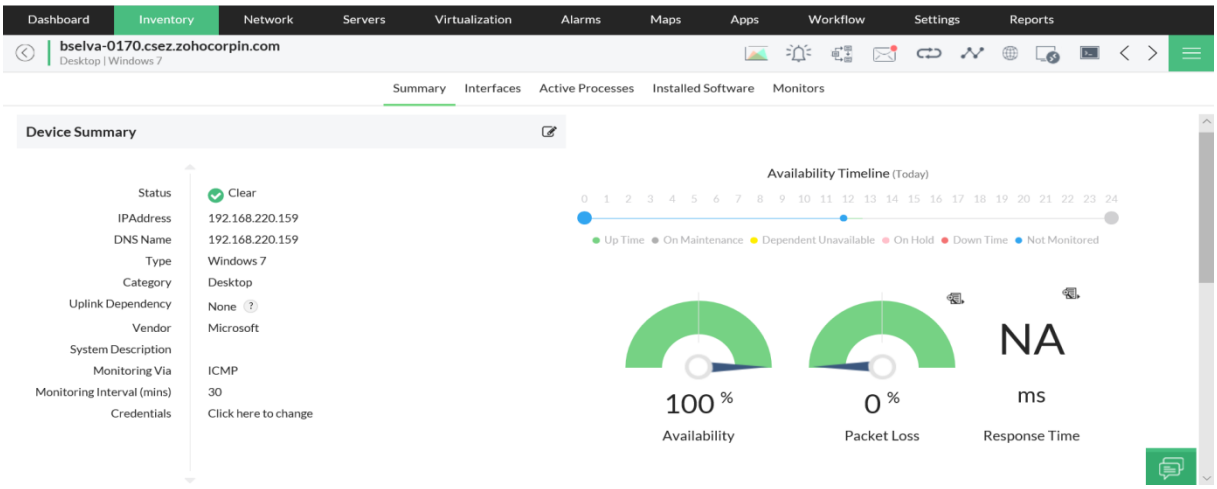


Figure 3.5 : disponibilité des appareils.

3.5.1.2 CPU et mémoire

Une utilisation élevée du processeur ou de la mémoire sur un serveur physique, une machine virtuelle ou un périphérique réseau peut considérablement affecter les performances des périphériques pour affecter l'utilisateur final. Ce logiciel vous permet de surveiller les périphériques à l'aide de l'API native SNMP, WMI, Telnet, SSH et VMware. Avec cela vous pouvez détecter et résoudre les goulots d'étranglement du processeur et du serveur avant qu'ils n'affectent l'utilisateur final. Vous pouvez également surveiller les mesures importantes du processeur telles que l'utilisation, la vitesse, le temps d'inactivité et le temps du processeur, et définir des seuils d'alarme indépendants pour chaque périphérique surveillé [39].

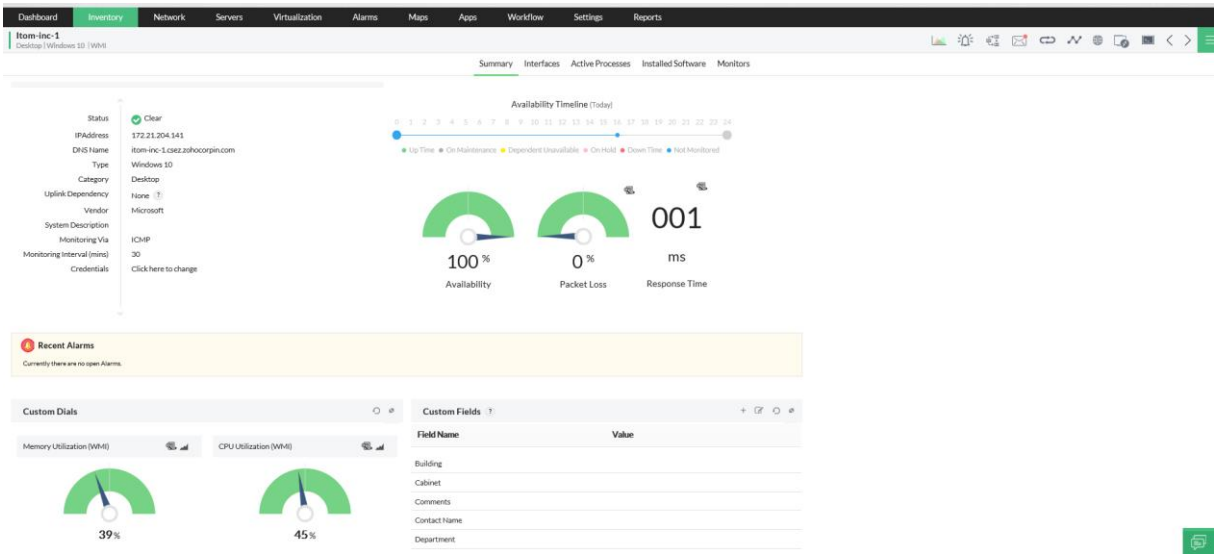


Figure 3.6 : mesures importantes du processeur telles que l'utilisation, la vitesse, le temps d'inactivité et le temps du processeur.

3.5.1.3 Trafic

La lenteur du trafic réseau est une préoccupation pour chaque organisation. Les réseaux peuvent être confrontés à des problèmes liés à la bande passante en raison d'une application, d'un système ou d'un WLAN spécifiques. Les outils de surveillance des performances du réseau vous permettent d'identifier les porcs de bande passante afin que vous puissiez optimiser votre trafic réseau avant qu'il n'affecte votre réseau. Prenez en charge la surveillance des performances du réseau en analysant les performances de la bande passante de votre réseau et les modèles de trafic avec le protocole de gestion de réseau simple de ce logiciel, qui vous permet de surveiller le trafic des appareils. Vous pouvez afficher le trafic d'interface, filtrer le trafic par intervalle de temps et afficher la dernière valeur de trafic interrogée [39].

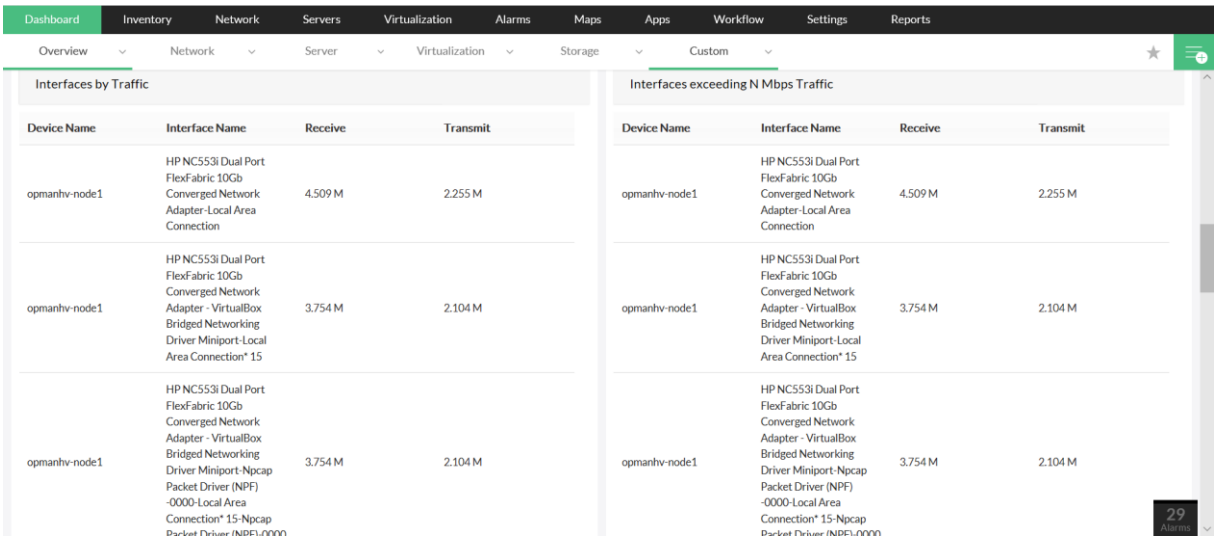


Figure 3.7: les interfaces des trafics.

3.5.1.4 Erreurs et rejets

Tous les périphériques réseau rejettent les paquets en fonction de leur mémoire, ce qui peut affecter les performances. Ces problèmes sont courants avec les routeurs et les commutateurs. Étant donné que les rejets augmentent la latence des applications, des rejets excessifs peuvent indiquer qu'il y a un problème avec le commutateur ou le périphérique interagissant avec le commutateur. L'allocation insuffisante de la bande passante est également une préoccupation pour les pertes de paquets. Les erreurs de réseau sont diverses ; ils peuvent être causés par un pr5oblème DNS, un délai d'expiration TCP ou un manque de réponse du serveur. Un commutateur ou un routeur peut mal interpréter un paquet en raison d'une incompatibilité de protocole lors de la mise à jour des configurations de périphérique. OpManager vous aide à surveiller et à réduire la perte de paquets due aux erreurs et aux rejets [39].

3.5.1.5 Performances WAN

La surveillance des liaisons WAN pour la disponibilité et la fiabilité est essentielle, car les organisations nécessitent une disponibilité continue, des temps de réponse rapides et des erreurs de transmission minimales, ce qui rend la surveillance des liaisons WAN pour la disponibilité et la fiabilité est essentielle. La plupart des organisations utilisent des liaisons WAN pour interconnecter des réseaux locaux (LAN) à partir de différents emplacements à travers le monde. Op Manager, peut aider à surveiller vos connexions WAN, vérifier la latence WAN et identifier le trafic réseau sur votre réseau WAN. Cela vous aide à allouer les ressources en conséquence pour hiérarchiser le trafic et réagir de manière proactive à tout problème affectant votre réseau WAN. Op Manager s'appuie principalement sur IP-SLA de Cisco pour surveiller le WAN, tandis que le moniteur de temps de trajet aller-retour WAN d'Op Manager fournit des détails sur la latence de la liaison WAN, l'utilisation de la bande passante, le temps de trajet aller-retour [39]**.**

3.5.2 Surveillance du matériel

Lorsque vous traitez avec d'énormes réseaux qui exécutent des applications critiques pour l'entreprise et permettent des opérations globales sur une base régulière, il est crucial que les blocs de construction fondamentaux de ces environnements de réseau soient protégés. La surveillance du matériel garantit une disponibilité continue, maintien des performances de pointe et minimise les risques commerciaux [40]**.**

3.5.3 Défis de la surveillance du matériel

Lorsqu'il s'agit d'identifier et de mettre en œuvre un moniteur matériel approprié pour maintenir la santé du matériel critique, les entreprises sont confrontées à de nombreux défis [40]**:**

- Environnements réseau multifournisseurs.
- Ressources matérielles distribuées.
- Surveillance proactive du matériel.
- Implémentation et configuration.
- Prise en charge des mises à niveau matérielles.

3.5.3.1 Environnements réseau multifournisseurs

Le défi le plus courant est la multitude de fournisseurs sur le marché. Dans un tel environnement réseau multifournisseur, vous devez surveiller une variété de matériel de différents fabricants d'équipement d'origine (OEM) afin de garantir de bonnes performances dans vos périphériques réseau. Sans le bon logiciel de surveillance matérielle, cela peut être difficile. En termes simples, vous devez vous assurer que le moniteur matériel que vous envisagez d'utiliser prend en charge les périphériques de votre réseau [40].

3.5.3.2 Ressources matérielles distribuées

Un autre défi majeur est la nature distribuée de votre environnement réseau. Par exemple, vous pouvez avoir des centres de données qui nécessitent une surveillance matérielle à travers le monde, toutefois votre moniteur matériel prend uniquement en charge la surveillance de votre matériel local. Il s'agit d'un piège qui peut être évité avec une prise de conscience appropriée, qui est pour permettre d'assurer les performances durables de votre réseau [40].

3.5.3.3 Surveillance proactive du matériel

La recherche suggère que plus de 50% des temps d'arrêt du réseau sont causés par des pannes matérielles. C'est un nombre énorme, d'autant plus que les catastrophes naturelles ne représentent qu'environ 6% des pannes imprévues. Cela souligne l'importance d'une surveillance proactive du matériel de votre réseau [40].

3.5.3.4 Implémentation et configuration

Dans un environnement composé de nombreux périphériques réseau différents, l'identification, l'ajout et la configuration manuelle des types de périphériques prennent du temps lors de la configuration d'une solution de surveillance matérielle. Une alternative intelligente consiste à déployer un moniteur matériel qui fournit une fonctionnalité de découverte et de configuration automatique prête à l'emploi. Cela vous aidera à obtenir un environnement réseau surveillé de manière saine [40].

3.5.3.5 Prise en charge des mises à niveau matérielles

Il est important de permettre à votre réseau de s'adapter et d'utiliser des ressources informatiques avancées qui seront développées dans un avenir proche. Pour ce faire, le logiciel de surveillance doit prendre en charge les nouveaux fournisseurs de matériel ou les appareils mis à niveau, De cette façon, vous ne limitez pas la portée du développement de votre infrastructure réseau [40].

3.5.4 Surveillance matérielle en temps réel

Obtenez des informations en temps réel sur l'état du matériel surveillé comme les serveurs , les routeurs , les commutateurs , les pare - feu , les machines virtuelles et les périphériques de stockage . Ces informations sont présentées sous forme de tableaux et de graphiques [40].

1. Température.
2. Vitesse du ventilateur.
3. Source de courant.
4. Vitesse d'horloge du processeur.
5. Batterie.
6. Tableau de disque.

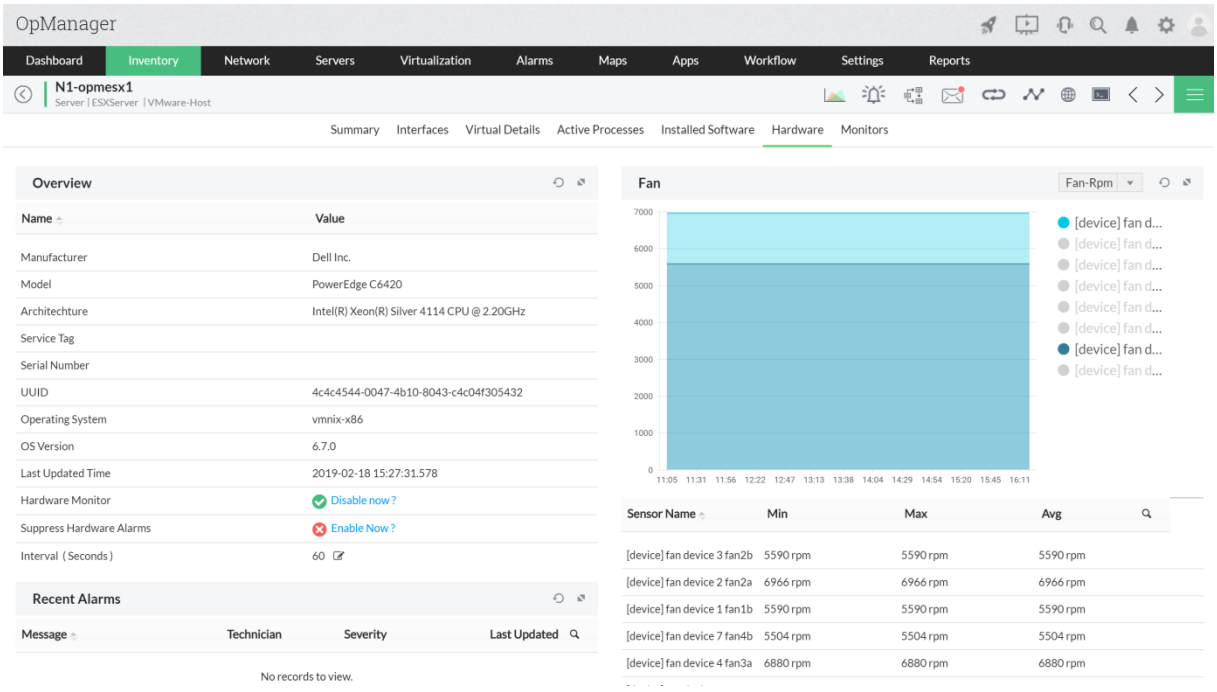


Figure 3.8 : Tableau d'bord de la présentation de la surveillance matérielle.

3.5.4.1 Température

Surveillez la température des composants critiques pour garantir des performances optimales et une longue durée de vie de votre matériel réseau [40].

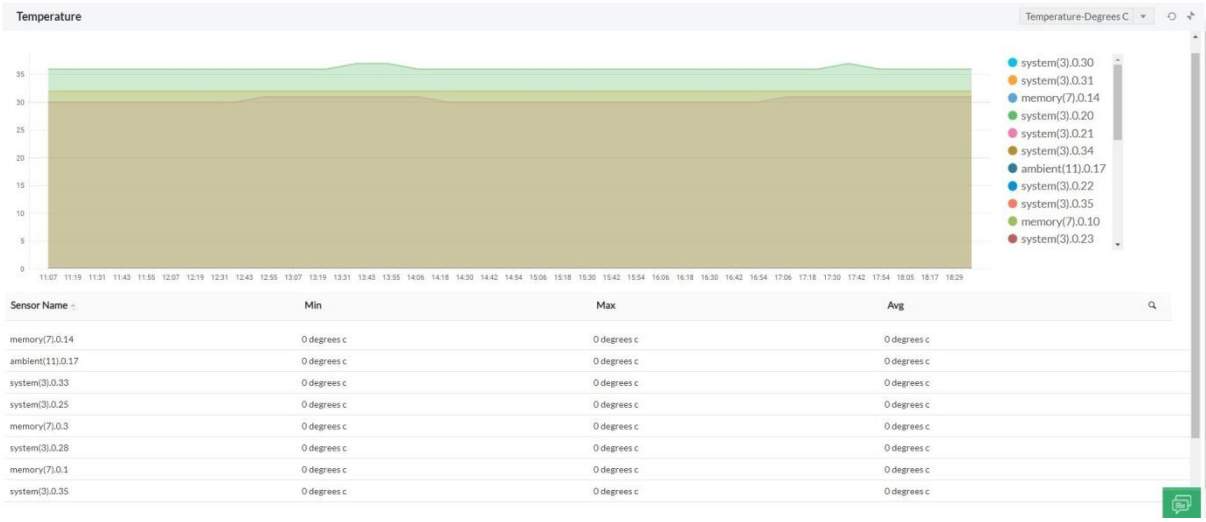


Figure 3.9 : moniteur de température matérielle.

3.5.4.2 Vitesse du ventilateur

Assurez-vous que vos racks, châssis, routeurs et autres composants critiques sont bien ventilés avec une bonne répartition du flux d'air [40].

Figure 3.10 : surveillance de la vitesse du ventilateur matériel.

3.5.4.3 Alimentation

Surveillez la tension et le courant fournis aux divers composants matériels et aux redondances des blocs d'alimentation pour éviter les pannes ou les court-circuit de l'appareil [40].

Figure 3.11 : surveillance de l'alimentation électrique du matériel.

3.5.4.4 Vitesse d'horloge du processeur

Surveillez la vitesse à laquelle votre processeur termine son cycle de traitement pour garantir une utilisation maximale des ressources disponibles [40].

Figure 3.12: surveillance du matériel du processeur.

3.5.4.5 Batterie

Surveillez les batteries de vos serveurs pour éviter la perte de données de cache, les BSOD et les arrêts anormaux [40].

3.5.4.6 Disque Array

Surveillez l'état de plusieurs disques durs pour éviter tout problème de stockage ou de transfert de données [40].

3.6 Surveillance de routeur

Les liaisons WAN et les routeurs qui les desservent sont généralement la partie la plus chère du réseau, et la gestion de l'allocation de bande passante peut être complexe. Un sous-abonnement à la bande passante peut signifier que l'entreprise paie plus de bande passante que nécessaire et un sous-abonnement peut entrainer une congestion et des performances

réseau inacceptables. La surveillance WAN et la surveillance des routeurs deviennent donc très importantes non seulement pour la productivité au jour le jour, mais aussi pour les résultats d'une entreprise. Les gestionnaires de réseau devront optimiser la qualité de service en équilibrant le débit, le débit d'information engagé (CIR) et le taux de rafale avec l'encombrement, le temps de réponse et les rejets. Certains des défis de la surveillance WAN incluent l'optimisation des allocations de bande passante, la garantie d'une haute disponibilité du réseau, la résolution rapide des problèmes WAN, la planification de la capacité pour les besoins futurs [41]**.**

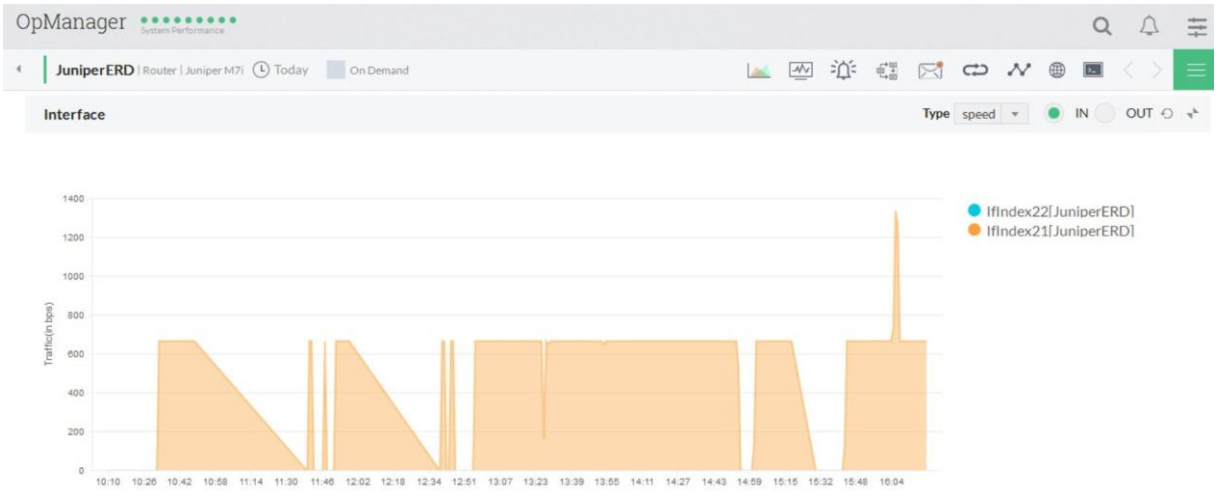


Figure 3.13: Surveillance et gestion des Routeurs.

3.7 Mesurer la bande passante et le trafic pour optimiser l'allocation de bande passante

Op Manager surveille la bande passante, l'utilisation, les erreurs, les rejets de vos liaisons WAN et vous aide ainsi à vérifier les accords de niveau de service (SLA) avec vos fournisseurs d'accès Internet (FAI). En présentant des informations précises sur le trafic et l'utilisation de chaque lien de votre réseau étendu, vous pouvez identifier les liens très utilisés et sous-utilisés vous permettant d'optimiser l'allocation de bande passante entre les liens [42].

3.8 Surveillance proactive des liaisons WAN et garantie d'une haute disponibilité du réseau

En surveillant de manière proactive la latence des liens et les erreurs de liens et en leur affectant des alertes de seuil, Op Manager vous alerte chaque fois qu'un lien tombe en panne. Les alertes peuvent être envoyées sous forme d'e-mails ou de messages texte contenant des détails sur les seuils franchis et des détails de lien pertinents, ce logiciel vous

fournit également un rapport de disponibilité détaillé de toutes vos interfaces. Vous pouvez utiliser ces rapports pour vérifier si vos SLA sont respectés [42].

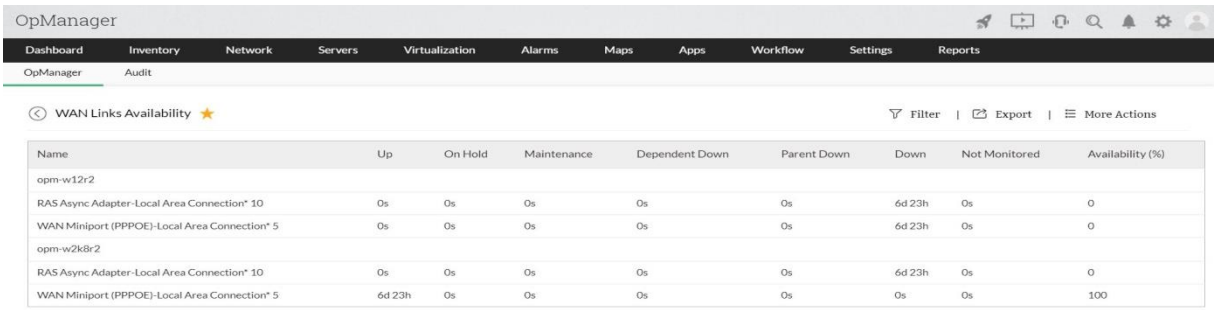


Figure 3.14: surveillance de la liaison WAN avec Op Manager.

3.9 Visualisez LES liens WAN et résolution rapide leur problème

Op Manager, vous aide à créer des vues d'entreprise (cartes) pour visualiser graphiquement l'ensemble de votre WAN. Vous bénéficiez désormais d'une visibilité complète sur vos liaisons WAN et suivez les pannes jusqu'au niveau du saut. Hormis votre infrastructure, les performances WAN dépendent beaucoup des FAI auxquels vous êtes abonné pour le service WAN, il fournit des informations sur les performances de votre liaison WAN en affichant le nombre de latences au niveau du saut à partir duquel vous pouvez identifier si le problème réside dans votre infrastructure ou chez les FAI [42].

3.10 Identifier les tendances actuelles du trafic, minimiser les couts récurrents actuels et planifier la capacité pour l'avenir

Le choix de ce logiciel est qu'il aide les gestionnaires de réseau à économiser sur les couts récurrents mensuels en identifiant les liens sous-utilisés. Armés d'histoires historiques des tendances du trafic et de rapports d'utilisation des liens, les gestionnaires de réseau peuvent également planifier une capacité supplémentaire bien à l'avance [43].

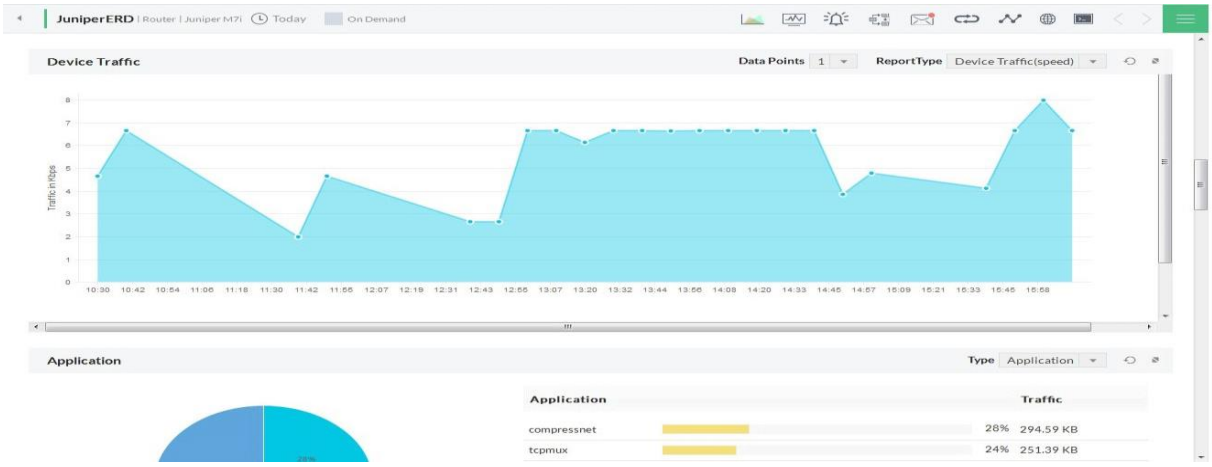


Figure 3.15: Rapports de trafic du Routeur avec OpManager.

3.11 Fonctionnalités de surveillance du commutateur Op Manager

Surveillance de la disponibilité des commutateurs et des ports de commutation, ce logiciel aide à créer des vues d'entreprise (cartes) pour visualiser graphiquement l'ensemble de votre réseau local et envoyer automatiquement des alertes lorsqu'un lien tombe en panne [43].

La fonctionnalité de génération de rapports d'Op Manager vous fournit également un rapport de disponibilité détaillé de vos commutateurs et ports de commutateur

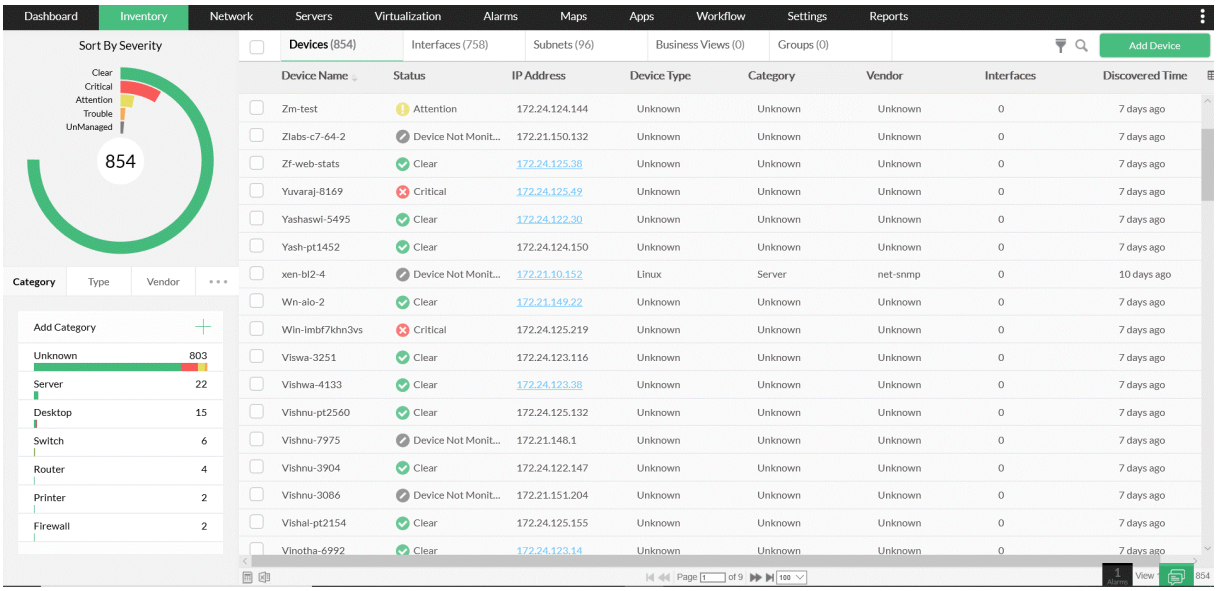


Figure 3.16 : surveillance des commutateurs.

3.11.1 Surveillance du trafic par port

Surveiller et à dépanner les ports de commutation pour le trafic, l'utilisation, les erreurs et la vérification de l'accord de niveau de service (SLA). En présentant des informations précises sur le trafic et l'utilisation des ports, Op Manage aide à identifier les meilleurs interlocuteurs sur le LAN [43] :

- Surveillez l'utilisation du port et le trafic avec des alertes de seuil.
- Détectez les orages de diffusion potentiels et prévenez-les de manière proactive.
- Identifiez les ports très utilisés et sous-utilisés.
- Soyez alerté lorsqu'un port commence à rejeter les paquets

3.11.2 Switch Monitoring Tools

Des outils de surveillance des commutateurs en temps réel tels que Switch Port Mapper et STP Tools sont fournis avec Op Manager [43].

3.11.3 Mappeur de ports de commutateur

Le Switch Port Mapper est un utilitaire utile intégré à Op Manager. Il aide à trouver rapidement la liste des périphériques connectés aux ports du commutateur [43].

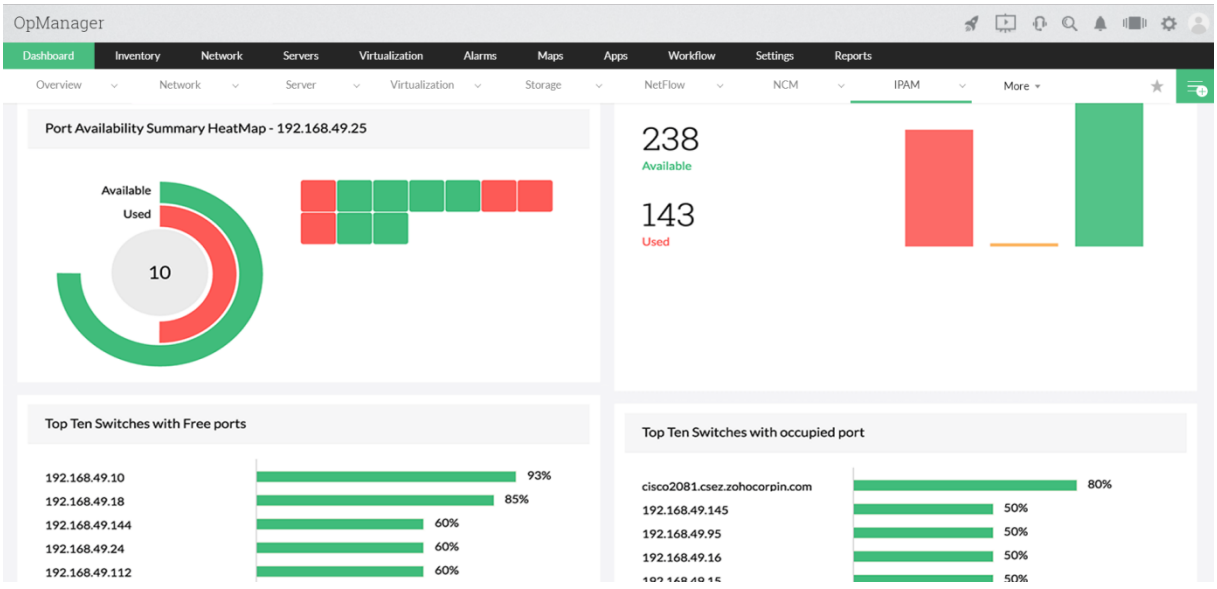


Figure 3.17 : Surveillance des commutateurs outils.

3.11.4 Outil STP

Les détails du protocole Spanning Tree pour chaque port peuvent être affichés à l'aide de l'outil STP. Cela donne des informations précieuses sur l'état de l'arbre couvrant de chaque port, tels que les ports qui bloquent et les ports qui transfèrent [43].

3.12 Moniteur de serveur

La surveillance du serveur est le processus de surveillance des ressources système d'un serveur comme l'utilisation du processeur, la consommation de mémoire, les E / S, le réseau, l'utilisation du disque, le processus, etc. La surveillance du serveur aide à la planification de la capacité en comprenant l'utilisation des ressources système du serveur. Ce logiciel de surveillance de serveur aide à automatiser le processus de surveillance de serveur. La surveillance des performances du serveur permet également d'identifier d'autres problèmes liés aux performances tels que l'utilisation des ressources, les temps d'arrêt des applications et les temps de réponse [43].

Pourquoi est-il important de surveiller les performances du serveur [43]?

- Pour surveiller la disponibilité du serveur et la perte de données.
- Pour surveiller la réactivité du serveur.
- Pour connaitre la capacité du serveur, la charge utilisateur et la vitesse du serveur.
- Pour détecter et prévenir tout problème susceptible d'affecter le serveur de manière proactive.

3.12.1 Analyseur de performances du serveur dans Op Manager

Op Manager fournit une assistance multifournisseur pour surveiller en continu les serveurs et les applications critiques ainsi que leurs services et processus. Il surveille périodiquement les serveurs via les protocoles SNMP et WMI pour s'assurer qu'ils fonctionnent et fonctionnent à leur niveau de performance optimal, 24h / 24 et 7j / 7. Il stocke toutes les données pour le suivi historique des performances et le dépannage, éliminant ainsi le besoin de plusieurs outils de surveillance de serveur et Obtenez des informations détaillées en temps réel et surveillez efficacement les performances du serveur [43] :

- Surveillance des performances du serveur en temps réel.

- Surveillance de la disponibilité et de l'intégrité du serveur.
- Surveillance proactive du serveur avec des seuils à plusieurs niveaux.
- Surveiller les performances des applications.
- Surveillez les performances des serveurs VMware ESX et du SE invité.
- Surveiller les performances du serveur Exchange.
- Suivi des services.
- Surveillance des services Windows.
- Surveillance des processus serveur.
- Surveillance du journal des évènements Windows.
- Surveillance des URL et des sites Web.

3.12.1.1 Surveillance des performances du serveur en temps réel

Op Manager fournit une vue graphique de ces mesures pour surveiller et mesurer les performances du serveur, en temps réel. Il permet également d'explorer un intervalle de temps particulier pour mieux comprendre le problème et prendre les mesures nécessaires de manière proactive. En utilisant cela, conclure il va résoudre les problèmes avant qu'ils ne causent de graves dommages à votre entreprise [43].

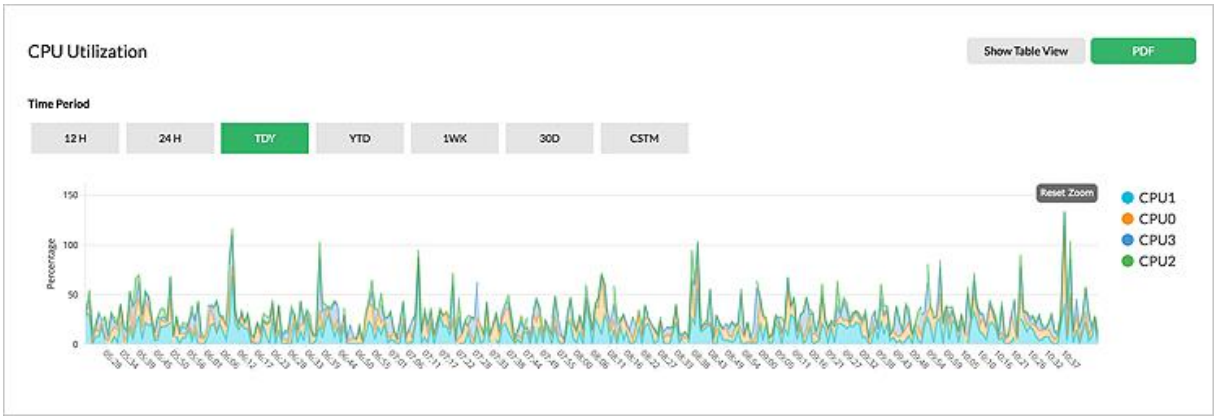


Figure 3.18 : utilisation du processeur.

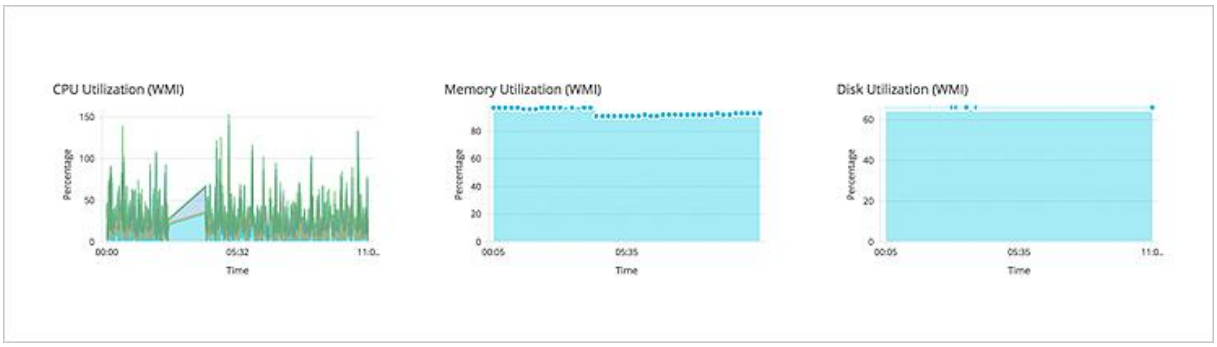


Figure 3.19: utilisation du processeur et la mémoire de WMI.

3.12.1.2 Surveillance de la disponibilité et de l'intégrité du serveur

Op Manager, surveille immédiatement la disponibilité du serveur et plus de 300 mesures de performances via les protocoles SNMP et WMI. Surveille les mesures de performances critiques chaque minute et détecter les problèmes de performances à un stade précoce. Outre les moniteurs par défaut, l'utilisateur peut également créer ses propres moniteurs personnalisés. Toutes les données collectées des mesures de performances du serveur sont stockées dans la base de données pour une analyse détaillée et pour la création de rapports de performances mensuels et annuels [43].

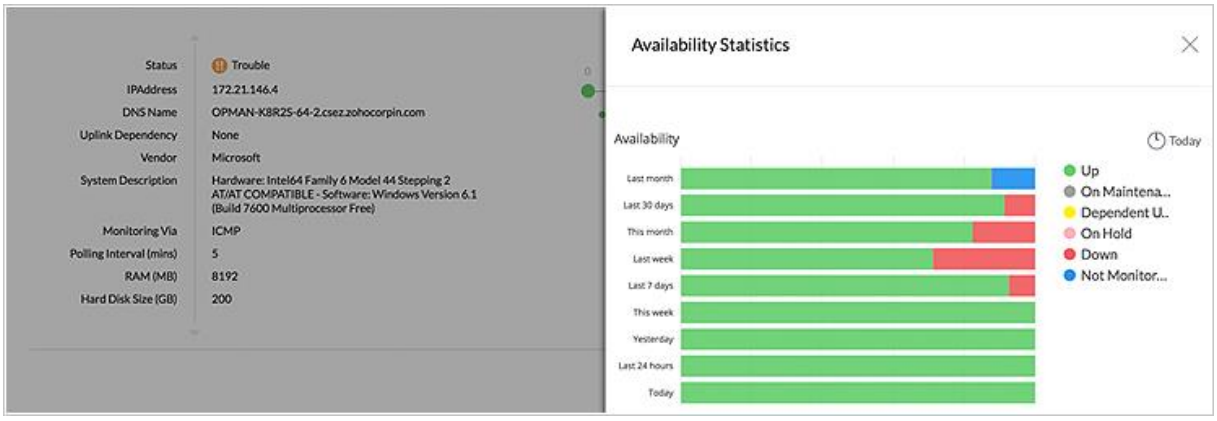


Figure 3.20 : les statistiques de disponibilité.

3.12.1.3 Surveillance proactive du serveur avec des seuils à plusieurs niveaux

En informatique, plus de 50% des problèmes sont signalés par les utilisateurs finaux et ce n'est pas une approche saine. La solution de surveillance du serveur doit identifier tout problème lié aux performances dès les premières étapes et en informer l'équipe informatique. Op Manager, offre une surveillance proactive des serveurs utilisant plusieurs seuils et permet de vérifier les performances à différents niveaux et de les notifier par e-mail et SMS en cas de violation [43].

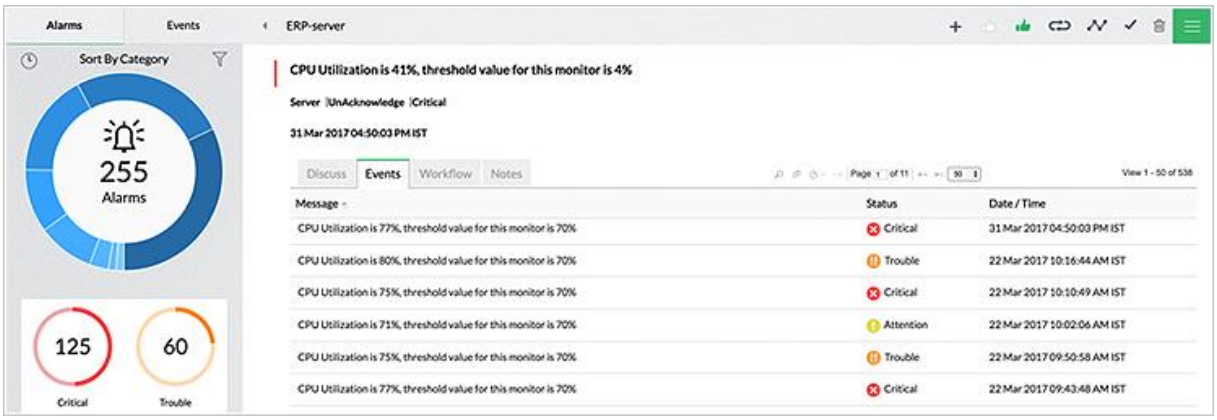


Figure 3.21 : Alarme des évènements.

3.12.1.4 En ce qui concerne les applications critiques pour l'entreprise

Op Manager offre des services de surveillance de serveur avancés et surveille les processus et les services Windows, la plupart de la découverte et de la surveillance étant prêtes à l'emploi. Il peut même détecter les tentatives d'effraction de sécurité sur vos serveurs d'applications (échecs de connexion en raison de mauvais mots de passe, verrouillages de compte, tentatives infructueuses d'accès à des fichiers sécurisés, etc.) [43].

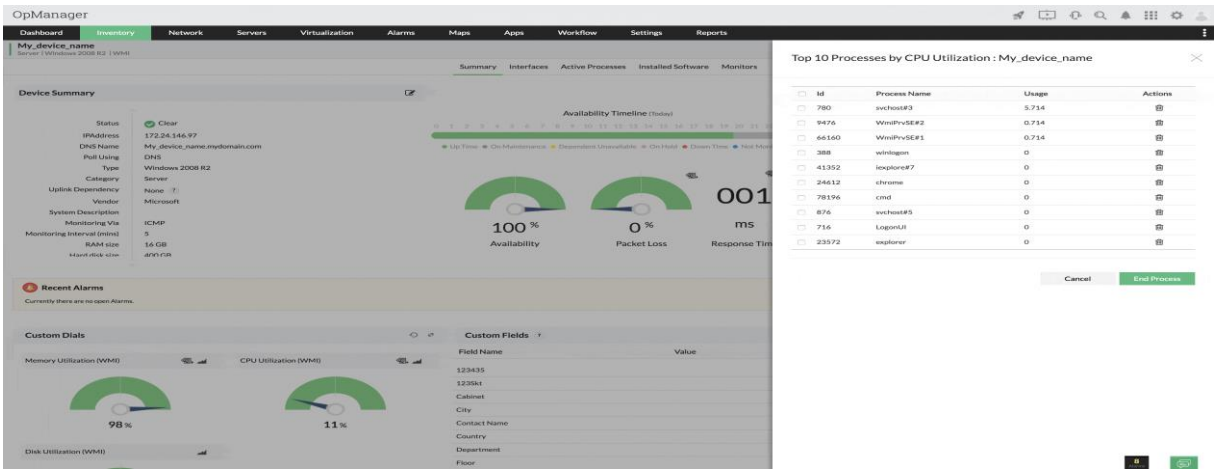


Figure 3.22: Les meilleures utilisations des processeurs.

3.12.1.5 Surveillez les performances des serveurs VMware ESX

Op Manager prend en charge la surveillance des serveurs virtuels. Il fournit un tableau de bord de surveillance exclusif pour chaque serveur ESX, montrant l'utilisation du processeur, de la mémoire et du disque pour chaque instance de machine virtuelle invitée sur le serveur ESX. Op Manager fournit également des options pour démarrer, arrêter et suspendre les instances de VM sur le serveur ESX. Recevez des alertes instantanées sur les machines virtuelles utilisant des ressources excessives et arrêtez même à distance les machines virtuelles avant qu'elles ne causent des problèmes sur le serveur ESX [43].

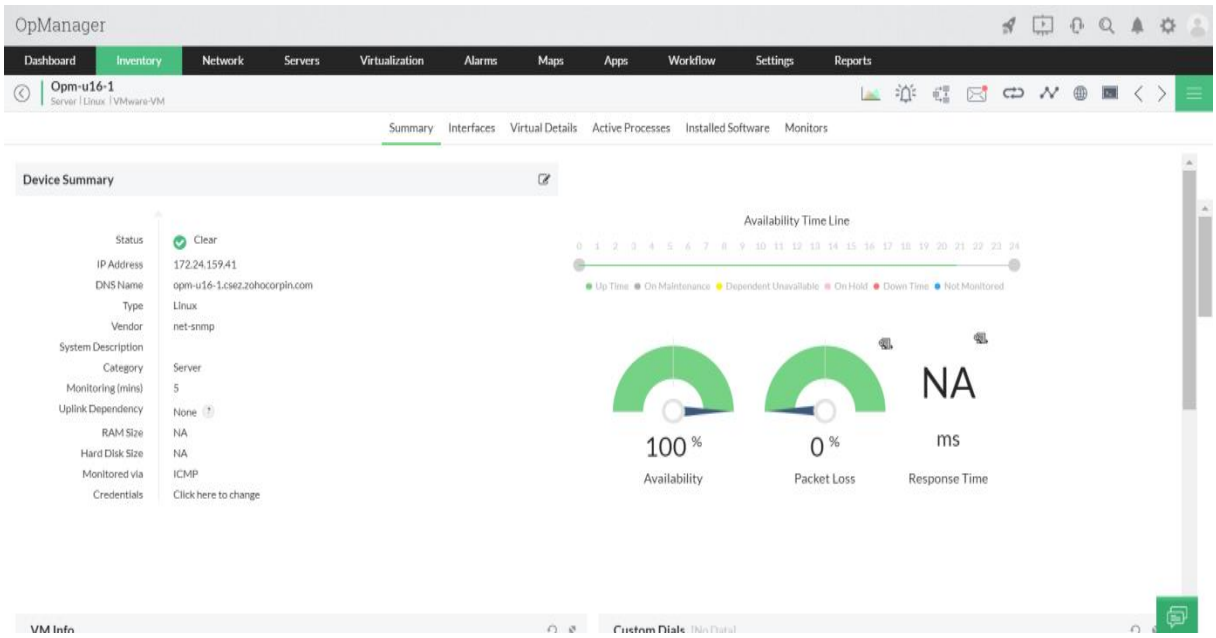


Figure 3.23: les performances des serveurs VMware ESX.

3.12.1.6 Surveiller les performances du serveur Exchange

Op Manager va au-delà des fonctionnalités de surveillance de serveur de base pour inclure la prise en charge de SMTP, POP et IMAP sur vos serveurs Exchange. Il surveille plus de 15 services clés et 50 variables critiques qui incluent la banque publique, la banque privée, la taille de la file d'attente reçue ou envoyée, etc. Tout cela, sur un tableau de bord de surveillance Exchange spécialement conçu qui attribue automatiquement des moniteurs de performances et des seuils préconfigurés selon que les serveurs sont Exchange 2000, 2003 ou 2005. Suivi des services, Au moment de la découverte de l'appareil, Op Manager découvre tous les services en cours d'exécution sur vos serveurs Windows et Linux et leur associe des moniteurs de disponibilité et de temps de réponse. Il prend également en charge l'ajout de moniteurs pour les services personnalisés exécutés sur le port TCP [43].

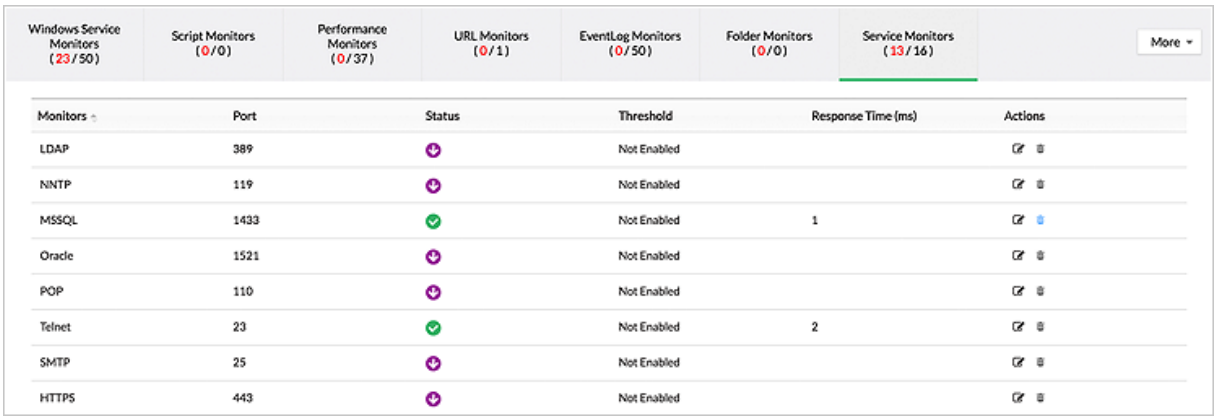


Figure 3.24 : les performances du serveur Exchange.

3.12.1.7 Surveillance des services Windows

Outre la surveillance des services de niveau système tels que HTTP, LDAP, SMTP, etc., Op Manager surveille également les services Windows, par exemple Alerter, FTP, Net Logon, DHCP Server, IAS, Spooler, etc. Une fois qu'un service surveillé a échoué, Op Manager peut être configuré pour redémarrer automatiquement le service Windows ou même le serveur [43].

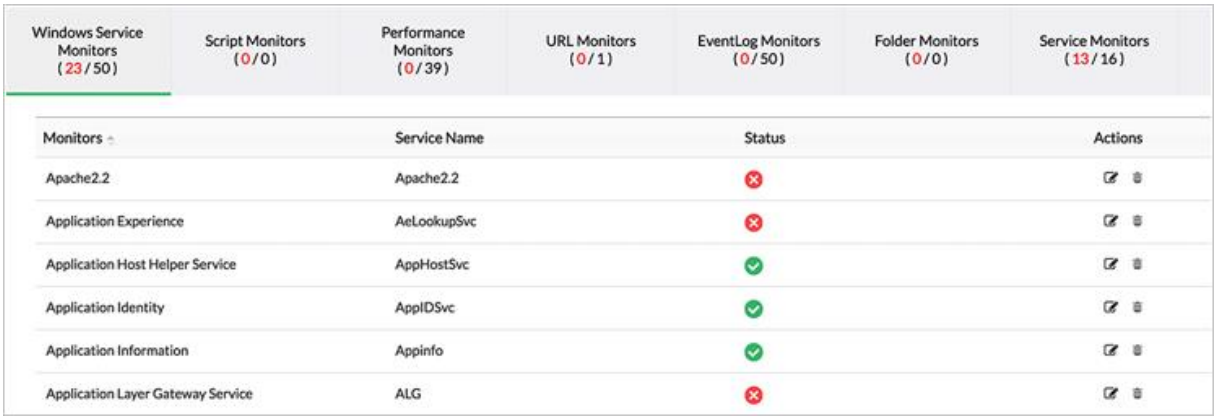


Figure 3.25 : Moniteur des services Windows.

3.12.1.8 Surveillance des processus serveur

Op Manager découvre tous les processus en cours d'exécution sur les serveurs et répertorie les détails tels que l'ID de processus, le nom de processus, le chemin de processus et l'argument de processus. Les « modèles de processus » permettent de découvrir, de gérer et de définir facilement des seuils sur plusieurs serveurs, à partir d'une seule fenêtre. La section Diagnostics des processus à distance fournit une vue rapide des principaux processus par CPU et utilisation de la mémoire. Cela permet de mettre un terme à distance aux processus troublants [43].

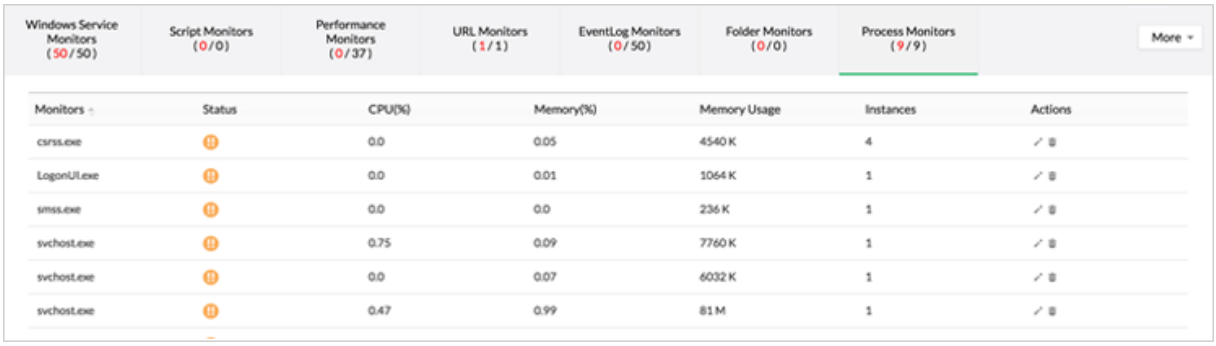


Figure 3.26 : Moniteur de processus serveur.

3.12.1.9 Surveillance du journal des évènements Windows

Op Manager peut aider à détecter les échecs de connexion dus à de mauvais mots de passe, des verrouillages de compte, des tentatives infructueuses d'accès aux fichiers sécurisés, la falsification des journaux de sécurité, etc. en traitant les journaux d'évènements de sécurité Windows. Outre les journaux de sécurité, encore peut également surveiller les journaux d'applications (règles prédéfinies pour les serveurs Exchange, IIS, MS – SQL et ISA), les journaux système et d'autres journaux d'évènements [43].

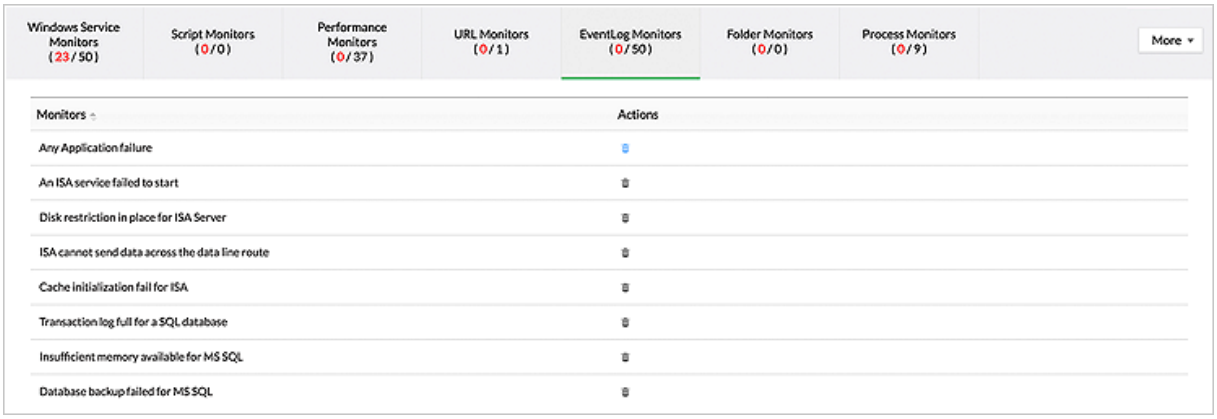


Figure 3.27: journal des évènements.

3.12.1.10 Surveillance des URL et des sites Web

S'appuyer simplement sur les vérifications de disponibilité et de temps de réponse (port TCP) ne vous aidera pas à savoir si votre site Web a été compromis. Op Manager permet de surveiller une URL et de rechercher un texte spécifique sur la page. Lorsque le texte est manquant, L'utilisateur sois immédiatement alerté et apprend en temps réel que le site Web a été compromis. La surveillance de site Web d'Op Manager prend en charge les sites HTTP⁄ HTTP et les sites authentifiés NTLM [43].

Figure 3.28 : moniteur des URL et des sites Web.

3.12.1.11 Surveillance de serveur à distance

Op Manager, le logiciel de surveillance de serveur en temps réel prend également en charge la surveillance de serveur à distance qui aide à surveiller les serveurs sur plusieurs emplacements. Également surveiller et tuer à distance les processus qui affectent les performances du serveur. La surveillance des serveurs à distance peut aider à résoudre les problèmes de performances et à effectuer des actions de dépannage du serveur comme le redémarrage ou le redémarrage d'un serveur n'importe où dans le monde [43].

3.13 Surveillance des pannes réseau

3.13.1Savoir "Quel est le problème ?" avant d'envoyer vos techniciens

La gestion des pannes réseau est un gros défi lorsque vous avez une petite équipe. La tâche devient plus compliquée si vous devez gérer un site distant et envoyer un technicien sur le site uniquement pour découvrir que le problème est quelque chose que vous auriez pu résoudre à distance ou vous pourriez constater que vous n'avez pas le bon équipement et que vous n'avez pas pour revenir en arrière et l'obtenir qui nuit à votre temps de restauration de service.

Dans la plupart des cas, le temps nécessaire pour identifier la cause première d'un problème est en réalité plus long que le temps nécessaire pour le résoudre [43].

3.13.2 Surveillance des pannes avec Op Manager

Op Manager simplifie le processus de gestion de l'alerte réseau en mettant en œuvre des capacités avancées de surveillance des alertes. Le fait d'avoir un outil proactif de surveillance des pannes de réseau comme Op Manage raide à identifier rapidement la cause première du problème et à le résoudre avant que les utilisateurs finaux ne le remarquent [43].

3.13.3 Prise en charge des interruptions SNMP

De nos jours, la plupart des périphériques réseau sont capables d'envoyer des interruptions SNMP en cas de panne. Un bon système de surveillance des pannes de réseau doit être capable de prendre en charge les interruptions SNMP et de fournir des informations significatives aux opérateurs. Op Manager fait exactement cela en fournissant une prise en charge des pièges SNMP de base prêts à l'emploi. Les opérateurs peuvent également ajouter la prise en charge des interruptions à partir de n'importe quelle MIB SNMP personnalisée. Op Manager peut extraire des informations utiles envoyées avec des interruptions SNMP sous forme de liaisons variables (varbinds SNMP) [43].

3.13.4 Outils de dépannage réseau

3.13.4.1 L'état actuel des réseaux dans les entreprises modernes

Au cours des dernières années, de nombreuses entreprises ont surfé sur une méga vague d'expansion technologique rapide avec des réseaux avancés servant de dorsales pour fournir des services essentiels aux utilisateurs finaux du monde entier.

Le développement des petites et moyennes entreprises vers les grandes entreprises, la demande croissante et l'augmentation de la taille du marché font que les infrastructures de réseau s'adaptent et évoluent sans cesse. Au cours de ce processus, les entreprises embauchent plus d'employés, ouvrent des succursales, se développent sur les marchés mondiaux et centralisent la gestion du réseau dans un Network Operations Center (NOC) [43].

3.13.4.2 Le rôle du dépannage réseau dans l'évolution de l'infrastructure réseau de l'entreprise

Cette croissance peut entrainer des problèmes de réseau sur les composants existants en raison de lourdes charges de travail et d'une mauvaise adaptation des nouvelles technologies. Il peut s'agir d'un câble défectueux ou endommagé, d'un problème de routage dû à une mauvaise configuration, une liaison sur utilisée, une mauvaise configuration des adresses IP ou des masques de sous-réseau, etc. perte de revenus, de clients, de données et d'opportunités commerciales, tout en entrainant des couts énormes pour l'extension du réseau.

Cela souligne la nécessité d'un puissant outil de gestion, de diagnostic et de dépannage du réseau pour identifier et prévenir les perturbations du réseau et respecter les accords de niveau de service (SLA) [43].

La nécessité d'outils de dépannage réseau robustes et complets**.**

3.13.4.3 Les outils de dépannage réseau

Le dépannage des performances du réseau est le processus d'identification d'un problème de réseau, d'établissement et de test d'une théorie de la cause probable, de construction d'un plan d'action et de mise en œuvre d'une résolution fonctionnelle. Ce processus nécessite des outils adaptés qui prennent en charge un administrateur réseau pour résoudre efficacement les problèmes de réseau. Les multiples outils impliqués dans ce processus de correction sont identifiés comme des outils d'analyse et de dépannage du réseau.

En termes simples, les outils de dépannage réseau sont des solutions autonomes ou intégrées qui aident les administrateurs réseau à identifier la cause première d'un problème réseau afin de le résoudre.

Op Manager est un outil de dépannage de gestion de réseau robuste qui vous permet de surveiller vos routeurs, commutateurs, serveurs, machines virtuelles et périphériques de stockage dans une seule console. Il fournit les fonctionnalités de tous ces outils de dépannage réseau de base dans une interface utilisateur (UI) simple qui facilite le dépannage fastidieux

Voici quelques-uns des outils de dépannage réseau disponibles dans Op Manager [43]**:**

- Ping (ICMP / SNMP / Proxy)
- Tracert / Traceroute
- Parcourir
- Bureau à distance
- Terminal

3.13.4.3.1 Outils Ping

L'outil de Ping ICMP est un outil de dépannage réseau de base qui vous permet d'évaluer si un périphérique est accessible sur le réseau. Il signale les erreurs telles que la perte de paquets, le temps d'aller-retour, etc [43].

Les requêtes Ping habituelles sont basées sur le protocole de demande d'écho ICMP. Il existe d'autres variantes de requêtes Ping telles que le Ping SNMP et le Ping proxy.

Ces commandes Ping sont utiles pour diagnostiquer les problèmes IP et les problèmes de connectivité réseau qui pourraient être dus à des interfaces défectueuses, des problèmes LAN,

des ports indisponibles, des problèmes de configuration, etc., et sont principalement utilisés en combinaison avec l'utilitaire de dépannage réseau traceroute [43].

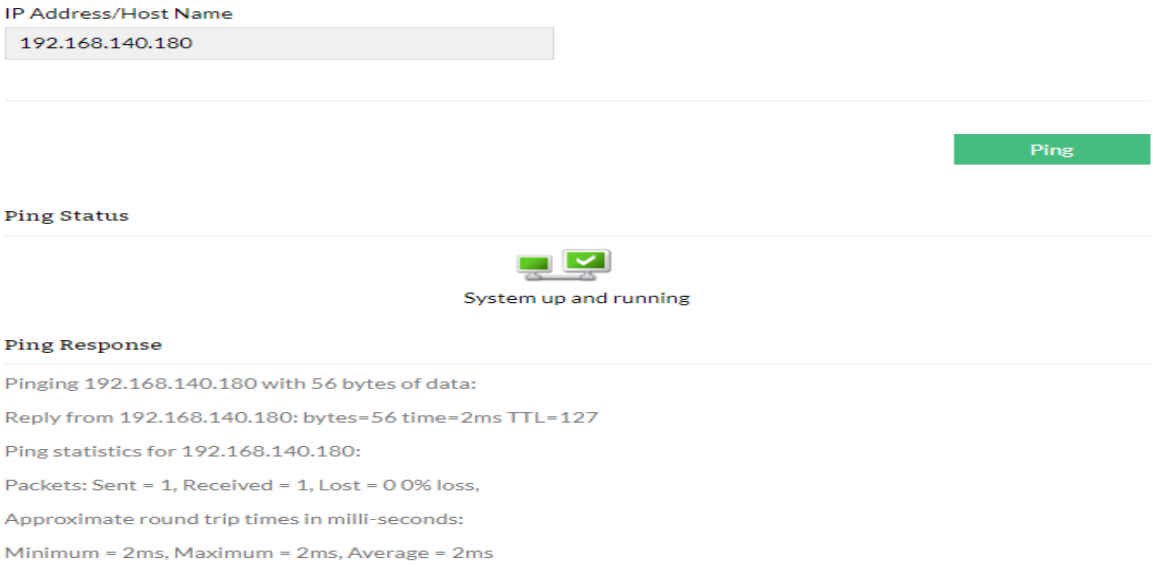


Figure 3.29 : outil Ping de Op Manager.

3.13.4.3.2 Tracert / Trace Route

Tracert (Windows) ou traceroute (Linux) est un outil de diagnostic et de dépannage réseau pour afficher l'itinéraire et mesurer les retards de transit des paquets de données dans un réseau. Il affiche le nombre de sauts entre les périphériques source et de destination en fonction du concept de limite de saut, en modifiant les valeurs de Time To Live (TTL) [43].

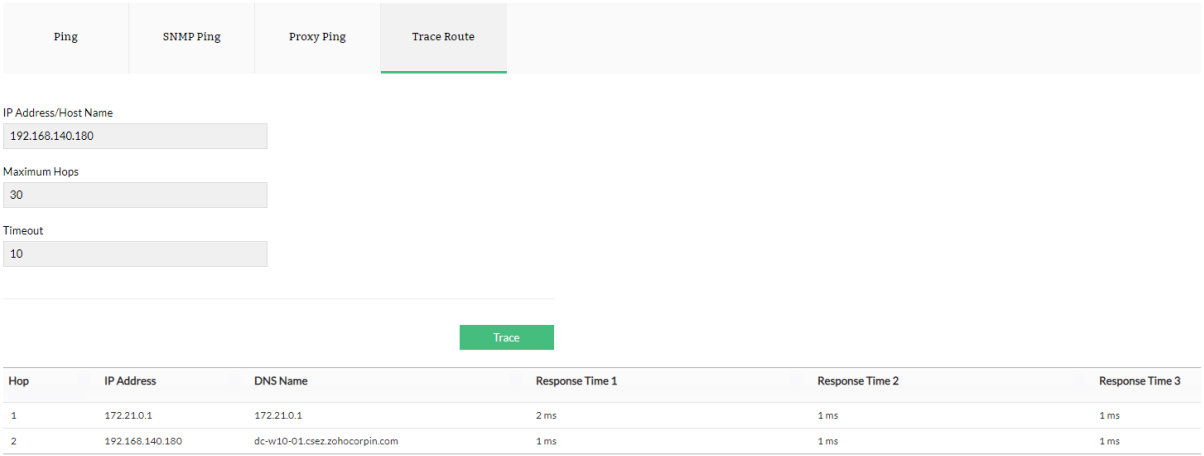


Figure 3.30: outil trace route.

Traceroute est utile pour identifier les retards de réponse (latence élevée), les boucles de routage et les points de défaillance ou de perte de paquets dans un réseau [43].

3.13.4.3.3 Parcourir

Parcourir vous permet de vous connecter à l'interface graphique intégrée de la plupart des périphériques réseau à l'aide d'une demande « http / https ». Cela vous permet d'accéder facilement aux paramètres ou à la configuration de l'appareil pour résoudre facilement les problèmes de réseau [43].

3.13.4.3.4 Bureau à distance

L'utilitaire de bureau à distance permet d'authentifier et d'accéder à l'environnement de bureau de tous les périphériques Windows distants du réseau, à partir de l'interface utilisateur (UI) d'Op Manager. Cela permet un dépannage rapide du réseau comme dans le cas des appareils basés sur Telnet / SSH pour Linux / Unix [43].

3.13.4.3.5 Terminal

Le terminal permet d'établir une connexion sécurisée et cryptée avec le périphérique distant pour exécuter diverses commandes, diagnostiquer et résoudre les problèmes de réseau [43].

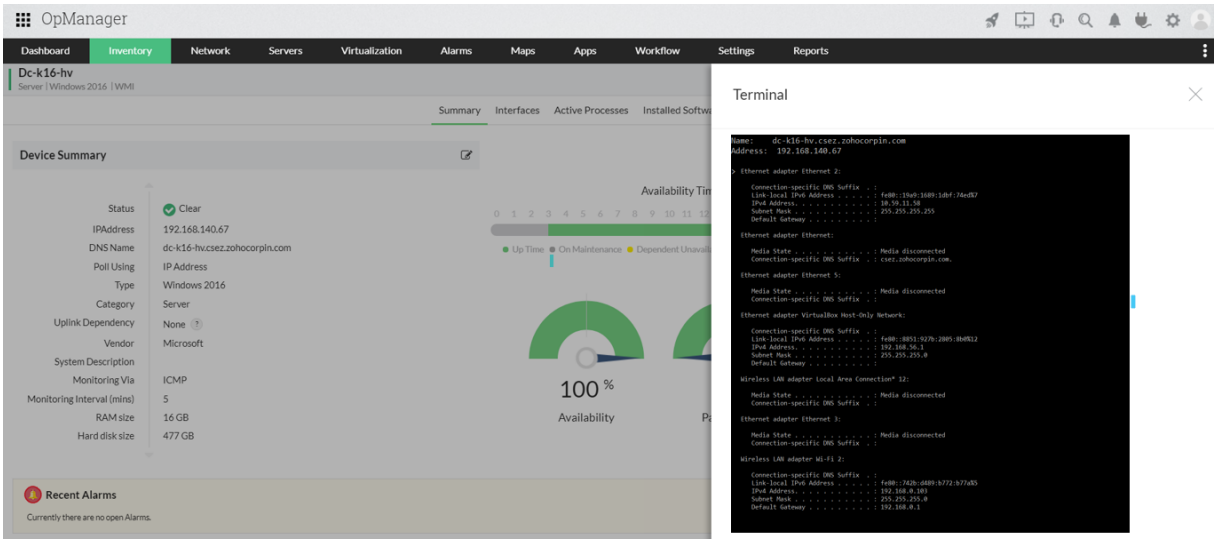


Figure 3.31 : émulateur de Terminal.

Dans le terminal, un administrateur réseau peut exécuter manuellement toutes les commandes prises en charge, largement interprétées comme des outils de dépannage réseau de base, tels que ping, tracert / trace route, ipconfig / ifconfig, netstat, nslookup, pathping / MTR, route, etc., pour analyser et résoudre les problèmes de réseau [43].

3.14 Outil de planification de réseau

Un logiciel de planification de réseau efficace aidera à visualiser l'ensemble de l'infrastructure réseau. L'inventaire de l'appareil sera suivi automatiquement et une carte du réseau en direct affiche également l'emplacement des périphériques réseau dans l'organisation. Eh bien, considérez que vous souhaitez délocaliser votre entreprise ou que vous vous développez à l'échelle mondiale - le processus de conception de votre réseau devient simplifié et est plus viable lorsque vous avez une carte de votre réseau en main. Op Manager est un outil de planification réseau complet de bout en bout qui offre une surveillance avancée de tous vos périphériques réseau, allant des serveurs, routeurs réseau, commutateurs et pare-feu aux serveurs de messagerie, serveurs Web / HTTP, trafic réseau, serveurs DNS, liaisons WAN , périphériques de stockage, bases de données et machines virtuelles (VM). Outre la surveillance et le dépannage du réseau, il vous aide principalement dans la planification du réseau - de la configuration d'un réseau à l'extension de votre réseau et tout au long de la durée de vie de votre réseau [43].

3.14.1 Découverte automatique du réseau

La première étape de la planification de la gestion du réseau consiste à dresser une liste des périphériques du réseau. Le processus simplifié de découverte de réseau d'Op Manager analyse automatiquement le réseau et ses profils de périphériques personnalisés facilitent la découverte d'une large gamme de périphériques réseau tels que des commutateurs, des routeurs et des pare-feu vers des serveurs et des machines virtuelles (VMware, Hyper-V, UCS, Xen) et le stockage périphériques (RAID, TapeLibrary, FC Switches). Aide également obtenir des informations sur les périphériques réseau après la découverte, qui peuvent être générées sous forme de rapport. Pour automatiser la découverte du réseau, également la planifier selon vos besoins et OpManager découvrira automatiquement les nouveaux périphériques de votre réseau [43].

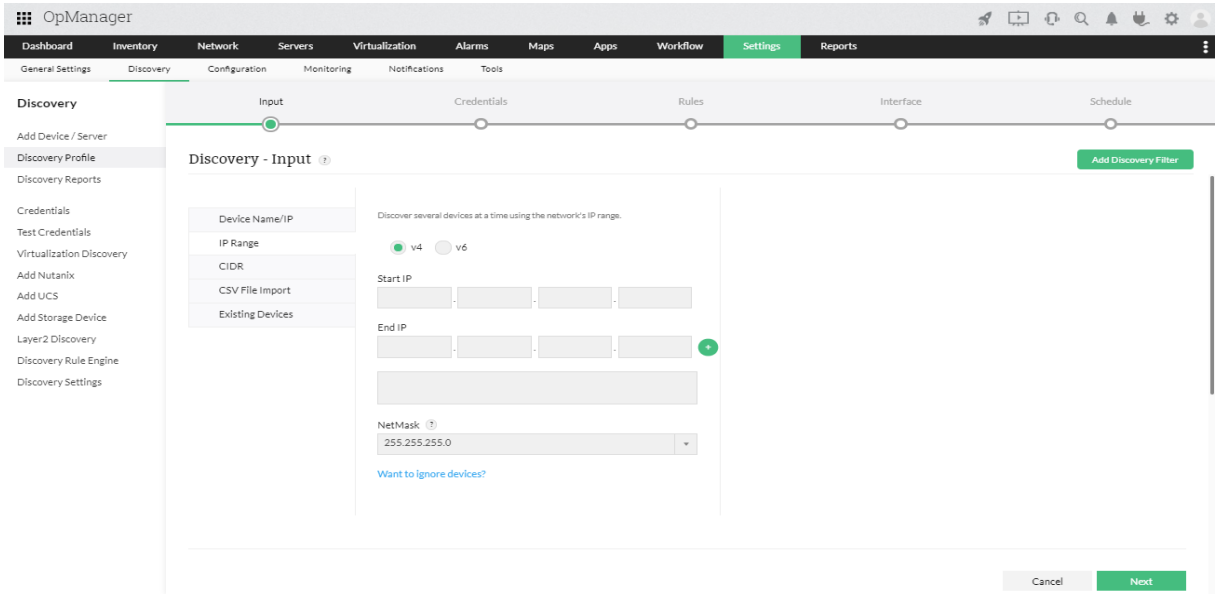


Figure 3.32 : Découvert automatique du réseau.

3.14.2 Regroupement

Un autre élément clé de la planification du réseau consiste à regrouper un ensemble de périphériques. Le regroupement peut être basé sur l'emplacement, le département ou le type d'appareil ou de fournisseur, etc. La fonction de regroupement avancée d'Op Manager permet de trier les appareils ou les interfaces ensemble pour organiser efficacement le réseau. Également configurer des critères spécifiques pour regrouper automatiquement les appareils. Une fois regroupé les périphériques ou les interfaces, Op Manager permet de définir des seuils pour la génération d'alarmes, de générer des rapports pour un groupe particulier et également de pousser les modifications de configuration en masse. Les groupes d'appareils peuvent être efficacement utilisés comme filtre à travers le produit, jouant ainsi un rôle important dans l'organisation de votre réseau pour les âges à venir [43].

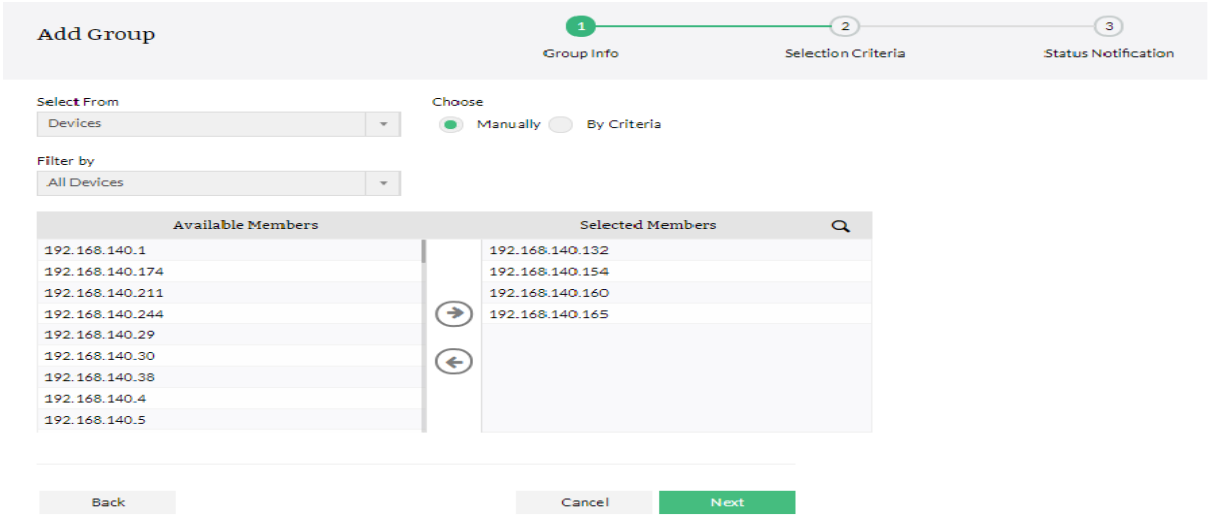


Figure 3.33: Regroupement d'appareils.

3.14.3 Cartes de couche 2

Comprendre la relation entre le parent et les appareils dépendants joue un rôle essentiel dans la planification et la conception du réseau. Un outil de planification de carte réseau efficace vous aidera à générer automatiquement une carte de votre réseau. Op Manager peut générer instantanément une carte de réseau logique ou un diagramme de topologie de réseau une fois le processus de découverte terminé. Cela fournit une visualisation claire des connexions réseau physiques et vous aide également à résoudre les problèmes de réseau en cas de panne d'un appareil. Vous obtenez des icônes codées par couleur en fonction de l'état avec des options pour explorer le spécifique. Avec la fonction de mappage Layer2 d'Op Manager [43].

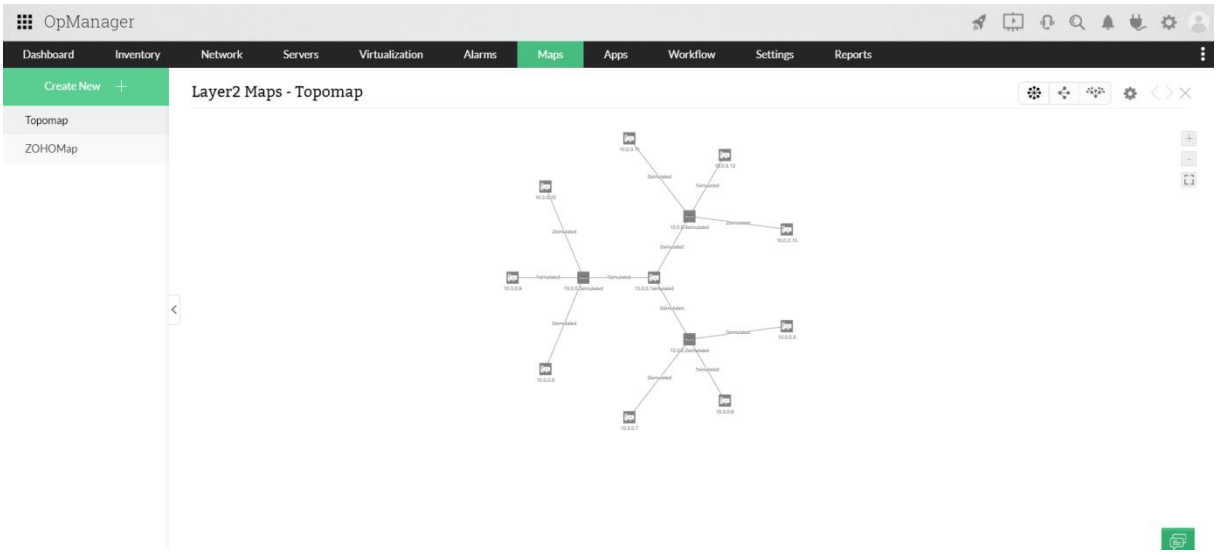


Figure 3.34 : cartes de couche 2.

3.14.4 Vues d'entreprise

Les entreprises étant en constante expansion, il est assez courant que les organisations se développent à l'échelle mondiale. Les vues d'entreprise d'Op Manager fournissent une représentation graphique de votre infrastructure réseau - avec prise en charge des cartes d'arrière-plan personnalisées. Les vues d'entreprise vous permettent de regrouper les appareils en fonction de leur emplacement géographique ou de leurs services professionnels. Un point fort important est que vous pouvez également ajouter des liens entre les appareils et surveiller la connectivité et la charge de trafic. Pour vous donner encore plus de contrôle sur votre réseau, vous pouvez restreindre l'accès des utilisateurs en fonction des

vues d'entreprise, prenant ainsi en charge la planification de la sécurité de votre réseau ainsi que les besoins de planification de la topologie du réseau [43].

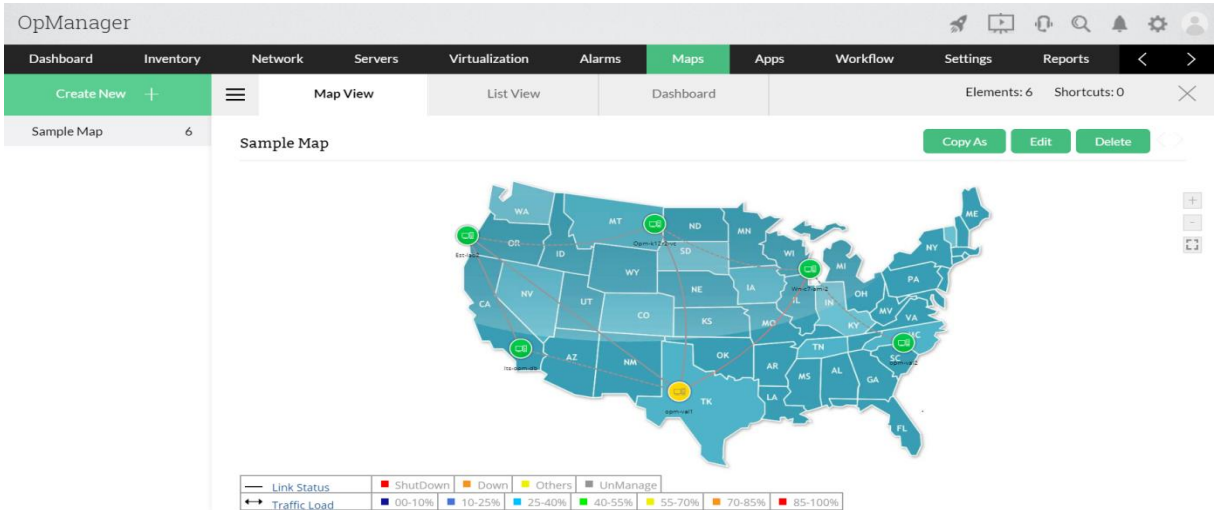


Figure 3.35 : vues d'entreprise.

3.15 Rapports sur les performances du réseau

En tant qu'administrateur réseau, la création et l'archivage de rapports exploitables constituent une tâche critique et parfois non planifiée impliquée dans l'entretien de l'infrastructure informatique. Habituellement, ces rapports sont rapidement établis et rassemblés lorsque la haute direction a besoin d'aide pour prendre des décisions importantes sur les ajouts de capacité / les mises à niveau des appareils / les vérifications SLA. Votre outil de surveillance réseau 24h / 24 et 7j / 7 aurait beaucoup de données capturées s'accumulant sur des giga-octets d'espace disque, mais c'est la capacité de l'outil à fournir des rapports intelligents immédiats qui fait la différence dans le fonctionnement d'une infrastructure informatique bien planifiée et optimisée [43].

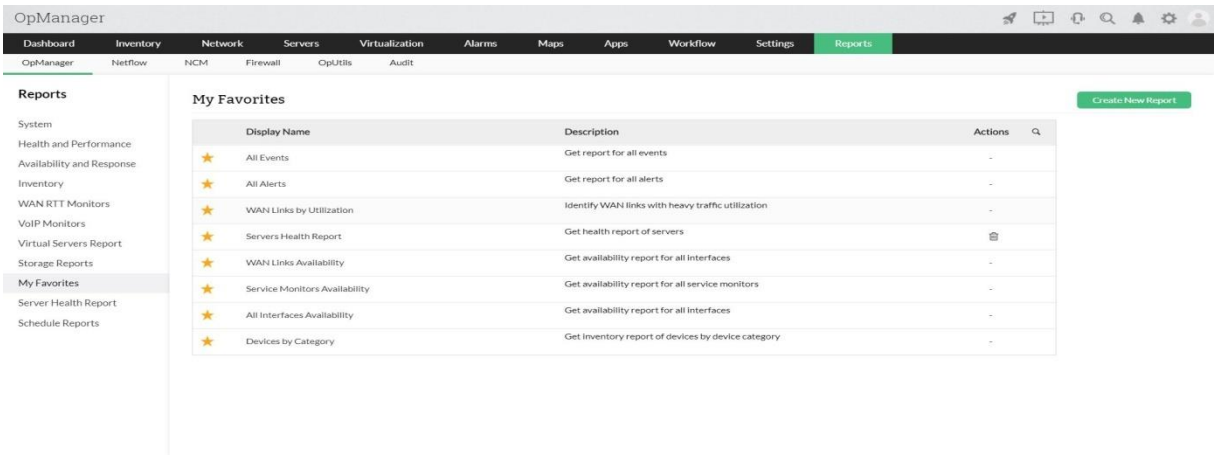


Figure 3.36 : rapport sur les performances du réseau.

Op Manager stocke toutes les informations de santé du réseau et des appareils surveillés dans sa base de données PGSQL intégrée pour une récupération immédiate. La section des rapports propose un certain nombre d'options flexibles qui aident à créer rapidement des rapports personnalisés et exploitables [43].

3.15.1 Plus de 100 rapports prêts à l'emploi

Op Manager fournit une interface simple avec plus de 100 profils de rapports intégrés, tous regroupés et classés intuitivement en tant que rapports de serveurs. Rapports sur les routeurs, rapports sur les commutateurs, rapports sur les services, etc. Chaque rapport peut être exporté et enregistré sous forme de fichier PDF / XLS ainsi qu'imprimé ou envoyé par courrier électronique à des collègues ou des gestionnaires. Diverses options de personnalisation supplémentaire sont fournies pour créer des rapports sur mesure à partir des rapports intégrés, par exemple la sélection de "Top N reports", la modification de la période de rapport, la modification de l'instantané d'entreprise de rapport pour envisager un autre groupe d'appareils pour le profil de rapport sélectionné, etc..

Les profils de rapport incluent [43]**:**

- Rapports d'utilisation sur CPU, mémoire, disque.
- Rapports de trafic d'interface entrants et sortants.
- Rapports d'intégrité de l'appareil qui incluent les tendances sur la disponibilité, le temps de réponse, la perte de paquets, la température, etc.
- Rapports sur les temps de réponse des services.
- Rapports d'inventaire répertoriant les différents appareils, leurs adresses IP, OS, RAM et configurations de disque.

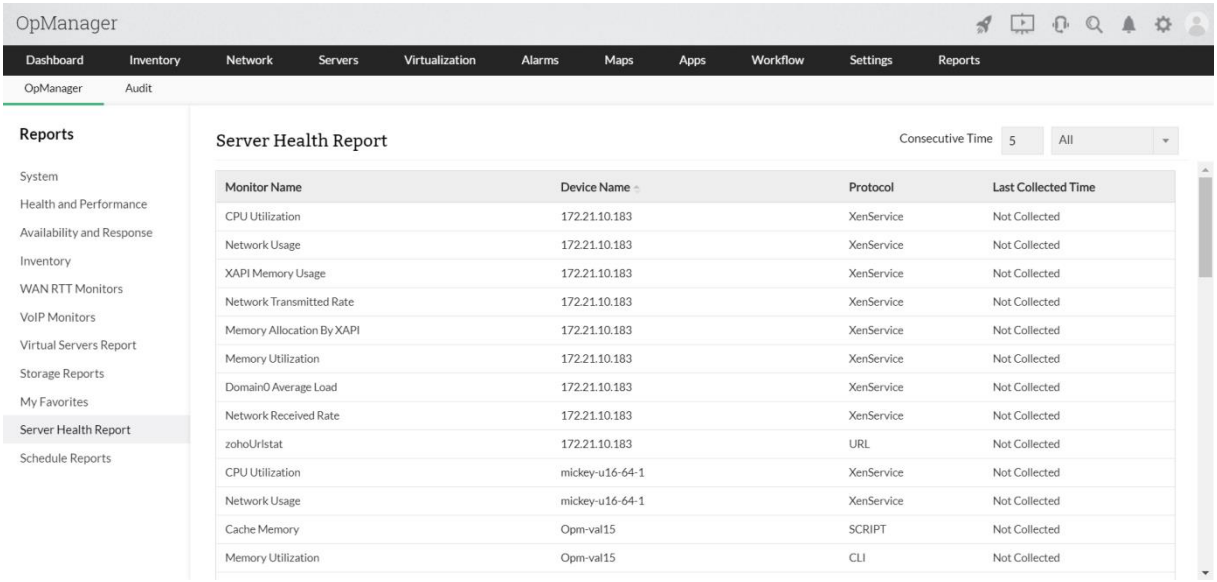


Figure 3.37: Rapports d'intégrité du serveur.

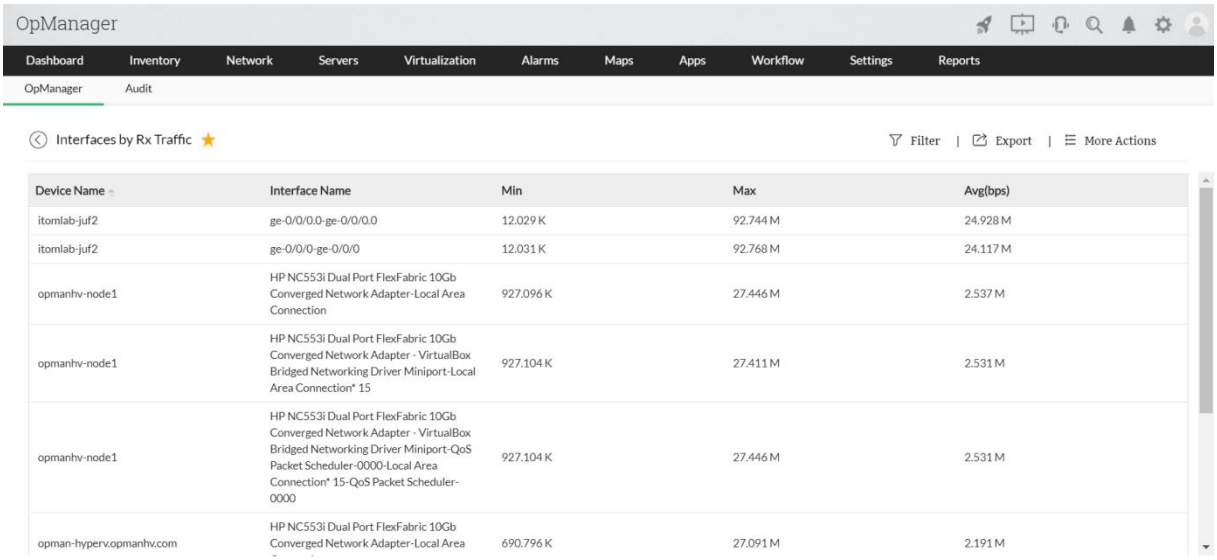


Figure 3.38 : Rapport de trafic d'interface.

3.15.2 Top N des rapports sur les performances ou la disponibilité des ressources

Les rapports intégrés d'Op Manager peuvent être organisés de manière à afficher les interfaces ou les périphériques qui ont le plus haut taux d'utilisation du processeur, l'utilisation de la mémoire, l'utilisation du disque, le trafic entrant et sortant, les erreurs d'interface, les temps de réponse, etc. "affiche une liste décroissante de 25 serveurs, en commençant par le serveur ayant la plus forte utilisation du processeur. Pour une enquête immédiate, tous les noms de serveur sont des liens sur lesquels vous pouvez cliquer davantage pour afficher les détails complets du périphérique surchargé [43].

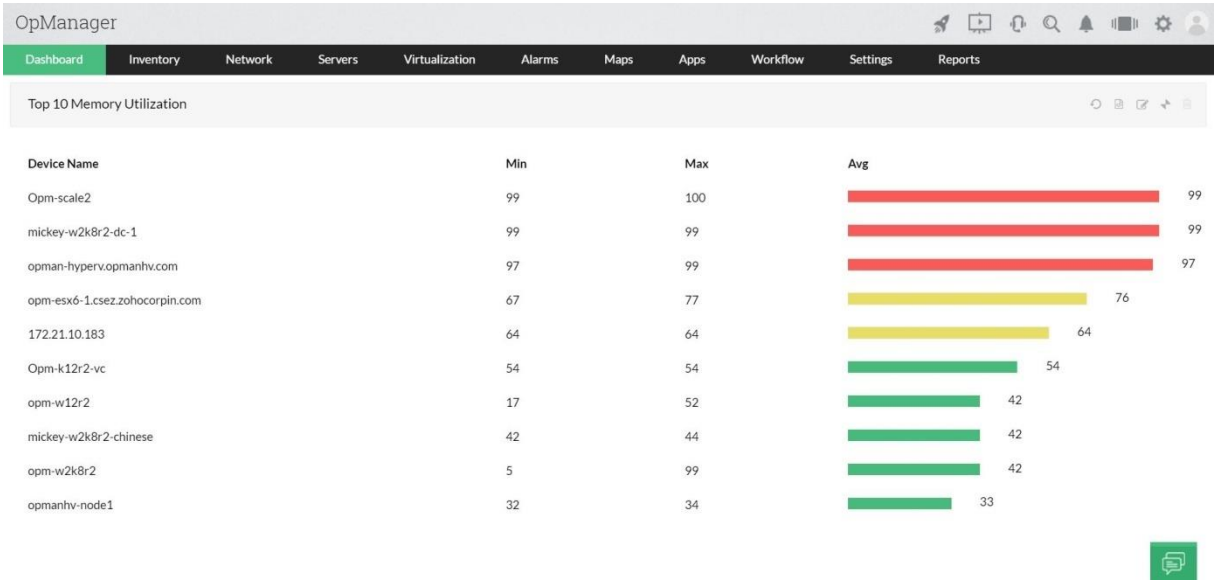


Figure 3.39 : serveur-mémoire-utilisation.

3.15.3 Rapports basés sur des instantanés d'entreprise

Op Manager fournit des rapports intégrés sur un groupe de périphériques et / ou une autre infrastructure réseau qui fonctionnent ensemble pour un groupe de services métier commun. Par exemple, considérez un service commercial critique tel que le système CRM de l'organisation. Un tel système pourrait avoir un serveur d'applications, un serveur Web et un serveur de base de données, chacun ayant une copie de sauvegarde à des fins de basculement. Une fois âpre avoir configuré une « vue d'entreprise », par exemple nommée « Système CRM » pour inclure tous les serveurs du groupe, Op Manager fournit des rapports combinés prêts à l'emploi sur les serveurs associés. Un rapport rapide sur l'utilisation du disque du serveur de la semaine permet facilement à l'administrateur d'allouer de manière optimale la mémoire du disque au sein du groupe de services CRM [43].

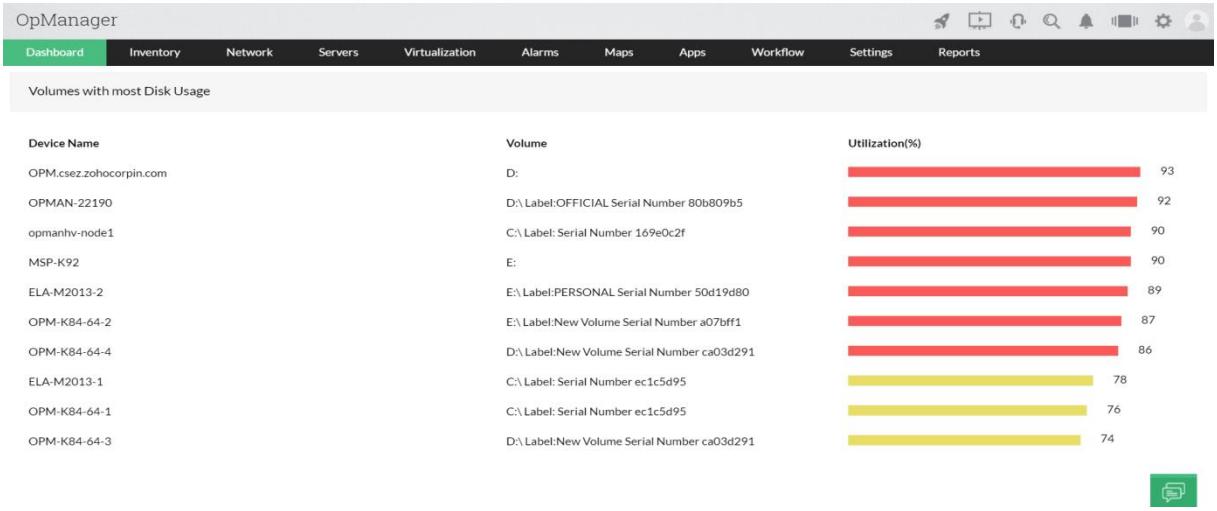


Figure 3.40: utilisation du disque pour chaque serveur.

Les rapports sur les vues d'entreprise sont utiles, en particulier lors de l'analyse des besoins en infrastructure d'un service / groupe d'entreprise. Envisagez un plan pour mettre à niveau le lien qui connecte votre succursale au siège social avec des périphériques qui connectent les deux sites commerciaux, à savoir deux routeurs et un pare-feu entre les deux. Certains des rapports importants requis pour la prise de décision seraient [43]**:**

- Tendances de l'utilisation de l'interface sur les routeurs de connexion au cours des 6 derniers mois.
- Statistiques mensuelles du trafic entrant et sortant de l'interface.
- Répartition application / utilisateur de la bande passante consommée sur la liaison.

3.15.4 Envoi par courrier électronique planifié et automatisé de rapports périodiques

Ce ne sont pas seulement les notifications de panne réseau qu'Op Manager envoie où que vous soyez, à tout moment de la journée. Le planificateur de rapports d'Op Manager permet d'automatiser la création de rapports et de les envoyer périodiquement aux destinataires souhaités. La création de rapports est facilitée par un certain nombre de dispositions flexibles qui aident à produire des rapports puissants et détaillés. Voici quelques exemples fréquemment utilisés de rapports automatisés [43]**:**

- Un rapport de fin de journée sur la disponibilité de tous les serveurs du Datacenter.
- Rapport hebdomadaire sur les performances de tous les processeurs, la mémoire et l'utilisation du disque de tous vos serveurs.

- Un rapport de fin de journée sur la disponibilité et les performances de tous les appareils d'un groupe de services aux entreprises, par exemple le système ERP.

- Rapports mensuels sur l'utilisation de la bande passante sur toutes les interfaces de routeur.

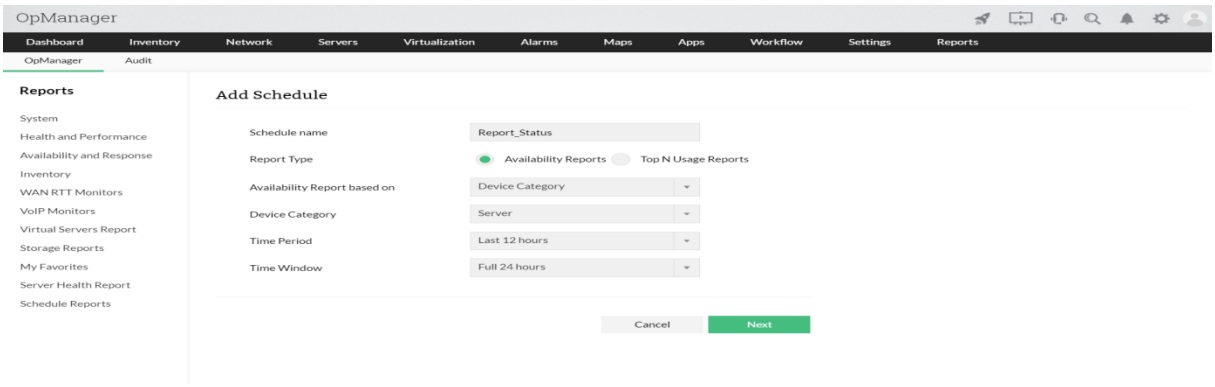


Figure 3.41 : Calendriers des rapports réseau.

3.16 But des rapports

Des tableaux de bord intuitifs et des rapports détaillés aide à déterminer les performances du réseau en très moins de temps. OpManager permet d'exporter les rapports par défaut vers d'autres formats de fichiers tels que l'exportation vers PDF ou XLS. Et également planifier les rapports à envoyer par courriel ou à publier. Les rapports par défaut disponibles dans OpManager incluent, on donne qu'elle que un [43]**:**

Système : Fournit un rapport complet sur toutes les activités liées au système de tous les appareils.

Santé et performance : vous présente un rapport détaillé sur la santé et les performances de tous les appareils.

Disponibilité et réponse : vous présente un rapport détaillé sur la disponibilité et le temps de réponse de tous les appareils.

Mettre en Œuvre un politique futur pour le développement et le besoin d'entreprise en matière bien physique et applicative.

3.17 Conclusion

Pour pouvoir effectue ce logiciel, la supervision doit donc impérativement être effectuée depuis différents points de contrôle sur une architecture distribuée avec des techniques permettant d'analyser et gérer en permanence les flux, op manager peut surveille, analyse, control la disponibilité, savoir qu'elle est le problème dans des pannes. Le chapitre suivant donnera une vue détaillée sur l'application du logiciel utilisé.

4 Chapitre 4 : Résultats et Testes

4.1 Introduction

Op manager comme on a vue dans le chapitre précèdent est un logiciel très puissant qui fournit un très grand ensemble d'utile pour la supervision qui couvre le matérielle et les serveurs ainsi qu'un ensemble rapport et d'alerte qui permettrons à un administrateur de gérer le bon fonctionnement du SI.

Dans ce qui suit on va faire un ensemble de test sur des machines virtuelles et physique qui serons connecté entre eux, les machines physiques de l'université Saad dahleb (switches, serveurs, routeurs et ESX), ce qui nous permettra d'avoir une supervision général de ces périphériques.

4.2 Introduction général sur Logiciel de supervision OpManager

La bonne marche de votre entreprise nécessite une disponibilité et des performances optimales. De plus, la gestion proactive des évènements par un administrateur permanent est devenue nécessaire pour vos réseaux locaux et distants.

OpManager simplifie la gestion réseau en alertant les administrateurs réseaux des dégradations de service et de performance ce qui permit [44]:

- Utilisation optimale des ressources.
- Prendre les bonnes décisions en identifiant les points de contention et les ressources non utilisées, grâce à de nombreux rapports disponibles en ligne ou en différé.
- Statistiques d'utilisation des ressources (CPU, mémoire, disque, applications, etc…).

OpManager propose également une visibilité permanente sur les performances réseau, en assurant de préserver les niveaux de service définis avec les utilisateurs, de contrôler et de planifier la montée en charge du réseau d'entreprise et d'offrir une optimisation maximum des investissements logiciels et matériels ce qui offre Une meilleure visibilité de l'infrastructure :

- Visualisation du réseau : classement automatique de vos routeurs, serveurs, switch et imprimantes.

- Visualisation organisationnelle : classement par systèmes, applications afin de mieux les gérer (classement géographique, etc…).

Vue globale de votre réseau à partir d'un seul point centralisé :

- Infrastructure WAN (interconnections, routeurs).
- Infrastructure LAN (Switch, Imprimantes et ordinateurs portables).
- Serveurs (HTTP, Mail, FTP, LDAP, DNS, etc…).
- Applications (MS-SQL, MS-Exchange, Oracle, MySQL, Lotus Notes, etc…).

4.3 OpManager - prérequis techniques Recommandations système

Tableau nous montre les Recommandations système [44].

	moins de 500 interfaces ou 100 serveurs	**de 500 à 2500 interfaces ou 500 serveurs**	**de 2500 à 5000 interfaces ou 750 serveurs**	**de 5000 à 10000 interfaces ou 1000 serveurs**
Processeurs	2.0 GHz	Dual Core 3.5 GHz	Quad Core 3.5 GHz	Quad Core 3.5 GHz
Mémoire	4 GB	4 GB	8 GB	16 GB
Espace disque disponible	20 GB	40 GB	60 GB	80 GB
NIC	10 Mbps	100 Mbps	1 Gbps	1 Gbps
Résolution écran	1024 x 768 ou supérieures			
OS 32bit et 64bit	Windows Server OSes: v7, 2008, 2003 Server, Vista, XP Pro et 2000 Professional SP4 Linux: RedHat 4.x and above, Debian 3.0, Suse, Fedora et Mandrake			
Base de données	MS SQL 2000, 2005 et 2008 ou OpManager bundled My SQL v5.0			
Navigateurs	IE 7.0 +, Firefox 2.0 + and Chrome 4.0 +			

Tableau 4.1 : Recommandations système.

4.4 Schéma utiliser

Pour des tests qui couvrirons presque tous les matériels réseaux existent aux de l'université sein on a opérer sur schéma qui contient les éléments suivant (figure 4.1).

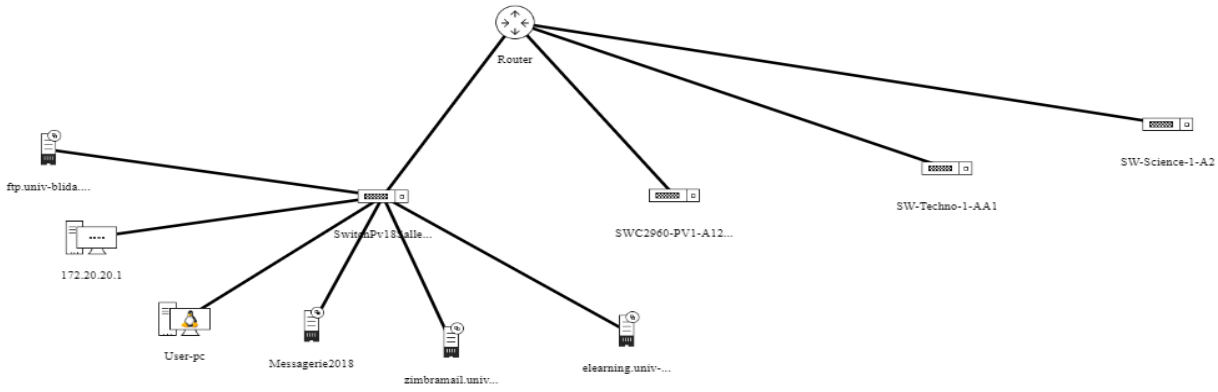


Figure 4.1 : Schéma utiliser.

Pour superviser notre infrastructure (switch, serveur, routeur, ESX et VCenter) on doit on premier lieu les reconnaitre, une foi l'infrastructure est reconnue par OpManager on aura la possibilité de la superviser, donc avoir des rapportes et des alertes ...

4.5 Les Etapes à suivre pour supervision un périphérique

Etape 1 : Attribution d'adresse IP au périphérique.

On fait l'attribution d'adresse IP pour connaitre le périphérique pour pouvoir l'ajouter.

Etape 2 : Vérification de la connectivité entre le gestionnaire et le périphérique.

Après avoir reconnue le périphérique, on aura besoin de le pingé pour bien s'assurer de la liaison.

Etape 3 : Configuration SNMP et ajouter les Credential.

La configuration du SNMP ce ferai dans nos différentes périphérique le but est L'activation de l'agent SNMP, lui permet de collecter la base de données d'informations de gestion à partir du périphérique localement et la met à la disposition du gestionnaire SNMP.

Pour reconnaitre un périphérique avec op manager on doit ajouter un Credential, OpManager accède aux périphériques distants à l'aide des protocoles SNMP ou WMI. Les informations d'identification comme la communauté mot de passe/snmp, le port, etc., Peuvent différer pour différents types d'appareils. La pré configuration d'un ensemble d'informations d'identification dans OpManager aide à les appliquer à plusieurs appareils à la fois, Économiser beaucoup d'efforts manuels.

Etape 4 : ajouter le Périphérique

Ajouter un périphérique à l'aide de son Credential.

4.6 Attribution D'adresse IP au périphérique

4.6.1 Attribution d'une adresse IP au switch

Pour pouvoir super visionné notre switch il faut lui attribuer une adresse (figure 4.2) :

Comme exemple ces commande :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip add 172.20.213.2 255.255.0.0
Switch(config-if)#no sh

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

Figure 4.2 : Attribution adresse IP au switch.

4.6.2 Donne une adresse IP au Routeur

Comme le Switch, c'est le tour du routeur, nous allons attribue une adresse IP a notre routeur (Figure 4.3).

```
Router(config)#int f0/0
Router(config-if)#ip add 172.20.18.137 255.255.0.0
```

Figure 4.3 : Attribution adresse IP au routeur.

On a attribué l'adresse 172.20.18.137 a notre interface.

4.7 Vérification de la connectivité entre les périphériques et le gestionnaire snmp.

4.7.1.1 Ping le switch

```
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\cc>ping 172.20.213.2

Envoi d_une requête 'Ping'  172.20.213.2 avec 32 octets de données :
Réponse de 172.20.213.2 : octets=32 temps=1 ms TTL=255
Réponse de 172.20.213.2 : octets=32 temps=1 ms TTL=255
Réponse de 172.20.213.2 : octets=32 temps<1ms TTL=255
Réponse de 172.20.213.2 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 172.20.213.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\cc>
```

Figure 4.4 : Ping entre le gestionnaire snmp et le switch.

4.7.1.2 Ping le serveur

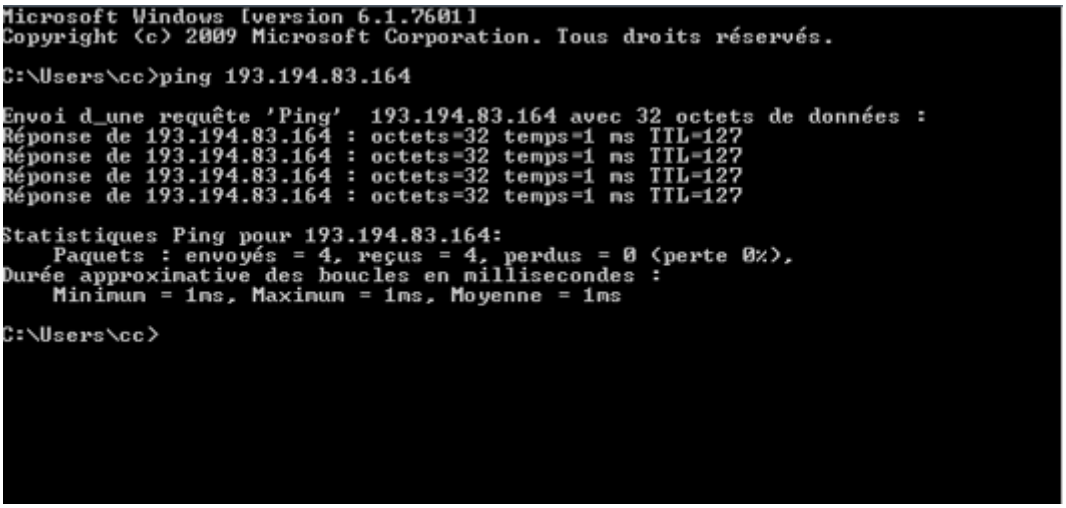


Figure 4.5 : Ping entre serveur et le gestionnaire snmp.

4.7.1.3 Ping le routeur

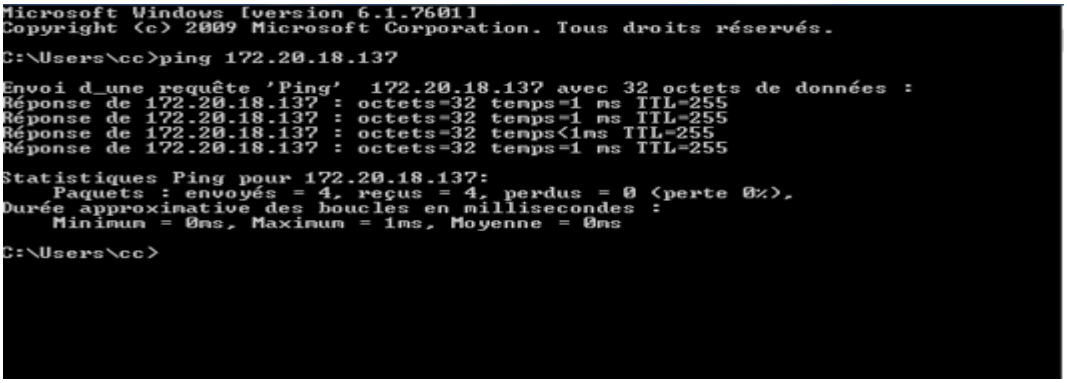


Figure 4.6 : Ping entre le routeur et le gestionnaire snmp.

4.8 Ajouter un Credential et configuration SNMP

Avant tout il faut ajouter les Credential , settings →Discovery → Credential → Add Credential.

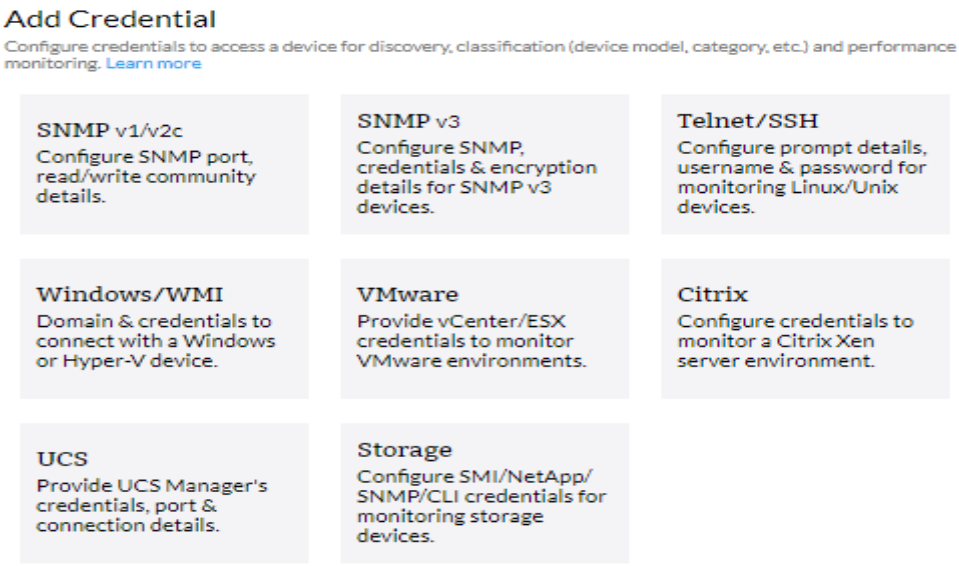


Figure 4.7 : Add Credential.

Cette figure 4.7 nous montre les différents Credential.

Avant d'ajouter un des périphériques, il faut savoir avoir quelle Credential qu'on doit utiliser, dans le cas d'un :

- Switch On va utiliser le snmp v1/ v2, dans le d'un multi layer switch on peut même utiliser la v3.
- Le routeur on peut utiliser les 3 version, mais de préférence le Credential le plus sécuriser la v3.
- Dans e cas d'un serveur on vas utiliser les deux protocole principales SNMP et WMI.
- Le cas d'un PC Linux on aura besoin du Telnet/SSH et l'aide SNMP.
- Pour les machines Virtuelle on aura besoin de VMware, Citrix...

4.8.1 Switch

4.8.1.1 Configuration SNMP v1 sur un switch

Apre avoir attribué une adresse IP au switch, nous allons effectuer une configuration snmp v1 sur l'un des switches.

La configuration de snmpv1 sur le switch est comme suivants (figure 4.5) :

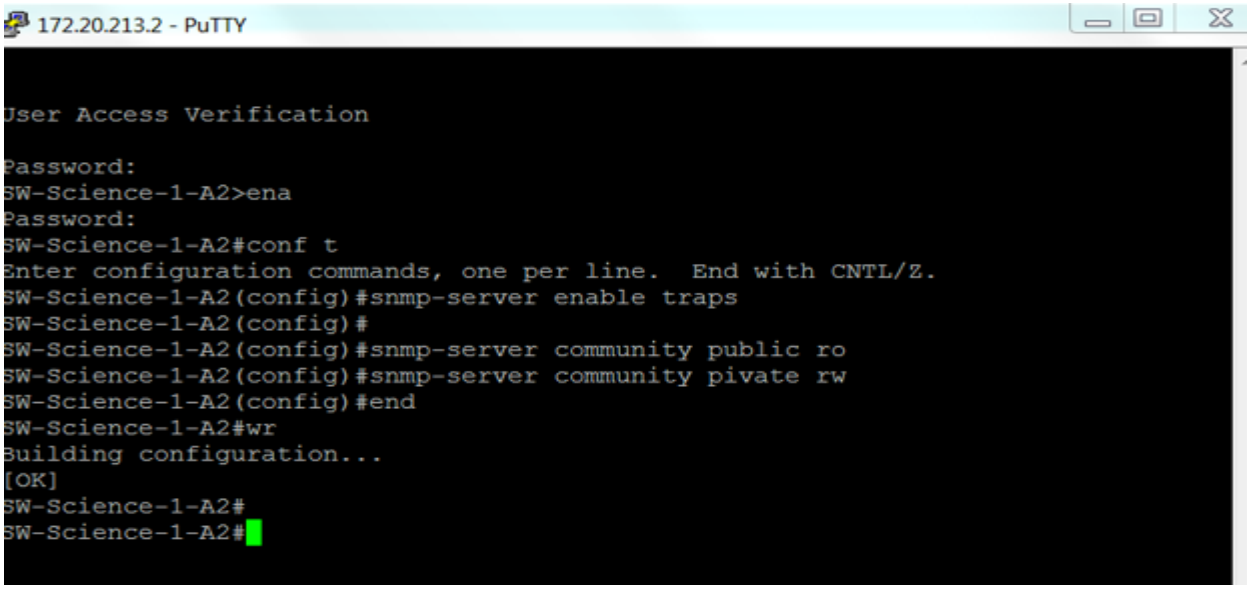


Figure 4.8 : Configuration SNMP.

Dans notre configurions on active snmp et défini les valeurs de snmp server Community public et private quand vas utiliser dans le Credential.

4.8.1.2 Ajouter Credential d'un switch

L'ajoute du Credential, pour SNMP Read community c'est Public et write c'est privet (figure 4.9).

Figure 4.9 : Ajouter un Credential pour le Switch.

4.8.1.3 Ajouter un switch

Pour cella on va sur setting → Discovery → Add Device.

Ou on va indiquer l'adresse IP du switch ainsi que le Credential utiliser.

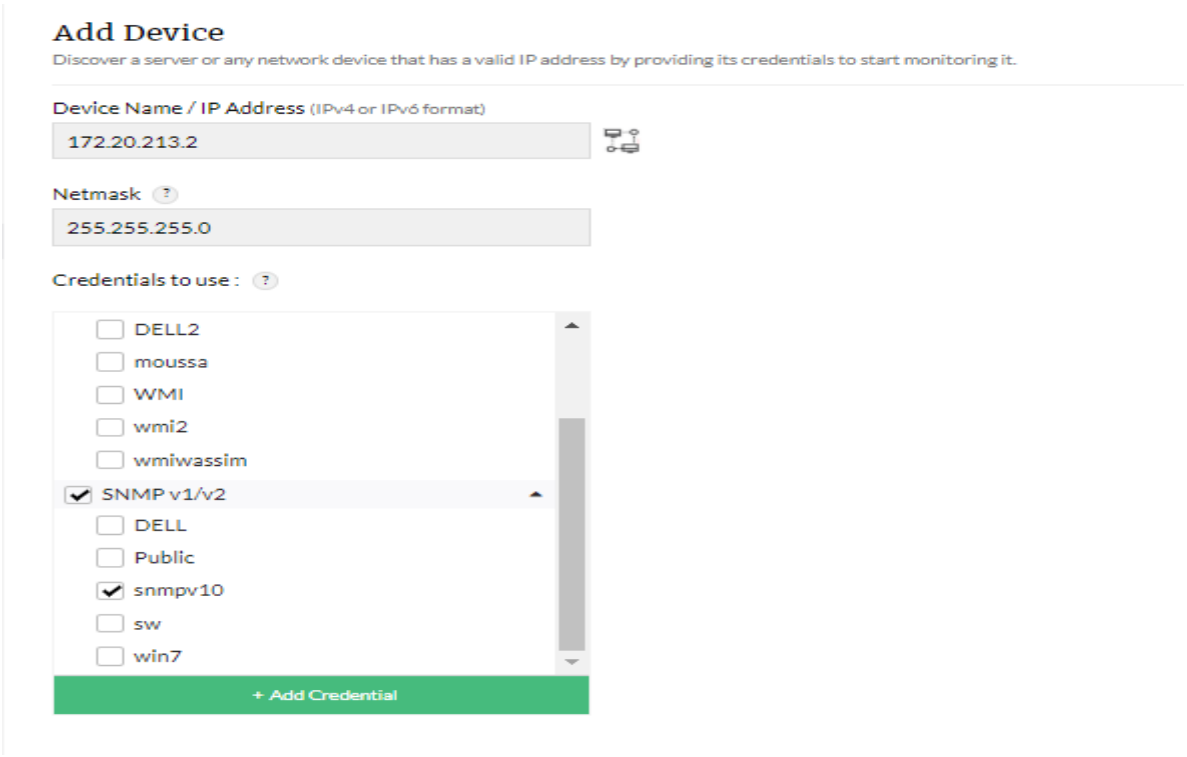


Figure 4.10 : Ajouter périphérique Serveur.

4.8.2 Serveur

4.8.2.1 Configuration SNMP et WMI dans un Serveur

Concernant les serveur Windows, il faut avant tout activé le service SNMP et WMI sur les serveurs.

L'activation de l'agent permet de collecter la base de données d'informations de gestion à partir du périphérique localement et la met à la disposition du gestionnaire SNMP.

L'activation se fait comme suivant, dans la barre recherche Windows taper Service.

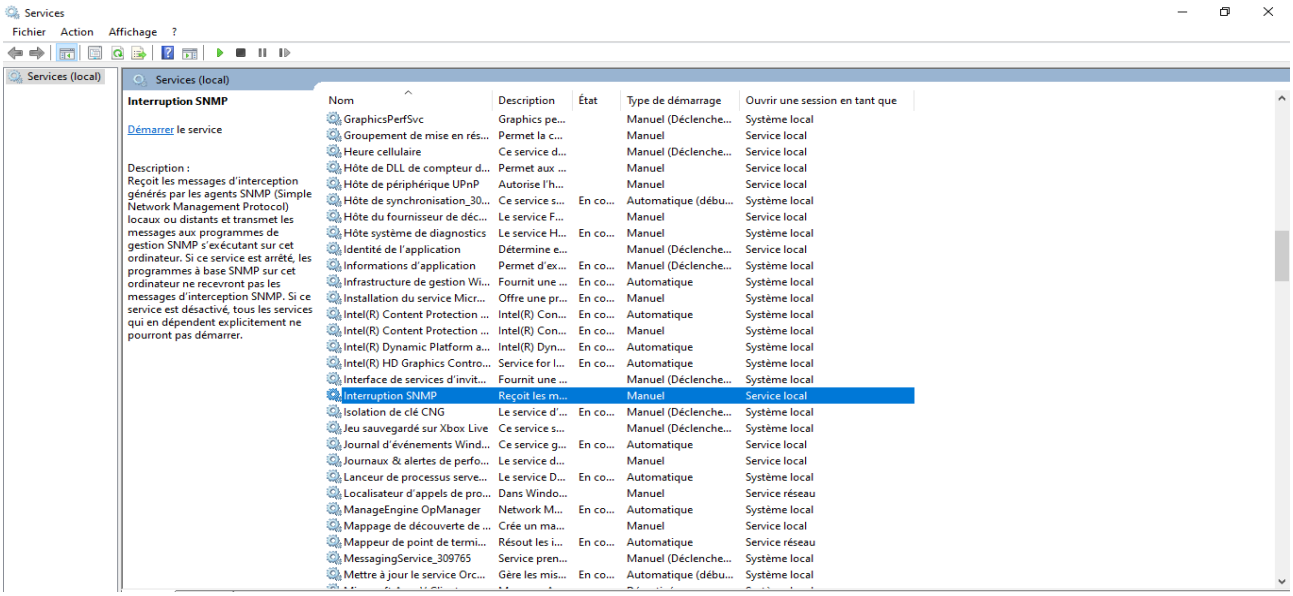


Figure 4.11 : Barre server local.

Chercher SNMP, si vous le trouvé, mettez démarrer (figure 4.11).

Si vous le trouvé pas, allez vers fonctionnalités de Windows et activez la case à cocher.

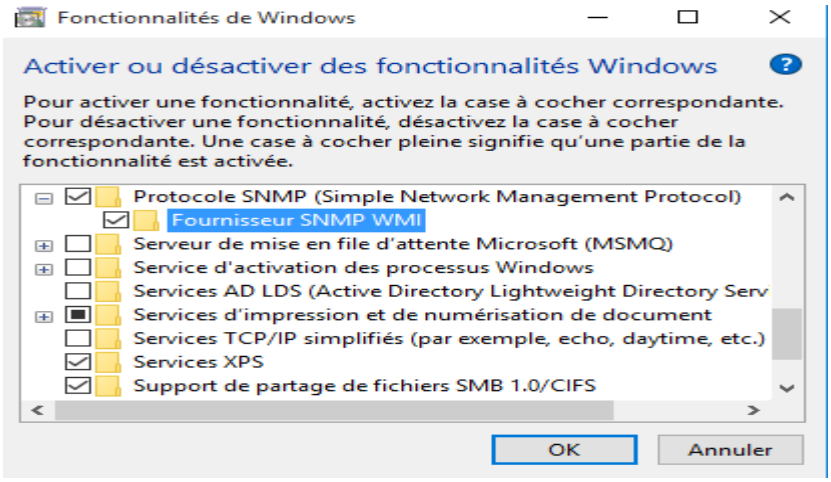


Figure 4.12 : FONCTIONNALITES DE Windows.

Même chose pour le WMI.

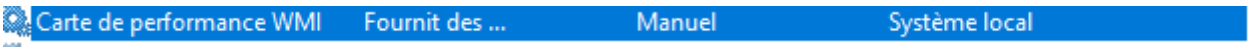


Figure 4.13 : Carte de performance WMI.

4.8.2.2 Propriétés de Service SNMP

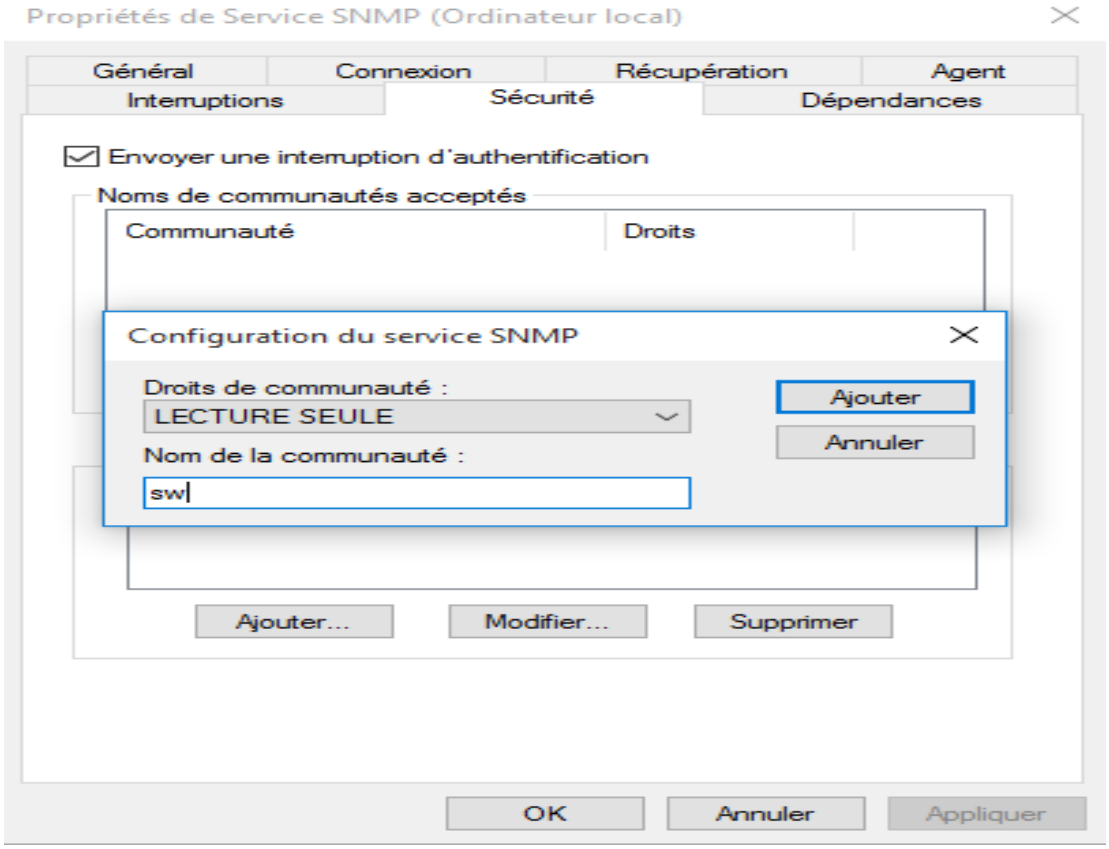


Figure 4.14 : Ajouter une communauté.

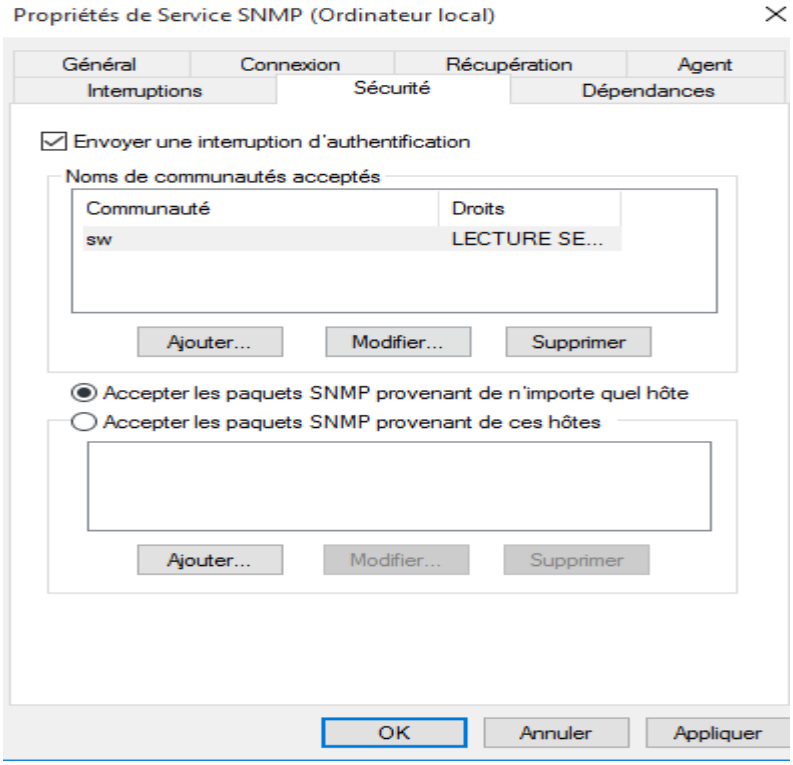


Figure 4.15 : Accepter les paquets SNMP provenant de n'importe quel Hôte.

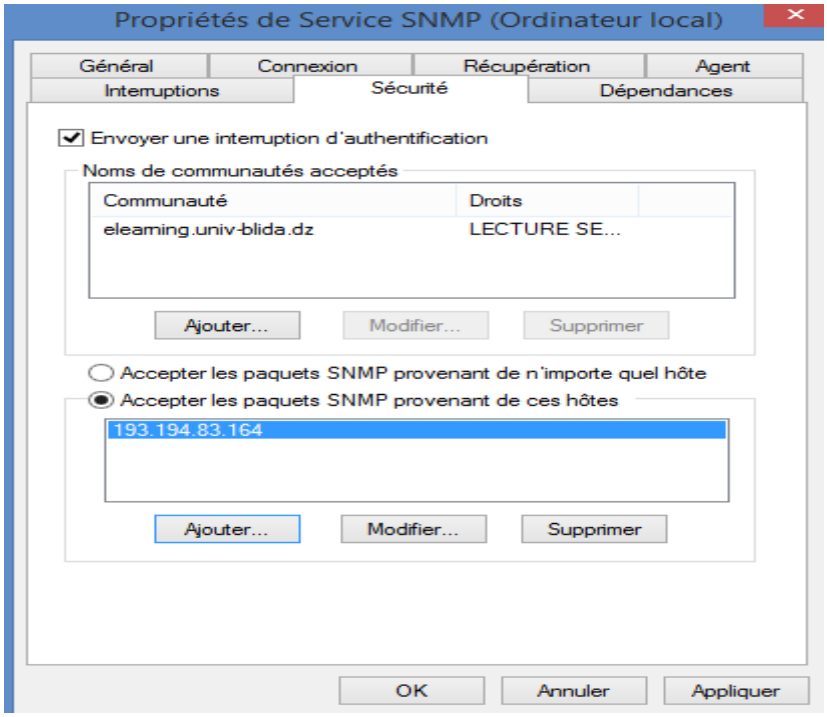


Figure 4.16 : Ajouter l'adresse IP de notre serveur SNMP.

4.8.2.3 Edit Credential pour un serveur

On va ajouter des Credential, pour le serveur on l'attribue SNMP v1/v2 et/ou MWI comme Credential (figure 4.17).

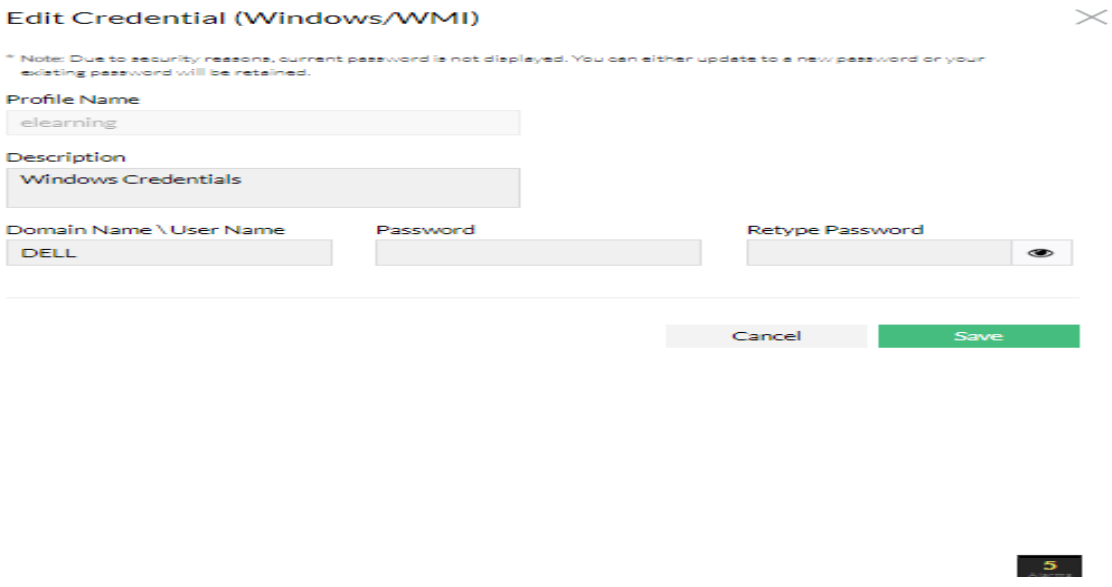


Figure 4.17 : Ajouter Credential WMI pour serveur.

4.8.2.4 Ajouter un serveur

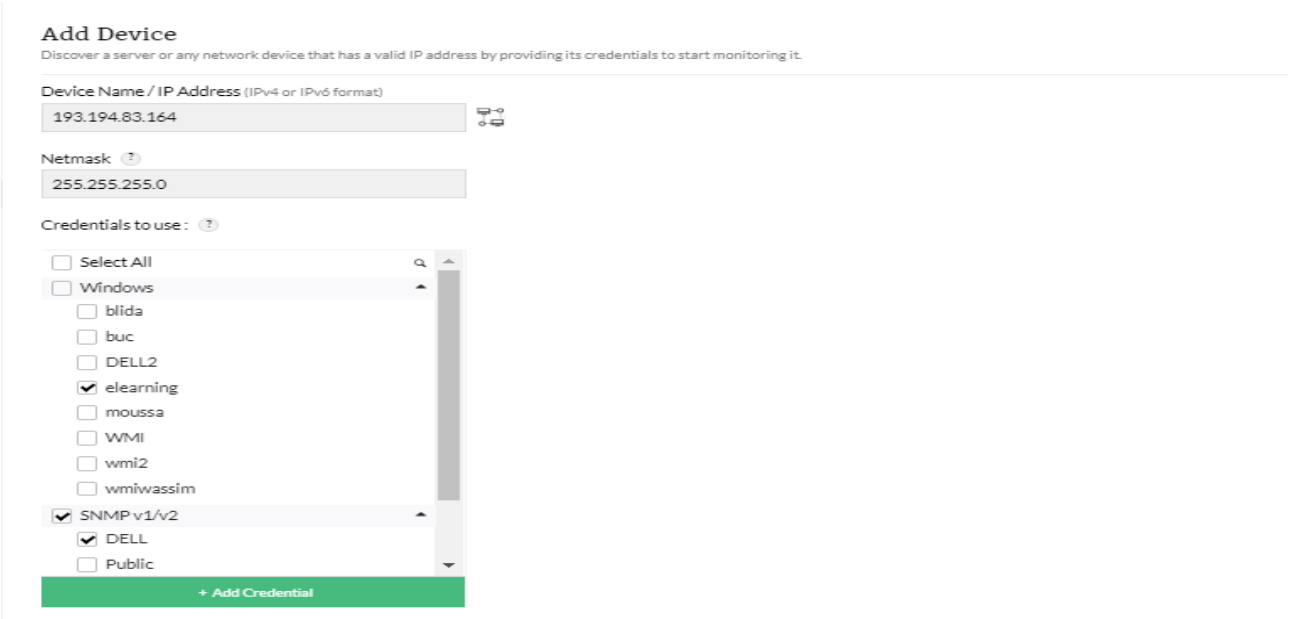


Figure 4.18 : Ajouter un périphérique Serveur.

4.8.3 Le Routeur

4.8.3.1 Configuration de snmp v1 dans Le Routeur.

Apre avoir attribué une adresse IP au routeur, nous allons effectuer une configuration, d'où c'est la configuration de notre snmp v1 ce l'un de ces routeurs. (Le routeur utiliser ne supporte pas snmp v3).

La configuration de snmpv1 sur le routeur est comme suivants (figure4.19) :

```
Router(config)#snmp-server community public ro
Router(config)#snmp-server community private rwo
Router(config)#end
```

Figure 4.19 : Configuration routeur.

4.8.3.2 Ajouter Credential d'un Routeur

L'ajoute du Credential, pour SNMP Read community c'est Public et write c'est private (figure 4.20).

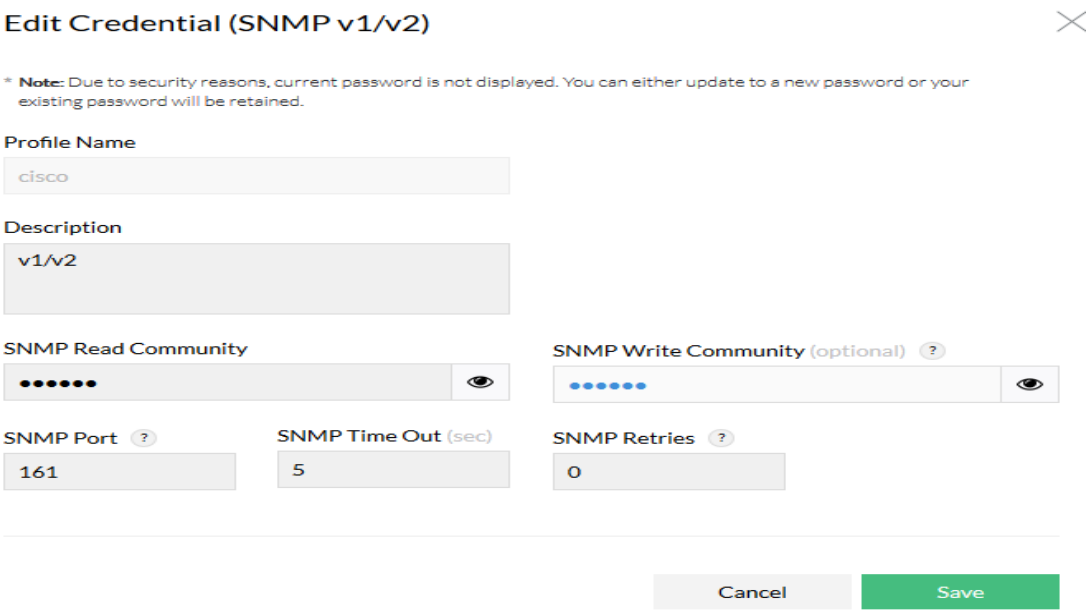


Figure 4.20 : Ajouter Credential pour le routeur.

4.8.3.3 Ajouter un routeur

Pour cella on va sur setting → Discovery → Add Device.

On ajoute le routeur qui porte l'IP 172.20.18.137 (figure 4.21)

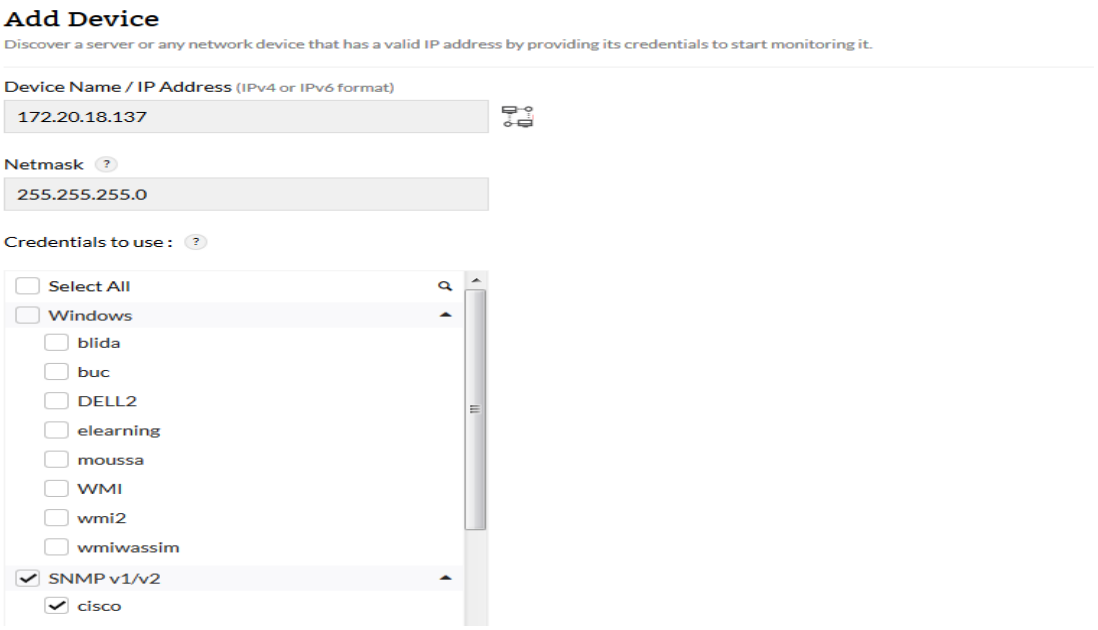


Figure 4.21 : Ajouter un routeur.

4.8.4 VMware

4.8.4.1 Ajouter Credential VMware

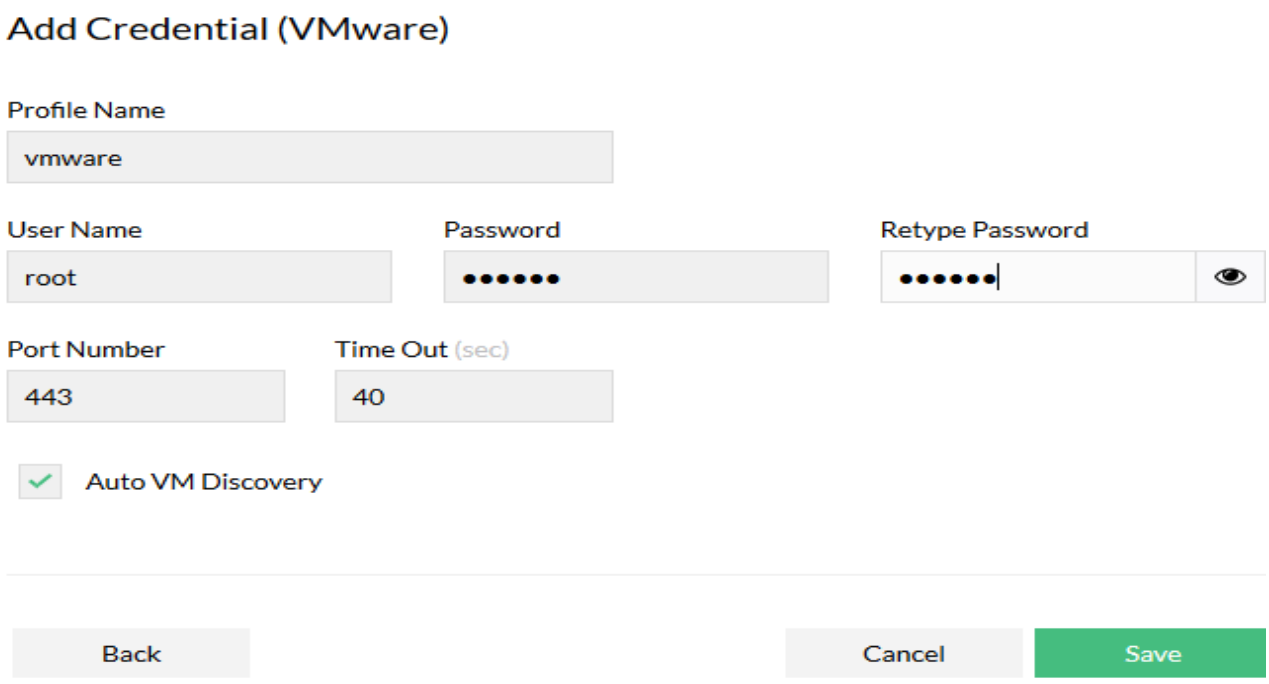


Figure 4.22 : Add Credential pour VMware.

4.8.4.2 VMware Discovery

Pour VMware Esx on doit écrire l'adresse IP du VCenter comme il le montre la figure 4.23.

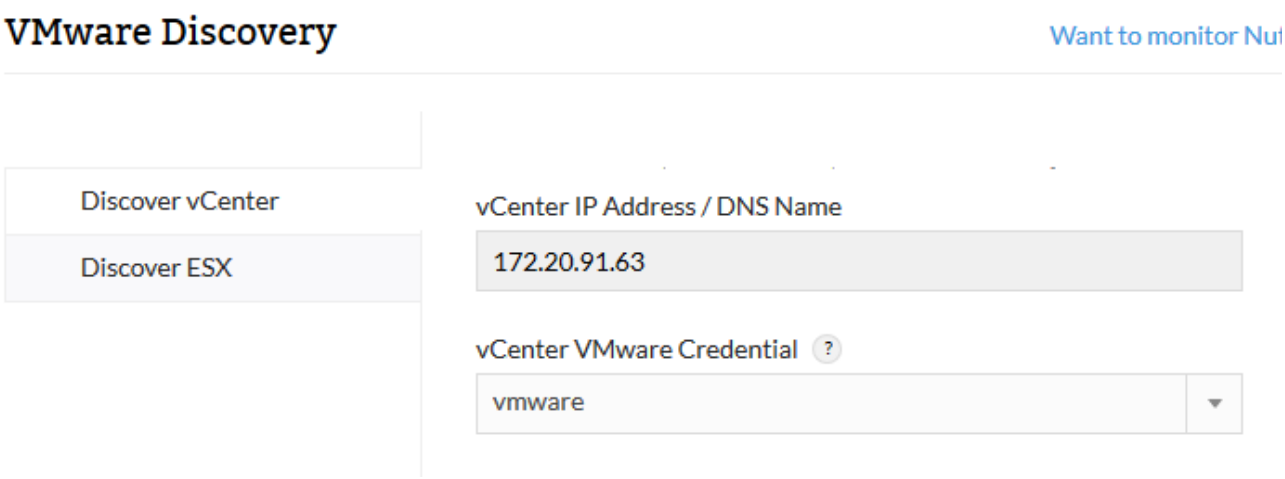


Figure 4.23 : VMware Discovery.

Une foi la détection du VCenter est réussi on va avoir tous les serveur ESX existant ainsi que l'ensemble des machines virtuel qui serrent traiter comme des serveurs physiques.

4.8.5 Résultat de l'application

Dans ce qui suit on va vous montrer quelque résultat concernons les différents matériaux étudie.

4.8.5.1 Résultat d'un switch

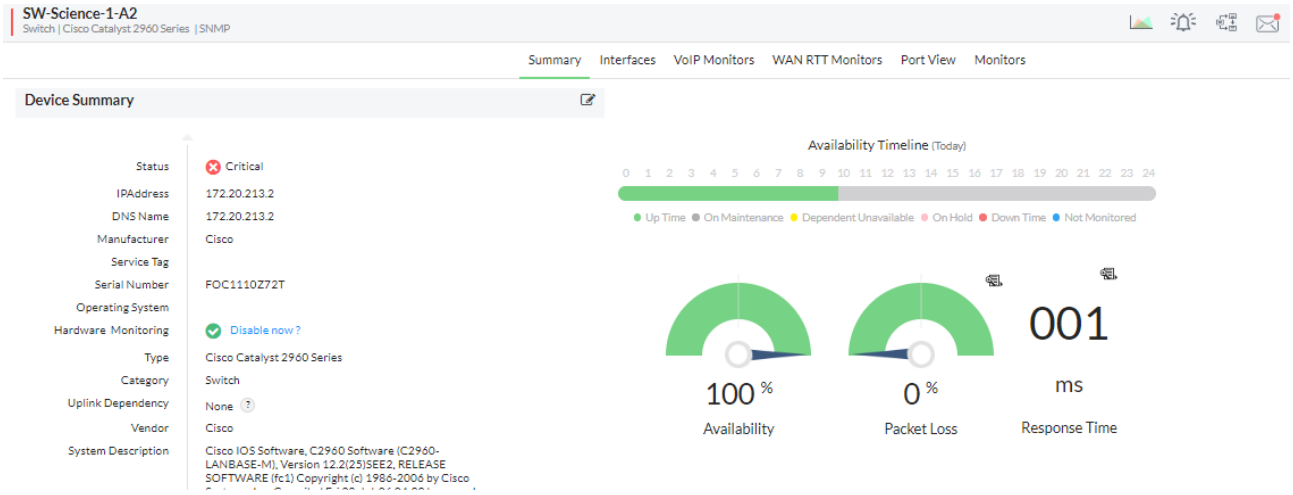


Figure 4.24 : Etat du switch.

La figure 4.24 nous montre l'état du switch (adresse IP sa version, login détaille, série Numbers ...).

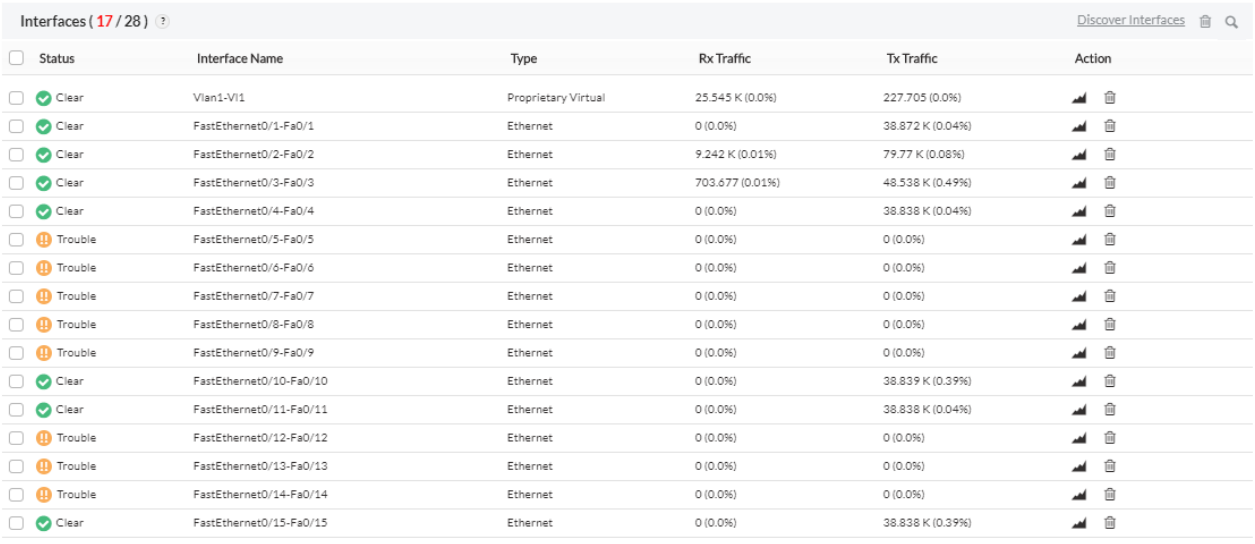


Figure 4.25 : Interface switch.

La figure 4.25 nous montre l'état des interfaces s'ils sont UP ou down, avec es différence type (Ethernet ou serial), la différence consommation de la bonde passante.

4.8.5.2 Résultat d'un serveur

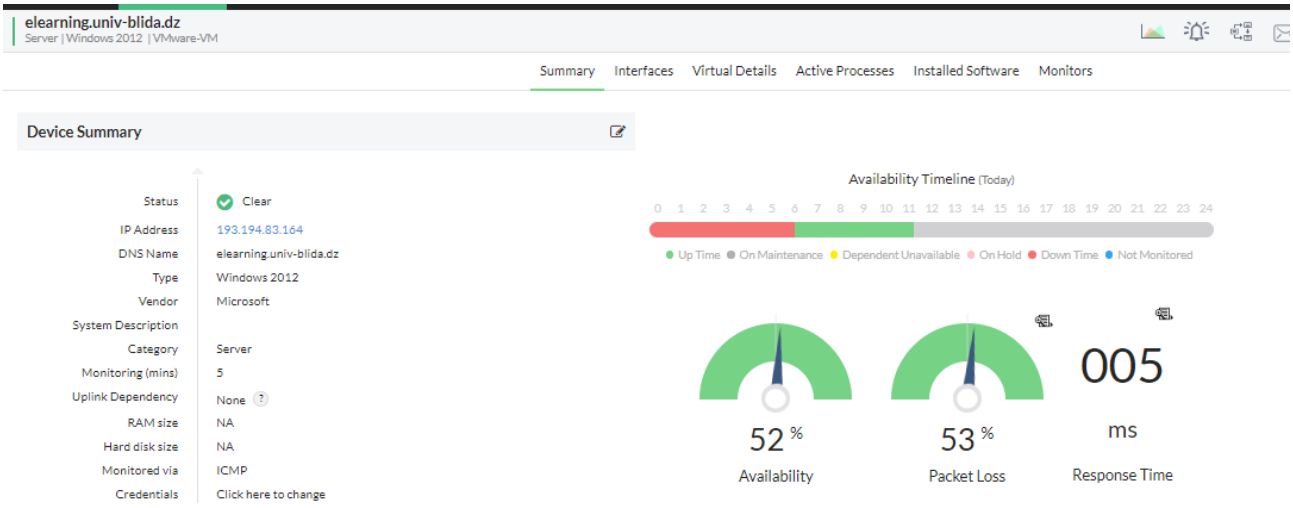


Figure 4.26 : Etat Serveur E-learning.

Voilà bien ce qu'on a obtenu comme résultat d'observation de performances de notre serveur (figure 4.27).

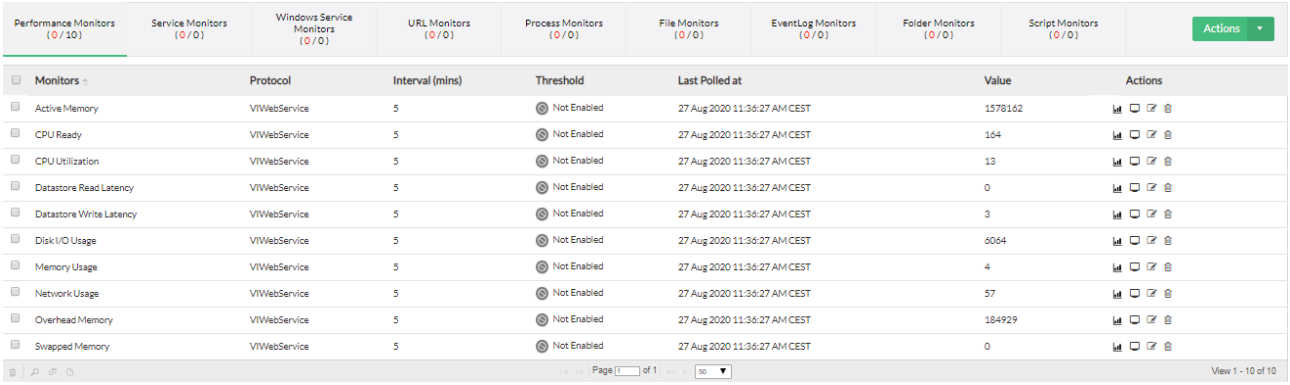


Figure 4.27 : Supervision outil physique de notre serveur.

La figure 4.28 Nous montre l'ensemble des activités qu'on peut superviser.

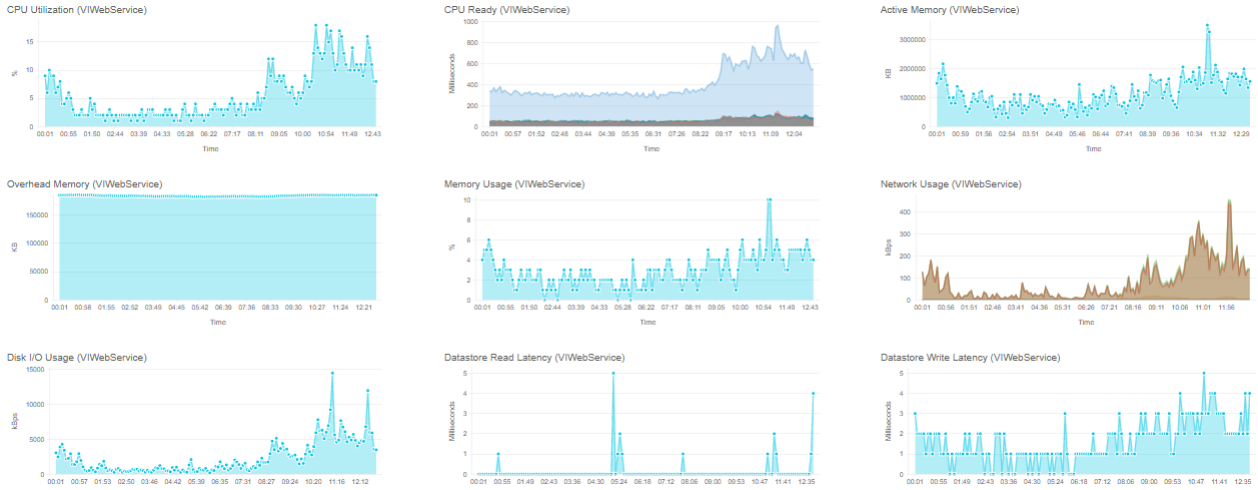


Figure 4.28 : Graphe des performances d'utilisation de notre serveur.

4.8.5.3 Résultat d'un routeur

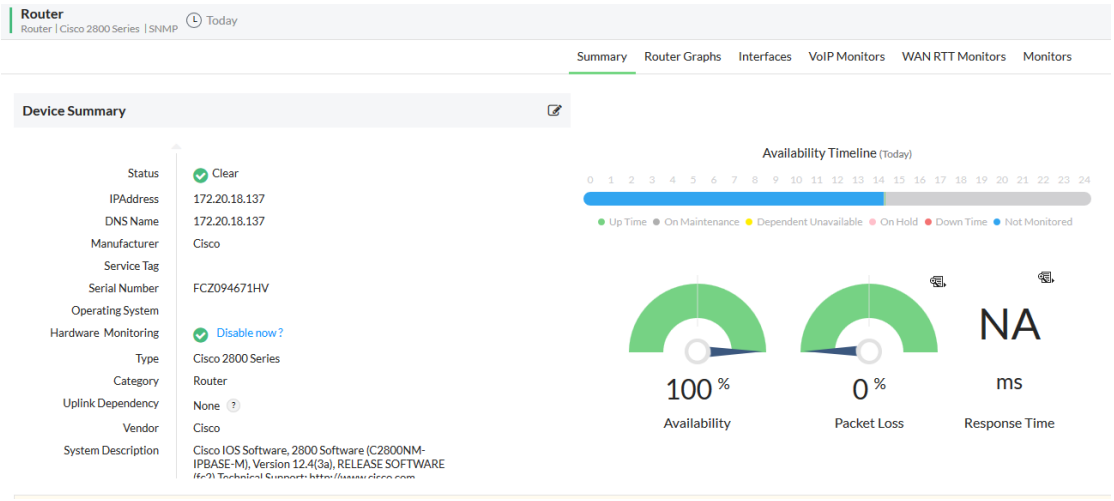


Figure 4.29 : Etat de notre routeur.

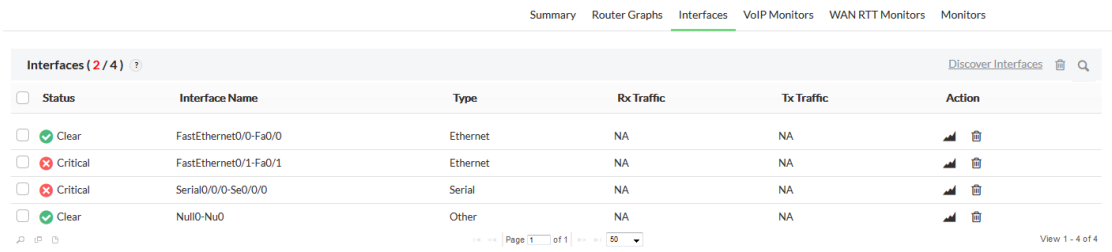
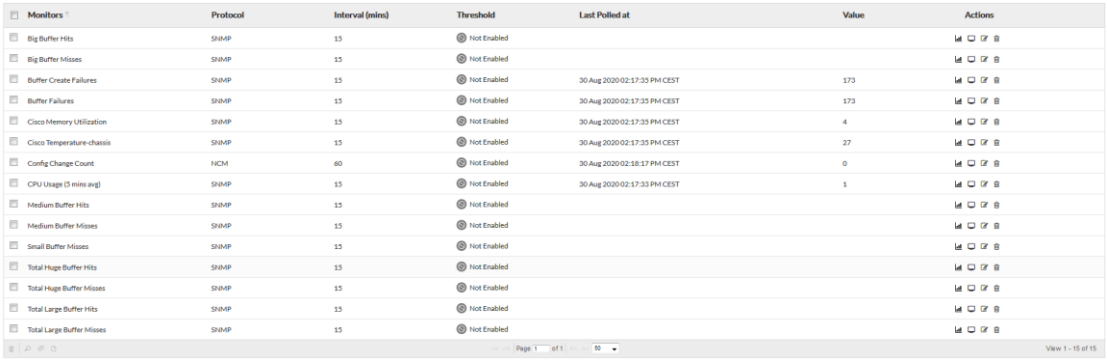


Figure 4.30 : Interface Routeur.



Monitors	Protocol	Interval (mins)	Threshold	Last Polled at	Value	Actions
Big Buffer Hits	SNMP	15	Not Enabled			
Big Buffer Misses	SNMP	15	Not Enabled			
Buffer Create Failures	SNMP	15	Not Enabled	30 Aug 2020 02:17:35 PM CEST	173	
Buffer Failures	SNMP	15	Not Enabled	30 Aug 2020 02:17:35 PM CEST	173	
Cisco Memory Utilization	SNMP	15	Not Enabled	30 Aug 2020 02:17:35 PM CEST	4	
Cisco Temperature-chassis	SNMP	15	Not Enabled	30 Aug 2020 02:17:35 PM CEST	27	
Config Change Count	NCM	60	Not Enabled	30 Aug 2020 02:18:17 PM CEST	0	
CPU Usage (5 mins avg)	SNMP	15	Not Enabled	30 Aug 2020 02:17:33 PM CEST	1	
Medium Buffer Hits	SNMP	15	Not Enabled			
Medium Buffer Misses	SNMP	15	Not Enabled			
Small Buffer Misses	SNMP	15	Not Enabled			
Total Huge Buffer Hits	SNMP	15	Not Enabled			
Total Huge Buffer Misses	SNMP	15	Not Enabled			
Total Large Buffer Hits	SNMP	15	Not Enabled			
Total Large Buffer Misses	SNMP	15	Not Enabled			

Figure 4.31 : Supervision outil physique de notre Routeur.

4.8.5.4 Résultat du VMware

VMware Discovery - Entities

ESX servers will be monitored by default, choose the VMs to be monitored from the below list.

ESX Servers

Entity Name	DNS Name
172.20.100.4	localhost
172.20.91.	localhost
172.20.91	TEMPUS

Figure 4.32 : ESX Servers.

La figure 4.32 nous montre l'ensemble des serveurs ESX relie au VCenter

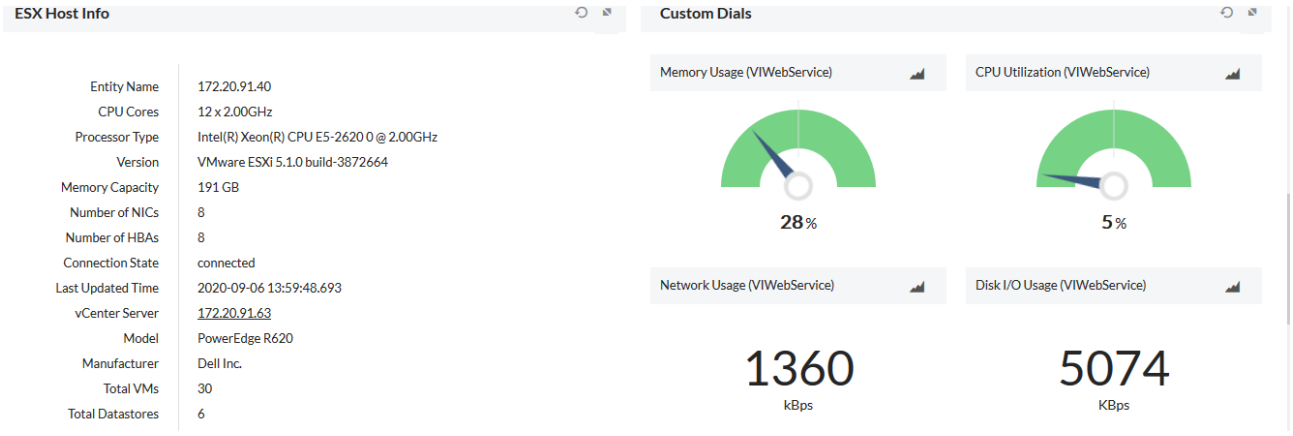


Figure 4.33 : ESX Host Info**.**

La figure 4.34 nous montre les caractéristiques physique et réseau de l'un des ESX.

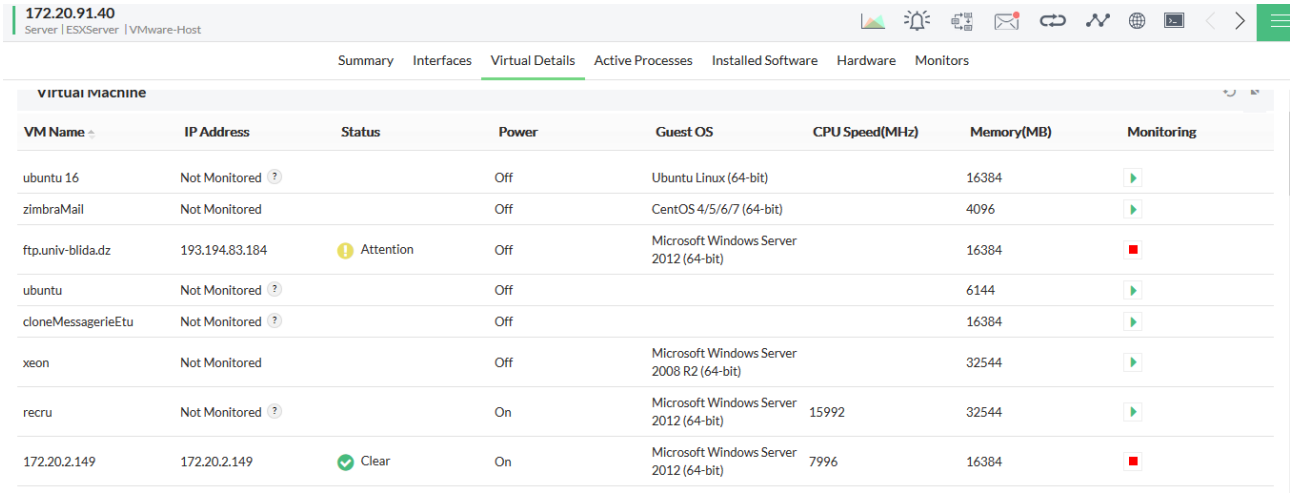


Figure 4.34 : Serveur de ESX.

La figure 4.34 nous montre les différentes machines virtuelles dans un ESX.

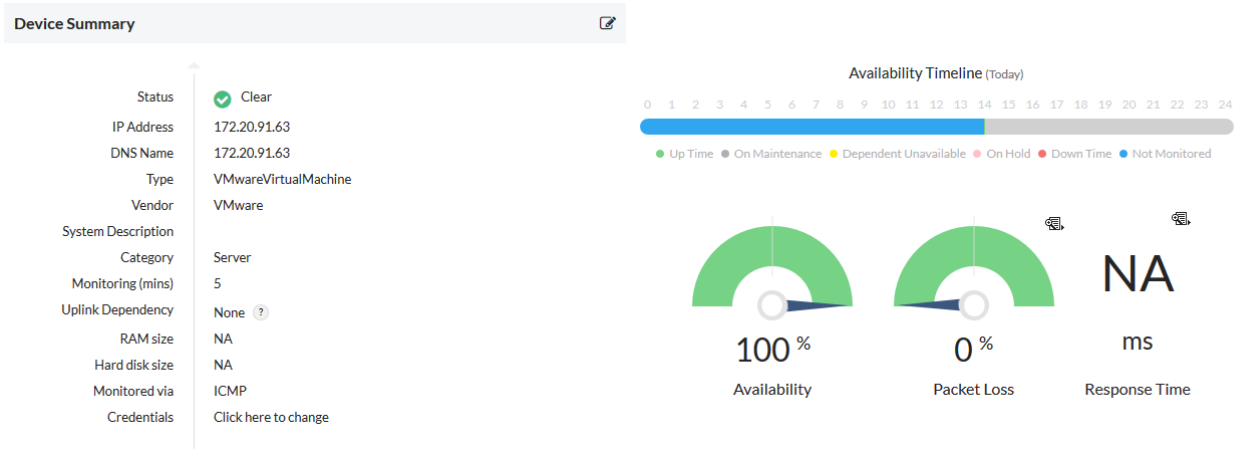


Figure 4.35 : Deuxième ESX.

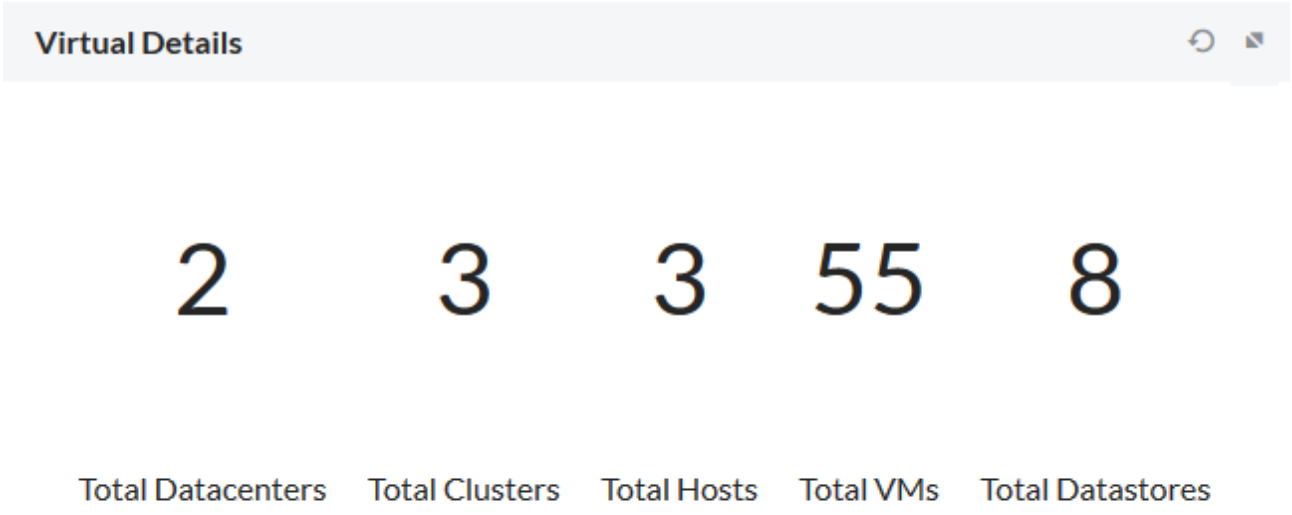


Figure 4.36 : Virtual Détails.

La figure 4.36 nous montre les caractéristiques du VCenter d'où :

Dans on trouve (les nombre de baille de stockage (2), les ESX (3), les machines virtuelle (55) et les sous data store (8)).

4.8.5.5 Les alertes

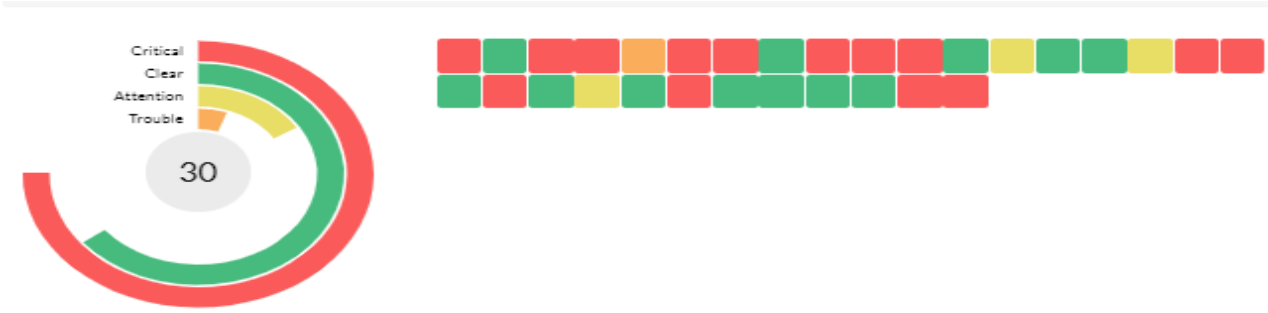


Figure 4.37 : Différents type d'alerte.

La figure 4.37 nous montre les différentes état d'une alerte en temps réel, d'où :

- Le rouge signifie que l'état critique le périphérique est éteint ou pas on l'état de marche.
- Le vert signifie que tout marche bien.
- Le jaune signifie qu'il faut faire attention souvent du au outil physique de notre périphérique (cpu, ram) ...
- L'orange signifie que le logiciel a des difficultés de voir l'Etat du périphérique.

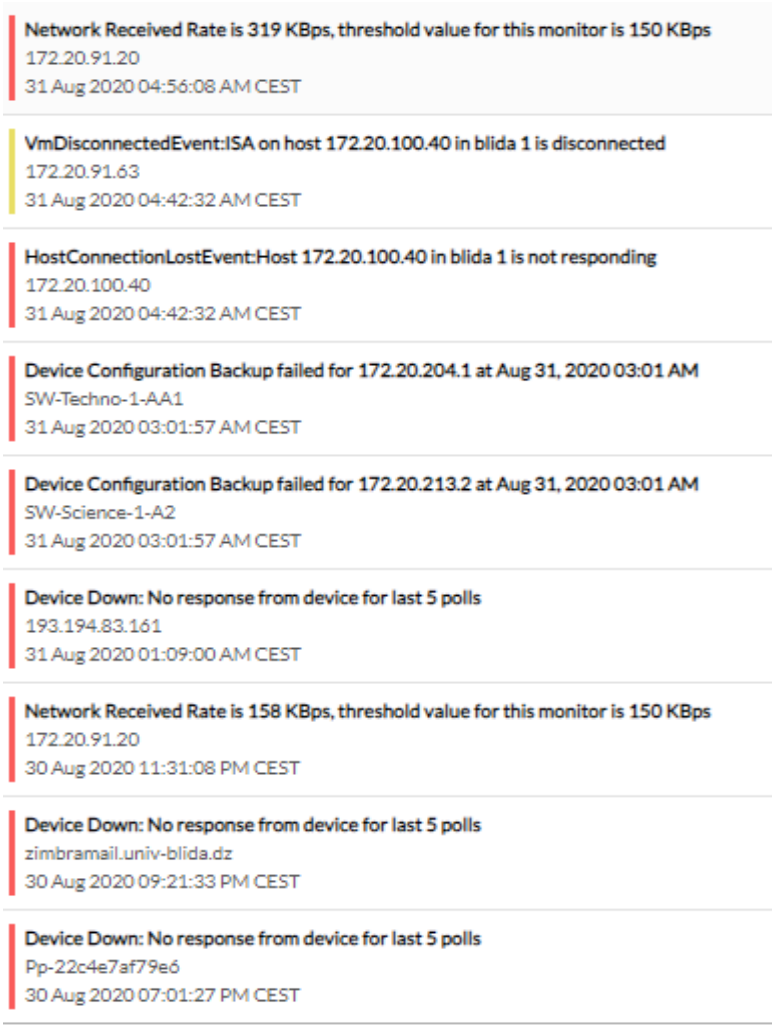


Figure 4.38 : Alertes Enregistrer.

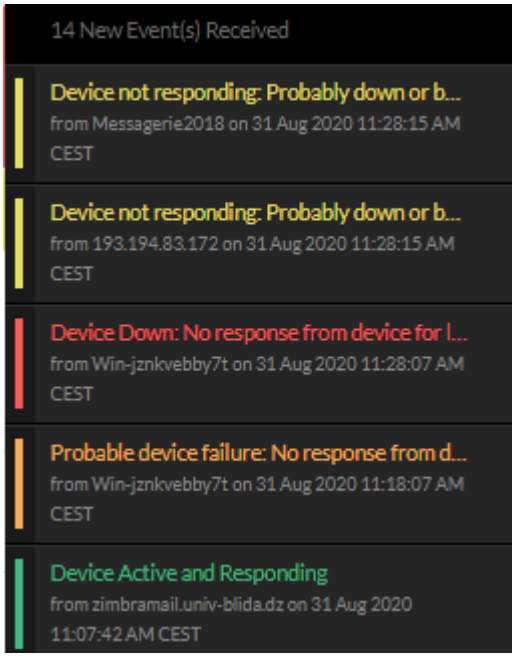


Figure 4.39 : Alertes en temps real.

Ces deux figures (4.39 et 4.40) nous montrent les différents type d'alertes, ces alertes peuvent être une quantité dépasse de la bonde passe utiliser dans un périphérique, allumé ou éteint d'un périphérique, les différents états de port (up ou down).

Figure 4.40 : Utilisation de bonde passante dans l'interface.

Cette figure nous montre l'utilisation de la bonde passante dans les interfaces (figure 112).

4.8.5.6 Maps

Une maps c'est une figure qui nous montre notre infrastructure, dans cette figure on trouve tous nos équipements relies entre eux et nous montre s'ils sont en bon fonction ou arrêt.

Pour crée une maps, on va sur :

Maps →business view → Create new .

Etape 1 : on place nos équipements comme dans la réalité.

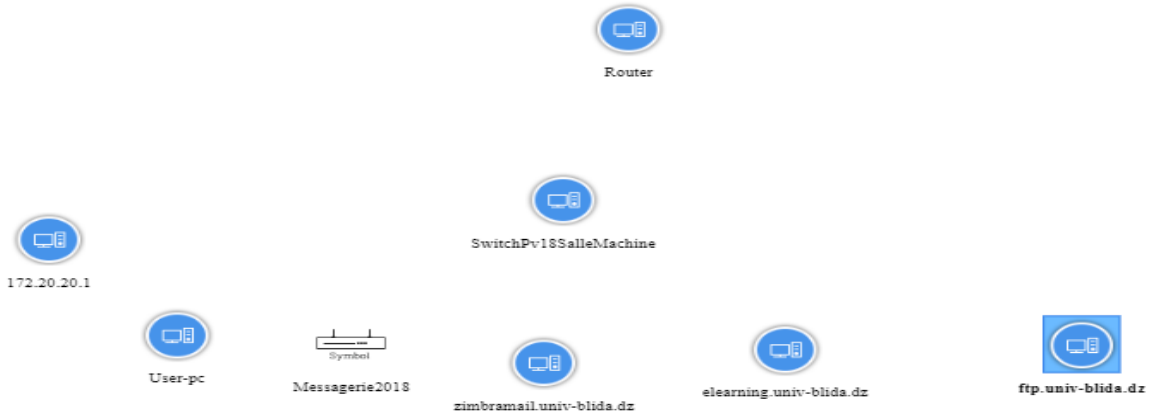


Figure 4.41 : Maps 1.

Etape 2 : change la forme du périphérique.

Chaque périphérique a une forme qui le définie.

Figure 4.42 : Maps 2.

Etape 3 : liaison entre les Périphérique.

Dans cette étape il faut faire attention aux différents interface relies entre les périphériques dans la réalité.

Exemple entre le serveur ftp et le switch par 18 :

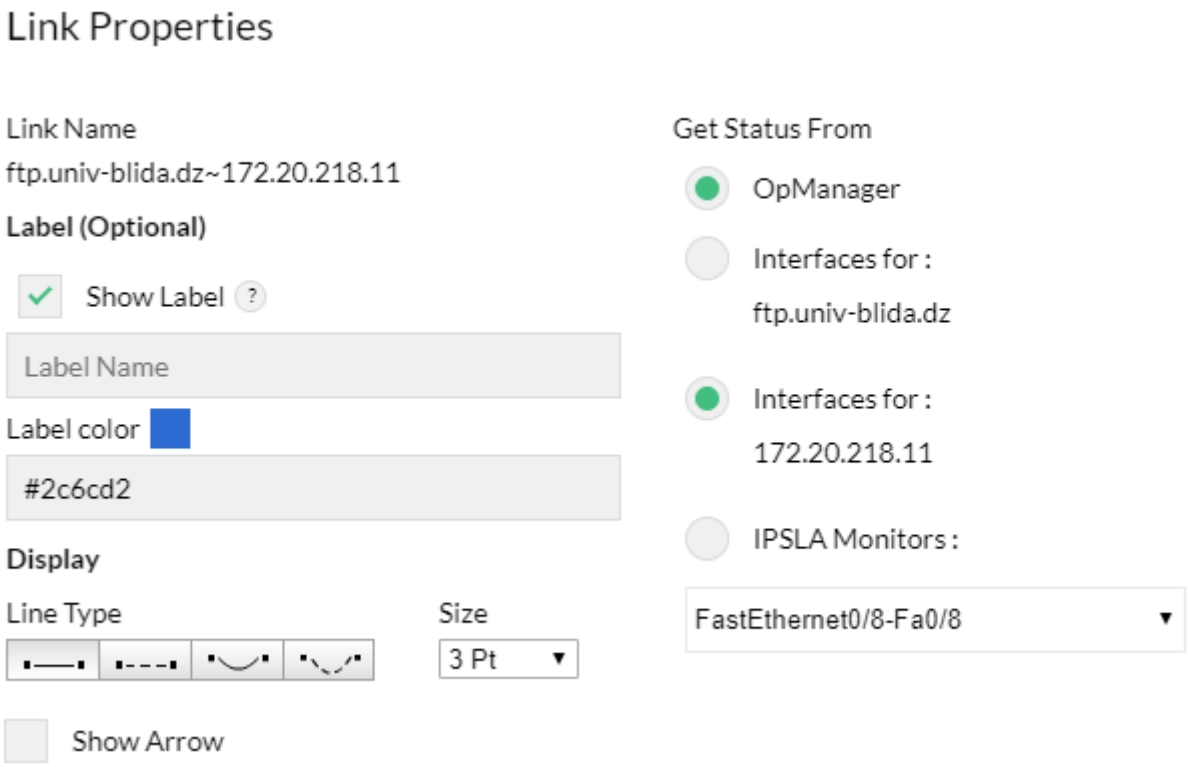


Figure 4.43 : Propriétés du lien.

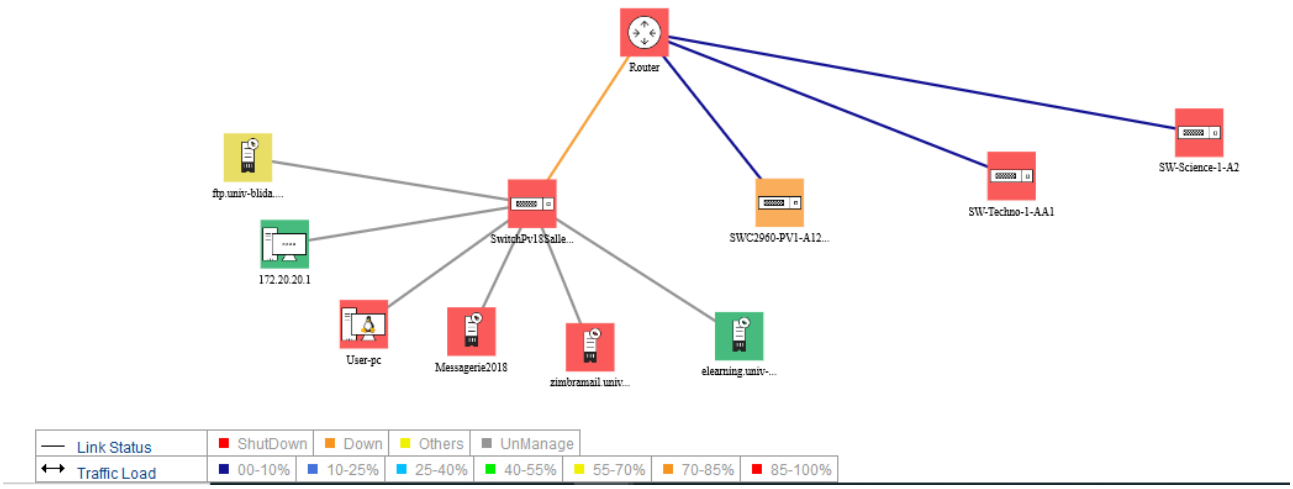


Figure 4.44 : Maps générale.

La figure 4.44 le MAP nous montre les différents périphériques ainsi que leur état, exemple le serveur messageries est éteint, serveur e-learning est up.

Les problèmes lient à l'informatique doivent être réduits au minimum, car une indisponibilité ou une baisse de QOS des systèmes d'information conduirait à des impacts très préjudiciables sur l'activité, l'économie et sur la notoriété de l'entreprise, ce qui rend les logiciels de supervision indispensable. Elle permet d'avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau et d'avoir des indicateurs sur la performance de son architecture.

L'étude que nous avons présentée dans ce mémoire concerne la supervision informatique en utilisant le logiciel OpManager sur les équipements de l'Université Saad dahleb a Blida, nous avons décrit c'est quoi vraiment une infrastructure réseau et quel équipement trouver dans une infrastructure pour pouvoir les superviser et les protocoles essentiels utiliser SNMP et WMI.

Nous avons défini le logiciel utilisé op manager on détails. Ainsi que les différentes tâches principales.

Ensuite, nous avons tester ce logiciel sur des équipements réels de l'Université Saad dahleb, et nous avons configuré op manager pour détecter des périphériques (routeur, switch, serveurs, Esx), ce qui nous a permet avoir une vue sur la structure de l'université et étudie les résultats et les rapports et les alerte.

Op manager offre un très grand nombre de rapport et d'alerte (54), et pour les étudie tous-il faut prévoir un autre projet qui doit s'approfondir dans leur étude.

Ainsi on doit étudie un certain nombre de serveur dédié tel :

- Serveurs (HTTP, Mail, FTP, LDAP, DNS, etc…).
- Applications (MS-SQL, MS-Exchange, Oracle, MySQL, Lotus Notes, etc…).
- Gestion d'imprimante.

La supervision est un moyen indispensable pour favoriser la croissance de rendement d'une entrepris.

Bibliographie

[1] http://www.indicerh.net/infrastructure-reseau-presentation-role-et-importance-en-entreprise%E2%80%89/. [En ligne].

[2] W. PUECH, *Classification des réseaux,* Centre universitaire de formation et de recherche de Nîmes , cours Mias L1, 2004.

[3] D. Lassalle, VPN et Solutions pour l'entreprise, Université de Pau et des Pays de l'Adour , Cours de C. Pham, 2002.

[4] F. Spies, *MPLS – Multi-Protocol Label Switching,* cours communication d'étiquette multiprotocole , Université de Franche-Comté – I.U.T. Belfort-Montbéliard , 1er novembre 2007..

[5] B. Jaumard, Les équipement d'interconnexion, cours IFT3320/IFT6320 téléinformatique , université de montreal, 2003.

[6] https://web.maths.unsw.edu.au/~lafaye/CCM/lan/concentrateurs.htm.

[7] https://web.maths.unsw.edu.au/~lafaye/CCM/lan/commutateurs.htm.

[8] Millysu, «Centre de Donées et Cloud,» Centre de Donées et Cloud , 2018 . [En ligne]. Available: http://millysu.e-monsite.com/blog/centre-de-donees-et-cloud/.

[9] https://web.maths.unsw.edu.au/~lafaye/CCM/lan/routeurs.htm.

[10] Djenna, *composants et fonctionnement et Configuration d'un routeur,* cours NEtwork L2 , Cisco #93930, 2015.

[11] R. Jayaprakash, *RIP, OSPF, EIGRP ROUTING PROTOCOLS,* INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS, 2015.

[12] C. CALECA, «Le protocole SNMP,» 2003. [En ligne]. Available: https://csricted.univ-setif.dz/Documents/cours-informatique/SNMP.pdf.

[13] L. Nadir, *Administration Réseaux informatique,* Mémoire de fin d'études pour l'obtention du diplôme Master Informatique ,Université Abou Bakr Belkaid– Tlemcen, 2013.

[14] http://flaubert-lyc.spip.ac-rouen.fr/IMG/pdf/Les_serveurs.pdf. [En ligne]. Available: http://flaubert-lyc.spip.ac-rouen.fr/IMG/pdf/Les_serveurs.pdf.

[15] Dvlin, «IDE,SATA,SSD : Les différents type de disque dur,» 2012. [En ligne]. Available: https://dvalin.info/2012/06/ide-sata-ssd-les-differents-disques-durs/.

[16] G. burel, *Les serveurs UE 103b,* cours Master IST-IE , Nancy université, 2008.

[17] C. CALECA, «le protocole DHCP,» 2005. [En ligne]. Available: www.coursehero.com.

[18] O. Losson, *Introduction aux Systèmes de Gestion de Bases de Données Relationnelles,* Bases de Données Relationnelles , Université de Lille – Sciences et Technologies.

[19] P. Poulin, *Système d'exploitation: Principe IFT6800 – E 2008,* slideplyaer.fr, 2016.

[20] M. MESTRALLET, *VIRTUALISATION (Concepts et Techniques de la Virtualisation),* Cours magistral , iPI / Groupe IGS, 2009.

[21] Abdoul, *Présentation de la virtualisation,,* évenement track SS-F : service internets évolutifs , tunisia, 24 may to 5 june 2015.

[22] D. ZERTAL, *cours sur le Cloud et la virtualisation,* université Larbi ben m'hidi- Oum el bouagh, 2019.

[23] Jean-Patrick, *introduction a la virtualisation,cours M2 TI+DS,,* université claude bernard-lyon 1.

[24] https://www.memoireonline.com/04/12/5604/m_Monitoring-dune-infrastructure-informatique-sur-base-doutils-libres14.html. [En ligne]. Available: https://www.memoireonline.com/04/12/5604/m_Monitoring-dune-infrastructure-informatique-sur-base-doutils-libres14.html.

[25] P. IRSAPOULLE, «Mise en place d'un outil de supervision et de contrôle distant,» Rapport de Stage de Master M2 , Université de la Réunion, 2014.

[26] S. Roulière, *Supervision Informatique,* Université catholique de l'Ouest..

[27] https://web.maths.unsw.edu.au/~lafaye/CCM/internet/snmp.htm. [En ligne]. Available: https://web.maths.unsw.edu.au/~lafaye/CCM/internet/snmp.htm.

[28] M. BELKHOUCHE, *Etude et Administration des Systèmesde Supervision dans un RéseauLocal,* Mémoire pour l'Obtention du Diplôme , Université Abou BakrBelkaid–Tlemcen, 2011.

[29] https://ram-0000.developpez.com/tutoriels/reseau/SNMP/. [En ligne]. Available: https://ram-0000.developpez.com/tutoriels/reseau/SNMP/.

[30] M. Graeber, «Abusing Windows Management Instrumentation (WMI) to Build a Persistent, Asyncronous and FilelessBackdoo,» 2015. [En ligne]. Available: www.blackhat.com.

[31] G. Leroy, «Gestion du déploiement d'une solution de supervision réseau multi-sites,» 2017. [En ligne]. Available: https://dumas.ccsd.cnrs.fr.

[32] https://fr.wikipedia.org/wiki/Supervision_(informatique). [En ligne]. Available: https://fr.wikipedia.org/wiki/Supervision_(informatique).

[33] https://www.orsenna.fr/logiciels/solarwinds/. [En ligne]. Available: https://www.orsenna.fr/logiciels/solarwinds/.

[34] https://www.paessler.com/prtg?gclid=Cj0KCQjwhb36BRCfARIsAKcXh6H4C4id1Vi-W0T5JXxUxpQqJ-21911uY7bZkp_T8AMcOTuFUjIquAEaAqqIEALw_wcB. [En ligne].

[35] https://www.manageengine.com/fr/network-monitoring/. [En ligne].

[36] D. produits, *guides d'installation,* livres blancs | OpManager.

[37] Editions, «ManageEngine OpManager Standard / Professional & Enterprise,» [En ligne]. Available: https://www.manageengine.com/network-monitoring/opmanager-editions.html?btmMenu.

[38] OpManager, *Real-Time Network Monitoring Tools | ManageEngine.*

[39] https://www.manageengine.com/network-monitoring/network-performance-monitoring.html. [En ligne]. Available: https://www.manageengine.com/network-monitoring/network-performance-monitoring.html.

[40] https://www.manageengine.com/network-monitoring/hardware-monitoring.html. [En ligne].

[41] https://www.manageengine.com/network-monitoring/router-monitoring.html. [En ligne].

[42] I. O. Management, *(ITOM) - ManageEngine OpManager.*

[43] https://www.manageengine.com/network-monitoring/features.html, «manageEngine opmanager,» manageEngine. [En ligne].

[44] https://www.manageengine.fr/produits/network-monitoring/caracteristiques.html. [En ligne].