OFFRE SUPERVISION RESEAU

Novembre 11

VOTRE CONTACT COMMERCIAL	

FLORENCE LAPREVOTE LIGNE DIRECTE : 01 34 93 35 30 EMAIL : FLAPREVOTE@ORSENNA.FR

VOTRE CONTACT TECHNIQUE	

JEAN-PHILIPPE SENCKEISEN EMAIL : JPSENCKEISEN@ORSENNA.FR

TABLE DES MATIERES

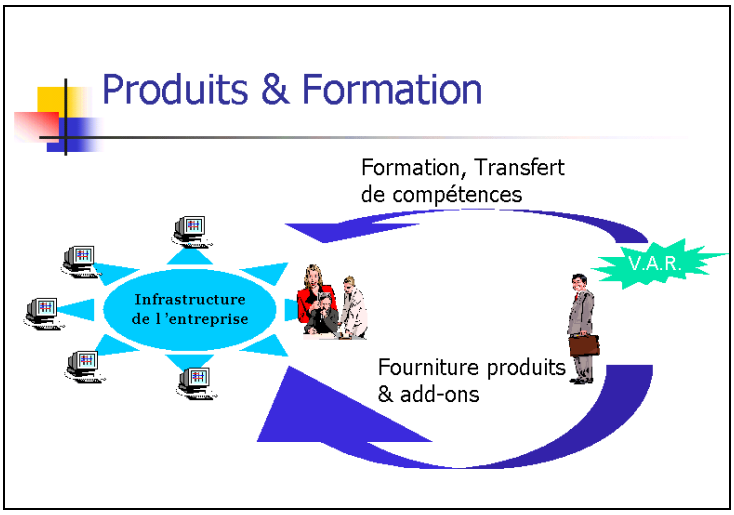
1 NOTRE REPONSE A VOS BESOINS

1.1 LE CONTEXTE

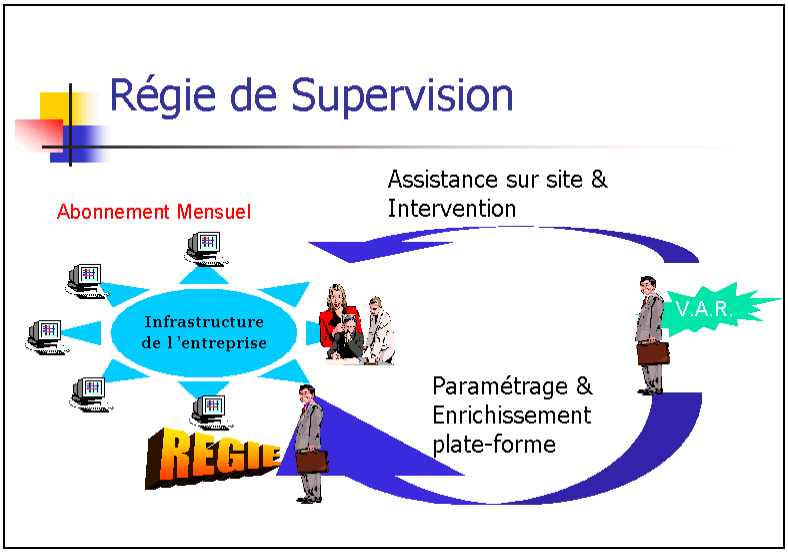
Si vous disposez d'une plateforme de supervision réseau ou si vous souhaitez en acquérir une, Orsenna propose une offre complète autour de ces produits :

- ***Fourniture des produits et des adds-ons (SMS, Serveur SYSLOG , MIB Browser,..) ;***
- ***Package de formation complémentaire ;***
- ***Régie de supervision : le contrat de service pour votre offre de supervision;***
- ***Package de supervision : l'ingénierie complète de votre solution*** ;

Ce document a pour objectif de décrire les items qui peuvent être proposés dans le cadre de votre projet.



Offre Produits & Formation 1



Offre Régie de supervision 1

1.2 NOTRE METIER, VOUS ACCOMPAGNEZ SUR VOS PROJETS DE SUPERVISION

Spécialiste des projets de supervision réseau, Orsenna apporte son expertise aux différents stades de vos projets.

1.2.1 Missions d'analyse du marché

Orsenna *est missionné régulièrement par les éditeurs ou les intégrateurs* afin de réaliser :

- Etude technique comparative des outils de supervisions (Ex: Ipswitch)
- Animation de séminaire de présentation d'outils de supervisions (Ex : Ipvista, Ipswitch, Solarwinds, Ground Work)

1.2.2 Benchmarks

Nous réalisons régulièrement une validation des produits du marché sur notre plate-forme de tests soit au titre de la veille technologique soit pour des besoins ponctuels de clients.

Notre plate-forme est constituée par des environnements variés au niveau des équipements et des plates-formes applicatives. Nous disposons aussi de plusieurs simulateurs d'objets réseaux afin d'évaluer les performances des outils pour des configurations comportant plusieurs milliers d'équipements.

1.2.3 Mise en œuvre

A ce titre Orsenna intervient sur *les projets de supervision auprès de grands comptes* dans différents secteurs d'activité tels :

Transport	COFIROUTE; SERVAIR, APPR
Banques, Assurances	FIDEURAM BANK ; BANQUE POPULAIRE, GIE Carte Bancaire, GMF, Caisse des Dépôts, Société Générale
Distribution	BRICORAMA; RELAY, NICOLAS, AELIA, HISTOIRE D'OR, LANVIN, MAC DONALDS, MIDAS
Industries	SCHLUMBERGER; ALCAN, ARCELOR, DANONE, EADS, IMAJE, STRYKER
Administration	ADEME, OPERA DE PARIS, MINISTERE DEFENSE
Ecoles, Universités	ENSAE, ENSTA,
Mairies, Conseil	Ville TROYES, CG16, CR PACA
Opérateur	CORIOLIS, B3G

Nous travaillons aussi en *sous-traitance pour les intégrateurs* du marché (EADS, TELINDUS, ALCATEL, DCI).

1.2.4 Développement

Orsenna réalise des développements complémentaires autour des outils de supervision su marché afin d'enrichir le périmètre de supervision des équipements.

A ce titre des plug-ins pour le logiciel WhatsUp ont été développés pour :

- SSH
- NRPE
- Oracle
- MySql
- Apache
- Websphere
- DNS…

1.3 PARTENAIRES

Orsenna s'appuie sur les produits du marché en intégrant les solutions adaptées à votre environnement avec 5 éditeurs de logiciels de supervision réseau :

IPSWITCH	Editeur de WhatsUp
SOLARWINDS.NET Network Management Tools	Editeur d'Orion et Kiwi Syslog
PAESSLER the network monitoring company	Editeur de PRTG
plixer International	Editeur de Scrutinizer (Logiciel Netflow, Sflow, Jflow)
inveaTECH	Editeur de Flow Mon (Appliance Netflow, Sflow, Jflow))

En complément Orsenna s'appuie sur des outils du marché pour enrichir les fonctionnalités de la console de supervision :

pathSolutions	Editeur de Switch Monitor
SOLARWINDS.NET Network Management Tools	Editeur de Solarwinds Engineer Toolset
SNMP Informant	Editeur de composants SNMP

1.4 OPEN SOURCE

Orsenna s'appuie également sur les environnements Open Source afin d'enrichir les solutions clientes:

Nagios® XI™	Open Source de référence pour la supervision

2 CONSOLE DE SUPERVISION

Orsenna s'appuie sur une gamme de console permettant de construire rapidement une offre de supervision de réseau :

- **WhatsUp**, console diffusée largement et assurant une supervision de l'ensemble des composants de votre réseau avec une présentation conviviale de l'état du réseau.

- **Orion,** console de supervision plus orientée vers la surveillance d'infrastructure réseau (routeurs et switches).

- **PRTG**, console permettant de mettre en place des surveillances basiques assez rapidement.

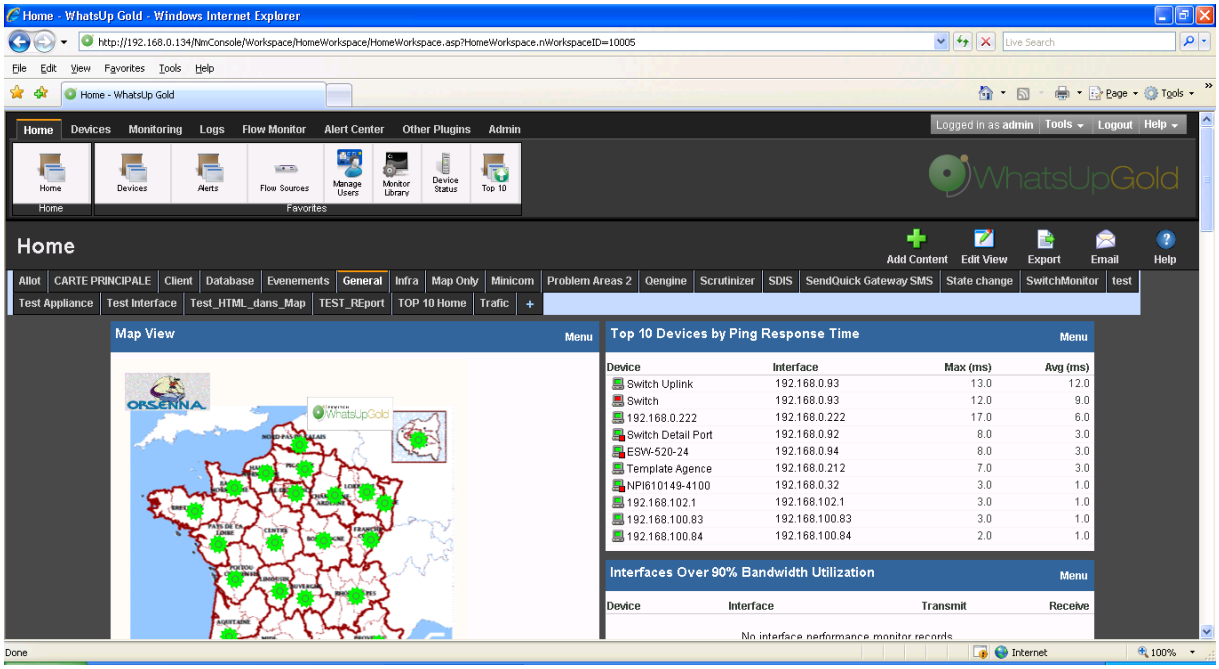
- **NagiosXI**, console de supervision assurant une supervision de l'ensemble des composants. Néanmoins elle reste principalement orientée pour les administrateurs utilisant déjà une plateforme de type Nagios et voulant avoir un support.

Ces consoles s'appuient tout d'abord sur du monitoring ICMP et SNMP. WhatsUp permet aussi d'effectuer des monitoring WMI et SSH (plugins Orsenna)

2.1 WHATSUP

WhatsUp est une solution conviviale de cartographie, de surveillance, de notification et d'évaluation des performances des réseaux qui aide les administrateurs et ingénieurs réseaux à localiser et résoudre les problèmes de réseaux . Sa caractéristique importante réside dans les possibilités de customisation du monitoring (SNMP, WMI, Script TCP, Script Java ou VB) et la cartographie.

Figure 1 : DashBoard WhatsUp



2.2 COMPLEMENTS WHATSUP

Une plateforme WhatsUp Gold peut comprendre différents plugins :

- WhatsUp Companion (Monitoring des applications)
- VoIP Monitor (Monitoring opération Cisco IP SLA)
- NetFlow Monitor (Monitoring de flux)
- WhatsConnected (Cartographie + inventaire)
- WhatsConfigured (Gestion des configurations)
- WULM (Gestion des évènements)

2.2.1 WhatsUp Companion

Différents plug-ins développés par Orsenna permettent d'étendre le monitoring des équipements :

- Monitoring Bases de Données : MySql, Oracle, Informix, PosgreSQL, DB2.
- Monitoring SSH / Telnet
- Monitoring avec agents: NRPE, Zabbix
- Monitoring Applications: File Parser, SFTP, Mailer
- Monitoring Applications infrastructure: DNS Extended, DNS Blacklist, HTTP Certificate, NTP
- Monitoring Serveur Web: Apache, TomCat, Zapcat, Websphere, JBoss

Figure 2 : PlugIn WhatsUp pour Oracle

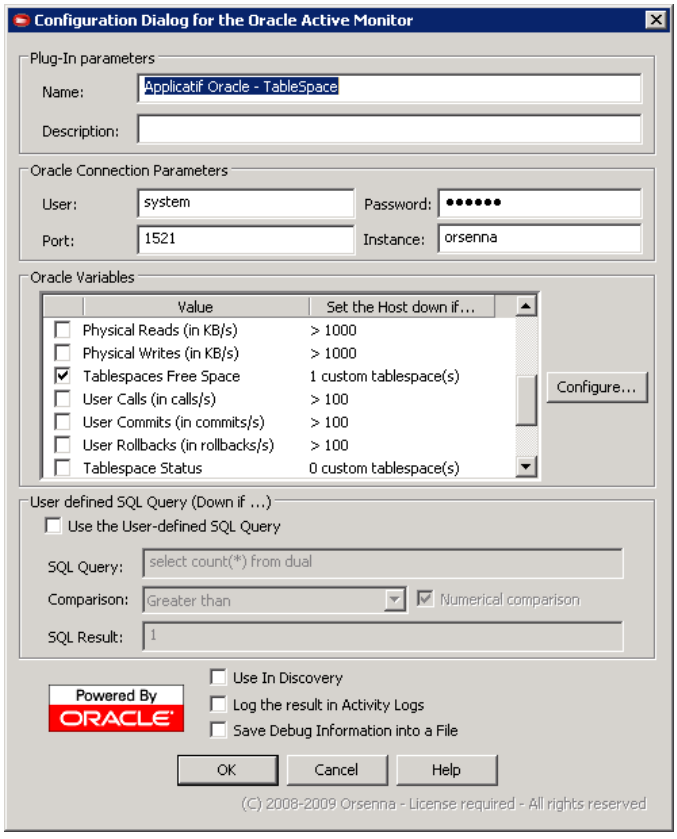


Figure 3 : Plug-Ins SSH

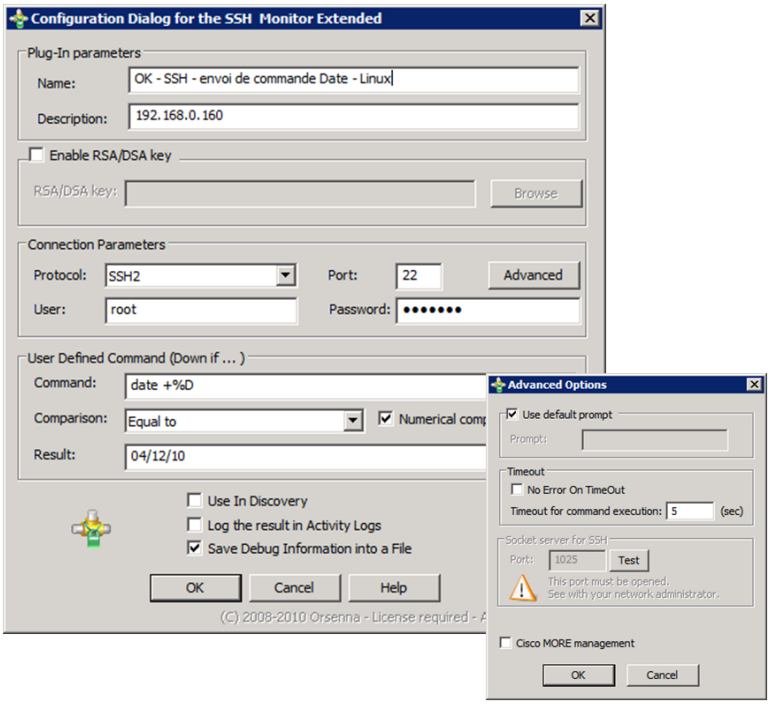
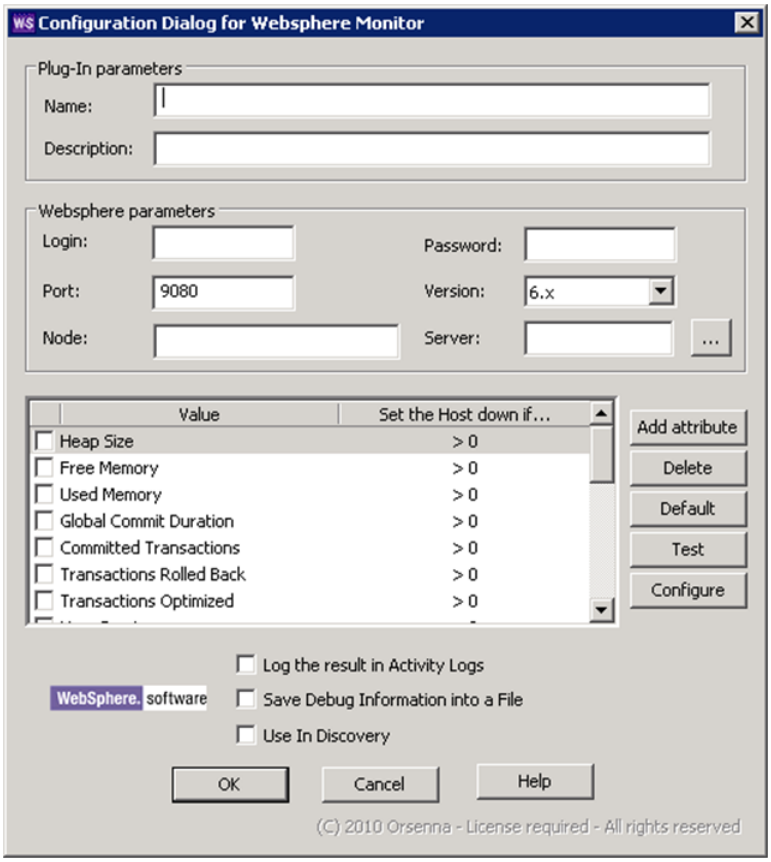


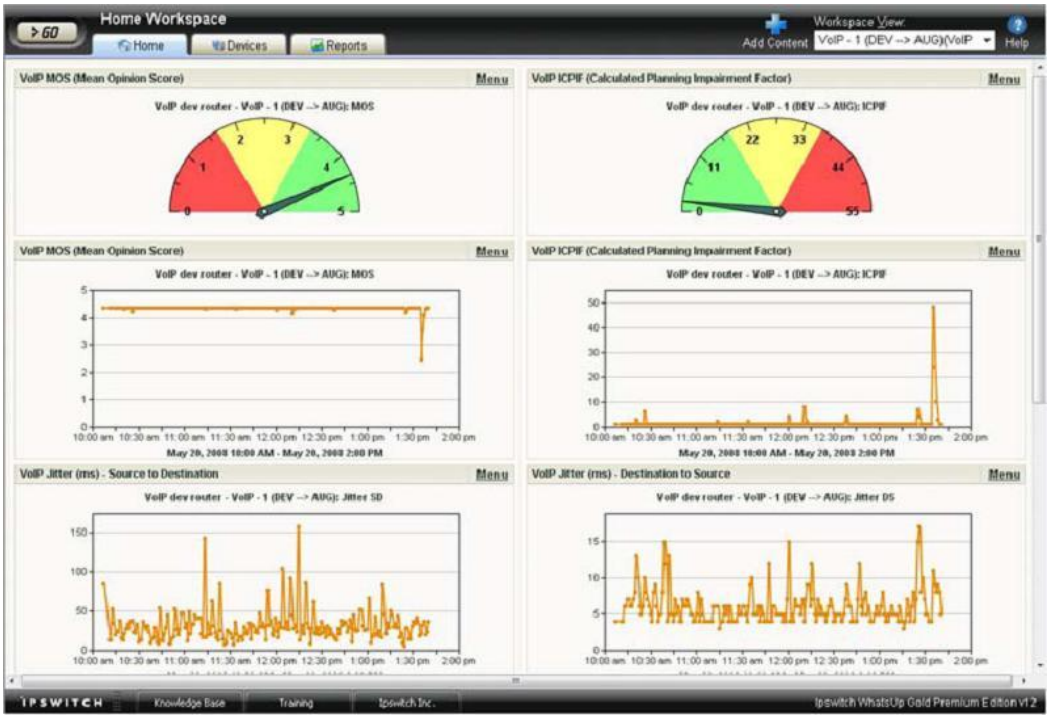
Figure 4 : Plug-Ins Websphere



2.2.2 Plug In VoIP

Ce module permet de collecter et de grapher les éléments d'informations issus des routeurs Cisco (Configuration IP SLA préalable)

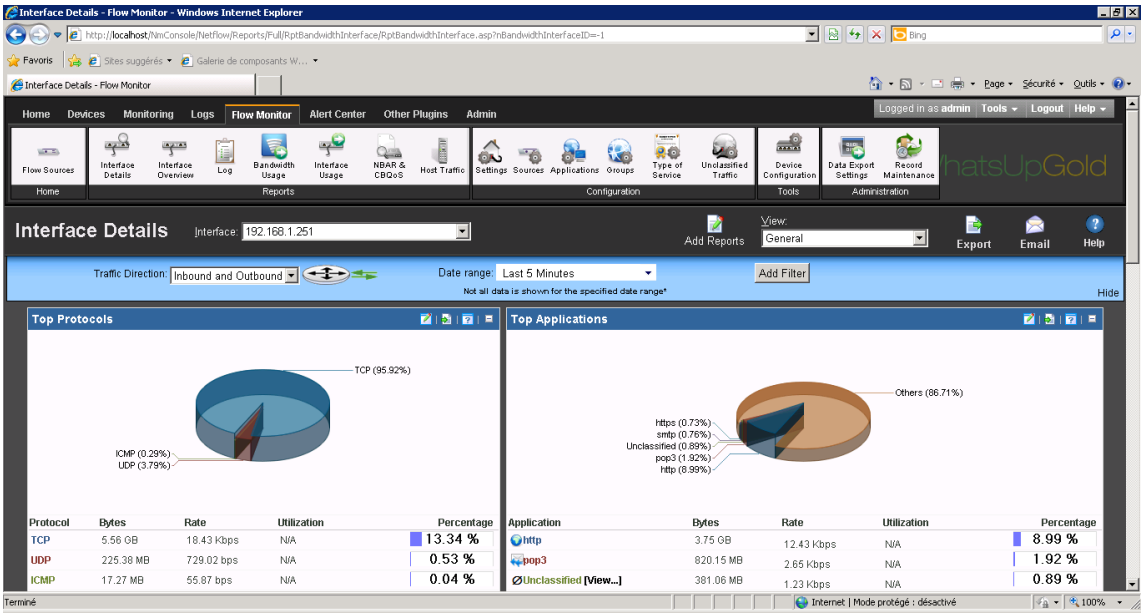
Figure 5 : Monitoring VOIP



2.2.3 Plug In NetFlow

Ce module permet d'intégrer une console Netflow avec la console WhatsUp

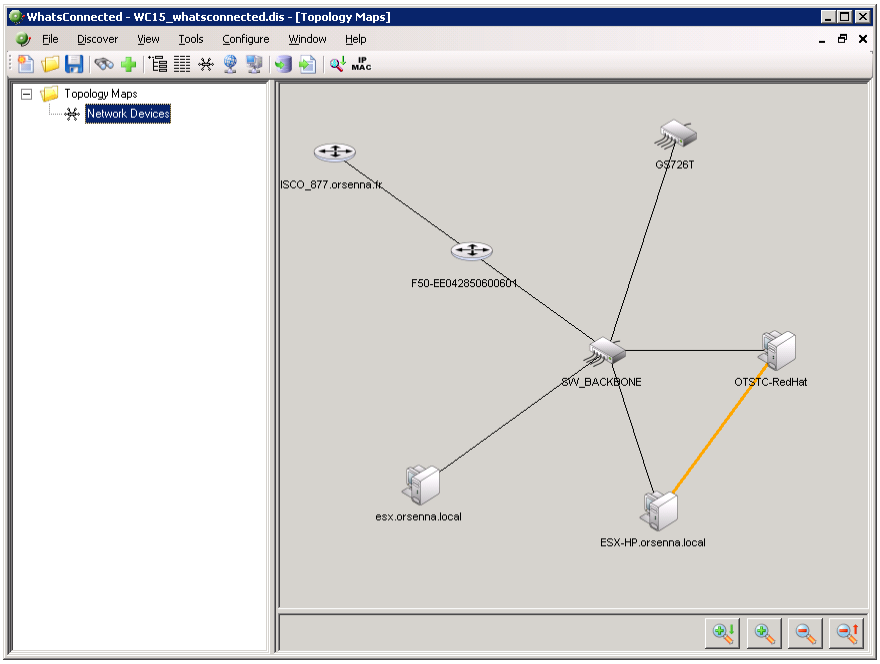
Figure 6 : Monitoring de Flux



2.2.4 Plug In WhatsConnected

Ce module permet de réaliser la cartographie réseau :

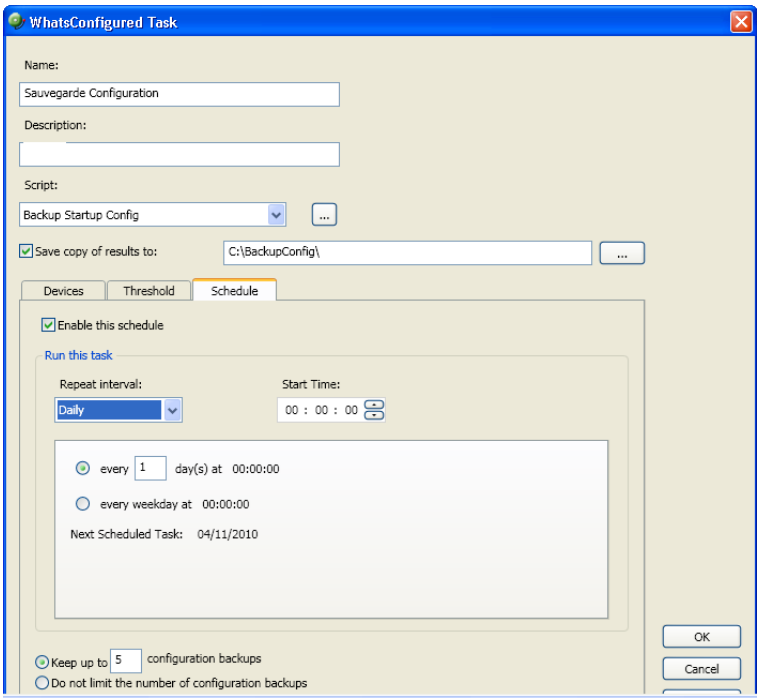
Figure 7 : Cartographie



2.2.5 Plug In WhatsConfigured

Ce module permet de gérer les configurations des équipements réseaux :

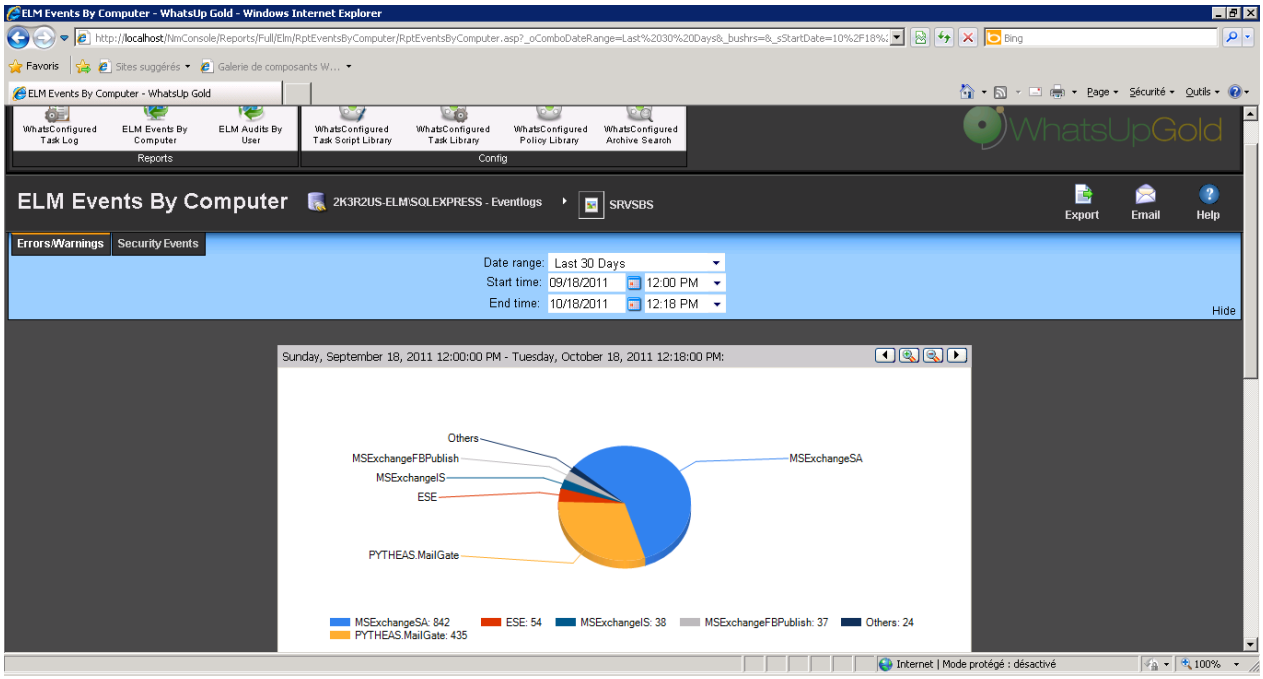
Figure 8 : Gestion des configurations



2.2.6 Plug In WULM – WhatsUp Logs Management

Ce module permet de gérer les différents types d'évènements de l'ensemble de vos équipements (EVT / EVTX, Syslog, W3C/IIS) :

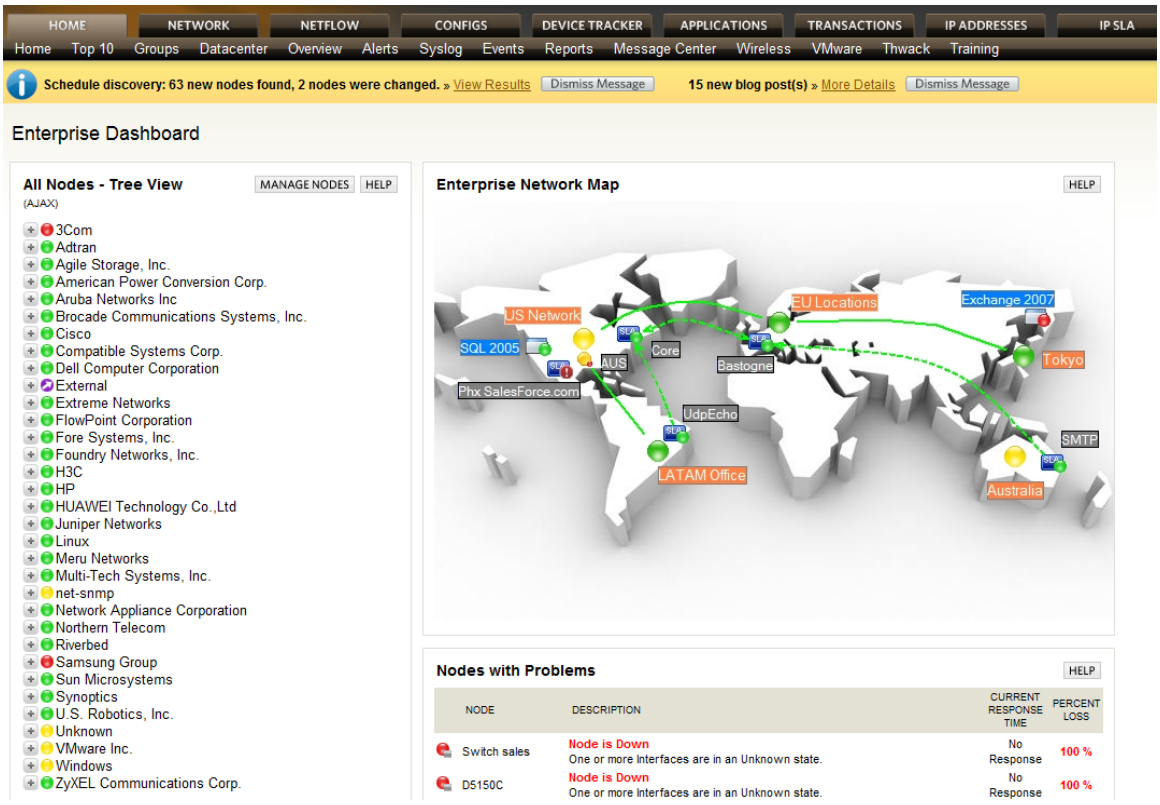
Figure 9 : WULM



2.3 ORION

Orion est une solution orientée vers la surveillance d'infrastructure. Le produit dispose de fonctions évoluées pour gérer finement les équipements réseaux (Rapports SNMPs prédéfinis , Gestion des compteurs 64 bits, Gestion de multiples moteurs de polling..).

Figure 10 : DashBoard Orion



2.4 COMPLEMENTS ORION

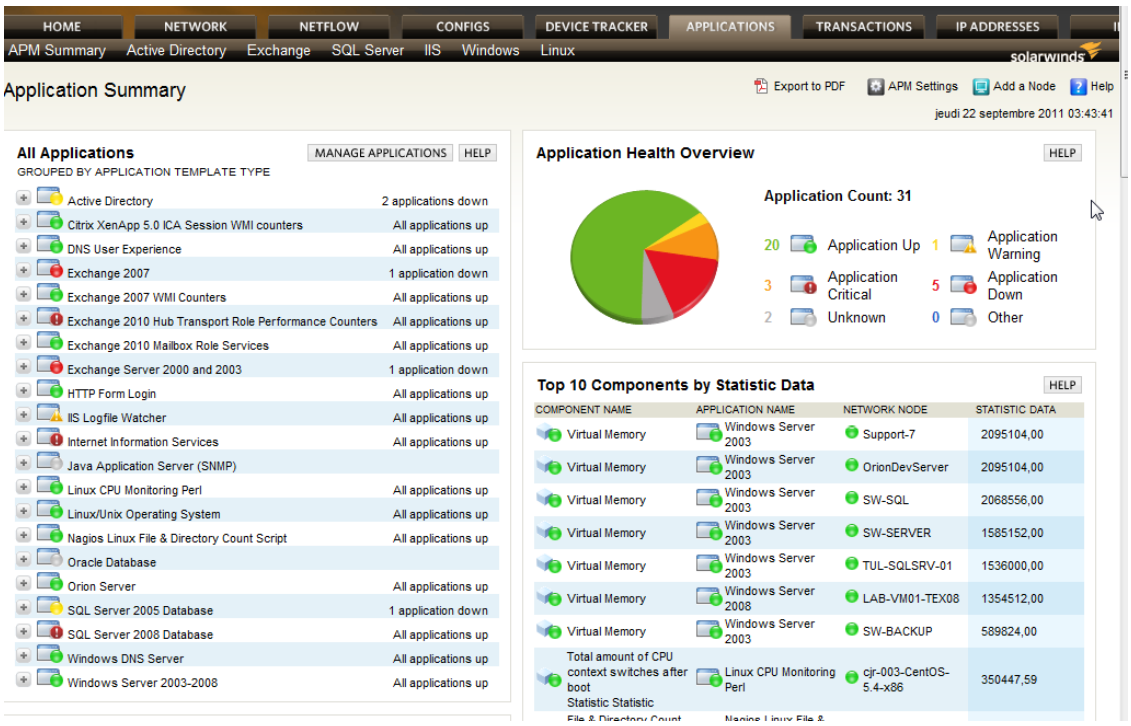
Une plateforme Orion peut comprendre différents plugins :

- APM (Monitoring serveur / applications)
- IP SLA (Monitoring opérations Cisco IP SLA)
- NTA (Monitoring des flux)
- IPAM (Gestion adressage)
- SEUM (Gestion des transactions)
- UDT (Gestion de la connectivité)
- NCM (Gestion des configurations)

2.4.1 APM

Le composant APM qui s'intègre dans la console de supervision Orion permet de disposer des surveillances sur la plupart des applications de l'entreprise. Une vue globale est disponible :

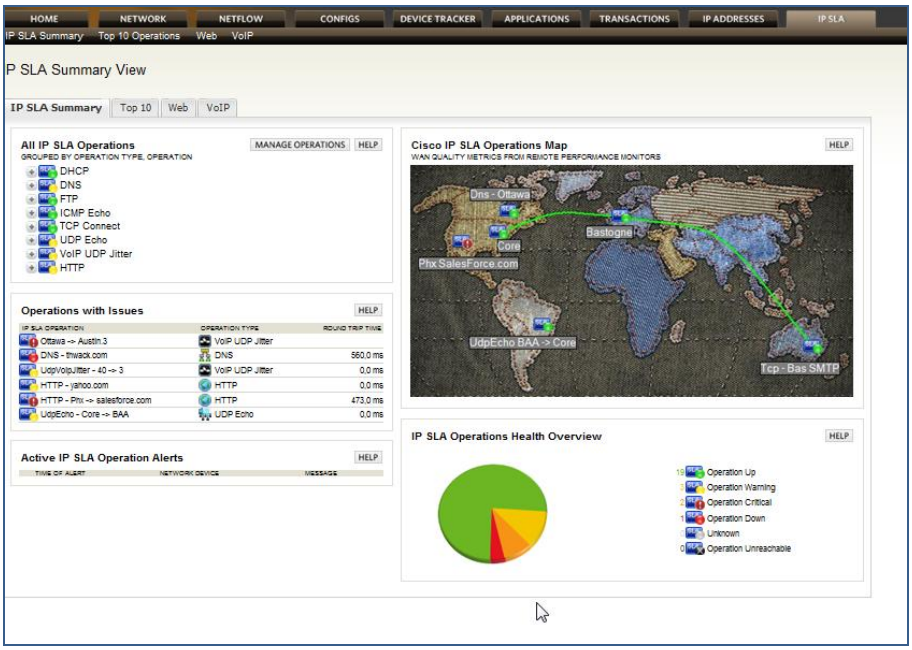
Figure 11 : Vue APM



2.4.2 IP SLA Manager

Un module spécifique permet de gérer les opérations IP SLA Cisco. Les opérations peuvent être configurées à partir de la console

Figure 12 : Console IP SLA



2.4.3 NTA

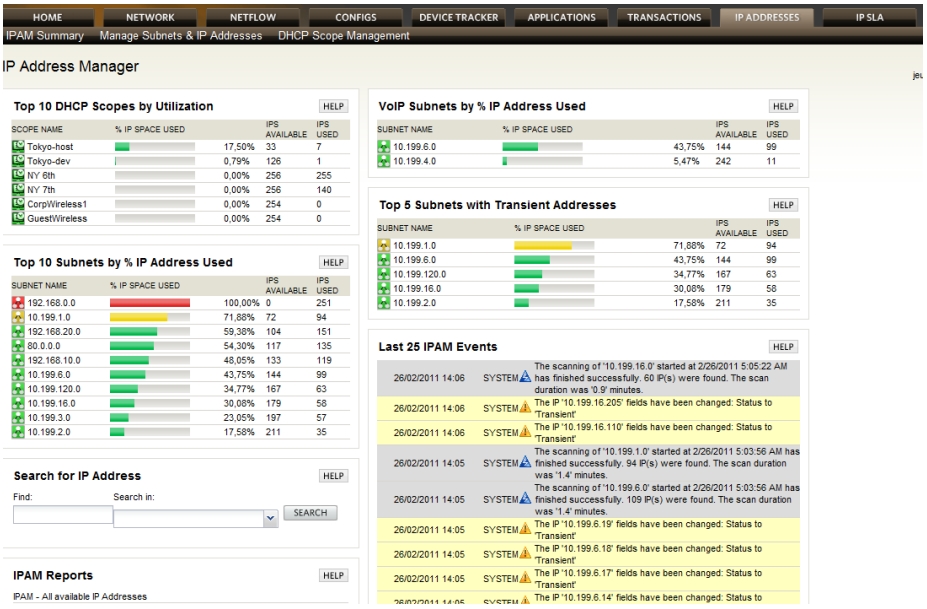
Le module NTA est un collecteur permettant d'analyser les flux sur la base de la réception de données de la plupart des équipementiers (Cisco® NetFlow, Juniper® J-Flow, IPFIX, sFlow, et Huawei NetStream™).

Figure 13 : Vue globale NTA

2.4.4 IPAM

Un composant IPAM peut être intégré à la plateforme et ainsi fournir des services autour de la gestion des adresses :

Figure 14 - Gestion des Adresses IP

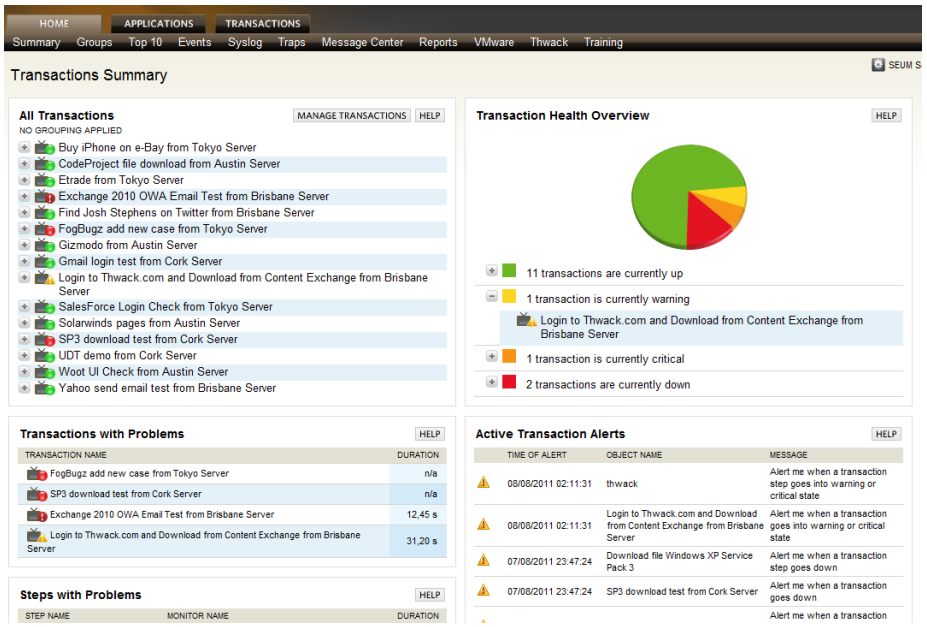


2.4.5 SEUM

Afin d'enrichir la supervision applicative un module de gestion des transactions permet d'effectuer de rejouer des sessions utilisateurs afin de valider leur bon déroulement.

Ce module s'appuie sur une architecture distribuée de modules « Player » de sessions.

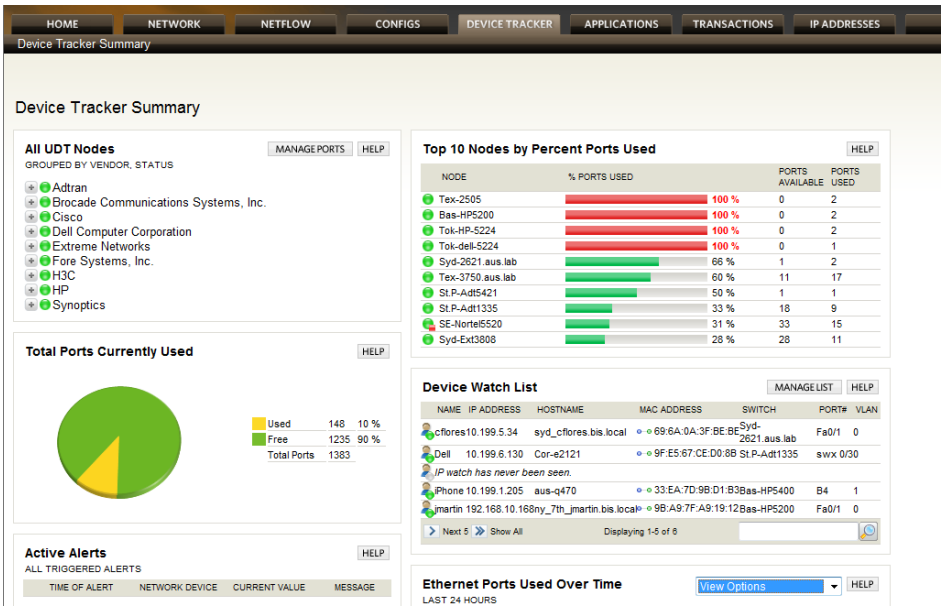
Figure 15 : Composant SEUM



2.4.6 UDT

Afin d'aider au diagnostic rapide et à la gestion du réseau le composant UDT permet d'accéder rapidement à des informations sur les ports et leur connectivité.

Figure 16 : Module UDT

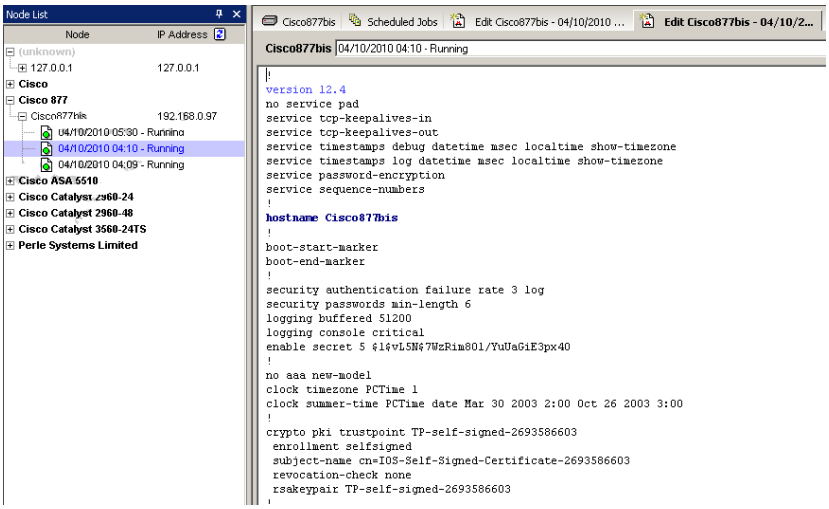


2.4.7 NCM

Ce module permet de gérer les configurations des équipements réseaux, il permettra de centraliser l'ensemble des configurations sur un unique serveur.

Il intègre également diverses fonctionnalités :

- Découverte des équipements.
- Analyse en temps réel des changements dans les configurations.
- Archivage
- Restauration
- Surveillance
- Interface Web…



2.5 PRTG

PRTG Network Monitor est un logiciel de surveillance réseau facile à utiliser.

PRTG Network Monitor couvre tous les aspects de la surveillance réseau: c'est à dire la surveillance de la disponibilité, la consommation et l'utilisation de la bande passante, les compteurs SNMP, les flux NetFlow, Packet Sniffing…

PRTG Network Monitor est optimisé pour une installation, une configuration et une utilisation faciles.

Figure 17 - Console PRTG

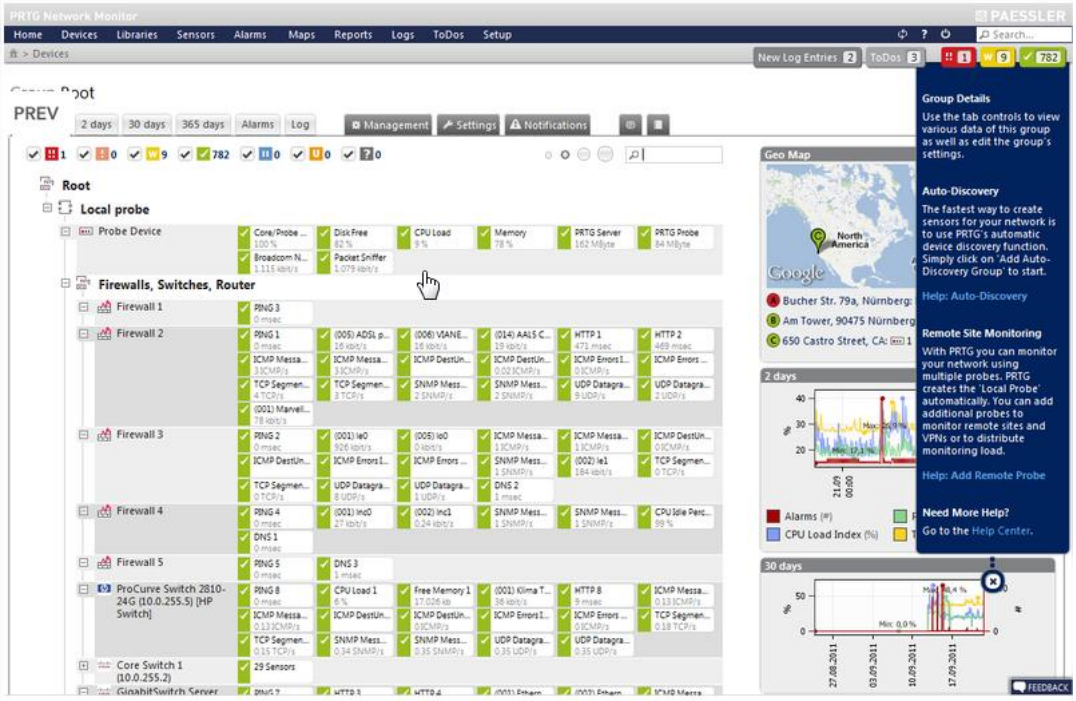
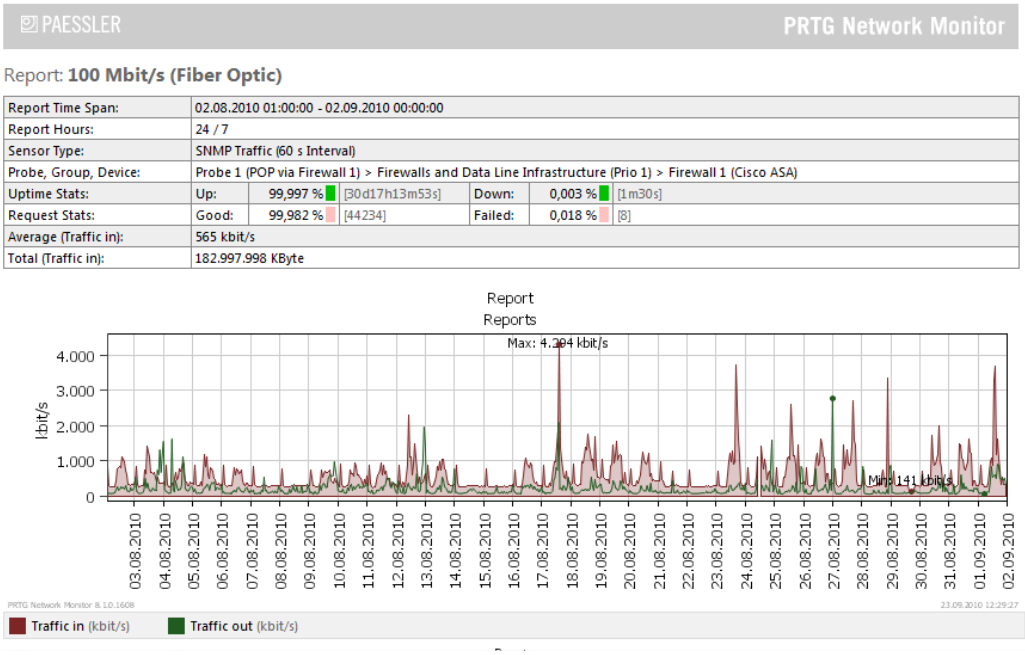


Figure 18 - Analyse de la bande passante



2.6 NAGIOS XI

Tout le monde connait Nagios, cette version XI pour eXtended Insights est clairement tournée vers l'entreprise. Cette console de supervision nous permet de surveiller l'ensemble des composants de votre réseau.

Comparé à la version classique de Nagios, elle offre les fonctionnalités suivantes :

- Nouvelle interface (customisation des vues par utilisateur).
- Les vues utilisateurs qui permettent de revenir rapidement aux écrans, informations les plus pertinentes, critiques.
- Configuration à partir de l'interface (et plus seulement en lignes de commandes)
- Des « wizards » de configuration qui permettent de rajouter facilement un hôte, un service, une application.
- Configuration avancée des droits utilisateurs.
- …

Figure 19 - Console d'administration

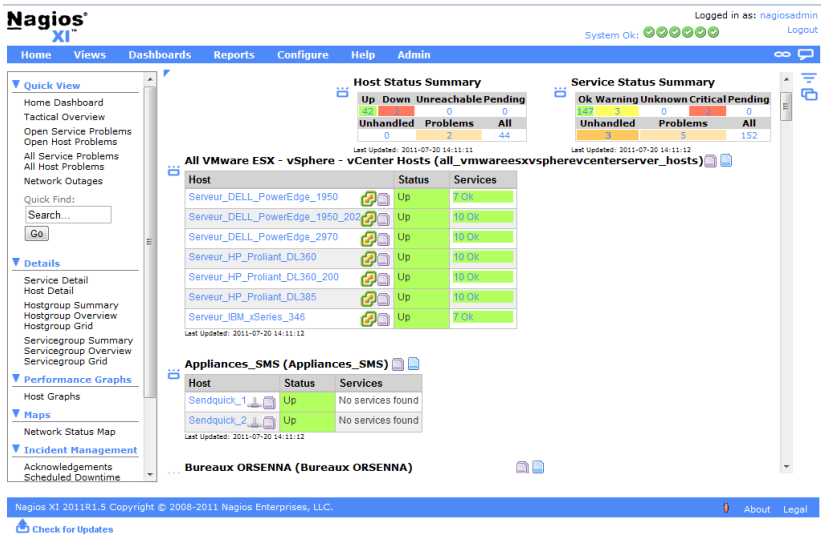
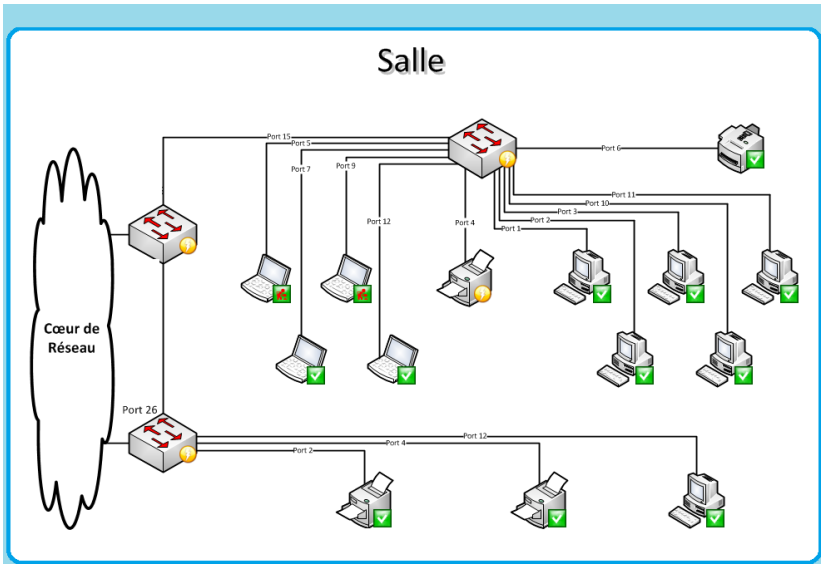


Figure 20 - Exemple de carte



3 CONSOLE D'ANALYSE DE FLUX

Orsenna s'appuie sur une gamme de console permettant de stocker et d'analyser le flux de votre réseau :

- **FlowMon**, Appliance dédiée au stockage et à l'analyse de flux.
- **Scrutinizer**, Logiciel dédié à l'analyse de flux.

Ces consoles s'appuient sur la technologie NetFlow.

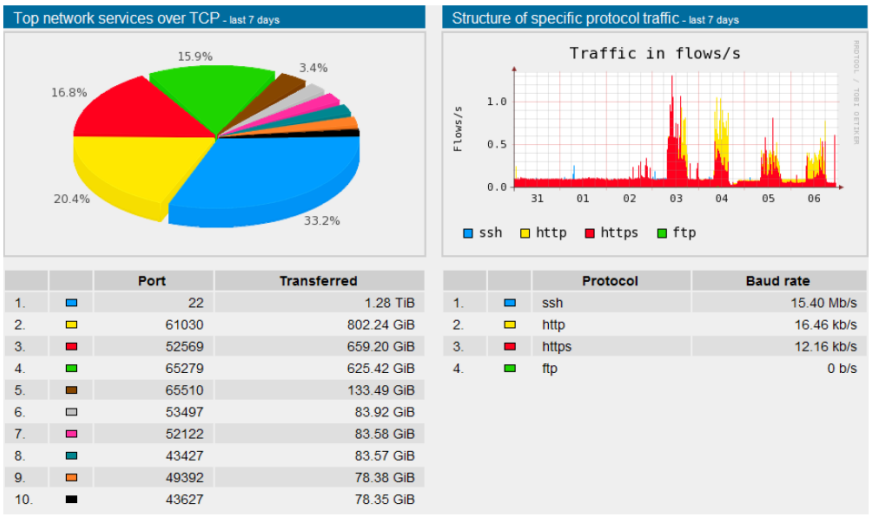
L'ensemble des flux sera stocké et analysé afin de vous générer des rapports en fonction de vos besoins.

3.1 FLOWMON

FlowMon est une solution complète permettant la surveillance et l'analyse des différents flux. Cette Appliance permet d'avoir des informations détaillées concernant l'ensemble des communications réalisées sur le réseau.

Ce qui signifie que vous allez pouvoir déterminer qui communique avec qui, quand, pendant combien de temps, à quelle fréquence, en utilisant tel service ou tel protocole mais aussi connaitre le nombre de bande passante utilisée durant ces communications. Grâce à l'ensemble de statistiques collectées nous avons ensuite la possibilité de réaliser des rapports (FlowMon Reporter).

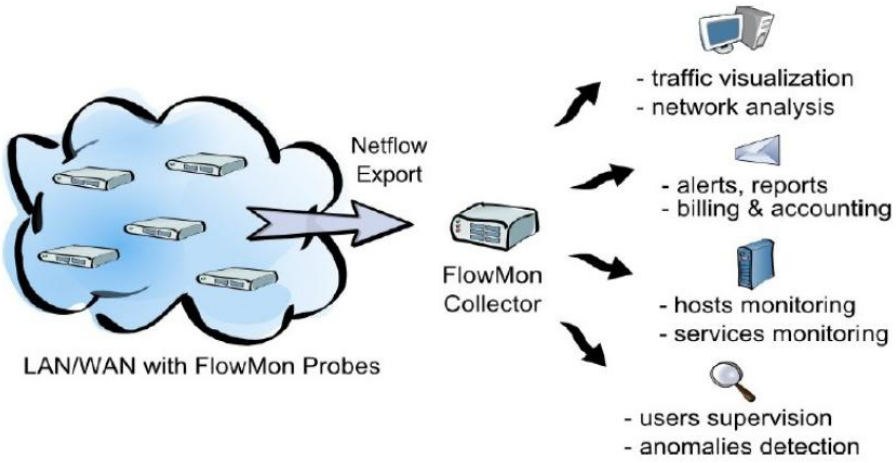
Figure 21- FlowMon



		Port	Transferred
1.		22	1.28 TiB
2.		61030	802.24 GiB
3.		52569	659.20 GiB
4.		65279	625.42 GiB
5.		65510	133.49 GiB
6.		53497	83.92 GiB
7.		52122	83.58 GiB
8.		43427	83.57 GiB
9.		49392	78.38 GiB
10.		43627	78.35 GiB

		Protocol	Baud rate
1.		ssh	15.40 Mb/s
2.		http	16.46 kb/s
3.		https	12.16 kb/s
4.		ftp	0 b/s

Figure 22 – Fonctionnement (possibilité d'utiliser des sondes additionnelles sur le réseau)



Voici les avantages de cette Appliance :

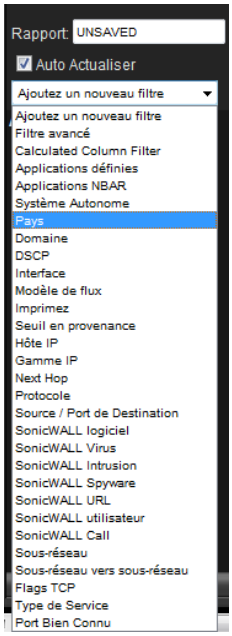
- Appliance dédiée à l'analyse des flux (administration + stockage).
- Centralisation de la console (administration + rapports + sonde).
- Gestion des utilisateurs et des vues.
- Possibilité de créer des groupes par site.
- Graphique facilement compréhensible.
- Envoi de rapports (automatique et périodique).

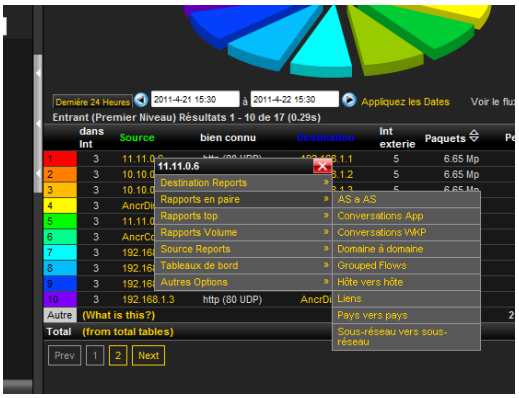
3.2 SCRUTINIZER

Scrutinizer est un logiciel permettant de capturer les flux de type Cisco NetFlow, sFlow, Jflow…

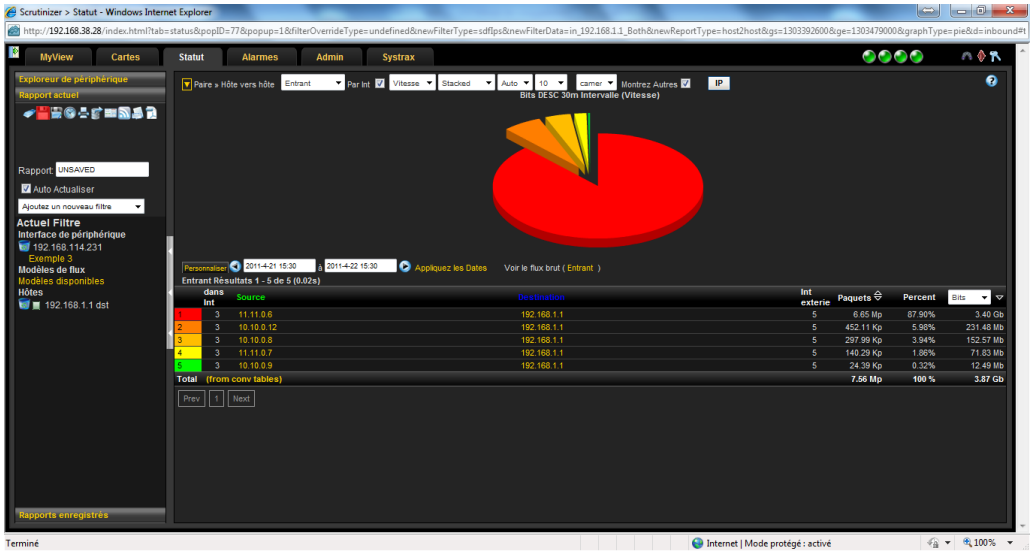
Il permet ensuite de réaliser des graphiques et des rapports personnalisés :

- Rapports concernant l'utilisation de la bande passante (par équipement, par application, par protocole…).
- Nous avons la possibilité de créer nos propres rapports en utilisant des filtres. Cela nous permet de garder seulement les informations dont nous avons besoins.
- Les modèles réalisés peuvent être sauvegardés pour une utilisation future.





- Utilisation d'une plage de ports, d'applications…
- Possibilité de créer des alertes lors de la détection de certains flux.
- Possibilité de créer des utilisateurs avec différents droits
- Sauvegarde des informations sur plusieurs années avec Flow Analytics.



4 AUTRES OUTILS

Orsenna s'appuie sur une gamme d'outils permettant d'auditer rapidement votre réseau :

- **SolarWinds Engineer's Edition Toolset :** Outils de diagnostic
- **Kiwi** , Serveur Syslog
- **QEngine WebTest** : Permet d'effectuer des scripts de sessions préenregistrés sur un serveur Intranet/Internet et de vérifier leur bon déroulement.
- **SNMP Informant : O**util de conversion WMI vers SNMP.
- **Outils Syslog de Kiwi :** Utilitaires Syslog
- **Switch Monitor** , Outil de monitoring détaillé des switches

4.1 DIAGNOSTIC

La suite d'outils "**SolarWinds Engineer's Edition Toolset"** est une suite comprenant des outils de découverte réseau et de suivi de performances. L'application "MIB Walk" est une des plus performantes du marché avec une base de 250,000 OID. Enfin l'outil « switch Port Mapper » permet d'associer aux ports d'un switch les adresses Mac et les DNS liés.

Figure 23 - SolarWinds Port Mapper

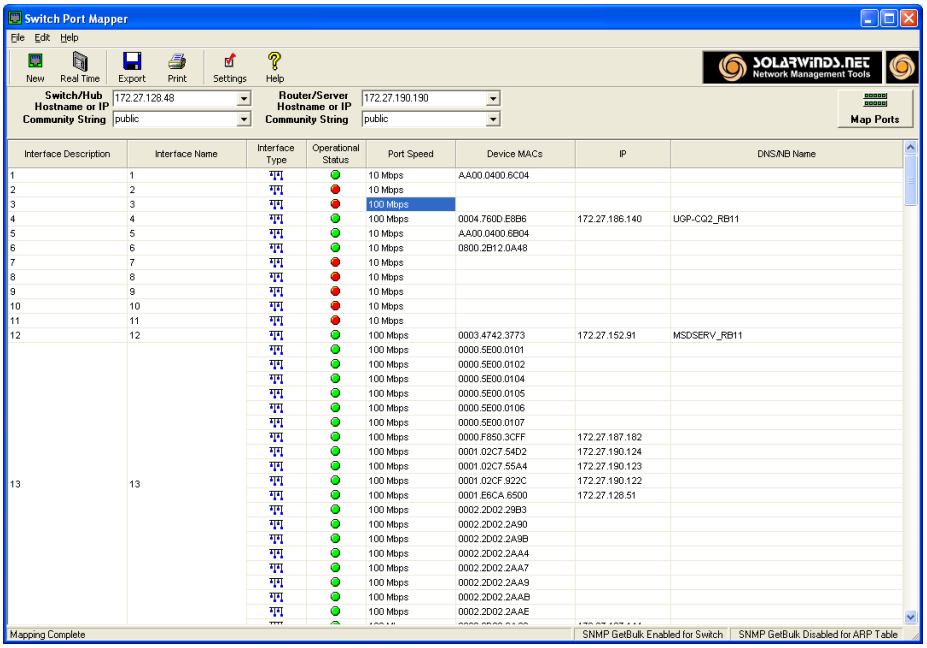
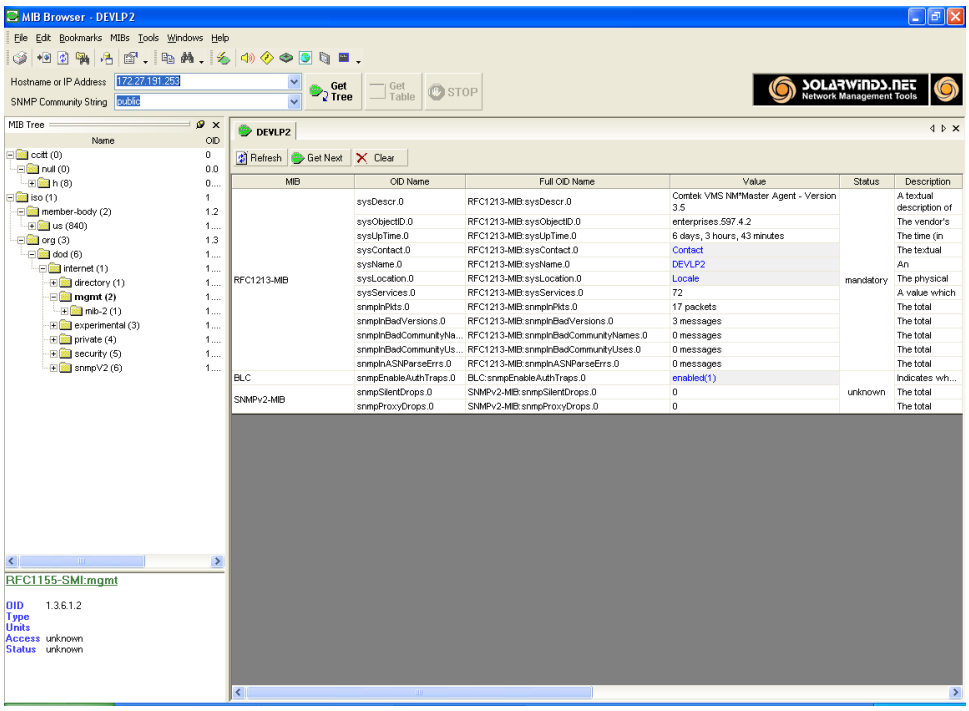


Figure 24 - SolarWinds Mib Browser



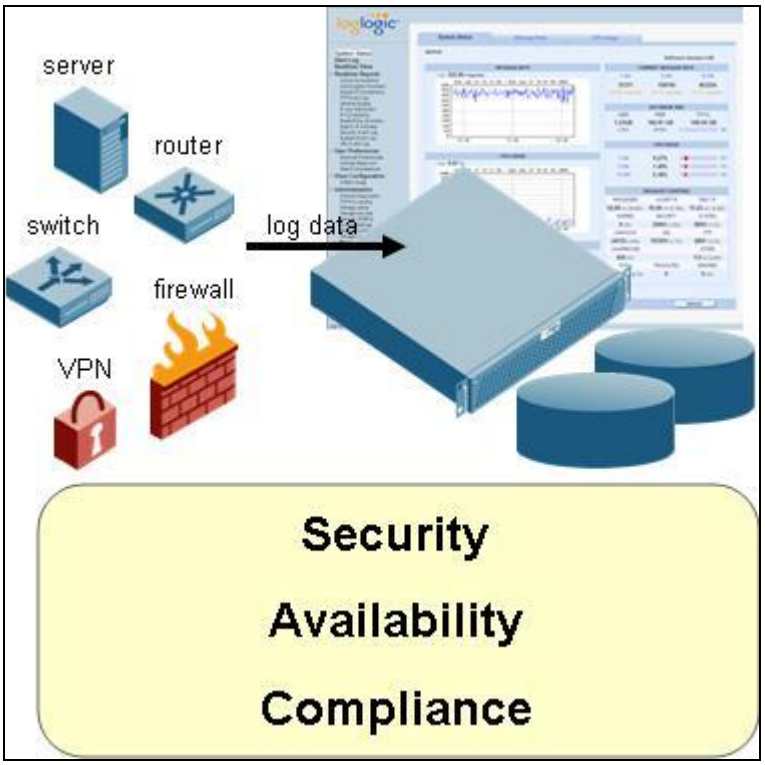
4.2 SERVEUR SYSLOG

Pour un stockage aisé et simplifié des messages Syslog, une suite d'outils est disponible auprès de Kiwi :

Kiwi Syslog Daemon	Kiwi Syslog Daemon est un freeware pour Windows. Il permet de recevoir, filtrer et retransmettre les messages Syslog.
Kiwi Logger	Kiwi Logger permet d'ajouter des fonctionnalités d'envoi de syslog à vos applications.
Kiwi Logfile Viewer	Kiwi Logfile Viewer permet de visualiser les fichiers logs créés par Kiwi Syslog Daemon. .

Pour des environnements plus lourds en termes de volumétries il est possible d'utiliser des Appliances spécifiques (LogLogic)

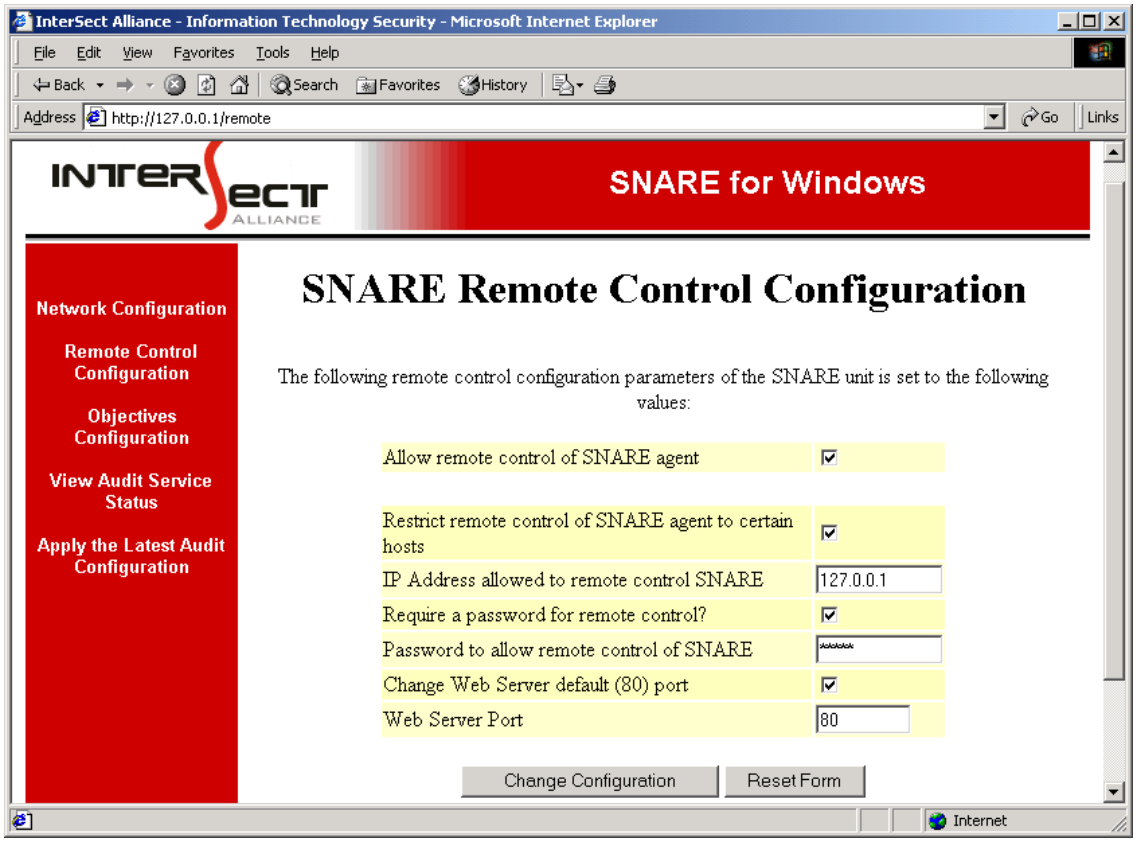
Figure 25 : Stockage de logs



4.3 GESTION DES JOURNAUX

La collecte des différents journaux d'événements des systèmes d'exploitation et éventuellement d'applicatifs peut s'effectuer soit en utilisant des agents sur les serveurs (Outils OpenSource Snare) , ces agents convertissant les événements en messages Syslog ou par requête vers les serveurs (WhatsUp, EventLogAnalyzer.,..)

Les agents Snare peuvent filtrer les évenements en amont afin de minimiser les messages Syslog envoyés.



4.4 REPORTING COMPLEMENTAIRE

4.4.1 Reporting Switch Monitor

L'outil Switch Monitor permet d'obtenir très rapidement des rapports globaux et détaillés sur l'état de l'ensemble du réseau. Les paramètres collectés sont détaillés (% Erreurs, MOS, …) ainsi que des préconisations sur la base des types d'erreurs rencontrées.

Figure 26 - Console SwitchMonitor

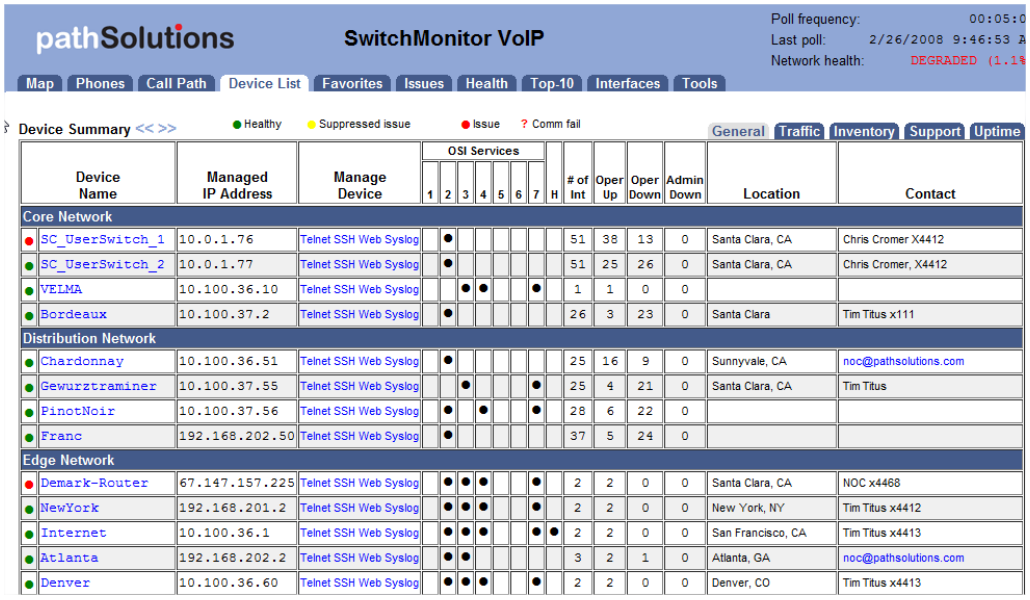
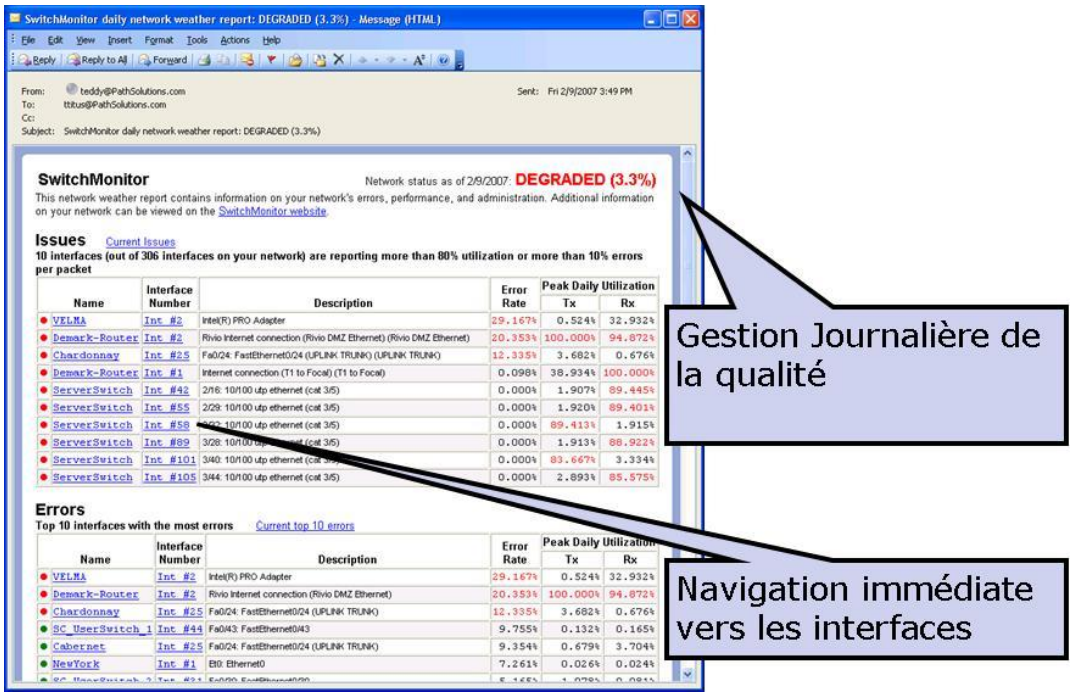


Figure 27 : Console Switch Monitor

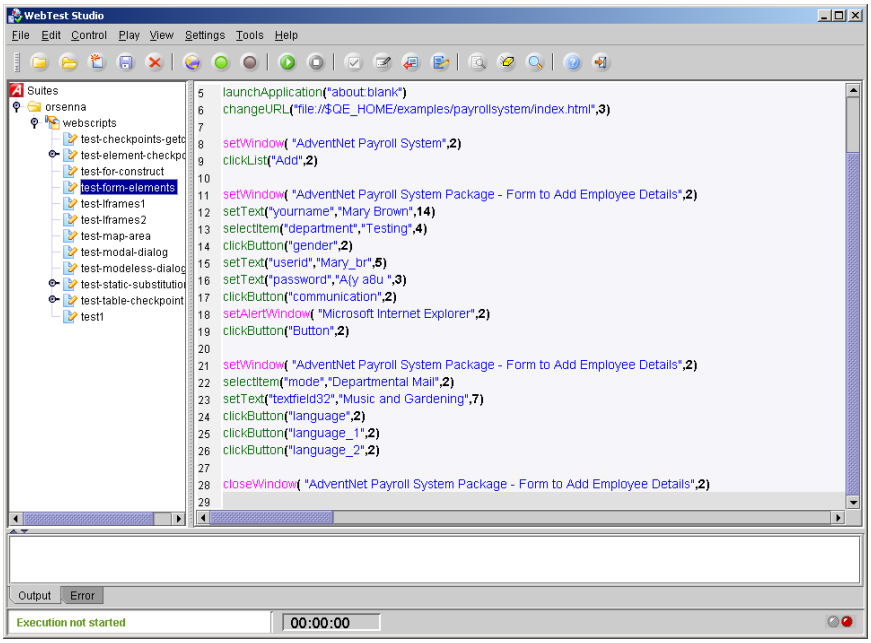


4.5 TEST APPLICATIFS WEB

QEngine Webtest permet d'effectuer des tests automatisés sur un site Web Intranet. Cet outil dispose d'un mode enregistrement et d'un mode playback permettant de vérifier le déroulement des sessions.

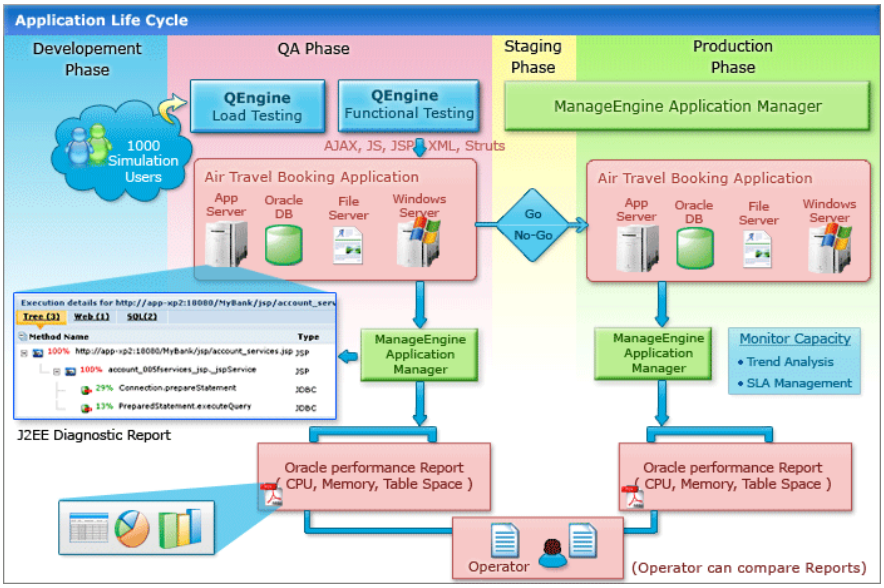
L'automatisation des tests permet de générer (avec un mode commande syslog) des messages syslog vers la console de supervision afin de signaler des erreurs du script qui est joué.

Figure 28 : Scripting Qengine



Un composant restreint de Qengine est intégré à l'outil Application Manager.

Figure 29 : Qengine & Application Manager

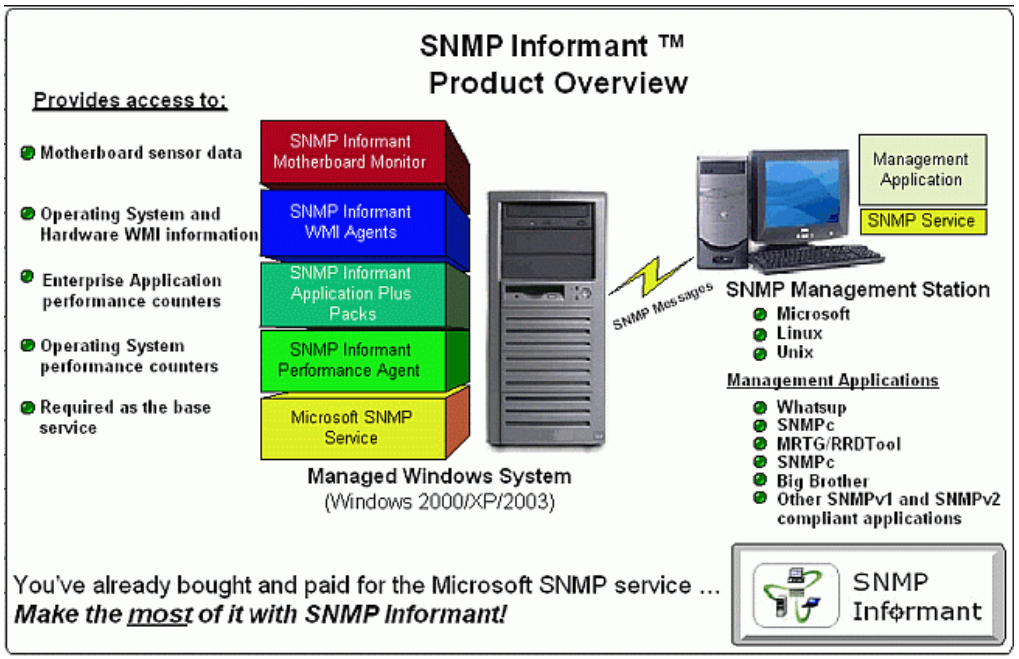


4.6 AGENT SNMP/WMI

SNMP Informant propose des agents spécifiques pour les systèmes Windows qui permettent d'accéder de manière aisée aux informations essentielles des systèmes.

Un **agent standard** permet de récupérer les informations de type (mémoire, CPU, espace disque).

Des **agents spécifiques** permettent de récupérer les informations WMI en SNMP et les informations applicatives pour Exchange, SQL Server, BizTalk Server, Cluster.



Ces agents permettent d'accéder à des compteurs WMI en s'affranchissant des problèmes de sécurité et de volumétrie de trafic.

5 MONITORING VOIP

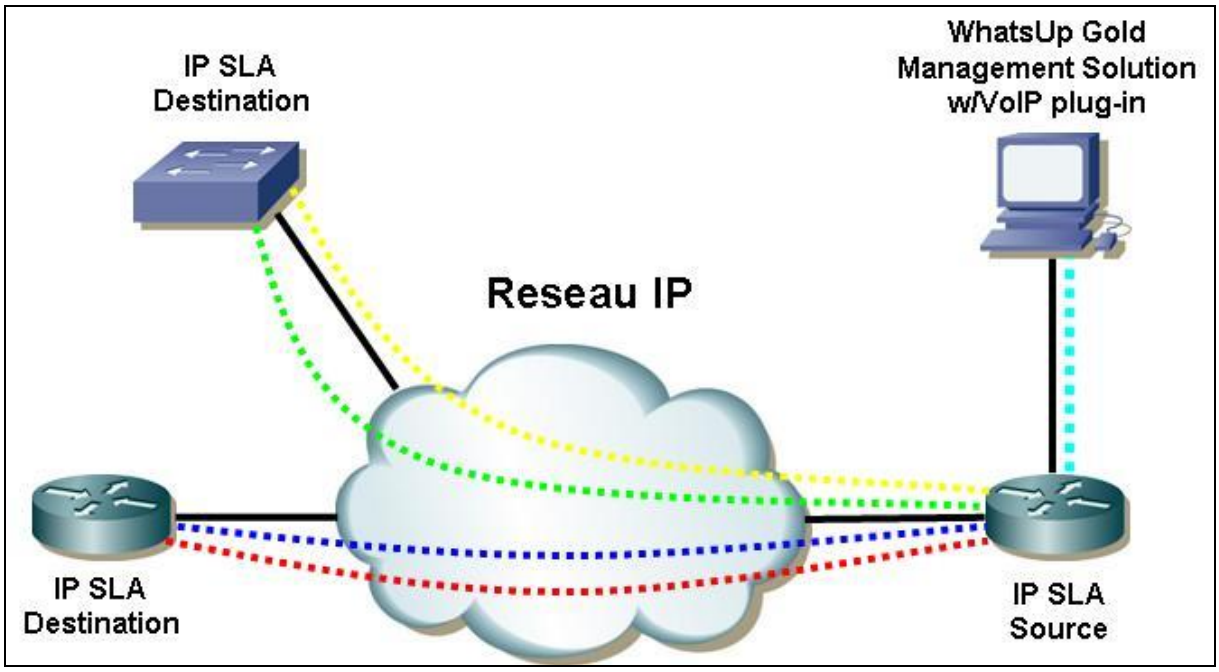
Orsenna s'appuie sur une gamme de produits permettant d'effectuer une analyse des flux de type VoIP

- Module VoIP WhatsUp permettant une analyse des compteurs Cisco (configuration IP SLA)
- Sondes de type Observer ou VqManager assurant une collecte de trafic et éventuellement une collecte des CDRs (Call detailed Records)
- Switch Monitor

5.1 WHATSUP

Le module WhatsUp collecte les paramètres VoIP d'équipements Cisco IP SLA, notamment le MOS et les valeurs de jitter, temps de latence.

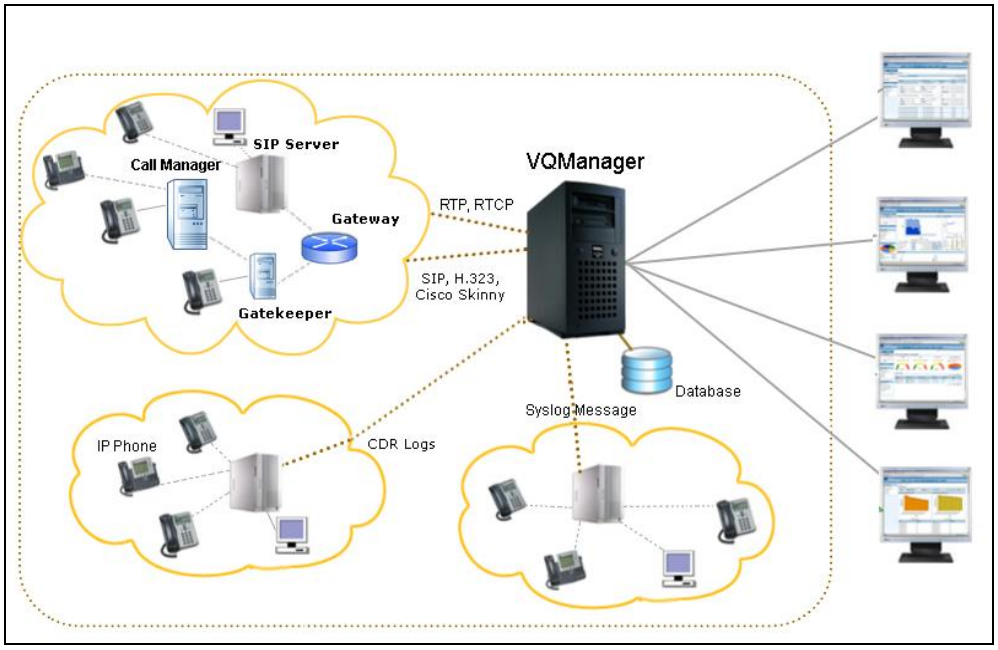
Figure 30 : VoIP WhatsUp Architecture



5.2 SONDES

Les sondes se positionnent en capture de trafic sur un port d'un switch (TAP ou Mirroring) et permettent aussi de collecter les journaux d'appels sous un format de type Syslog.

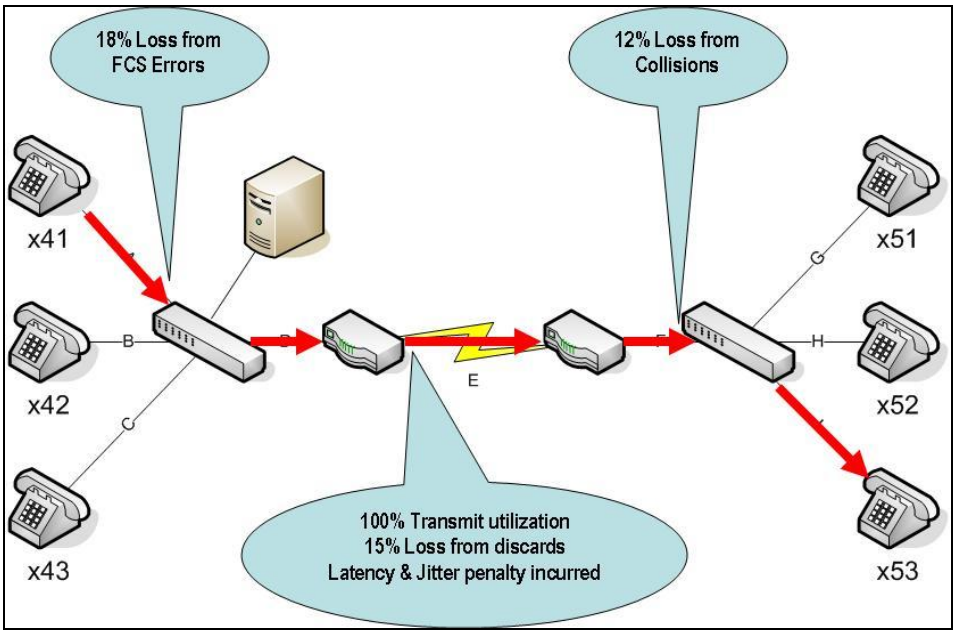
Figure 31 : Sonde VQManager



5.3 SWITCH MONITOR

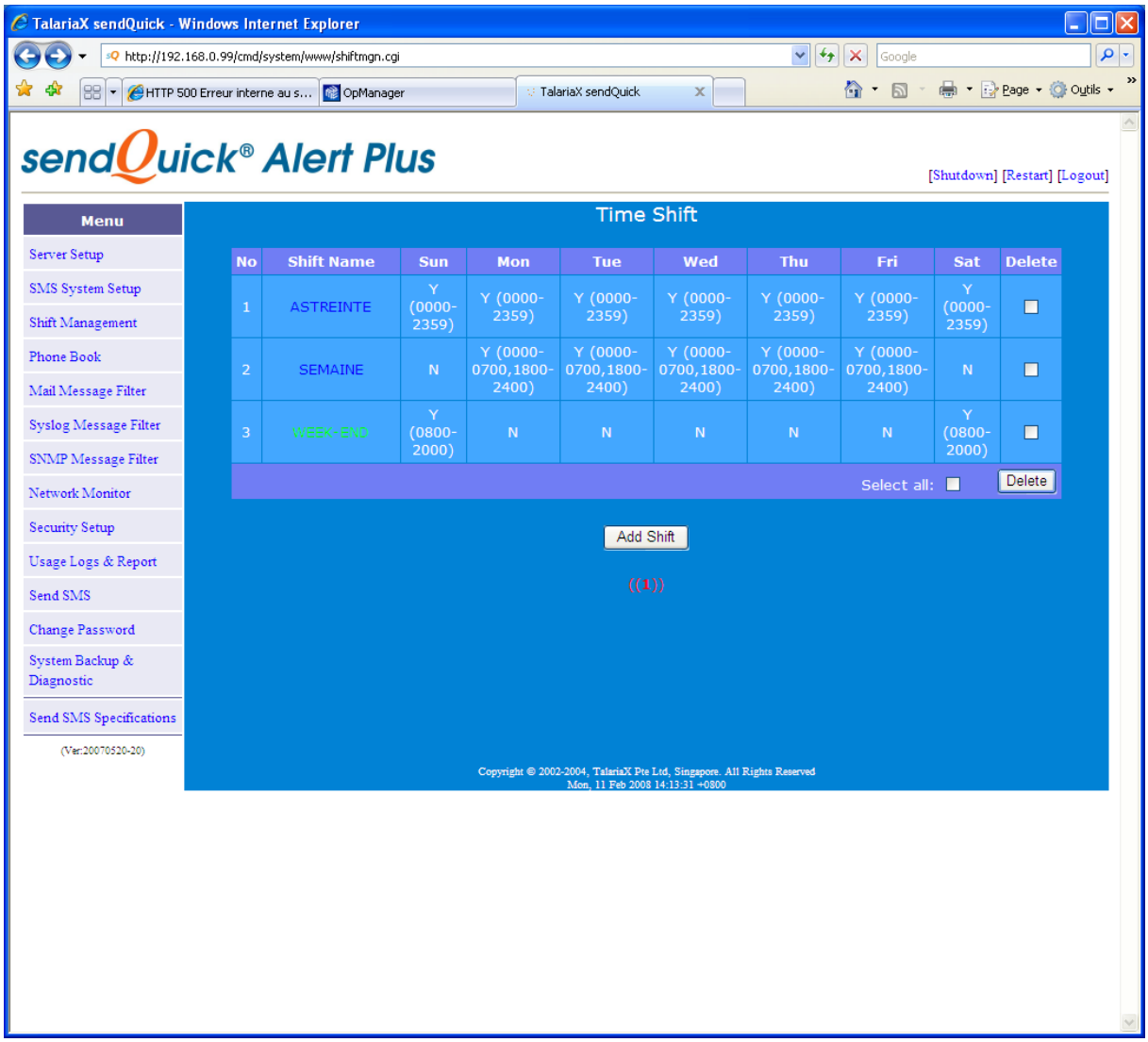
Le produit Switch Monitor est intéressant dans sa découpe car il permet au travers une collecte de valeurs SNMP sur l'ensemble des équipements d'établir des diagnostics sur l'ensemble d'un chemin réseau . Cette fonctionnalité « Call Path » restant très simple à mettre en œuvre.

Figure 32 : Analyse "Call Path" de Switch Monitor



6 SMS – GESTION ASTREINTE

Orsenna intègre une Appliance de gestion d'astreinte qui permet de gérer l'envoi d'alertes par SMS aux correspondants des équipes d'astreinte.



Cette appliance permet aussi de diffuser des SMS à partir d'un envoi d'email, d'envoi de traps SNMP ou de messages SYSLOG.

7 PROJET SUPERVISION DE RESEAU

La mise en place de votre projet de supervision réseau nécessite au préalable la description de votre environnement technique. Cette description doit être effectuée en prenant en compte les objectifs de base de la supervision (Surveillance proactive, Diagnostic, Gestion des statistiques,..).

7.1 DESCRIPTIF PERIMETRE TECHNIQUE

La mise en place du projet de supervision réseau nécessite au préalable de définir l'ensemble des éléments qui seront dans le périmètre du projet.

La base technique s'appuie alors sur les descriptions suivantes :

- Descriptif interne de l'architecture sur la base des documents internes existants (plan d'adressage, VLAN, …)

- Descriptif des composants réseaux
  - Pour chaque type de composant une fiche descriptive décrivant l'accessibilité du composant (SNMP, IP, Syslog, WMI, SSH), les événements à gérer (ressources utilisées, état d'une interface,..) , criticité du composant, procédure de diagnostic et de dépannage (Appel astreinte,…).
- Descriptif des serveurs
  - Pour chaque type de machine une fiche descriptive décrivant l'accessibilité du composant (SNMP, IP, Syslog, journaux, WMI, SSH), les états et événements à gérer (ressources utilisées, état d'un service,..), criticité du serveur, procédure de diagnostic et de dépannage (Appel astreinte,…), événements et actions associées (sur incident lancement processus XYZ,..).

- Descriptif des applications
  - Pour chaque type de machine une fiche descriptive décrivant l'accessibilité du composant (SNMP, IP, Syslog, script, agent distant, journaux, WMI, SSH), les états et événements à gérer (service arrêté, événement syslog,..), criticité du serveur, procédure de diagnostic et de dépannage (Appel astreinte,…), événements et actions associées (sur file attente pleine lancement processus XYZ,..).

7.2 OBJECTIFS SUPERVISION DE RESEAU

Les différentes orientations de la supervision réseau doivent être décrites afin d'effectuer les choix de paramétrages adéquats :

- Diagnostic et résolution rapide de problèmes
- Surveillance proactive
- Statistiques de la qualité de service
- Collecte et mesure de performances

Sur la base de ces orientations, les différents items décrivant les fonctions attendues de la supervision réseau sont à décrire.

7.3 PARAMETRAGE

7.3.1 Cartographie

Les différentes cartes et sous-cartes nécessaires sont à définir :

- Les cartes techniques correspondantes à la topologie physique des équipements.
- Les cartes fonctionnelles correspondantes à l'ensemble des objets assurant une fonction donnée.
- Les cartes orienté métier correspondants à l'ensemble des fonctions liées à un processus métier.

L'accessibilité de ces cartes au niveau Web sera définie.

Les fonctions d'import ou d'export souhaitées seront décrites.

Les fonctions d'interdépendances souhaitées seront décrites.

7.3.2 Etats du réseau et des équipements

Sur la base des descriptifs des composants réseaux, serveurs et applicatifs, une liste des événements et états à traiter est à définir.

Les états d'une carte ou d'un équipement sont à définir ainsi que les dépendances associées

7.3.3 Gestion des événements et définition des alertes

L'ensemble des évènements et données collectables sur le réseau constituent une base d'informations sur laquelle un filtrage sera effectuée en terme de seuil, de comptage, d'état.

Les filtrages souhaités seront décrits ainsi que les processus associés (déclenchement de rapport, d'alertes,…).

7.3.4 Gestion des alertes

Les différents modes souhaités en termes de traitement d'alertes seront décrits, ainsi que les paramètres et informations associés aux alertes:

- Informations associées (log, référence,…)
- Email, SMS, …
- Gestion d'astreinte
- Processus externe

7.3.5 Diagnostics

Sur la base d'une réception d'alerte, les processus de diagnostics mis en œuvre sont à décrire. Les fonctions associées en termes d'outils de supervision sont à décrire

7.3.6 Outils

Les outils complémentaires de diagnostics et les outils constructeurs à intégrer sont à définir ainsi que les interfaces applicatives éventuelles.

7.3.7 Rapports

Les rapports d'états nécessaires à l'activité seront décrits :

- Rapports de disponibilité
- Rapports de performance (taux d'utilisation, temps de réponse)
- Rapport d'inventaire
- Etats des exceptions
- Historiques

L'accessibilité et les contraintes en termes de format seront décrites.

7.3.8 Sécurité

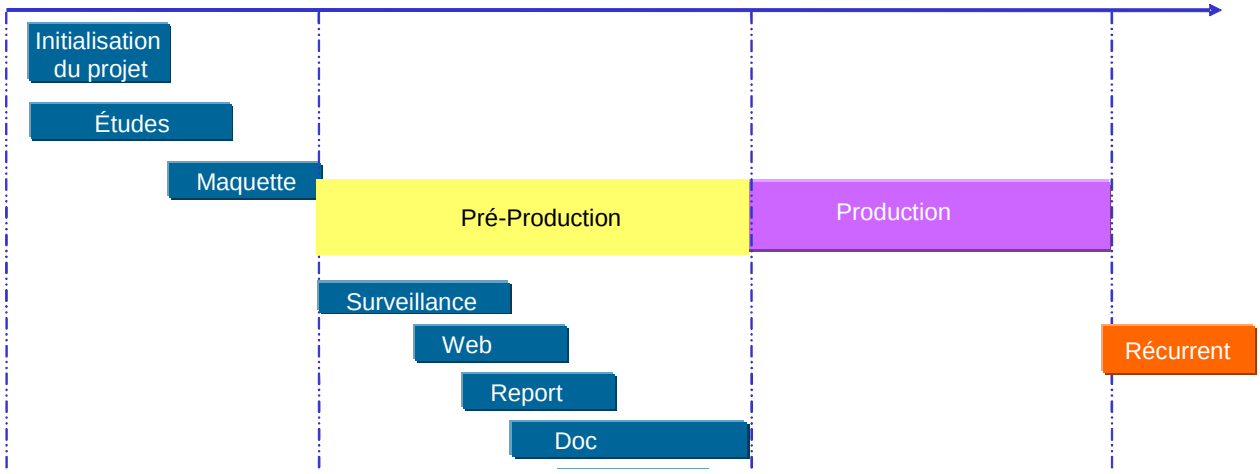
Les contraintes de sécurité de la plateforme de supervision sont à définir :

- Sécurité d'accès
- Redondance
- Mode de Backup

7.4 PLANNING

L'implémentation de ce type de projet s'effectue généralement sur des bases de planning suivantes :

La phase de pré-production correspond à la mise en place en réelle de l'outil de supervision avec un suivi plus spécifique des événements et alertes gérées afin de déterminer la pertinence des événements. Cette phase doit être d'au moins 3 à 4 semaines afin d'avoir une volumétrie suffisante d'évènements.



8 PACKAGE DE SUPERVISION

Orsenna est à même de vous proposer l'ingénierie de votre projet de supervision sur la base d'un canevas technique éprouvé.

Lot	Description	Composants	Délivrables
0	*Audit technique , description de l'architecture technique*	*Pré-étude technique des différents composants existants vis à vis d'une supervision réseau Pré-définition des objectifs et fonctions attendues*	• *Description contexte technique et cahier des charges général*
	Comparatif	*Etat des lieux des outils du marché Grille de sélection*	• *Comparatif des outils et préconisation*
1	Définition des objectifs de la supervision	Description des objectifs Description des fonctions attendues Evaluation des possibilités SNMP des composants du réseau Evaluation de l'aspect sécurité (VLAN)	• Cahier des charges Implémentation – Doc (*)
2	Cartographie	Mapping des cartes physiques et des différents sous réseaux – Surveillance IP	• Mise en place des cartes génériques – Outil (*)
3	SNMP	Mise en place des gestions SNMP et des liens inter-commutateurs	• Compléments SNMP - Outil
4	Surveillance	Mise en place d'une surveillance plus fine (Gestion de seuil,..)	• Compléments surveillance – Outil
5	WEB	Mise en place de l'interface Web et modifications éventuelles	• Compléments Web - Outil
6	Report	Définition des rapports à générer	• Compléments reporting - Outil
7	Documentation	Documentation sur les spécificités de l'installation	• Documentation d'exploitation - Doc
8	Alerte	Définition des alertes à gérer , des informations à transmettre et de la gestion d'astreinte	• Compléments Alerte - Outil

Doc : Documentation
Outil : Eléments intégrés sur la plateforme

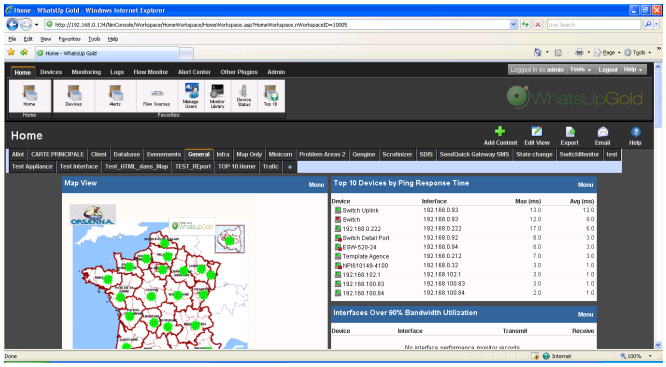
Les charges liées à ces lotissements dépendent essentiellement de la volumétrie en termes de cartes réseaux et de nombre de type d'équipements à intégrer dans la supervision. La mise en place de projet est habituellement réalisée sur une durée comprise entre 4 à 20 jours.

9 EXEMPLE DE PLANNING

Dans le cadre d'un projet nous pouvons proposer une solution de supervision sur la base d'un planning de travail découpé comme suit :

Description	Volumétrie	Ressources
Préétude - Récupération des listes de matériel et compréhension du réseau	300 Objets	0,5 Jour
Validation de l'accessibilité des composants sur site de production et compléments d'information (Accès IP, SNMP, Syslog) Cette partie peut nécessiter une reconfiguration des équipements	5 types d'équipements différents	1 Jour
Mapping carte physique avec différents sous réseaux : Surveillance IP – Alerte Minimum	4 à 5 cartes	0,5 jour
Compléments mapping Physique Liens entre Switchs		0,5 Jour
Validation des éléments sur site et définition de surveillance plus fine (Trafic ,..) - Test des valeurs Snmps Accessibles - test Syslog		0,5 Jour
Traitement des traps, journaux et syslog		0,5 Jour
Validation rapports, analyse des historiques et ajustement des seuils de déclenchement sur site		0,5 Jour
Documentation sur les spécificités de l'installation et pré-requis sur le déploiement sur l'ensemble des objets du réseau		1 jour
Sélection des alertes nécessitant des transmissions d'informations de type Email, Définition, mise en place et test		0,5 jour
Recette		0,5 Jour
TOTAL		6 Jours

10 PACKAGE DE FORMATION WHATSUP



Vous souhaitez :

- ✓ **Mettre en place** votre console de supervision,
- ✓ **Vérifiez** la pertinence des surveillances mises en place,
- ✓ **Consolider** la connaissance du produit.

Nous proposons :

- ✓ **Des formations adaptées à votre environnement**
- ✓ **Un canevas éprouvé** au sein de multiples entreprises,
- ✓ **Une formation interactive** avec la mise en place d'une maquette par vos soins avec l'aide du formateur.

Ces formations se déclinent sur la base des différentes versions du produit en fonction de vos besoins :

WhatsUp Gold V15 & V14
IPSWITCH WhatsUpGold

Elles se déroulent d'après le canevas suivant :

Canevas		*Présentation Générale Supervision*	*Présentation Fonctionnelle WhatsUp*	*Présentation Détaillée WhatsUp*	*Maquette Mode Simulation*	*Présentation Add-Ons*	*Maquette Live*	*Exploitation*
Modules		A	B	C	D	E-E'	F	G
Durée (à titre indicatif)		2H	3H-4H	4H-6H	3H-4H	2H–6H	2H-4H	6H
Formation Standard	Modules BC (6H)		**X**		**X**			
Formation Pro	Modules ABCDEF (18H)	**X**	**X**	**X**	**X**	**X**	**X**	
Formation Expert	Modules ABCDE'FG (32H)	**X**	**X**	**X**	**X**	**XX**	**XX**	**X**

Contenu de la formation

- ✓ **Présentation générale (A) :**
  - Les offres de supervision du marché,
  - Présentation de la conduite projet pour la mise en place d'une console de supervision,
  - Présentation des protocoles et composants SNMP, MRTG, RRDTOOL, terminologie réseau,

- ✓ **Présentation fonctionnelle de WhatsUp Gold (B) :**
  - Définition des objets réseaux et création des cartes,
  - Monitoring actif (ICMP, SNMP , TCP, Services NT, WMI*, Script*),
  - Monitoring passif (Traps SNMP, Syslog, Evénement Windows),
  - Rapports de performances,
  - Groupes dynamiques,
  - Gestion des notifications et des événements,
  - Intégration de Mibs constructeurs,
  - Rapports d'états,
  - Accès Web, configuration.
  - Version Distributed et MSP Edition

- ✓ **Présentation détaillée de WhatsUp Gold (C) :**
  - Définition des rôles, découverte automatique,
  - Gestion et tuning des performances de la solution
  - Gestion des dépendances et des éléments critiques
  - Monitoring SNMP spécifiques (UPS, Printer, Statistiques, Processus, Alimentation, température)
  - Plug-ins WMI - Exchange 2003-2007, SQL Server,
  - Monitoring FTP, Fichier, http Content
  - Intégration de scripts spécifiques
    - Gestion Http – Proxy
    - Gestion Script JS-SNMP – Disques – Spanning Tree
    - Gestion Script VB-WMI – Comptage process, Partage réseaux
  - Scripts de monitoring de performances
  - Gestion de l'Alert Center,
  - Schéma de la base de données
  - Gestion de scripts sur la réception d'évènements,

- ✓ **Mise en place d'une maquette prédéfinie (D) :**
    - Intégration switches et routeurs,
    - Surveillance par port,
    - Surveillance Spanning Tree,
    - Surveillance Trafic,
  - Intégration serveurs :
    - Surveillance CPU, Disque, mémoire,
    - Surveillance avec composants constructeurs (OpenManage, InsightManager, ,..) – Etat Raid , température.
  - Intégration applicatifs :
    - Surveillance TCP,
    - Surveillance Services NT,

        - Surveillance WMI*, SQL Server, Email
        - Script JS & VB. *
    - Autres équipements :
        - Surveillance des équipements non SNMP,
        - Gestion des SMS.

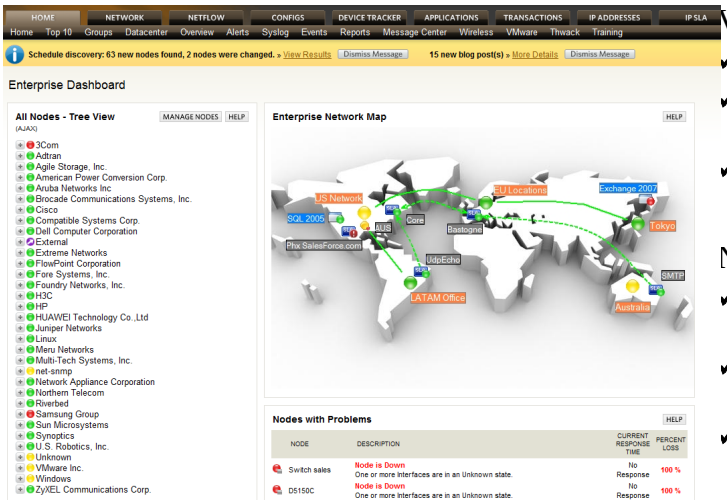
- ✓ **Adds-ons supervision (E) :**
    - Plugs-Ins WhatsUp Companion (NRPE, Oracle, MySql, SSH, SFTP,Telnet, Tomcat, Apache, JMX)
    - Plugs In Flow, WhatsConnected, VoIP, WhatsConfigured (** V15)
    - Plugs-Ins WhatsUp Virtual
    - Script WMI – Microsoft.

- ✓ **Formation Expert - Adds-ons supervision (E') :**
    - Mise en place environnement NRPE – Tâches planifiées
    - Mise en place environnement SSH – Surveillance espace disque
    - Mise en place environnement surveillance Oracle et MySql
    - Configuration IP-SLA Cisco
    - Configuration Netflow – Sflow - Jflow
    - Architecture de gestion d'èvenements – Syslog et Snare
    - Utilisation WhatsConfigured – Exemple de gestion de configuration
    - SNMP Informant & Kiwi Syslog,

- ✓ **Assistance à la mise en place d'une maquette sur le réseau réel de l'entreprise (F) :**
    - Analyse des objets spécifiques du réseau,
    - Intégration de Mibs Constructeurs et de scripts spécifiques.

- ✓ **Exploitation (G) :**
    - Gestion de la base de données
    - Scripts d'exploitations.

11 PACKAGE DE FORMATION ORION



Vous souhaitez :

- ✓ **Mettre en place** votre console de supervision,
- ✓ **Vérifiez** la pertinence des surveillances mises en place,
- ✓ **Consolider** la connaissance du produit.

Nous proposons :

- ✓ **Des formations adaptées à votre environnement**
- ✓ **Un canevas éprouvé** au sein de multiples entreprises,
- ✓ **Une formation interactive** avec la mise en place d'une maquette par vos soins avec l'aide du formateur.

Elles se déroulent d'après le canevas suivant :

Canevas		*Présentation Générale Supervision*	*Présentation Fonctionnelle*	*Maquette Mode Simulation*	*Présentation Add-Ons*	*Maquette Live*
Modules		A	B	C	D	E
Durée (à titre indicatif)		2H	3-4H	3-4H	2-3H	6H
Formation Standard	Modules BC		**X**	**X**		
Formation Pro	Modules ABCD	**X**	**X**	**X**	**X**	
Formation Pro + 1 jour Ingénierie	Modules ABCDE	**X**	**X**	**X**	**X**	**X**

Contenu de la formation

- ✓ **Présentation générale (A) :**
  - ✓ Les offres de supervision du marché,
  - ✓ Présentation de la conduite projet pour la mise en place d'une console de supervision,
  - ✓ Présentation des protocoles et composants SNMP, MRTG, RRDTOOL, terminologie réseau,

- ✓ **Présentation fonctionnelle d'Orion (B) :**
  - ✓ Définition des objets réseaux,
  - ✓ Monitoring switches et routeurs
  - ✓ Monitoring Serveurs
  - ✓ Gestion rapports
  - ✓ Gestion de la base de données
  - ✓ Gestions événements (Traps Snmp, Syslog),
  - ✓ Alertes et notifications ,
  - ✓ Configuration Web,
  - ✓ Gestion de la cartographie,

- ✓ **Mise en place d'une maquette prédéfinie (C) :**
  - ✓ Intégration switches et routeurs,
  - ✓ Custom Mib Poller
  - ✓ Intégration serveurs :
    - ✓ Surveillance CPU, Disque, mémoire,
  - ✓ Intégration applicatifs :
    - ✓ Surveillance TCP,

- ✓ **Adds-ons Orion (D) :**
  - ✓ Netflow Analyzer
  - ✓ Network Configuration Management
  - ✓ Engineers ToolSet,
  - ✓ Additional Polling Engine,
  - ✓ Application Monitor

- ✓ **Assistance à la mise en place d'une maquette sur le réseau réel de l'entreprise (E) :**
  - ✓ Analyse des objets spécifiques du réseau,
  - ✓ Intégration.

12 REGIE DE SUPERVISION

C'est un contrat de service mensuel comprenant des prestations d'installation, de rédaction de procédures, de transfert de compétences et de la délégation sur site d'un ingénieur dédié (à temps partiel ou à temps plein selon la taille du réseau). Ce contrat lie Orsenna à ses clients par une obligation de moyens. Il assure à nos clients une haute disponibilité de l'intervenant avec des garanties de délais d'interventions et de moyens mis en œuvre aux côtés de ses propres équipes.

L'objectif de la régie de supervision est d'assurer la maintenance évolutive de votre environnement de supervision réseau :

«

Votre réseau évolue → Intégration des nouveaux composants

Création de nouvelles cartes « métiers » → Mise en place

Gestion de nouveaux paramètres SNMP → Mise à jour IOS et intégration

Nouvelle version WhatsUp → Formation

«

L'offre de régie de supervision vous garantit une disponibilité de vos outils de supervision au plus près de votre schéma réel d'infrastructure.

Cette offre se décline sous la forme de prestations trimestrielles réalisées en fonction des besoins des équipes d'exploitation.