Supervision de réseau et remontée d'alertes par push-mail

Julien Soulas

▶ **To cite this version:**

Julien Soulas. Supervision de réseau et remontée d'alertes par push-mail. Réseaux et télécommunications [cs.NI]. 2011. dumas-00581719

HAL Id: dumas-00581719

https://dumas.ccsd.cnrs.fr/dumas-00581719

Submitted on 31 Mar 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE DE NANTES

_____

MEMOIRE

Présenté en vue d'obtenir

le DIPLOME d'INGENIEUR CNAM

SPECIALITE : INFORMATIQUE

OPTION : RESEAUX, SYSTEMES ET MULTIMEDIA

par

SOULAS Julien

_____

SUPERVISION DE RESEAU ET REMONTEE D'ALERTES PAR PUSH-MAIL

Soutenu le 18 février 2011

_____

JURY

PRESIDENT : Mme METAIS

MEMBRES : M. BRIAND

M. GERARDIN

Remerciements

Je souhaite remercier tout particulièrement la Direction de la Clinique Saint-Augustin pour m'avoir donné l'opportunité de réaliser le projet présenté dans mon mémoire d'Ingénieur au sein de l'établissement.

Je tiens également à remercier Monsieur Alain Chevalier et Monsieur Erwan Lemaître pour leurs précieux conseils ainsi que pour m'avoir encadré tout au long de mon mémoire.

Je remercie Monsieur Alain Gérardin pour ses conseils avisés.

Enfin, je remercie ma famille et mes proches pour leur soutien.

Liste des abréviations

ALP : Address Lookup Protocol

ASN.1 : Abstract Syntax Notation One

BER : Basic Encoding Rules

BES : BlackBerry Enterprise Server

BESX : BlackBerry Enterprise Server Express

CICAL : Compressed Internet Calendar

CIM : Common Information Model

CIMOM : CIM Object Manager

CMIME : Compressed Multipurpose Internet Mail Extension

CMIP : Common Management Information Protocol

CMOT : CMIP over TCP/IP

COM : Component Object Model

DES : Data Encryption Standard

DFTP : Device File Transfert Protocol

DNS : Domain Name System

EGP : Exterior Gateway Protocol

FTP : File Transfer Protocol

GME : Gateway Message Envelope

GSM : Global System for Mobile Communications

HMAC : Hash-based Message Authentication Code

HTTP : Hypertext Transfer Protocol

HTTPS : Hypertext Transfer Protocol Secure

ICMP : Internet Control Message Protocol

IETF : Internet Engineering Task Force

IIS : Internet Information Services

iOS : iPhone Operating System

IP : Internet Protocol

IPPP : Internet Protocol Proxy Protocol

IPv4 : Internet Protocol version 4

IPv6 : Internet Protocol version 6

ISO : International Organization for Standardization

KB : Knowledge Base

MD5 : Message Digest 5

MIB : Management Information Base

MPLS : MultiProtocol Label Switching

NMS : Network Management Station

OEM : Original Equipment Manufacturer

OID : Object IDentifier

OS : Operating System

OSI : Open System Interconnection

OTAFM : Over The Air Folder Management

OTAKEYGEN : Over The Air KEY GENeration

PC-1 : Permuted Choice 1

PC-2 : Permuted Choice 2

PDU : Protocol Data Unit

PIN : Personal Identification Number

PMSI : Programme de Médicalisation des Systèmes d'Information

POP3 : Post Office Protocol Version 3

RFC : Request For Comments

RIM : Research In Motion

RMON : Remote Network MONitoring

SAN : Storage Area Network

SCOM : System Center Operations Manager

SCVMM : System Center Virtual Machine Manager

SHA-1 : Secure Hash Algorithm 1

SMI : Structure of Management Information

SMTP : Simple Mail Transfer Protocol

SNMP : Simple Network Management Protocol

SP2 : Service Pack 2

SQL : Structured Query Language

SRP : Server Routing Protocol

SSL : Secure Sockets Layer

SYNC : Synchronization

TCP : Transmission Control Protocol

TFTP : Trivial File Transfer Protocol

UDP : User Datagram Protocol

USM : User-based Security Model

UTC : Universal Time Coordinates

VACM : View-based Access Control Model

VPN : Virtual Private Network

WBEM : Web-Based Enterprise Management

WMI : Windows Management Instrumentation

XOR : eXclusive OR (OU exclusif)

Glossaire

Adresse mac : Adresse physique d'une interface réseau fixée par le constructeur qui permet d'identifier de façon unique une machine sur un réseau local.

Agent : Elément logiciel embarqué dans un élément actif du réseau permettant sa gestion par une station de supervision.

Alerte : Signal qui prévient d'un incident.

ASN.1 : Standard international spécifiant une notation destinée à décrire des structures de données.

Authentification : Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.

Autorité de certification : Organisme reconnu dont le rôle est de délivrer et de gérer des certificats numériques.

Certificat : Document électronique délivré par une autorité de certification, qui garantit l'authenticité des clés publiques contenues dans un annuaire.

Console : Périphérique qui permet la communication à distance avec un ordinateur central par une ligne de transmission de données, comprenant généralement un clavier, un écran et un circuit de contrôle, parfois combinés en une seule unité.

Couche : Module qui regroupe des services et des fonctions propres à une classe particulière d'événements et qui traite ceux-ci, en interaction avec d'autres modules disposés dans une structure de traitement hiérarchisée.

Datagramme : Paquet de données circulant dans un réseau TCP/IP.

Evénement : Signal qui permet, par ses différents états, d'indiquer la situation ou l'évolution d'une partie d'un système.

Firmware : Microcode logiciel permettant de piloter le matériel associé.

Hachage : Opération qui consiste à appliquer une fonction mathématique permettant de créer l'empreinte numérique d'un message, en transformant un message de taille variable en un code de taille fixe, en vue de son authentification ou de son stockage.

Horodatage : Marquage avec date et heure, de tout élément protocolaire pour une gestion a posteriori.

Hôte : Ordinateur qui, dans un réseau, fournit divers services aux utilisateurs et gère les commandes d'accès au réseau.

IETF : Groupe informel et autonome, engagé dans le développement des spécifications pour les nouveaux standards d'Internet, et composé de personnes qui contribuent au développement technique et à l'évolution d'Internet et de ses technologies.

Interface : Ensemble de moyens permettant la connexion et l'interrelation entre le matériel, le logiciel et l'utilisateur.

Interopérabilité : Capacité que possèdent des systèmes informatiques hétérogènes à fonctionner conjointement, grâce à l'utilisation de langages et de protocoles communs, et à donner accès à leurs ressources de façon réciproque.

IP : Protocole de télécommunications utilisé sur les réseaux qui servent de support à Internet, qui permet de découper l'information à transmettre en paquets, d'adresser les différents paquets, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée.

Manager : Station de gestion de réseau.

Métadonnée : Donnée qui renseigne sur la nature de certaines autres données et qui permet ainsi leur utilisation pertinente.

Modèle OSI : Cadre de référence pour l'organisation des réseaux locaux, qui décompose la gestion du transfert des données en sept couches superposées réalisant une interface entre l'application locale et le matériel utilisé pour la transmission des données.

Nœud : Dans un réseau, tout point constituant un carrefour d'où les informations sont acheminées.

Notification : Emission d’un message d’information vers un utilisateur ou vers un système.

Open source : Logiciel distribué avec l'intégralité de ses programmes-sources, afin que l'ensemble des utilisateurs qui l'emploient, puissent l'enrichir et le redistribuer à leur tour.

Ordre lexicographique : Ordre que l'on définit sur les suites finies d'éléments d'un ensemble ordonné.

Paquet : Ensemble de bits et d'éléments numériques de service constituant un message ou une partie de message, organisé selon une disposition déterminée par le procédé de transmission et acheminé comme un tout.

PDU : Paquet de données élémentaires échangé entre deux ordinateurs au moyen des protocoles appropriés, et ce, au niveau d'une seule des couches du modèle OSI.

Ping : Commande issue du monde Unix qui permet de mesurer le temps de réponse d'une machine à une autre sur un réseau.

Port : Dans une architecture client-serveur, connexion virtuelle permettant d'acheminer les informations directement dans le logiciel d'application approprié de l'ordinateur distant.

Protocole : Ensemble des spécifications décrivant les conventions et les règles à suivre dans un échange de données.

Push-mail : Service de messagerie instantanée dans lequel des copies des courriels destinés à un usager sont créées et envoyées immédiatement vers son terminal mobile, au fur et à mesure qu'ils arrivent au serveur désigné pour les distribuer, sans attendre qu'une demande de livraison soit émise par l'appareil sans fil.

Requête : Ensemble de commandes dont l'exécution permet d'obtenir un résultat.

RFC : Publication de référence portant sur le réseau Internet et rédigée par les experts du réseau.

Routage : Détermination par des routeurs du chemin que doit emprunter une information sur un réseau afin de parvenir à sa destination dans les meilleures conditions possibles.

Supervision : Surveillance de l’état d’un réseau et de ses composants.

Trame : Ensemble de bits consécutifs formant un bloc à l'intérieur duquel se trouvent des zones pour la transmission des données de l'utilisateur et des informations de service.

Sommaire

Introduction

Les entreprises utilisent de façon croissante les systèmes d'information. Dans la gestion de ces systèmes, elles sont exposées à des pannes, à des baisses de performance et à d'autres problèmes opérationnels. Pour mieux gérer ces problèmes, de nombreuses entreprises mettent en place une solution de supervision de réseau, afin de surveiller le bon fonctionnement du système informatique devenu moyen d'accès essentiel à toutes les données de l'entreprise. La plateforme de supervision est incontestablement le point névralgique du réseau. Elle facilite la gestion des infrastructures afin d'optimiser son utilisation, d'offrir une meilleur qualité de service aux utilisateurs et de réduire les coûts grâce à une meilleure estimation des besoins et un contrôle de l'allocation des ressources associées.

Les systèmes d'information étant composés d'une très grande variété d'équipements, il est très important de définir le périmètre de ceux à superviser. La définition de ce périmètre doit couvrir l'ensemble des équipements névralgiques, dépendant du type de métier de l'entreprise afin de prioriser certains équipements pour obtenir une meilleure vision globale de l'état système. Il faut considérer de manière abstraite chaque équipement comme étant un objet managé. Il est également important de bien choisir les événements de chaque équipement à superviser correspondant aux besoins du service ou du métier. Certains événements restent incontournables quel que soit l'équipement. C'est le cas de l'analyse des performances qui permet de détecter un dysfonctionnement lié au matériel ou à un logiciel ainsi que des insuffisances de ressources entrainant une dégradation des performances.

Ce rapport présentera les technologies de supervision et de gestion de réseau, puis exposera les choix effectuées dans la mise en place de la plateforme de supervision.

1 Contexte du projet

L'Association Hospitalière de l'Ouest (AHO) est une structure qui regroupe deux cliniques : la clinique Saint-Augustin, spécialisée en chirurgie, et la clinique Jeanne d'Arc, spécialisée en chirurgie de la main. L'AHO emploie entre 400 et 450 personnes.

Le service informatique qui gère les deux cliniques est composé de trois personnes, un Responsable des Systèmes d'Informations, un Responsable Informatique (moi-même) et un Technicien Informatique. Le service s'occupe de la gestion informatique, ainsi que de la maintenance des outils de communication (mails, téléphones, fax, GSM (Global System for Mobile Communications)) et des systèmes d'impressions (imprimantes, photocopieurs et duplicopieurs).

Le système informatique est centralisé sur un site, celui de la clinique Saint-Augustin. Il comprend vingt serveurs et des logiciels métiers spécifiques. Le parc informatique comprend un peu moins de deux cent postes, aussi bien des PC, des clients légers que des portables.

Depuis 2006, l'AHO, voulant sécuriser, organiser et fiabiliser les données médicales pour favoriser la communication entre les membres du personnel soignant et les praticiens, a décidé de mettre en place une solution complètement informatisée du dossier patient. Ce logiciel intitulé « Emed », permet de gérer le dossier médical, les prescriptions et le dossier de soins répondant aux normes du dossier médical personnel initié au plan national.

Figure 1 : Présentation du logiciel Emed

Début 2009, la clinique Saint-Augustin a informatisé le premier service. Fin 2009, un deuxième service à son tour a été informatisé. Les cinq autres services ont été informatisés en 2010. Au regard de la criticité de l'application, la mise en place d'une plateforme de supervision est indispensable. La remontée d'alerte par push-mail va permettre une meilleure réactivité du service informatique en diminuant le temps de coupure ou en anticipant certains problèmes.

Le logiciel Emed est arrivé en complément du logiciel de gestion hospitalière, intitulé Sigems. Celui-ci est actuellement utilisé pour la gestion administrative, le traitement de la facturation et de la codification des actes (PMSI : Programme de Médicalisation des Systèmes d'Information), la gestion comptable, la gestion des lits et la gestion du bloc opératoire.

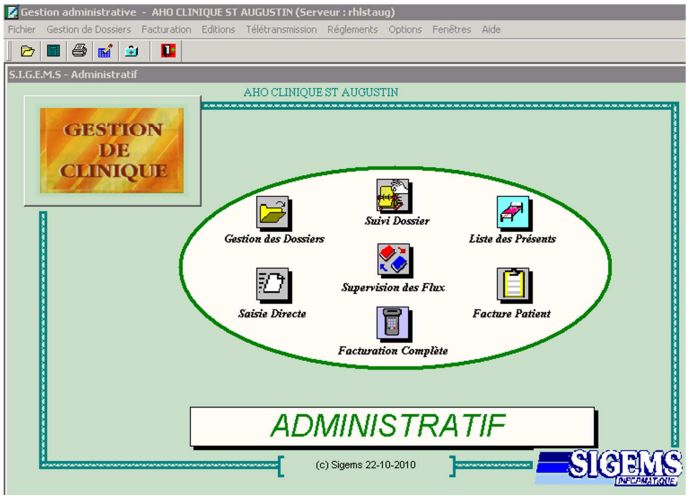


Figure 2 : Présentation du logiciel Sigems

Avant même l'arrivée du patient à la clinique, des informations concernant son hospitalisation sont entrées dans le logiciel Sigems. Pendant le séjour du patient à la clinique, de nouvelles informations sont saisies, dans Sigems comme dans Emed, jusqu'à sa sortie et même après sa sortie. Tout au long de son séjour, le personnel de santé doit avoir accès au dossier médical du patient à tout moment.

L'informatisation de ce dossier permet de le rendre accessible plus facilement à tous, y compris depuis le domicile ou le cabinet des praticiens, mais en cas d'incident informatique, son inaccessibilité peut engendrer des conséquences graves pour le patient.

En ce qui concerne le logiciel de gestion administrative, son arrêt perturbe les entrées et les sorties des patients, mais surtout empêche les praticiens de coder les actes médicaux qu'ils ont

effectués sur un patient, engendrant un problème de facturation des actes, et bloquant ainsi les flux financiers.

Pour limiter ces types de risques, il a fallu mettre en place un système permettant d'alerter le service informatique dès qu'un incident survient sur le réseau, afin d'éviter des pannes ou de limiter le temps d'indisponibilité.

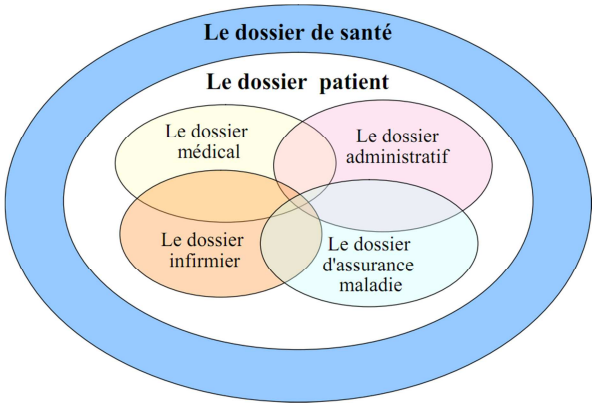


Figure 3 : Présentation du dossier patient (DEGOULET, 2005)

Ce schéma reprend la totalité des informations que doit traiter un établissement hospitalier pour chaque patient. Dans le cas de la clinique Saint-Augustin, le dossier administratif et le dossier d'assurance maladie sont gérés par le logiciel Sigems, tandis que le dossier médical et le dossier infirmier relèvent du dossier patient informatisé et sont gérés par Emed.

1.1 Environnement Technique

L'architecture informatique de l'AHO comprend 20 serveurs et 25 équipements réseaux. Les serveurs sont reliés à un réseau de stockage SAN (Storage Area Network) et répartis dans 2 salles informatiques sur le site de la clinique Saint-Augustin et 1 salle informatique sur le site de la clinique Jeanne d'Arc.

Les 2 salles de la clinique Saint-Augustin sont reliées à 7 baies informatiques réparties dans 3 bâtiments. La clinique Jeanne d'Arc ne comprend qu'une seule salle informatique hébergeant un serveur et reliée à une baie informatique. Tous les logiciels sont installés sur les serveurs de la clinique Saint-Augustin et sont accessibles grâce à une liaison sécurisée, gérée par Gigalis, entre les deux cliniques. Le serveur situé sur le site de Jeanne d'Arc ne sert que pour authentifier les utilisateurs et leur donner accès à leurs documents plus rapidement.

Le dossier patient informatisé est pour l'instant déployé uniquement sur le site de Saint-Augustin. Emed est réparti sur 4 serveurs (un serveur Web et un serveur de bases de données dans chaque salle informatique). Le logiciel du dossier patient est accessible grâce au réseau filaire de l'entreprise mais également grâce à l'infrastructure Wi-Fi. Ainsi, des chariots mobiles équipés d'ordinateurs portables peuvent être déplacés jusqu'au lit du patient afin d'avoir accès en permanence aux informations du dossier patient informatisé. Une liaison sécurisée a également été mise en place pour que les praticiens puissent y avoir accès en dehors de la clinique.

En revanche, le logiciel de gestion hospitalière Sigems est déployé dans les deux cliniques. Il est réparti sur 3 serveurs (un serveur TSE (Terminal Server) et un serveur de bases de données dans la première salle informatique et un deuxième serveur TSE dans la deuxième salle informatique).

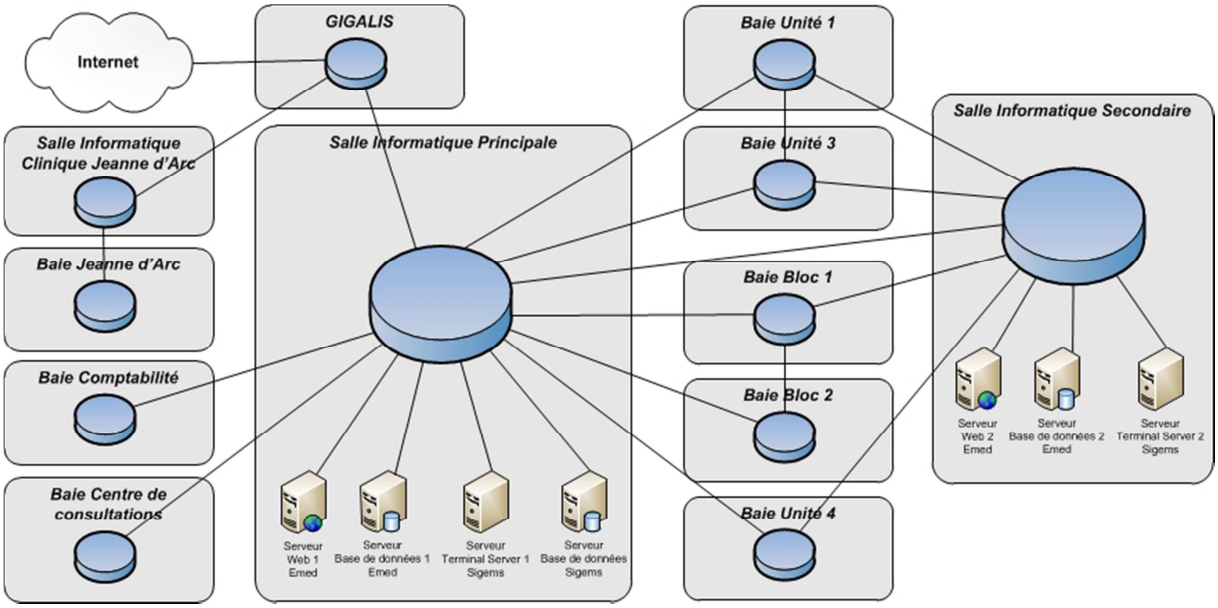


Figure 4 : Schéma simplifié de l'architecture informatique de la clinique Saint-Augustin

Cet été, la clinique a fait l'acquisition de trois serveurs supplémentaires afin de mettre en place une infrastructure de virtualisation avec VMware. Ceci permet d'augmenter la disponibilité des serveurs en rendant possible un déplacement à chaud des serveurs d'une salle à l'autre. Le dossier patient informatisé ne fait pour l'instant pas partie de cette infrastructure de virtualisation mais son intégration est envisagée à moyen terme.

1.2 Objectifs

L'objectif est de superviser l'infrastructure informatique des deux cliniques, comprenant les unités de soins, les blocs opératoires, les services administratifs et les cabinets médicaux, afin d'être avertis lorsqu'un équipement réseau, un serveur ou même un service précis d'un serveur ne fonctionne plus. Cela permet de réagir plus vite pour rétablir son fonctionnement. Dans certains cas, une alerte doit également être envoyée lorsqu'un seuil défini comme critique est atteint.

Toutes les alertes seront visibles à travers le logiciel de supervision de réseau sur un moniteur dédié à cela dans le bureau du service informatique. Les remontées d'alertes se feront par mail. Les téléphones GSM étant synchronisés en push-mail recevront instantanément les alertes.

1.3 Cahier des charges

La direction de l'AHO nous a imposé une série de contraintes. Tout d'abord, la plateforme matérielle choisie doit s'appuyer sur le réseau de stockage SAN existant.

Ensuite, le logiciel de supervision doit être installé sur une plateforme Microsoft Windows et doit avoir une interface de préférence en français. Ce logiciel pourra être payant sans toutefois dépasser un budget de 1 000 €. Il est souhaitable que le logiciel puisse être installé sur une machine virtuelle afin d'être intégré à la nouvelle infrastructure de virtualisation.

Il faut également choisir une technologie GSM simple d'utilisation car la technologie push-mail sera également utilisée dans d'autres contextes par des responsables non spécialistes en informatique.

La solution de supervision de réseau doit être interfaçable avec le logiciel de messagerie de l'entreprise Microsoft Exchange Server 2003.

Enfin, la direction souhaite que la mise en place de la solution soit terminé en septembre 2010 afin d'être opérationnelle rapidement.

2 La supervision de réseau

2.1 La gestion de réseau avec SNMP

2.1.1 Historique du protocole SNMP

Pour répondre aux difficultés de surveillance et de maintien des réseaux informatiques, un protocole d'administration, intitulé SNMPv1 (Simple Network Management Protocol) a été finalisé en 1990. Ce protocole permet de modifier la configuration des équipements, de détecter et d'analyser les problèmes du réseau par interrogation ou remontée d'alarmes, de surveiller ses performances et de réaliser des statistiques.

Dans cette première version, le protocole est défini par un standard IETF (Internet Engineering Task Force) intitulé RFC (Request For Comments) 1157 « A Simple Network Management Protocol (SNMP) » datant de mai 1990. Le but de cette architecture est de faciliter son utilisation, d'être suffisamment extensible pour être compatible dans le futur et qu'elle soit indépendante de l'architecture et des mécanismes des hôtes ou serveurs particuliers. (IETF, 1990)

La sécurité de SNMPv1 est basée sur des noms de communautés qui sont utilisés comme des mots de passe pour accéder à une arborescence de données de l'équipement appelée MIB (Management Information Base). Le nom de la communauté est transmis en clair dans le message SNMP.

La première version n'étant pas sécurisée, le protocole SNMP a ainsi évolué en une deuxième version finalisée en janvier 1996, intitulée SNMPv2C (RFC 1901 à 1908). La sécurité de cette version est encore faible car elle s'appuie sur le modèle de SNMPv1 en réutilisant les noms de communauté, d'où la lettre C de SNMPv2C. Cependant, elle comble des lacunes de la version 1, en particulier au niveau de la définition des objets, du traitement des notifications et du protocole lui-même.

Une troisième version finale, intitulé SNMPv3, a été approuvée comme projet de norme en avril 1999. Elle est devenue un standard en décembre 2002 (RFC 3410 à 3418). Elle a pour but principal d'assurer la sécurité des échanges.

2.1.2 L'architecture SNMP

La technologie SNMP s'appuie sur le modèle OSI (Open System Interconnection). Ce modèle de communication mis en place par l'Organisation internationale de normalisation (ISO : International Organization for Standardization) comporte 7 couches (1 = Physique, 2 = Liaison Données, 3 = Réseau, 4 = Transport, 5 = Session, 6 = Présentation et 7 = Application). Le rôle du modèle OSI, décrit dans la norme ISO 7498-1, est de standardiser la communication entre les machines.

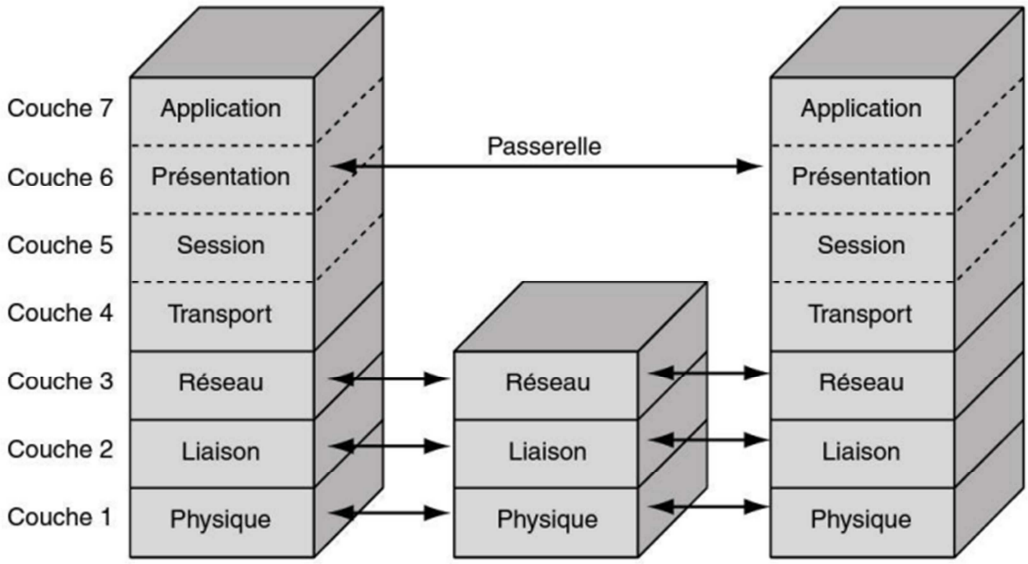


Figure 5 : Le modèle OSI (PUJOLLE, 2007)

SNMP est un protocole situé entre la couche 4 et la couche 7 de ce modèle OSI. Il s'appuie sur le protocole de télécommunication UDP (User Datagram Protocol). Le paquet UDP est encapsulé dans un paquet IP (Internet Protocol). UDP est plus simple à utiliser que TCP (Transmission Control Protocol) car il fonctionne en mode non connecté. Le mode non connecté n'oblige pas les deux entités à établir une connexion entre elles avant de transférer des données puis de mettre fin à leur connexion. En revanche, UDP ne permet pas de savoir si les datagrammes sont bien arrivés et s'ils sont arrivés dans un ordre différent de celui d'émission.

Cette architecture SNMP fonctionne sur un modèle client-serveur. Le client correspond à la station de gestion de réseau, souvent appelée Manager ou encore Network Management Station (NMS) par certains éditeurs. Les serveurs correspondent aux agents SNMP qui

enregistrent en permanence des informations les concernant dans leur MIB. La station interroge les MIB des différents agents pour récupérer les informations qu'elle souhaite.

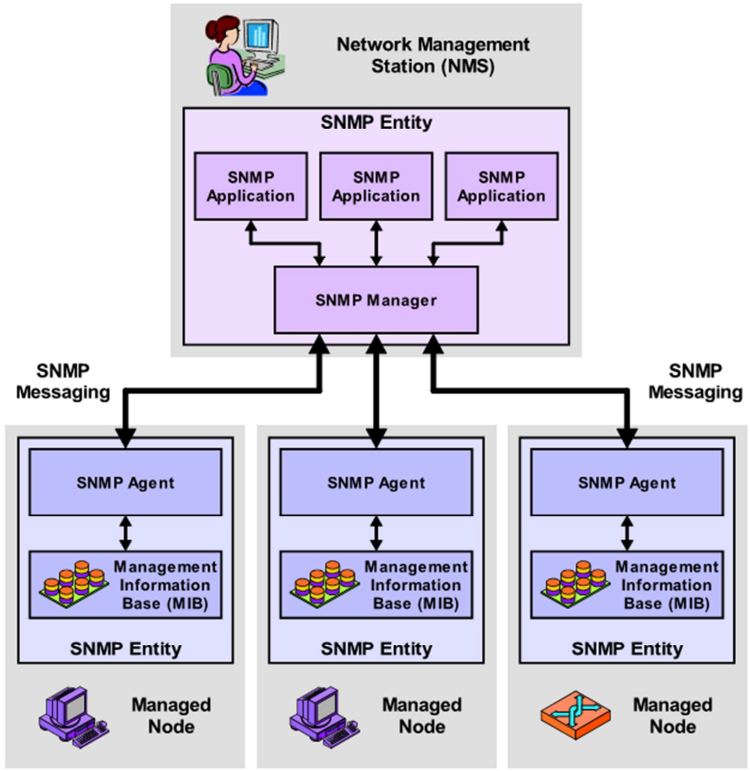


Figure 6 : Architecture SNMP (Kozierok, 2005)

2.1.2.1 SMI

Chaque équipement possède une MIB similaire. Pour ce faire, l'IETF a mis en place une première norme RFC 1155, en mai 1990, intitulé « Structure and Identification of Management Information for TCP/IP-based Internets ».

2.1.2.1.1 SMIv1

Cette norme SMIv1 a permis de définir une structure commune, de définir un système de représentation des objets de la MIB, incluant la syntaxe et les valeurs de chaque objet, et de définir une méthode d'encodage standard des valeurs des objets.

La définition des objets gérés se décompose en trois attributs :

- Nom : Le nom ou identificateur d'objet (OID : Object IDentifier), définit de manière unique un objet managé. Les noms apparaissent souvent sous deux formes : numérique et « lisible par l'homme ». Dans les deux cas, les noms sont longs et incommodes.

- Type et syntaxe : Un objet de type de données managé est défini en utilisant un sous-ensemble d'ASN.1 (Abstract Syntax Notation One). Dans le cadre de SNMP, ASN.1 est un moyen de spécifier comment les données sont représentées et transmises entre le Manager et les agents.
- Encodage : Une seule instance d'un objet managé est encodée en une chaîne d'octets en utilisant l'encodage BER (Basic Encoding Rules). Le codage BER définit la manière dont les objets sont encodés et décodés afin qu'ils puissent être transmis à la couche 4 (Transport) ou la couche 5 (Session) du modèle OSI.

Les objets gérés sont organisés en une hiérarchie arborescente. Cette structure est la base de nommage SNMP. Un OID est composé d'une série d'entiers sur la base des nœuds dans l'arbre, séparés par des points. Il existe également une représentation lisible par l'homme qui est une série de noms séparés également par des points, chacun représentant un nœud de l'arbre.

L'arborescence d'objets est constitué du nœud au sommet de l'arbre appelé racine ou Root-Node, des nœuds possédant des enfants appelés branches et des nœuds ne possédant pas d'enfant appelés feuille.

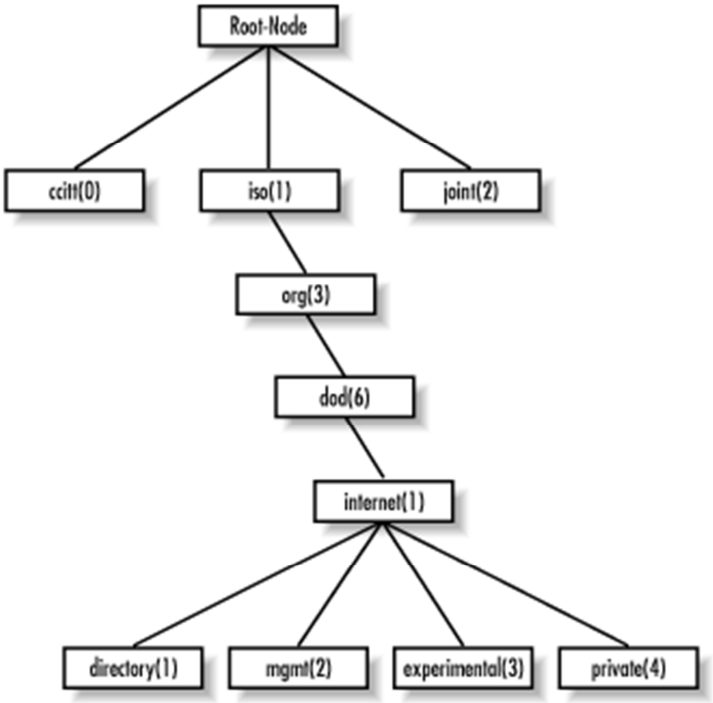


Figure 7 : Structure de l'arborescence SMIv1 (MAURO, et al., 2005)

SMIv1 définit plusieurs types de données qui sont primordiaux pour la gestion des réseaux et des périphériques réseau. Ces types de données permettent d'identifier le type d'information que l'objet peut contenir.

Tableau I : Types de données de SMIv1 (MAURO, et al., 2005)

Types de données	Description
Integer	Nombre de 32 bits souvent utilisé pour spécifier les types énumérés dans le contexte d'un objet unique géré. Par exemple, l'état de fonctionnement d'une interface d'un routeur peut être « up », « down », ou « testing ». Avec les types énumérés, 1 représenterait « up », 2 « down », et 3 « testing ». La valeur zéro (0) ne doit pas être utilisé comme un type énuméré, selon la RFC 1155.
Octet String	Chaîne de zéro octet ou plus généralement utilisée pour représenter des chaînes de texte, mais aussi parfois utilisée pour représenter des adresses physiques.
Counter	Nombre de 32 bits avec comme valeur minimale 0 et comme valeur maximale de 2^{32} - 1 (4 294 967 295). Lorsque la valeur maximale est atteinte, il repasse à zéro et recommence. Il est principalement utilisé pour le suivi des informations telles que le nombre d'octets envoyés et reçus sur une interface ou le nombre d'erreurs et les rejets vu sur une interface. Un compteur est automatiquement incrémenté et ne doit jamais diminuer au cours de son fonctionnement normal. Lorsqu'un agent est redémarré, tous les compteurs doivent être remis à zéro. Les deltas sont utilisés pour déterminer si quelque chose d'utile peut être dit suite aux requêtes successives pour obtenir la valeur du compteur. Un delta est calculé en interrogeant au moins deux fois le compteur et en prenant la différence entre les résultats de la requête sur un intervalle de temps.
Object Identifier	Chaîne décimale qui représente un objet géré au sein de l'arborescence d'objets. Par exemple, 1.3.6.1.4.1.9 représente l'OID de l'entreprise privée Cisco Systems.
Null	Non utilisé actuellement dans le protocole SNMP.
Sequence	Définit les listes qui contiennent zéro ou plusieurs autres types de données ASN.1.
Sequence Of	Définit un objet managé qui est composé d'une séquence de types ASN.1.
IpAddress	Représente une adresse IPv4 32 bits. SMIv1 et SMIv2 ne supporte pas une adresses IPv6 128 bits.
NetworkAddress	Identique au type de « IpAddress », mais peut représenter différents types d'adresses réseau.
Gauge	Nombre de 32 bits avec comme valeur minimale 0 et comme valeur maximale 2^{32} - 1 (4 294 967 295). Contrairement à « Counter », « Gauge » peut augmenter ou diminuer à volonté, mais il ne peut jamais dépasser sa valeur maximale. La vitesse de l'interface sur un routeur est mesurée ce type de données.
TimeTicks	Nombre de 32 bits avec comme valeur minimale 0 et comme valeur maximale 2^{32} - 1 (4 294 967 295). « TimeTicks » permet de compter une durée en centièmes de seconde à partir d'un temps origine.

Opaque	Permet de passer une syntaxe ASN.1 arbitraire sous forme d'un octet string.

L'objectif de tous ces types d'objet est de définir les objets gérés.

2.1.2.1.2 SMIv2

SMIv1 ne supportant que des compteurs de 32 bits, il a fallu créer une nouvelle version afin d'ajouter des nouveaux objets pour pallier aux différents problèmes. SMIv2 étend donc l'arborescence d'objets SMI en ajoutant la branche SNMPv2 à la sous-arborescence « Internet ».

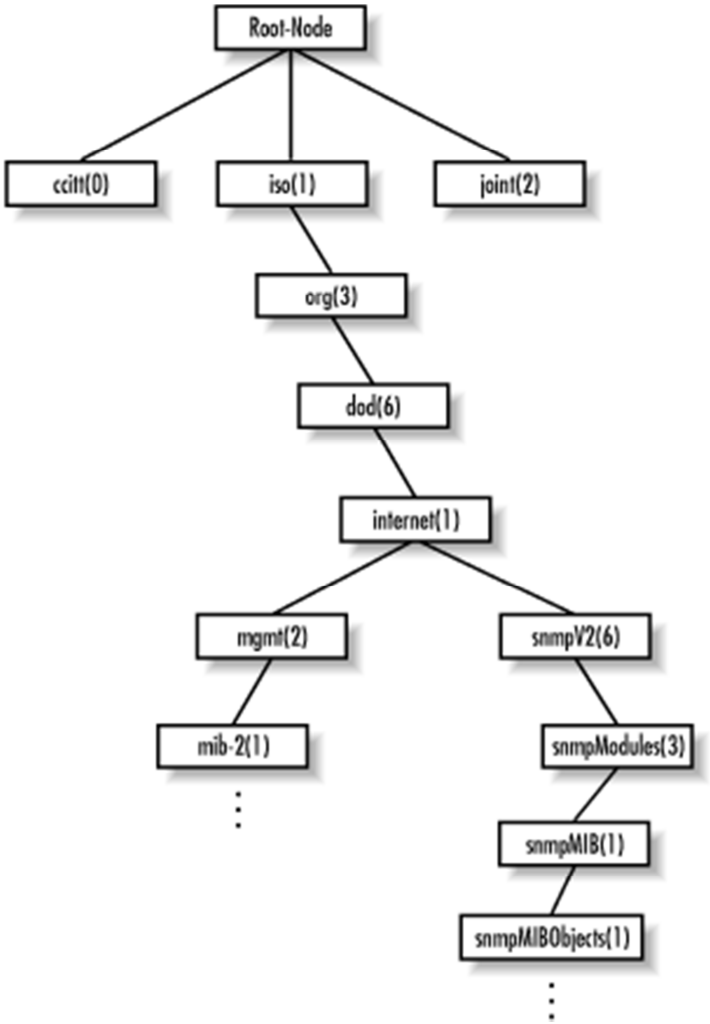


Figure 8 : Structure de l'arborescence SMIv2 pour SNMPv2 (MAURO, et al., 2005)

SMIv2 définit également quelques nouveaux types de données, qui sont résumés dans le tableau ci-dessous.

Tableau II : Nouveaux types de données pour SMIv2 (MAURO, et al., 2005)

Types de données	Description
Integer32	Identique à « Integer »
Counter32	Identique à « Counter »
Gauge32	Identique à « Gauge »
Unsigned32	Représente les valeurs décimales dans la plage de 0 à 2^{32} -1 inclus.
Counter64	Similaire à « Counter32 », mais sa valeur maximale est 18 446 744 073 709 551 615. « Counter64 » est idéal pour les situations dans lesquelles « Counter32 » peut repasser à 0 dans un court laps de temps.
Bits	Ensemble de bits nommés.

SMIv2 apporte des fonctionnalités nouvelles dans la manipulation des tables. « Augment » permet de prolonger une table existante par l'ajout de colonnes et « RowStatus », permet d'additionner ou de supprimer dynamiquement des rangées dans les tables.

2.1.2.2 La MIB

La MIB est une base d'informations de gestion. Elle comprend des informations à consulter, des paramètres à modifier, ainsi que des alarmes à émettre. La MIB est structurée sous une forme arborescente. Chaque objet de la MIB est identifié par un nom et un OID. Le chemin suivi pour aller de la racine à l'objet constitue l'OID de celui-ci. Les OIDs permettent de parcourir la MIB jusqu'à atteindre la variable souhaitée pour en lire ou modifier les attributs. Ce sont des identifiants universels permettant d'assurer l'interopérabilité entre différents logiciels indépendamment du matériel.

Les objets administrés (aussi bien les objets de type scalaire que tabulaire) sont composés d'une ou plusieurs instances d'objets, lesquelles sont essentiellement des variables. Les objets scalaires définissent une seule instance d'objets alors que les objets tabulaires définissent plusieurs instances liées d'objets, et celles-ci sont regroupées dans des tables MIB. Chaque niveau de l'arborescence est repéré par un index numérique.

2.1.2.2.1 MIB I

L'IETF a standardisé une première version intitulé RFC 1156 « Management Information Base for Network Management of TCP/IP-based internets » en mai 1990.

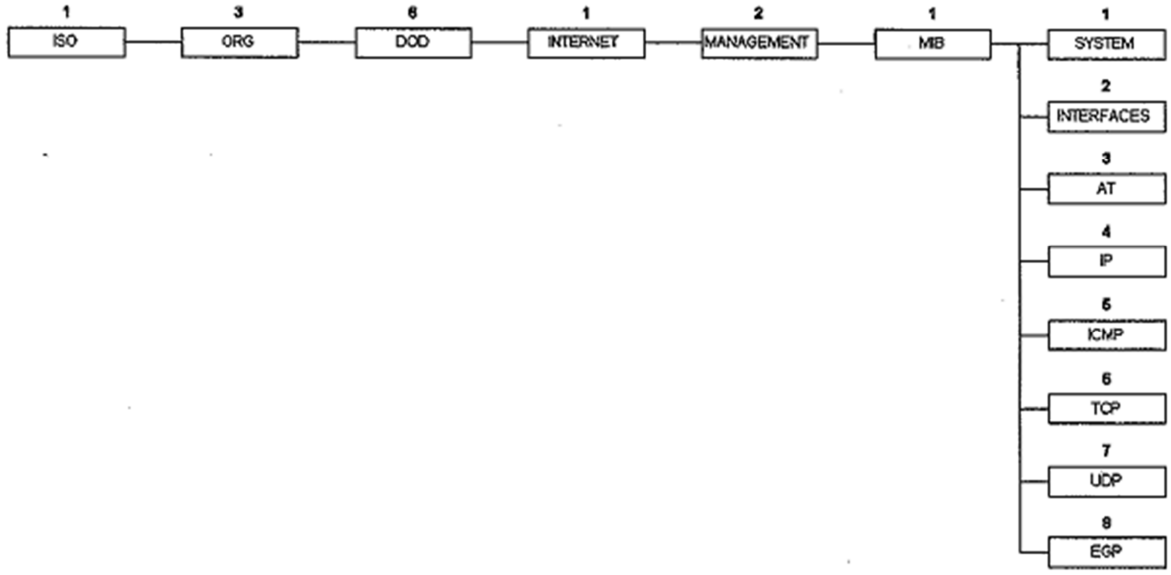


Figure 9 : Arborescence de la MIB I (PIGNET, 2008)

La MIB I se décompose en 8 groupes :

1. System : Groupe fournissant des informations d'ordre général sur le système lui-même.
2. Interfaces : Ce groupe contient toutes les informations sur les interfaces physiques ou virtuelles présentes, leur type, le fabricant, leurs caractéristiques et enfin les statistiques d'usage.
3. Address Translation : Le groupe AT est une seule table de correspondances entre les adresses physiques (adresses MAC) et les adresses logiques (adresses IP).
4. IP : Ce groupe contient toutes les informations concernant le protocole IP.
5. ICMP : Groupe contenant toutes les informations concernant le protocole ICMP (Internet Control Message Protocol).
6. TCP : Ce groupe indique les paramètres liés au protocole TCP.
7. UDP : Groupe indiquant les paramètres liés au protocole UDP.
8. EGP : Le groupe EGP (Exterior Gateway Protocol) contient les informations relatives au protocole de routage intersystèmes autonomes EGP.

2.1.2.2.2 MIB II

Très rapidement après la mise en place de la MIB I, l'IETF a standardisé une deuxième version un peu plus riche intitulée RFC 1213 « Management Information Base for Network Management of TCP/IP-based internets : MIB-II ».

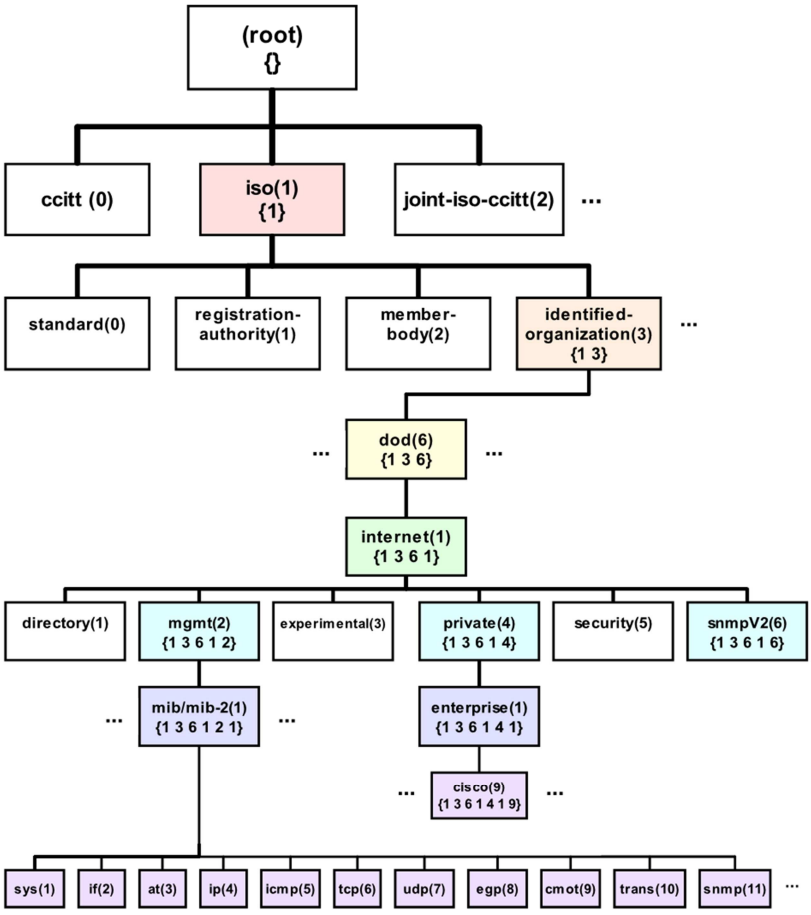


Figure 10 : Arborescence de la MIB II (Kozierok, 2005)

La MIB II a enrichi les groupes de la MIB I avec de nouvelles variables. Elle a également créé des nouveaux groupes dont ceux ci-dessous :

9. CMOT : Le groupe CMOT (CMIP over TCP/IP) est obsolète. Seul l'OID est réservé dans MIB II.
10. Transmission : Le groupe transmission regroupe d'autres modules de MIB qui concernent des médias de transmission plus spécifiques qui viennent compléter les informations contenues dans le groupe Interfaces (2).
11. SNMP : Ce groupe donne des informations sur l'implémentation et l'exécution de SNMP lui-même.

2.1.2.2.3 Les MIBs privées

Une MIB privée apporte de nouvelles variables propres à chaque équipement que la MIB I et la MIB II ne pouvaient pas apporter. La MIB privée différencie les constructeurs par un numéro unique qui est attribué par l'ISO. Ainsi, chaque constructeur possède un OID différent. Exemple : Informix possède l'OID 1.3.6.1.4.1.893 et Cisco possède l'OID 1.3.6.1.4.1.9.

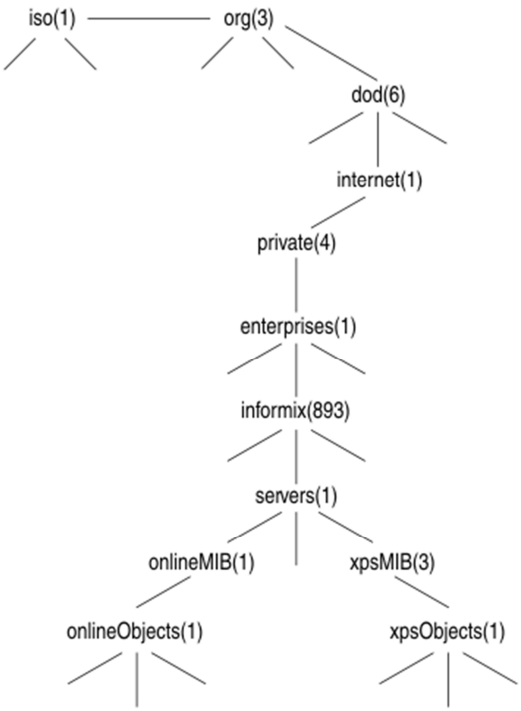


Figure 11 : Arborescence de la MIB privée Informix (IBM Corporation, 2005)

Les mécanismes SNMP de lecture et de modification de la MIB privée sont identiques à ceux des MIBs I et II.

2.1.2.2.4 RMON

La MIB RMON (Remote Network MONitoring) est un standard d'interopérabilité pour la supervision et le dépannage des réseaux locaux. Ce standard, intitulé RFC 1271 « Remote Network Monitoring Management Information Base », a été ratifié par l'IETF en novembre 1991. Implémenté de manière complète ou partielle sur des éléments actifs (hubs, switchs, routeurs…) ou sous forme d'équipements dédiés à la fonction d'analyse (Sondes RMON), RMON permet aux agents de renseigner un Manager sur le fonctionnement de ses interfaces

réseau. La MIB RMON comprend des tables permettant de collecter des statistiques liées à la couche Interface Réseau du modèle TCP/IP.

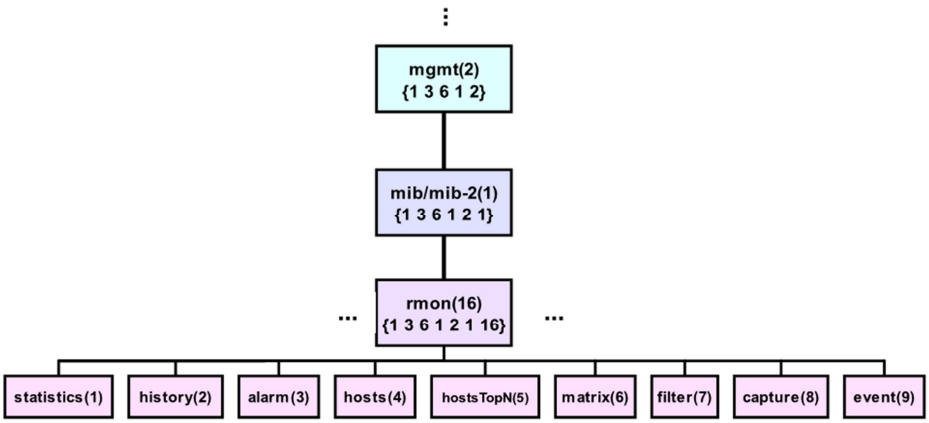


Figure 12 : Organisation de RMON dans la MIB (Kozierok, 2005)

La MIB RMON est composée de 9 groupes :

1. Statistics : Donne l'état en temps réel des segments mis sous surveillance (utilisation, erreurs, distribution du trafic par taille de paquets, broadcasts, multicasts...). Utilisé en dépannage (en temps réel) ou par les applications non évoluées pour le reporting, ou encore pour définir des seuils d'alarme sur la sonde.
2. History : Une table permet de paramétrer l'acquisition des données. Une table d'historiques met à disposition ces données pour interrogation.
3. Alarm : Une table (alarmTable) permet de mettre en place une surveillance locale sur n'importe quelle variable de la MIB enregistrée par l'agent, selon une fréquence donnée (alarmInterval), par rapport à des valeurs de seuils d'alarme montantes et descendantes (alarmFallingThreshold et alarmRisingThreshold). Les événements générés lors d'un dépassement de seuil sont identifiés par leur index dans la table des événements définis dans le groupe event (alarmRisingEventIndex et alarmFallingEventIndex).
4. Hosts : Donne les statistiques des machines du réseau vues par la sonde, avec des rapports sur une période donnée. La table hostControlTable permet de définir les rapports, tandis que les résultats sont donnés par hostTable (indexation par les adresses MAC) et hostTimeTable (indexation par date de création de la ligne).
5. HostsTopN : Fournit un rapport sur les *N* plus grands hosts, basé sur les statistiques du groupe statistics. Chaque entrée dans la table de résultats constitue un rapport.

6. Matrix : Stocke les erreurs et les statistiques d'utilisation pour les paires d'équipements qui communiquent sur le réseau (par exemple : Error, bytes, packets).
7. Filter : Moteur de filtre permettant d'isoler un flux de paquets à partir de la combinaison logique d'un filtre de données (correspondance d'un *pattern* de bits) et d'un filtre d'état (correspondance de l'état des paquets : CRC, etc.).Le résultat appliqué à une interface constitue un *channel*. Un *channel* peut être activé par un événement, et sa définition sera utilisée pour la configuration des captures de paquets, ou simplement pour le comptage des paquets ou la génération d'un événement (préalablement défini dans la table eventTable) lors de l'arrivée du premier paquet et/ou des suivants.
8. Capture : Permet la capture de paquets qui correspondent à un channel défini dans le groupe filter : BufferControlTable permet de définir le buffer de capture pour un channel, ainsi que la stratégie en cas de buffer plein ; CaptureBufferTable permet au manager SNMP de récupérer les paquets (une ligne pour chaque paquet capturé). Un système de fenêtre sur le buffer de capture permet de faire avec les contraintes du protocole SNMP (taille maximum des PDU).
9. Event : La table eventTable permet de définir des événements qui peuvent déclencher un trap SNMP et/ou l'ajout d'une entrée dans un fichier journal (« log ») conservé sur l'agent sous la forme d'une table de nom logTable.

En septembre 1993, la RFC 1513, intitulé « Token Ring Extensions to the Remote Network Monitoring MIB », ajoute un nouveau groupe spécifique au protocole Token Ring :

10. TokenRing : Ce groupe étend RMON aux réseaux Token Ring.

RMON permet de faire des analyses de niveau 2, c'est-à-dire que les tables de host et les matrices de trafic se font par rapport à des adresses MAC. Une deuxième version, intitulée RFC 2021 « Remote Network Monitoring Management Information Base Version 2 using SMIv2 », datant de janvier 1997, permet de remonter dans les couches et de faire des analyses concernant les couches 3 et supérieures. RMON2 ajoute 10 groupes de plus :

11. Protocol Directory : table des protocoles (RFC 2074) que l'agent observe et pour lesquels il maintient des statistiques.

12. Protocol Distribution : Statistiques de trafic en paquets et octets pour chaque protocole du directory.
13. Address Map : Liste des équivalences adresse MAC – adresse réseau découvertes par la sonde.
14. Network Layer Host : Statistiques de trafic de et vers chaque adresse réseau découverte par la sonde.
15. Network Layer Matrix Group : Statistiques de trafic pour les paires d'adresses réseau, avec la possibilité d'établir des matrices de trafic source-destination et destination-source, ainsi que des rapports de type « top N ».
16. Application Layer Host : Statistiques par protocole « applicatif » pour chaque adresse réseau du segment.
17. Application Layer Matrix : Statistiques de trafic par protocole pour chaque paire d'adresses réseau (source, destination) identifiée par la sonde.
18. User History : Il permet de mettre en place des historiques similaires à ceux définis dans RMON, mais sur n'importe quel objet de type INTEGER ou dérivé.
19. Probe Configuration : Définition des groupes supportés par la sonde, liste des machines destinatrices des traps SNMP, définition du fichier de boot TFTP (Trivial File Transfer Protocol).
20. rmonConformanceProvides : Information aux logiciels de gestion concernant le statut de soutien pour les groupes.

2.1.2.3 L'agent SNMP

Pour être supervisé, chaque équipement doit comporter un agent SNMP. Le but étant de remonter les informations de la MIB au Manager. L'implantation des agents n'étant pas standardisée, ils peuvent ainsi être intégrés dans les équipements sous la forme d'un firmware, dans l'OS (Operating System) ou dans un programme additionnel. L'agent nécessite des ressources en processeur et en mémoire. Il reste à l'écoute d'éventuelles requêtes sur le port UDP 161. Il répondra aux requêtes reçues uniquement si le demandeur a les droits nécessaires correspondant à sa demande. L'agent peut fournir des informations à un ou plusieurs Managers.

De plus, l'agent SNMP peut également être paramétré pour émettre des alertes concernant des points critiques de l'équipement, comme la surchauffe de l'équipement, sans avoir auparavant reçu une requête du Manager.

2.1.2.4 La station de gestion de réseau

Le Manager contient le protocole de communication ainsi que les applications de gestion. Il se compose d'une console, d'une base de données représentant tous les périphériques gérés du réseau et de toutes les variables MIB des équipements du réseau. Elle permet de récupérer et d'analyser les données relatives aux différents équipements reliés au réseau et de les gérer. Le Manager peut ensuite interpréter ces informations pour faire des rapports d'incidents.

Le Manager envoie des requêtes aux agents sur le port UDP 161 et reste à l'écoute d'éventuels messages d'alarme, appelés traps, envoyés sur le port UDP 162 par un agent SNMP.

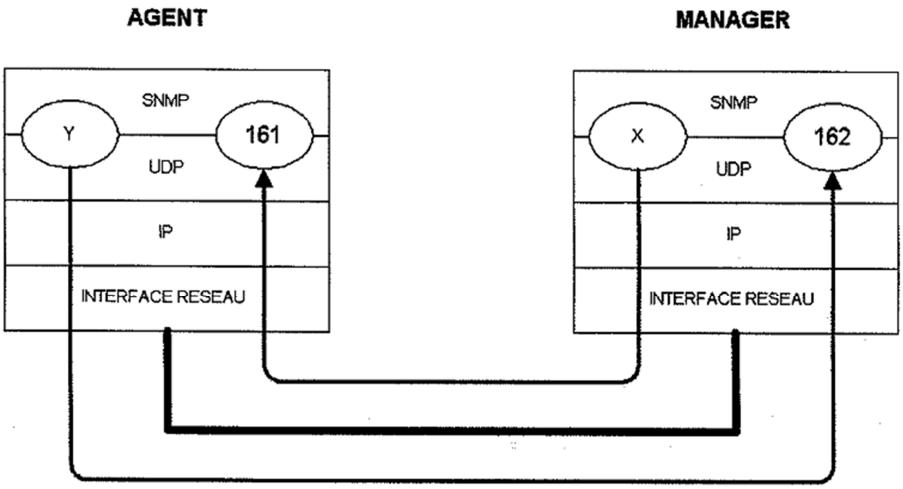


Figure 13 : Ports UDP utilisés par SNMP (PIGNET, 2008)

2.1.2.5 La communauté SNMP

La communauté SNMP est utilisée dans les échanges entre le Manager et l'agent SNMP. Elle définit à la fois l'authentification et le contrôle d'accès. L'agent peut être configuré de trois façons : lecture-seule, lecture-écriture et trap. Le nom de communauté est utilisé comme un mot de passe pour accéder aux informations de la MIB de l'équipement. Il peut y avoir autant de communautés que d'agents. Vice versa, un agent peut avoir une communauté par Manager.

Le paramétrage de la communauté en lecture-seule permet au Manager de lire ces informations mais ne permet pas de modifier certaines valeurs. Le nom de la communauté par défaut est « public ». Le mode lecture-écriture permettra de modifier des valeurs dans la MIB de l'équipement sans avoir à s'y connecter. Le nom de la communauté par défaut est « private ». Cela permet par exemple de remettre facilement des compteurs à zéro. Enfin, le mode trap permet l'envoi d'alertes uniquement de l'agent vers le Manager.

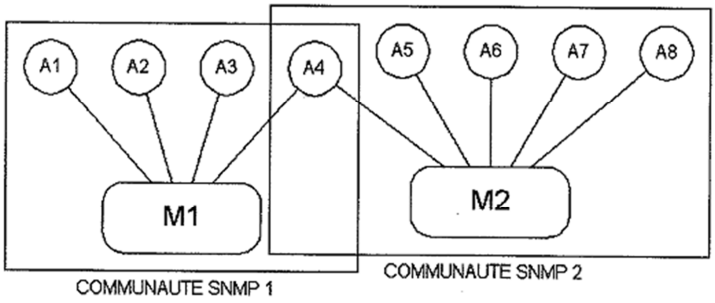


Figure 14 : Organisation des communautés SNMP (PIGNET, 2008)

2.1.3 Le protocole SNMPv1

2.1.3.1 Structure du message

Le message SNMPv1 se compose de trois parties principales (Version, Community et PDU (Protocol Data unit)).

- Version : Entier permettant d'identifier la version utilisée (0 = SNMPv1, 2 = SNMPv2, 3 = SNMPv3).
- Community : Chaine d'octet contenant le nom de la communauté utilisée.
- PDU : Corps du message SNMP.

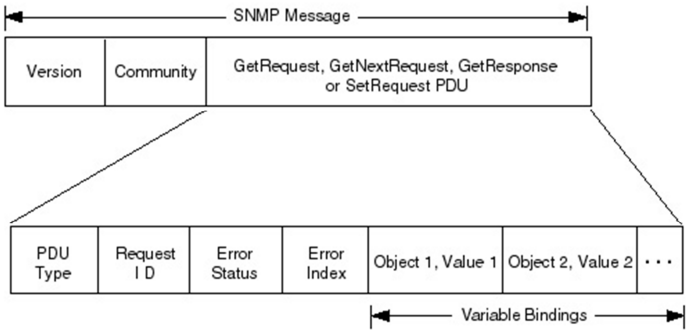


Figure 15 : Format des messages SNMPv1 (MILLER, 1997)

La partie PDU se décompose en 6 morceaux :

- PDU Type : Entier permettant de distinguer le type de message (0 = GetRequest, 1 = GetNextRequest, 2 = GetResponse, 3 = SetRequest).
- Request ID : Identifiant utilisé par le Manager pour vérifier la cohérence des échanges, représenté par un entier.
- Error Status : Entier défini à 0x00 dans la requête envoyé par le Manager. L'agent SNMP inscrit au même endroit un code erreur si une erreur survient pendant le traitement de la requête. (0x00 = noError, 0x01 = tooBig, 0x02 = noSuchName, 0x03 = badValue, 0x04 = readOnly, 0x05 = genErr).
- Error Index : Entier servant de pointeur pour indiquer l'objet qui a généré l'erreur si le champ Error Status est non-nul. Le champ est toujours égal à zéro dans une demande.
- OID (Object IDentifier) : Indicateur de variable de l'objet.
- Value : Valeur de la variable.

Le partie PDU de la trame est différente lorsqu'il s'agit d'un message de type Trap.

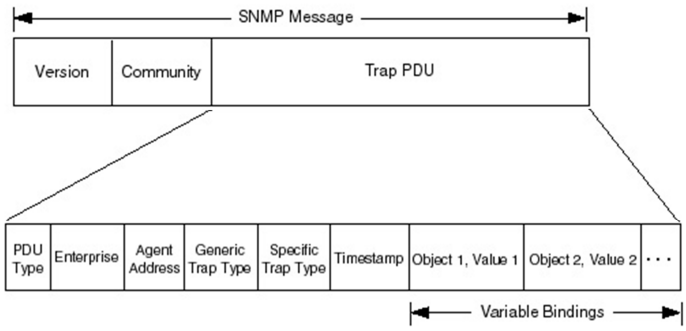


Figure 16 : Format des messages SNMPv1 de type Trap (MILLER, 1997)

La partie Trap PDU se décompose en 8 morceaux :

- PDU Type : Entier permettant de distinguer le type de message (4 = Trap).
- Enterprise :
- Agent Address :
- Generic Trap Type :
- Specific Trap Type :

- Timestamp :
- OID (Object IDentifier) : Indicateur de variable de l'objet.
- Value : Valeur de la variable.

2.1.3.2 Les requêtes

Le protocole SNMP s'appuie sur le protocole UDP pour interroger les différentes MIB. Il supporte trois types de requêtes, GET, SET et TRAP.

2.1.3.2.1 Get

Il existe trois types de message GET :

- **GetRequest** : Requête qui permet au Manager de demander la valeur des variables de la MIB des différents agents passée en paramètre. SNMPv1 ne permet d'obtenir qu'une seule variable par requête car le champ de données du datagramme UDP ne comporte que 484 octets. Chaque requête porte un identifiant appelé Request ID qui est repris dans la réponse générée par l'agent.

- **GetNextRequest** : Requête permettant au Manager d'interroger toute la MIB de l'agent sans forcément la connaître. La requête demande la valeur de l'OID de la MIB juste après celui fourni dans la requête. Ce mécanisme sert à faire une découverte automatique de sa MIB en suivant l'ordre lexicographique des OID.

- **GetResponse** : Requête uniquement émise par l'agent à la suite d'une interrogation. Cette requête ne peut pas être émise sans avoir au préalable reçu une requête d'interrogation de type GetRequest et GetNextRequest. La réponse comportera toujours l'identifiant Request ID de la requête d'interrogation ainsi qu'un code erreur. En cas de non concordance des noms de communautés, la valeur de la réponse sera nulle.

2.1.3.2.2 Set

Le protocole SNMPv1 ne comporte qu'une seule requête Set.

- SetRequest : Requête permettant de modifier la valeur d'un objet de la MIB ou d'une variable et de lancer des périphériques. Chaque requête SetRequest est suivie d'un message GetResponse comportant le même identifiant Request_ID. En cas de mauvaise demande de modification de la MIB, la réponse comportera un code erreur.

2.1.3.2.3 Trap

Les requêtes Trap sont utilisées uniquement par les agents afin de signaler des anomalies aux Managers. La RFC 1157 (IETF, 1990) définit sept cas différents :

- ColdStart(0) trap : signifie que l'agent a été initialisé.
- WarmStart(1) trap : signifie que l'agent a été réinitialisé sans que celui-ci ait été modifié.
- LinkDown(2) trap : signifie qu'il y a une défaillance dans l'un des liens de communication de l'agent.
- LinkUp(3) trap : signifie qu'un des liens de communication de l'agent a été activé ou rétabli.
- AuthenticationFailure(4) trap : signifie qu'il y a eu une tentative de connexion par SNMP avec une communauté invalide.
- EgpNeighborLoss(5) trap : signifie qu'il y a eu des modifications dans le routage EGP d'un routeur.
- EnterpriseSpecific(6) trap : trap générique pouvant contenir une information propriétaire.

2.1.3.3 Emission d'un message.

Lors d'un envoi de message SNMP, le PDU construit est soumis à un service d'authentification. Ce service décidera, en fonction de l'adresse source, de l'adresse de destination et du nom de la communauté, si le PDU doit être crypté. Une fois le message prêt il est envoyé.

2.1.3.4 Réception d'un message.

Lors de la réception d'un message, celui-ci est soumis à une analyse syntaxique. Les messages défectueux sont ignorés. Si le numéro de version n'est pas correct, le message est également ignoré.

La phase d'authentification du message vérifie l'adresse source, l'adresse de destination, le nom de la communauté et le PDU. Si l'authentification échoue, une alarme est envoyée à l'émetteur et le message est ignoré. En revanche, si l'authentification réussit, un PDU est renvoyé.

2.1.4 Le protocole SNMPv2

SNMPv2 introduit deux nouvelles branches dans la MIB, intitulé « snmpV2 » et « snmpV2-M2M » (*Manager to Manager*). Il corrige également des failles de sécurité dont le fait de ne pas diffuser le nom de la communauté en clair sur le réseau.

2.1.4.1 Structure du message

Tout comme le message SNMPv1, SNMPv2 se compose également de trois parties principales (Version, Community et PDU). La requête Trap, dans SNMPv1, est remplacée par la requête SNMPV2-Trap qui possède le même format de trame que les autres requêtes SNMPv2.

- Version : Entier permettant d'identifier la version utilisée (0 = SNMPv1, 2 = SNMPv2).
- Community : Chaine d'octets contenant le nom de la communauté utilisée.
- PDU : Corps du message SNMP.

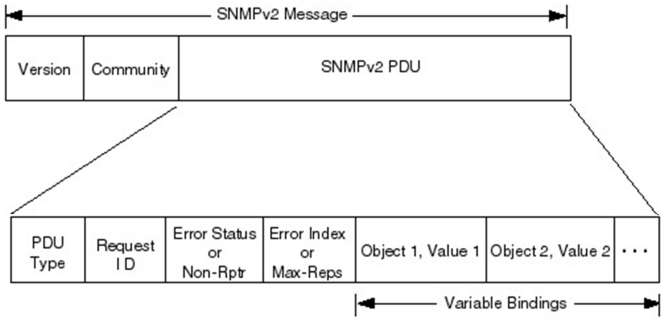


Figure 17 : Format des messages SNMPv2 (MILLER, 1997)

La partie PDU se décompose en 6 morceaux (PDU Type, Request ID, Error Status ou Non-Repeaters, Error Index ou Max-Repetitions, OID et Value).

- PDU Type : Entier permettant de distinguer le type de message (0 = GetRequest, 1 = GetNextRequest, 2 = Response, 3 = SetRequest, 4 = plus utilisé, 5 = GetBulkRequest, 6 = InformRequest, 7 = Trapv2, 8 = Report).
- Request ID : Identifiant utilisé par le Manager pour vérifier la cohérence des échanges, représenté par un entier.
- Error Status : Entier défini à 0x00 dans la requête envoyée par le Manager. L'agent SNMP inscrit au même endroit un code erreur si une erreur survient pendant le traitement de la requête. (0x00 = noError, 0x01 = tooBig, 0x02 = noSuchName, 0x03 = badValue, 0x04 = readOnly, 0x05 = genErr, 0x06 = noAccess, 0x07 = wrongType, 0x08 = wrongLength, 0x09 = wrongEncoding, 0x10 = wrongValue, 0x11 = noCreation, 0x12 = inconsistentValue, 0x13 = resourceUnavailable, 0x14 = commitFailed, 0x15 = undoFailed, 0x16 = authorizationError).
- Non-Repeaters : Spécifie le nombre d'instances d'objets qui ne doivent pas être récupérés plusieurs fois à partir du début de la requête.
- Error Index : Entier servant de pointeur pour indiquer l'objet qui a généré l'erreur si le champ Error Status est non-nul. Le champ est toujours égal à zéro dans une demande.
- Max-Repetitions : Définit le nombre maximal de fois où d'autres variables situées au-delà de celles spécifiées dans le champ Non-Repeaters doivent être récupérées.
- OID : Indicateur de variable de l'objet.
- Value : Valeur de la variable.

2.1.4.2 Les requêtes

SNMPv2 ajoute deux nouvelles requêtes (GetBulk et Inform) à celles de SNMPv1.

- GetBulk : Requête permettant de récupérer une suite de successeurs lexicographiques d'identificateurs d'objets. Les champs « non-repeaters » et « max-repetitions » permettent de déterminer le nombre de variables non répétées et le nombre des variables répétées. Cette requête attend en retour un message de type « Response-PDU ».

- Inform : Requête permettant à un Manager d'envoyer une liste d'identificateurs d'objets avec leurs valeurs à un autre Manager. Cette requête attend également en retour un message de type « Response-PDU ».

2.1.5 Le protocole SNMPv3

La sécurité de SNMPv3 est basée sur le concept User-based Security Model (USM) et le concept View-based Access Control Model (VACM).

2.1.5.1 Structure du message

Le message SNMPv3 se compose de sept parties principales (Message Version, Message Identifier, Maximum Message Size, Message Flags, Message Security Model, Message Security Parameters et Scoped PDU).

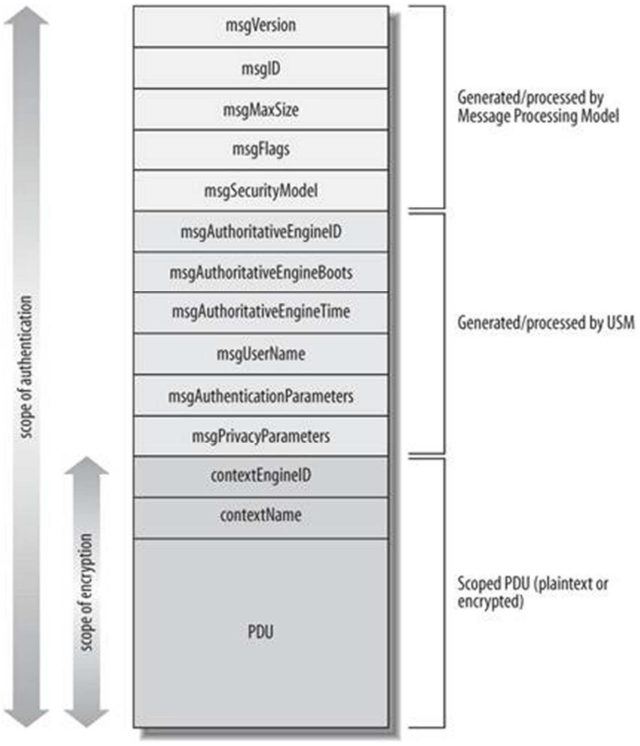


Figure 18 : Format des messages SNMPv3 (MAURO, et al., 2005)

- Message Version : Entier permettant d'identifier la version utilisée (3 = SNMPv3).
- Message Identifier : Entier permettant de désigner le type de message SNMPv3 envoyé.

- Maximum Message Size : Entier spécifiant la taille maximum d'un message que l'expéditeur peut recevoir. La valeur minimum est 484.
- Message Flags : Ensemble d'indicateurs qui contrôle le traitement du message.
- Message Security Model : Entier indiquant le modèle de sécurité utilisé pour ce message.
- Message Security Parameters : Ensemble de champs contenant les paramètres requis pour mettre en œuvre le modèle de sécurité utilisé pour ce message.
- ScopedPDU : Champ contenant le message qui doit être chiffré.

La taille de Message Flags est de 1 octet. Il se décompose en 4 morceaux (Reserved (5 bits), Reportable Flag (1 bit), Privacy Flag (1 bit), Authentification Flag (1 bit)).

- Reserved : Réservé pour un usage futur.
- Reportable Flag : Indique qu'une réponse est attendue à la réception de ce paquet.
- Privacy Flag : Indique qu'un modèle de cryptage a été utilisé.
- Authentification Flag : Indique qu'un modèle d'authentification a été utilisé.

Message Security Parameters se décompose en 6 parties :

- msgAuthoritativeEngineID : Valeur utilisée pour contrer les attaques dans lesquelles des messages d'un moteur SNMP à un autre moteur SNMP sont renvoyés à un moteur SNMP différent.
- msgAuthoritativeEngineBoots : Valeur indiquant le nombre de fois où l'équipement a été allumé.
- msgAuthoritativeEngineTime : Valeur indiquant le nombre de secondes depuis la dernière fois où l'équipement a été allumé.
- msgUserName : Champ contenant le nom de l'utilisateur dont la clé secrète a été utilisée pour authentifier et éventuellement crypter le paquet.
- msgAuthenticationParameters : Champ contenant le chiffrage, HMAC-MD5 (Hash-based Message Authentication Code - Message Digest 5) ou HMAC-SHA (Hash-based Message Authentication Code - Secure Hash Algorithm), du message utilisé pour le paquet.

- msgPrivacyParameters : Si la partie scopedPDU du paquet a été cryptée, ce champ contient alors une variable aléatoire qui a été utilisée comme entrée pour l'algorithme DES.

Scoped PDU se décompose en 3 parties (Context Engine ID, Context Name et PDU) :

- Context Engine ID : Identifie de façon unique une entité SNMP. Une entité SNMP est la combinaison d'un moteur SNMP et les applications SNMP.
- Context Name : Identifie un contexte particulier au sein d'un moteur SNMP.
- PDU : Identique à SNMPv2

2.1.5.2 Les requêtes

SNMPv3 utilise les mêmes requêtes que SNMPv2 et SNMPv1.

On retrouve donc GetRequest, GetNextRequest, GetBulk, Response, SetRequest, Inform, SNMPV2-Trap.

2.1.5.3 User-based Security Model

USM intègre trois mécanismes afin de contrer différents types d'attaques. Le premier est un mécanisme d'authentification permettant d'assurer la non modification d'un paquet SNMPv3 lors de sa transmission et de vérifier la validité du mot de passe de l'expéditeur de la requête. Le deuxième est un mécanisme de chiffrement. Il permet d'empêcher la lecture des informations de gestion d'un paquet SNMPv3. Enfin, le troisième est un mécanisme d'horodatage empêchant la réémission d'un paquet SNMPv3 déjà envoyé.

2.1.5.3.1 Authentification

La phase d'authentification de l'information a pour but d'empêcher la modification du contenu du paquet sans connaître un mot de passe connu seulement par l'émetteur et le receveur du paquet. L'authentification n'a pas pour rôle d'empêcher l'envoi de données en clair sur le réseau malgré le fait qu'elle s'appuie sur un algorithme de hachage

cryptographique, comme MD5 (Message Digest 5) ou SHA-1 (Secure Hash Algorithm 1). Elle permet de vérifier que l'émetteur du paquet est bien celui prévu grâce à cet algorithme de hachage. Prenons comme exemple le mécanisme d'authentification avec l'algorithme de hachage cryptographique MD5. MD5 travaille avec un message de taille variable et produit une séquence de 128 bits ou 32 caractères en notation hexadécimale.

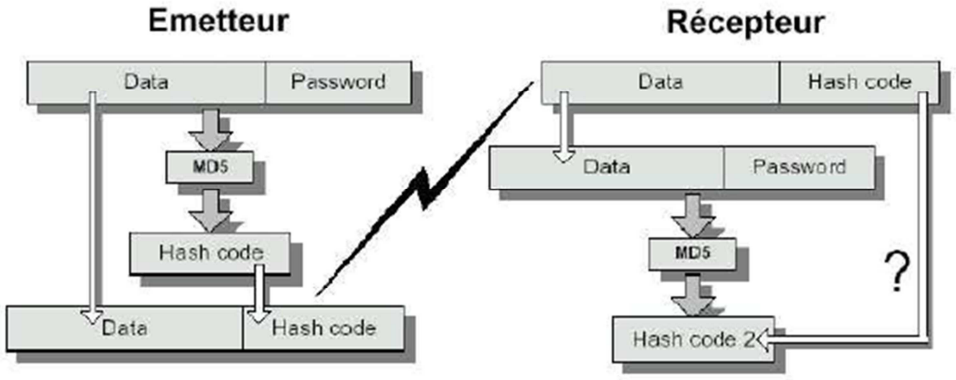


Figure 19 : Mécanisme d'authentification avec l'algorithme MD5 (PERAIRE, et al., 2007)

Tout d'abord, on groupe des données à transmettre avec le mot de passe que l'on soumet à l'algorithme de hachage cryptographique MD5. Une séquence de 128 bits, appelée « Hash code », est alors créée puis transmise avec les données au receveur. Celui-ci soumet à l'algorithme de hachage cryptographique MD5 les données reçues avec le mot de passe afin d'obtenir un nouveau « Hash code ». Les deux « Hash code » sont alors comparés. S'ils sont identiques, l'émetteur est alors authentifié.

SNMPv3 s'appuie sur l'algorithme de hachage HMAC-MD5-96 ou sur HMAC-SHA-96 qui est un peu plus complexe que celui décrit dans ce paragraphe.

2.1.5.3.2 Chiffrement

Afin que les données ne soient pas envoyées en clair sur le réseau, un mécanisme de chiffrement, basé sur un mot de passe connu du Manager et de l'agent SNMP, est alors utilisé. SNMPv3 utilise deux mots de passe afin d'augmenter la sécurité des échanges. Le premier est utilisé dans la phase d'authentification décrite précédemment et le deuxième est utilisé dans cette phase de chiffrement.

SNMPv3 s'appuie sur l'algorithme de chiffrement par bloc DES (Data Encryption Standard) de 64 bits (8 octets) pour le chiffrement des paquets. Le principe est de chiffrer les données (Data) par blocs de 64 bits en entrée avec un bloc de 64 bits contenant une clé (Key) et d'obtenir en sortie les données chiffrées (Coded) par blocs de 64 bits. L'algorithme effectue des combinaisons, des substitutions et des permutations entre les données à chiffrer et la clé. Les étapes de permutation et de substitution, appelés rondes, sont répétées 16 fois. Pour déchiffrer, il suffit de soumettre les blocs de données chiffrées avec la clé de chiffrement de 56 bits à l'algorithme DES pour obtenir les données déchiffrées.

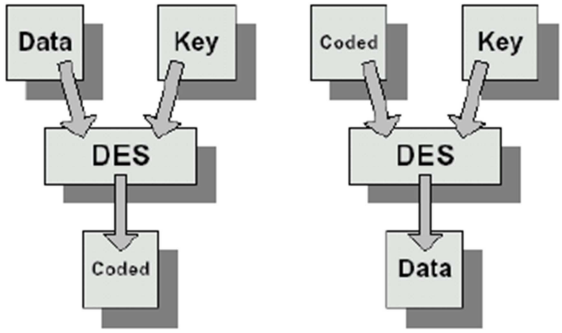


Figure 20 : Principe de fonctionnement de l'algorithme DES (PERAIRE, et al., 2007)

Création de la clé :

Le bloc « Key » de 64 bits est constitué d'une clé de 56 bits et de 8 bits de parité pour vérifier l'intégrité de cette clé. Celui-ci est donc constitué de 8 octets et chaque octet est composé de 7 bits de clé suivis d'un bit de parité. Chacun de ces bits de parité est choisi en fonction du nombre de bits par octet ayant comme valeur '1'. Comme il s'agit d'un test de parité impaire la somme des bits par octet ayant comme valeur '1' doit être impaire. Le bit de parité prendra donc la valeur '1' lorsque le nombre de '1' dans l'octet auquel il appartient est pair et prendra la valeur '0' lorsque le nombre de '1' dans l'octet auquel il appartient est impair. La clé étant réellement constituée de 56 bits, il existe donc 2^{56} clés différentes, soit $7{,}2*10^{16}$ clés.

L'algorithme utilise à chacune des 16 rondes 48 bits différents de ce bloc de clé de 64 bits. Tout d'abord, les bits de clé sont permutés selon un ordre prédéfini représenté par la matrice ci-dessous intitulée PC-1 (Permuted Choice 1). Le 1^{er} bit se retrouve à la $57^{ème}$ position et le $2^{ème}$ bit se retrouve à la $49^{ème}$ position. La permutation ignore les bits de parité.

Cette matrice de permutation se parcourt de gauche à droite et de haut en bas.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Figure 21 : Matrice de la permutation PC-1 de l'algorithme DES (STALLINGS, 2010)

Une fois la permutation effectuée, le bloc de 56 bits est divisé en deux blocs de 28 bits appelés Gauche (G ou C en anglais) et Droite (D). On note C_0 et D_0 l'état initial de ces deux blocs. A chacune des 16 rondes, les bits de ces deux blocs sont décalés vers la gauche d'autant de bits que la table ci-dessous le mentionne. Pour la première ronde, le 1er bit se retrouve en dernière position, le 2ème bit en première position et ainsi de suite. Les deux blocs modifiés seront utilisés pour la ronde d'après permettant de conserver les décalages précédents.

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure 22 : Table de décalage de bits pour la clé de l'algorithme DES (STALLINGS, 2010)

Une fois les deux blocs de 28 bits décalés du nombre de bits correspondant à la ronde à laquelle on se trouve, ils sont regroupés afin de former un seul bloc de 56 bits. Il est à son tour permuté selon un ordre prédéfini représenté par la matrice ci-dessous intitulée PC-2 (Permuted Choice 2).

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Figure 23 : Matrice de la permutation PC-2 de l'algorithme DES (STALLINGS, 2010)

Cette nouvelle permutation fournit en sortie un bloc de 48 bits appelé clé (K). On note K_1 la clé de la 1ère des 16 rondes.

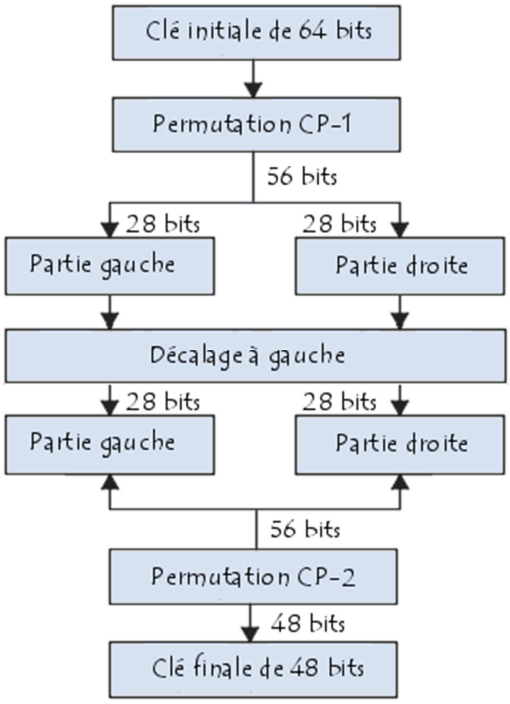


Figure 24 : Calcul de la clé dans l'algorithme DES (Comment ça marche, 2008)

Chiffrement des données :

Les données à chiffrer sont fractionnées en blocs de 64 bits. Chaque bloc subit une permutation initiale des 64 bits. Le 1er bit se retrouve positionné à la 58ème position, le 2ème bit à la 50ème position et ainsi de suite. La permutation initiale peut être représentée par la matrice ci-dessous.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Figure 25 : Matrice de la permutation initiale de l'algorithme DES (STALLINGS, 2010)

Une fois la permutation effectuée, le bloc de 64 bits est séparé en deux blocs de 32 bits, appelés Gauche (G ou L en anglais) et Droite (D ou R en anglais). On note L_0 et R_0 l'état initial de ces deux blocs sur le schéma ci-dessous.

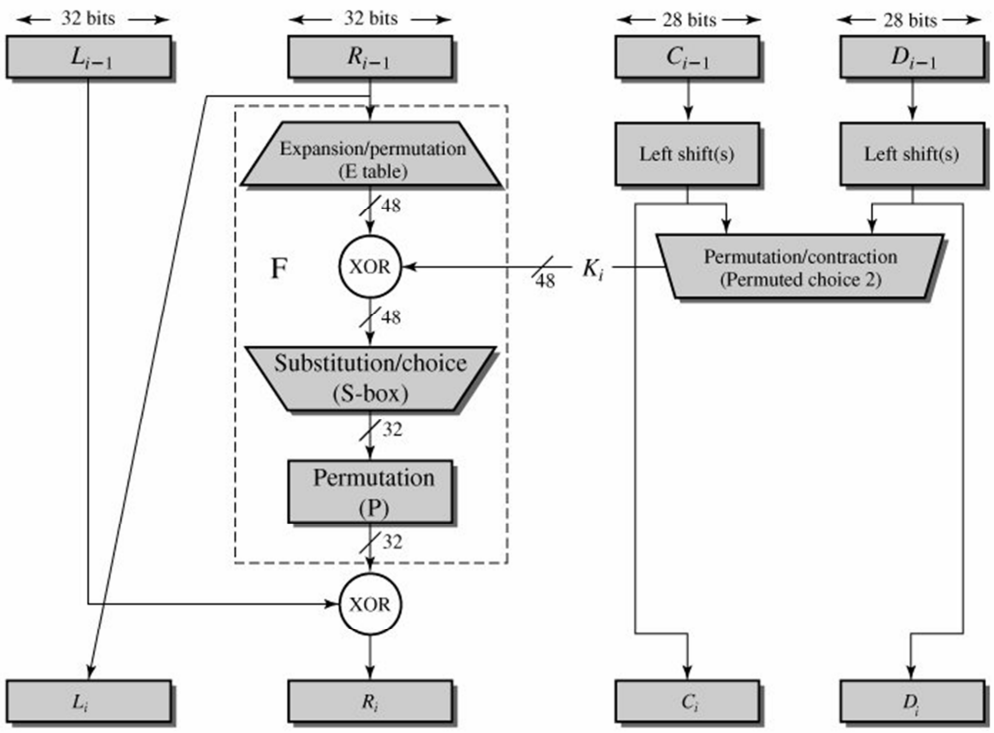


Figure 26 : Fonctionnement de l'algorithme DES (STALLINGS, 2010)

Le bloc de 32 bits de droite, D_0 au départ, est étendu à 48 bits par une matrice intitulé Table d'expansion. Cette matrice duplique 16 des 32 bits et ensuite permute ces 48 bits selon un ordre prédéfini. Ce nouveau bloc de 48 bits est appelée E [R_0] ou bien R'$_0$.

Ensuite, la clé K_1 et le bloc E [R_0] sont soumis à la fonction XOR (eXclusive OR), ou plus précisément à un OU exclusif, qui donnera en sortie une nouvelle matrice de 48 bits. Cette nouvelle matrice est scindée en 8 blocs de 6 bits. Chaque bloc est soumis à une fonction de sélection (S_1 à S_8) qui donne en sortie 8 blocs de 4 bits, regroupés en un seul bloc de 32 bits. Ce bloc de 32 bits subit à son tour une permutation suivant une matrice prédéfinie appelée P.

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Figure 27 : Matrice de la permutation P de l'algorithme DES (STALLINGS, 2010)

Une fois que le bloc de 32 bits est permuté, il est soumis avec le bloc de 32 bits L_0 à la fonction XOR. Le résultat donne un nouveau bloc de 32 bits appelé R_1. Le bloc R_0 initial s'appelle à présent L_1.

Ces différentes étapes sont répétées jusqu'à obtention du bloc L_{16} et R_{16}. Une fois ces deux blocs obtenus, ils sont recollés afin de former un bloc de 64 bits qui à son tour est soumis à la permutation initiale inverse. Cette permutation peut être représentée par la matrice ci-dessous.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Figure 28 : Matrice de la permutation initiale inverse de l'algorithme DES (STALLINGS, 2010)

Une fois cette permutation initiale inverse effectuée, on obtient en sortie un bloc de 64 bits de données chiffrées.

2.1.5.3.3 Horodatage

Afin d'empêcher la réémission de paquets déjà envoyés, SNMPv3 a ajouté un système d'horodatage des paquets. Le temps dans chaque paquet est comparé avec le temps actuel. Si la différence est supérieure à 150 secondes, alors le paquet est ignoré.

Afin de complexifier les échanges, chaque agent possède une horloge différente. Les agents possèdent deux compteurs, intitulés « Boots » et « Times », qui peuvent être utilisés pour l'horodatage. Le compteur « Boots » retient le nombre de fois où l'équipement a été allumé. Le compteur « Times » retient le nombre de secondes depuis la dernière fois où l'équipement a été allumé. La combinaison de ces deux compteurs donne une valeur qui s'accroit en permanence. Le Manager doit donc synchroniser une horloge pour chaque agent. Pour cela, le Manager obtient la valeur des deux compteurs lors du contact initial avec l'agent.

2.1.5.4 View-based Access Control Model

VACM est utilisé pour contrôler l'accès à la MIB. Les champs msgFlags, msgSecurityModel et scopedPDU sont utilisés pour l'accès au message par VACM. Chaque paramètre est utilisé pour déterminer l'accès aux objets gérés. Une erreur est retournée à l'expéditeur si l'accès n'est pas autorisé pour ce type de demande.

Cet accès est réglementé par 4 tables (vacmSecurityToGroupTable, vacmContextTable et vacmAccessTable, vacmViewFamilyTable) :

- vacmSecurityToGroupTable : Table utilisée pour stocker des informations de groupe. Ce groupe, stocké dans le champ « groupName, est constitué par une combinaison des champs « securityModel » et « securityName » permettant de définir les accès aux objets gérés.
- vacmContextTable : Il s'agit d'une collection d'objets gérés ayant des contraintes d'accès associés à un nom de contexte. Cette table, indexée par un « contextName », est utilisée pour stocker tous les contextes disponibles.
- vacmAccessTable : Table utilisée pour stocker les droits d'accès définis pour les groupes. Cette table est indexée par un « groupName », un « contextPrefix », un « securityModel » et un « securityLevel ».
- vacmViewTreeFamilyTable : Table utilisée pour stocker les vues des MIB's. Cette table est indexée par un « viewName » et un « OID » de l'arborescence de la MIB. La MIB VACM définit le vérouillage vacmViewSpinLock qui est utilisé pour permettre à plusieurs moteurs SNMP de coordonner les modifications de la table.

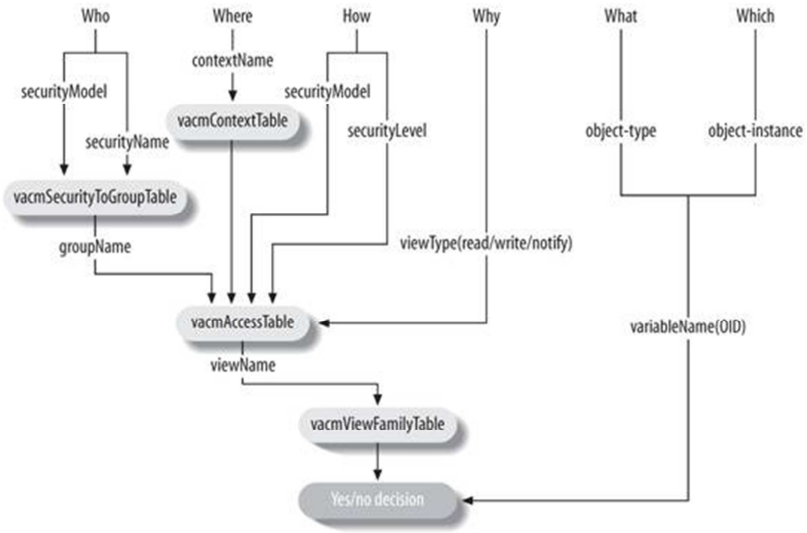


Figure 29 : Fonctionnement logique de VACM (MAURO, et al., 2005)

2.2 Autres méthodes de gestion de réseau

2.2.1 La Technologie de Microsoft

La technologie de Microsoft, intitulée « Windows Management Instrumentation » (WMI), est un système interne de gestion de Windows, préinstallé dans le système d'exploitation, qui permet de surveiller et de contrôler les ressources système grâce à un ensemble d'interfaces. WMI est une implémentation Microsoft de la norme « Web-Based Enterprise Management » (WBEM). WBEM est une technologie permettant d'avoir accès aux informations de gestion sur un réseau grâce à un ensemble de standards intégrés aux outils de supervision, permettant d'unifier la gestion des environnements. WMI prend en charge le modèle de données CIM (Common Information Model), qui définit la représentation des éléments administrés sous forme d'un ensemble d'objets cohérents et d'un ensemble de relations entre ces objets. Les interfaces WMI sont basées sur le modèle COM (Component Object Model) permettant le dialogue entre programmes.

WMI peut fournir à une application de gestion (Management Application) les informations qu'il a pu récupérer sur les ressources système ou matériel (Managed System). Ces informations sont collectées grâce à un composant logiciel appelé Fournisseur (Provider). Celui-ci recueille les informations et les stocke dans un référentiel CIM (CIM Repository). Ce référentiel se comporte comme une zone de stockage.

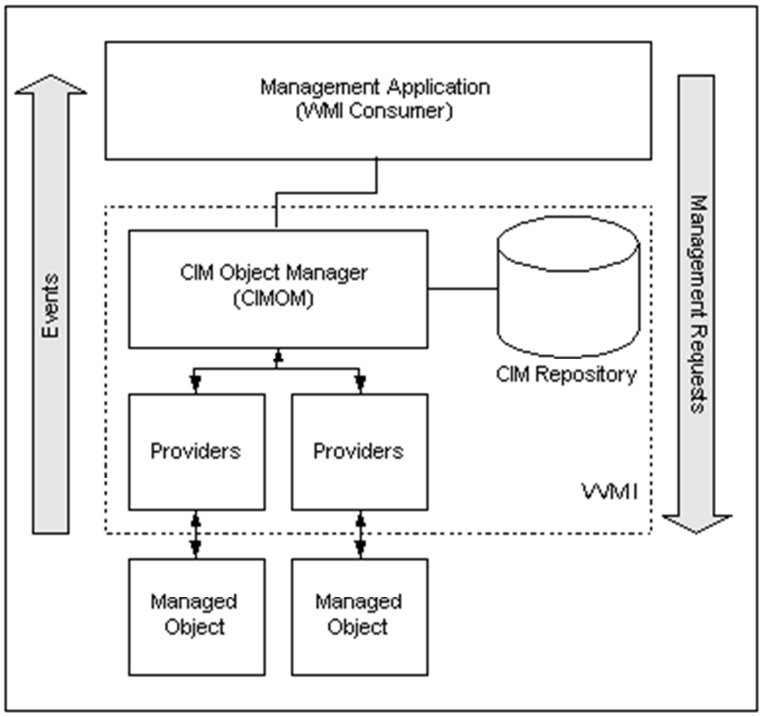


Figure 30 : Fonctionnement de l'environnement WMI (Microsoft Corporation, 2001)

Le service de gestion de Windows, appelé CIM Object Manager (CIMOM), agit en tant qu'intermédiaire entre le Fournisseur, l'application de gestion et le référentiel CIM, en positionnant les informations provenant du Fournisseur dans le référentiel CIM. Ce service a également accès au référentiel CIM lorsque l'application de gestion effectue des requêtes ou lui envoie des instructions pour un objet.

Lors de l'installation de la plupart des logiciels Microsoft, une extension du modèle d'objet CIM est installée en même temps. Cette extension est appelée WMI class. Cette classe permet au Fournisseur de collecter de nouvelles informations.

Le référentiel CIM est divisé en plusieurs zones appelées « Namespace ». Chaque « Namespace » contient un ensemble de fournisseurs avec leurs classes spécifiques liés à une zone de gestion. La « Namespace » intitulée « RootSNMP » contient des Fournisseurs SNMP servant de passerelle vers des systèmes et des équipements qui utilisent le protocole SNMP.

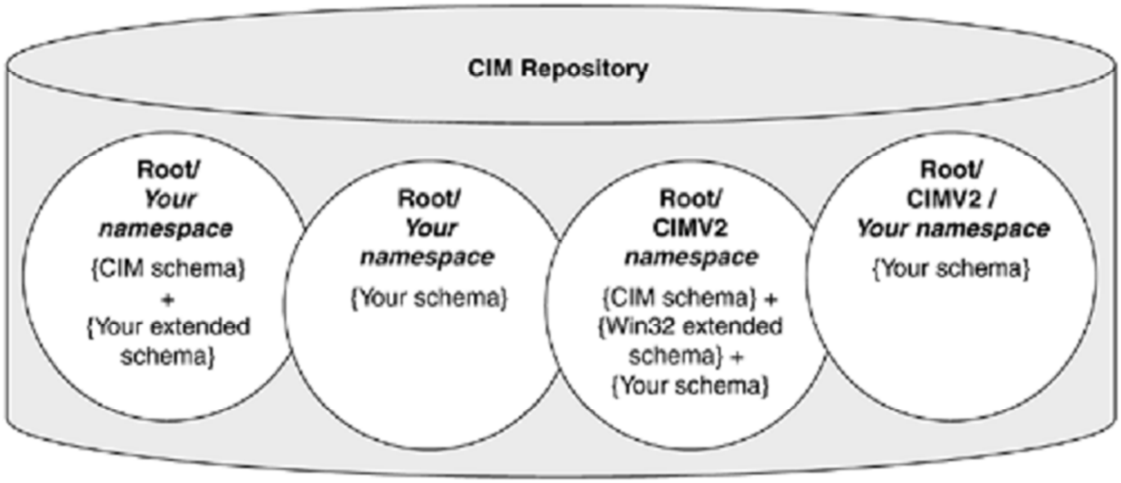


Figure 31 : Structure du référentiel CIM (TUNSTALL, et al., 2002)

2.2.2 La technologie de Cisco

La technologie développée par Cisco System, intitulé NetFlow, a pour but de collecter des informations afin de surveiller le trafic IP. Elle s'appuie sur la notion de flux. Ce flux est défini par plusieurs critères (adresses IP source, adresse IP de destination, port source, port de destination, protocole, classe de service et interface de l'équipement). Un équipement utilisant NetFlow analyse les différents flux et met en mémoire cache les informations sous forme de table. L'équipement compte le nombre de paquets et d'octets reçus pour chaque flux et le renseigne dans cette table appelée « Cache NetFlow ». A chaque paquet reçu, l'équipement

met à jour ce cache en incrémentant les différents compteurs d'une entrée existante ou en créant une nouvelle entrée dans ce cache. Le cache supprime les infos d'un flux lorsque celui-ci reste inactif trop longtemps, 15 secondes par défaut, ou que le flux est actif depuis trop longtemps, 30 minutes par défaut.

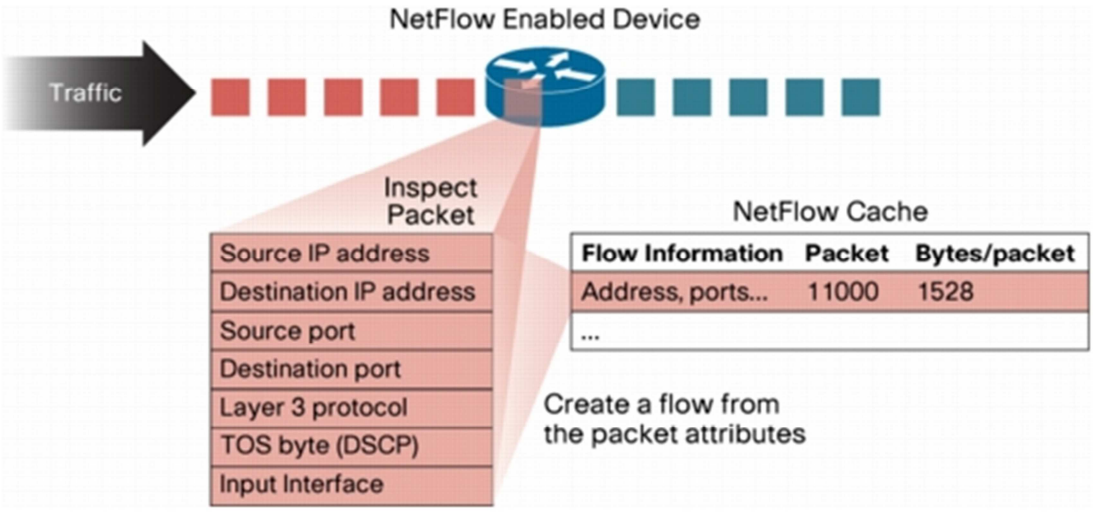


Figure 32 : Création d'un flux dans le cache NetFlow (Cisco System, 2007b)

Une fois l'expiration d'un flux, celui-ci peut être exporté vers une station de supervision. La station reçoit des trames NetFlow d'export suivant un protocole défini par Cisco, groupant plusieurs flux dans le même paquet afin de réduire l'utilisation de la bande passante.

Il existe plusieurs versions du protocole. La version 5 ne supporte que des adresses IP en IPv4 (Internet Protocol version 4) mais permet d'exporter beaucoup d'informations vers la station de supervision. La version 7 reste très proche de la version 5 mais ne sert que pour les switchs de la gamme « Catalyst ». La version 8 a permis d'introduire des schémas d'agrégation. Enfin, la version actuelle est la version 9. Cette version est devenue un standard en octobre 2004, intitulé RFC 3954 « Cisco Systems NetFlow Services Export Version 9 ». Elle apporte la notion de modèles, appelés « templates », ainsi que le support d'IPv6 (Internet Protocol version 6) et de MPLS (MultiProtocol Label Switching).

La trame NetFlow d'export est structurée en trois parties : Packet Header, Template FlowSet et Data FlowSet. Une trame NetFlow d'export contient des informations qui doivent être analysées puis interprétées par l'équipement qui reçoit ces trames. Un FlowSet est un terme générique désignant une série de données qui suivent le PacketHeader. Il existe deux types différents de FlowSet : Template et Data. Une trame NetFlow d'export contient un ou plusieurs FlowSets, et les deux Template et Data FlowSets peuvent être mélangés dans le même paquet d'export.

Figure 33 : Format des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

- Packet Header : Première partie de la trame fournissant des informations simples comme la version de la trame.
- Template FlowSet : Série d'un ou plusieurs modèles d'enregistrement qui ont été regroupés dans un paquet d'export.
- Data FlowSet : Série d'un ou plusieurs modèles de données qui ont été regroupés dans un paquet d'export.

Le Format de l'entête des trames NetFlow d'export version 9 reste relativement inchangé par rapport aux versions précédentes. Il se base sur l'entête de la version 5.

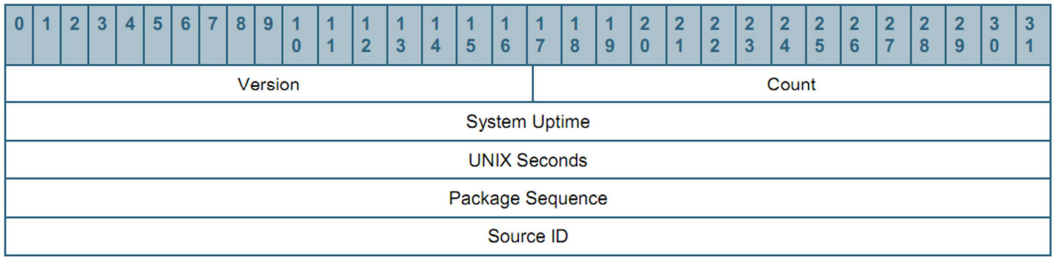


Figure 34 : Format du Packet Header des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

La partie Packet Header se décompose en 6 morceaux présentés dans le tableau ci-dessous.

Tableau III : Champs du Packet Header des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

Nom	Valeur
Version	Version des enregistrements Netflow exportés dans le paquet. Pour la version 9, la valeur est 0x0009.
Count	Nombre d'enregistrements de Template FlowSet et Data FlowSet contenus dans le paquet.
System Uptime	Temps en milliseconde depuis le premier démarrage de l'équipement.
UNIX Seconds	Nombre de secondes écoulées depuis le 1er janvier 1970 00:00:00 UTC (Universal Time Coordinates).
Package Sequence	Compteur incrémental pour l'envoi de paquets d'export par l'équipement. Cette valeur est cumulative, et il peut être utilisé afin de vérifier qu'aucun paquet exporté ne manque.
Source ID	Valeur de 32 bits utilisée pour garantir l'unicité de tous les flux exportés à partir d'un équipement particulier. Le format de ce champ est spécifique à la marque de l'équipement.

Les modèles améliorent considérablement la flexibilité du format des enregistrements NetFlow. Les modèles permettent au collecteur de paquets NetFlow de traiter les données sans connaître au préalable le format des données fournies dans le paquet. Les modèles sont utilisés pour décrire le type et la longueur de chaque champ dans un enregistrement de données NetFlow qui correspondent à un modèle d'identification, appelé Template FlowSet.

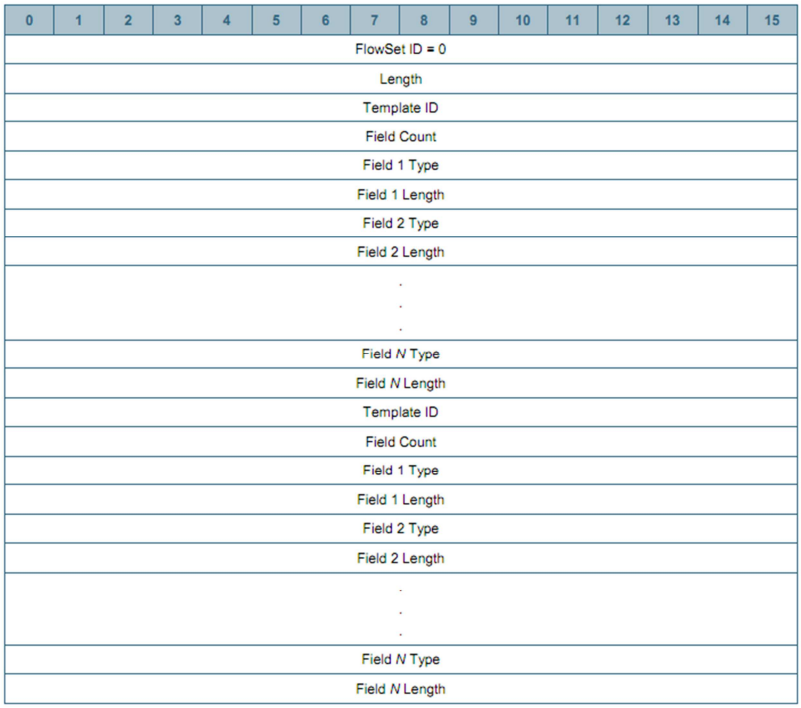


Figure 35 : Format du Template FlowSet des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

La partie Template FlowSet se décompose en 6 morceaux présentés dans le tableau ci-dessous.

Tableau IV : Champs du Template FlowSet des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

Nom	**Valeur**
FlowSet ID	FlowSet ID est utilisé pour distinguer les enregistrements de gabarit à partir des enregistrements de données. Un modèle d'enregistrement a toujours un FlowSet ID dans la plage de 0 à 255.
Length	Longueur totale du FlowSet. Un Template FlowSet peut contenir des identifiants de plusieurs Templates. La valeur Length doit être utilisée pour déterminer la position de l'enregistrement FlowSet suivant. Cela peut être soit un Template FlowSet ou un Data FlowSet.
Template ID	Chaque équipement génère différents Template FlowSets, ainsi qu'un identifiant à chacun d'eux, afin d'exporter les données associées. La numérotation des identifiants commence à 256 car la plage de 0 à 255 est réservé aux FlowSet ID.
Field Count	Nombre de champs contenus dans le modèle d'enregistrement. Un Template FlowSet peut contenir plusieurs modèles d'enregistrement. Ce champ permet à l'analyseur de déterminer la fin du modèle d'enregistrement actuel et le début du suivant.
Field Type	Valeur numérique représentant le type du champ. Les valeurs possibles sont spécifiques au fabricant. Cisco fournit des valeurs uniformes dans toutes ses plates-formes qui prennent en charge la version 9 de NetFlow. Au début de la version 9 initiale, Cisco possédait une liste de 89 valeurs différentes.
Field Length	Valeur en octets donnant la longueur du champ défini ci-dessus.

Après un Template FlowSet, on peut avoir dans la trame un nouveau Template FlowSet ou un Data FlowSet.

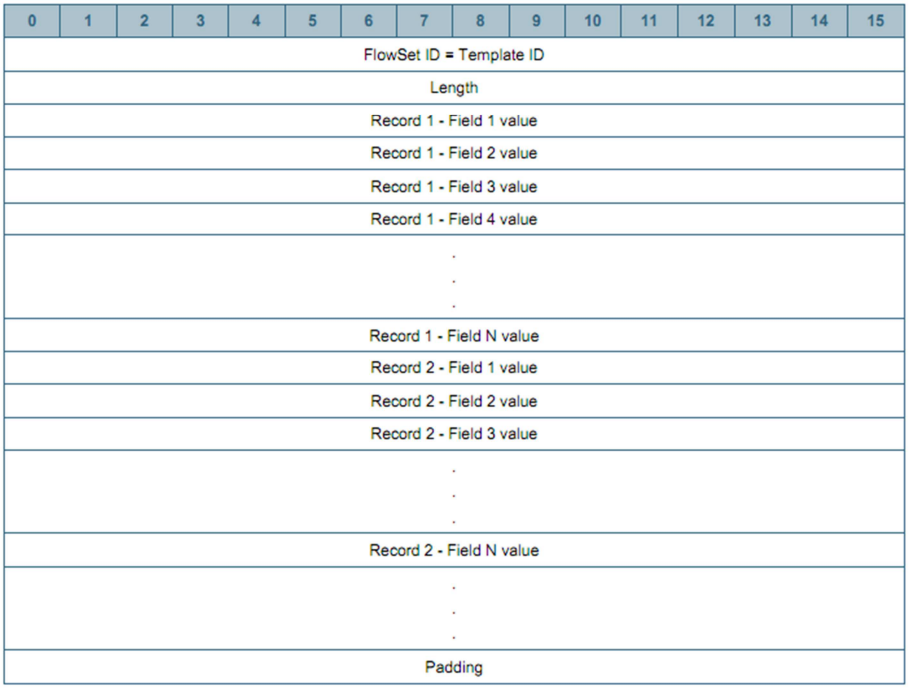


Figure 36 : Format du Data FlowSet des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

La partie Data FlowSet se décompose en 4 morceaux présentés dans le tableau ci-dessous.

Tableau V : Champs du Data FlowSet des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

Nom	**Valeur**
FlowSet ID = Template ID	Un FlowSet ID précède chaque groupe d'enregistrements dans un Data FlowSet d'un paquet NetFlow version 9. Un FlowSet ID correspond à un Template ID déjà reçu. Le collecteur de paquets et les applications d'affichage doivent utiliser le FlowSet ID pour faire correspondre le type et la longueur de toutes les valeurs de champs qui suivent.
Length	Champ définissant la longueur du Data FlowSet.
Record N – Field N	Le reste du Data FlowSet version 9 est une série de valeurs de champs. Le type et la longueur de ces champs ont déjà été définis dans le modèle d'enregistrement référencé par le FlowSet ID / Template ID.
Padding	Champ permettant d'ajouter des bits de bourrage afin d'aligner la fin de la partie Data FlowSet sur une limite de 32 bits. Le champ Length doit comprendre ces bits de bourrage.

Les enregistrements reçus ne peuvent être interprétés que si l'on a reçu auparavant un Template ID approprié. Si cela n'est pas le cas, les enregistrements sont ignorés.

Un type d'enregistrement supplémentaire est très important au sein des spécifications de la version 9 de NetFlow. Il s'agit des modèles d'options, appelés Option Templates. Ces modèles d'option correspondent aux options d'enregistrement de données, appelés Options Data Record. Ces options permettent d'alimenter les métadonnées du processus NetFlow.

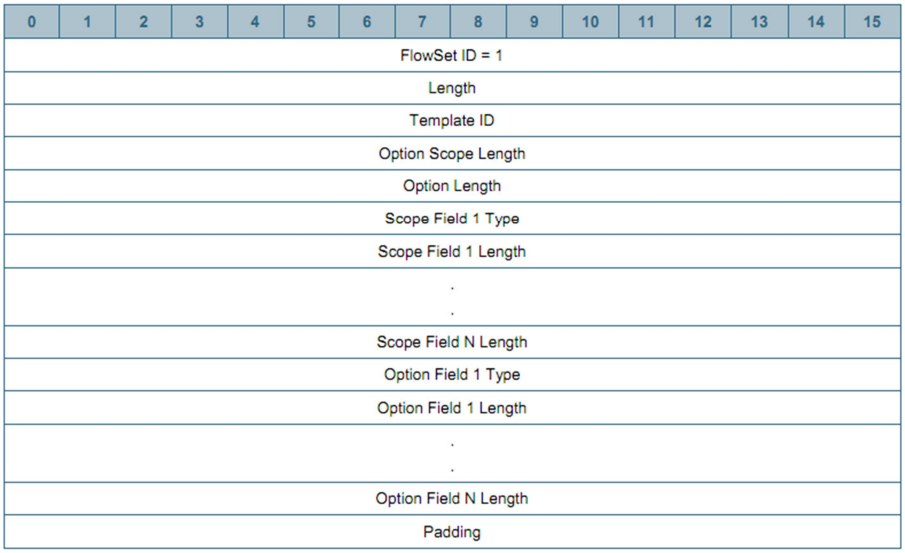


Figure 37 : Format d'Option Template des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

La partie Option Template se décompose en 10 morceaux présentés dans le tableau ci-dessous.

Tableau VI : Champs d'Option Template des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

Nom	Valeur
FlowSet ID = 1	Champ utilisé pour différencier les Template Records des Data Records. La valeur d'un Template Record est toujours '1'. La valeur d'un Data Record est non nulle et toujours supérieure à 255.
Length	Champ définissant la longueur totale de la partie Option Template.
Template ID	Chaque équipement génère différents Template FlowSets, ainsi qu'un identifiant à chacun d'eux, afin d'exporter les données associées. La numérotation commence à 256.
Option Scope Length	Ce champ donne la longueur en octets de tous les champs Scope Field contenus dans cet Option Template.
Options Length	Ce champ donne la longueur totale en octets de tous les champs Option Field contenus dans cet Option Template.

Scope Field 1 Type	Ce champ indique la partie du processus de NetFlow auxquelles les données d'enregistrement se réfèrent. Actuellement, les valeurs définies sont : 0x0001 System, 0x0002 Interface, 0x0003 Line Card, 0x0004 Cache NetFlow et 0x0005 Template.
Scope Field 1 Length	Ce champ donne la longueur en octets du champ Scope Field, tel qu'il apparaît dans un Option Record.
Option Field 1 Type	Valeur numérique représentant le type du champ qui apparait dans les Options Record. Les valeurs possibles sont spécifiques au fabricant. Au début de la version 9 initiale, Cisco possédait une liste de 89 valeurs différentes.
Option Field 1 Length	Ce champ donne la longueur en octets du champ Option Field, tel qu'il apparaît dans un Option Record.
Padding	Champ permettant d'ajouter des bits de bourrage afin d'aligner la fin de la partie Option Template sur une limite de 32 bits. Le champ Length doit comprendre ces bits de bourrage.

On peut constater sur la figure ci-dessous qu'il y a bien un lien entre les Options Template et les Options Data Record.

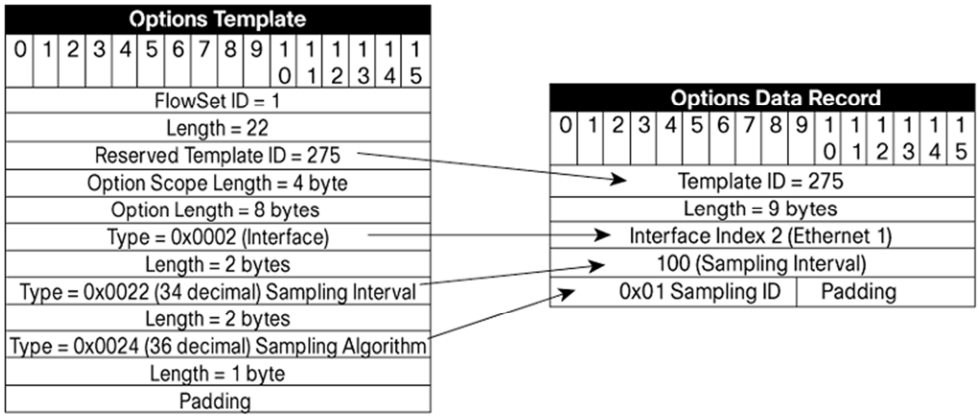


Figure 38 : Exemple d'un Option Template des trames NetFlow d'export version 9 (Cisco Systems, 2007a)

2.3 Fonctionnement des remontées d'alertes

2.3.1 Alertes visuelles et sonores

Lorsqu'un incident survient une alerte est déclenchée. Elle est aussitôt visible sur l'écran de la station de gestion de réseau. L'alerte est classée par importance en fonction de son impact sur le réseau et de sa gravité. Elle possède un code couleur. Rouge permet de signaler que la sonde n'a pas pu récupérer l'information, et orange signale les anomalies permettant parfois d'anticiper une panne. La couleur verte est utilisée pour signaler le bon fonctionnement de la sonde. Les sondes en vert ne figurent pas dans l'affichage des alertes mais peuvent se visualiser lors de l'affichage du détail des sondes de chaque équipement.

Une alerte visuelle peut être couplée avec une alerte sonore. Lorsqu'un incident survient, un son peut être déclenché en même temps que l'apparition de l'alarme sur la station de gestion de réseau.

Ces deux solutions d'alerte obligent une personne à rester constamment devant l'écran des alertes ou à proximité pour pouvoir réagir au plus vite dès qu'un incident survient.

2.3.2 Alertes par mail

La notification par mail consiste à informer le superviseur du réseau par un message électronique dont le contenu est intimement lié à un événement. Un retour à la normale déclenchera de nouveau un message vers cette même personne. L'administrateur doit définir les sondes qui doivent envoyer un mail lorsqu'une anomalie survient.

Le mail contient des informations précises sur la sonde en défaut. Les informations sont variables en fonction du logiciel de supervision.

L'objet du mail contient généralement le nom de l'équipement, son état et la durée de son indisponibilité.

Exemple des rubriques contenues dans un mail d'alerte avec le logiciel PRTG :

Détails de l'événement

- Status : Etat de la sonde
- Date/Heure : Date et heure de départ du problème

Détails de la sonde

- Sonde : Nom de la sonde
- Priorité : Importance de la sonde
- Agent : Nom du serveur de supervision
- Groupe : Nom du groupe auquel appartient la sonde
- Equipement : Nom de l'équipement qui possède cette sonde

Status de la sonde

- Dernier résultat : Dernière valeur de la sonde
- Dernier message : Dernier message d'erreur de la sonde
- Dernière mesure : Date et heure de la dernière mesure
- Dernier OK : Date et heure de la dernière bonne mesure
- Dernier "Non fonctionnel" : Date et heure du dernier échec
- Total du temps de disponibilité : Durée de disponibilité de la sonde
- Total du temps de non disponibilité : Durée de non disponibilité de la sonde
- Collecté depuis : Date et heure de la création de la sonde
- Emplacement : Emplacement de l'équipement
- Réglages : Durée de l'intervalle entre chaque mesure
- Historique de la sonde : Affiche les derniers messages d'erreurs de la sonde

2.3.3 Alertes par push-mail

La technologie push-mail consiste à synchroniser sa messagerie d'entreprise avec son téléphone. Ainsi dès qu'un mail arrive sur le serveur de messagerie de l'entreprise, celui-ci l'envoie instantanément au téléphone qui émet une alerte visuelle et sonore à l'utilisateur pour signaler sa présence. Le superviseur du réseau va alors mettre en œuvre l'intervention nécessaire.

3 Analyse et conception de la plateforme

L'objectif est de superviser l'infrastructure informatique de toute la clinique, afin d'être avertis lorsqu'un équipement réseau, un serveur ou même un service précis d'un serveur ne fonctionne plus. Cela permet de réagir plus vite pour rétablir son fonctionnement. Une alerte pourra également être envoyée lorsqu'un seuil défini comme critique est atteint.

3.1 Choix du logiciel de supervision

Le logiciel de supervision ne doit pas excéder 1 000 €. L'environnement à superviser comprend 20 serveurs et 25 équipements. Il faut que la solution puisse être évolutive.

Nous pouvions envisager plusieurs logiciels open source ou certains logiciels propriétaires.

3.1.1 Logiciels open source

3.1.1.1 Nagios

Nagios est un logiciel open source de supervision. Il permet de surveiller aussi bien les réseaux que les systèmes. Il peut, par exemple, suivre l'évolution d'une charge processeur, le fonctionnement d'un service précis ainsi que la bande passante internet. Une fois une anomalie détectée il est capable d'alerter d'un dysfonctionnement.

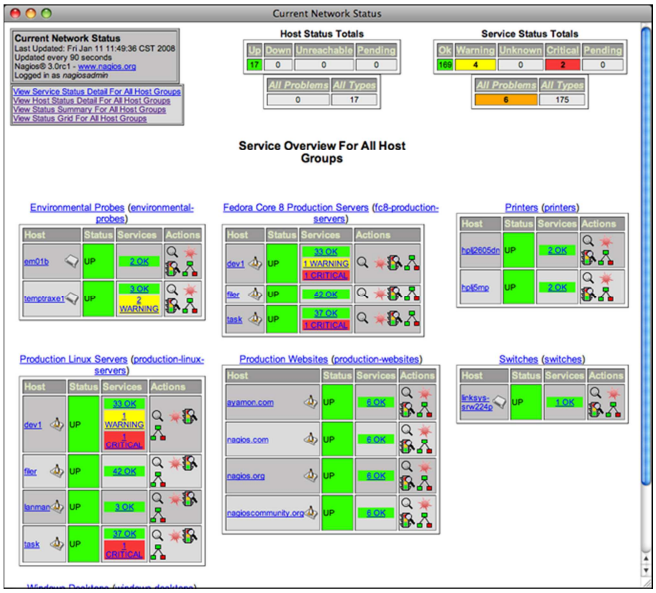


Figure 39 : Présentation du monitoring sous Nagios Core (Nagios Enterprises, 2009)

Nagios est composé d'un moteur d'application (permettant d'organiser les tâches de supervision), d'une interface web (permettant de visualiser l'état du fonctionnement du système d'information) et de plugins (permettant d'ajouter de nouvelles fonctionnalités au logiciel). Ces plugins peuvent être écrits dans de nombreux types de langages.

Ce logiciel a l'avantage de pouvoir superviser tous les types de ressources et de services grâce à des centaines de plugins. Nagios est bien adapté aux systèmes d'information de taille moyenne et aussi de taille importante. Nagios a comme défaut d'être difficile à administrer et de ne fonctionner que sous Linux ou une variante Unix.

Afin de simplifier son implantation au sein des entreprises, Nagios Enterprises a lancé une version payante, appelée Nagios XI. Ainsi, Nagios Enterprises propose donc une version communautaire gratuite appelée Nagios Core et cette version payante. Nagios XI s'appuie sur le moteur Nagios Core mais inclut une nouvelle interface de gestion plus simple à mettre en place. Cette version payante permet de configurer les sondes directement depuis l'interface web alors que la version gratuite conserve sa méthode de paramétrage consistant à modifier des fichiers en lignes de commandes. Le prix varie en fonction du nombre d'hôtes à superviser. Nagios XI coûte pour 1 à 50 hôtes 1 295 $, pour 51 à 100 hôtes 1 995 $ et est illimité en nombre d'hôtes pour 2 495 $.

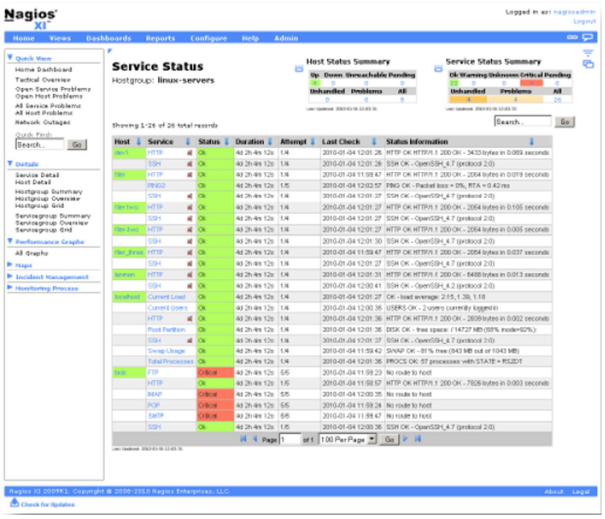


Figure 40 : Présentation du monitoring sous Nagios XI (Nagios Enterprises, 2010)

Nagios XI semble être un produit intéressant par sa configuration simplifiée. Son coût est légèrement supérieur au budget (1 995 $). Son principal défaut par rapport aux préconisations est qu'il ne s'installe pas sur un serveur Windows, tout comme la version gratuite.

3.1.1.2 Cacti

Cacti est un logiciel libre ayant pour but principal de mesurer les performances du réseau. Il permet de réaliser principalement des graphiques et de faire des statistiques grâce à ces graphiques. Il fonctionne grâce à un serveur web et une base de données. Il est possible d'ajouter des plugins afin de lui apporter des services supplémentaires.

Cacti est gratuit. Il fonctionne aussi bien sous Unix que Windows. Il peut déclencher des alertes par mail en cas de dépassement de certains seuils d'alerte par l'ajout d'un plugin appelé Thold.

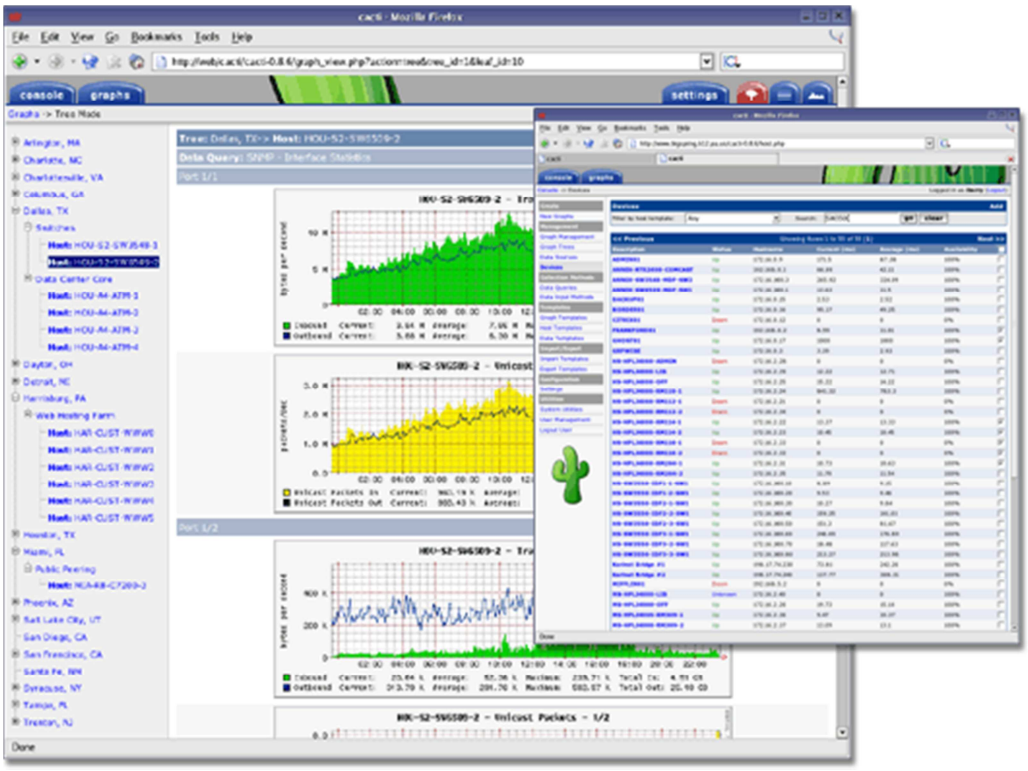


Figure 41 : Présentation du monitoring sous Cacti (The Cacti Group, 2010)

Cacti est une bonne solution pour faire des graphiques, mais il ne répond pas complètement aux besoins de la clinique en matière de supervision de serveurs.

3.1.1.3 Centreon

Centreon est également un logiciel open source permettant de superviser le réseau. Il fonctionne grâce au moteur de récupération d'informations de Nagios. Il s'agit en fait d'une surcouche web de Nagios.

Ce logiciel gratuit a été conçu pour faciliter l'administration de Nagios et avoir une interface simplifiée. Il permet de faire du monitoring en temps réel ainsi que de la remontée d'alerte en cas d'incident. En revanche, Centreon ne fonctionne que sous Linux ou Solaris.

Figure 42 : Présentation du monitoring sous Centreon (MERETHIS, 2010)

Centreon est une bonne solution. Il répond aux attentes de la clinique mais il ne peut pas s'installer sur un serveur Windows.

3.1.2 Logiciels propriétaires

Trois solutions ont été étudiées afin de connaître ce qui était proposé sur le marché, sans tenir sans tenir compte a priori des contraintes budgétaires.

3.1.2.1 HP – OpenView

OpenView est un ensemble de modules permettant la supervision des infrastructures informatiques. Chaque module a sa spécificité et possède un coût élevé. Seuls les trois modules ci-dessous correspondent aux besoins.

Le module OpenView Network Node Manager est un logiciel permettant d'avoir une représentation cartographique d'un réseau selon la typologie des équipements. Les alertes sont ainsi visibles par un code couleur. A partir d'une alarme, il est possible de zoomer sur la partie du réseau en dérangement afin de mieux comprendre la panne pour intervenir plus efficacement. Les alertes peuvent également être envoyées par mail. Network Node Manager Starter Edition 250 nœuds coûte 8 300 € HT. La version Starter Edition illimitée en nombre

de nœuds coûte 49 000 € HT. La version la plus élevée, intitulée Advanced Edition illimitée coûte 208 000 € HT. Ce logiciel fonctionne aussi bien sous Windows que Linux ainsi que d'autres systèmes d'exploitation.

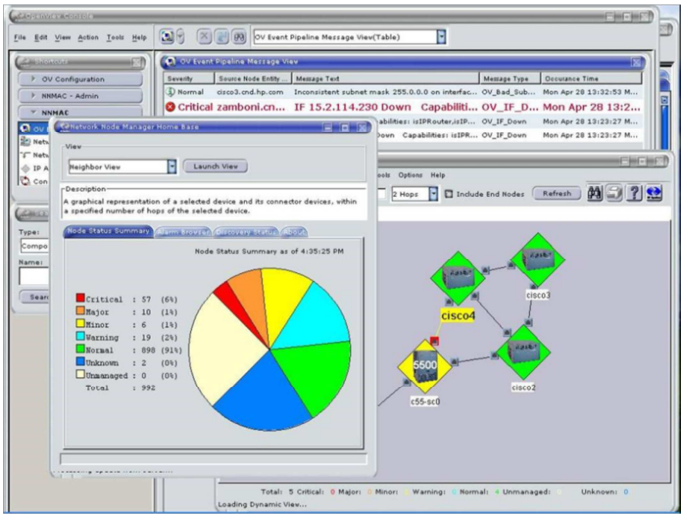


Figure 43 : Présentation du monitoring sous OpenView Network Node Manager (Hewlett-Packard, 2004)

Le module OpenView Operation permet de surveiller le bon fonctionnement et la disponibilité des systèmes. Operations Edition Limitée à 20 nœuds coûte 18 800 € HT. La version limitée à 30 nœuds coûte 25 000 € HT. La version illimitée coûte 30 000 € HT.

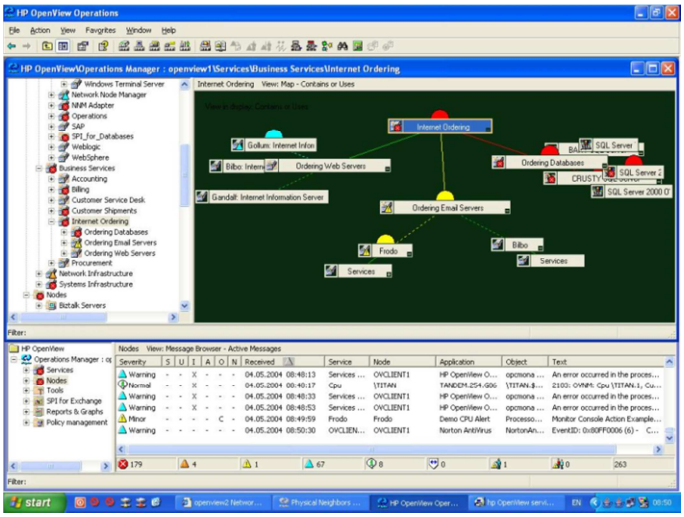


Figure 44 : Présentation du monitoring sous OpenView Operation (Hewlett-Packard, 2005)

Il est également possible d'acquérir les « Smart Plug-Ins » pour la supervision d'Exchange et d'Active Directory si nécessaire. Leur objectif est de fournir la supervision d'un applicatif

instantanément. Le coût d'achat des plug-ins varie en fonction de leur spécificité et de leur complexité. Les plug-ins pour Exchange et pour Active Directory coûtent de 1 200 à 12 600 € HT en fonction des informations qu'ils vont fournir.

La solution HP OpenView est bien trop onéreuse pour la clinique (environ 40 000 € HT) et semble trop compliquée à maintenir avec un effectif de deux personnes au service informatique. Cette solution est adaptée pour des très grosses infrastructures (minimum 1 000 postes).

3.1.2.2 Microsoft – System Center

Microsoft System Center se décompose en plusieurs modules. Dans notre cas, nous souhaitons superviser des serveurs physiques, des serveurs virtuels ainsi que des équipements réseaux. Il faut donc prévoir l'acquisition du logiciel System Center Operations Manager (SCOM), gérant les serveurs physiques, ainsi que System Center Virtual Machine Manager (SCVMM), gérant les serveurs virtuels.

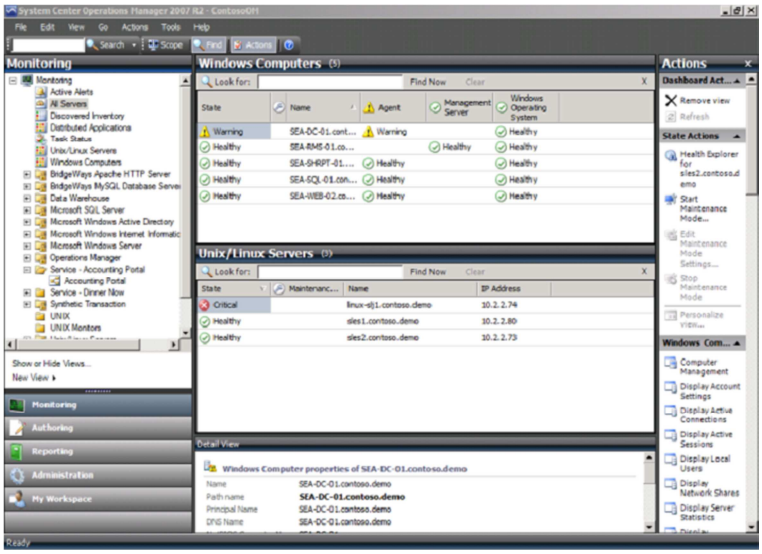


Figure 45 : Présentation du monitoring sous Microsoft SCOM (Microsoft Corporation, 2009b)

SCOM est une solution de supervision de réseau comprenant à la fois les équipements réseau et les serveurs, aussi bien ceux fonctionnant sous Windows que ceux sous Linux. Elle facilite l'accès aux données afin d'être plus réactif en cas de panne. Elle peut surveiller les performances d'un serveur ainsi que ses processus. Lorsqu'une panne survient, une alerte est déclenchée visuellement sur la console ainsi que par mail, sms ou encore messagerie

instantanée. Des rapports détaillés de chaque équipement peuvent être créés facilement décrivant les performances actuelles des applications.

La tarification se fait par un système de licences assez compliqué. Il faut compter 900 € HT pour le logiciel SCOM ainsi que pour le logiciel SCVMM. Ensuite, il faut rajouter des licences par système d'exploitation (OS) géré par SCOM et par SCVMM. Soit 660 € HT par OS et 1 250 € HT par serveur virtualisé avec un nombre d'OS illimité. Il est également possible d'acheter un système de licence plus global au niveau des OS et des serveurs virtualisés. Il faut alors compter 1 250 € HT par serveur physique comprenant 4 OS serveurs ainsi que l'OS hôte, ou alors 1 550 € HT par processeur physique (minimum 2) avec un nombre illimité d'OS.

Cette solution est également trop coûteuse pour la clinique (environ 12 000 € HT). De plus, elle est surtout orientée sur la supervision des systèmes.

3.1.2.3 Paessler – PRTG Network Monitor

PRTG Network Monitor est un logiciel permettant de surveiller l'état du réseau en observant la disponibilité des équipements, pour un coût de 300 € les 100 sondes, 900 € les 500 sondes, 1 375 € les 1 000 sondes, ou encore 3 500 € pour un nombre illimité de sondes. PRTG facilite la mise en place de ces sondes par une base de plus de 80 types de sondes (comme PING, HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol Version 3), DNS (Domain Name System), FTP (File Transfer Protocol) ou encore NetFlow). Il permet également de réaliser des graphiques d'utilisation des bandes passantes. PRTG est capable d'envoyer un mail ou encore un SMS lorsqu'un équipement devient indisponible ou qu'un seuil a été atteint.

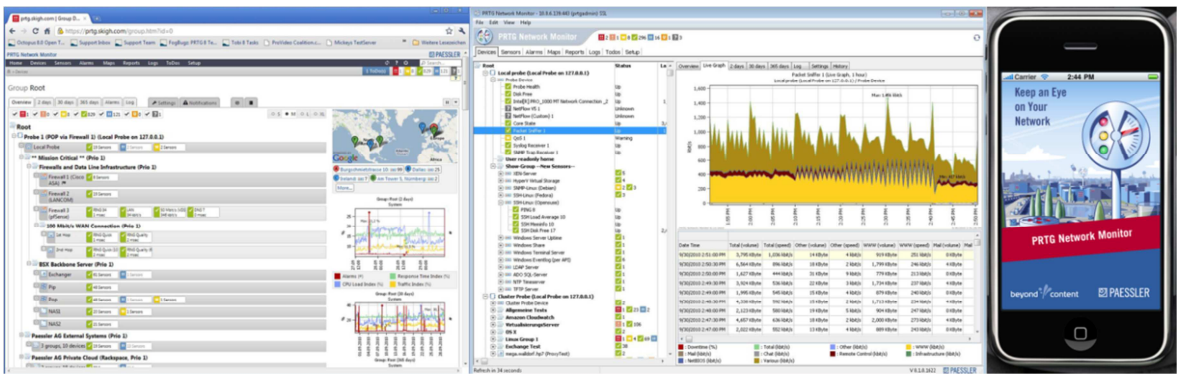


Figure 46 : Présentation du monitoring sous PRTG Network Monitor (Paessler, 2010a)

PRTG Network Monitor ne fonctionne que sous Windows et son interface peut être en français. Il possède également une application pour iPhone intitulé iPRTG permettant de visualiser les alarmes et de les recevoir en push. L'application est vendue 10 €.

La configuration de la clinique impliquant de mettre en place environ 250 sondes réparties sur 20 serveurs et 25 équipements, le logiciel PRTG Network Monitor, seul logiciel répondant à tous les critères définis par la Direction de la clinique, se trouve être plus attractif que les autres logiciels. PRTG est donc retenu pour le projet de supervision.

3.2 Choix de la plateforme

Le logiciel PRTG ayant été choisi, ses prérequis doivent être pris en compte, notamment le fait qu'il ne fonctionne que sur une plateforme Windows (PC, serveur ou machine virtuelle). Trois possibilités existent.

La première possibilité consiste à installer le logiciel sur un PC. Cette solution engendre un problème de performance à moyen et long terme, dû à une accumulation de données et de sauvegarde, d'autant plus qu'il n'est pas prévu de licence pour la sauvegarde de ce PC. Cette solution n'est donc pas envisageable.

La deuxième possibilité est d'installer le logiciel sur un serveur physique. Les performances du serveur étant bien supérieurs à celles d'un PC, il n'y a aucun risque de rencontrer des problèmes de lenteur. Cependant, le problème de sauvegarde persiste car aucune licence n'est prévue pour ce serveur. Il faut donc en acquérir une. Pour des raisons de budget cette solution n'est pas non plus envisagée.

Enfin, la troisième possibilité consiste à installer PRTG sur une machine virtuelle positionnée sur dans la nouvelle infrastructure de virtualisation. Cette solution répond aux attentes car elle évite les problèmes de performance et de sauvegarde.

La clinique a donc décidé d'installer le logiciel PRTG dans la nouvelle infrastructure de virtualisation sur une machine virtuelle sous Windows Server 2003, afin de pouvoir ajouter d'autres fonctionnalités que la simple supervision du réseau. Cette machine virtuelle pourra être sauvegardée grâce au logiciel VMware Data Recovery sans aucun coût supplémentaire.

3.3 Choix de l'infrastructure de messagerie

Deux entreprises proposaient des solutions envisageables : la société RIM avec BlackBerry et Microsoft.

3.3.1 Les solutions BlackBerry

3.3.1.1 Architecture BlackBerry

Afin de faciliter la mise en place d'une infrastructure BlackBerry au sein des entreprises, la société RIM (Research In Motion) propose deux solutions : BlackBerry Enterprise Server et BlackBerry Enterprise Server Express (BESX).

Ces deux solutions consistent à installer au sein du réseau informatique un logiciel BlackBerry. Ce logiciel (BES ou BESX) peut fonctionner tout seul ou avec le logiciel Microsoft Exchange Server. Il peut également s'installer sur un serveur dédié ou sur le même serveur que celui qui héberge Microsoft Exchange Server.

Ces deux versions permettent de transmettre en push les mails, les événements du calendrier, les contacts, les tâches et les mémos. Il est également possible de déployer des applications sur tous les smartphones BlackBerry de la flotte de mobiles ainsi que de gérer les paramètres.

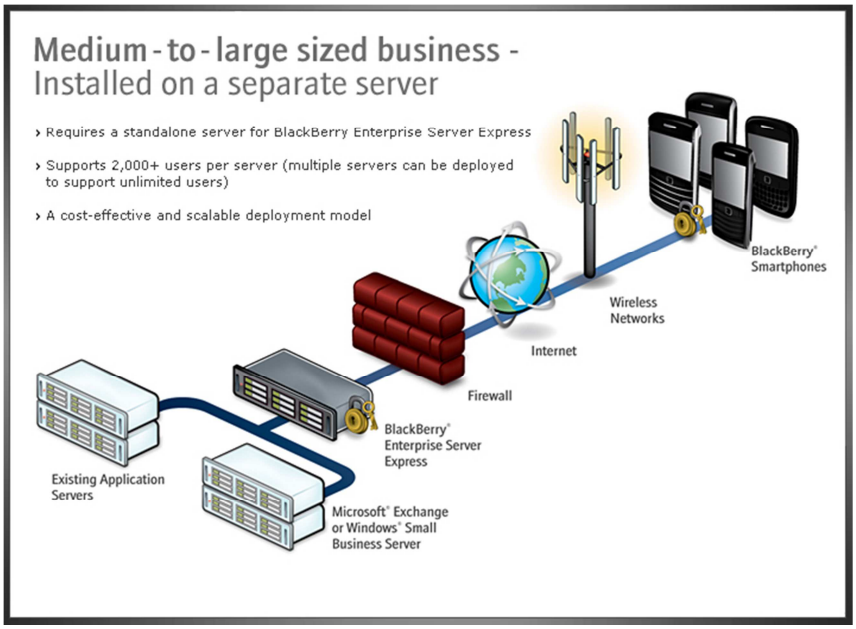


Figure 47 : Présentation de l'architecture BlackBerry (Research In Motion, 2010a)

3.3.1.1.1 BlackBerry Enterprise Server Express

La version BlackBerry Enterprise Server Express est une version gratuite. Il s'agit d'une version simplifiée BlackBerry Enterprise Server. BESX est destiné aux petites structures ayant peu de téléphones ou ne souhaitant pas avoir toutes les fonctionnalités. BESX s'appuie sur un serveur de bases de données SQL (Structured Query Language). Comme BESX est gratuit, le serveur SQL fourni est également une version gratuite appelée SQL Server Express. Cette version de SQL permet de gérer jusqu'à 300 utilisateurs de smartphones BlackBerry. Au cas où le nombre d'utilisateurs serait supérieur, il faut prévoir l'achat d'une licence SQL Server Standard (environ 1 000 € pour la version 2008) ou Entreprise (environ 10 000 € pour la version 2008). Cette version de serveur BlackBerry possède une licence pour 10 000 utilisateurs mais n'est certifiée que jusqu'à 2 000 utilisateurs.

BESX n'est compatible qu'avec Microsoft Exchange Server et Microsoft Small Business Server. En cas d'installation de BESX sur le même serveur que Microsoft Exchange Server, il faut lui allouer 1,5 Go de mémoire et il ne faut pas avoir plus de 75 utilisateurs pour ne pas dégrader les performances de Microsoft Exchange Server.

3.3.1.1.2 BlackBerry Enterprise Server

La version BlackBerry Enterprise Server est une version payante. Elle offre plus de possibilités que BESX. Elle permet de faire de la haute disponibilité permettant au système de basculer automatiquement sur le serveur redondé. Elle facilite également une restauration rapide après une interruption de service. Cette option peut aussi bien être déployée sur des serveurs physiques que sur des serveurs virtuels.

BES gère 450 politiques de gestion contre 35, permettant une plus grande souplesse dans le paramétrage. Cette version permet également de migrer les utilisateurs vers une nouvelle version, de façon transparente, sans intervention de leur part.

BES inclut également une solution de supervision de réseau de l'infrastructure BlackBerry. Cette solution, intitulée BlackBerry Monitoring Service, surveille l'infrastructure et envoie des alertes en cas de problèmes. Des rapports peuvent être générés.

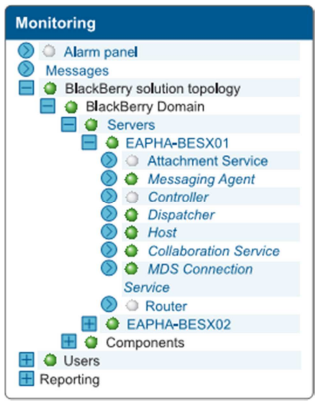


Figure 48 : Présentation du monitoring sous BlackBerry Monitoring Service (Research In Motion, 2009)

BlackBerry Enterprise Server coûte 2 999 $, incluant une licence pour un utilisateur de smartphone BlackBerry, ou 3 999 $, incluant vingt licences utilisateurs. Il est également possible d'acheter des licences additionnelles. Pour cela, il faut compter 99 $ pour un utilisateur, 429 $ pour 5 utilisateurs, 699 $ pour 10 utilisateurs, 3 299 $ pour 50 utilisateurs, 5 999 $ pour 100 utilisateurs et 27 499 $ pour 500 utilisateurs.

Si le nombre d'utilisateurs est inférieur à 300, l'utilisation de la base de données SQL Server Express suffit. Dans le cas contraire, il faut donc acheter en plus la licence SQL Server Standard ou Enterprise évoquée précédemment.

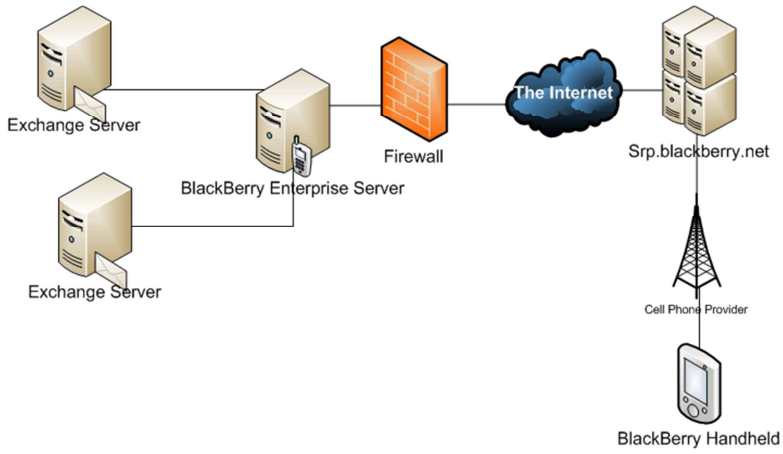


Figure 49 : Fonctionnement de l'architecture BlackBerry (InfotechGuyz, 2008)

Cette architecture BlackBerry ne fonctionne qu'avec des smartphones BlackBerry ou des smartphones fabriqués par des titulaires de licence BlackBerry Connect. Ces smartphones doivent être équipés du logiciel BlackBerry Connect. Pour pouvoir fonctionner, le firewall de

l'entreprise doit laisser passer les trames TCP dans les deux sens sur le port 3101, depuis le serveur BlackBerry vers l'adresse fr.srp.blackberry.com (93.186.25.33). Si les échanges de données ne peuvent pas se faire sur le port 3101, elles se feront sur le port 3500.

3.3.1.2 La technologie de push-mail BlackBerry

Le terminal BlackBerry utilise 11 protocoles propriétaires différents pour dialoguer principalement avec le serveur BlackBerry : Address Lookup Protocol (ALP), Compressed Internet Calendar (CICAL), Compressed Multipurpose Internet Mail Extension (CMIME), Device File Transfert Protocol (DFTP), Gateway Message Envelope (GME), IP Proxy Protocol (IPPP), Over The Air Folder Management (OTAFM), Wireless Key Generation (OTAKEYGEN), Service Book Protocol, Server Routing Protocol (SRP) et Synchronization (SYNC).

Le push-mail s'appuie principalement sur le protocole IPPP et le protocole SYNC. Le protocole IPPP permet le transfert de paquets de type TCP et HTTP entre le terminal BlackBerry et sa destination. Le protocole SYNC permet le transfert de paquets contenant des données d'agenda, des modifications de données, des mails et des signatures de mail entre le terminal BlackBerry et le service de synchronisation du BlackBerry Enterprise Server (BES).

Exemple d'un fichier journal montrant un BlackBerry Enterprise Server initiant la connexion par proxy en push :

```
<LAYER = IPPP, DEVICEPIN = <devicepin>, DOMAINNAME = kmtestd,
CONNECTION_TYPE = PUSH_CONN, CONNECTIONID = -432667474,
DURATION(ms) = 600090, MFH_KBytes = 0, MTH_KBytes = 10.477,
MFH_PACKET_COUNT = 0, MTH_PACKET_COUNT = 4>
```

Figure 50 : Présentation d'une connexion initié par BlackBerry Enterprise Server (Research In Motion, 2010c)

Exemple d'un fichier journal montrant un terminal BlackBerry initiant la connexion par proxy :

```
<LAYER = IPPP, DEVICEPIN = u29, DOMAINNAME = test.rim.net,
CONNECTION_TYPE = DEVICE_CONN, CONNECTIONID = 852164874,
DURATION(ms) = 3500, MFH_KBytes = 0.908, MTH_KBytes = 38.218,
MFH_PACKET_COUNT = 1, MTH_PACKET_COUNT = 2>
```

Figure 51 : Présentation d'une connexion initié par un terminal BlackBerry (Research In Motion, 2010c)

Informations contenues dans les fichiers journaux du serveur BlackBerry :

- LAYER : Protocole utilisé pour la connexion entre le terminal mobile et le serveur.
- DEVICEPIN : Code PIN (Personal Identification Number) ou identifiant utilisateur du terminal BlackBerry.
- DOMAINNAME : Nom de domaine.
- CONNECTION_TYPE : Type de connexion. DEVICE_CONN lorsqu'il s'agit d'une connexion faite par le terminal BlackBerry. PUSH_CONN lorsqu'il s'agit d'une connexion faite par le BlackBerry Enterprise Server.
- CONNECTIONID : Identificateur unique pour une connexion IPPP. Lorsqu'il s'agit d'une connexion push le signe moins est ajouté devant.
- DURATION(ms) : Durée de la connexion en millisecondes.
- MFH_KBytes : taille des messages envoyés par le terminal BlackBerry, en Kilo-octets.
- MTH_KBytes : taille des messages reçus par le terminal BlackBerry, en Kilo-octets.
- MFH_PACKET_COUNT : Nombre de paquets envoyés par le terminal BlackBerry.
- MTH_PACKET_COUNT : Nombre de paquets reçus par le terminal BlackBerry.

Dans le cadre de la clinique, le serveur BlackBerry Enterprise Server Express suffit car l'infrastructure ne concernerait que cinq utilisateurs. La base de données SLQ Server Express est donc bien suffisante et permet de limiter les dépenses. BESX serait donc installé sur le même serveur que Microsoft Exchange Server. La solution BlackBerry Enterprise Server Express reviendrait à un coût d'acquisition de 0 € contre 3 395 $ pour la version payante.

3.3.2 La solution Microsoft

3.3.2.1 Architecture Microsoft

Pour mettre en place une infrastructure de push-mail avec la technologie Microsoft Direct Push, il suffit uniquement du logiciel Microsoft Exchange Server 2003, SP2 minimum. Afin d'autoriser la synchronisation des éléments d'un compte utilisateur sur un téléphone, il faut tout d'abord l'identifier puis l'authentifier. Pour cela, l'utilisateur doit faire partie de l'annuaire de l'entreprise Active Directory. L'annuaire Active Directory peut être sur le même serveur

que le logiciel Microsoft Exchange Server. L'architecture Microsoft n'a donc besoin d'aucun logiciel ou matériel spécifique.

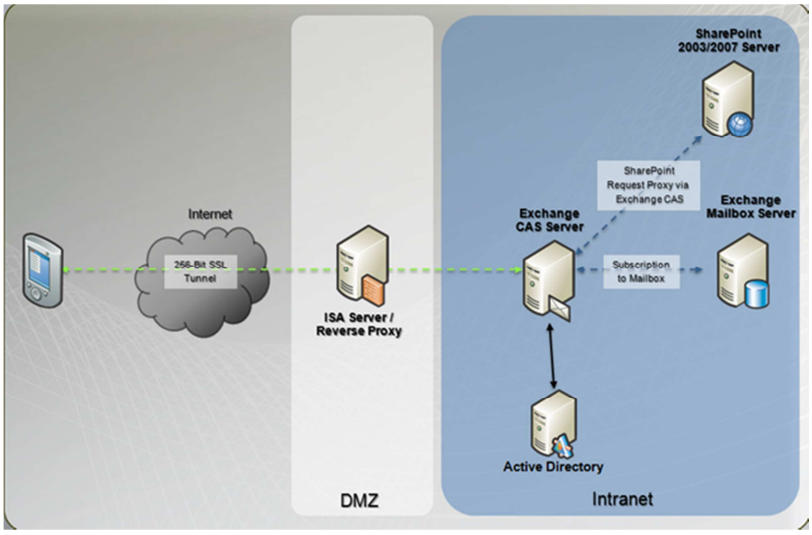


Figure 52 : Fonctionnement de l'architecture Microsoft (Microsoft Corporation, 2009a)

Cette architecture Microsoft ne fonctionne qu'avec des smartphones utilisant un OS titulaire d'une licence Exchange ActiveSync (Android, iPhone, Symbian, Windows Mobile) et compatibles avec la fonction Direct Push. Pour pouvoir fonctionner, le firewall de l'entreprise doit laisser passer les trames TCP dans les deux sens sur le port 443, depuis le serveur de messagerie Microsoft Exchange Server vers les adresses IP des téléphones.

3.3.2.2 La technologie de push-mail Microsoft

Microsoft utilise la technologie Direct Push pour synchroniser en push les téléphones avec le serveur de messagerie Exchange. Cette technologie a été introduite dans Exchange Server 2003 SP2 (Service Pack 2). Le téléphone doit utiliser un OS titulaire d'une licence Exchange ActiveSync et doit être compatible avec la fonction Direct Push.

Le téléphone envoie une requête en HTTPS (Hypertext Transfer Protocol Secure) au serveur Exchange pour lui demander d'être informé en cas de modification d'éléments configurés pour la synchronisation dans les 15 prochaines minutes. Une fois que le téléphone a reçu, de la part du serveur, un message « OK » en HTTP, il se met en attente. Cet intervalle de 15 minutes est appelé intervalle d'interrogation. En cas de modification ou de réception de nouveaux éléments dans ce délai de 15 minutes, le serveur envoie un message au téléphone

lui signalant le ou les dossiers où se trouvent les éléments à synchroniser. Le téléphone envoie donc une demande de synchronisation des répertoires en question. Une fois terminé, le téléphone envoie à nouveau une requête en HTTPS au serveur Exchange pour être informé des modifications dans les 15 prochaines minutes. Une fois que le téléphone a reçu le message « OK » en HTTP de la part du serveur, il se met en attente.

L'intervalle d'interrogation du réseau opérateur est ajusté en fonction des délais d'interrogation Tout d'abord, le téléphone demande un intervalle d'interrogation de 15 minutes. S'il ne reçoit pas de réponse, il diminue ce délai en le passant à 8 minutes. A la fin des 8 minutes, il reçoit un message « OK » du serveur. Alors, il allonge l'intervalle en le passant à 12 minutes. Il reçoit à nouveau un message « OK » du serveur. De ce fait, il allonge encore le délai en le passant à 16 minutes. Comme il n'a rien reçu au bout des 16 minutes, il revient au délai d'interrogation de 12 minutes qui a fonctionné auparavant.

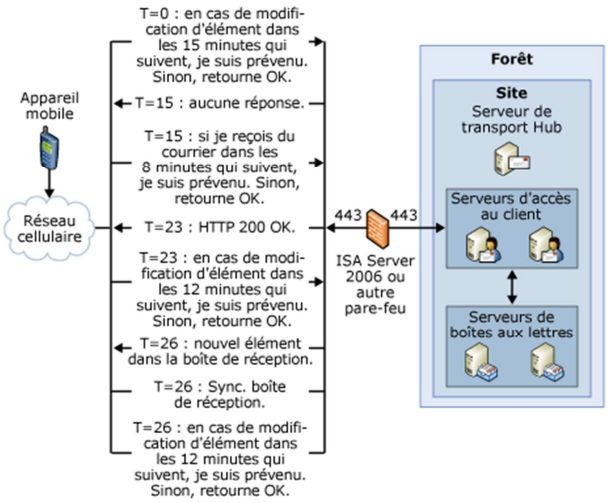


Figure 53 : Fonctionnement de la technologie Direct Push (Microsoft Corporation, 2010)

Cette architecture est la plus adaptée pour la clinique. Sa simplicité de mise en place à un coût de 0 € la rend bien plus intéressante que l'architecture BlackBerry. Son large choix de mobiles permet aussi de répondre plus facilement à la variété des attentes des utilisateurs.

3.4 Choix des terminaux GSM

Les terminaux devant être utilisés par des responsables non spécialistes en informatique, ils doivent être simples d'utilisation. La clinique retenant donc l'architecture Microsoft a le choix entre plusieurs systèmes d'exploitation de mobiles (Android, iPhone OS (iOS), Symbian OS et Windows Mobile).

3.4.1 Android

Le système d'exploitation Android possède un avantage majeur, le fait d'être open-source. Cela facilite le développement d'applications spécifiques pour les entreprises. Cependant, la trop grande variété des téléphones engendre une difficulté de maintenance du parc de téléphones car les différentes plateformes Android ont des caractéristiques et des fonctionnalités uniques. Chaque fabricant de téléphone crée une interface propriétaire augmentant les différences entre les téléphones de l'entreprise. Pour limiter les problèmes, il est préférable d'acheter tous les téléphones en même temps et lorsqu'il faut les changer, il faut le faire également en même temps afin d'avoir le même téléphone avec la même version du système d'exploitation.

3.4.2 Symbian OS

Le système d'exploitation Symbian est embarqué dans des téléphones de plusieurs fabricants, dont le plus connu est Nokia. Cet OS permet de se synchroniser avec le serveur de messagerie Microsoft Exchange Server, mais il n'est pas aussi souple qu'Android car il est propriétaire.

3.4.3 Windows Mobile

Le système d'exploitation Windows Mobile, créé par Microsoft, est également embarqué dans des téléphones de plusieurs fabricants. Il a comme avantage d'être totalement compatible avec tous les outils Microsoft. En revanche, le système est relativement lent. Il n'est pas simple d'utilisation et demande à l'utilisateur un temps d'adaptation assez long.

3.4.4 Apple iOS

Le système d'exploitation iOS est seulement embarqué dans les iPhones, simplifiant la gestion du parc de téléphones. Ce système à l'avantage d'être simple d'utilisation. Depuis sa version 2, l'iOS peut se synchroniser avec le serveur de messagerie Microsoft Exchange Server. L'iPhone peut donc synchroniser les mails, l'agenda et les contacts d'un utilisateur.

Figure 54 : Présentation de l'iPhone (Apple Inc., 2010a)

La Direction de la clinique a opté pour l'achat d'iPhones, pour leur simplicité d'utilisation. Le choix d'un type unique de téléphones facilitera également la gestion du parc de téléphones.

4 Réalisation et mise en place de la solution

Afin de veiller au bon fonctionnement de l'infrastructure informatique de la clinique, nous avons mis en place la solution de supervision de réseau PRTG Network Monitor. Ce logiciel peut envoyer des alertes par mail aux administrateurs du réseau. Ces informations peuvent être directement synchronisées avec les téléphones iPhone grâce à la technologie du push-mail.

4.1 Installation et configuration du logiciel PRTG Network Monitor

PRTG Network Monitor a été installé sur une machine virtuelle fonctionnant sous Windows Server 2003. L'installation de ce logiciel inclut la mise en place d'un serveur web afin de pouvoir consulter les pages web du logiciel ainsi qu'une base de données propre au logiciel. Il fonctionne grâce à la mise en place de deux services sur le serveur (PRTG Core Server Service et PRTG Probe Service). PRTG Core Server comprend entre autres la gestion des données, la gestion du serveur web, la création des rapports et la gestion des alertes. PRTG Probe gère principalement les sondes.

4.1.1 Installation du logiciel

Lors de la phase d'installation du logiciel, il est demandé de renseigner le login et le mot de passe qui seront utilisés pour lancer l'interface web.

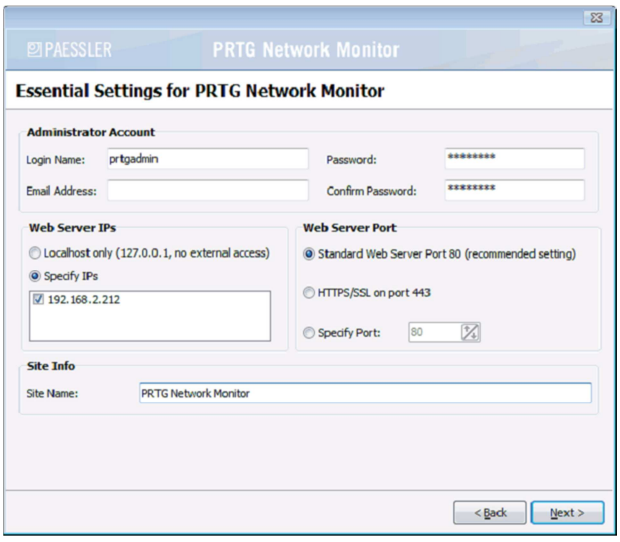


Figure 55 : Paramétrage d'installation du logiciel PRTG Network Monitor (Paessler, 2010b)

Il est possible de limiter l'accès à l'interface web à la machine qui héberge le logiciel PRTG. Pour cela, il suffit de cocher « Localhost only ».D'autre part, il est possible de spécifier le port sur lequel le serveur web est joignable. Cela permet d'éviter les conflits avec d'autres sites web qui seraient déjà joignables sur ce port. Ces options ne nous ont pas paru pertinentes pour la clinique.

Une fois la phase d'installation terminée, il faut lancer le logiciel « PRTG Server Administrator » afin de pouvoir enregistrer la clé de licence.

Figure 56 : Paramétrage de la licence PRTG Network Monitor

Une fois la clé saisie dans le logiciel « PRTG Server Administrator », il faut se rendre sur l'interface web de PRTG et cliquer sur « Configuration », puis sur « Etat d'activation ». Enfin, cliquer sur « Start Activation Now » pour activer la licence.

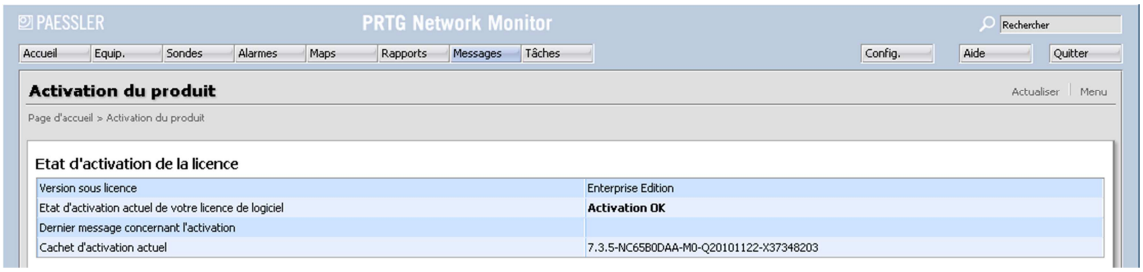


Figure 57 : Etat d'activation de la licence PRTG

4.1.2 Paramétrage du logiciel

Une fois le logiciel activé, il faut configurer le serveur afin qu'il puisse envoyer des alertes par mail. Pour cela, il faut cliquer sur « Configuration », puis sur « Editer la configuration système ». Enfin, cliquer sur l'onglet « Réglages de l'envoi des notifications ». On peut

choisir s'il on souhaite que cela soit le serveur relais de messagerie intégré à PRTG qui envoie les mails ou le serveur de relais de messagerie d'un autre serveur. Différents paramétrages sont également possibles, comme la modification de l'email expéditeur de l'alerte ainsi que le nom de l'objet du mail.

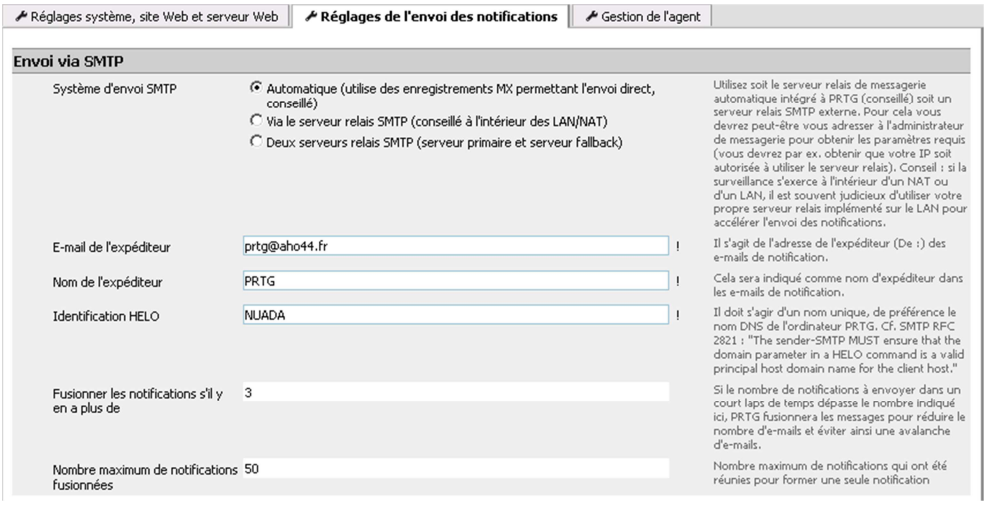


Figure 58 : Paramétrage de l'envoi des alertes

Il est également possible de créer des plages horaires d'alertes en fonction des jours, permettant de suspendre l'envoi des alertes, le week-end par exemple. Pour cela, il faut cliquer sur « Configuration », puis sur « Editer les plannings ». Enfin, cliquer sur « Ajouter un nouveau planning » pour créer une nouvelle plage horaire pour l'envoi des alertes.

Dans notre cas, nous avons créé une plage horaire pour les alertes intitulée « 24/24 7J/7 » afin que d'être prévenus de toutes les pannes à n'importe quel moment de la semaine.

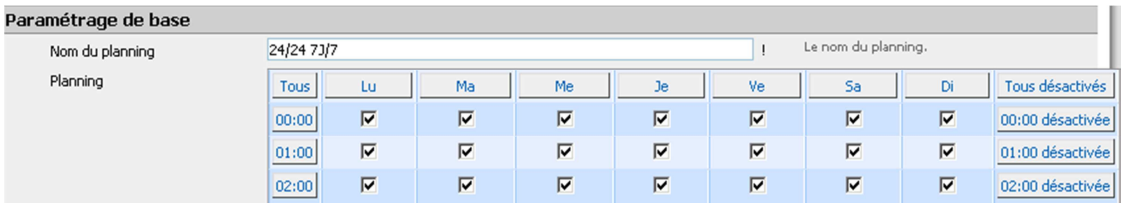


Figure 59 : Configuration des plages horaires pour l'envoi des alertes

4.1.3 Création d'une sonde

Une fois le logiciel paramétré, il faut créer des sondes afin de pouvoir surveiller un équipement. Les sondes peuvent être positionnées dans des groupes, sous forme de hiérarchie. On trouve tout en haut de la pyramide le groupe principal, appelé « Root Group ». Ensuite, on trouve le serveur de supervision lui-même, appelé « Probe ». A l'intérieur de ce groupe, on peut créer différents groupes, appelés « Group », correspondant aux catégories des équipements, comme les serveurs et les switchs. Dans chacun de ces groupes on trouve les équipements, appelés « Device ». A l'intérieur de chaque équipement, on trouve les différentes sondes propres à cet équipement, appelées « Sensor ». Chaque sonde peut également avoir plusieurs canaux, appelés « Channel », afin d'obtenir plusieurs informations similaires en même temps.

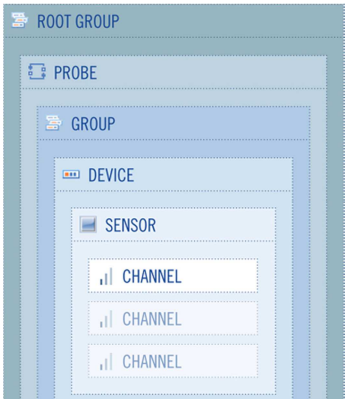


Figure 60 : Structure organisationnelle des sondes (Paessler, 2010b)

Pour créer une sonde, il faut créer un nouveau groupe ou se positionner à l'intérieur. Puis, on peut créer un équipement ou en choisir un déjà créée. Ensuite, on clique sur « Paramètres » afin de saisir les informations qu'il faut utiliser pour interroger l'équipement (son adresse IP, sa priorité, sa version SNMP et sa communauté).

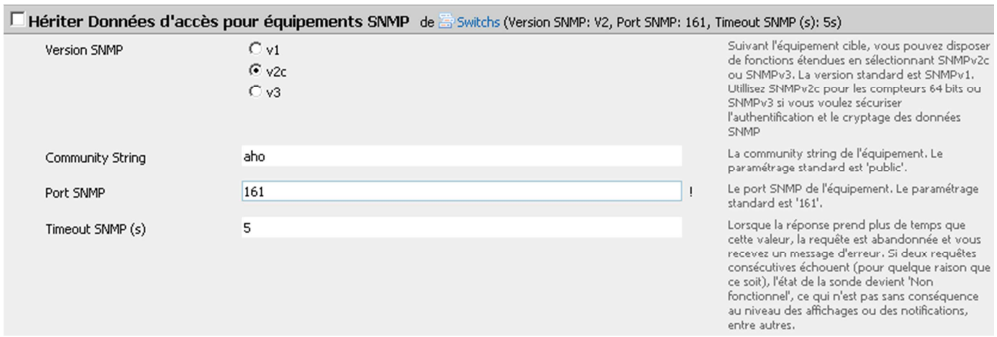


Figure 61 : Paramétrage SNMP d'un équipement

L'équipement peut hériter du paramétrage du groupe auquel il appartient. Chaque niveau de hiérarchie peut ainsi avoir un paramétrage spécifique ou hériter de son parent. Cela permet de simplifier l'installation de la solution.

Une fois l'équipement paramétré, il est possible de lancer une recherche de sonde au lieu de les installer une par une. Une fois que toutes les sondes sont installées, il est important de supprimer toutes celles qui sont inutiles afin d'éviter d'être alerté pour rien.

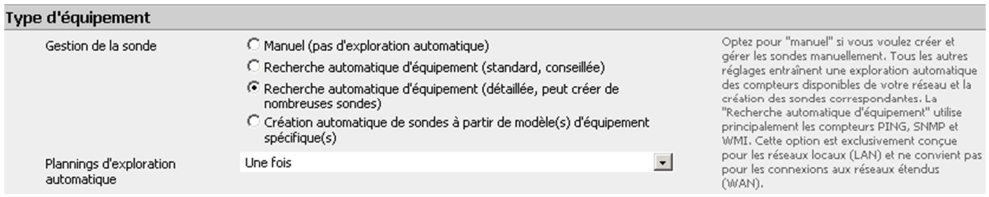


Figure 62 : Paramétrage de la recherche automatique des sondes pour un équipement

Pour ajouter une sonde manuellement, il faut cliquer sur « Ajouter une sonde ». Une longue liste de sondes préconfigurées apparait. Choisir l'une d'entre elle et cliquer sur « Poursuivre à l'étape 2 ».

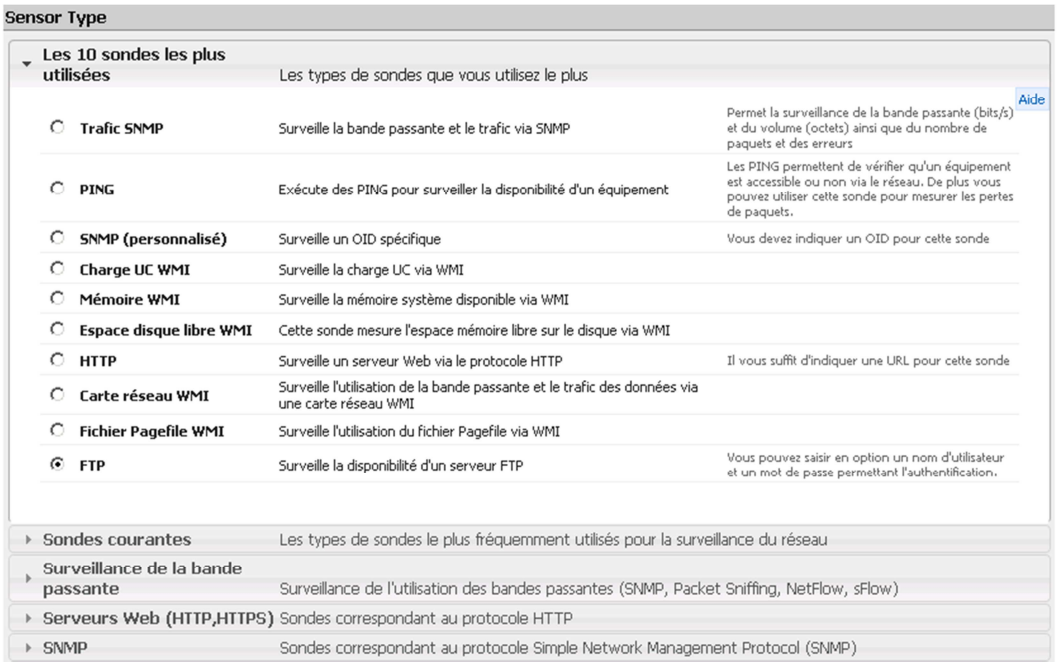


Figure 63 : Choix d'un type de sonde

Ensuite, on peut modifier le nom de la sonde, lui attribuer une priorité allant de 1 à 5 ou encore paramétrer les intervalles entre chaque envoi de requête. Une fois le paramétrage terminé, il faut cliquer sur « Poursuivre ». La sonde est à présent ajoutée à l'équipement.

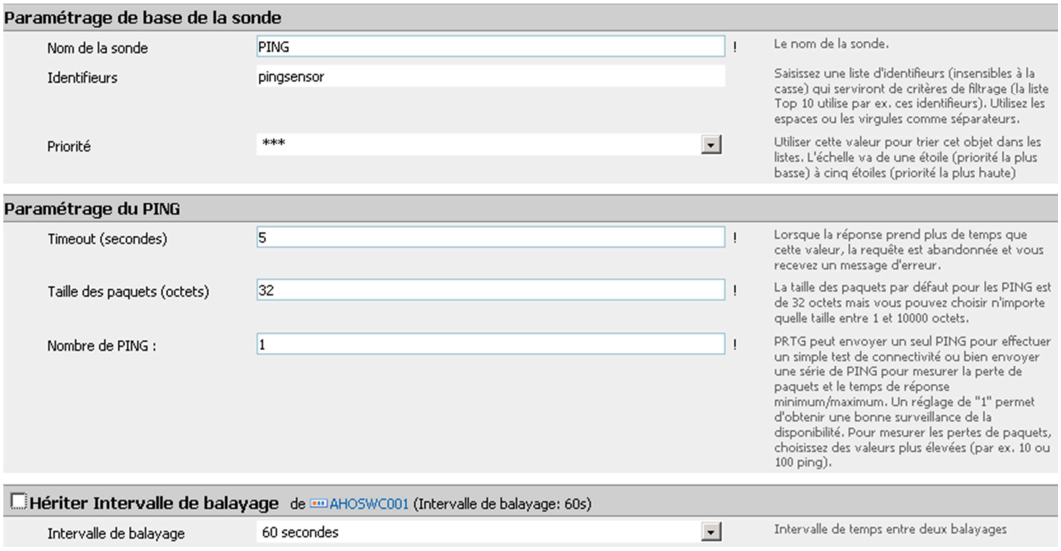


Figure 64 : Paramétrage d'une sonde

Une fois la sonde créée, on peut modifier ses paramètres en cliquant sur la sonde, puis sur « Paramètres ». On peut ainsi modifier le canal primaire qui permet d'être la valeur principale du graphique créé à partir des valeurs récupérées.

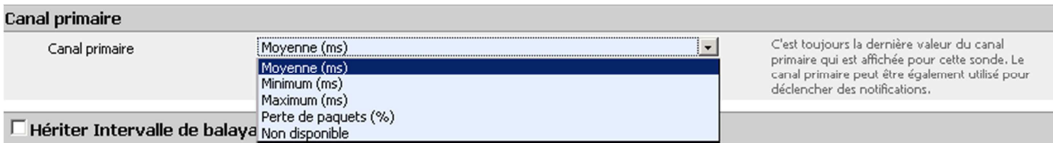


Figure 65 : Choix du canal primaire d'une sonde

Dans l'onglet « Notifications » de la sonde, il est possible d'activer les alertes en fonction de différents critères (modification d'état, seuil de bande passante atteint, volume de données atteint, seuil atteint ou encore fichier modifié).

Pour activer l'alerte, il faut cliquer sur « ajouter un déclenchement », puis choisir la condition de l'envoi de l'alerte ainsi qu'une plage horaire pour recevoir les alertes.

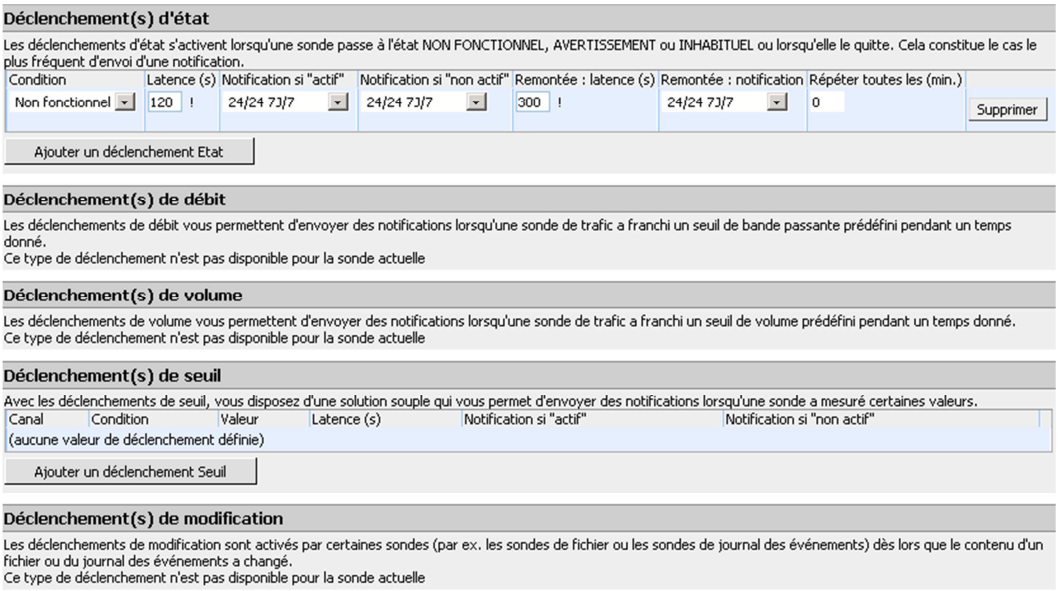


Figure 66 : Paramétrage du déclenchement d'une alerte

La solution est complètement opérationnelle lorsque toutes les sondes ont été paramétrées.

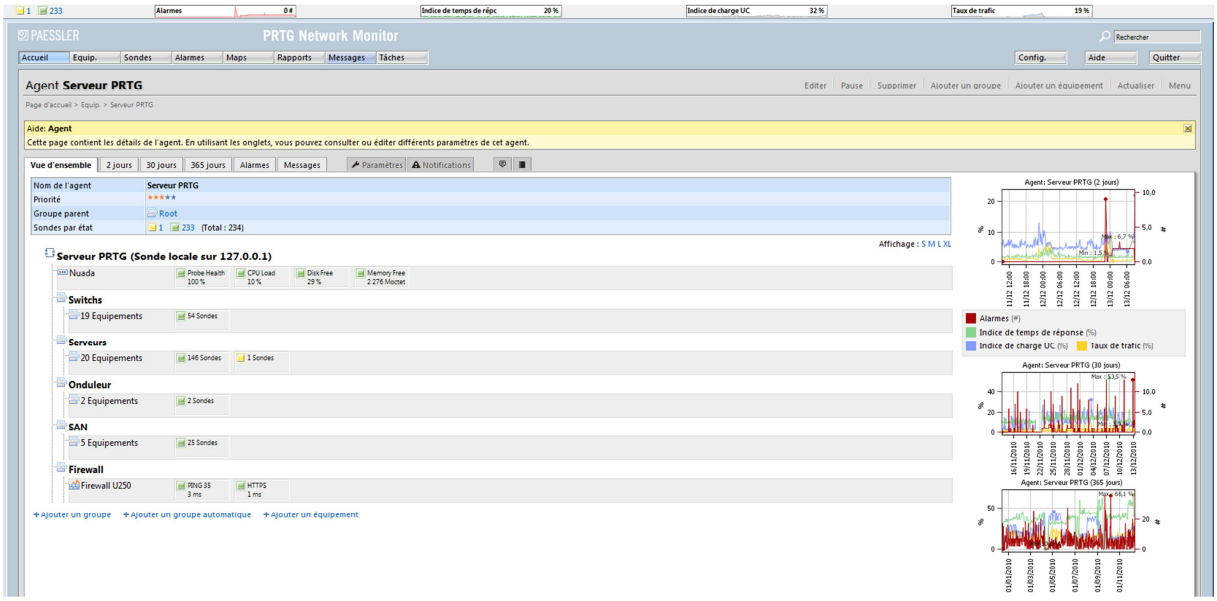


Figure 67 : Vue générale des sondes par catégories

4.2 Choix des sondes

Il est important de bien choisir ses sondes afin d'avoir une vision pertinente et globale du système d'information. Chaque sonde doit avoir une utilité et doit permettre d'expliquer un problème. Les équipements réseaux et les serveurs n'ont pas besoin des mêmes sondes.

4.2.1 Sondes pour les équipements réseaux

Les équipements réseaux ont des sondes en commun, appelées sondes indispensables, quel que soit le type d'équipement. Il existe également des sondes optionnelles qui permettent d'avoir des informations propres à un équipement précis ou qui peuvent donner des informations intéressantes sur des problèmes rencontrés.

4.2.1.1 Sondes indispensables

Tous les équipements réseaux ont des sondes communes car elles permettent de surveiller le bon fonctionnement de l'équipement. C'est le cas des sondes suivantes :

Ping : Cette sonde est indispensable à tous les équipements car elle permet de dire si l'équipement est opérationnel ou non. Cette sonde interroge toutes les 30 secondes l'équipement pour vérifier son état de fonctionnement. On a donc mis une sonde Ping sur tous les équipements réseaux avec une remontée d'alerte si l'équipement n'est plus fonctionnel.

Charge processeur : La surveillance de l'utilisation du processeur d'un équipement réseau permet de déceler un problème sur l'équipement lui-même ou sur une anomalie réseau touchant cet équipement. Une trop forte sollicitation de l'équipement peut entrainer une diminution des performances. Une alerte est envoyée lorsque l'équipement atteint 80% de sa charge processeur.

Charge mémoire : La surveillance de la mémoire permet également d'anticiper un problème réseau. Une trop forte charge entraine une diminution des performances. Pour cette raison, il y a une alerte qui est envoyée lorsque la charge mémoire atteint 80%.

4.2.1.2 Sondes optionnelles

Les équipements réseaux peuvent avoir des sondes optionnelles. Ces sondes n'ont pas forcément besoin d'être associées avec une remontée d'alerte. Elles peuvent permettent d'apporter des explications à des problèmes.

Trafic d'un port : Cette sonde permet de surveiller la bande passante d'un port d'un équipement. Cela permet de surveiller l'état du réseau et d'éviter l'engorgement dans certaines zones. Nous avons donc mis en place une surveillance uniquement des ports qui relient l'équipement à un autre équipement réseau ou à un serveur. Ainsi, on peut visualiser l'utilisation globale de la bande passante du réseau.

Surveillance d'un port : La sonde Port surveille la disponibilité d'un port sur un équipement réseau. Nous avons mis en place une sonde sur le port 443 (HTTPS) sur le firewall permettant ainsi de vérifier que ce port est accessible pour le push-mail.

4.2.2 Sondes pour les serveurs

Tous les serveurs ont des sondes communes qui sont considérées comme critiques. Ils ont également tous des sondes que l'on peut considérer comme optionnelles car elles ne sont pas indispensables. Elles permettent juste d'apporter de l'information sur le serveur, permettant d'expliquer ou d'apporter des éléments d'explication à une panne. Cependant, chaque serveur ayant des fonctions différentes possède des sondes spécifiques permettant de surveiller un élément précis du serveur. Toutes les sondes peuvent utiliser le protocole SNMP pour interroger le serveur mais certaines d'entre elles peuvent également utiliser la technologie WMI s'il s'agit d'un serveur fonctionnant sous Windows.

4.2.2.1 Sondes indispensables

Les sondes indispensables aux serveurs permettent de surveiller le fonctionnement général du serveur. Les sondes indispensables sont :

Ping : Cette sonde est indispensable à tous les serveurs. Elle permet de signaler qu'un équipement est opérationnel ou non. Une sonde a donc été placée pour chaque serveur. Cette sonde vérifie toutes les 30 minutes que le serveur est joignable. Une alerte est envoyée si le serveur n'est plus opérationnel.

Charge processeur : Cette sonde permet de vérifier la charge processeur du serveur. En cas de trop forte charge, le serveur devient instable et ses performances diminuent. Une sonde a été placée sur tous les serveurs. Une alerte est envoyée lorsque la valeur de sa charge processeur atteint 80%.

Charge mémoire : La surveillance de la mémoire permet d'anticiper un arrêt du serveur. La trop forte consommation en mémoire dégrade considérablement les performances du serveur. Pour cette raison, tous les serveurs sont équipés de cette sonde. Une alerte est envoyée lorsque la charge mémoire atteint également 80%.

Espace disque libre : Cette sonde mesure l'espace disque libre sur toutes les partitions du serveur. Cela permet d'éviter une saturation d'une partition pouvant entraîner l'arrêt d'un service, voir même du serveur s'il s'agit de la partition système. Une alerte est envoyée lorsqu'il ne reste plus que 20% d'espace disque sur un serveur.

4.2.2.2 Sondes optionnelles

Il est également possible de mettre en place des sondes uniquement dans un but informatif. Ces sondes permettent simplement d'apporter éventuellement des explications à une panne.

Trafic carte réseau : Cette sonde a pour but de surveiller l'utilisation de la bande passante de la carte réseau. Cela permet de constater s'il n'existe pas un problème d'accès au serveur provoquant un ralentissement.

Charge du fichier Pagefile : La surveillance de ce fichier permet de savoir si le serveur manque de mémoire vive et si nécessaire d'étendre la mémoire vive du système.

4.2.2.3 Sondes spécifiques

Chaque serveur possède une spécificité différente de celle des autres. Ils n'ont pas tous les même logiciels, les mêmes fonctions, ni les même services. C'est pour cela qu'il existe d'autres types de sondes.

Surveillance d'un service : Cette sonde permet du surveiller un service précis sur un serveur. Certains logiciels s'appuient sur des services pour fonctionner. En cas d'arrêt d'un service, une alerte est envoyée s'il s'agit d'un service critique. Nous avons mis en place une

surveillance de certains services, comme le modem qui assure le transfert des facturations, car leurs arrêts empêchent le bon fonctionnement de l'application associée.

Surveillance d'un port : Cette sonde permet de s'assurer que le serveur reste joignable sur un port précis. Cette surveillance ne devient critique que si l'utilité de ce port est critique.

Surveillance d'un fichier : Il est parfois nécessaire de s'assurer qu'un fichier n'est pas modifié. Pour cela, une sonde peut être placé dessus afin d'être alerté d'une modification ou d'une suppression de ce fichier.

Surveillance d'un dossier : Cette sonde permet de surveiller les modifications et suppressions d'un répertoire et de ses sous-répertoires. Nous avons mis en place une surveillance sur les répertoires des fichiers de mise à jour du logiciel métier car l'éditeur n'informe pas de leurs mises à disposition sur les serveurs. Cela nous permet d'être plus réactifs pour mettre en place ces mises à jour qui sont souvent importantes.

Surveillance du service de bureau à distance : Cette sonde nous permet d'être alertés de l'impossibilité de nous connecter au serveur par le système du bureau à distance. La prise en main à distance sur les serveurs se fait la plupart du temps grâce à ce système. Nous avons placé une sonde sur tous les serveurs mais plus particulièrement sur les deux serveurs qui ont comme fonction d'être des serveurs TSE. Ces serveurs permettent aux utilisateurs d'accéder au logiciel métier grâce au système de bureau à distance. Si ce service ne fonctionne plus, l'application métier n'est plus accessible.

Surveillance d'un serveur web : Cette sonde vérifie que le serveur web fonctionne. Elle peut également surveiller l'accès à une page web. Nous avons mis en place cette sonde sur les serveurs hébergeant le logiciel du dossier patient informatique qui est en interface web. La sonde vérifie que l'adresse de la page web est accessible. Une alerte est envoyée en cas d'indisponibilité de la page web.

Surveillance d'un serveur DNS : La sonde surveille le fonctionnement du DNS sur le serveur. Si le DNS ne fonctionne plus, la résolution de nom ne se fait plus. Une sonde a été positionnée sur les deux serveurs DNS de la clinique.

Surveillance d'un serveur FTP : Cette sonde permet de vérifier le fonctionnement du serveur FTP. En cas d'arrêt, il devient impossible de déposer des fichiers. Cette sonde a été

positionnée sur un serveur qui utilise le serveur FTP pour recevoir des fichiers de laboratoires. Si le serveur FTP ne fonctionne plus, cela engendre des problèmes de facturation.

Surveillance d'un serveur SQL : Cette sonde permet de vérifier le bon fonctionnement d'un serveur SQL. Une sonde a été positionnée sur les deux serveurs de bases de données du dossier patient informatisé. En cas d'arrêt des deux serveurs, le dossier patient informatisé n'est plus joignable. Une alerte par mail a donc été positionnée sur cette sonde.

Surveillance d'un serveur Exchange : La sonde permet d'avoir des informations sur le serveur de messagerie Exchange. On peut ainsi connaître son fonctionnement. Une sonde a été placée sur le serveur de messagerie afin d'obtenir le nombre de messages en attente d'envoi. Si le nombre est supérieur à 5, une alerte est déclenchée signalant que l'envoi des mails ne fonctionne plus.

4.3 Mise en place du push-mail

4.3.1 Paramétrage du serveur de messagerie

Pour mettre en place le push-mail avec la technologie Microsoft Direct Push, il faut que le serveur de messagerie soit au minimum Microsoft Exchange Server 2003 SP2.

La clinique ayant déjà la version minimum requise peut mettre en place le push-mail sans avoir besoin de faire une mise à jour du logiciel de messagerie.

4.3.1.1 Création d'un certificat

Pour que le serveur soit accessible depuis internet sur le port 443 en HTTPS, il faut lui attribuer un certificat. Ce certificat associe une clé publique à un serveur afin d'en assurer la validité. Pour cela, il existe une méthode payante et une méthode gratuite pour en obtenir un. La méthode payante consiste à faire une demande auprès d'un organisme appelé autorité de certification. Ce certificat a pour principal but d'assurer la sécurité des échanges avec des utilisateurs anonymes. La méthode gratuite consiste à générer soi-même un certificat signé par un serveur local ayant comme usage principal un usage interne. Ce certificat n'est pas reconnu par les autorités de certification.

La clinique a privilégié la création d'un certificat en interne afin de limiter les dépenses. Pour cela, il faut que les « Services de certificats » soient installéssur un serveur de l'entreprise, afin de créer une autorité de certification.

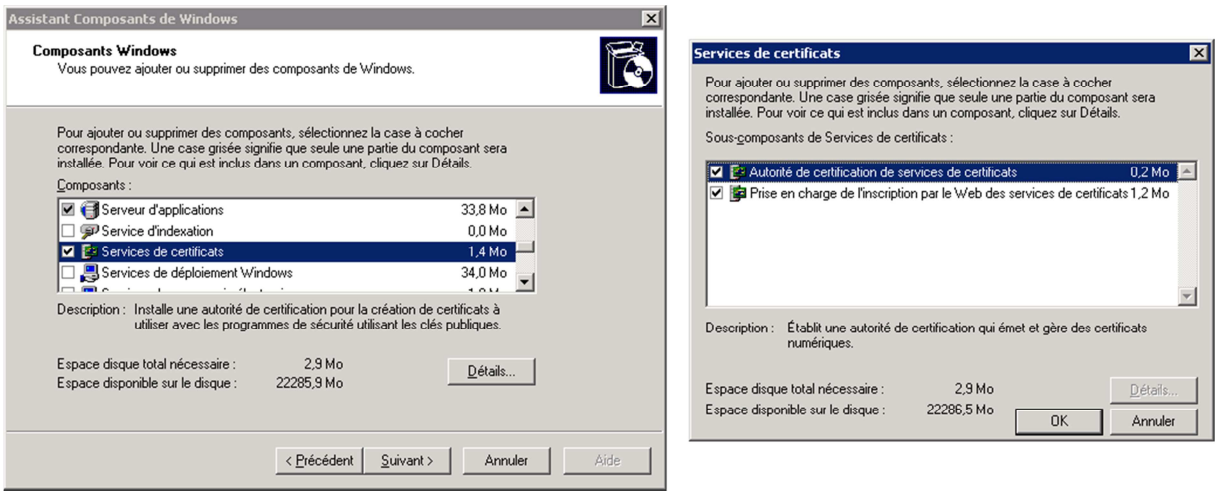


Figure 68 : Présentation des services de certificats

La clinique possède déjà une autorité de certification avec un certificat racine de cette autorité de certification.

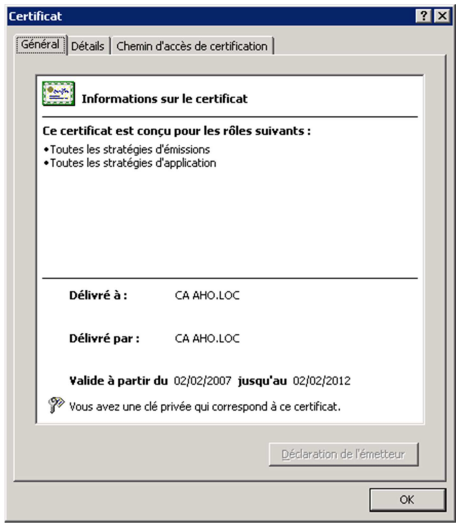


Figure 69 : Certificat racine de l'entreprise

La mise en place du certificat est décrite dans l'annexe 12 (Sécurisation d'un serveur web).

Normalement, le nom du certificat correspond au nom du serveur. Mais pour notre cas, le nom doit correspondre à l'adresse IP publique de l'entreprise car le téléphone compare l'adresse IP saisie pour joindre le serveur avec le nom du certificat. Si le téléphone n'arrive pas à faire une correspondance entre le nom du certificat et une adresse IP, il refuse la connexion. C'est pour cela que le certificat du serveur possède une adresse IP publique plutôt qu'un nom de serveur ou une adresse IP privée.

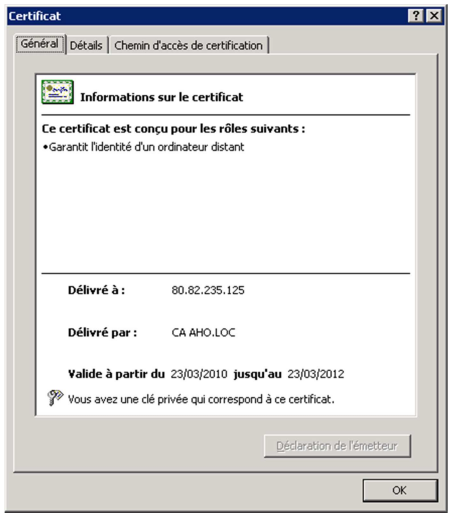


Figure 70 : Préparation d'une demande de certificat

4.3.1.2 Paramétrage du serveur web

La technologie Microsoft Direct Push s'appuie sur ActiveSync Exchange. Afin de pouvoir dialoguer avec des téléphones, le serveur de messagerie utilise le serveur web de Microsoft, appelé IIS (Internet Information Services). Pour que les échanges de données entre le téléphone et le serveur web se déroulent bien, il faut créer un nouveau répertoire virtuel que l'on peut appeler « exchange-oma ». Le paramétrage est décrit dans la « méthode 2 » de l'annexe 13 (Configuration d'Exchange ActiveSync).

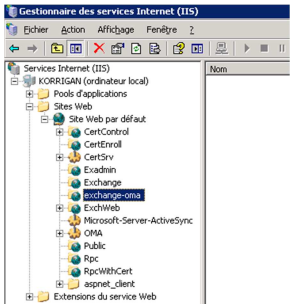


Figure 71 : Paramétrage du Gestionnaire des services Internet

4.3.1.3 Activation du push-mail sur le serveur

Pour que le push-mail fonctionne, il faut activer les services mobiles dans les paramétrages d'Exchange. Pour cela, il faut lancer le « Gestionnaire système Exchange », développer « Paramètres globaux », afficher les propriétés de « Services mobiles » et cocher les cases « Activer la synchronisation initiée par l'utilisateur » et « Activer la poussée directe sur HTTP ».

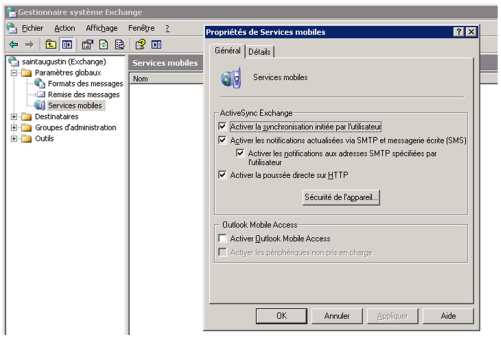


Figure 72 : Paramétrage du Gestionnaire système Exchange

Une fois l'activation faite, il est important de vérifier que les services mobiles soient bien activés pour tous les utilisateurs qui en ont besoin. Par défaut, ils sont tous activés. Pour cela,

il faut lancer « Utilisateurs et ordinateurs Active Directory », afficher les propriétés d'un utilisateur et aller dans l'onglet « Fonctionnalités Exchange ».

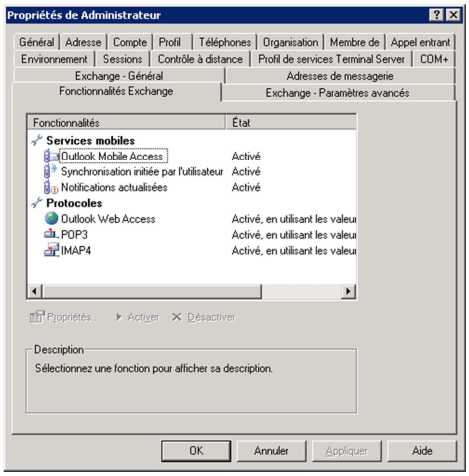


Figure 73 : Paramétrage d'un utilisateur dans Active Directory

4.3.2 Paramétrage du firewall

La technologie Microsoft Direct Push utilise le port TCP 443. Pour cela il faut autoriser les échanges entre les téléphones et le serveur de messagerie sur ce port.

La clinique est équipée d'un Firewall Netasq qui utilise déjà le port 443 pour effectuer des connexions sécurisées à la clinique en VPN-SSL (Virtual Private Network-Secure Sockets Layer). Pour contourner le problème, il faut créer une nouvelle adresse IP publique qui doit correspondre au nom du certificat du serveur de messagerie et rediriger les échanges dans les deux sens sur cette nouvelle adresse IP. Le serveur de messagerie s'appelle Korrigan. AHO_Publique_2 a comme IP 80.82.235.125.

Figure 74 : Règle de translation sur le firewall

Ensuite, il faut sécuriser ces échanges en mettant une règle de filtrage n'autorisant que les échanges sur le port TCP 443. Ainsi, seuls les messages en HTTPS sont autorisés.

Figure 75 : Règle de filtrage sur le firewall

4.3.3 Paramétrage du téléphone

Pour pouvoir configurer un compte de messagerie relié au serveur de messagerie Microsoft Exchange Server de l'entreprise en push-mail sur un iPhone, il faut ajouter un compte Exchange sur le téléphone. Dans le champ « Adresse », il faut saisir l'adresse IP publique de l'entreprise prévu pour les échanges en HTTPS. Dans le champ « Serveur », il faut également renseigner la même adresse IP publique pour que cela fonctionne.

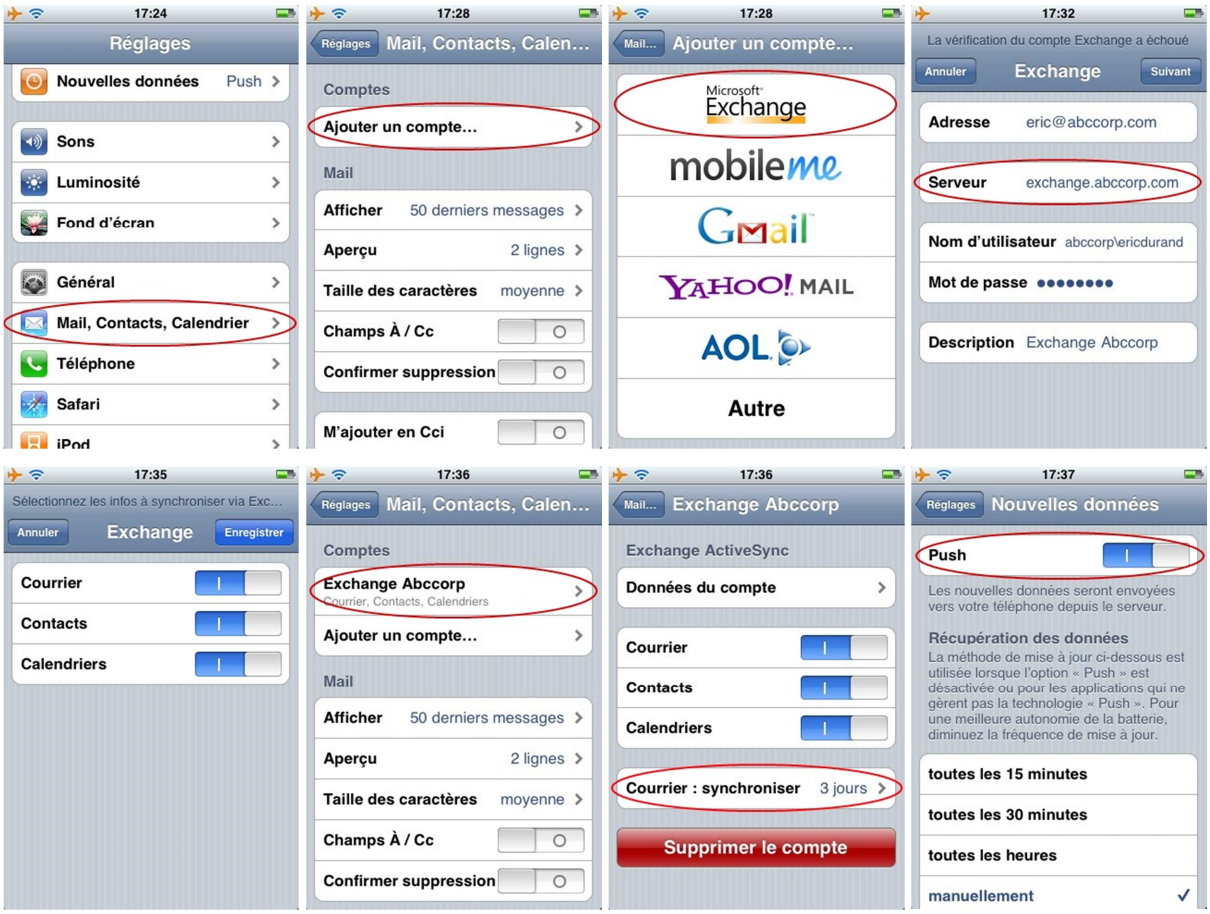


Figure 76 : Paramétrage du push-mail sur un iPhone (LE YAVANC, 2009)

Une fois la configuration effectuée, le téléphone récupère les nouvelles données automatiquement.

4.4 Suivi du projet

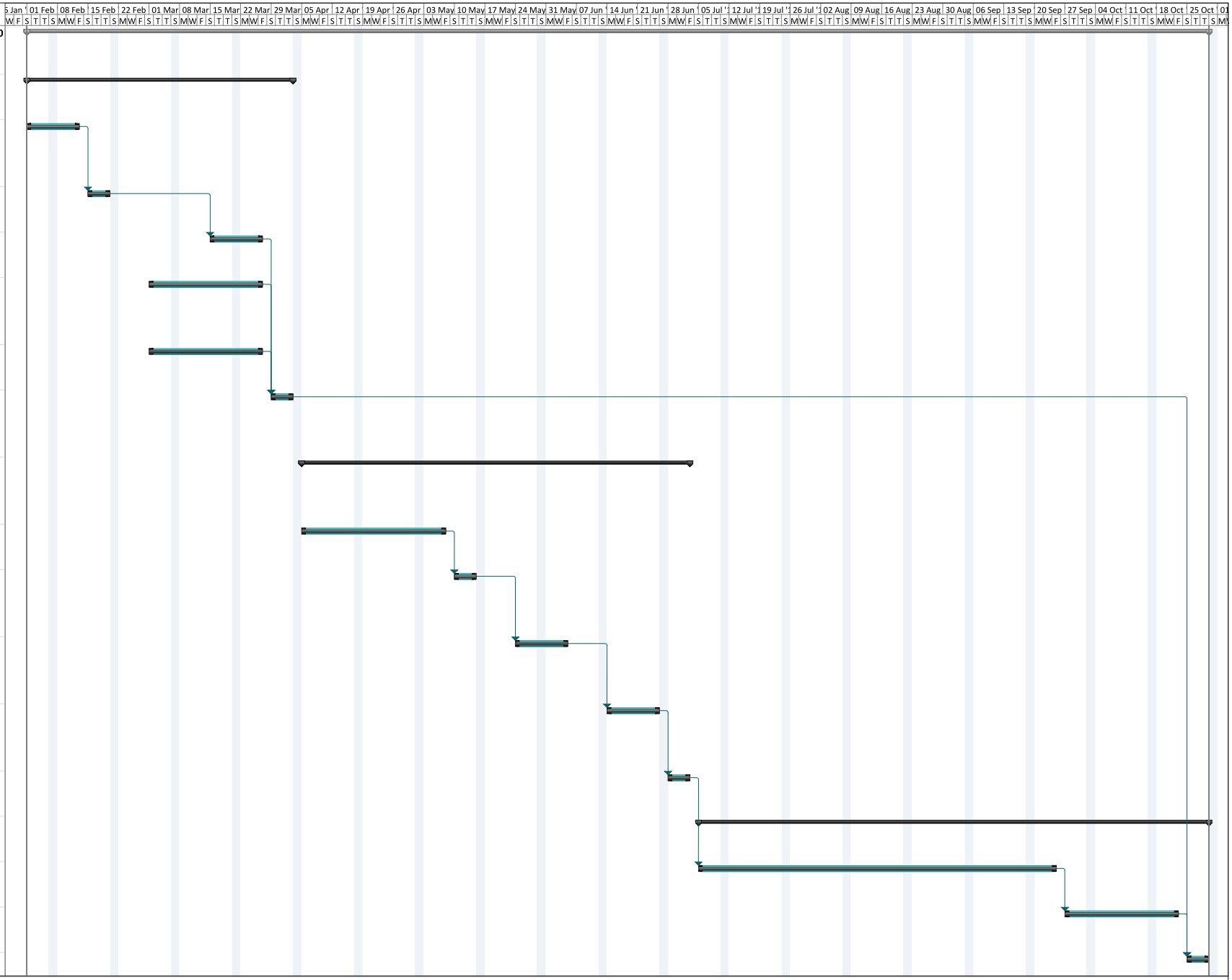
Le projet s'est déroulé de février 2010 à octobre 2010. Il s'est décomposé en trois parties principales.

La première étape a consisté à mettre en place une solution de push-mail afin de pouvoir proposer à des responsables d'avoir leurs mails sur un téléphone. Cette étape s'est déroulée de février à mars. Ceci a permis de vérifier le bon fonctionnement du push-mail dans le cadre de la clinique.

La deuxième étape a consisté à installer le logiciel de supervision. Pour cela, il a fallu étudier différents logiciels et d'en choisir un adapté aux attentes. Cette étape s'est déroulée d'avril à juillet.

Enfin, la troisième étape a consisté à mettre en place les sondes et les alertes. Cette étape s'est déroulée de juillet à octobre. Le déroulement du projet est visible sur le diagramme de la page suivante.

ID	Task Name	Duration	Start	Finish
0	**Supervision de réseau**	**195 days**	**Mon 01/02/10**	**Fri 29/10/10**
1	**Mise en place du push-mail**	**45 days**	**Mon 01/02/10**	**Fri 02/04/10**
2	Choix de la technologie push-mail	10 days	Mon 01/02/10	Fri 12/02/10
3	Choix des téléphones	5 days	Mon 15/02/10	Fri 19/02/10
4	Paramétrage des téléphones	10 days	Mon 15/03/10	Fri 26/03/10
5	Paramétrage du serveur de messagerie	20 days	Mon 01/03/10	Fri 26/03/10
6	Paramétrage du Firewall	20 days	Mon 01/03/10	Fri 26/03/10
7	Tests du fonctionnement du push-mail	5 days	Mon 29/03/10	Fri 02/04/10
8	**Mise en place du logiciel de supervision**	**65 days**	**Mon 05/04/10**	**Fri 02/07/10**
9	Choix du logiciel de supervision	25 days	Mon 05/04/10	Fri 07/05/10
10	Choix de la plateforme matérielle	5 days	Mon 10/05/10	Fri 14/05/10
11	Préparation de la plateforme matérielle	10 days	Mon 24/05/10	Fri 04/06/10
12	Installation du logiciel de supervision	10 days	Mon 14/06/10	Fri 25/06/10
13	Paramétrage du logiciel	5 days	Mon 28/06/10	Fri 02/07/10
14	**Paramétrage des sondes et alertes**	**85 days**	**Mon 05/07/10**	**Fri 29/10/10**
15	Mise en place des sondes	60 days	Mon 05/07/10	Fri 24/09/10
16	Paramétrage des alertes	20 days	Mon 27/09/10	Fri 22/10/10
17	Tests d'alertes	5 days	Mon 25/10/10	Fri 29/10/10



Project: Supervision de réseau

Task	Summary	External Milestone	Inactive Summary	Manual Summary Rollup	Finish-only		
Split	Project Summary	Inactive Task	Manual Task	Manual Summary	Deadline		
Milestone	External Tasks	Inactive Milestone	Duration-only	Start-only	Progress		

4.4.1 Problèmes rencontrés

Pendant la mise en place du projet, quelques problèmes sont apparus.

Le problème majeur a été le paramétrage du firewall. Le push-mail ne fonctionnant qu'avec le port 443 (HTTPS), il devenait incompatible avec le firewall qui utilise ce port pour faire fonctionner le VPN-SSL. Comme le VPN-SSL est entièrement géré par le firewall, il est impossible de le faire fonctionner sur un autre port. Il a fallu trouver une solution pour faire cohabiter le VPN-SSL avec le push-mail. La mise en place d'une deuxième adresse IP publique a permis de résoudre le problème. Pour cela, une règle spécifique a été créée dans le firewall afin de rediriger les flux en HTTPS provenant du serveur de messagerie vers cette nouvelle adresse IP publique. Cette règle est visible sur la figure 55 (Règle de translation sur le firewall).

Un deuxième problème est apparu au bout d'un certain temps de fonctionnement. Les téléphones n'arrivaient plus à se connecter au serveur de messagerie. Le redémarrage du firewall permettait de refaire fonctionner la synchronisation des téléphones avec le serveur de messagerie. Un événement d'avertissement a été enregistré dans le journal des événements d'application sur le serveur de messagerie. Cet événement d'avertissement portait le numéro 3033. Ce problème est expliqué dans un article de la base de connaissance de Microsoft sous la référence KB (Knowledge Base) 905013. Cet article est consultable en annexe 14 (Evénement d'avertissement Microsoft numéro 3033).

Type d'événement : Avertissement
Source de l'événement : Server ActiveSync
Catégorie de l'événement : Aucune
ID de l'événement : 3033
Date :
Heure :
Utilisateur :
Ordinateur :
Nom_ordinateur
Description :
La moyenne des intervalles d'interrogation les plus récents [200] utilisés par les clients est inférieure ou égale à [9]. Assurez-vous que votre configuration de pare-feu est configurée pour fonctionner correctement avec la technologie Exchange ActiveSync et Direct Push. Plus précisément, assurez-vous que votre pare-feu est configuré de sorte que les demandes à Exchange ActiveSync n'expirent pas avant de pouvoir être traitées.

Ce problème peut se produire si le pare-feu n'a pas été configuré pour conserver les requêtes HTTP(S) actives plus longtemps que l'intervalle d'interrogation minimum configuré sur le serveur Exchange Server 2003 SP2. Par défaut, l'intervalle d'interrogation minimum auquel le serveur Exchange déclenche cet événement est de neuf minutes.

Figure 77 : Evénement d'avertissement numéro 3033 (Microsoft Corporation, 2007a)

Afin de résoudre le problème, nous avons mis à jour le firewall puis vérifié les règles de paramétrage des connexions HTTPS du firewall et la durée de vie des requêtes HTTPS. Ce problème n'est plus réapparu depuis la mise à jour du firewall.

Un nouveau problème est apparu plusieurs mois après la mise à jour du firewall. Les téléphones ne pouvaient également plus se synchroniser. Le redémarrage du firewall n'a rien changé, en revanche le redémarrage du serveur de messagerie a permis de résoudre le problème mais seulement pour quelques jours. Le problème est à nouveau survenu et il a à nouveau été résolu par le redémarrage du serveur. Un événement d'avertissement a été enregistré dans le journal des événements d'application sur le serveur de messagerie. Cet événement d'avertissement portait le numéro 3031. Ce problème est expliqué dans un article de la base de connaissance de Microsoft sous la référence KB 817379. Cet article est consultable en annexe 13 (Configuration d'Exchange ActiveSync).

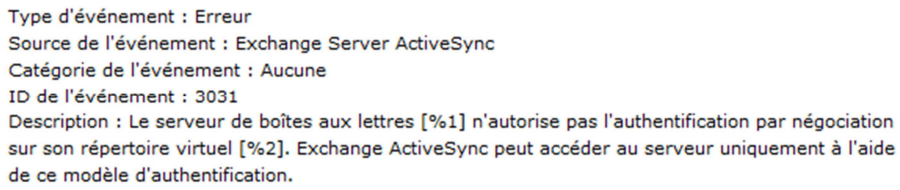

Type d'événement : Erreur
Source de l'événement : Exchange Server ActiveSync
Catégorie de l'événement : Aucune
ID de l'événement : 3031
Description : Le serveur de boîtes aux lettres [%1] n'autorise pas l'authentification par négociation sur son répertoire virtuel [%2]. Exchange ActiveSync peut accéder au serveur uniquement à l'aide de ce modèle d'authentification.

Figure 78 : Evénement d'avertissement numéro 3031 (Microsoft Corporation, 2007b)

Le problème a été résolu en suivant la méthode de résolution de la panne de l'article KB 817379. Nous avons suivi la « méthode 2 » de ce document.

4.4.2 Bilan de l'installation

N'ayant aucun serveur disponible au moment de l'installation, le logiciel de supervision a été dès le départ installé sur une machine virtuelle fonctionnant sous Windows 2003 serveur. Cette machine virtuelle a été placée sur un serveur physique qui n'était plus utilisé car l'infrastructure de virtualisation n'avait pas encore été achetée.

N'ayant également pas de licence Windows 2003 Open, permettant de déplacer la licence sur un autre serveur physique, nous avons dû utiliser la licence OEM (Original Equipment Manufacturer) qui existait pour ce serveur. La licence OEM est associée au serveur physique.

Au moment de l'installation, le logiciel VMware Data Recovery, permettant de faire les sauvegardes des machines virtuelles, n'était pas encore en place. Le logiciel de sauvegarde permettant de sauvegarder les serveurs physiques n'avait également pas de licence d'avance pour pouvoir sauvegarder cette machine virtuelle. Faute de pouvoir effectuer des sauvegardes régulières nous avons créé une image de cette machine virtuelle afin de pouvoir la restaurer en cas de besoin.

4.4.3 Evolutions possibles

Il est prévu de faire évoluer la solution en positionnant la machine virtuelle sur la nouvelle infrastructure de virtualisation utilisant VMWare. La machine virtuelle pourra ainsi être positionnée sur le nouveau SAN utilisant la technologie Data Core qui a comme avantage d'être répliqué en temps réel dans une deuxième salle, afin de pouvoir faire de la haute disponibilité. Ainsi, la machine virtuelle pourra être sauvegardée gratuitement avec le logiciel VMware Data Recovery.

En ce qui concerne la licence Microsoft associée au serveur physique utilisé dans la machine virtuelle, il existe trois possibilités d'évolution. La première évolution serait de migrer la licence OEM vers une licence Open. La deuxième consisterait à réinstaller toute la machine virtuelle avec une licence Open. Et la troisième serait de positionner la machine virtuelle avec cette licence OEM en réservant une licence Open pour ce serveur afin d'avoir toujours un nombre de licences Microsoft achetées en version Open équivalent au nombre de licences utilisés.

Enfin, les données concernant le dossier patient circule en claire sur le réseau. Afin de préserver la confidentialité de ces informations, il pourrait être envisagé un chiffrement des données.

Conclusion

La généralisation des systèmes d'information au sein des entreprises a poussé le ministère de la santé à contraindre les établissements de santé à s'équiper d'un logiciel, appelé dossier patient informatisé, permettant de dématérialiser les dossiers papiers pour faciliter le suivi médical.

L'ensemble du personnel de la clinique Saint-Augustin doit désormais pouvoir avoir accès en permanence aux données contenues dans le dossier patient. Or, la forte utilisation des systèmes d'information peut engendrer des ralentissements réseau et une saturation des espaces de stockage.

Il était donc nécessaire de mettre en place une solution de supervision de réseau afin d'anticiper ou de résoudre au plus vite les dysfonctionnements et les incidents survenant sur le système d'information. Ainsi, le service informatique peut intervenir rapidement sur les pannes pour ne pas paralyser le fonctionnement des services de soin qui sont au cœur de l'activité de la clinique. En effet, si le dossier patient n'est plus accessible les malades ne peuvent plus recevoir les soins appropriés.

Pour répondre à ces problématiques propres à la clinique et, en complément de l'installation du logiciel du dossier patient, le service informatique a donc dû étudier des solutions de supervision de réseau et de remontée d'alertes soit par mail, soit sur téléphone grâce à la technologie du push-mail.

Une contrainte particulière est apparue : les données étant confidentielles, les envois des informations contenues dans le dossier patient devaient donc pouvoir être effectués via des liaisons sécurisées.

La mise en place de cette solution m'a permis d'approfondir mes connaissances sur le protocole SNMP et de découvrir différentes solutions de supervision. La supervision est devenue un enjeu important pour les entreprises en raison du développement croissant des systèmes d'information.

Annexes

Table des annexes

Annexe 1 : Présentation de Nagios XI

(Nagios Enterprises, 2010)

Nagios XI – Product Overview

The Industry Standard in IT Infrastructure Monitoring

Nagios® XI™ is an enterprise-class solution that provides organizations with extended insight into their IT infrastructure before problems affect critical business processes.

Nagios XI monitors your entire IT infrastructure to ensure systems, applications, services, and business processes are functioning properly. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affect business processes, end-users, or customers. With Nagios you'll never be left having to explain why an unseen infrastructure outage hurt your organization's bottom line.

Nagios XI is a complete IT infrastructure monitoring and alerting system providing:

- **Comprehensive IT Infrastructure Monitoring:** Provides monitoring of all mission-critical infrastructure components – including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house applications, services, and systems.

- **Visibility:** Provides a central view of your entire IT operations network and business processes. Powerful dashboards provide at-a-glance access to powerful monitoring information and third-party data. Views provide users with quick access to the information they find most useful.

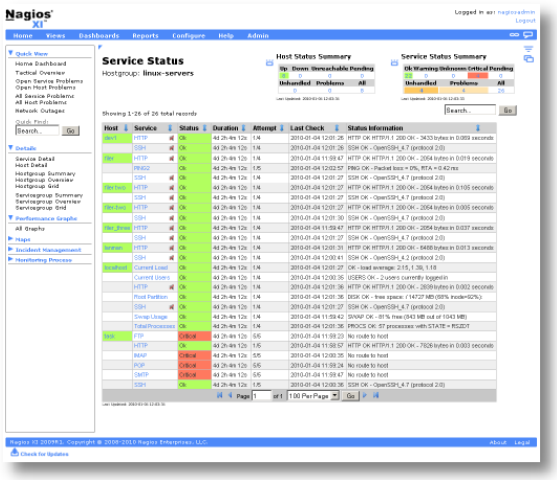
- **Awareness:** Alerts are sent to IT staff, business stakeholders, and end users via email or mobile text messages, providing them with outage details so they can start resolving issues immediately.

- **Proactive Planning:** Automated, integrated trending and capacity planning graphs allow organizations to plan for infrastructure upgrades before outdated systems catch them by surprise.

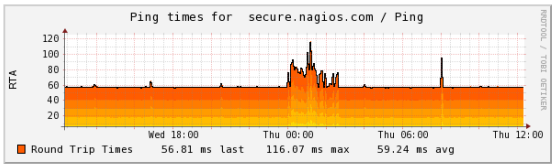
- **Customizability:** A powerful GUI provides for customization of layout, design, and preferences on a per-user basis, giving your customers and team members the flexibility they want.

- **Ease of Use:** Integrated web-based configuration interface lets admins hand out control of managing monitoring configuration, system settings, and more to end users and team members easily. Configuration wizards guide users through the process of monitoring new devices, services, and applications – all without having to understand complex monitoring concepts.

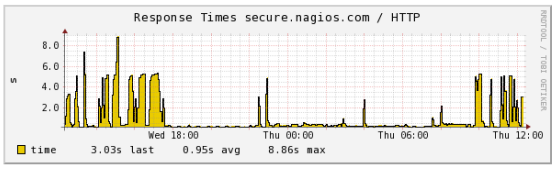
- **Multi-Tenant Capabilities:** Multi-user access to web interface allows stakeholders to view relevant infrastructure status. User-specific views ensures clients only see the infrastructure components they're authorized for. Advanced user management simplifies administration by allowing you to manage user accounts easily. Provision new user accounts with a few clicks and users automatically receive an email with their login credentials.



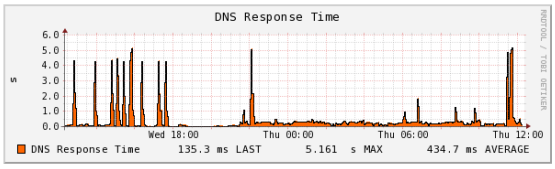
Ping



HTTP



DNS Resolution



- **Extendable Architecture:** Multiple APIs provide for simple integration with in-house and third-party applications. Hundreds of community-developed addons extend monitoring and native alerting functionality. Custom interface and addon development is available to tailor Nagios XI to meet your organization's exact needs.

Nagios Enterprises
Nagios Enterprises, LLC
P.O. Box 8154
Saint Paul, MN 55108
USA

US: 1-888-NAGIOS-1
Int'l: +1 651-204-9102
Fax: +1 651-204-9103

Web: www.nagios.com
Email: sales@nagios.com

Revision 1.9 – January, 2010

Solid Open Source Core

We designed Nagios XI to take full advantage of the power of well-known, rock-solid Open Source components. With over ten years of experience in the IT monitoring space, we know great software when we see it. Nagios XI extends the capabilities of award-winning components to bring you an unbeatable monitoring and alerting system at a great price.

Whats Included

- **Technical Support.** Nagios Enterprises offers priority tech support for Nagios XI via a special customer-only section of our support forum.
- **Perpetual License.** Purchase Nagios XI for a one-time fee and you can use it as long as you'd like.
- **Updates.** Customers will receive access to free updates and patches released for the major version of XI they purchase. For example, customers who purchase Nagios XI 2009R1 will receive free updates to 2009R1.1 and 2009R1.2. Customers who purchase maintenance contracts will receive free updates to future major releases of XI while their maintenance contract is in effect.
- **Upgrade Discounts.** Customers are eligible for special discount pricing when upgrading to future major releases.
- **Nagios Library.** Get a full year of access to the Nagios Library with special customer-only tutorials, videos, and tech tips.
- **Product Influence.** We listen to all Nagios users when determining our product roadmaps, but your feature requests will get bumped up to the front of the line. Tell us what you'd like to see and we'll build our future products to include the newest features you're looking for.
- **Builder Licensing Freedom.** Build extensions for Nagios XI using our APIs and you choose the license for your dashlet, wizard, or component: Open Source, proprietary, or public domain - the choice is yours.

More Information

For more information about Nagios products and services, or to order Nagios XI, contact us:

- Online: **www.nagios.com**
- Phone: **888-NAGIOS-1** or **+1 651-204-9102**
- Email: **inquiries@nagios.com**

Copyright © 2009 Nagios Enterprises. The information contained in this document is provided for informational purposes only. Nagios Enterprises makes no warranties, express or implied, in this summary. All prices shown are in US Dollars and are subject to change.

Annexe 2 : Présentation de Centreon

(MERETHIS, 2010)

Merethis

www.centreon.com

Le logiciel CENTREON

Centreon est un des logiciels de supervision sous licence GPL des plus flexibles et performants. Destiné à un large type de besoin de supervision, il s'adapte parfaitement à la mesure d'indicateurs systèmes, réseaux et applicatifs. Centreon regroupe un ensemble de fonctionnalités essentielles pour une gestion professionnelle de vos infrastructures critiques. Modulaire, il se conforme à vos besoins et vous permet d'étendre davantage la portée de ses fonctionnalités avec des modules complémentaires.

Monitoring temps réel

- Détection des pannes
- Détection de la disponibilité
- Définition avancée de seuils pour les alertes
- Interrogation active (pull)
- Réception passive de résultats (push)
- Réception de Trap SNMP
- Regroupement des informations par groupes d'hôtes
- Regroupement des informations par groupes de services
- Vues agrégées
- Agrégat de métrique de services (Meta service)
- Planification de temps d'arrêts programmés
- Prise en compte des problèmes par les utilisateurs
- Ajouts de commentaires
- Possibilité de parcourir les logs avec filtres de recherche
- Période et fréquence de collecte paramétrable

Traitement des performances

- Historisation des données de performance (MySQL)
- Affichage des données sous forme de graphiques RRDTool
- Comparaison des métriques / graphiques
- Affichage de graphiques de statuts (" Trends ")
- Suivi de l'évolution des données dans le temps
- Export CSV/XML
- Corrélation entre les données de performance et les états
- Modèles d'affichage des graphiques paramétrables
- Période de visualisation paramétrable

Configuration flexible

- Compatibilité Nagios 3
- Gestion de modèles de configurations
- Liaison entre les modèles d'hôtes et de services
- Gestion de bibliothèque de modèles applicatifs
- Héritages des modèles à n niveaux
- Collecte et gestion automatique des traps SNMP
- Définition de macro "sur mesure"
- Gestion de la topologie réseau
- Configuration atomique des indicateurs

Tableaux de bord

- Statistiques journalières basées sur la durée des états
- Statistiques journalières basées sur le nombre d'alertes
- Affichage des rapports par hôtes
- Affichage des rapports par groupes d'hôtes
- Affichage des rapports par groupes de services
- Période de visualisation paramétrable
- Export des rapports au format CSV
- Timeline interactive pour suivre l'évolution des rapports

Répartition de charge / haute disponibilité

- Possibilité d'éclatement de la charge de manière :
    - stratégique (sécurité) ;
    - géographique (WAN) ;
    - topologique.
- Mise en place de satellite "fail-over"
- Mise en place de satellite "pré-production"
- Possibilité de mise en place de haute disponibilité :
    - base MySQL répliquée ;
    - interface Web ;
    - moteur de supervision ;
    - graphiques / rapports.

Contrôle des accès utilisateurs

- Gestion des groupes d'accès
- Limitation d'accès aux pages de l'interface
- Limitation de visualisation des groupes d'hôtes
- Limitation de visualisation des groupes de services
- Limitation de visualisation des catégories de services
- Authentification LDAP
- Suivi des actions utilisateurs

Notification hiérarchisée

- Dépendances "métiers"
- Dépendances du réseau
- Pont vers des outils de ticketing (Request Tracker, etc)
- Notification mail, SMS ou autres
- Escalades hiérarchisées

Modularité

Possibilité d'intégrer et de développer des modules complémentaires :

- Centreon Syslog
- Centreon Disco
- Centreon WeatherMap
- Centreon NTOP
- Centreon Map
- Centreon CLAPI
- Centreon Business Activity Monitoring
- Centreon Business Intelligence
- Centreon Auto Deployment Tool

Consultez Merethis pour connaître l'ensemble des modules disponibles.

Pilotage

Possibilité de piloter Centreon en ligne de commande :

- ajout d'hôtes ;
- redémarrage de Nagios ;
- génération des configurations.

Chargement des configuration au format CSV ou NAGIOS.

Centreon s'adapte parfaitement à la mesure d'indicateurs systèmes, réseaux et applicatifs.

L'offre de formation complémentaire

Merethis propose des formations visant à découvrir le fonctionnement et la configuration des outils Centreon et Nagios.

Formation " Exploitation et analyse des résultats "

Objectifs : Utiliser le portail d'analyse Centreon et diagnostiquer l'origine d'un problème de disponibilité ou de performance par une analyse détaillée des mesures Centreon et Nagios. Connaître l'ensemble des actions possibles dans le cadre du traitement des remontées d'incidents.

Durée : 1/2 journée - Formation intra-entreprise uniquement.

Formation " Méthodologie et déploiement de la supervision "

Objectifs : Découvrir les logiciels Centreon et Nagios. Mettre en oeuvre de points de surveillance sur des ressources cibles hétérogènes. Créer une bibliothèque de modèles de supervision.

Durée : 3 jours - Formation Intra/Inter entreprises.

Formation " Administration de la plateforme de supervision "

Objectifs : Etre capable d'administrer et de maintenir en conditions opérationnelles la plateforme de supervision Centreon. Gérer l'installation de nouveaux serveurs de collecte, optimiser et ajuster les points de fonctionnement du moteur Nagios.

Durée : 2 jours - Formation Intra/Inter entreprises.

Formation " Développement de sondes Perl-SNMP "

Objectifs : Acquérir les bases du langage Perl, maîtriser l'API des sondes de supervision, connaître le protocole SNMP afin de maintenir et développer de nouvelles sondes de collecte.

Durée : 2 jours - Formation Intra/Inter entreprises.

Consulter Merethis afin de connaître les dates des prochaines sessions de formation sur ces modules.

L'offre de support Centreon et Nagios

Compléter l'utilisation de Centreon par l'acquisition de l'une de nos offres de support professionnel Merethis. Celles-ci vous garantissent une grande qualité de service dans la résolution des incidents liés à votre plate-forme Centreon et Nagios.

MERETHIS
12 avenue Raspail - 94250 Gentilly
R.C.S. Créteil 483 494 589
SARL au capital de 400 000 €

Tél : + 33 (0)1 49 69 97 12
Fax : + 33 (0)1 78 12 00 28
E-mail : commercial@merethis.com
Web : www.merethis.com

Annexe 3 : Présentation de Network Management Center

(Hewlett-Packard, 2010b)

HP Network Management Center

Brochure

Enhance network availability and performance, improve resource utilization, deliver compliant and more secure networks, and meet service level agreements.

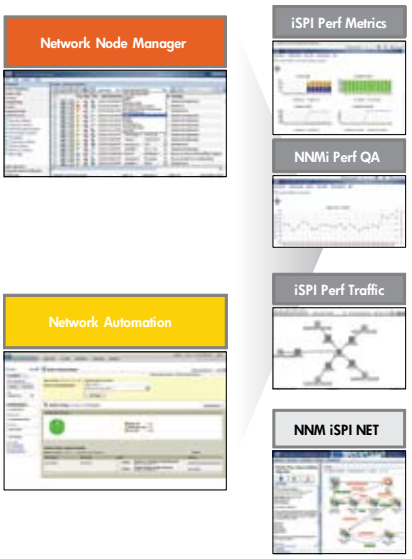
HP Network Management Center provides IT organizations with network management solutions that unify fault, availability, and performance capabilities with change, configuration, and compliance while automating the technology process workflow across these capabilities. This integrated approach, called automated network management (ANM), enables companies to reduce the cost of meeting service level agreements (SLAs), enhance network availability, and achieve compliant and hardened networks.

Meet your network management challenges

As the Internet era has evolved, IP networks have become essential enablers of business. Today's networks support unified communications, including email, IP telephony, and the media services that support revenue-generating transactions. Due to the strategic reliance on networks, companies cannot afford unplanned network downtime. Consequently, business requirements are now driving the operational objectives for network engineering and operations teams, including:

- Increasing revenue—enhancing network availability and performance
- Reducing expense—improving resource utilization (people and infrastructure)
- Reducing liability and risk—delivering compliant and secure networks
- Proving accountability—meeting and reporting on SLAs
- Managing change effectively and efficiently—without disruption

Automated Network Management (ANM)
Complete control of your infrastructure



Fault and availability monitoring
Improve network availability with a model based network management solution

Change, configuration, and compliance
Comprehensive network automation spanning all tasks from provisioning and change management to compliance enforcement and reporting

Performance monitoring
Increase operator productivity and efficiency and reduced MTTR

Engineering Toolset
Automate common network engineering and network tool administrators tasks

Network engineering and operations teams face significant challenges in their pursuit of these objectives. First of all, they are tasked with managing a moving target. Today's networks are large, complex, and constantly changing. Networking technology now includes virtualization technologies, such as virtual LANs and router redundancy protocols, but it has also expanded to encompass the discovery and monitoring of virtual servers and the applications they are hosting. New network services are running over today's IP networks, such as IP multicast, Multiprotocol Label Switching (MPLS), and IP telephony. And, through mergers and acquisitions, a company's network can change substantially—overnight. All of this must be managed effectively, but keeping up with the new technology, controlling incident and fault management, and dealing with fluctuating network size can consume valuable time and resources.

Also creating challenges are incomplete and/or ineffective management solutions. For example, many companies still rely on manual processes to accomplish various network engineering and operations tasks (that is, network change and configuration, fault isolation, or root-cause analysis). Furthermore, companies may have cumbersome management frameworks consisting of a conglomeration of disparate point tools. This can contribute to contention between groups. And incomplete and ineffective management frameworks consume technology staff time as they work to plug the holes and fill the gaps in suboptimal systems.

What's needed is a comprehensive network management solution consisting of an integrated set of tools that span the network infrastructure.

Automated network management is more than a strategy—it's a solution to the problems of today's network management organizations, offering complete control of your infrastructure.

HP Network Management Center

To address the objectives of enhancing network availability and performance, improving resource utilization, delivering compliant and secure networks, and meeting SLAs, HP provides a complete Automated Network Management (ANM) solution. ANM is focused on automating technology workflow processes across the network infrastructure, which is the foundation for all business services delivered. Through this unique, and fully integrated combination of capabilities, ANM helps network engineering and operations teams overcome their challenges and meet their operational objectives.

Typical use cases for ANM include rolling out an IP telephony infrastructure, working through a data center consolidation project, managing network traffic at the edge, or just managing the day-to-day churn of a modern network. HP provides capabilities to plan for changes, including:

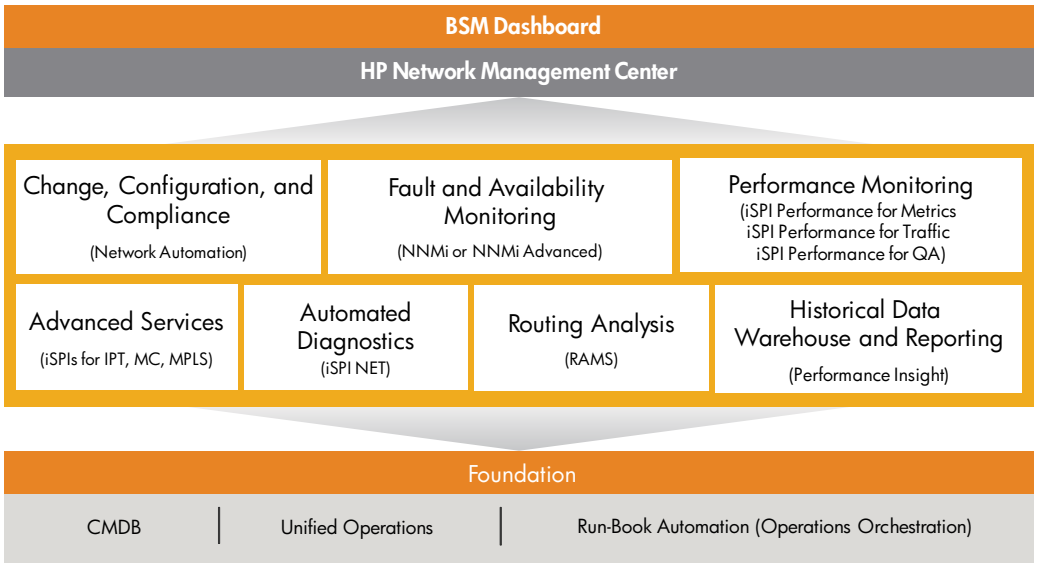
- Network design, simulation, and modeling capabilities
- The ability to deliver designs such as configuring the network change and configuration management
- Root-cause analysis
- The ability to operate physical and virtual networks to make sure that a desired state is maintained, including service and business-impact operational views and run-book automation

Streamline
HP Network Node Manager i software (NNMi) is your single solution for managing fault, availability, performance, and advanced network services for your physical and virtualized network infrastructure.

NNMi software offers extreme scale, unified polling, a single configuration point, and a common console for configuration and administration to reduce your costs and improve the efficiency of your network operations.

It enables you to unify fault, availability, and performance monitoring with:

- NNMi and NNMi Advanced
- NNM iSPI Performance for Metrics
- NNM iSPI Performance for Traffic
- NNM iSPI Performance for Quality Assurance



Enhance
NNMi software provides unmatched insight into advanced network services through NNMi Smart Plug-Ins (iSPIs).

NNM iSPIs for Advanced Network Services deliver consistent presentation of IP telephony, MPLS, and IP multicast information in the context of your network topology. Presenting this type of information in the context of topology allows for easy association of network faults to interruption in advanced services, improved service quality, and end-to-end performance monitoring of the infrastructure used for service delivery.

NNMi software for advanced network services consists of:

- NNM iSPI for IP Telephony
- NNM iSPI for IP Multicast
- NNM iSPI for MPLS

Control
HP software for ANM complements the unified fault and performance capabilities of NNMi with change, configuration, and compliance management through HP Network Automation software.

The main goal of our approach to automated network management is to make sure that the desired state of the network—the foundation for all business services—is continuously maintained. To help ensure this desired state, we provide unified network fault, availability, performance, configuration, change, and compliance as well as diagnostic automation capabilities. This is provided through a single pane of glass for network operations. We then drive increased network service levels and performance through a comprehensive network-monitoring solution with integrated remediation and change automation. Finally, we provide a solution that enforces compliance and security by making sure that changes are checked for policy compliance on an ongoing basis.

HP offers a complete set of capabilities to make sure that the desired state of the network is maintained. These capabilities include:

- **Fault and availability monitoring:** Improve network availability with a model-based network-management solution using NNMi or NNMi Advanced
- **Change, configuration, and compliance:** Experience comprehensive network automation spanning all tasks from provisioning and change management to compliance enforcement and reporting
- **Performance monitoring:** Increase operator productivity and efficiency and reduce mean time to recovery (MTTR) using NNM iSPI Performance for Metrics, Traffic, and Quality Assurance
- **Engineering Toolset:** Automate common network engineering and network tool administrators tasks using the NNMi iSPI Network Engineering Toolset
- **Expand the capabilities of the HP automated network management solution with:**
  - Real-time layer-3 WAN optimization management using HP Route Analytics Management software (RAMS)
  - Historical data warehousing and reporting using HP Performance Insight
  - Run-book automation using HP Operations Orchestration

Center components

The HP Network Management Center is an integrated solution designed to support ANM.

The core of the Network Management Center is composed of products that provide coverage across network fault, availability, performance, configuration, change, and compliance as well as diagnostic automation capabilities. The solution is integrated to provide greater operator efficiency and effectiveness. Lastly, the products can be extended through add-on modules called Smart Plug-ins for managing advanced services such as IP telephony, MPLS, and IP multicast.

The foundation components of the Network Management Center allow for integration with element management systems, third-party applications, and the HP Universal Configuration Management Database (CMDB)—all of which extend the value and reach of this center.

The products that make up the HP Network Management Center include:

- HP Network Node Manager i software
- HP Network Node Manager Smart Plug-ins
- HP Network Automation software
- HP Route Analytics Management software
- HP Performance Insight

A complete solution

Comprehensive training
HP provides a comprehensive curriculum of HP software and IT Service Management courses. These offerings provide the training you need to realize the full potential of your HP solutions, increase your network optimization and responsiveness, and achieve better return on your IT investments.

With more than 30 years of experience in meeting complex education challenges worldwide, HP knows training. This experience, coupled with unique insights into HP Software & Solutions products, positions HP to deliver an outstanding training experience. For more information about these and other educational courses, visit **www.hp.com/learn**

The smartest way to invest in IT
HP Financial Services provides innovative financing and financial asset management programs to help you cost-effectively acquire, manage, and ultimately retire your HP solutions. For more information on these services, contact your HP sales representative or visit **www.hp.com/go/hpfinancialservices**

HP Services

Get the most from your software investment
HP provides high-quality software services that address all aspects of your software application lifecycle needs. With HP, you have access to standards-based, modular, multi-platform software coupled with global services and support. The wide range of HP service offerings—from online self-solve support to proactive mission-critical services—enables you to choose the services that best match your business needs.

For an overview of HP software services, visit **www.managementsoftware.hp.com/service**

To access technical interactive support, visit Software Support Online at **www.hp.com/managementsoftware/services**

To learn more about HP Software Customer Connection, a one-stop information and learning portal for software products and services, visit **www.hp.com/go/swcustomerconnection**

Global citizenship at HP

At HP, global citizenship is our commitment to hold ourselves to high standards of integrity, contribution, and accountability in balancing our business goals with our impact on society and the planet. To learn more, visit **www.hp.com/hpinfo/globalcitizenship**, and for information about the HP Eco solutions program, go to **www.hp.com/ecosolutions**

To know how HP Network Management Center can help meet your network management challenges, visit **www.hp.com/go/nmc**

Share with colleagues

Get connected
www.hp.com/go/getconnected
Get the insider view on tech trends, alerts, and HP solutions for better business outcomes

© Copyright 2007, 2009–2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA1-6185ENW, Created October 2007; Updated April 2010, Rev. 2

Annexe 4 : Présentation de HP Operation Center

(Hewlett-Packard, 2010a)

HP Operations Center

Monitor, diagnose, and prioritize infrastructure problems based on business impact

Overview

Modern businesses rely on complex IT infrastructures composed of servers, storage, networks, middleware, and other application components to support their critical business services. Initiatives such as virtualization aim to reduce costs and improve agility, but at the same time, they add a layer of complexity that can slow diagnosis and repair of problems that span multiple silos.

HP provides visibility across the physical and virtual infrastructure that lets operations teams identify issues, isolate causes, and resolve or remove outages quickly, before any users feel the impact. The result is that business users experience better availability and performance of their applications.

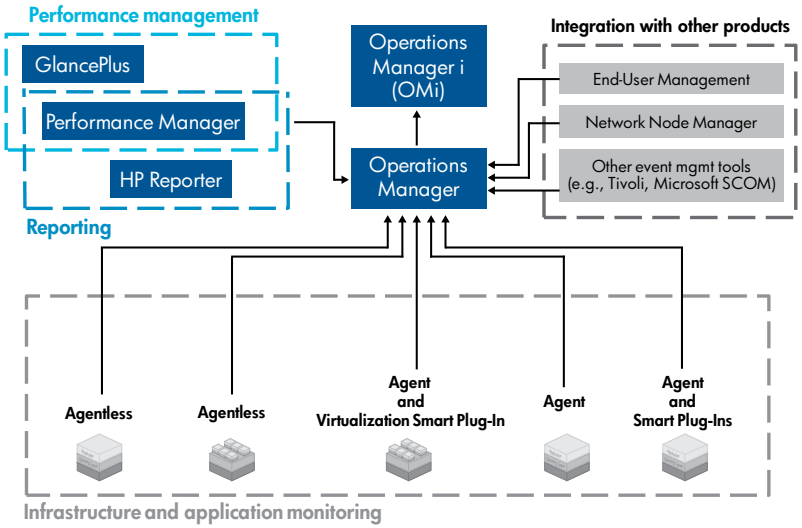
By consolidating events arising from all technology silos such as servers, storage, applications, and networks, HP Operations Center enables comprehensive, infrastructure-wide operational management. HP Operations Center detects fault and performance events using a combination of agents, agentless monitoring, and alerts from HP and third-party element managers. It uses correlation technologies at the managed node and central console to suppress unnecessary data and allow operators to focus on fixing the underlying problems rather than chasing symptom events. The end result is improved availability and performance with reduced operational costs.

Benefits

HP Operations Center is a suite of IT management products that offer the following benefits:

Greater operational efficiency and reduced costs: An integrated console consolidates event and performance data from heterogeneous sources, both physical and virtual, to reduce duplicate monitoring efforts caused by multiple IT silos in an organization.

HP Operations Center: HP Operations Center consolidates fault and performance events across servers, storage, applications, and networks, using a combination of agents and agentless monitoring.



Virtualization Management
Virtualization can reduce capital costs, but it also causes two major management problems:

- Duplication of effort by virtualization specialists and operations teams, resulting in extra costs
- Increased downtime due to complexity of troubleshooting

HP Operations Center provides a single console for monitoring both virtual and physical infrastructure:

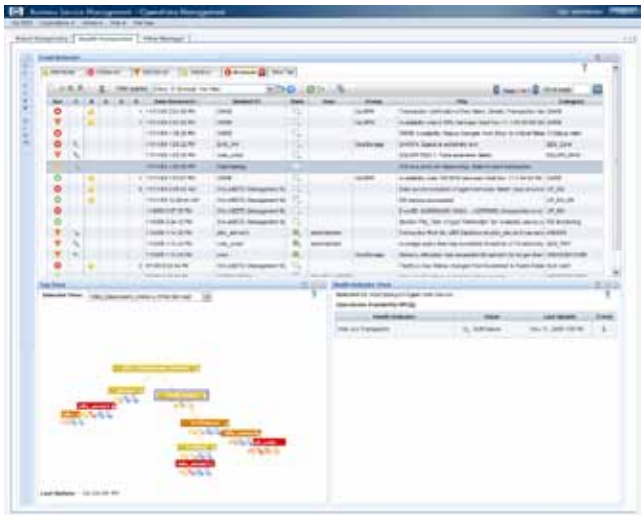
- Centralized fault event processing reduces redundancy to cut costs
- Consolidated performance data collection and event processing links applications to virtual and physical layers to speed diagnosis time and reduce downtime

Reduced time to repair: Operators can quickly and accurately prioritize and filter numerous events through a centralized Operations Bridge. Topology-based event correlation analyzes complex event streams using the context of the automatically discovered infrastructure to further enhance productivity by allowing operations staff to quickly determine the cause of a problem.

Improved quality of service: Users experience outstanding availability and performance when you manage the IT infrastructure as a comprehensive ecosystem rather than disparate domains.

Investment protection: As your IT infrastructure grows, HP Operations Center scales with your needs.

- HP Operations Manager—event consolidation and correlation
  - Reduce costs and duplication of effort by consolidating events from disparate IT domains into a single enterprise console.
  - Speed the resolution of issues with improved visibility across the entire enterprise IT infrastructure.
  - Decrease the number of costly escalations by empowering Operations Bridge staff to resolve incidents on their own.
- HP Operations Manager i (HP OMi)—Operations Bridge event-management improvement
  - Accelerate time to repair by focusing operators on causal events with topology-based event correlation.
  - Reduce outages proactively by linking business services to the underlying IT infrastructure, enabling operators to prioritize their activities.
  - Visualize application and service health.
- Performance management
  - Identify resource problems across virtual and physical infrastructure to reduce business risks associated with downtime or slow performance.
  - Analyze historical performance trends to identify bottlenecks and drive infrastructure optimization.
  - Provide immediate performance-issue identification with real-time diagnostic capabilities to lower business service impact.
- Reporting
  - Identify issues with reports that unify performance, system, and availability information on a single graph.
  - Clarify performance and usage trends based on historical application and system data to enable capacity management.
- Agent and agentless monitoring
  - Enable fault and performance detection across a wide variety of physical and virtual host types and application platforms using combinations of agent and agentless monitoring.
  - Use agents to perform autonomous actions to resolve problems immediately, even with no connection to the management server.
  - Use agentless monitoring with HP SiteScope to gain low overhead and rapid deployment with no need to install software onto managed nodes, enabling very fast time to value.
- HP Operations Smart Plug-Ins (SPIs)
  - Use application-specific auto-discovery, pre-defined monitoring policies, and corrective actions to monitor industry-standard applications out of the box.



Assuming that at $1,500 per minute of downtime (typical for online retailers), a single 15-minute outage costs a company over $20,000. Other industries such as financial services can incur downtime costs that exceed $100,000 per minute, according to industry reports. Using HP Operations Manager reduces downtime by empowering first-level operators to resolve more issues more rapidly.

Key use cases

Reducing duplication of effort with silo consolidation

Different IT domains often require specialized monitoring tools and teams of experts to enhance their performance. But each of these groups duplicates efforts in monitoring the IT infrastructure. And, since most business services share common components, when a problem occurs these teams must collaborate to isolate the cause. One example is the parallel monitoring teams that often exist for physical and virtual infrastructure.

This duplicated effort results in extra costs and increased downtime. In a complex, heterogeneous, and virtualized environment, troubleshooting spans IT silos and often requires iteration among multiple groups if they do not determine the cause of an outage or performance problem on the first attempt. Using a consolidated event console for multiple IT domains allows a single group of operators to more effectively monitor first-level events, allowing highly compensated subject-matter experts and architects to focus more on innovation and less on troubleshooting.

Benefits

- Cuts costs by reducing duplication of effort
- Streamlines troubleshooting time by providing a single view across disparate IT silos
- Correlates events from various IT domains into a single location, isolating causes from symptoms
- Improves quality of service by enhancing visibility across the enterprise

Products

- Operations Manager
- Performance Manager
- Virtualization Smart Plug-In

Increasing staff efficiency and effectiveness

Managing increasingly complex IT ecosystems poses two significant challenges. First, there is a heavy interdependence of IT components, where there is a high likelihood that a failure in one area will affect another. For example, a storage issue (causal event) can cause database, e-mail, and connectivity issues (symptom events). The second challenge is the sheer volume of events that most enterprises must handle.

HP OMi Topology Based Event Correlation (TBEC) uses automatically discovered information about the IT infrastructure to further consolidate and classify events as either symptoms or causes. This allows Operations Bridge personnel to prioritize which events they need to deal with immediately and which they can leave alone—and which they can ultimately resolve by fixing the causal event.

Benefits

- Increases operations staff productivity and effectiveness through the use of TBEC, which allows quicker correlation of events and their relationships to each other
- Reduces mean time to repair (MTTR) because focusing on only causal, not symptomatic, events allows operators to solve problems more quickly
- Cuts costs by reducing duplication of effort expended on separate but related issues

Products

- Operations Manager i

Some HP Operations Orchestration customers use about 10 flows to automatically remediate half of their events. It typically costs $75 to manually process each event, according to HP customer research. Just automating 100 events per day equates into saving more than $2.7 million per year.

Automated remediation

Multiple operating systems, virtualization, and multi-tier applications mean the volume of events arriving at the Operations Bridge has exploded—to the point where staff cannot deal with them manually. Combining HP Operations Orchestration with HP Operations Manager provides IT organizations with the ability to remediate recurring IT issues automatically.

For example, the HP Operations Manager SPI for Virtual Infrastructure detects a performance degradation of a virtual machine, which creates an event. This event arrives at HP Operations Manager and initiates an HP Operations Orchestration flow that determines which server has available resources. The flow then opens a ticket and automatically performs a migration of the deteriorating virtual machine to the server with excess capacity. After verifying the operation was completed successfully, HP Operations Orchestration closes the ticket and acknowledges the alert in HP Operations Manager. The software has resolved the problem without human intervention.

Benefits

- Automate mundane tasks, reducing the labor required to manage IT operations and enabling consistent application of IT processes
- Speed time to problem resolution, reducing the impact on the customer experience
- Improve productivity of subject-matter experts by capturing their knowledge in automated run books and protecting them from routine troubleshooting functions

Products

- HP Operations Manager
- HP Operations Orchestration

Why HP Software?

HP software is uniquely positioned to meet your IT infrastructure operations and business service management requirements. We offer:

Proven successes: Thousands of customers worldwide have successfully deployed HP Operations Center to support consolidated operations and business service management.

Market leadership: HP is the proven market leader for availability and performance management. HP is documented as a leading vendor by market share and recognized by analysts as a leader in completeness of solution, vision, and the ability to execute.

A complete solution: Unlike other vendors, HP provides a complete event management solution that includes topology-based event correlation, run-book automation, and integrated performance management, along with end-user monitoring and advanced application diagnostics.

Technology leadership: HP Operations Manager i provides an automated root cause analysis engine in the industry that is able to dynamically adapt to infrastructure topology changes and use that information to separate causal events from symptoms.

Partnership: HP has a large and experienced partner community that extends the value and reach of our event and performance management solutions.

For more information

To find out more about how HP can help you monitor, diagnose, and prioritize infrastructure problems based on business impact, download the HP white paper, **Consolidated IT event management: five requirements for greater efficiency**. For more resources on HP Operations Center including product downloads and our blog, visit **www.hp.com/go/opc**

Get connected

www.hp.com/go/getconnected

Get the insider view on tech trends, alerts and HP solutions for better business outcomes

Technology for better business outcomes

To learn more, visit www.hp.com/go/opc

© Copyright 2008, 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA2-0443ENW Rev. 1, February 2010

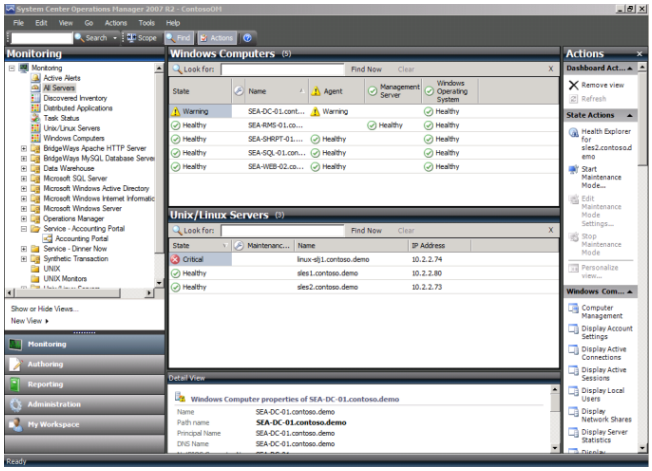
Annexe 5 : Présentation de System Center Operations Manager 2007 R2

(Microsoft Corporation, 2009b)

Microsoft

Microsoft® System Center Operations Manager 2007 R2

Réduire les coûts dans les centres de données avec Operations Manager 2007 R2



La virtualisation des systèmes et la multitude de technologies et d'applications accueillies par les centres de données conduisent les organisations à déployer différents outils d'administration : outils spécifiques, propriétaires, développés en interne, etc.

Autant d'outils, autant d'interfaces différentes et de procédures distinctes. À cause du manque d'intégration entre ces produits, il devient pratiquement impossible d'automatiser des actions qui mettent en jeu des outils d'origines différentes. En conséquence, les coûts de déploiement, d'adaptation et de maintenance de ces outils augmentent, ainsi que le besoin en formation des équipes d'administrateurs.

System Center Operations Manager 2007 R2 vous permet de réduire le coût de gestion du centre de données, des systèmes d'exploitation serveur et des hyperviseurs via une interface unique, connue et simple à utiliser. En étendant à UNIX et Linux la facilité d'administration des applications déployées sur Windows Server, les organisations répondent mieux à leurs besoins en niveau de service pour leurs centres de données.

Avec Operations Manager 2007 R2, les organisations améliorent les mesures de performance et de disponibilité en contrôlant mieux le niveau de service. Les exploitants accèdent plus facilement aux principales fonctionnalités dont ils ont besoin pour assurer et améliorer les prestations fournies aux utilisateurs.

Avantages d'Operations Manager 2007 R2

- **Améliore la disponibilité et les performances des applications des plateformes hétérogènes** du centre de données : capacité à superviser les serveurs UNIX, Linux et Windows à partir d'une console unique.
- **Simplifie la supervision des applications** du centre de données grâce à des rapports détaillés qui indiquent les performances actuelles des applications et leur relation avec les niveaux de service souhaités. Les capacités de supervision sont capables de croître pour s'adapter aux charges.
- **Accélère l'accès aux informations et aux fonctionnalités** pour permettre l'identification rapide d'un problème et l'application d'actions pour résoudre rapidement les problèmes avant qu'ils ne deviennent critiques.

Principales fonctionnalités

Architecture flexible et capable de monter en charge

- L'architecture à plusieurs niveaux permet de superviser tous les environnements, même les plus complexes.
- Supervision de domaines uniques, multiples et sans relations d'approbation, ainsi que des sites distants, tout cela à partir d'un même groupe d'administration.
- Possibilité en natif de superviser à la fois les systèmes physiques et virtuels, et leurs applications.
- Contrôle intégré, approfondi et puissant des systèmes et applications Linux, UNIX et Windows.
- Forte capacité à monter en charge (par exemple, possibilité de surveiller plus de 1000 URL par serveur d'administration).

Sécurité intégrée

- Exploite Active Directory pour gérer les accès des groupes et des utilisateurs.
- Accès basé sur les rôles permettant des accès limités à certaines vues et tâches via la console.
- Sert de proxy entre les utilisateurs et les systèmes sous contrôle, ce qui permet d'encadrer les activités autorisées sur les systèmes contrôlés.

Supervision intégrée et adaptable

- Contrôle approfondi et sophistiqué des applications Microsoft ou non Microsoft, via des packs d'administration fournis par Microsoft et ses partenaires.
- Surveillance de l'état et des performances des principales composants des systèmes d'exploitation, comme les processeurs, les disques physiques et logiques, la mémoire, les interfaces réseau, etc.
- Outils puissants permettant la création et l'adaptation de packs d'administration.
- Assistant d'installation pour simplifier le déploiement des packs d'administration à partir du Catalogue System Center.

Surveillance des niveaux de service

- Permet une définition fine des objectifs en termes de niveaux de service, pour tous les composants informatiques.
- Présente le niveau de service atteint par une application ou un service informatique comme la somme des niveaux de service des composants de cette application ou de ce service.
- Des rapports d'exploitation permettent de présenter les informations, avec une lecture à plusieurs niveaux.

Rapports complets et précis

- Des rapports détaillés sont fournis sur les performances, la disponibilité et d'autres facteurs pour les éléments supervisés, qu'il s'agisse de systèmes d'exploitation, d'applications ou de services.
- Les rapports permettent d'analyser en profondeur jusqu'au niveau de détail souhaité.
- Affichage sous forme de tableaux de bord complets, diffusables avec Microsoft SharePoint (par exemple), pour exploiter vos investissements dans les technologies Microsoft.

Création et personnalisation

- Des modèles permettent aux exploitants de créer rapidement de nouveaux contrôles pour surveiller l'état et les performances des applications et des systèmes cibles.
- Un outil permet de créer rapidement des modèles d'états, via la définition des composants qui interviennent dans les applications cibles.
- Possibilité de personnaliser et d'adapter certains éléments des packs d'administration.
- Les affichages de synthèse tiennent compte des personnalisations des packs d'administration.

Infrastructure de notification flexible

- Notifications par courriels, SMS, messagerie instantanée, et autres.
- Un Assistant de notification simplifie la création et la maintenance des notifications.
- Chaque exploitant peut s'inscrire pour recevoir les notifications de son choix.

Automatisation et interopérabilité puissantes

- Des packs d'administration répondent de façon automatique à des incidents dans des environnements virtualisés (par exemple, déplacement dynamique d'applications d'un serveur vers un autre en cas de panne matérielle sur un hôte de virtualisation).
- Des connecteurs d'interopérabilité assurent la circulation des informations et la synchronisation des alertes entre Operations Manager 2007 R2 et d'autres systèmes d'administration.
- PowerShell permet d'héberger des cmdlets pour surveiller l'état et les performances d'un système, plutôt que de faire exécuter ces cmdlets sur le système cible.

Ressources et informations supplémentaires

Téléchargez une version d'évaluation de Operations Manager 2007 R2

Téléchargez une version gratuite qui vous permet d'évaluer le produit pendant 180 jours et obtenez des informations supplémentaires à l'adresse

http://www.microsoft.com/france/serveur/system-center/operations-manager/default.mspx

Connecteurs et packs d'administration

Pour connaître les derniers packs d'administration et les connecteurs édités par Microsoft et ses partenaires pour Operations Manager 2007, visitez le catalogue System Center à l'adresse

http://technet.microsoft.com/en-us/opsmgr/cc539535.aspx

Ce document est diffusé uniquement à titre d'information. MICROSOFT N'APPORTE AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, DANS CE DOCUMENT. Microsoft, Active Directory, Windows, le logo Windows et Windows Server System sont soit des marques déposées soit des marques commerciales de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Toutes les autres marques citées appartiennent à leurs propriétaires respectifs.

© 2009 Microsoft Corporation. Tous droits réservés.

Annexe 6 : Présentation de System Center Virtual Machine Manager 2008 R2

(Microsoft Corporation, 2009c)

Microsoft® System Center Virtual Machine Manager 2008 R2

Économies, agilité et facilité d'administration pour les centres de données virtualisés

System Center Virtual Machine Manager (SCVMM) 2008 R2 est une solution d'administration des centres de données virtualisés qui centralise l'administration de l'infrastructure informatique, améliore le taux d'utilisation des serveurs et optimise les ressources sur des plateformes virtuelles et physiques.

Virtual Machine Manager 2008 R2 présente les caractéristiques suivantes :

- Administration des systèmes virtuels hébergés sur Windows Server® 2008 & 2008 R2 Hyper-V™ et Microsoft Hyper-V Server.
- Prise en charge de systèmes virtuels fonctionnant sous Microsoft Virtual Server et VMware ESX.
- Déplacement à chaud des machines virtuelles (live migration).
- Ajout et suppression à chaud des ressources de stockage.
- Prise en charge des volumes partagés d'un cluster (CSV – Cluster Shared Volume).
- Fonction PRO (Performance and Resource Optimization) pour une administration dynamique et réactive de l'infrastructure virtuelle.
- Répartition intelligente des charges virtuelles sur les serveurs physiques les mieux appropriés.

Optimisation des ressources informatiques

Virtual Machine Manager 2008 R2 fournit une solution simple pour consolider les serveurs physiques dans un environnement virtuel, mieux exploiter les serveurs physiques et réduire les coûts liés à la consommation électrique, à la place occupée et au refroidissement.

Administration de plateformes virtuelles hétérogènes depuis une console unique

En plus de gérer Microsoft Hyper-V et Virtual Server, Virtual Machine Manager (SCVMM) assure le pilotage de VMware. SCVMM exploite tout aussi bien des fonctions propres à VMware (comme VMotion) que les siennes (répartition intelligente sur des serveurs VMware). Il propose aussi un assistant simple pour convertir les systèmes virtuels VMware en VHD dans un processus de conversion virtuel à virtuel (V2V), simple et rapide.

Conversions P2V rapides et fiables

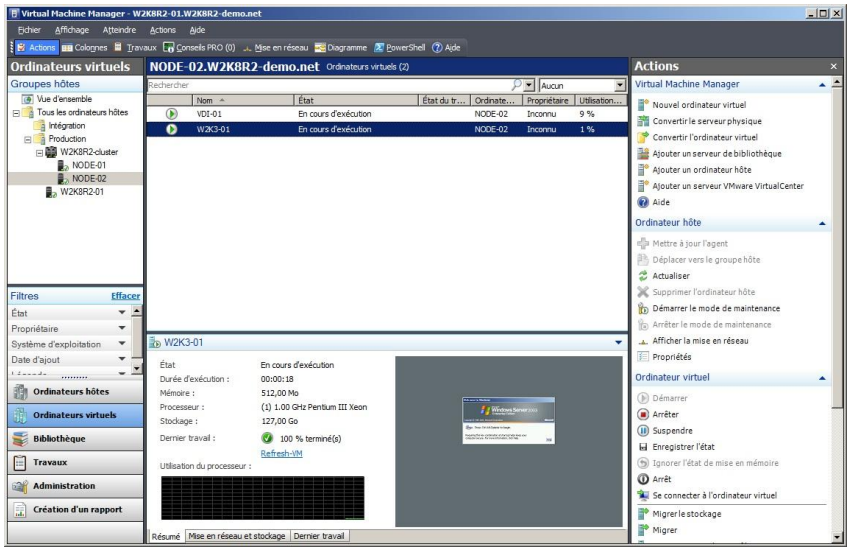
Virtual Machine Manager améliore la conversion de système physique en système virtuel (P2V) en intégrant le processus P2V et en utilisant le Service de cliché instantané de volume de Windows pour créer très rapidement un système virtuel sans interrompre le serveur physique source

Répartition intelligente

Lors du déploiement d'un système virtuel, Virtual Machine Manager analyse les données de performances et les besoins en ressources de la charge et de l'hôte. L'administrateur peut alors modifier les algorithmes de placement du système virtuel. L'utilisation des serveurs physiques est optimisée et ce, que l'entreprise cherche à équilibrer la charge entre les hôtes existants ou à exploiter au mieux les ressources de chacun d'entre eux.

Administration centralisée des ressources

La console d'administration de Virtual Machine Manager sert de plateforme centrale pour optimiser les ressources. Il est possible d'ajuster les paramètres des systèmes virtuels sans interrompre leur exploitation et d'effectuer la migration de systèmes virtuels d'un hôte à l'autre à des fins d'optimisation.



Console d'administration de System Center Virtual Manager 2008 R2

Ce document est fourni uniquement à titre indicatif. MICROSOFT EXCLUT TOUTE GARANTIE, EXPRESSE OU IMPLICITE, EN CE QUI CONCERNE CE DOCUMENT

Microsoft® System Center Virtual Machine Manager 2008 R2

Agilité optimale

Virtual Machine Manager 2008 R2 permet aux administrateurs et utilisateurs habilités de déployer rapidement des systèmes virtuels.

Optimisation des ressources de façon dynamique ou suite à des événements

La fonction Performance and Resource Optimization (PRO) de VMM et System Center Operations Manager aide à s'assurer du parfait fonctionnement de l'infrastructure virtuelle. PRO réagit dynamiquement, en fonction de règles définies par les administrateurs, aux baisses de performances ou aux incidents éventuels rencontrés dans les applications, les systèmes d'exploitation ou les systèmes virtualisés. Structure extensible et ouverte, PRO peut être utilisée par les éditeurs de logiciels et les informaticiens à partir de leurs produits et solutions.

Déplacement à chaud

Virtual Machine Manager 2008 R2 prend en charge le déplacement à chaud des machines virtuelles, permettant de déplacer des systèmes virtuels entre hôtes Hyper-V sans temps d'arrêt. Elle limite en outre les interruptions dues à la maintenance du système. Couplée avec la fonction PRO, elle permet de créer un environnement informatique dynamique et de réallouer automatiquement les charges des systèmes virtuels selon la consommation des ressources et la capacité disponible.

Bibliothèque centralisée

La bibliothèque de Virtual Machine Manager centralise les éléments constitutifs d'un centre de données virtuel : disques durs virtuels, images des CD/DVD, scripts de personnalisation post-déploiement, configurations matérielles, modèles et images ISO.

Déploiement rapide de modèles de systèmes virtuels

La bibliothèque apporte un nouvel outil à l'administrateur : les modèles de systèmes virtuels. Ces modèles contiennent les configurations logicielle et matérielle du système d'exploitation virtuel hébergé de façon à assurer une grande cohérence dans le centre de données.

Supervision centralisée

Une fois les charges consolidées dans une infrastructure virtuelle, Virtual Machine Manager propose aux administrateurs des rapports et données de supervision. Operations Manager 2007 permet d'étendre ces fonctionnalités.

Rôle d'administrateur délégué

Avec cette version de Virtual Machine Manager apparaît le rôle d'administrateur délégué. Il est possible de lui confier des tâches et fonctions d'administrateur dans un périmètre défini. Par exemple, un administrateur délégué pourrait gérer les besoins en virtualisation d'un groupe spécifique de serveurs ou d'un ensemble d'utilisateurs.

Migration rapide du stockage

Grâce à cette fonction, un administrateur peut déplacer le stockage d'une machine virtuelle vers un autre LUN (Logical Unit Number), ou vers un autre hôte, quasiment sans interruption de service. Généralement, la migration rapide du stockage prend moins de 2 minutes. Le temps d'arrêt réel dépend toutefois du niveau d'activité du système virtuel lors du déplacement. En outre, VMM 2008 R2 exploite désormais la fonction VMotion™ de VMware pour déplacer des systèmes virtuels VMware d'un stockage à un autre sans temps d'arrêt. Les entreprises exploitant la nouvelle fonctionnalité CSV (Cluster Shared Volume) de Windows Server 2008 R2 apprécient pleinement ce nouveau type de migration.

Exploitation des compétences existantes

Avec Virtual Machine Manager 2008 R2, les départements informatiques capitalisent sur leur expertise de Windows Server et System Center. Cela réduit au minimum les besoins en formation des administrateurs et du personnel du support technique.

Interface familière, socle commun

La console d'administration de Virtual Machine Manager reprend l'interface utilisateur de la suite System Center. Cela permet aux administrateurs de se familiariser rapidement avec la gestion de leurs systèmes virtuels.

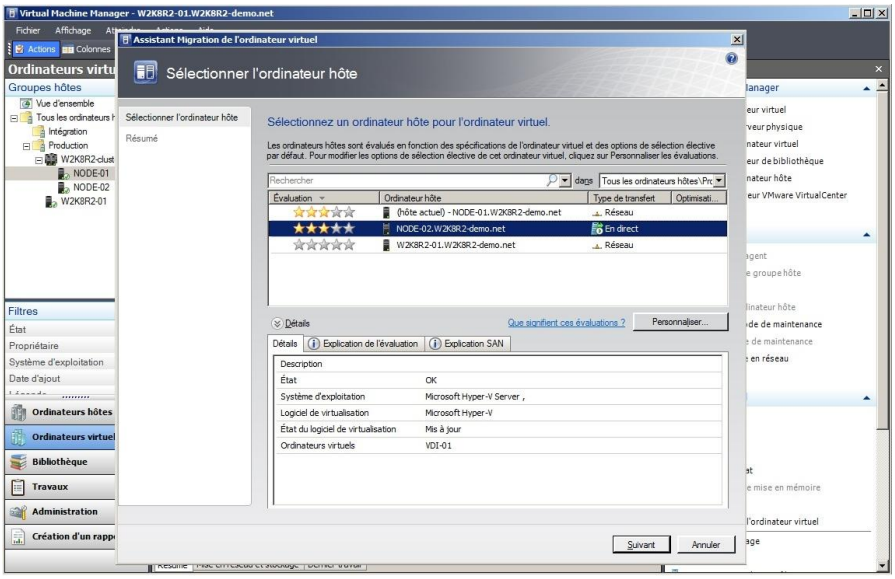
Intégration de Windows PowerShell™

Virtual Machine Manager est complètement écrit en Windows PowerShell, un langage de script destiné aux administrateurs, proposant plus de 170 outils de ligne de commande standards, exemples de syntaxes et utilitaires.

Pour plus d'informations visitez les pages :

www.microsoft.com/france/scvmm

www.microsoft.com/france/virtualisation/default.mspx



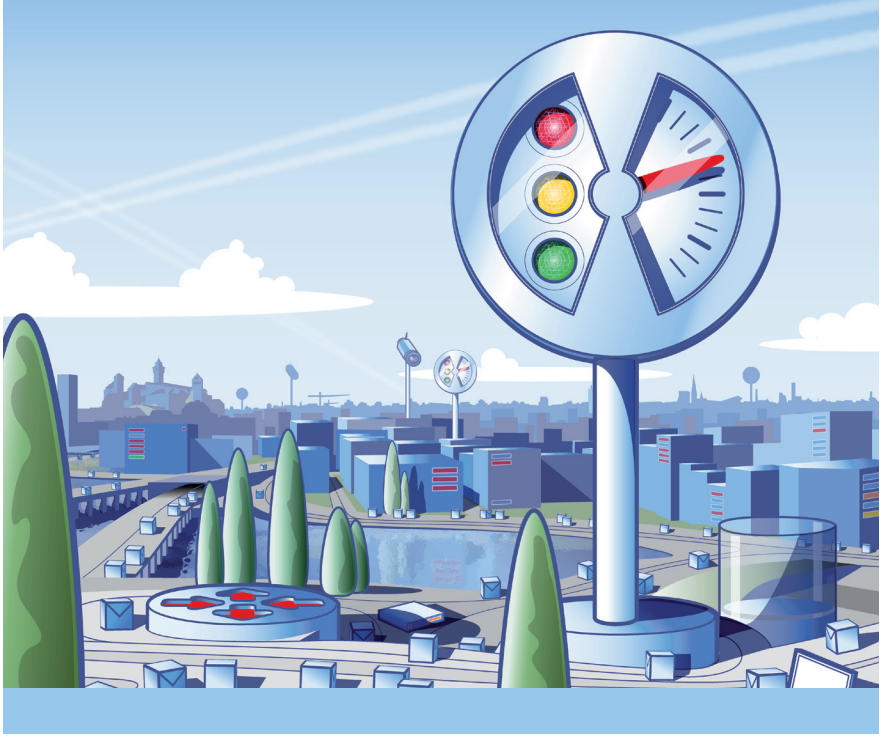
Ce document est fourni uniquement à titre indicatif.
MICROSOFT EXCLUT TOUTE GARANTIE EXPRESSE OU IMPLICITE, EN CE QUI CONCERNE CE DOCUMENT.

Microsoft® System Center

Annexe 7 : Présentation de PRTG Network Monitor

(Paessler, 2010c)

PAESSLER®



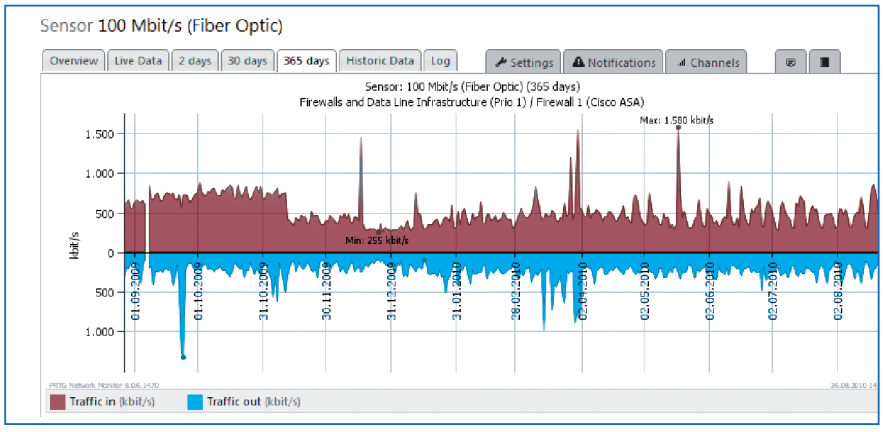
Easy, failsafe and complete control over your network, proven in more than 150,000 installations worldwide.

PRTG Network Monitor

The All-In Monitoring Solution

PRTG Network Monitor is the all-in monitoring solution that combines the whole expertise of the network monitoring company Paessler with a comprehensive set of monitoring features, an easy to use, intuitive interface, and a state-of-the-art monitoring engine which is suitable for networks of any size. All with one license: no hidden costs, no add-ons, no extra efforts!

PRTG assures the availability of network components, and measures traffic and usage. It saves costs by avoiding outages, optimizing connections, saving time, and controlling service level agreements (SLAs).



Clear graphs give a quick overview of your network's components and traffic status. This picture shows the traffic on a firewall.

You're looking for . . .

. . . an easy to use monitoring solution for Windows based networks?

PRTG Network Monitor... runs under Windows Server 2003 and 2008, as well as under XP, Vista, and Windows 7 and monitors Windows, Linux, Unix, and MacOS systems. PRTG is installed and set up within minutes; it comes with its own, integrated databaseand web server, and an automatic network discovery. PRTG is consequently optimized for easy usage.

. . . one software to monitor your entire network, devices as well as applications, traffic as well as availability?

PRTG Network Monitor... supports SNMP, WMI, Flow monitoring, as well as packet sniffing, and offers more than 80 special sensors for VoIP monitoring, website monitoring, email monitoring, application monitoring, database monitoring, monitoring of virtual environments, and many others.

. . . monitoring of different sites from one central installation?

PRTG Network Monitor... comes with so called 'remote probes' which can be installed to locally distributed networks and then send the monitoring data SSL-encrypted via Internet (no VPN required) to the core server of the central installation.

. . . a comprehensive network monitoring solution that fits to your budget?

PRTG Network Monitor... offers comprehensive monitoring functionality and scales up to larger networks of some thousand devices and even more for the price of an entry level monitoring software.

. . . clear and fair licensing?

PRTG Network Monitor... includes the entire monitoring functionality in every license. No add-ons are required—no extra costs, no extra configuration and maintenance efforts, no extra traffic load.

. . . high availability monitoring?

PRTG Network Monitor... comes with at least one failover cluster in every license (up to 5 clusters for Unlimited Site and Corporate), which is a fully monitoring cluster that makes sure monitoring will not be interrupted in case of a server failure or even for updates.

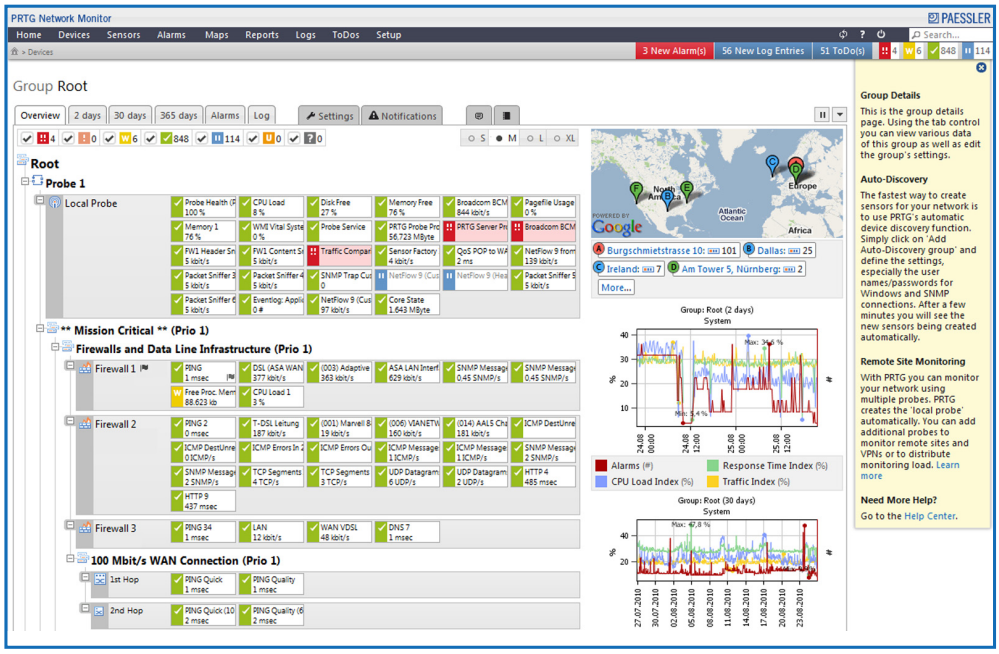
"We were able to fully implement PRTG with about ten-times the features for less than the annual maintenance cost on the previous system. Plus, it runs on about one-third of the hardware. I've been in IT for more than 20 years and I've never seen anything like it."

Jim Kirby,
Director of Engineering,
Dataware Services

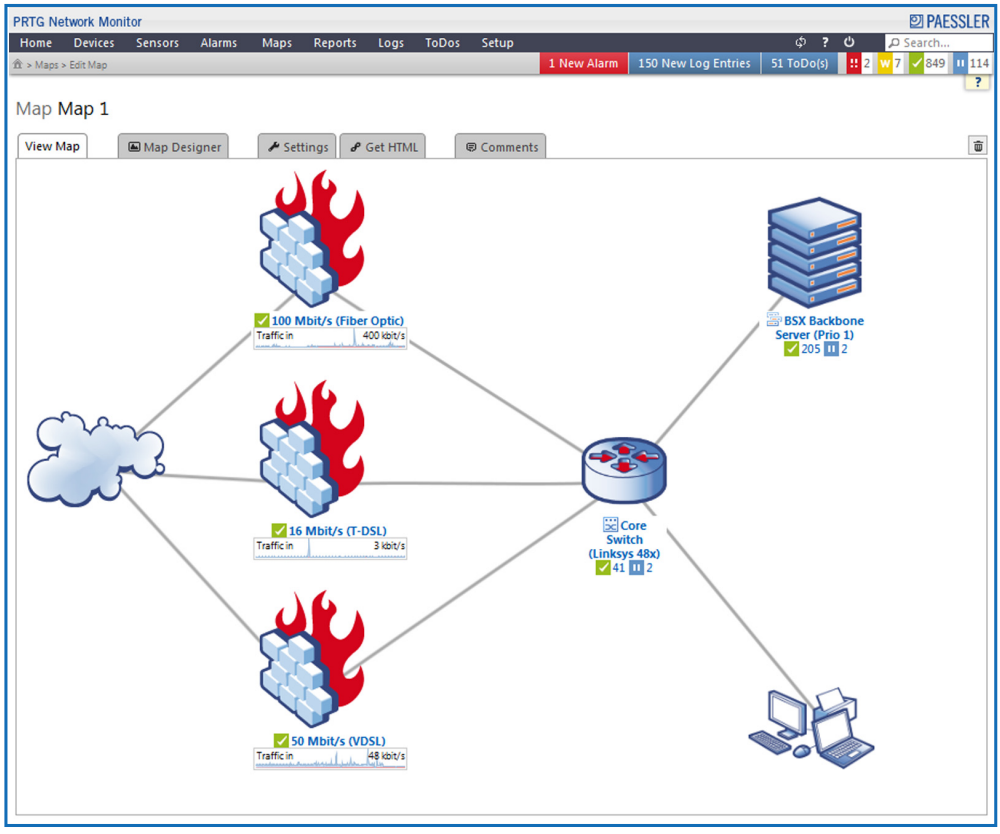
Dataware Services, LLC, operates one of the largest public data centers in South Dakota

Save time and money: Systematic network monitoring helps you avoid failures, optimize networks, and improve services.

Practical Example



The web interface: fast and powerful, optimized for easy and intuitive use. This picture shows Google Maps integration and a hierarchical device tree view.



Create customized 'Maps' using PRTG's built-in appealing icons and view monitoring status, graphs, and tables.

Technical Data

Basic Features

- Bandwidth, usage, activity, uptime and SLA monitoring
- Suitable for networks of all sizes
- Monitoring of multiple networks/locations with one license
- Failover cluster included in every license, multiple clusters possible
- HTTP-based API for interfacing with other applications
- Automatic network discovery & sensor configuration

Sensors and Protocols

- More than 80 sensor types (Ping, HTTP, WMI, SMTP, POP3, DNS, and many others)
- Network traffic and behavior analysis using SNMP, NetFlow v5/v9, and packet sniffing
- Smart sensors (e.g. automatic cognition and monitoring of multiprocessor systems)
- Preconfigured device templates for Cisco routers, SQL servers, network printers, etc.
- Sensors for monitoring virtualized environments (VMware, XEN, HyperV, etc.)
- Programmable triggers and custom sensors
- Native and agent-less Linux monitoring

Display

- Elegant, fast and powerful web-based interface
- Google Maps integration
- Optional Windows GUI
- iPhone App and 'Mini-HTML' interface for mobile devices
- Hierarchical view (probes, groups, devices, sensors, channels)
- List of sensors (alphabetical, fastest, slowest, by tag, by type, etc.)
- Appealing graphs (for sensors, devices, groups, and probes) showing the monitoring data of the last 2 hours, last 48 hours, last 30 days and last 365 days
- Customizable 'Maps' that bring together monitoring status, graphs, and tables, using personalized layouts

Alerting and Reporting

- Alerts according to individually configured criteria
- Various means of notification (email, SMS, pager message, HTTP request, syslog, etc.)
- Periodic and customizable reports (HTML, PDF)
- Reports and log files (detailed logs of all activity and results)

System Requirements and Data Storage

- Data is stored in Paessler's own powerful data storage system, highly optimized for monitoring data (no SQL-Server required)
- Small download, easy to install
- Runs on Windows Server 2003 and 2008, XP, Vista, or Windows 7

Licensing

- All features included in every license, no add-ons
- Easy upgrade by paying the price difference

"PRTG is a key to maximizing productivity in a tough economy," Foschini said. "It ensures that we're always providing the best service to students, but also positions each resource for maximum benefit to the traditional employees, yielding higher results and less wait time throughout."

Travis Foschini, Manager of Information Technology, Columbia Southern University

Columbia Southern University is one of the first completely online universities in the USA

PAESSLER®
the network monitoring company

www.paessler.com · info@paessler.com

Annexe 8 : Tableau de comparaison BlackBerry

(Research In Motion, 2010b)

Tableau de comparaison BlackBerry

	Service BlackBerry® via votre fournisseur d'accès sans fil	BlackBerry® Enterprise Server Express	Hosted BlackBerry® Services	BlackBerry® Enterprise Server
De quoi s'agit-il ?	Plan de service de votre fournisseur d'accès sans fil donnant accès aux services BlackBerry tels que la messagerie Internet (Yahoo®, Google®, Hotmail®, etc.), Internet, la messagerie instantanée, les réseaux sociaux et BlackBerry App World™.	Conçu pour les petites et grandes entreprises disposant de serveurs de messagerie sur site, BlackBerry Enterprise Server Express est un logiciel gratuit exploitant les e-mails et les données professionnelles sur un smartphone BlackBerry. BlackBerry Enterprise Server Express représente une solution sûre et à moindre coût pour les entreprises souhaitant connecter les smartphones BlackBerry professionnels et personnels à la messagerie électronique de l'entreprise.	Conçu pour les entreprises qui externalisent leur infrastructure de messagerie. Associe une sécurité avancée aux fonctionnalités du smartphone BlackBerry tout en étant géré par un partenaire certifié BlackBerry®.	Conçu pour répondre aux besoins mobiles des entreprises et organismes publics ; inclut des fonctionnalités avancées telles que la haute disponibilité et prend en charge les produits add-on premium.
Avantages	• Utilisez votre messagerie électronique en quelques étapes • Accédez sans fil aux applications populaires de MI et de réseaux sociaux • BlackBerry® Browser • Personnalisez votre appareil et téléchargez des applications depuis BlackBerry App World	• Fonctionne avec tous les plans de données BlackBerry incluant Internet • Logiciels et licences d'accès client gratuits • Permet aux entreprises de multiplier le nombre d'utilisateurs de smartphones BlackBerry à moindre coût tout en maintenant la sécurité et le contrôle sur les utilisateurs professionnels et personnels • Installation directe sur le serveur de messagerie existant*	• Pas besoin d'acheter, d'installer ou de gérer un logiciel de serveur ou un matériel informatique supplémentaire • Coûts mensuels prévisibles	• Assure un niveau optimal en matière de contrôle informatique et de fonctionnalités avancées • Offre la possibilité d'ajouter des produits tels que BlackBerry® Mobile Voice System
Plates-formes de messagerie prises en charge	POP3, IMAP, ISP, OWA	Microsoft® Exchange, Microsoft Small Business Server	Microsoft Exchange, IBM® Lotus® Domino®	Microsoft Exchange, IBM® Lotus® Domino®, Novell® GroupWise®
Nombre d'utilisateurs BlackBerry pris en charge	Individuel	Jusqu'à 75 utilisateurs sur le serveur de messagerie ou plus de 2 000 avec serveur(s) dédié(s)	Illimité	Prise en charge possible d'un large groupe d'utilisateurs professionnels (plus de 2 000 par serveur)
Frais supplémentaires par utilisateur (USD)	Uniquement plan de données requis	Uniquement plan de données requis	Renseignez-vous auprès de votre fournisseur de Hosted BlackBerry Services	1 LAC - 99 $; 5 LAC - 429 $, 10 LAC - 699 $, 50 LAC - 3 299 $; Packs de LAC plus importants disponibles
Synchronisation sans fil de la messagerie électronique	✓	✓	✓	✓
Synchronisation sans fil du calendrier et des contacts	Requiert une synchronisation avec le PC via un câble	✓	✓	✓
Fonctionnalité de calendrier avancée	✗	✓	✓	✓
Messageries instantanées prises en charge	Interface Web (BlackBerry® Messenger, AIM®, Yahoo!® Messenger, Windows Live™ Messenger, Google Talk™ et ICQ®)	Interface Web (comme Facebook®, MySpace®)	Interface Web (BlackBerry Messenger, AIM, Yahoo! Messenger, Windows Live Messenger, Google Talk et ICQ) et d'entreprise hébergée	Interface Web (BlackBerry Messenger, AIM, Yahoo! Messenger, Windows Live Messenger, Google Talk et ICQ) et d'entreprise (comme Microsoft Office Communicator)
Réseaux sociaux pris en charge	Interface Web (comme Facebook, MySpace)	Interface Web (BlackBerry Messenger, AIM, Yahoo! Messenger, Windows Live Messenger, Google Talk et ICQ)	Interface Web (comme Facebook, MySpace) et d'entreprise hébergée	Interface Web (comme Facebook, MySpace) et d'entreprise (comme IBM® Lotus® Connections)
Intégration téléphone de bureau/PBX	✗	✗	✗	✓ (avec BlackBerry Mobile Voice System)
Accès aux fichiers à distance	✗	✓	Contactez votre fournisseur de Hosted BlackBerry Services pour davantage de détails	✓
Accès à Intranet	✗	✓	Contactez votre fournisseur de Hosted BlackBerry Services pour davantage de détails	✓
Aperçu et modification des pièces jointes	✓	✓	✓	✓
Prise en charge des applications	BlackBerry App World et applications Web	BlackBerry App World™, applications Web et applications professionnelles client-serveur	BlackBerry App World, applications Web et applications professionnelles hébergées	BlackBerry App World, applications Web et applications professionnelles client-serveur
Sécurité	Niveau de sécurité dépendant de votre source de messagerie électronique	Classe entreprise avec plus de 35 stratégies informatiques et le chiffrement des données AES 256 bits	Classe entreprise avec plus de 450 stratégies informatiques et le chiffrement des données AES 256 bits	Classe entreprise avec plus de 450 stratégies informatiques et le chiffrement des données AES 256 bits
Installation	Configuration effectuée par l'utilisateur avec l'assistant d'installation du dispositif	Installation possible sur le serveur de messagerie existant ou sur un serveur dédié	Installation effectuée par un fournisseur de solutions hébergées	Installation effectuée par le service informatique sur un serveur dédié
Administrabilité	BlackBerry® Desktop Manager sur PC	Console dynamique à interface Web pour une gestion facile des stratégies et des utilisateurs	Gestion effectuée par un fournisseur de solutions hébergées	Console dynamique à interface Web pour une gestion facile des stratégies et des utilisateurs
Fonctionnalités informatiques Premium	✗	✗	Contactez votre fournisseur de Hosted BlackBerry Services pour davantage de détails	Inclut la haute disponibilité, la surveillance, l'accès sans fil et plus de 450 stratégies informatiques

BlackBerry

* jusqu'à 75 utilisateurs pour une installation directe sur le serveur de messagerie

Certaines fonctionnalités présentées dans ce document requièrent une version minimale de BlackBerry® Enterprise Server, BlackBerry® Desktop Software et/ou de BlackBerry® Device Software. ©2010 Research In Motion Limited. Tous droits réservés. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ et les marques, noms et logos associés sont la propriété de Research In Motion Limited et sont déposés et/ou utilisés aux États-Unis et dans d'autres pays. AIM est une marque commerciale d'AOL LLC., Facebook est une marque commerciale de Facebook, Inc., Google Talk est une marque commerciale de Google Inc., ICQ est une marque commerciale d'AOL LLC., Microsoft est une marque commerciale de Microsoft Corporation., Windows Live est une marque commerciale de Microsoft Corporation., Yahoo! est une marque commerciale de Yahoo! Inc. Toutes les autres marques sont la propriété de leurs détenteurs respectifs. Renseignez-vous auprès de votre fournisseur de service pour des informations sur les services itinérants, les plans de services ainsi que les fonctionnalités et services pris en charge. Certaines fonctionnalités présentées dans ce document requièrent BlackBerry Enterprise Server v4.1.5, BlackBerry® Desktop Software et/ou BlackBerry® Device Software v4.5. RIM décline toute responsabilité et n'offre aucune représentation, garantie ou approbation à l'égard de tout aspect relatif à tout produit ou service tiers.

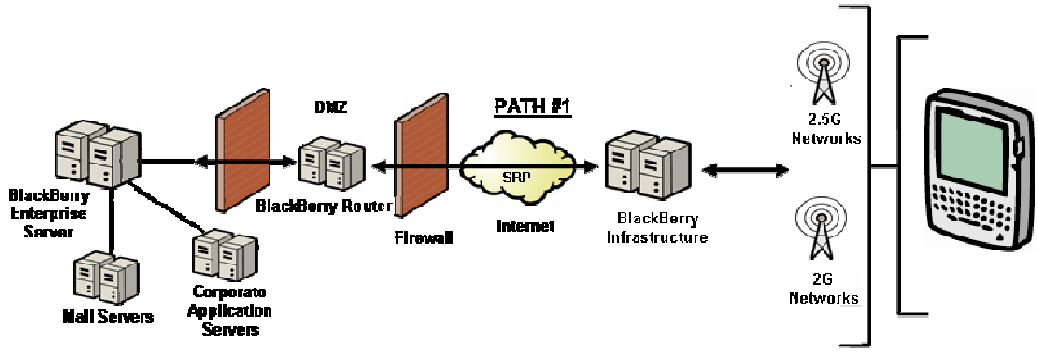
Annexe 9 : Pré-requis techniques pour BlackBerry Enterprise Server version 5.x

(Bouygues Telecom, 2010)

PRE-REQUIS TECHNIQUES

BlackBerry Enterprise Server (BES) Version 5.x
For Microsoft Exchange 2003, 2007, 2010.

Composants	Pre-requis	
Hardware	**La machine doit être dédiée au service BlackBerry**. L'installation sur un serveur hébergeant une autre application n'est pas supportée par RIM - BlackBerry. . La configuration minimum de la machine requise pour héberger le serveur BES est : ü **Pour moins de 200 utilisateurs :** Ø Monoprocesseur Intel Xéon 2.0 Ghz (biprocesseur recommandé) Ø 2 Go de RAM, 60 Go de disque. Ø SQL Express 2005 sur la même machine ü **Entre 200 et 500 utilisateurs :** Ø Biprocesseur Intel Xéon 2.0 Ghz. Ø 2 Go de RAM, 60 Go de disque. Ø SQL Express 2005 sur la même machine ü **Entre 500 et 1 000 utilisateurs :** Ø Biprocesseur Intel Xéon 2.0 Ghz. Ø 3 Go de RAM, 60 Go de disque. Ø SQL Express 2005 sur la même machine ü **Entre 1 000 et 2 000 utilisateurs :** Ø Biprocesseur Intel Xéon 2.8 Ghz, ou Biprocesseur Intel Xéon 1.86 Ghz Dual Core. Ø 4 Go de RAM, 60 Go de disque. Ø SQL Express 2005 sur la même machine. ! Pour plus de 300 utilisateurs, il est fortement conseillé d'utiliser une base de données sur un serveur Microsoft SQL, afin de ne pas surcharger le serveur BES ! Dans tous les cas, il est possible d'utiliser un serveur SQL.	q
Système	**Systèmes d'exploitation disponibles pour le serveur BES :** Ø Windows Server 2003 SP1 ou supérieur. Ø Windows Server 2003 R2 Ø Windows Server 2003 (64-bit). Ø Windows Server 2003 R2 SP2 (64-bit). Ø Windows Server 2008 ou supérieur. Ø Windows Server 2008 (64-bit). **Microsoft Exchange System tools** doit être installé sur le BES : Ø Microsoft Exchange Server MAPI client and CDO 1.2.1. Microsoft Internet Explorer version 6.0 ou supérieur. ! Microsoft Terminal Server **ne doit pas être installé en "Application Server Mode"** sur le BES. Il peut toutefois être installé et utilisé en "Administration Mode" ! **Microsoft Outlook NE DOIT PAS être installé sur le serveur BES**	q

Composants	Pre-requis	
DMZ	**Le serveur BES ne doit pas être en DMZ. Cette configuration n'est pas supportée.** Le BlackBerry Enterprise Server doit être installe dans le LAN avec une connexion directe vers les serveurs Exchange en utilisant les ports MAPI fixes. On peut installer le composant BlackBerry Router en DMZ, comme ci-dessous. 	q
Connexion au relais	Le BES crée une connexion TCP/IP permanente sur le port 3101 vers srp.eu.blackberry.net. **Les règles ci-dessous doivent être créées sur le firewall :** Ø Initialisation Outbound only Ø Trafic TCP (bidirectionnel) Ø Port 3101 Ø Depuis le BES vers srp.eu.blackberry.net (193.109.81.33) Cette configuration n'autorise que le serveur BES à initier la connexion au relai. Le BES s'authentifie auprès du relai en SHA1 (avec son SRP ID et l'Authentication Key). Le BES supporte les proxys transparents (Microsoft ISA Server par ex). Pour tester la connexion TCP, **utilisez BBSRPTEST.EXE sur le BES** comme ci-dessous. c:\Program Files\Research In Motion\BlackBerry Enterprise Server\Tools\bbsrptest.exe srp.eu.blackberry.net	q
Compte de service	**Un compte utilisateur doit être créé (BESAdmin par ex).** Il sera utilisé par le BES pour démarrer les services Windows, ainsi que pour accéder aux BAL des utilisateurs. BESAdmin doit : Etre ajouté au groupe local "**Administrateurs**" du serveur BES. Avoir le droit local de "**Ouvrir une session en tant que service**". Avoir une BAL **Exchange** avec une adresse email valide. Avoir les droits suivant sur ***Exchange 2003*** : - "**View Only Administrator**" sur le premier groupe d'administration - "**Administer information store**" sur les groupes de stockage - "**Send As**" and "**Receive As**" sur les groupes de stockage - "**Send As**" sur le compte utilisateur AD ou sur tous les comptes utilisateurs AD. Avoir les droits suivant sur ***Exchange 2007*** : - Dans l'interface de commande Power Shell du serveur Exchange 2007, entrez les commandes :	q

- **get-mailboxserver "<*messaging_server_name*>" | add-exchangeadministrator "BESAdmin" –role ViewOnlyAdmin**
- **get-mailboxserver "<*messaging_server_name*>" | add-adpermission –user "BESAdmin" –accessrights ExtendedRight –extendedrights Send-As, Receive-As, ms-Exch-Store-Admin**

- "**Send As**" sur le compte utilisateur AD ou sur tous les comptes utilisateurs AD

Avoir les droits suivant sur ***Exchange 2010*** :

Pré-requis : Le Rollup 1 doit être installé sur le serveur Exchange.

- **Get-MailboxDatabase | Add-ADPermission -User "BESAdmin" -AccessRights ExtendedRight -ExtendedRights Receive-As, ms-Exch-Store-Admin**
- **Add-RoleGroupMember "View-Only Organization Management" -Member "BESAdmin"**

Droit « SEND AS »
- **Add-ADPermission -InheritedObjectType User -InheritanceType Descendents -ExtendedRights Send-As -User "BESAdmin" -Identity "CN=Users,DC=<domain_1>,DC=<domain_2>,DC=<domain_3>"**

Désactiver les restrictions de client dans Microsoft Exchange 2010
- **Get-ThrottlingPolicy | where {$_.IsDefault -eq $true} | Set-ThrottlingPolicy -RCAMaxConcurrency $null.**

Augmenter le nombre maximal de connexions au service de carnet d'adresses dans Microsoft Exchange 2010

- Sur l'ordinateur qui héberge le rôle CAS de Microsoft Exchange, dans <*lecteur*>:\Program Files\Microsoft\ExchangeServer\V14\Bin, ouvrir le fichier microsoft.exchange.addressbook.service.exe.config dans un éditeur de texte.
- Définir la valeur de la clé MaxSessionsPerUser à 100 000.
- Redémarrer le service de carnet d'adresses.

Dans le cas de l'utilisation des Web Services :

1- Configurer un rôle de gestion pour Microsoft Exchange Web Services.
- **New-ManagementRoleAssignment -Name "BES Admin EWS" -Role ApplicationImpersonation –User "BESAdmin**".

2- Configuration du serveur hébergeant le serveur BES pour une exécution sans dossiers publics.

Créer ou modifier la clé de registre suivante :
• Pour Windows 32 bits:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsMessaging Subsystem\CDO.

• Pour Windows 64 bits :
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Messaging Subsystem\CDO.
Créer ou modifier la clé de Registre de type DWORD, nommée « Ignore No PF » et lui affecter la valeur 1.

Annexe 10 : Surveillance de BlackBerry Enterprise Server

(Research In Motion, 2009)

BlackBerry Enterprise Server

Surveillance de BlackBerry Enterprise Server

BlackBerry® Monitoring Service fournit des fonctionnalités de surveillance, d'alerte et de création de rapports améliorées qui offrent une plus grande visibilité quant à la santé de BlackBerry® Enterprise Server, ce qui permet l'identification et la résolution proactives des problèmes, et aide à maintenir un niveau de fonctionnement optimal sur vos smartphones BlackBerry®.

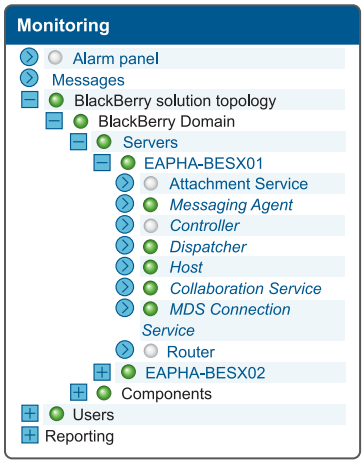
Incluses dans BlackBerry Enterprise Server version 5.0 et ultérieure, les fonctionnalités de surveillance améliorées sont accessibles via BlackBerry Administration Service sur le Web.

BlackBerry®

Fournir des informations de dépannage au personnel du centre d'assistance

Le personnel du centre d'assistance peut accéder à BlackBerry Monitoring Service à l'aide d'un navigateur Web ; il offre ainsi de la visibilité et des informations conçues pour aider au dépannage des problèmes d'assistance du BlackBerry.

Faciliter l'identification et la résolution proactives des problèmes



BlackBerry Monitoring Service est conçu pour surveiller continuellement l'état de BlackBerry Enterprise Server ; il peut être configuré afin d'alerter les administrateurs d'événements pouvant mener à des coupures des services BlackBerry ou à une détérioration des performances. Une notification peut permettre aux administrateurs de prendre des mesures proactives avant que l'indisponibilité n'apparaisse. Vous pouvez surveiller des valeurs pertinentes au niveau du serveur, de l'utilisateur ou de la connexion, grâce à des seuils d'événements définis par l'administrateur. Vous pouvez utiliser l'outil de recommandation de seuil pour recommander des seuils selon des déviations standard tirées d'un historique de données. Cet outil est exécutable à la demande et comprend un champ Remarques, qui fournit des détails sur la manière dont la recommandation a été obtenue. Vous pouvez spécifier une fenêtre de maintenance pour un seuil, afin de suspendre sa surveillance pour une période récurrente.

Optimiser l'infrastructure BlackBerry Enterprise Solution via l'ajustement des performances

BlackBerry Monitoring Service capture des statistiques de performances système, destinées à fournir aux administrateurs des informations utiles pour analyser et améliorer le fonctionnement de leur version de BlackBerry® Enterprise Solution. Les alertes sont affichées et gérées visuellement dans une console intuitive et configurable par l'administrateur pour les e-mails, les messages texte SMS et les messages de déroutement Simple Network Management Protocol (SNMP, protocole de gestion simple de réseau). Un sous-système d'instrumentation SNMP mis à jour est compris ; il fournit des données SNMP descriptives pour tous les composants et permet de garantir la compatibilité des déroutements avec les systèmes de surveillance tiers.

Augmenter l'efficacité et réduire les coûts de gestion

BlackBerry Monitoring Service est conçu pour automatiser les tâches de surveillance manuelles longues et pour effectuer des vérifications régulières configurables, visant à gagner du temps pour l'administrateur et à conserver des ressources informatiques essentielles. Ce service peut également offrir aux administrateurs des descriptions affinées des problèmes, destinées à diminuer la durée nécessaire à l'analyse des informations du système et de l'infrastructure. La création de rapports est utile pour visualiser des informations statistiques complètes sur le serveur, des informations statistiques avancées sur l'utilisateur, ainsi que pour afficher l'orientation et l'analyse graphique des statistiques du serveur et créer des rapports et graphiques personnalisables et définis par l'utilisateur. Des données de diagnostic du terminal peuvent être demandées et reçues sur les smartphones BlackBerry, améliorant ainsi leur efficacité.

Pour plus d'informations sur BlackBerry, rendez-vous sur le site **www.blackberry.com/go/serverupgrade**.

©2009 Research In Motion Limited. Tous droits réservés. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™, ainsi que les marques commerciales, noms et logos associés, sont la propriété de Research In Motion Limited et sont déposés et/ou utilisés aux États-Unis et dans d'autres pays dans le monde.
MKT-24425-002

Annexe 11 : Fonctionnement de l'iPhone en entreprise

(Apple Inc., 2010b)

iPhone en entreprise
Exchange ActiveSync

Règles de sécurité Exchange ActiveSync prises en charge

- Effacement à distance
- Appliquer le mot de passe sur l'appareil
- Nombre minimum de caractères
- Nombre maximum de tentatives (avant effacement local)
- Exiger à la fois des chiffres et des lettres
- Délai d'inactivité en minutes (de 1 à 60 minutes)

Règles Exchange ActiveSync supplémentaires (pour Exchange 2007 et 2010 seulement)

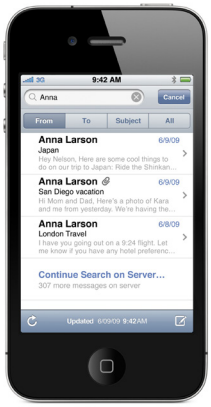
- Autoriser ou interdire les mots de passe simples
- Expiration du mot de passe
- Historique des mots de passe
- Intervalle d'actualisation des règles
- Nombre minimum de caractères complexes dans le mot de passe
- Exiger la synchronisation manuelle pendant l'itinérance
- Autoriser l'appareil photo
- Autoriser la navigation Web

iPhone communique directement avec votre serveur Microsoft Exchange via Microsoft Exchange ActiveSync (EAS), autorisant la transmission en mode "push" du courrier électronique, des calendriers et des contacts. Exchange ActiveSync fournit également aux utilisateurs l'accès à la Liste d'adresses globales et aux administrateurs des capacités de mise en œuvre de politiques de code d'appareil et d'effacement à distance. iPhone prend en charge l'authentification tant de base que par certificat pour Exchange ActiveSync. Si votre entreprise a actuellement Exchange ActiveSync activé, elle a déjà les services nécessaires en place pour prendre en charge iPhone — aucune configuration supplémentaire n'est requise. Si vous avez Exchange Server 2003, 2007 ou 2010 mais que votre société découvre Exchange ActiveSync, suivez les étapes ci-dessous.

Configuration d'Exchange ActiveSync

Présentation de la configuration du réseau

- Assurez-vous que le port 443 est ouvert sur le coupe-feu. Si votre entreprise utilise Outlook Web Access, le port 443 est probablement déjà ouvert.
- Vérifiez qu'un certificat de serveur est installé sur le serveur frontal et activez le protocole SSL pour le répertoire virtuel Exchange ActiveSync dans IIS.
- Si un serveur Microsoft Internet Security and Acceleration (ISA) est utilisé, vérifiez qu'un certificat de serveur est installé et mettez à jour le serveur DNS public de manière à ce qu'il résolve les connexions entrantes.
- Assurez-vous que le DNS de votre réseau retourne une adresse unique routable en externe au serveur Exchange ActiveSync pour les clients intranet et Internet. C'est obligatoire afin que l'appareil puisse utiliser la même adresse IP pour communiquer avec le serveur lorsque les deux types de connexions sont actives.
- Si vous utilisez un serveur Microsoft ISA, créez un écouteur web ainsi qu'une règle de publication d'accès au client web Exchange. Consultez la documentation de Microsoft pour plus de détails.
- Pour tous les coupe-feu et équipements réseau, définissez à 30 minutes le délai d'attente en cas de session inactive. Pour en savoir plus sur les autres intervalles de pulsations et de délai d'attente, consultez la documentation Microsoft Exchange à l'adresse http://technet.microsoft.com/en-us/library/cc182270.aspx.
- Configurez les fonctionnalités, les stratégies et les réglages en matière de sécurité des appareils mobiles à l'aide d'Exchange System Manager. Pour Exchange Server 2007 et 2010, il faut utiliser la console de gestion Exchange.
- Téléchargez et installez l'outil Microsoft Exchange ActiveSync Mobile Administration Web Tool, qui est nécessaire afin de lancer un effacement à distance. Pour Exchange Server 2007 et 2010, un effacement à distance peut aussi être lancé à l'aide d'Outlook Web Access ou de la console de gestion Exchange.



Autres services Exchange ActiveSync

- Consultation de la liste d'adresses globale (GAL)
- Acceptation et création d'invitations dans le calendrier
- Synchronisation des repères Répondre et Transférer à l'aide d'Exchange Server 2010
- Recherche de courrier électronique sur Exchange Server 2007 et 2010
- Prise en charge de plusieurs comptes Exchange ActiveSync
- Authentification par certificats
- Envoi de courrier électronique en mode "push" vers des dossiers sélectionnés
- Découverte automatique

Authentification de base (nom d'utilisateur et mot de passe)

- Activer Exchange ActiveSync pour certains utilisateurs ou groupes à l'aide du service Active Directory. Ces fonctionnalités sont activées par défaut sur tous les appareils mobiles au niveau organisationnel dans Exchange Server 2003, 2007 et 2010. Pour Exchange Server 2007 et 2010, voir l'option Configuration du destinataire dans la console de gestion Exchange.
- Par défaut, Exchange ActiveSync est configuré pour l'authentification de base des utilisateurs. Il est recommandé d'activer le protocole SSL pour l'authentification de base afin que les références soient chiffrées lors de l'authentification.

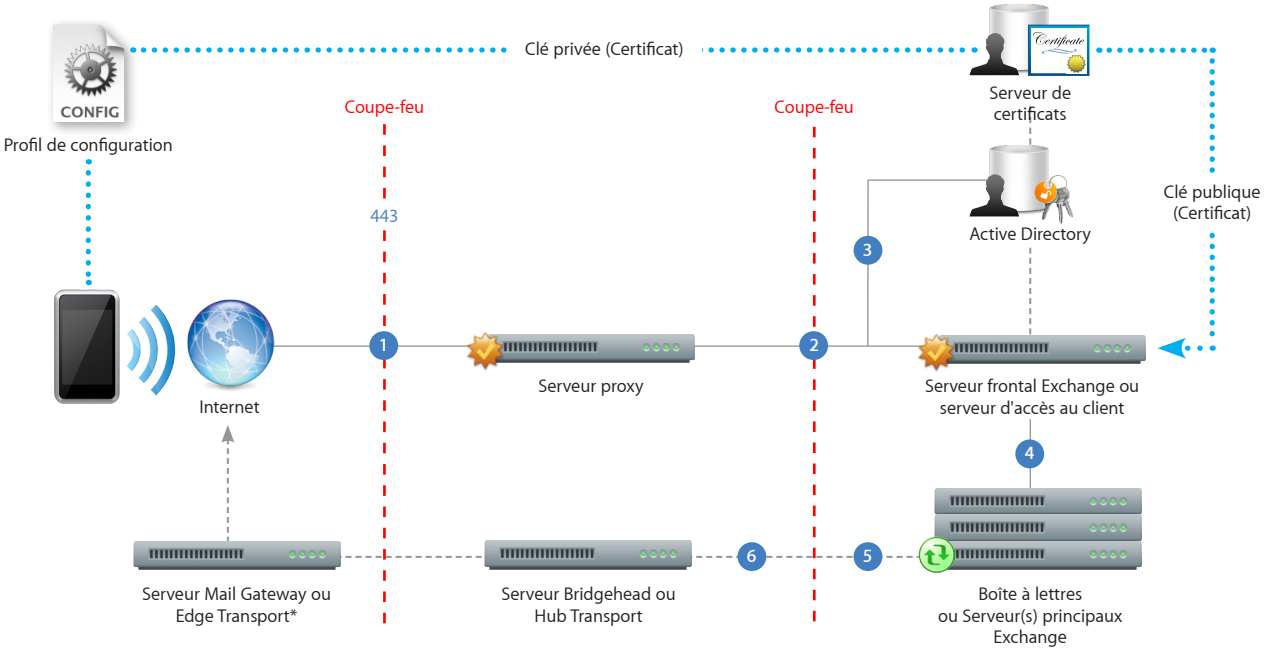
Authentification par certificats

- Installez les services de certificats d'entreprise sur un contrôleur de domaine ou un serveur membre de votre domaine (celui-ci sera votre serveur d'autorité de certification).
- Configurez IIS sur votre serveur frontal Exchange ou votre Serveur d'Accès Client afin d'accepter l'authentification par certificats pour le répertoire virtuel Exchange ActiveSync.
- Pour autoriser ou exiger des certificats pour tous les utilisateurs, désactivez "Authentification de base" et sélectionnez "Accepter les certificats clients" ou "Exiger les certificats clients".
- Générez les certificats clients au moyen de votre serveur d'autorité de certification. Exportez la clé publique et configurez IIS de manière à utiliser cette clé. Exportez la clé privée et utilisez un Profil de configuration pour fournir cette clé à iPhone. L'authentification par certificats peut uniquement être configurée à l'aide d'un Profil de configuration.

  Pour plus d'informations sur les services de certificats, veuillez vous reporter aux ressources disponibles auprès de Microsoft.

Scénario de déploiement d'Exchange ActiveSync

Cet exemple montre comment iPhone se connecte à un déploiement Microsoft Exchange Server 2003, 2007 ou 2010 standard.



*Selon la configuration de votre réseau, le serveur Mail Gateway ou Edge Transport peut résider dans la zone démilitarisée (DMZ).

1. iPhone demande l'accès aux services Exchange ActiveSync via le port 443 (HTTPS). (Il s'agit du même port utilisé pour Outlook Web Access et d'autres services web sécurisés. Dans de nombreux déploiements, ce port est donc déjà ouvert et configuré pour autoriser un trafic HTTPS avec chiffrement SSL.)
2. ISA offre un accès au serveur frontal Exchange ou au serveur d'accès au client. ISA est configuré comme un proxy ou, dans de nombreux cas, comme un proxy inverse, pour acheminer le trafic vers le serveur Exchange.
3. Le serveur Exchange identifie l'utilisateur entrant à l'aide du service Active Directory et du serveur de certificats (si vous utilisez une authentification par certificats).
4. Si l'utilisateur saisit les informations d'identification correctes et a accès aux services Exchange ActiveSync, le serveur frontal établit une connexion à la boîte de réception correspondante sur le serveur principal (via le catalogue global Active Directory).
5. La connexion Microsoft Exchange ActiveSync est établie. Les mises à jour/modifications sont envoyées en mode "push" ('Over The Air' OTA) sur iPhone, et les modifications effectuées sur iPhone sont répercutées sur le serveur Exchange.
6. Les courriers électroniques envoyés depuis l'iPhone sont également synchronisés avec le serveur Exchange via Exchange ActiveSync (étape 5). Pour acheminer le courrier électronique sortant vers des destinataires externes, celui-ci est généralement envoyé par le biais d'un serveur Bridgehead (ou Hub Transport) vers une passerelle Mail (ou Edge Transport) externe via SMTP. Selon la configuration de votre réseau, la passerelle Mail ou le serveur Edge Transport externe peut résider dans la zone démilitarisée ou à l'extérieur du coupe-feu.

© 2010 Apple Inc. Tous droits réservés. Apple, le logo Apple et iPhone sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays. Les autres noms de produits et de sociétés mentionnés dans ces pages peuvent être des marques de leurs sociétés respectives. Les caractéristiques des produits sont susceptibles d'être modifiées sans préavis. Les informations contenues dans ce document sont fournies à titre indicatif uniquement ; Apple n'assume aucune responsabilité quant à leur utilisation. Juin 2010 L419822A

Annexe 12 : Sécurisation d'un serveur web

(Microsoft Corporation, 2007c)

http://support.microsoft.com/kb/299875/

Numéro d'article: 299875 - Dernière mise à jour: lundi 3 décembre 2007 - Version: 3.6

Comment faire pour implémenter SSL dans IIS

Cliquez ici si vous souhaitez afficher en côte à côte l'article anglais et sa traduction automatique en français ATTENTION : Cet article est issu du système de traduction automatique

Résumé

Internet a ouvert des nouvelles méthodes pour les organisations communiquer, en interne et externe. Une meilleure communication entre employés, fournisseurs et clients permet à une organisation de réduire les coûts, amener produits plus rapide du marché et créer des relations client plus puissants. Cette communication améliorée nécessite--parfois--transmission des informations sensibles sur l'Internet et réseaux intranet. Il devient ainsi impératif pour pouvoir effectuer la communication privée et tamper-preuve avec des tiers connus. Pour importer ce sur, les organisations peuvent créer une infrastructure sécurisée basée sur la cryptographie de clé publique à l'aide des certificats numériques avec les technologies telles que SSL (Secure Sockets Layer). Ce guide étape par étape décrit comment configurer SSL sur un ordinateur de Services (IIS).

Configuration requise

Les éléments suivants décrivent le matériel recommandé, les logiciels, infrastructure réseau, compétences et connaissances, service packs dont vous aurez besoin :

- Windows 2000 Server, Advanced Server ou professionnel, avec services Internet (IIS) version 5.0 et Microsoft Certificate Server 2.0 installé et configuré.
- Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Datacenter Edition ou ordinateur Windows Server 2003 Web Edition avec services Internet (IIS) 6.0 et des services de certificats installé et configuré.

Si l'ordinateur qui héberge le serveur de certificats n'est pas le même ordinateur que possède des services Internet (IIS), vous devez un réseau valide ou une connexion Internet au serveur qui héberge le serveur de certificats.

Créer une demande de certificat

Tout d'abord, le serveur Web doit effectuer une demande de certificat. Pour ce faire, procédez comme suit :

1. Démarrez le Internet Service Manager (ISM), qui charge le composant logiciel enfichable IIS pour MMC (Microsoft Management Console). Pour ce faire, cliquez sur **Démarrer** , pointez sur **programmes** , pointez sur **Outils d'administration** , puis cliquez sur **Gestionnaire des services Internet** ou le **Gestionnaire des services IIS** .
2. Double-cliquez sur le nom du serveur afin que vous voir tous les sites Web. Dans IIS 6.0, développez **sites Web** .
3. Cliquez avec le bouton droit sur le site Web sur lequel vous souhaitez installer le certificat, puis cliquez sur **Propriétés** .
4. Cliquez sur l'onglet **Sécurité de répertoire** , puis cliquez sur **Certificat de serveur** sous **Communications sécurisées** pour démarrer l'Assistant Certificat de serveur Web.
5. Dans IIS 6.0, cliquez sur **suivant** . Si vous exécutez IIS 5.0, passez à étape 6.
6. Sélectionnez **Créer un certificat** et cliquez sur **suivant** .
7. Sélectionnez **préparer la demande maintenant, mais il ultérieurement envoyer** et cliquez sur **suivant** .
8. Tapez un nom pour le certificat. Vous souhaiterez peut-être correspond au nom certificat sur le nom de ce site. Maintenant, sélectionnez une longueur de bit ; plue la longueur de bits, le plus puissant le chiffrement de certificat. Sélectionnez **Server Gated Cryptography** si vos utilisateurs peuvent provenir de pays avec restrictions de cryptage.
9. Tapez votre nom d'organisation et l'unité organisationnelle (par exemple, Mon_site_web et service développement). Cliquez sur **suivant** .
10. Tapez le nom de domaine pleinement qualifié (FQDN) ou le nom du serveur que le nom commun. Si vous créez un certificat qui sera utilisé sur Internet, il est préférable d'utiliser un nom de domaine complet (par exemple, www.MyWeb.com). Cliquez sur **suivant** .
11. Entrez vos informations d'emplacement, puis cliquez sur **suivant** .
12. Tapez le nom de chemin d'accès et à enregistrer les informations de certificat pour, puis cliquez sur **suivant** pour continuer.

    note Si vous tapez rien autres que l'emplacement par défaut et le nom de fichier, veillez à noter le nom et à l'emplacement que vous choisissez, car vous devez accéder à ce fichier dans les étapes ultérieures.
13. Vérifiez les informations que vous avez tapées, puis cliquez sur **suivant** pour terminer le processus et créer la demande de certificat.

Soumettre une demande de certificat

La demande de certificat que vous venez créée doit être envoyé à une autorité de certificat (CA). Cela peut être votre propre serveur avec Certificate Server 2.0 installé sur elle ou d'une autorité de CERTIFICATION en ligne telle que VeriSign. Contactez le fournisseur de certificats de votre choix et déterminer le meilleur niveau de certificat à vos besoins. Il existe différentes méthodes d'envoyer votre demande. Contactez l'autorité de certification de votre choix pour demander et recevoir votre certificat. Vous pouvez créer votre propre certificat avec Certificate Server 2.0, mais vos clients doivent vous approuver implicitement en tant que l'autorité de certification. La procédure décrite ci-dessous suppose que vous utilisez Certificate Server 2.0 comme fournisseur de certificats.

note L'Assistant certificat D'IIS reconnaît uniquement le modèle Default Web Server. Lorsque vous sélectionnez une autorité de CERTIFICATION en ligne d'entreprise, l'autorité de ne pas être répertoriée, sauf si l'autorité de CERTIFICATION utilise le modèle Default Web Server.

1. Ouvrez un navigateur et accédez à http:// Votre_nom_serveur_web/certsrv /.
2. Dans IIS 5.0, sélectionnez **Demander un certificat** et cliquez sur **suivant** . Dans IIS 6.0, cliquez sur **Demander un certificat** .
3. Dans IIS 5.0, sélectionnez **demande avancée** et cliquez sur **suivant** . Dans IIS 6.0, cliquez sur **demande de certificat avancée** .
4. Dans IIS 5.0, sélectionnez **Envoyer une demande de certificat utilisant un codage Base64** et cliquez sur **suivant** . Dans IIS 6.0, cliquez sur **Soumettre un certificat demander en utilisant un base 64 codé CMC ou PKCS # 10 fichier, ou envoyer une demande de renouvellement en utilisant un fichier PKCS # 7 base 64 codé.**
5. Dans le Bloc-notes Microsoft, ouvrez le document demande qui vous avez créé dans la section « Création d'une demande de certificat ». Dans IIS 6.0, vous pouvez également cliquer sur **Rechercher un fichier à insérer** .
6. Copiez le contenu du document. Le contenu doit ressembler à celui-ci :

   ```
   -----BEGIN NEW CERTIFICATE REQUEST----- MIICcjCCAhwCAQAwYjETMBEGA1UEAxMKcm9ic3NlcnZlcjELMAkGA1UECxMCTVMx CzAJBgNVBAoTAk1TMREwDwYDVQQHEwhCZWxsZXZ1ZTERMA8GA1UECBMIV2FzaGl0
   b24xCzAJBgNVBAYTAlVTMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALYK4sYDNQ7h LmSfL0qpIvUfY7Ddw7fNCvDp3rM7z4QqoLhA2c8TkyamqWTBsV0WRHIidf/J6mU4 wN4wrUzJTLUCAwEAAaCCAVMwGgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMDUG
   CisGAQQBgjcCAQ4xJzAlMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEF BQcDATCB/QYKKwYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0 ACAAUgBTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBw
   AGgAaQBjACAAUAByAG8AdgBpAGQAZQBy A4GJAGka0jzBn8fkxScrWsdnU2eUJOMU K5Ms87Q+fjP1/pWN3PJnH7x8MBcSisFCjww6YnIjD8c3OfYfjkmWc04BZuGoH7Zo D6YNfv/SfAvQmr90eGmKOFfiTD+h11hM08gu2oxFU7mCvfTQ/2IbXP7KYFGEqaJ6
   wn0Z5yLOByPqb1QZAAAAAAAAAAAwDQYJKoZIhvcNAQEFBQADQQCgRCWkaXlY2nVa tbn6p5miPwWfrbViYo0B62wkuH0f7J0nSGcxMnn/6Q/iLEIsgHqFhox5PWCzIV0J tXKPWrBL -----END NEW CERTIFICATE REQUEST-------
   ```

   Remarque si vous enregistrez le document avec le nom et l'emplacement par défaut, il se trouve au C:\Certreq.txt.

   note Veillez à copier tout le contenu comme indiqué.

7. Coller le contenu du document dans la zone de texte du formulaire **demande de certificat crypté en Base64** .
8. Sous **modèle de certificat** , sélectionnez **utilisateur** ou le **serveur Web** , puis cliquez sur **Envoyer** .
9. Si **Certificate Server** est définie à **toujours émettre le certificat** , vous pouvez accéder immédiatement le certificat. Pour ce faire, procédez comme suit :
   a. Cliquez sur **télécharger le certificat CA** (ne cliquez pas sur **un chemin d'accès au certificat d'autorité de CERTIFICATION télécharger** ou **téléchargement de chaîne de certificats**).
   b. Lorsque vous êtes invité, sélectionnez **Enregistrer ce fichier sur disque** et enregistrer le certificat à votre bureau ou un autre emplacement que vous vous souvenez pas. Vous pouvez maintenant accéder directement au « installer le certificat et configurer un site Web SSL » section.

Émettre et télécharger un certificat

Pour émettre un certificat dans Certificate Server, procédez comme suit :

1. Ouvrez le composant logiciel enfichable MMC Autorité de CERTIFICATION. Pour ce faire, cliquez sur **Démarrer** , pointez sur **programmes** , pointez sur **Outils d'administration** , puis sur **une autorité de certification** .
2. Dans IIS 5.0, développez **une autorité de certification** puis cliquez sur le dossier **Demandes en attente** . Vos demandes de certificat en attente s'affichent dans le volet droit. Dans IIS 6.0, développez le nom du serveur.
3. Cliquez avec le bouton droit sur la demande de certificat en attente que vous venez de soumettre, sélectionnez **Toutes les tâches** et puis cliquez sur **le problème** .

   note Après avoir sélectionné le **problème** , le certificat est plus affiché dans cette fenêtre et le dossier. Il réside maintenant dans le dossier Certificats délivrés.
4. Après avoir émis (et autorisé) le certificat, vous pouvez revenir à l'interface Web des serveurs de certificats pour sélectionner et télécharger le certificat. Pour ce faire, procédez comme suit :
   a. Naviguez jusqu'à http:// Votre_nom_serveur_web/certsrv /.
   b. Sur la page par défaut, sélectionnez **Vérifier un certificat en attente** et cliquez sur **suivant** . Dans IIS 6.0, cliquez sur **Afficher le statut d'une demande de certificat en attente** .
   c. Sélectionnez votre certificat en attente, puis cliquez sur **suivant** pour atteindre la page de téléchargement.
   d. Dans la page de téléchargement, cliquez sur **Télécharger un certificat d'autorité de CERTIFICATION** (ne cliquez pas sur **un chemin d'accès au certificat d'autorité de CERTIFICATION télécharger** ou **téléchargement de chaîne de certificats**).
   e. Lorsque vous êtes invité, sélectionnez **Enregistrer ce fichier sur disque** et enregistrer le certificat à votre bureau ou un autre emplacement que vous vous souvenez pas.

Installer le certificat et configurer un site Web SSL

Pour installer le certificat, procédez comme suit :

1. Ouvrez le Gestionnaire des services Internet et développez le nom du serveur afin que vous pouvez afficher les sites Web.
2. Cliquez avec le bouton droit sur le site Web pour laquelle vous créé la demande de certificat, puis cliquez sur **Propriétés** .
3. Cliquez sur l'onglet **Sécurité de répertoire** . Sous **Communications sécurisées** , cliquez sur **Certificat de serveur** . L'Assistant Installation certificat démarre. Cliquez sur **suivant** pour continuer.
4. Sélectionnez **traiter la demande en attente et installer le certificat** et cliquez sur **suivant** .
5. Tapez l'emplacement du certificat que vous avez téléchargé dans la section « problèmes et télécharger un certificat », puis cliquez sur **suivant** . L'Assistant affiche le résumé du certificat. Vérifiez que les informations sont correctes, puis cliquez sur **suivant** pour continuer.
6. Cliquez sur **Terminer** pour terminer le processus.

Configurer et tester le certificat

Pour configurer et tester le certificat, procédez comme suit :

1. Sous l'onglet **Sécurité de répertoire** , sous **Communications sécurisées** , notez qu'il existe maintenant trois options disponibles. Pour définir le site Web pour qu'il exige des connexions sécurisées, cliquez sur **Modifier** . La boîte de dialogue **Communications sécurisées** s'affiche.
2. Sélectionnez **Secure Channel (SSL)** et cliquez sur **OK** .
3. Cliquez sur **Appliquer** , puis sur **OK** pour fermer la feuille de propriétés.

4. Accédez au site et vérifiez qu'il fonctionne. Pour ce faire, procédez comme suit :
   a. Accéder au site via HTTP en tapant **http://localhost/Postinfo.html** dans le navigateur. Vous recevez un message d'erreur semblable au suivant : HTTP interdit le 403.4 : SSL requis.
   b. Essayez de naviguer sur la même page Web utilisant une connexion sécurisée (HTTPS) en tapant **https://localhost/postinfo.html** dans le navigateur. Vous pouvez recevoir une alerte de sécurité indiquant que le certificat n'est pas émanant d'une source approuvée autorité de CERTIFICATION. cliquez sur **Oui** pour continuer à la page Web. Si la page s'affiche, vous avez correctement installé votre certificat.

Résolution des problèmes

- L'utilisation du protocole SSL ralentit les performances entre les serveurs HTTP et les navigateurs. Pour plus d'informations, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft : 150031 (http://support.microsoft.com/kb/150031/) Utilisation du protocole SSL crée une surcharge de performance pour les navigateurs
- Lorsque vous utilisez Microsoft Visual InterDev version 6.0 à l'auteur sites Web avec le protocole SSL, il existe plusieurs problèmes et limitations à prendre en compte. Pour plus d'informations, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft : 238662 (http://support.microsoft.com/kb/238662/) À l'aide Visual InterDev et Secure Sockets Layer
- Cet article décrit les certificats de serveur. Un certificat de serveur permet aux utilisateurs de s'authentifier votre serveur, vérifier la validité du contenu Web et établir une connexion sécurisée. Si vous envisagez également authentifier les utilisateurs qui navigueront sur votre site Web, vous pouvez envisager d'utiliser les certificats clients. Un certificat client typique contient plusieurs éléments d'informations : l'identité de l'utilisateur, l'identité de l'autorité de certification, une clé publique qui est utilisée pour établir des communications sécurisées et informations de validation, comme une date d'expiration et le numéro de série numéro.

RÉFÉRENCES

Pour plus d'informations, cliquez sur les numéros ci-dessous pour afficher les articles correspondants dans la Base de connaissances Microsoft : 228991 (http://support.microsoft.com/kb/228991/) Comment faire pour créer et installer un certificat SSL dans Internet Information Server 4.0 257591 (http://support.microsoft.com/kb/257591/) Description de la négociation SSL (Secure Sockets LAYER) 299525 (http://support.microsoft.com/kb/299525/) Comment configurer SSL à l'aide IIS 5.0 et de Certificate Server 2.0 298805 (http://support.microsoft.com/kb/298805/) Comment faire pour activer SSL pour tous les clients qui interagir avec votre site Web dans Internet Information Services Pour plus d'informations, consultez le site de Web MSDN (Microsoft Developer Network) suivant : http://msdn2.microsoft.com/en-us/library/aa302412.aspx (http://msdn2.microsoft.com/en-us/library/aa302412.aspx)

Les informations contenues dans cet article s'appliquent au(x) produit(s) suivant(s):

Mots-clés : kbmt kbhowto KB299875 KbMtfr

Traduction automatiqueIMPORTANT : Cet article est issu du système de traduction automatique mis au point par Microsoft (http://support.microsoft.com/gp/mtdetails). Un certain nombre d'articles obtenus par traduction automatique sont en effet mis à votre disposition en complément des articles traduits en langue française par des traducteurs professionnels. Cela vous permet d'avoir accès, dans votre propre langue, à l'ensemble des articles de la base de connaissances rédigés originellement en langue anglaise. Les articles traduits automatiquement ne sont pas toujours parfaits et peuvent comporter des erreurs de vocabulaire, de syntaxe ou de grammaire (probablement semblables aux erreurs que ferait une personne étrangère s'exprimant dans votre langue !). Néanmoins, mis à part ces imperfections, ces articles devraient suffire à vous orienter et à vous aider à résoudre votre problème. Microsoft s'efforce aussi continuellement de faire évoluer son système de traduction automatique.La version anglaise de cet article est la suivante: 299875 (http://support.microsoft.com/kb/299875/en-us/) L'INFORMATION CONTENUE DANS CE DOCUMENT EST FOURNIE PAR MICROSOFT SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE. L'UTILISATEUR ASSUME LE RISQUE DE L'UTILISATION DU CONTENU DE CE DOCUMENT. CE DOCUMENT NE PEUT ETRE REVENDU OU CEDE EN ECHANGE D'UN QUELCONQUE PROFIT.

Vous avez besoin d'une aide supplémentaire ?
Contactez le support technique par email, en ligne ou par téléphone

Aide et Support Microsoft

Microsoft
©2010 Microsoft

Annexe 13 : Configuration d’Exchange ActiveSync

(Microsoft Corporation, 2007b)

Numéro d'article: 817379 - Dernière mise à jour: jeudi 29 novembre 2007 - Version: 17.2

Des erreurs Exchange ActiveSync et Outlook Mobile Access se produisent lorsque Exchange Server 2003 nécessite une authentification SSL ou une authentification par formulaire

Important Cet article contient des informations sur la modification du Registre. Avant de modifier le Registre, pensez à le sauvegarder et assurez-vous que vous savez le restaurer en cas de problème. Pour plus d'informations sur la sauvegarde, la restauration et la modification du Registre, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft. 256986 (http://support.microsoft.com/kb/256986/) Description du Registre de Microsoft Windows

Symptômes

Lorsque vous essayez d'accéder à un ordinateur Microsoft Exchange Server 2003 en utilisant Microsoft Outlook Mobile Access ou Exchange ActiveSync, vous pouvez rencontrer l'un des symptômes suivants.

Outlook Mobile Access

- Le message d'erreur suivant s'affiche : Impossible de se connecter à votre boîte aux lettres sur le serveur *nom_serveur*. Veuillez réessayer ultérieurement. Si le problème persiste, contactez votre administrateur. En outre, le message d'erreur suivant est entré dans le journal d'application dans l'Observateur d'événements de l'ordinateur Exchange :

  Date : *Date*
  Source : MSExchangeOMA
  Heure : *Heure*
  Catégorie : (1000)
  Type : Erreur
  ID d'événement : 1805
  Utilisateur : N/A
  Ordinateur : *nom_serveur*

  Description : La requête de l'utilisateur UtilisateurA@domaine.com a provoqué le renvoi par le serveur principal Microsoft(R) Exchange <nom_serveur> d'une erreur HTTP avec le code d'état 403 : Refusé

  Réponse :
  Longueur du contenu : 1409
  Type de contenu : texte/html
  Serveur : Microsoft-IIS/6.0
  MicrosoftOfficeWebServer : 5.0_Pub
  X-alimenté par : ASP.NET
  Date : vendredi 21/02/2003 02:25:34 GMT

  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>La page doit être affichée sur un canal sécurisé.</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">

- Le message d'erreur suivant s'affiche : Une erreur système s'est produite lors du traitement de votre demande. Veuillez réessayer. Si le problème persiste, contactez votre administrateur. En outre, le message d'erreur suivant est entré dans le journal d'application dans l'Observateur d'événements de l'ordinateur Exchange :

  Date : *Date*
  Source : MSExchangeOMA
  Heure : *Heure*
  Catégorie : (1000)
  Type : Erreur
  ID d'événement : 1507
  Utilisateur : N/A
  Ordinateur : *nom_serveur*

  Description :
  Une erreur inconnue est survenue lors du traitement de votre demande : une exception de type Microsoft.Exchange.OMA.DataProviderInterface.ProviderException a été levée.

  Trace de pile :
  at Microsoft.Exchange.OMA.UserInterface.Global.Session_Start(Object sender, EventArgs e)
  at System.Web.SessionState.SessionStateModule.CompleteAcquireState ()
  at System.Web.SessionState.SessionStateModule.BeginAcquireState(Object source, EventArgs e, AsyncCallback cb, Object extraData)
  at System.Web.AsyncEventExecutionStep.System.Web.HttpApplication+IExecutionStep.Execute()
  at System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously)

  Erreur interne : Une exception a été levée par la cible d'un appel.

  Trace de pile :
  at System.Reflection.RuntimeConstructorInfo.InternalInvoke(BindingFlags invokeAttr, Binder binder, Object[] parameters, CultureInfo culture, Boolean isBinderDefault)
  at System.Reflection.RuntimeConstructorInfo.Invoke(BindingFlags invokeAttr, Binder binder, Object[] parameters, CultureInfo culture)
  at System.RuntimeType.CreateInstanceImpl(BindingFlags bindingAttr, Binder binder, Object[] args, CultureInfo culture, Object[] activationAttributes)
  at System.Activator.CreateInstance(Type type, BindingFlags bindingAttr, Binder binder, Object[] args, CultureInfo culture, Object[] activationAttributes) at Microsoft.Exchange.OMA.UserInterface.Global.Session_Start(Object sender, EventArgs e)

  Erreur interne : Le serveur distant a renvoyé une erreur : (440) Délai de connexion dépassé.

  Trace de pile :
  at Microsoft.Exchange.OMA.ExchangeDataProvider.OmaWebRequest.GetRequestStream()
  at Microsoft.Exchange.OMA.ExchangeDataProvider.ExchangeServices.GetSpecialFolders()
  at Microsoft.Exchange.OMA.ExchangeDataProvider.ExchangeServices..ctor(UserInfo user)

Exchange ActiveSync

Le message d'erreur suivant s'affiche : La synchronisation a échoué en raison d'une erreur sur le serveur. Réessayez. Code d'erreur : HTTP_500

Exchange Server 2003

Sur un serveur qui exécute Exchange Server 2003 Service Pack 2 (SP2), les événements suivants sont enregistrés dans le journal des applications.

Événement 1

Type d'événement : Erreur
Source de l'événement : Exchange Server ActiveSync
Catégorie de l'événement : Aucune
ID de l'événement : 3029
Description : Le répertoire virtuel [%2] du serveur de boîtes aux lettres [%1] est configuré pour utiliser SSL. Exchange ActiveSync ne peut pas accéder au serveur si le protocole SSL est requis.

Pour plus d'informations sur la façon de configurer correctement les paramètres des répertoires virtuels Exchange, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft. 817379 (http://support.microsoft.com/kb/817379/) Des erreurs Exchange ActiveSync et Outlook Mobile Access se produisent lorsque Exchange Server 2003 nécessite une authentification SSL ou une authentification basée sur les formulaires

Événement 2

Type d'événement : Erreur
Source de l'événement : Exchange Server ActiveSync
Catégorie de l'événement : Aucune
ID de l'événement : 3030
Description : L'authentification basée sur les formulaires est activée sur le serveur virtuel du serveur de boîtes aux lettres [%1]. Exchange ActiveSync ne peut pas accéder au serveur lorsque l'authentification basée sur les formulaires est activée.

Pour plus d'informations sur la façon de configurer correctement les paramètres des répertoires virtuels Exchange, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft. 817379 (http://support.microsoft.com/kb/817379/) Des erreurs Exchange ActiveSync et Outlook Mobile Access se produisent lorsque Exchange Server 2003 nécessite une authentification SSL ou une authentification basée sur les formulaires

Événement 3

Type d'événement : Erreur
Source de l'événement : Exchange Server ActiveSync
Catégorie de l'événement : Aucune
ID de l'événement : 3031
Description : Le serveur de boîtes aux lettres [%1] n'autorise pas l'authentification par négociation sur son répertoire virtuel [%2]. Exchange ActiveSync peut accéder au serveur uniquement à l'aide de ce modèle d'authentification.

Pour plus d'informations sur la façon de configurer les paramètres des répertoires virtuels Exchange, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft. 817379 (http://support.microsoft.com/kb/817379/) Des erreurs Exchange ActiveSync et Outlook Mobile Access se produisent lorsque Exchange Server 2003 nécessite une authentification SSL ou une authentification basée sur les formulaires Pour plus d'informations sur la façon de configurer correctement IIS (Internet Information Services) pour la prise en charge de l'authentification Kerberos et NTLM, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft. 215383 (http://support.microsoft.com/kb/215383/) Comment faire pour configurer IIS pour la prise en charge du protocole Kerberos et du protocole NTLM poir l'authentification réseau Ce problème peut se produire lorsque vous avez installé Microsoft Windows SharePoint Services sur un serveur qui exécute Exchange Server 2003. Pour plus d'informations sur la façon de configurer correctement à la fois Windows SharePoint Services et Exchange Server 2003, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft. 823265 (http://support.microsoft.com/kb/823265/) Vous recevez le message d'erreur « Page non trouvée » lorsque vous utilisez Outlook Web Access (OWA) pour parcourir le client Exchange Server 2003 après avoir installé Windows SharePoint Services

Cause

Exchange Server ActiveSync et Exchange Outlook Mobile Access (OMA) utilisent le répertoire virtuel /Exchange pour accéder aux modèles OWA et au protocole DAV (Distributed Authoring and Versioning) sur les serveurs principaux Exchange contenant la boîte aux lettres de l'utilisateur. Exchange Server ActiveSync et OMA ne peuvent pas accéder à ce répertoire virtuel si l'une des conditions suivantes est vérifiée :

- Le répertoire virtuel /Exchange sur un serveur principal Exchange est configuré pour utiliser SSL.
- L'authentification basée sur les formulaires est activée.

Ce problème ne se produit pas lorsque vous activez ces paramètres sur le répertoire virtuel /Exchange d'un serveur frontal.

Remarque Il n'est pas nécessaire d'exécuter les méthodes décrites dans la section « Résolution » pour configurer un serveur frontal de sorte qu'il requière SSL et pour activer l'authentification basée sur les formulaires sur le serveur frontal.

Remarque Si vous exécutez Microsoft Small Business Server 2003, les spécifications décrites dans la Méthode 1 et la Méthode 2 de la section « Résolution » sont automatiquement configurées lors de l'installation. Si vous recevez les erreurs décrites dans la section « Symptômes » avec Small Business Server 2003, exécutez l'Assistant Configuration de la messagerie et de la connexion Internet. Cet Assistant vous aide à reconfigurer le répertoire virtuel /Exchange et l'authentification basée sur les formulaires pour une utilisation avec Outlook Mobile Access et Exchange ActiveSync.

Résolution

Pour résoudre ce problème, appliquez l'une des méthodes ci-dessous :

Méthode 1

Installez et configurez un ordinateur Exchange Server 2003 comme serveur frontal. Pour plus d'informations, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft. 818476 (http://support.microsoft.com/kb/818476/) Possibilité de configurer Exchange Server 2003 Édition Standard ou Exchange Server 2003 Édition Entreprise en tant que serveur frontal

Méthode 2

Avertissement Des problèmes sérieux peuvent se produire si vous modifiez le Registre de façon incorrecte à l'aide de l'Éditeur du Registre ou de toute autre méthode. Ces problèmes peuvent vous obliger à réinstaller le système d'exploitation. Microsoft ne peut pas garantir que ces problèmes puissent être résolus. Vous assumez l'ensemble des risques liés à la modification du Registre.

Important La Méthode 2 doit être utilisée exclusivement dans un environnement ne comportant aucun serveur frontal Exchange Server 2003. Vous pouvez apporter des modifications au Registre uniquement sur le serveur sur lequel se trouvent les boîtes aux lettres.

Créez un répertoire virtuel secondaire pour Exchange qui ne requiert pas SSL, puis ajoutez une valeur de Registre pointant sur ce nouveau répertoire virtuel. Pour créer un répertoire virtuel secondaire pour Exchange basé sur les étapes 1 à 4 de la procédure suivante, assurez-vous que l'authentification basée sur les formulaires est désactivée pour le répertoire virtuel Exchange avant d'effectuer la copie. Avant d'effectuer cette procédure, désactivez l'authentification basée sur les formulaires dans le Gestionnaire système Exchange, puis redémarrez IIS.

En outre, vous devez utiliser le Gestionnaire des services Internet (IIS) pour créer ce répertoire virtuel pour que Exchange ActiveSync et Outlook Mobile Access puissent fonctionner. Si vous utilisez Windows Server 2003, procédez comme suit.

Remarques Ces étapes affectent les connexions Outlook Mobile Access comme les connexions Exchange ActiveSync. Une fois ces étapes effectuées, les connexions Outlook Mobile Access et Exchange ActiveSync utilisent le nouveau répertoire virtuel que vous aurez créé.

1. Démarrez le Gestionnaire des services Internet.
2. Localisez le répertoire virtuel Exchange. L'emplacement par défaut est le suivant : Web Sites\Default Web Site\Exchange
3. Cliquez avec le bouton droit sur le répertoire virtuel Exchange, cliquez sur **Toutes les tâches**, puis sur **Sauvegarder la configuration dans un fichier**.
4. Dans la zone **Nom de fichier**, tapez un nom. Par exemple, tapez **RépExchange**. Cliquez ensuite sur **OK**.
5. Cliquez avec le bouton droit sur la racine de ce site Web. En général, il s'agit de Site Web par défaut. Cliquez sur **Nouveau**, puis sur **Répertoire virtuel (à partir du fichier)**.
6. Dans la boîte de dialogue **Importer une configuration**, cliquez sur **Parcourir**, recherchez le fichier créé à l'étape 4, cliquez sur **Ouvrir**, puis sur **Fichier de lecture**.
7. Sous **Sélectionnez une configuration à importer**, cliquez sur **Exchange**, puis sur **OK**.

   Une boîte de dialogue indiquant que le « répertoire virtuel existe déjà » s'affiche.
8. Dans la zone **Alias**, tapez un nom pour le nouveau répertoire virtuel à utiliser par Exchange ActiveSync et Outlook Mobile Access. Par exemple, tapez **exchange-oma**. Cliquez ensuite sur **OK**.
9. Cliquez avec le bouton droit sur le nouveau répertoire virtuel. Dans cet exemple, cliquez sur **exchange-oma**. Cliquez sur **Propriétés**.
10. Cliquez sur l'onglet **Sécurité de répertoire**.
11. Sous **Authentification et contrôle d'accès**, cliquez sur **Modifier**.
12. Assurez-vous que seules les méthodes d'authentification suivantes sont activées, puis cliquez sur **OK** :
    - **Authentification Windows intégrée**
    - **Authentification de base**
13. Sous **Restrictions par adresse IP et nom de domaine**, cliquez sur **Modifier**.
14. Cliquez sur **refusé**, sur **Ajouter**, sur **Ordinateur unique**, tapez l'adresse IP du serveur que vous configurez, puis cliquez sur **OK**.
15. Sous **Sécurisation des communications**, cliquez sur **Modifier**. Assurez-vous que l'option **Requérir un canal sécurisé (SSL)** n'est pas sélectionnée, puis cliquez sur **OK**.
16. Cliquez sur **OK**, puis fermez le Gestionnaire IIS.
17. Cliquez sur **Démarrer**, puis sur **Exécuter**. Tapez **regedit**, puis cliquez sur **OK**.
18. Recherchez la sous-clé de Registre suivante : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MasSync\Parameters
19. Cliquez avec le bouton droit sur **Paramètres**, pointez sur **Nouveau**, puis cliquez sur **Valeur chaîne**.
20. Tapez **ExchangeVDir**, puis appuyez sur ENTRÉE. Cliquez avec le bouton droit sur **ExchangeVDir**, puis cliquez sur **Modifier**.

    RemarqueExchangeVDir respecte la casse. Si vous ne tapez pas **ExchangeVDir** exactement comme il apparaît dans cet article, ActiveSync ne trouve pas la clé lorsqu'il recherche le dossier **exchange-oma**.
21. Dans la zone **Données de la valeur**, tapez le nom du nouveau répertoire virtuel que vous avez créé à l'étape 8. Par exemple, tapez **exchange-oma**. Cliquez ensuite sur **OK**.
22. Quittez l'Éditeur du Registre.
23. Redémarrez le service d'administration IIS. Pour cela, procédez comme suit :
    a. Cliquez sur **Démarrer**, sur **Exécuter**, tapez **services.msc**, puis cliquez sur **OK**.
    b. Dans la liste de services, cliquez avec le bouton droit sur **Service d'administration IIS**, puis cliquez sur **Redémarrer**.

Remarque Si votre serveur est Microsoft Windows Small Business Server 2003 (SBS), le nom du répertoire virtuel Exchange OMA doit être **exchange-oma.**

L'installation intégrée de Microsoft Windows Small Business Server 2003 crée le répertoire virtuel **exchange-oma** dans IIS. En outre, il pointe la clé de Registre ExchangeVDir sur **/exchange-oma** lors de l'installation initiale. D'autres assistants SBS, tel que l'**Assitant Configuration de la messagerie et de la connexion Internet (CEICW)** supposent également que le nom de répertoire virtuel dans IIS est **exchange-oma.**

Plus d'infomations

Pour accéder au contenu de la boîte aux lettres d'un utilisateur dans Exchange Server 2003, les répertoires virtuels Microsoft-Serveur-ActiveSync et Outlook Mobile Access effectuent une ouverture de session DAV explicite au répertoire virtuel Exchange. L'appel est similaire au suivant : http://*nom_netbios_serveur_boîtes_aux_lettres*/exchange/*alias_boîte_aux_lettres* Les répertoires virtuels Microsoft Server ActiveSync et Outlook Mobile Access ne peuvent pas accéder au contenu de la boîte aux lettres de l'utilisateur si le répertoire virtuel Exchange est configuré pour utiliser SSL. Les répertoires virtuels Microsoft-Serveur-ActiveSync et Outlook Mobile Access essaient seulement de se connecter au répertoire virtuel Exchange via le port TCP 80 (HTTP), et non via le port TCP 443 (HTTPS).

Outlook Mobile Access essaie de se connecter au répertoire virtuel Exchange en utilisant toutes les méthodes d'authentification suivantes :

- Kerberos
- NTLM
- De base

Lorsque vous configurez l'authentification par formulaire sur le serveur Exchange Server 2003, la méthode d'authentification pour le répertoire virtuel Exchange est définie sur l'authentification de base, et le domaine par défaut est défini sur la barre oblique inverse. Le répertoire virtuel Microsoft-Serveur-ActiveSync peut se connecter uniquement au répertoire virtuel Exchange à l'aide de l'authentification Kerberos.

Les informations contenues dans cet article s'appliquent au(x) produit(s) suivant(s):

Mots-clés : kbtshoot kbprb KB817379

L'INFORMATION CONTENUE DANS CE DOCUMENT EST FOURNIE PAR MICROSOFT SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE. L'UTILISATEUR ASSUME LE RISQUE DE L'UTILISATION DU CONTENU DE CE DOCUMENT. CE DOCUMENT NE PEUT ETRE REVENDU OU CEDE EN ECHANGE D'UN QUELCONQUE PROFIT.

Vous avez besoin d'une aide supplémentaire ?
Contactez le support technique par email, en ligne ou par téléphone

Aide et Support Microsoft

Microsoft
©2010 Microsoft

Annexe 14 : Evénement d'avertissement Microsoft numéro 3033

(Microsoft Corporation, 2007a)

Numéro d'article: 905013 - Dernière mise à jour: mercredi 21 novembre 2007 - Version: 3.4

Configuration du pare-feu de l'entreprise pour la technologie ActiveSync Direct Push Exchange

INTRODUCTION

Après l'installation de Microsoft Exchange Server 2003 Service Pack 2 (SP2), un événement d'avertissement semblable au suivant est enregistré dans le journal des événements d'application :

Type d'événement : Avertissement
Source de l'événement : Server ActiveSync
Catégorie de l'événement : Aucune
ID de l'événement : 3033
Date :
Heure :
Utilisateur :
Ordinateur :
Nom_ordinateur
Description :
La moyenne des intervalles d'interrogation les plus récents [200] utilisés par les clients est inférieure ou égale à [9]. Assurez-vous que votre configuration de pare-feu est configurée pour fonctionner correctement avec la technologie Exchange ActiveSync et Direct Push. Plus précisément, assurez-vous que votre pare-feu est configuré de sorte que les demandes à Exchange ActiveSync n'expirent pas avant de pouvoir être traitées.

Ce problème peut se produire si le pare-feu n'a pas été configuré pour conserver les requêtes HTTP(S) actives plus longtemps que l'intervalle d'interrogation minimum configuré sur le serveur Exchange Server 2003 SP2. Par défaut, l'intervalle d'interrogation minimum auquel le serveur Exchange déclenche cet événement est de neuf minutes.

Plus d'informations

Pour résoudre ce problème, modifiez les valeurs de délai d'attente du pare-feu pour les connexions HTTP(S) au serveur Exchange de sorte qu'elles soient supérieures à la limite de délai d'attente par défaut de huit minutes.

Remarque Cette connexion ne fait pas référence au champ **Délai de connexion** situé dans le composant logiciel enfichable IIS pour la console MMC. Ou bien, modifiez l'intervalle d'interrogation minimum. Nous vous recommandons de définir la valeur de délai d'attente du pare-feu avec 15 minutes ou une valeur supérieure pour que la fonctionnalité AUTD de la technologie Direct Push Exchange fonctionne de façon optimale.

L'intervalle d'interrogation est le laps de temps calculé par un périphérique mobile entre les pings du périphérique mobile au serveur. La session entre le serveur et le périphérique mobile se termine si l'une des conditions suivantes est remplie :

- Aucun message électronique n'arrive dans la boîte aux lettres pour initialiser une notification.
- Aucune réponse n'est reçue du serveur avant l'expiration de l'intervalle d'interrogation.

La technologie Direct Push Exchange utilise cet intervalle d'interrogation pour maintenir la connectivité entre le serveur et le périphérique mobile. Par conséquent, une session est ouverte pour que le serveur puisse notifier le périphérique mobile lors de la réception d'un message électronique.

Exchange Server 2003 maintient une fenêtre défilante des intervalles d'interrogation les plus récents fournis au serveur par les clients mobiles. La valeur par défaut de cette fenêtre défilante est de 200 intervalles d'interrogation. Vous pouvez configurer cette valeur dans la clé de Registre HbiSampleSize. Toutefois, il est très peu probable que la valeur par défaut doive être ajustée. Consultez le tableau présenté dans cette section répertoriant les valeurs de la clé de Registre HbiSampleSize.

Un événement est enregistré dans le journal des événements d'application lorsque les deux conditions suivantes sont remplies :

- La moyenne des intervalles d'interrogation dans cette fenêtre défilante est inférieure ou égale au seuil d'alerte.
- Il existe des exemples HbiSampleSize.

Le seuil d'alerte par défaut est de 540 secondes (9 minutes). Toutefois, vous pouvez configurer le seuil d'alerte dans la clé de Registre HbiAlertThreshold. Consultez le tableau présenté dans cette section répertoriant les valeurs de la clé de Registre HbiAlertThreshold. L'événement ne sera pas enregistré plus d'une fois par heure. Il est très peu probable que la valeur par défaut doive être ajustée.

Nous vous recommandons d'augmenter les valeurs de délai d'attente du pare-feu pour les requêtes HTTP(S) au répertoire virtuel Microsoft-Server-ActiveSync d'Exchange Server pour offrir une expérience plus riche « toujours à jour ». La méthode que vous utilisez pour augmenter les valeurs de délai d'attente du pare-feu dépend du produit pare-feu utilisé. Reportez-vous à la documentation du pare-feu pour obtenir des informations sur la façon d'augmenter les valeurs de délai d'attente du pare-feu.

Pour configurer les valeurs du délai d'attente de session de Microsoft Internet Security and Acceleration Server (ISA) 2004 pour la technologie Direct Push Exchange

1. Dans l'arborescence de la console **Gestion ISA Server**, cliquez sur **Stratégie de pare-feu**.
2. Sous l'onglet **Boîte à outils**, cliquez sur **Objets de réseau**.
3. Développez le nœud **Ports d'écoute Web**, puis affichez les propriétés du port d'écoute Web concerné.
4. Cliquez sur l'onglet **Préférences**, puis sur **Avancées**.
5. Modifiez le **Délai de connexion** de la valeur par défaut de 120 secondes (2 minutes) en 1800 secondes (30 minutes).
6. Cliquez deux fois sur **OK** pour accepter les modifications.
7. Cliquez sur **Appliquer**.

Le tableau suivant contient les valeurs qui peuvent être modifiées dans la mesure où elles sont liées à l'intervalle d'interrogation. Ces valeurs de Registre n'existent pas dans une nouvelle installation d'Exchange Server 2003 SP2. Le serveur rétablit les valeurs par défaut codées de manière irréversible si ces valeurs de Registre sont manquantes. L'administrateur doit créer ces valeurs de Registre manuellement s'il souhaite définir les valeurs. Ces valeurs peuvent être définies dans la clé de Registre suivante : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MasSync\Parameters

Nom	Type de données	Valeurs	Par défaut	Description
MinHeartbeatInterval	DWORD	1 - MaxHearbeatInterval	60 secondes	Intervalle d'interrogation minimum
MaxHeartbeatInterval	DWORD	MinHeartbeatInterval -3540	2700 secondes (45 minutes)	Intervalle d'interrogation maximum
HbiSampleSize	DWORD	1 ou valeur supérieure	200 exemples	Taille de l'exemple d'intervalle d'interrogation
HbiAlertThreshold	DWORD	1 ou valeur supérieure	480 secondes	Seuil d'alerte de l'intervalle d'interrogation

Remarques

- Dans ce tableau, la valeur « 1 - MaxHearbeatInterval » indique une valeur comprise entre 1 et la valeur de MaxHearbeatInterval. De même, la valeur « MinHeartbeatInterval -3540 » indique une valeur comprise entre la valeur de MinHeartbeatInterval et 3540.
- Si l'une de ces valeurs est définie dans le Registre et que la valeur spécifiée est en dehors des valeurs répertoriées pour ce paramètre, l'initialisation d'Exchange ActiveSync rétablira les valeurs par défaut. En outre, un ID d'événement sera enregistré dans le journal des événements d'application. Toutefois, aucun événement n'est enregistré dans le journal des événements d'application si la valeur est définie sur zéro. Lorsqu'une valeur est définie sur zéro, le programme se comporte comme si la valeur était absente. En d'autres termes, il utilise la valeur par défaut codée de manière irréversible.
- Exchange ActiveSync lit ces valeurs une fois lors du démarrage. Par conséquent, si un administrateur décide de modifier les valeurs, le service d'administration IIS doit être redémarré pour que les modifications soient appliquées.

Les informations contenues dans cet article s'appliquent au(x) produit(s) suivant(s):

Mots-clés : kbexchmobility KB905013

L'INFORMATION CONTENUE DANS CE DOCUMENT EST FOURNIE PAR MICROSOFT SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE. L'UTILISATEUR ASSUME LE RISQUE DE L'UTILISATION DU CONTENU DE CE DOCUMENT. CE DOCUMENT NE PEUT ETRE REVENDU OU CEDE EN ECHANGE D'UN QUELCONQUE PROFIT.

Vous avez besoin d'une aide supplémentaire ?
Contactez le support technique par email, en ligne ou par téléphone

Aide et Support Microsoft

Microsoft
©2010 Microsoft

Bibliographie

Apple Inc. 2010a. iPhone en entreprise - Intégration. *Apple.* [En ligne] Apple Inc., 24 Juin 2010. [Citation : 1 Décembre 2010.] http://www.apple.com/fr/iphone/business/integration/.

—. 2010b. iPhone en entreprise - Exchange ActiveSync. *Apple.* [En ligne] Apple Inc., 8 Octobre 2010. [Citation : 1 Décembre 2010.] http://images.apple.com/fr/iphone/business/docs/iPhone_ EAS.pdf.

ARNAUDO, Fabrice. 2005. Solution mobilité BlackBerry. *Techniques de l'ingénieur*. Weka, 2005.

AUFFRAY, Christophe. 2009. Système d'information : comment garantir performance et qualité de service ? *ZDNet France.* [En ligne] CBS Interactive, 28 Septembre 2009. [Citation : 1 Décembre 2010.] http://www.zdnet.fr/actualites/systeme-d-information-comment-garantir-performance-et-qualite-de-service-39707538.htm.

BEL, Vincent, NATAF, Sarah et VEYSSET, Franck. 2004. Techniques de supervision de la sécurité des réseaux IP. *Techniques de l'ingénieur*. Weka, 2004.

BERGSTRA, Jan et BURGESS, Mark. 2007. *Handbook of Network and System Administration.* s.l. : Elsevier Science Ltd, 2007. p. 1028.

Bouygues Telecom. 2010. Pré-requis Techniques - BlackBerry Enterprise Server (BES) Version 5.x For Microsoft Exchange 2003, 2007, 2010. *LabI2s.* [En ligne] Bouygues Telecom, 31 Mars 2010. [Citation : 1 Décembre 2010.] http://www.labi2s.com/mmu/prerequis/blackberry_5.x_ exchange_prerequis.pdf.

CHEVASSUS, Madeleine. 2003. Administration des systèmes d'information. *Techniques de l'ingénieur*. Weka, 2003.

Cisco Systems. 2007a. Cisco IOS NetFlow Version 9 Flow-Record Format. *Cisco Systems.* [En ligne] Cisco System, Inc., Février 2007. [Citation : 1 Décembre 2010.] http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.pdf.

—. 2007b. Introduction to Cisco IOS NetFlow. *Cisco Systems.* [En ligne] Cisco System, Inc., Octobre 2007. [Citation : 1 Décembre 2010.] http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.pdf.

COHEN, Peter. 2008. iPhone ready to take on BlackBerry with enterprise push. *Macworld.com.* [En ligne] Mac Publishing LLC, 6 Mars 2008. [Citation : 1 Décembre 2010.] http://www.macworld.com/article/132399/2008/03/enterprise.html.

Comment ça marche. 2008. Introduction au chiffrement avec DES. *Comment ça marche.* [En ligne] Quidea, 14 Octobre 2008. [Citation : 1 Décembre 2010.] http://www.commentcamarche.net/contents/crypto/des.php3.

DEGOULET, Patrice. 2005. Dossier patient informatisé. *Laboratoire de Santé Publique et Informatique Médicale.* [En ligne] 9 Novembre 2005. [Citation : 1 Décembre 2010.] www.spim.jussieu.fr/IMG/pdf/dossier.2005.P2.partie1.pdf.

Hewlett-Packard. 2004. OpenView - Network Node Manager. *Hewlett-Packard.* [En ligne] Hewlett-Packard, 2004. [Citation : 1 Décembre 2010.] http://h41087.www4.hp.com/solutions/entreprises/grandes_entreprises/openview/fiche_produit/infrastructure/nnm.html.

—. 2005. OpenView - Operations for Windows. *Hewlett-Packard.* [En ligne] Hewlett-Packard, 2005. [Citation : 1 Décembre 2010.] http://h41087.www4.hp.com/solutions/entreprises/ grandes_entreprises/openview/fiche_produit/infrastructure/op_windows.html.

—. 2010a. HP Operations Center. *Hewlett-Packard.* [En ligne] Hewlett-Packard, 1 Février 2010. [Citation : 1 Décembre 2010.] https://h10078.www1.hp.com/cda/hpdc/navigation.do?action=downloadPDF&caid=29005&cp=54_4000_100&zn=bto&filename=4AA2-0443ENW.pdf.

—. 2010b. HP Network Management Center. *Hewlett-Packard.* [En ligne] Hewlett-Packard, Avril 2010. [Citation : 1 Décembre 2010.] https://h10078.www1.hp.com/cda/hpdc/navigation.do?action=downloadPDF&caid=9604&cp=54_4000_100&zn=bto&filename=4AA1-6185ENW.pdf.

IBM Corporation. 2005. IBM Informix SNMP Subagent Guide. *IBM.* [En ligne] IBM Corporation, 2 Novembre 2005. [Citation : 1 Décembre 2010.] http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.snmp.doc/snmp60.htm.

IETF. 1990. RFC 1157 - A Simple Network Management Protocol (SNMP). s.l. : IETF, Mai 1990. p. 36.

InfotechGuyz. 2008. How a BlackBerry Infrastructure Works. *InfotechGuyz.com.* [En ligne] InfotechGuyz, 20 Juillet 2008. [Citation : 1 Décembre 2010.] http://www.infotechguyz.com/BlackBerryServer/BlackBerryInfrastructure.html.

Kozierok, Charles M. 2005. *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.* s.l. : No Starch Press, 2005. p. 1616.

LE YAVANC, Eric. 2009. iPhone et Microsoft Exchange: 10 étapes pour profiter du push mail. *Business Mobile.* [En ligne] CBS Interactive, 16 Janvier 2009. [Citation : 1 Décembre 2010.] http://www.businessmobile.fr/actualites/iphone-et-microsoft-exchange-10-etapes-pour-profiter-du-push-mail-39382450.htm.

LEVY-ABEGNOLI, Thierry. 2005. Supervision: comment Aelia anticipe les pannes de son réseau monétique. *ZDNet France.* [En ligne] CBS Interactive, 24 Octobre 2005. [Citation : 1 Décembre 2010.] http://www.zdnet.fr/actualites/supervision-comment-aelia-anticipe-les-pannes-de-son-reseau-monetique-39281200.htm.

MAURO, Douglas R. et SCHMIDT, Kevin J. 2005. *Essential SNMP.* Second Edition. s.l. : O'Reilly Media, 2005. p. 442. Vol. 2005.

MERETHIS. 2010. Centreon software. *Centreon* [En ligne] MERETHIS, 3 Novembre 2010. [Citation : 1 Décembre 2010.] http://www.centreon.com/documents/Products/MERETHIS-Centreon-Fr.pdf.

Microsoft Corporation. 2001. Monitoring in .NET Distributed Application Design. *Microsoft MSDN.* [En ligne] Microsoft Corporation, Août 2001. [Citation : 1 Décembre 2010.] http://msdn.microsoft.com/en-us/library/ee817668.aspx.

—. 2007a. Configuration du pare-feu de l'entreprise pour la technologie ActiveSync Direct Push Exchange. *Aide et support Microsoft.* [En ligne] Microsoft Corporation, 21 Novembre 2007. [Citation : 1 Décembre 2010.] http://support.microsoft.com/kb/905013.

—. 2007b. Des erreurs Exchange ActiveSync et Outlook Mobile Access se produisent lorsque Exchange Server 2003 nécessite une authentification SSL ou une authentification par

formulaire. *Aide et support Microsoft.* [En ligne] Microsoft Corporation, 29 Novembre 2007. [Citation : 1 Décembre 2010.] http://support.microsoft.com/kb/817379.

—. 2007c. Comment faire pour implémenter SSL dans IIS. *Aide et support Microsoft.* [En ligne] Microsoft Corporation, 3 Décembre 2007. [Citation : 1 Décembre 2010.] http://support.microsoft.com/kb/ 299875/.

—. 2009a. What is new with Exchange Server 2010 ActiveSync and Outlook Mobile? *TechNet Blogs.* [En ligne] Microsoft Corporation, 31 Mai 2009. [Citation : 1 Décembre 2010.] http://blogs.technet.com/b/ucedsg/archive/2009/05/31/what-is-new-with-exchange-server-2010-activesync-and-outlook-mobile.aspx.

—. 2009b. Microsoft System Center Operations Manager 2007 R2. *Microsoft System Center.* [En ligne] Microsoft Corporation, 27 Août 2009. [Citation : 1 Décembre 2010.] http://download.microsoft.com/documents/France/Serveur/2009/systemcenter/operations-manager/Datasheet_SCOM_2007_ R2_FR.pdf.

—. 2009c. Microsoft System Center Virtual Machine Manager 2008 R2. *Microsoft System Center.* [En ligne] Microsoft Corporation, 11 Décembre 2009. [Citation : 1 Décembre 2010.] http://download.microsoft.com/documents/France/Serveur/2009/systemcenter/Dadasheet-VMM-2008-R2-FR.pdf.

—. 2010. Présentation de Direct Push. *Microsoft TechNet.* [En ligne] Microsoft Corporation, 18 Mars 2010. [Citation : 1 Décembre 2010.] http://technet.microsoft.com/fr-fr/library/aa997252.aspx.

MILLER, Mark A. 1997. *Managing Internetworks With Snmp.* s.l. : M & T Books, 1997. p. 704.

Nagios Enterprises. 2009. Nagios Screenshots. *Nagios.* [En ligne] Nagios Enterprises, LLC, 2009. [Citation : 1 Décembre 2010.] http://www.nagios.org/about/screenshots.

—. 2010. Nagios XI – Product Overview. *Nagios.* [En ligne] Nagios Enterprises, LLC, Janvier 2010. [Citation : 1 Décembre 2010.] http://assets.nagios.com/datasheets/nagiosxi/Nagios%20XI%20-%20Product%20Overview.pdf.

Paessler. 2010a. PRTG Network Monitor - intuitive network monitoring software. *Paessler.* [En ligne] Paessler, 2010. [Citation : 1 Décembre 2010.] http://www.paessler.com/prtg.

—. 2010b. PRTG Network Monitor V7 - User Manual. *Paessler*. [En ligne] Paessler, 4 Mars 2010. [Citation : 1 Décembre 2010.] http://download.paessler.com/download/ prtg7manual.pdf.

—. 2010c. PRTG Network Monitor - The All-In Monitoring Solution. *Paessler*. [En ligne] Paessler, 7 Septembre 2010. [Citation : 1 Décembre 2010.] http://media.paessler.com/ common/files/pdf/productflyer_prtg_en_r2165.pdf.

PERAIRE, Sandra, FONTAINE, Sébastien et CALON, Stéphane. 2007. SNMP. *FrameIP*. [En ligne] FrameIP TcpIP, 9 Décembre 2007. [Citation : 1 Décembre 2010.] http://www.frameip.com/snmp/.

PIGNET, François. 2008. *Réseaux informatique - Supervision et administration.* s.l. : Editions ENI, 2008. p. 274.

PUJOLLE, Guy. 2007. *Les Réseaux.* édition 2008. s.l. : Eyrolles, 2007. p. 1099.

Research In Motion. 2009. Surveillance de BlackBerry Enterprise Server. *BlackBerry.* [En ligne] Research In Motion, 27 Avril 2009. [Citation : 1 Décembre 2010.] http://fr.blackberry.com/services/ business/server/express/pdf-monitoring-service.pdf.

—. 2010a. Getting Started with BlackBerry Enterprise Server Express for Microsoft Exchange. *BlackBerry.* [En ligne] Research In Motion, 2010. [Citation : 1 Décembre 2010.] http://us.blackberry.com/apps-software/business/server/express/gettingstarted.jsp.

—. 2010b. Tableau de comparaison BlackBerry. *BlackBerry.* [En ligne] Research In Motion, 8 Février 2010. [Citation : 1 Décembre 2010.] http://fr.blackberry.com/services/business/ server/express/pdf-comparison-chart.pdf.

—. 2010c. Using BlackBerry MDS Connection Service log files to view information for proxied connections to BlackBerry devices. *BlackBerry.* [En ligne] Research In Motion, 16 Février 2010. [Citation : 1 Décembre 2010.] http://docs.blackberry.com/en/admin/ deliverables/14334/Using_BB_MDS_CS_log_files_view_proxied_BB_connect_579081_ 11.jsp.

STALLINGS, William. 2010. *Cryptography and Network Security: Principles and Practice.* 5th Edition. s.l. : Prentice Hall, 2010. p. 744.

The Cacti Group. 2010. About Cacti. *Cacti* [En ligne] The Cacti Group, 2010. [Citation : 1 Décembre 2010.] http://www.cacti.net/.

TUNSTALL, Craig et COLE, Gwyn. 2002. *Developing WMI Solutions: A Guide to Windows Management Instrumentation.* s.l. : Addison-Wesley Professional, 2002. p. 816.

WILLM, Olivier. 2003. Administration de réseaux informatiques : protocole SNMP. *Techniques de l'ingénieur*. Weka, 2003.

Liste des figures

Liste des tableaux

Table des matières

RESUME

Les solutions de supervision de réseau jouent désormais un rôle essentiel dans les systèmes d'information. La solution mise en place à la clinique Saint-Augustin suite à l'implémentation du dossier patient informatisé devait garantir la continuité de service des fonctions critiques. Il fallait concilier prévention et détection rapide des pannes en tenant compte d'un budget limité. Le projet a été réalisé en comparant les différents produits sur le marché, puis en analysant les éléments critiques du réseau pour y implanter les sondes, puis en créant un système de remontée d'alertes par push-mail sur téléphones portables.

Mots clés : Supervision de réseau, SNMP, sondes, push-mail, alertes, protocole.

SUMMARY

Network management solutions now play an essential role in information systems. The solution implemented at the clinique Saint-Augustin following the implementation of computerized patient records was meant to ensure the continuity of critical functions. The purpose was both the prevention and early detection of failures while operating on a restricted budget. The project involved comparing the different products on the market, then analyzing the critical elements of the network to position the probes, then creating a system of feedback alerts by push email on mobile phones.

Key words : Network Management, SNMP, probes, push-mail, alerts, protocol.