

MISE EN ŒUVRE D'UNE SOLUTION DE SUPERVISION NAGIOS XI V 5.4.13

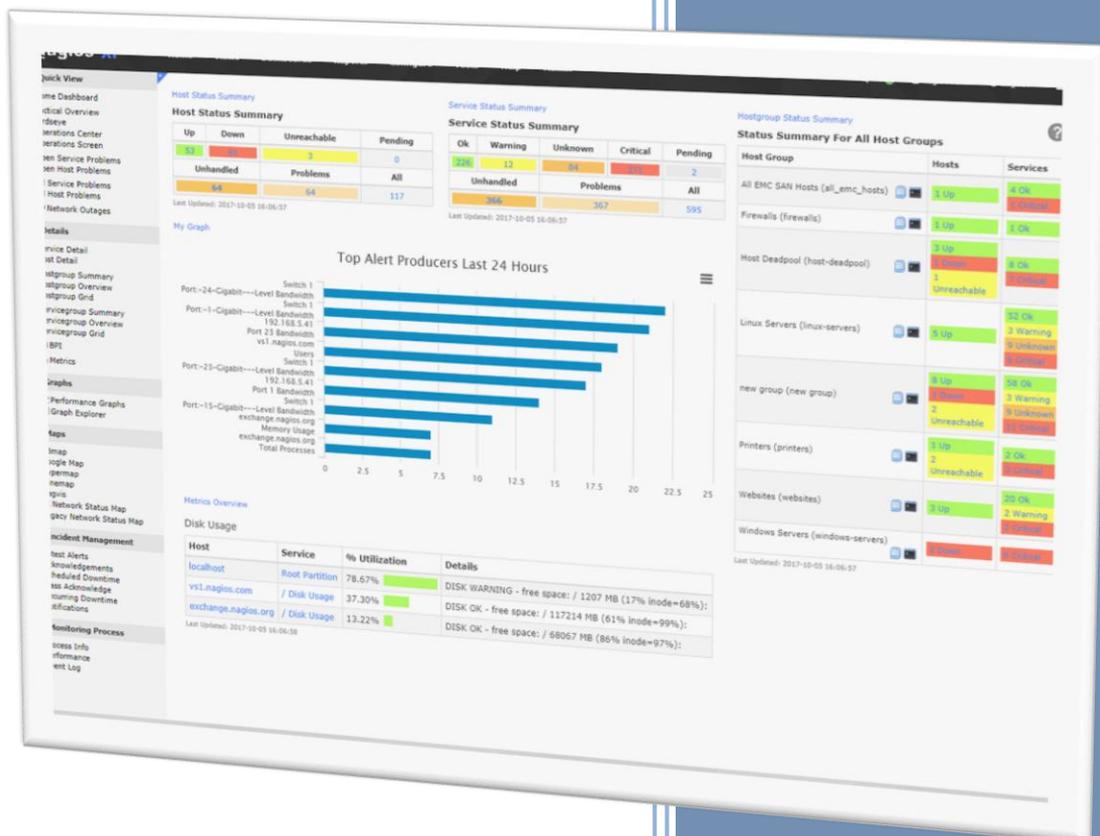


Table des matières

1. Versions.....	5
2. Préambule.....	5
2.1. Orsenna.....	5
2.2. Notre métier, vous accompagnez sur vos projets de supervision	5
1.....	5
2.2.1. Missions d’analyse du marché	5
2.2.2. Benchmarks.....	5
2.2.3. Mise en œuvre	6
2.2.4. Partenaires Editeurs.....	6
2.2.5. Open Source.....	7
3. Analyse Globale Projet.....	8
3.1. Présentation globale	8
3.1.1. Périmètre de surveillance	8
3.2. Choix Technique.....	8
3.3. Choix Commercial	12
3.4. Produits mis en œuvre.....	15
3.5. Analyse Supervision – Conformité aux objectifs.....	16
3.5.1. Centralisation surveillance.....	16
3.5.2. Surveillance Disque – CPU – Mémoire.....	17
3.5.3. Surveillance Serveurs Windows	18
3.5.4. Surveillance Serveurs Linux.....	20
3.5.5. Surveillance MySQL.....	21
3.5.6. Surveillance Oracle.....	21
3.5.7. Surveillance Postgres	22
3.5.8. Surveillance Web.....	22
3.5.9. Surveillances des interfaces Switchs et Routers	23
3.5.10. Surveillance applicatives	24
3.5.11. Surveillance VMware	25
3.5.12. Capacity planning.....	26
3.5.13. Autres surveillances	27
3.5.14. Cartographie, Views et Dashboard.	28
3.5.15. Rapports.....	32
3.5.16. Authentification LDAP	34

3.5.17.	Core Config Manager	34
3.6.	Complément Gestion de logs	35
3.7.	Complément NetFlow	36
3.8.	Options : Appliance SMS	37
3.8.1.	SendQuick – Talariax	37
3.8.2.	SMSEagle – SMSEAGLE	38
3.9.	Option : MiniFlowProbe	39
4.	Conclusion	40
4.1.	Bilan	40
4.1.1.	Bilan Analyse	40
4.1.2.	Bilan logiciel	40
4.2.	Pré-requis Environnement Serveur	40
4.2.1.	Recommandations éditeur	40
4.2.2.	Recommandations Orsenna	41
4.2.3.	Environnement de supervision	41
5.	Mise en œuvre – Mode Projet	41
5.1.	Présentation de la démarche méthodologique pour la réalisation de la prestation	42
5.2.	Phase 1 : Initialisation du projet	42
5.2.1.	Description	42
5.2.2.	Points d’entrée	43
5.3.	Phase 2 : Spécifications Générales	43
5.3.1.	Description	43
5.3.2.	Points d’entrée	43
5.3.3.	Fournitures et revues	43
5.4.	Phase 3 : Spécifications Détaillées	44
5.4.1.	Description	44
5.4.2.	Points d’entrée	44
5.4.3.	Fournitures et revues	44
5.5.	Phase 4 : Maquette	45
5.5.1.	Description	45
5.5.2.	Points d’entrée	45
5.5.3.	Fournitures et revues	45
5.6.	Phase 5 : Mise en œuvre	46
5.6.1.	Description	46
5.6.2.	Points d’entrée	46

5.6.3.	Fournitures et revues.....	46
5.7.	Phase 6 : Recette et Pré-production.....	47
5.7.1.	Description.....	47
5.7.2.	Points d'entrée.....	47
5.7.3.	Fournitures et revues.....	47
5.8.	Phase 7 Formation et transfert de compétence.....	47
5.9.	Livrables et documentation.....	48
6.	Mise en œuvre – Mode Assistance.....	48
7.	Mise en œuvre – Mode POC.....	49
8.	Charges.....	50
8.1.	Tableau de charge de travail - Mode Projet.....	50
8.2.	Charges – Mode Assistance.....	51
8.3.	Charges – Mode POC.....	52
9.	Prestations complémentaires.....	53
9.1.	Maintenance.....	53
9.2.	Assistance, expertise et formation.....	53
10.	Conclusion.....	53

1. Versions

1.0 : Version initiale

2. Préambule

2.1. Orsenna

Orsenna est présent depuis 2000 sur le marché de la supervision avec plus de 500 installations d'outils de supervision et réalise actuellement une cinquantaine d'installation annuellement.

Orsenna intervient à toutes les étapes de vos projets de supervision :

- Analyse des besoins
- Consultation des éditeurs
- Mise en œuvre des solutions

2.2. Notre métier, vous accompagnez sur vos projets de supervision

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

2.2.1. 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: Nagios)
- Animation de séminaire de présentation d'outils de supervisions (Ex : Ipvista, Ipswitch, Solarwinds, Ground Work, Nagios)

2.2.2. Benchmarks

Nous réalisons régulièrement une validation des produits du marché sur notre plate-forme de tests soit au titre de la ville 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.

2.2.3. 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, ASF
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).

2.2.4. Partenaires Editeurs

Orsenna s'appuie sur les produits du marché en intégrant les solutions adaptées à votre environnement avec 3 éditeurs de logiciels de supervision réseau :

	Editeur de WhatsUp
	Editeur d'OpManager & Applications Manager
	Editeur d'Orion
	Editeur de Nagios XI

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

	Editeur de Denika & Logalot Distributeur de Scrutinizer (Netflow, Sflow, Jflow))
	Editeur de Solarwinds Engineer Toolset
	Editeur de composants SNMP
	Editeur de Kiwi Syslog

2.2.5. Open Source

Orsenna s'appuie sur différents environnements open Source du marché afin de compléter les possibilités d'intégration :

	<p>Open Source de référence pour la supervision</p>
	<p>Open Source commercial s'appuyant sur Nagios, Cacti,...</p>
	<p>Open Source commercial</p>
	<p>Agents Open Source pour la gestion des journaux</p>

3. Analyse Globale Projet

Le client souhaite mettre en place un logiciel de supervision des serveurs et des éléments du réseau.

Le client souhaite donc se doter d'un outil capable de :

- vérifier en continu la connectivité et l'activité réseau des différents équipements locaux et distants.
- vérifier le fonctionnement des systèmes d'exploitation et de leurs services « de base ».
- surveiller certains éléments applicatifs (bases de données, services applicatifs spécifiques, services WEB...).
- alerter les administrateurs internes et externes par des moyens comme l'e-mail.

L'objectif de ce document est de décrire les différentes phases du projet et les moyens humains et techniques mis en œuvre pour la réalisation de ces travaux.

3.1. Présentation globale

3.1.1. Périmètre de surveillance

Le périmètre de surveillance est constitué notamment par les points suivants :

- Contrôle d'espace disque disponible sur les serveurs Windows et Linux,
- Vérification que certains services Windows sont bien démarrés et redémarrage automatique si c'est souhaitable,
- Vérification que certains seuils de saturation de CPU, ou de réseau ne sont pas dépassés,
- Vérification de certains seuils accessibles en SQL dans les bases de données ORACLE ou autres (espace disponible dans TABLESPACES ou certains seuils purement applicatifs ...),
- Vérification du bon fonctionnement d'applications WEB par envoi d'un URL et test du résultat (test de présence d'une chaîne dans le résultat).
- Possibilité de réaliser d'autres tests en mode protocolaire type DNS, DHCP, envoi d'email, etc.....
- Possibilité de créer des scénarios de test applicatifs et de rejouer ces scénarios sur des machines de test
- Surveiller les éléments actifs du réseau (commutateur, routeurs ...) avec l'état de leurs différentes interfaces et l'activité réseau sur ces interfaces
- Supervision des serveurs VMWare

3.2. Choix Technique

Un comparatif technique des différentes offres de supervision du marché nous conduit à travers l'analyse des besoins à sélectionner le produit Nagios XI en produit principal.

Notre grille d'analyse est la suivante :

En complément un serveur Syslog est positionné afin de ne pas surcharger la console de supervision en cas d'avalanches importantes de messages Syslog.

	Nagios XI
Installation	
Installation de toute l'application par script shell	
Machine virtuelle	
Web	
Accès remote -multiutilisateurs	
Gestion Utilisateurs	
Authentification interne	
Authentification LDAP (p34)	
Authentification Active Directory	
Droits Lecture/Ecriture	
Groupe (Autre que groupe LDAP)	
Rapports (voir p32)	
Facilité de prise en main	
Intégration de toutes les fonctionnalités	
Découverte du réseau	
Découverte des équipements	
Découverte des surveillances disponibles	
Utilisation des sysObjectID	
Supervision Réseau	
ICMP	
SNMP v1/v2	
SNMP v3	
TCP	
Scripts TCP	
UDP	

SSL	
SSH	
Web	
WMI	
Templates SNMP	
Surveillance via scripts personnalisés	
Gestion de seuil et conditions d'alertes	
Seuil basic	
Seuil avancé (Hystérésis)	
Surveillance système	
Template Vmware	
Template Citrix	Via Add-ons
Template DELL	
Template Unix/Linux	
Surveillance via Plugins	Plugins disponible sur Nagios Exchange
Configuration de Wizard	Via développement
Surveillance applicative	
Service Windows	
Surveillance Processus	
Surveillance WMI	
Template WMI	
Template Exchange	Via add-ons
Template Lotus	Via add-ons
Template Apache	Via add-ons
Template IIS	via WMI
Template AD	Via add-ons

Template RADIUS	
Template Solaris	
Surveillance Base de données	
Template SQL	Via add-ons
Template Oracle	Via add-ons
Template MySQL	
Evénements	
Traps SNMP	
Syslog	Via add-ons
Windows Event Log	
Cartographie	
Auto-map	Partiel
Vue personnalisée	
Logos/Images	
Pastilles de couleurs	
Gestion des équipements	
Ajout de façon manuel	
Découverte automatique	
Ajout depuis un format CSV	
Ajout d'une surveillance sur un équipement	
Ajout d'une surveillance sur plusieurs équipements	
Création de groupe dynamique (p34)	Via Nagios BPI
Création de modèle (Template)	
Planification (Maintenance, absence...) via email	
Actions	
Notification	
Email	

SMS	
Son	
Trap SNMP	
Syslog	Via add-ons
Scripts	
Reporting	
Rapports prédéfinis (p32)	
Rapports personnalisés	
Exports de rapports	
Graphiques	
Planification	
Dashboard	
personnalisé	
Sauvegarde / Restauration	
Configuration	
Base de données	
Maintenance	

3.3. Choix Commercial

Le choix d'un produit Nagios XI est conforté par le positionnement mondial de la solution assurant une pérennité sur l'environnement proposé. NagiosXI est développé et maintenu par l'équipe fondatrice du noyau Nagios. L'éditeur de Nagios XI est le garant des évolutions du Nagios Core (Actuellement en version 4), noyau de la solution NagiosXI. La plupart des autres solutions OpenSource s'appuie toujours la version 3 du Nagios Core (version 2007-2008).

NagiosXI : La solution Nagios, par l'équipe fondatrice de Nagios...



- Première version de **NagiosXI** en 2009
- **Fortes évolutions** du produit et **développement de solutions additionnelles** depuis 2010:
 - Nagios Fusion
 - Nagios Log Manager
 - Nagios Network Analyzer
 - Nagios Incident Manager
 - Nagios Reactor
- Nagios est le **garant des évolutions du noyau** (NagiosCore 4 en 2013-2014) à ce jour exploité par de nombreuses solutions OpenSource
- Fork de Nagios le plus pérenne



Fonctionnellement, NagiosXI est l'une des solutions OpenSource les plus complète et aboutie. Elle met à disposition de ses administrateurs une base importante de templates afin de faciliter le déploiement de surveillance et de limiter le temps d'intégration. De même, le développement de l'outil est très actif, et corrélé avec les demandes de la communauté d'utilisateurs, ce qui se traduit dans les faits par un enrichissement régulier de la solution.

Pourquoi NagiosXI ?



- L'un des meilleurs choix techniques de solution de supervision OpenSource:
 - Solution pérenne
 - Large choix de templates et de surveillance natives
 - Hautement configurable
 - Facilement extensible
 - Fiable et Robuste
 - Développement très actifs (4 releases annuels)
 - Communauté active
 - Interface conviviale
 - Rapide de prise en main
 - Large choix de tableaux de bords et rapports

NagiosXI est fort d'une communauté d'utilisateurs et d'un réseau de revendeurs, sans équivalent pour les solutions de supervision OpenSource. La base documentaire, ainsi que les tutoriels et sessions de trainings régulières, permettent de faciliter la prise en main de l'outil ainsi que la veille technologique.

La dynamique NagiosXI ...



- La plus importante communauté d'utilisateur pour une solution de supervision
- Un réseau de revendeurs très étendu, dans le monde entier



- Une forte communication sur les pratiques d'exploitation et les évolutions :
 - Webinars hebdomadaires
 - Forums et Conférences
- Une large base documentaire
- Sessions de formations certifiantes online

3.4. Produits mis en œuvre

Dans le cadre de notre proposition, les produits pouvant être mis en œuvre sur votre environnement vis-à-vis des thèmes abordés sont les suivants :

- Nagios XI 5.4.13
- Nagios Fusion (Si plusieurs console Nagios)
- Nagvis 1.8.5 (Cartographie)

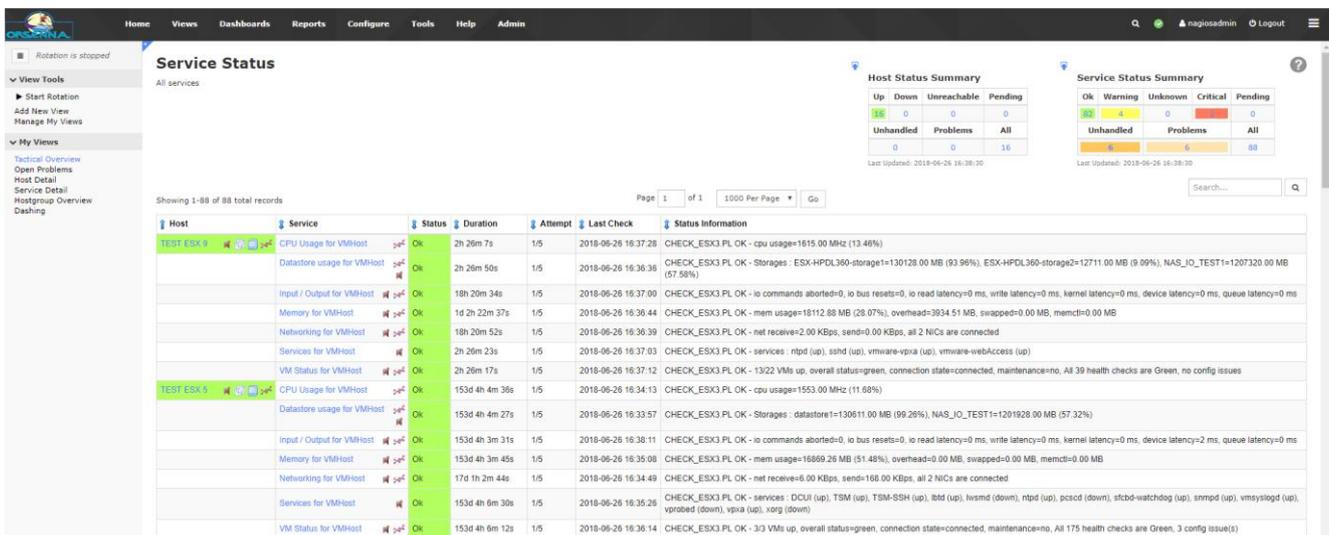
Une multitude de plugins sont disponibles depuis le site de Nagios, et certains pourront être mis en place selon les besoins spécifiques de la solution de supervision.

3.5. Analyse Supervision – Conformité aux objectifs

3.5.1. Centralisation surveillance

L'environnement Nagios XI permet de centraliser la surveillance des différents systèmes dans une console unique. Des outils externes peuvent être intégrés à cette console afin d'homogénéiser l'accès aux environnements.

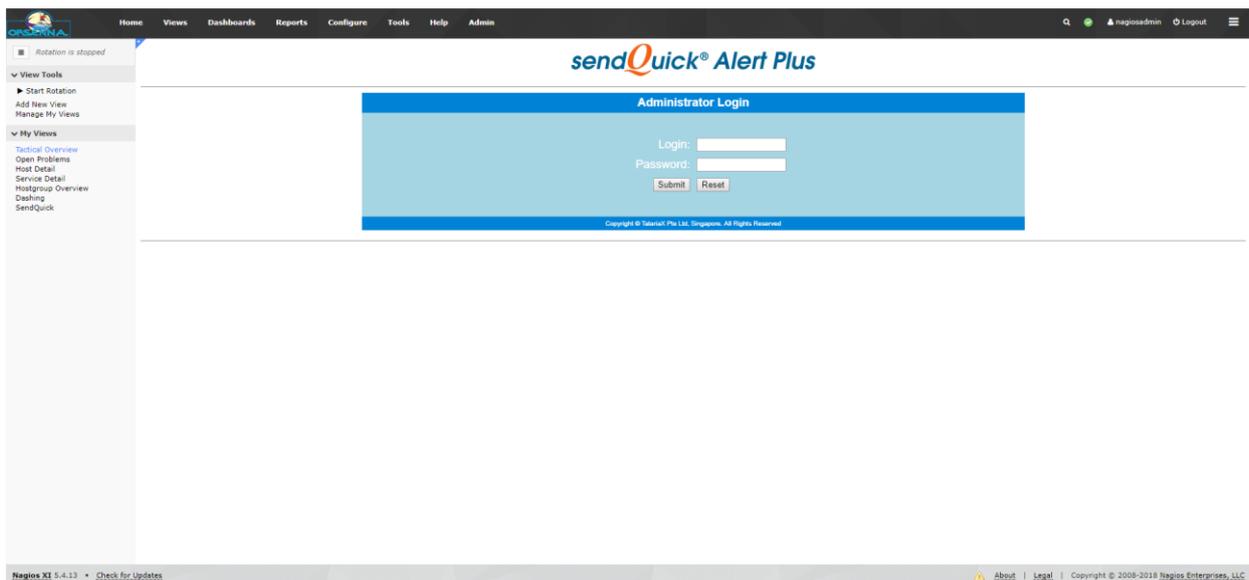
Exemple de console



The screenshot displays the Nagios XI 'Service Status' page. It features a navigation menu on the left, a 'Service Status' header, and two summary boxes: 'Host Status Summary' and 'Service Status Summary'. The main content is a table listing services with columns for Host, Service, Status, Duration, Attempt, Last Check, and Status Information. The table shows various services like 'TEST ESX 9' and 'TEST ESX 5' with their respective statuses and last check times.

Host	Service	Status	Duration	Attempt	Last Check	Status Information
TEST ESX 9	CPU Usage for VMHost	Ok	2h 26m 7s	1/5	2018-06-26 16:37:28	CHECK_ESX3.PL.OK - cpu usage=1615.00 MHz (13.46%)
	Datstore usage for VMHost	Ok	2h 26m 50s	1/5	2018-06-26 16:36:38	CHECK_ESX3.PL.OK - Storages: ESX-HPDCL360-storage1=130128.00 MB (93.96%), ESX-HPDCL360-storage2=127111.00 MB (9.09%), NAS_JO_TEST1=1207320.00 MB (57.58%)
	Input / Output for VMHost	Ok	18h 20m 34s	1/5	2018-06-26 16:37:00	CHECK_ESX3.PL.OK - io commands aborted=0, io bus resets=0, io read latency=0 ms, write latency=0 ms, kernel latency=0 ms, device latency=0 ms, queue latency=0 ms
	Memory for VMHost	Ok	1h 2h 22m 37s	1/5	2018-06-26 16:36:44	CHECK_ESX3.PL.OK - mem usage=18112.88 MB (28.07%), overhead=3934.51 MB, swapped=0.00 MB, memctd=0.00 MB
	Networking for VMHost	Ok	18h 20m 52s	1/5	2018-06-26 16:36:39	CHECK_ESX3.PL.OK - net receive=2.00 KBps, send=0.00 KBps, all 2 NICs are connected
	Services for VMHost	Ok	2h 26m 23s	1/5	2018-06-26 16:37:03	CHECK_ESX3.PL.OK - services: ntpd (up), sshd (up), vmware-vpxa (up), vmware-webAccess (up)
	VM Status for VMHost	Ok	2h 26m 17s	1/5	2018-06-26 16:37:12	CHECK_ESX3.PL.OK - 13/22 VMs up, overall status=green, connection state=connected, maintenance=no, All 39 health checks are Green, no config issues
TEST ESX 5	CPU Usage for VMHost	Ok	153d 4h 4m 36s	1/5	2018-06-26 16:34:13	CHECK_ESX3.PL.OK - cpu usage=1553.00 MHz (11.68%)
	Datstore usage for VMHost	Ok	153d 4h 4m 27s	1/5	2018-06-26 16:33:57	CHECK_ESX3.PL.OK - Storages: datastore1=130611.00 MB (99.26%), NAS_JO_TEST1=1201928.00 MB (57.32%)
	Input / Output for VMHost	Ok	153d 4h 3m 31s	1/5	2018-06-26 16:30:11	CHECK_ESX3.PL.OK - io commands aborted=0, io bus resets=0, io read latency=0 ms, write latency=0 ms, kernel latency=0 ms, device latency=2 ms, queue latency=0 ms
	Memory for VMHost	Ok	153d 4h 3m 45s	1/5	2018-06-26 16:35:08	CHECK_ESX3.PL.OK - mem usage=16969.29 MB (51.48%), overhead=0.00 MB, swapped=0.00 MB, memctd=0.00 MB
	Networking for VMHost	Ok	17d 1h 2m 44s	1/5	2018-06-26 16:34:49	CHECK_ESX3.PL.OK - net receive=6.00 KBps, send=168.00 KBps, all 2 NICs are connected
	Services for VMHost	Ok	153d 4h 6m 30s	1/5	2018-06-26 16:35:28	CHECK_ESX3.PL.OK - services: DCUI (up), TSM (up), TSM-SSH (up), lrd (up), hsrmd (down), ntpd (up), pcsd (down), stfcd-watchdog (up), tnmpp (up), vmsyslogd (up), vprobred (down), vpxa (up), xorg (down)
	VM Status for VMHost	Ok	153d 4h 6m 12s	1/5	2018-06-26 16:36:14	CHECK_ESX3.PL.OK - 3/3 VMs up, overall status=green, connection state=connected, maintenance=no, All 175 health checks are Green, 3 config issue(s)

Intégration d'outils externes dans la console



The screenshot shows the Nagios XI console with the 'sendQuick® Alert Plus' integration. A blue banner at the top reads 'sendQuick® Alert Plus'. Below it, there is an 'Administrator Login' form with fields for 'Login:' and 'Password:', and 'Submit' and 'Reset' buttons. The footer of the page includes 'Nagios XI 5.4.13' and 'Copyright © 2008-2018 Nagios Enterprises, LLC'.

3.5.3. Surveillance Serveurs Windows

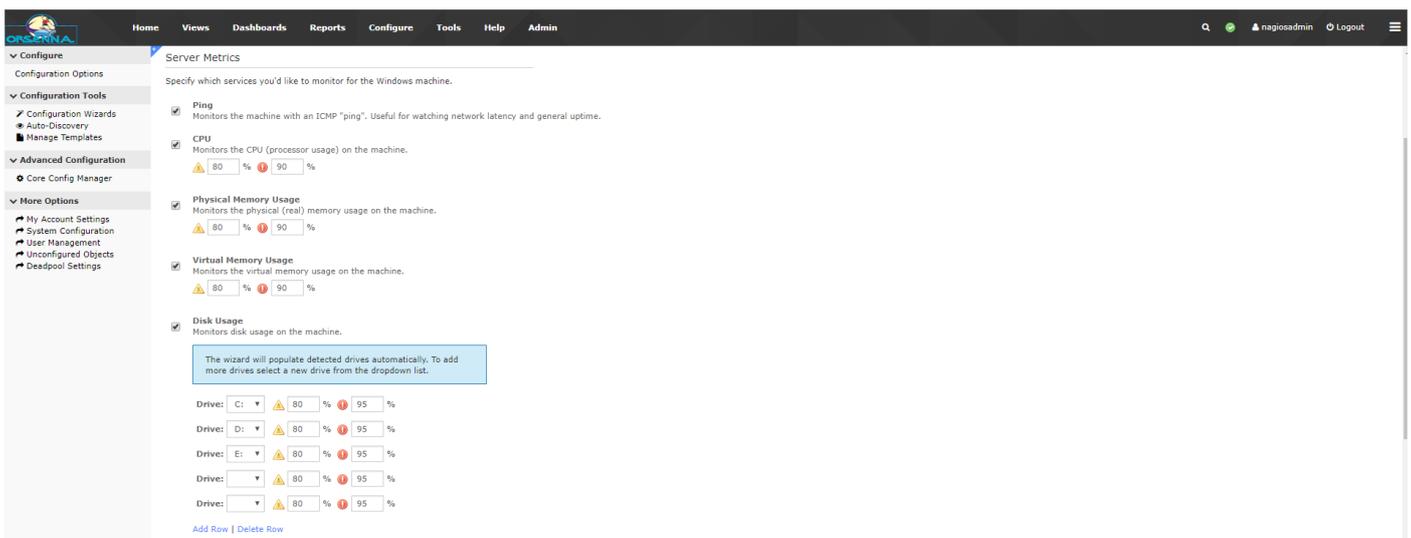
Plusieurs outils sont fournis par Nagios XI pour surveiller les serveurs Windows :

- Surveillances de base
- Surveillances WMI
- Windows Event Log

Monitoring Wizards Windows

<input type="radio"/>		Windows Desktop Monitor a Microsoft® Windows XP, Windows Vista, or Windows 7 desktop.
<input type="radio"/>		Windows Event Log Monitor Windows event logs.
<input type="radio"/>		Windows Server Monitor a Microsoft® Windows 2000, 2003, 2008 or 2012 server.
<input type="radio"/>		Windows SNMP Monitor a Microsoft® Windows workstation or server using SNMP.
<input type="radio"/>		Windows WMI Monitor a Microsoft® Windows workstation or server using WMI.

Surveillances serveurs

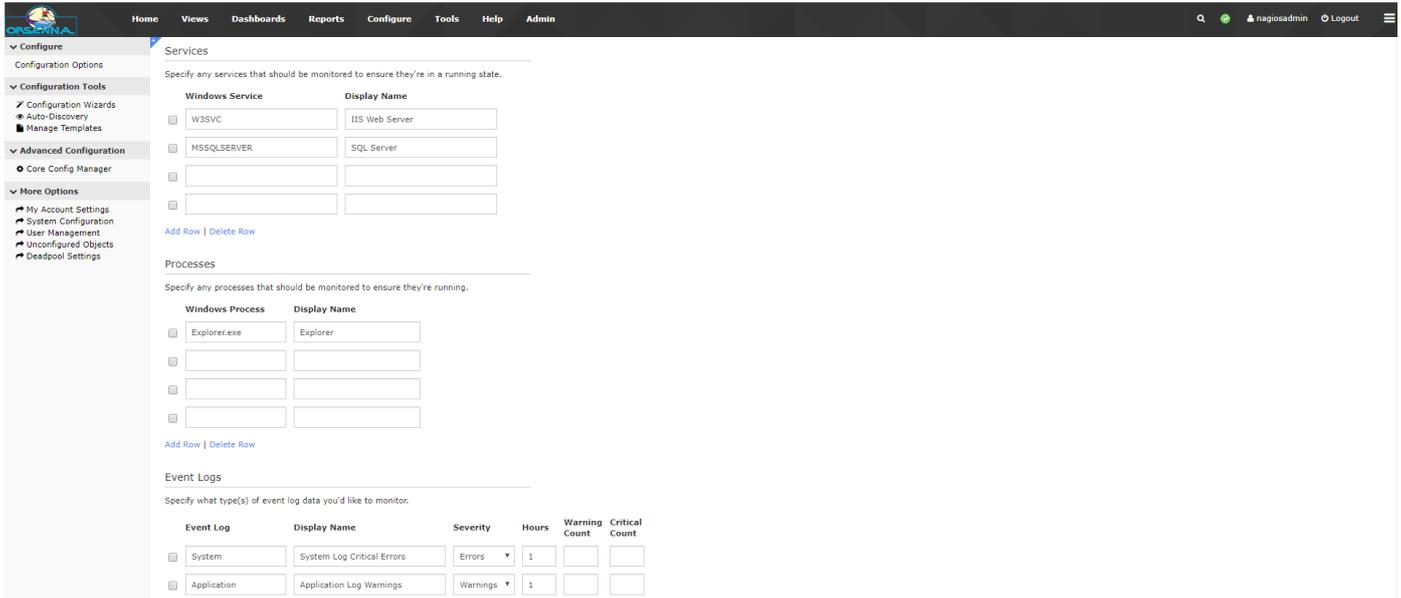


The screenshot shows the Nagios XI configuration interface for 'Server Metrics'. The left sidebar contains navigation options like 'Configure', 'Configuration Tools', 'Advanced Configuration', and 'More Options'. The main content area is titled 'Server Metrics' and includes a sub-header 'Specify which services you'd like to monitor for the Windows machine.' Below this, several monitoring options are listed with checkboxes and threshold settings:

- Ping**: Monitors the machine with an ICMP "ping". Useful for watching network latency and general uptime. (Thresholds: 80% / 90%)
- CPU**: Monitors the CPU (processor usage) on the machine. (Thresholds: 80% / 90%)
- Physical Memory Usage**: Monitors the physical (real) memory usage on the machine. (Thresholds: 80% / 90%)
- Virtual Memory Usage**: Monitors the virtual memory usage on the machine. (Thresholds: 80% / 90%)
- Disk Usage**: Monitors disk usage on the machine. A blue callout box states: 'The wizard will populate detected drives automatically. To add more drives select a new drive from the dropdown list.' Below this, five drive entries are shown, each with a dropdown menu and threshold settings (80% / 95%):
 - Drive: C: [80% / 95%]
 - Drive: D: [80% / 95%]
 - Drive: E: [80% / 95%]
 - Drive: [80% / 95%]
 - Drive: [80% / 95%]

At the bottom of the configuration area, there are links for 'Add Row' and 'Delete Row'.

Surveillances WMI



Services

Specify any services that should be monitored to ensure they're in a running state.

Windows Service	Display Name
<input type="checkbox"/> W3SVC	IIS Web Server
<input type="checkbox"/> MSSQLSERVER	SQL Server
<input type="checkbox"/>	
<input type="checkbox"/>	

[Add Row](#) | [Delete Row](#)

PROCESSES

Specify any processes that should be monitored to ensure they're running.

Windows Process	Display Name
<input type="checkbox"/> Explorer.exe	Explorer
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

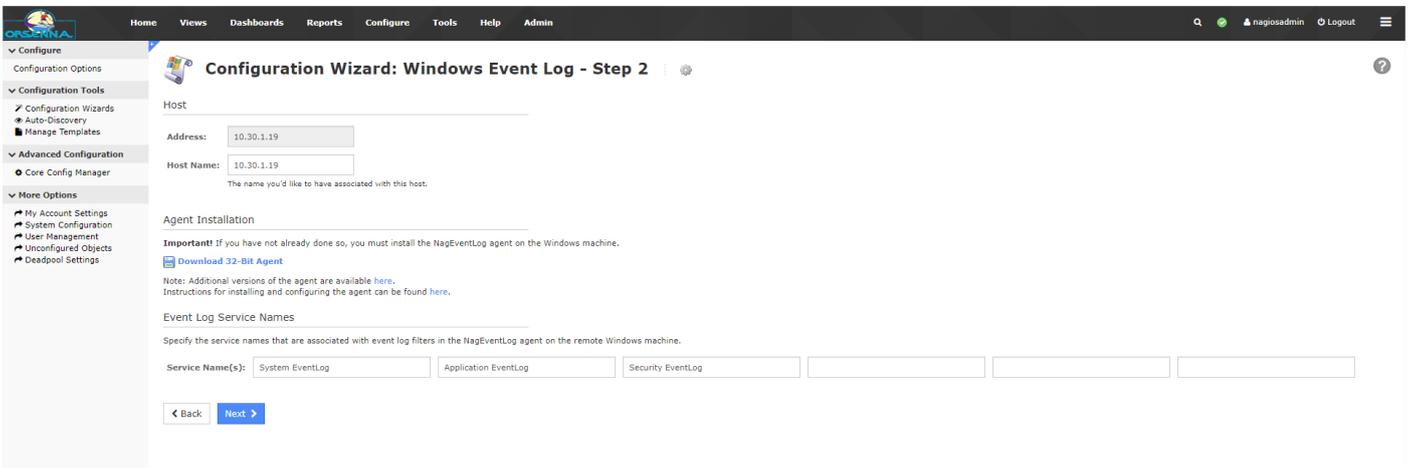
[Add Row](#) | [Delete Row](#)

Event Logs

Specify what type(s) of event log data you'd like to monitor.

Event Log	Display Name	Severity	Hours	Warning Count	Critical Count
<input type="checkbox"/> System	System Log Critical Errors	Errors ▼	1		
<input type="checkbox"/> Application	Application Log Warnings	Warnings ▼	1		

Windows Event Log



Configuration Wizard: Windows Event Log - Step 2

Host

Address:

Host Name:

The name you'd like to have associated with this host.

Agent Installation

Important! If you have not already done so, you must install the NagEventLog agent on the Windows machine.

[Download 32-Bit Agent](#)

Note: Additional versions of the agent are available [here](#).
Instructions for installing and configuring the agent can be found [here](#).

Event Log Service Names

Specify the service names that are associated with event log filters in the NagEventLog agent on the remote Windows machine.

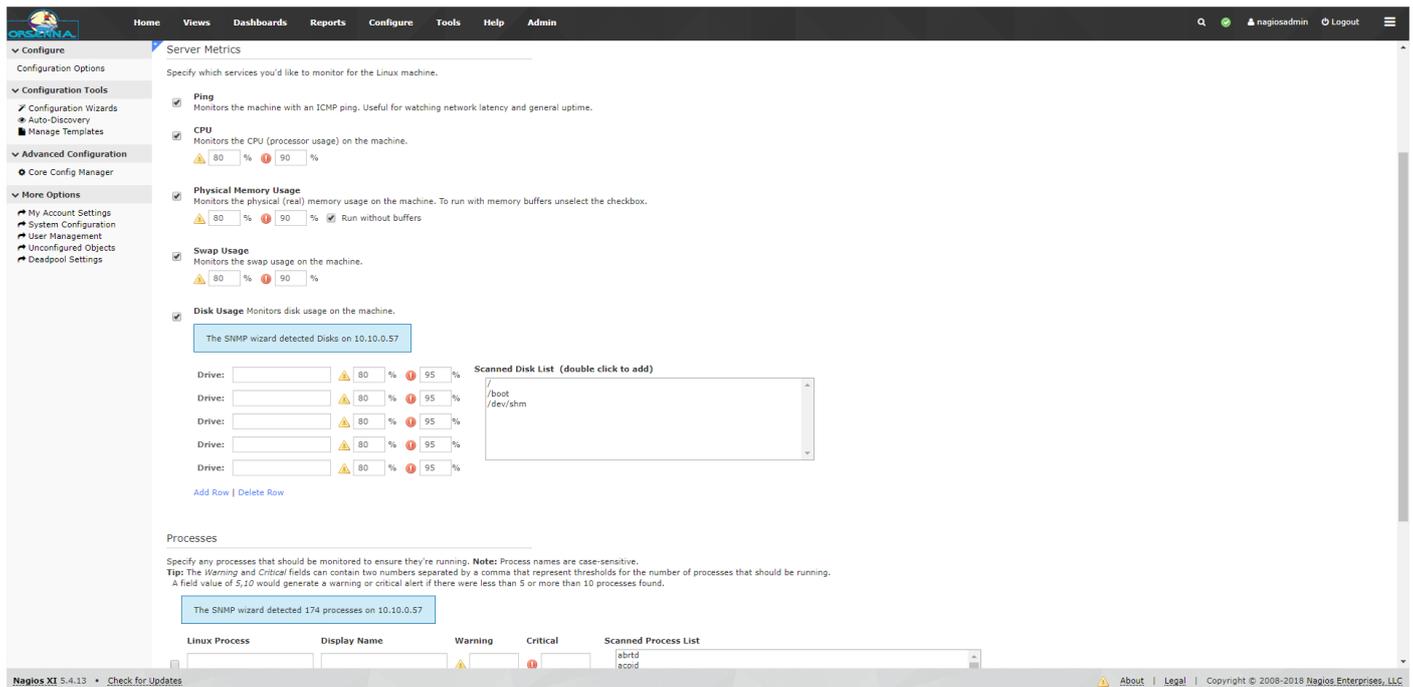
Service Name(s):

[Back](#) [Next](#)

3.5.4. Surveillance Serveurs Linux

Des outils sont fournis par la console Nagios XI, permettant de surveiller et de découvrir les serveurs Linux, via un agent fourni (NT, NRPE).

Surveillance d'un serveur linux

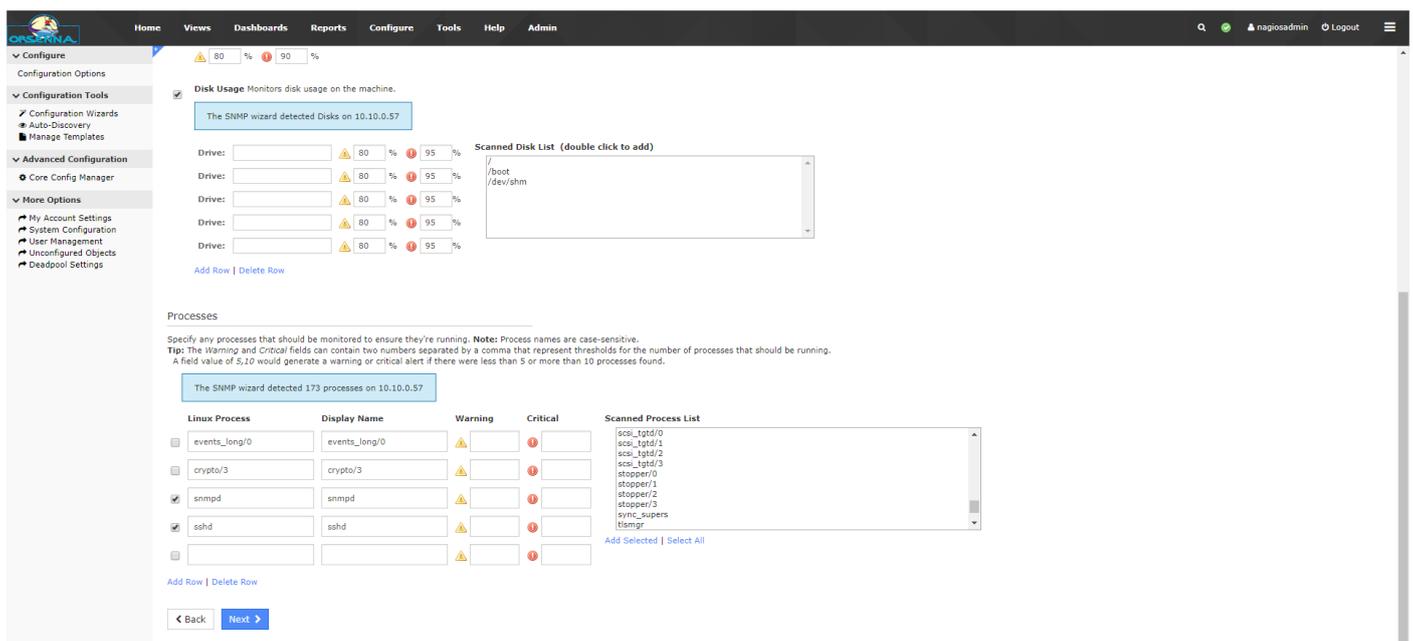


The screenshot shows the 'Server Metrics' configuration page in Nagios XI. It includes sections for 'Physical Memory Usage', 'Swap Usage', and 'Disk Usage'. The 'Disk Usage' section shows a table of scanned disks with columns for Drive, Warning, and Critical thresholds. Below this is the 'Processes' section, which includes a table for scanned processes with columns for Linux Process, Display Name, Warning, Critical, and Scanned Process List.

Drive	Warning	Critical
/boot	80 %	95 %
/dev/shm	80 %	95 %

Linux Process	Display Name	Warning	Critical
abrtid			
acpid			

Surveillance des services et processus



The screenshot shows the 'Disk Usage' and 'Processes' configuration pages in Nagios XI. The 'Disk Usage' section shows a table of scanned disks with columns for Drive, Warning, and Critical thresholds. Below this is the 'Processes' section, which includes a table for scanned processes with columns for Linux Process, Display Name, Warning, Critical, and Scanned Process List.

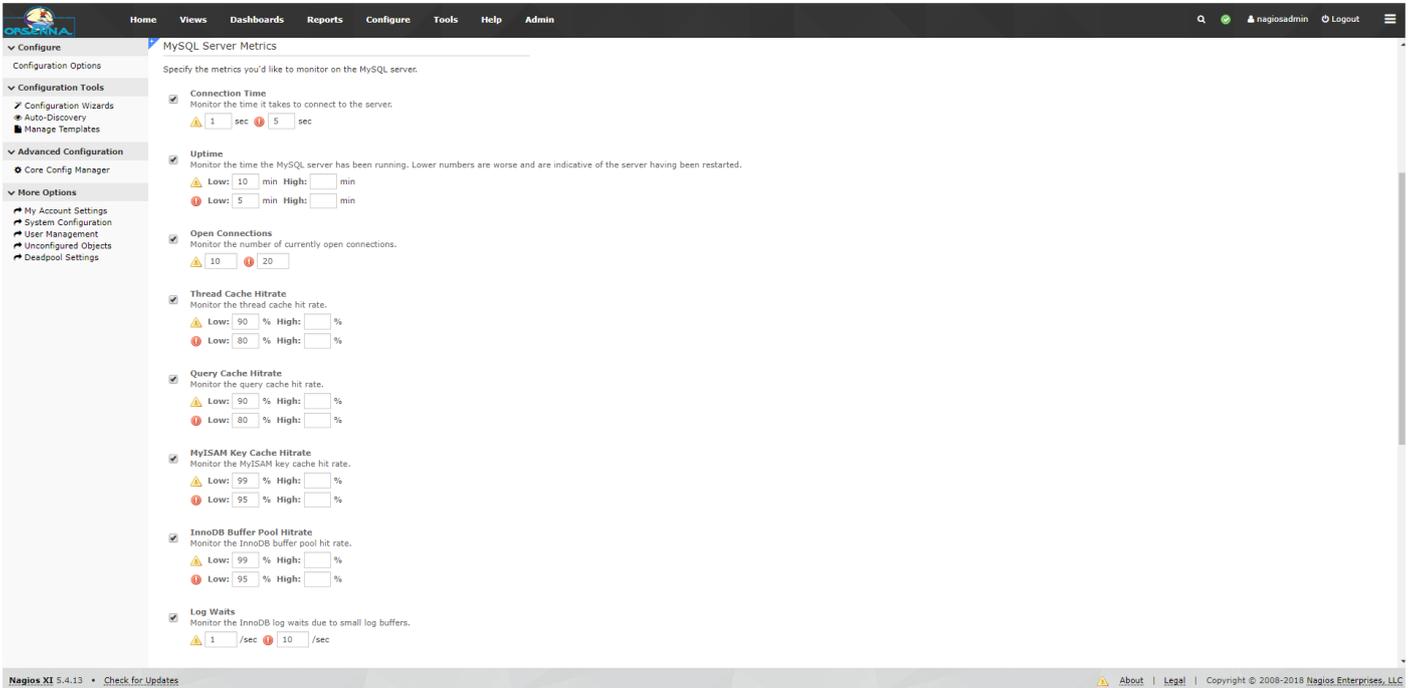
Drive	Warning	Critical
/boot	80 %	95 %
/dev/shm	80 %	95 %

Linux Process	Display Name	Warning	Critical
events_long/0	events_long/0		
crypto/3	crypto/3		
snmpd	snmpd		
sshd	sshd		

3.5.5. Surveillance MySQL

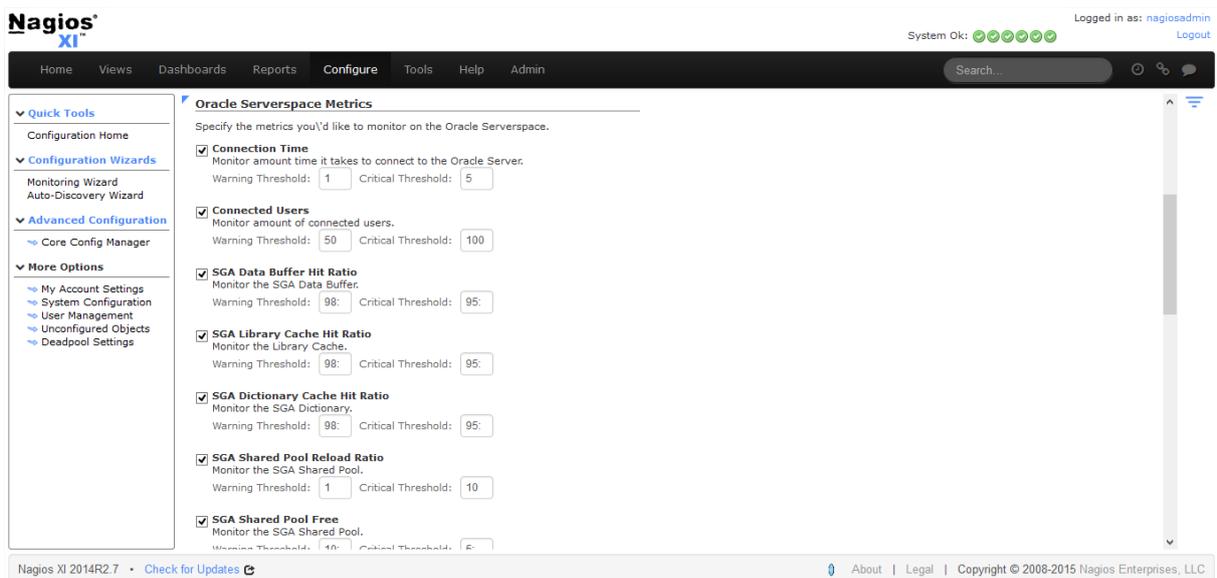
Nous disposons d'outils applicatifs dans Nagios XI, permettant d'accéder aux compteurs de surveillances sur les bases de données MySQL.

Surveillance base de données



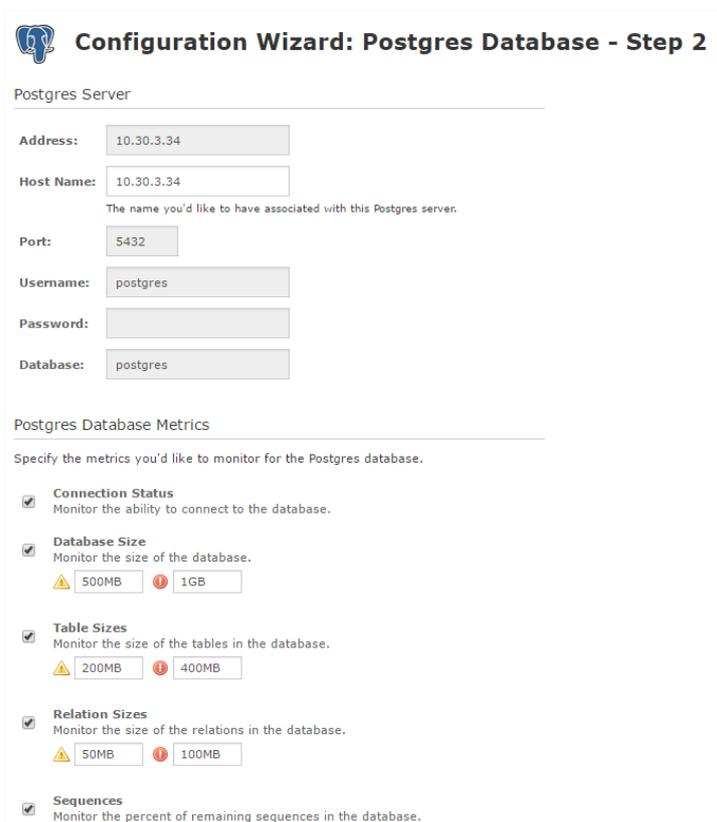
3.5.6. Surveillance Oracle

Nous disposons également d'outils applicatifs dans Nagios XI, permettant d'accéder aux compteurs de surveillances sur les bases de données Oracle.



3.5.7. Surveillance Postgres

Nous disposons également d’outils applicatifs dans Nagios XI, permettant d’accéder aux compteurs de surveillances sur les bases de données Postgres.



Configuration Wizard: Postgres Database - Step 2

Postgres Server

Address: 10.30.3.34

Host Name: 10.30.3.34
The name you'd like to have associated with this Postgres server.

Port: 5432

Username: postgres

Password: [Redacted]

Database: postgres

Postgres Database Metrics

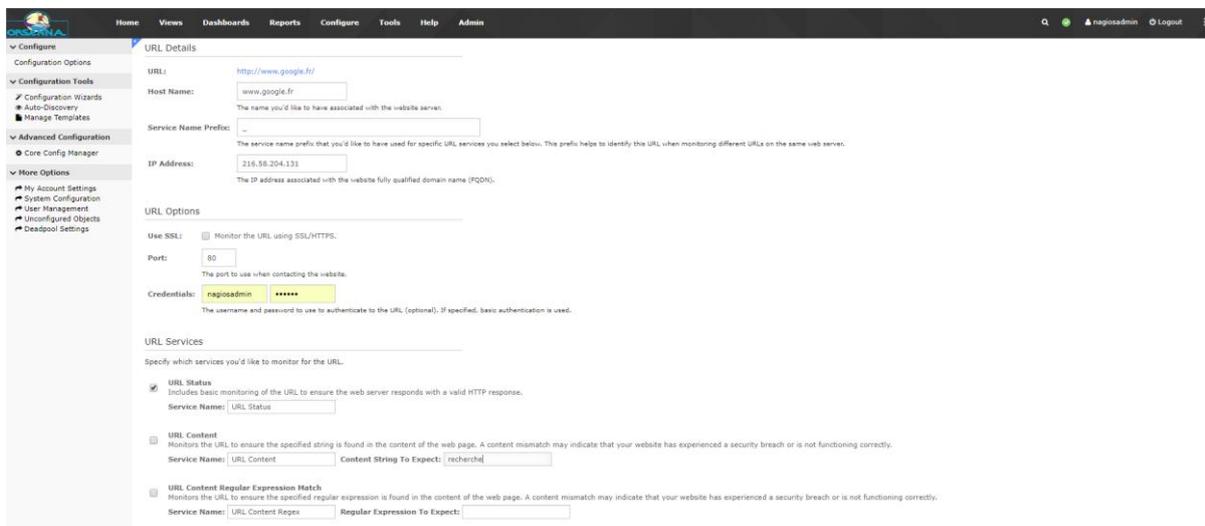
Specify the metrics you'd like to monitor for the Postgres database.

- Connection Status**
Monitor the ability to connect to the database.
- Database Size**
Monitor the size of the database.
500MB 1GB
- Table Sizes**
Monitor the size of the tables in the database.
200MB 400MB
- Relation Sizes**
Monitor the size of the relations in the database.
50MB 100MB
- Sequences**
Monitor the percent of remaining sequences in the database.

3.5.8. Surveillance Web

Une surveillance d’applications WEB peut être mise en place grâce à l’envoi d’une URL et au test du résultat.

Surveillance URL



Home Views Dashboards Reports Configure Tools Help Admin

Configuration Options

Configuration Tools

Advanced Configuration

More Options

URL Details

URL: http://www.google.fr/

Host Name: www.google.fr
The name you'd like to have associated with the website server.

Service Name Prefix: -
The service name prefix that you'd like to have used for specific URL services you select below. This prefix helps to identify the URL when monitoring different URLs on the same web server.

IP Address: 216.58.204.131
The IP address associated with the website fully qualified domain name (FQDN).

URL Options

Use SSL: Monitor the URL using SSL/HTTPS.

Port: 80
The port to use when contacting the website.

Credentials: nagiosadmin *****
The username and password to use to authenticate to the URL (optional). If specified, basic authentication is used.

URL Services

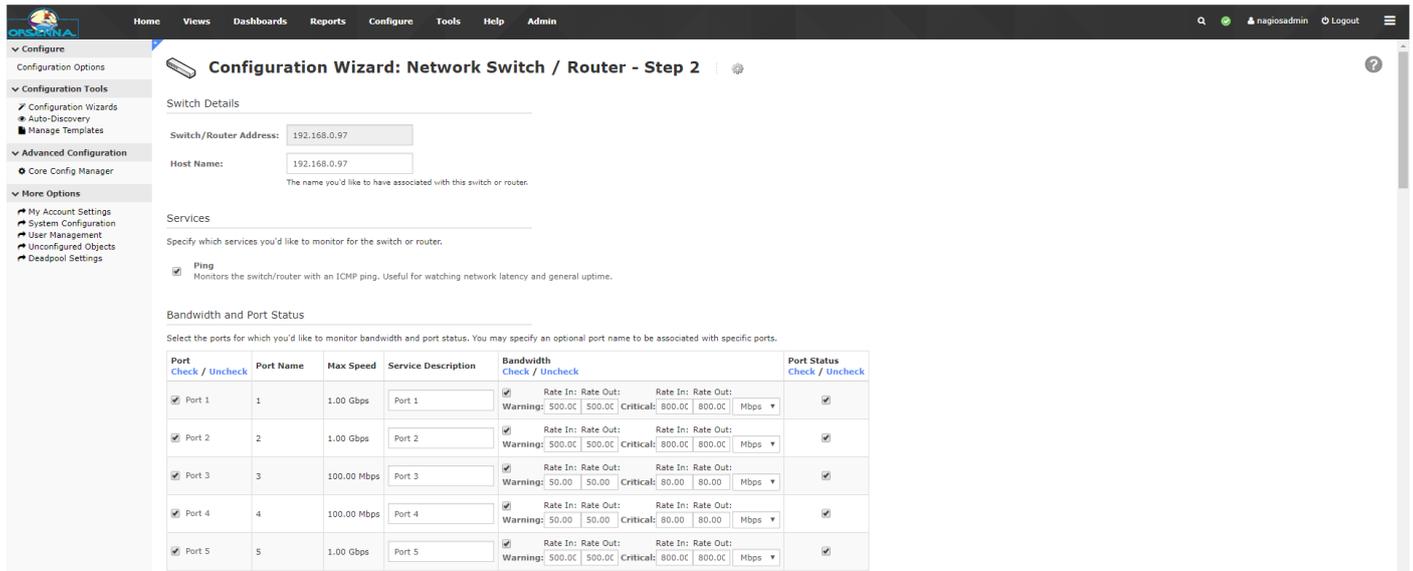
Specify which services you'd like to monitor for the URL.

- URL Status**
Includes basic monitoring of the URL to ensure the web server responds with a valid HTTP response.
Service Name: URL Status
- URL Content**
Monitors the URL to ensure the specified string is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.
Service Name: URL Content Content String To Expect: recherche
- URL Content Regular Expression Match**
Monitors the URL to ensure the specified regular expression is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.
Service Name: URL Content Regex Regular Expression To Expect:

3.5.9. Surveillances des interfaces Switchs et Routers

La console permet le monitoring d'interface de switchs et de Routers via SNMP. Le monitor propose des tests de disponibilités et de bandes passantes.

Découverte des interfaces



Configuration Wizard: Network Switch / Router - Step 2

Switch Details

Switch/Router Address: 192.168.0.97
Host Name: 192.168.0.97

Services

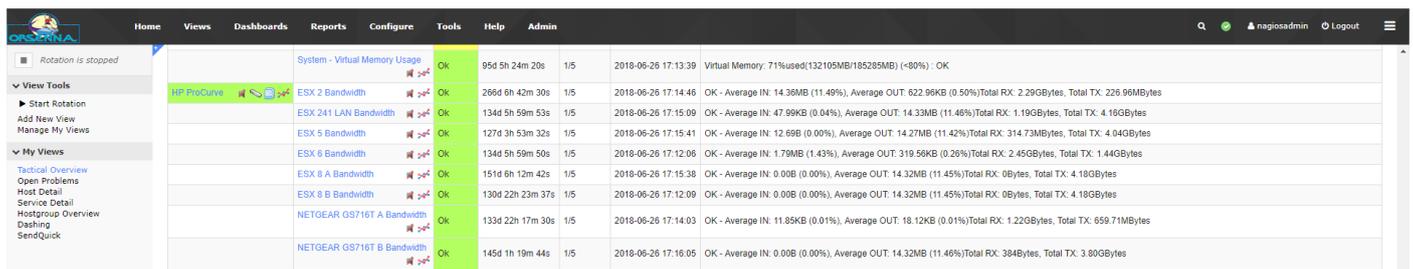
Ping
Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.

Bandwidth and Port Status

Select the ports for which you'd like to monitor bandwidth and port status. You may specify an optional port name to be associated with specific ports.

Port Check / Uncheck	Port Name	Max Speed	Service Description	Bandwidth Check / Uncheck	Port Status Check / Uncheck
<input checked="" type="checkbox"/>	Port 1	1.00 Gbps	Port 1	<input checked="" type="checkbox"/> Rate In: Rate Out: Warning: 500.0C 500.0C Critical: 800.0C 800.0C Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Port 2	1.00 Gbps	Port 2	<input checked="" type="checkbox"/> Rate In: Rate Out: Warning: 500.0C 500.0C Critical: 800.0C 800.0C Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Port 3	100.00 Mbps	Port 3	<input checked="" type="checkbox"/> Rate In: Rate Out: Warning: 50.00 50.00 Critical: 80.00 80.00 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Port 4	100.00 Mbps	Port 4	<input checked="" type="checkbox"/> Rate In: Rate Out: Warning: 50.00 50.00 Critical: 80.00 80.00 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Port 5	1.00 Gbps	Port 5	<input checked="" type="checkbox"/> Rate In: Rate Out: Warning: 500.0C 500.0C Critical: 800.0C 800.0C Mbps	<input checked="" type="checkbox"/>

Visualisation de l'état des interfaces



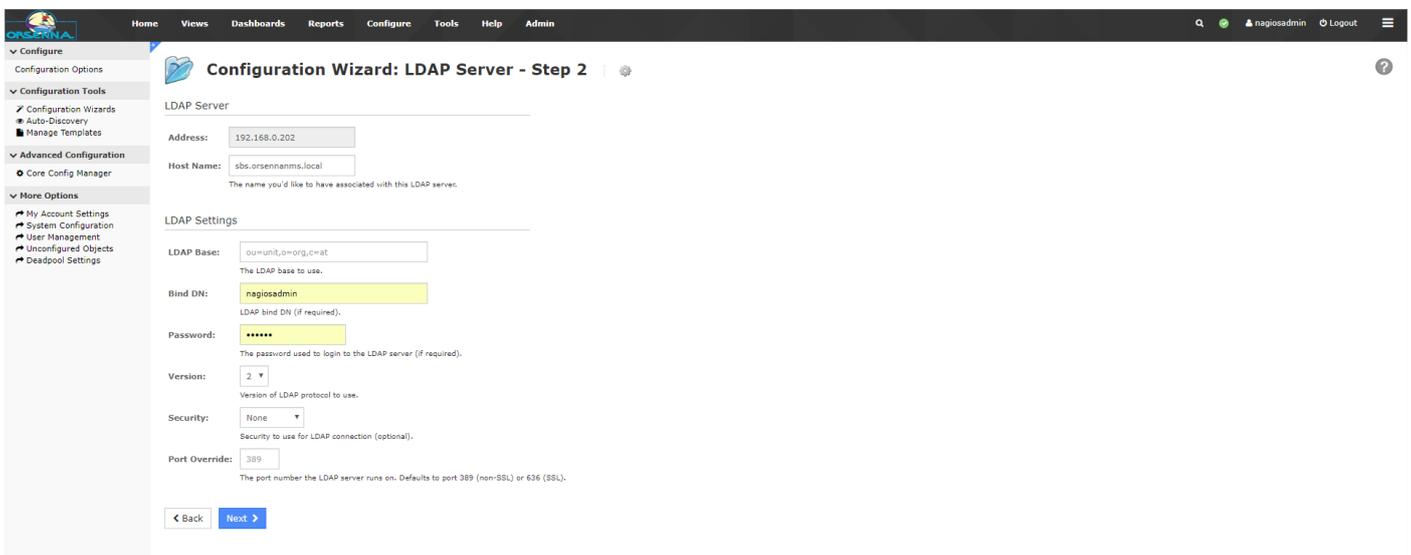
System / Interface	Status	Uptime	Alerts	Last Check	Details
System - Virtual Memory Usage	Ok	95d 5h 24m 20s	1/5	2018-06-26 17:13:39	Virtual Memory: 71%used(132105MB/185285MB) (-80%) - OK
HP ProCurve ESX 2 Bandwidth	Ok	266d 6h 42m 30s	1/5	2018-06-26 17:14:46	OK - Average IN: 14.36MB (11.49%), Average OUT: 622.96KB (0.50%)/Total RX: 2.29GBytes, Total TX: 226.86MBytes
ESX 241 LAN Bandwidth	Ok	134d 5h 59m 53s	1/5	2018-06-26 17:15:09	OK - Average IN: 47.99KB (0.04%), Average OUT: 14.33MB (11.46%)/Total RX: 1.19GBytes, Total TX: 4.16GBytes
ESX 5 Bandwidth	Ok	127d 3h 53m 32s	1/5	2018-06-26 17:15:41	OK - Average IN: 12.69B (0.00%), Average OUT: 14.27MB (11.42%)/Total RX: 314.73MBytes, Total TX: 4.04GBytes
ESX 6 Bandwidth	Ok	134d 5h 59m 50s	1/5	2018-06-26 17:12:06	OK - Average IN: 1.79MB (1.43%), Average OUT: 319.50KB (0.26%)/Total RX: 2.45GBytes, Total TX: 1.44GBytes
ESX 8 A Bandwidth	Ok	151d 6h 12m 42s	1/5	2018-06-26 17:15:38	OK - Average IN: 0.00B (0.00%), Average OUT: 14.32MB (11.45%)/Total RX: 0Bytes, Total TX: 4.18GBytes
ESX 8 B Bandwidth	Ok	130d 22h 23m 37s	1/5	2018-06-26 17:12:09	OK - Average IN: 0.00B (0.00%), Average OUT: 14.32MB (11.45%)/Total RX: 0Bytes, Total TX: 4.18GBytes
NETGEAR GS716T A Bandwidth	Ok	133d 22h 17m 30s	1/5	2018-06-26 17:14:03	OK - Average IN: 11.85KB (0.01%), Average OUT: 18.12KB (0.01%)/Total RX: 1.22GBytes, Total TX: 659.71MBytes
NETGEAR GS716T B Bandwidth	Ok	145d 1h 19m 44s	1/5	2018-06-26 17:16:05	OK - Average IN: 0.00B (0.00%), Average OUT: 14.32MB (11.46%)/Total RX: 384Bytes, Total TX: 3.80GBytes

3.5.10. Surveillance applicatives

Quelques surveillances applicatives sont disponibles dans la console Nagios XI :

- DNS
- DHCP
- FTP
- LDAP
- Radius

Exemple de surveillance d'un serveur LDAP



The screenshot shows the Nagios XI Configuration Wizard for an LDAP Server, Step 2. The interface includes a navigation menu on the left with categories like 'Configure', 'Configuration Tools', 'Advanced Configuration', and 'More Options'. The main content area is titled 'LDAP Server' and contains the following fields and options:

- Address:** 192.168.0.202
- Host Name:** sbs.orsennams.local (with a note: 'The name you'd like to have associated with this LDAP server.')
- LDAP Settings:**
 - LDAP Base:** ou=unit,o=org,c=at (with a note: 'The LDAP base to use.')
 - Bind DN:** nagiosadmin (with a note: 'LDAP bind DN (if required).')
 - Password:** [Redacted] (with a note: 'The password used to login to the LDAP server (if required).')
 - Version:** 2 (with a note: 'Version of LDAP protocol to use.')
 - Security:** None (with a note: 'Security to use for LDAP connection (optional).')
 - Port Override:** 389 (with a note: 'The port number the LDAP server runs on. Defaults to port 389 (non-SSL) or 636 (SSL).')

At the bottom of the form, there are 'Back' and 'Next' buttons.

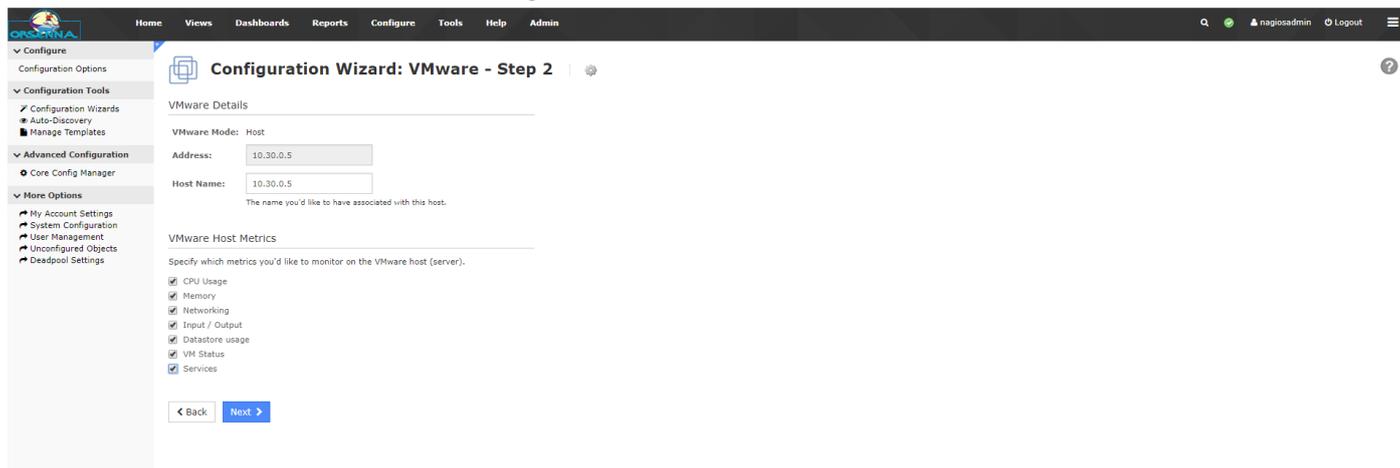
D'autres surveillances sont disponibles, notamment pour les applications liées à Windows, via WMI.

- Exchange
- IIS

3.5.11. Surveillance VMware

Nagios XI permet aussi une surveillance de vos environnements virtualisés VMware. Il est possible de s'attacher aux informations de vCenter, de vos ESX via vSphere et de vos machines virtuelles.

Configuration des surveillances d'un ESX

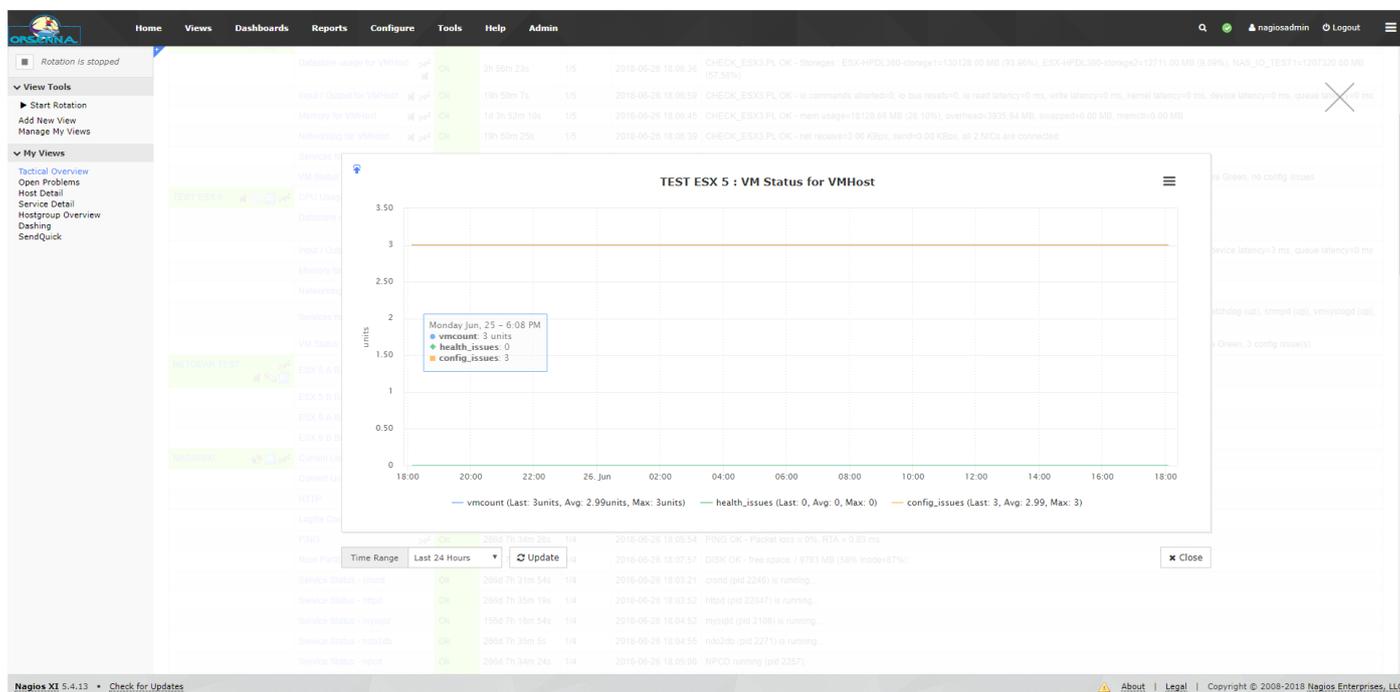


The screenshot shows the 'Configuration Wizard: VMware - Step 2' interface. It includes a sidebar with navigation options like 'Configure', 'Configuration Options', and 'Advanced Configuration'. The main area is titled 'VMware Details' and contains the following fields and options:

- VMware Mode:** Host
- Address:** 10.30.0.5
- Host Name:** 10.30.0.5 (with a note: 'The name you'd like to have associated with this host.')
- VMware Host Metrics:** A section with a note 'Specify which metrics you'd like to monitor on the VMware host (server).' and several checked checkboxes: CPU Usage, Memory, Networking, Input / Output, Database usage, VM Status, and Services.

At the bottom of the configuration area, there are 'Back' and 'Next' buttons.

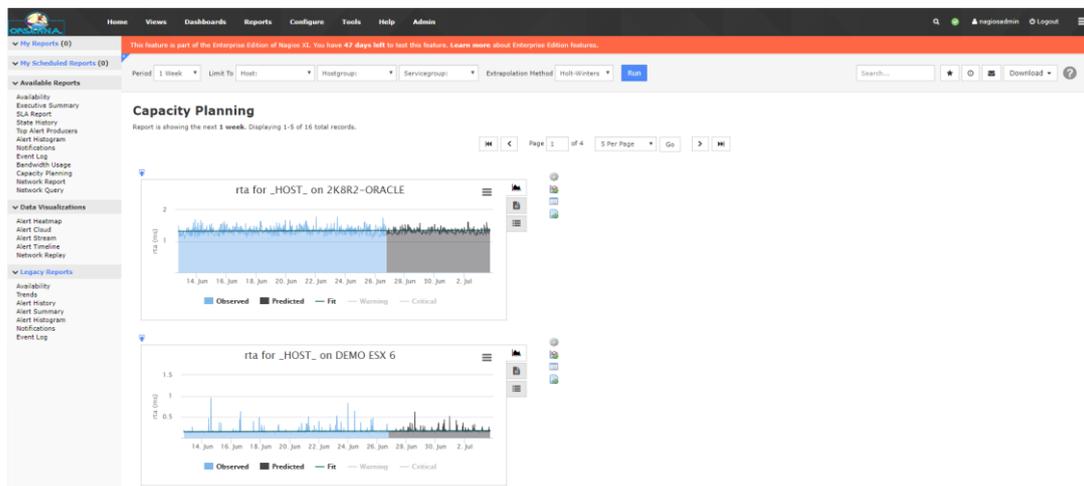
Surveillance d'un ESX et de ces VMs



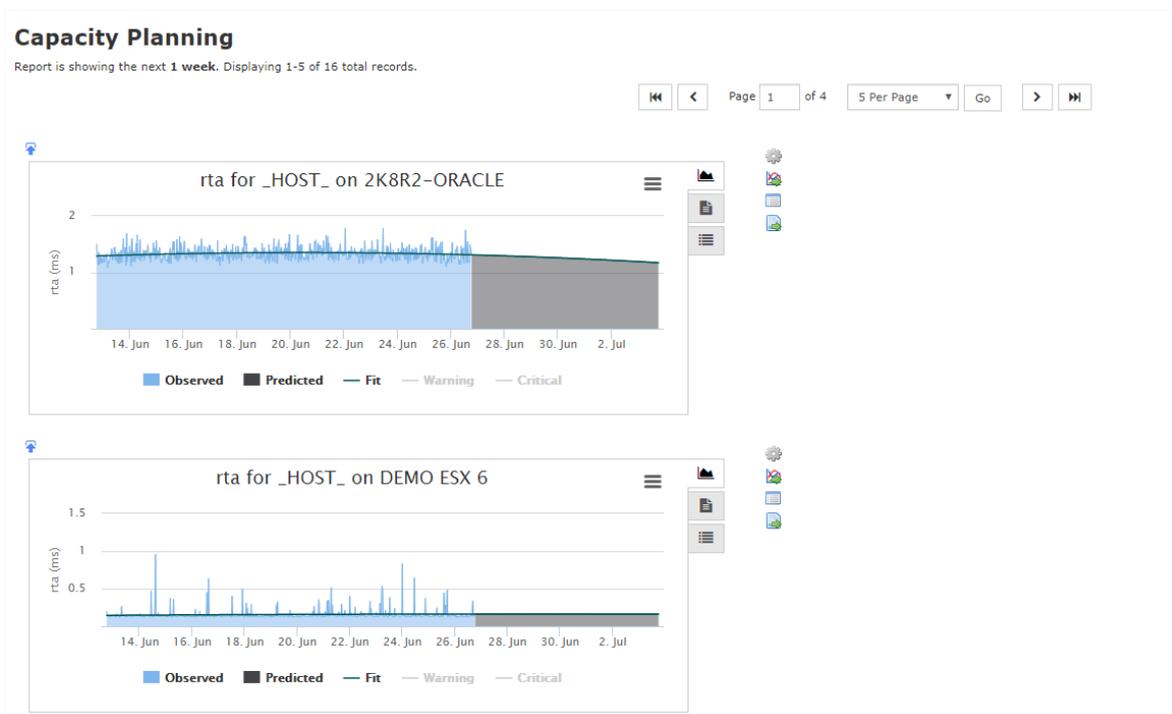
The screenshot displays the Nagios XI monitoring dashboard for VMware. The top navigation bar includes 'Home', 'Views', 'Dashboards', 'Reports', 'Configure', 'Tools', 'Help', and 'Admin'. The main content area is titled 'TEST ESX 5 : VM Status for VMHost' and features a line graph showing 'units' over time. The graph has three data series: 'vmcount' (blue line), 'health_issues' (green line), and 'config_issues' (orange line). A tooltip for Monday, Jun, 25 - 6:08 PM shows: vmcount: 3 units, health_issues: 0, config_issues: 3. The graph shows a constant vmcount of 3 units and zero health or config issues. Below the graph, there is a table of service status for various VMs, including 'ESX 5 A D', 'ESX 5 B D', and 'ESX 5 C D'. The table columns include 'Service Name', 'Status', 'Host', 'Last Update', and 'Details'. The footer of the dashboard shows 'Nagios XI 5.4.13' and 'Copyright © 2008-2018 Nagios Enterprises, LLC'.

3.5.12. Capacity planning

NagiosXi offre un service de « capacity planning » seulement pour la version entreprise.



Il est possible de choisir l'extrapolation, la date, le type de donnée ... et lorsque tous les paramètres sont choisis, il y a possibilité d'extraire ce graph en fichier image ou de l'ajouter sur un Dashboard



3.5.13. Autres surveillances

Plusieurs autres surveillances sont disponible seulement elles ne sont pas native dans NagiosXI il faut donc aller chercher les plugins nécessaire sur la plateforme d'échange : <https://exchange.nagios.org/>

Voici une liste de possibilités d'équipements à supervisés :

Constructeurs / Éditeurs	Services disponibles	
Baie de stockage		
Dell	<ul style="list-style-type: none"> - Supervision matérielle - Supervision des volumes 	
Netapp		
Quantum DXI		
Chassis		
Dell	En fonction des remontées de la MIB du constructeur	<ul style="list-style-type: none"> - Etat des composants - Etat des ventilateurs - Températures - Consommation électrique
HP		
IBM		
Librairie de Sauvegarde		
Scalar 1500	<ul style="list-style-type: none"> - Lecteurs LT06 - Mécanique de la robotique 	
Session		
Citrix XenApp	<ul style="list-style-type: none"> - SQL Serveur - Web Interfaces - Storefront - ZDC - Serveurs PVS - Serveurs XenApp - Consommation CPU, RAM, I/O sur les serveurs de publication XenApp - Nombre de serveurs XenApp (OK, chargés, KO) - Nombres de sessions ouvertes - Nombres de licences consommées - Etat du serveur de licence - Services Citrix (y compris service d'impression) 	
Serveur d'application		
JMX	<ul style="list-style-type: none"> - Etat de la mémoire au sein de la JVM (Heap et PermGen) - Nombre de threads - Nombre de threads Actifs - Nombre de threads bloqués - Etat des pools JDBC - Etat des pools JMS 	

JVM	<ul style="list-style-type: none"> - Consommation CPU - Mémoire du processus JVM
-----	--

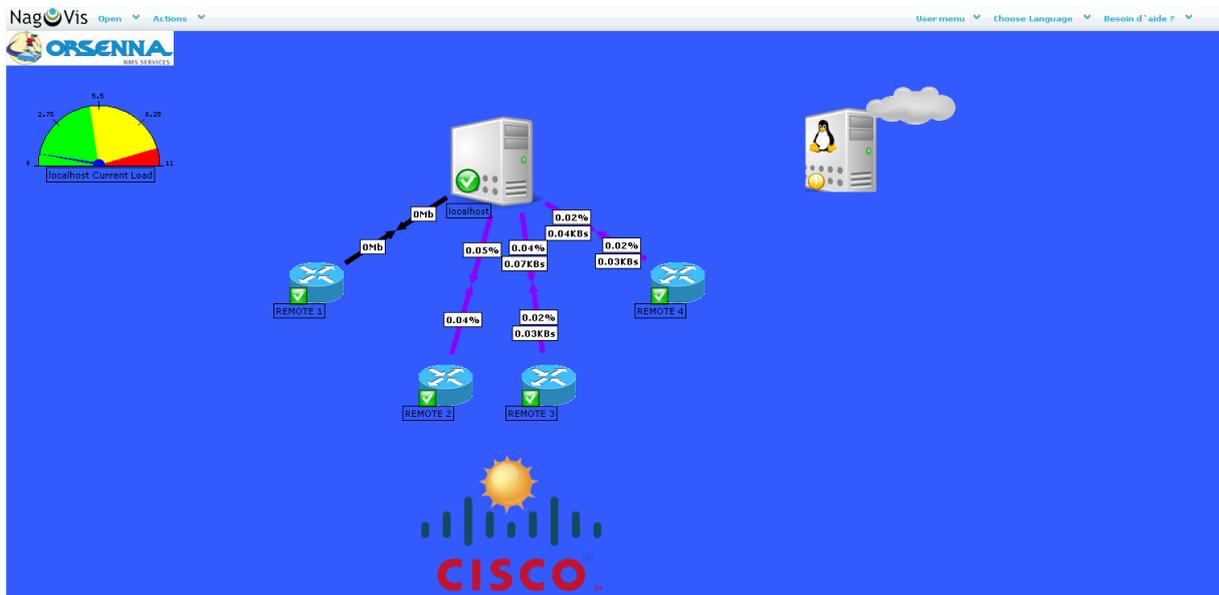
3.5.14. Cartographie, Views et Dashboard.

Cartographie :

Seule une carte automatique est disponible sur la console de Nagios. La cartographie des différents éléments de Nagios XI se fait donc via un logiciel indépendant: Nagvis. Les différentes cartes pourront tout de même être incorporées à la console grâce à l'outil 'views'.

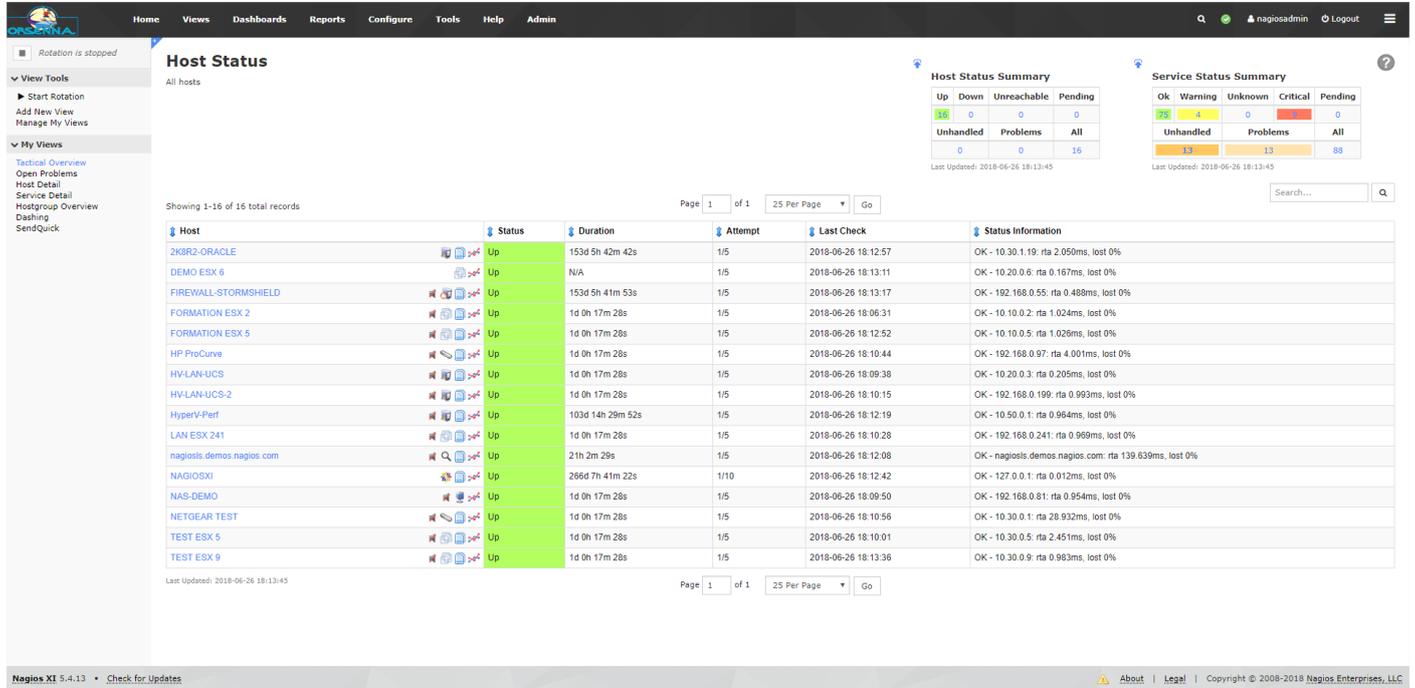
Il y a possibilité d'avoir une météo des services ainsi que d'avoir une map à l'effigie de l'entreprise. Nagvis est entièrement configurable via l'interface web.

Exemple de carte



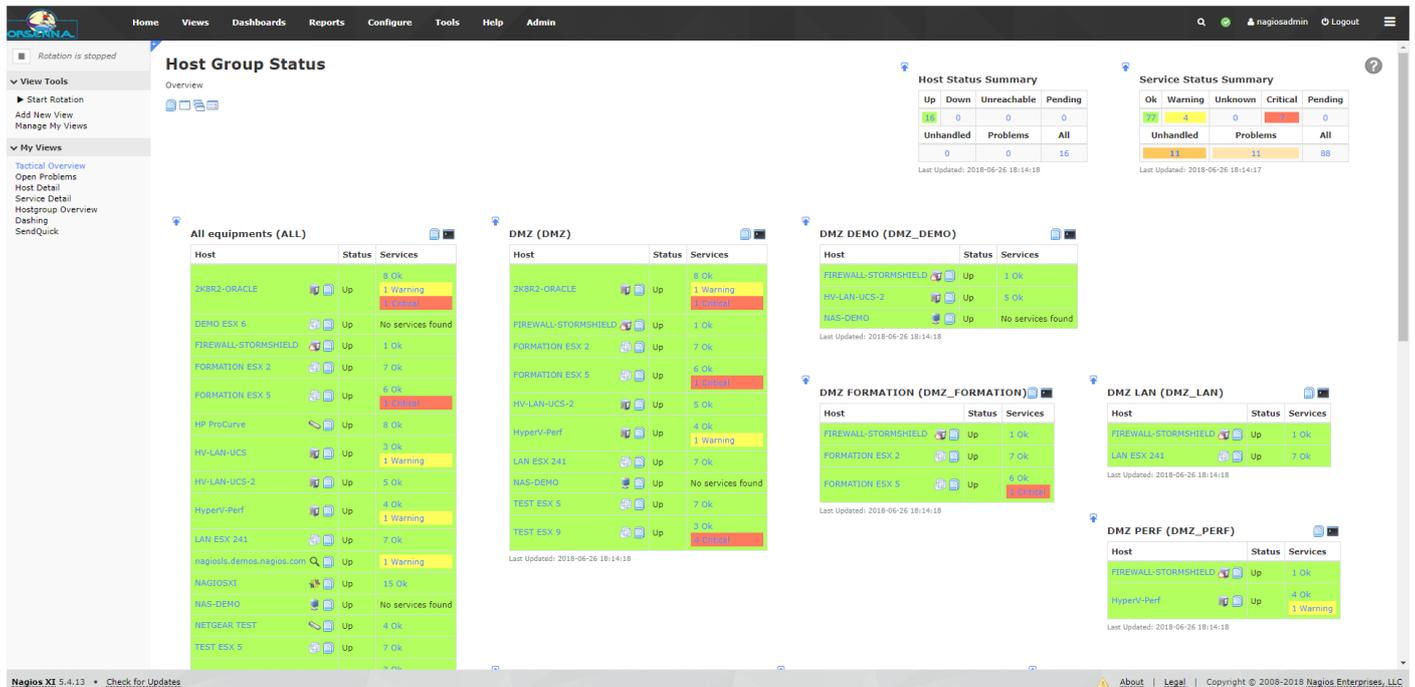
par emplacement géographique, les vues permettant l'intégration de carte Google Map. Ces vues peuvent contenir des tableaux, des graphes ou bien des cartes.

Exemple de vue



The screenshot shows the Nagios XI interface for the 'Host Status' view. It features a navigation menu on the left, a main content area with a table of host records, and summary panels on the right. The table lists various hosts such as '2KBR2-ORACLE', 'DEMO ESX 6', and 'FIREWALL-STORMSHIELD', along with their status (Up), duration, attempt count, last check time, and status information. Summary panels provide a quick overview of host counts for different states like Up, Down, Unreachable, and Pending.

Vue par groupe

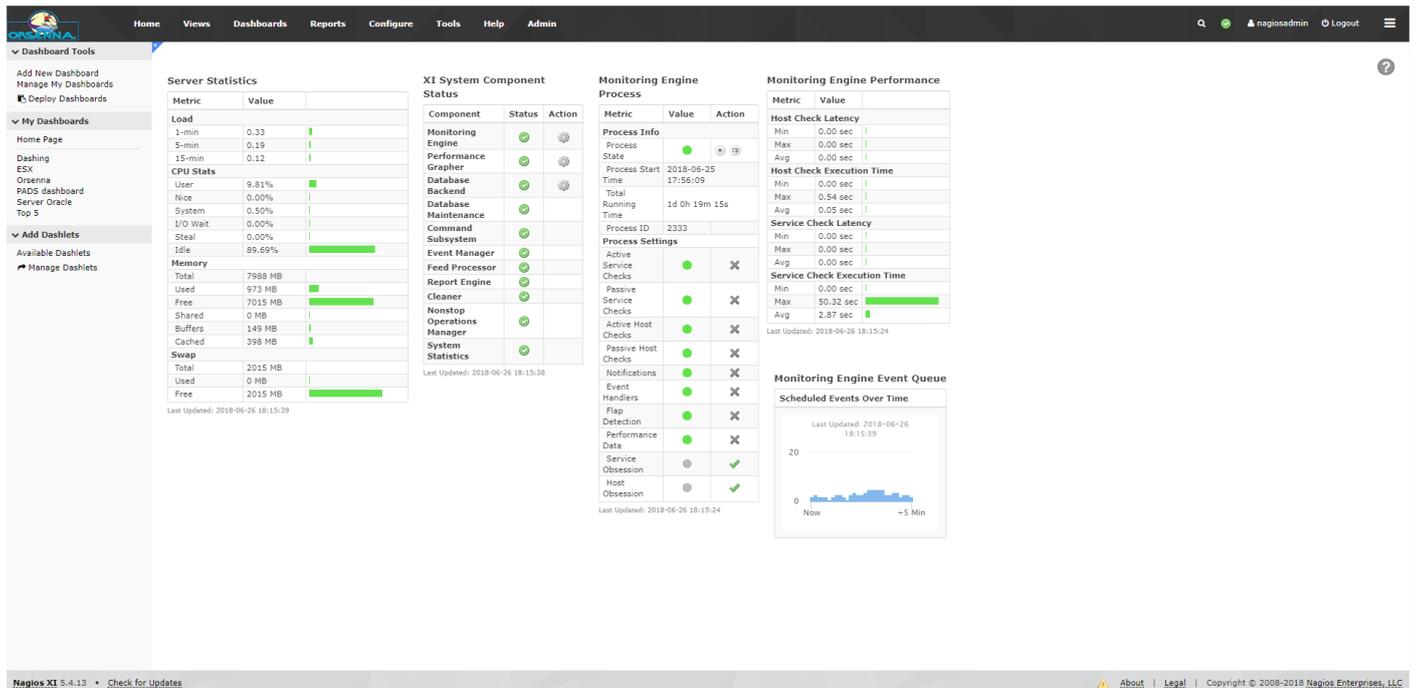


The screenshot displays the 'Host Group Status' view in Nagios XI. It provides an overview of host groups, with each group having its own detailed status table. The groups shown include 'All equipments (ALL)', 'DMZ (DMZ)', 'DMZ DEMO (DMZ_DEMO)', 'DMZ FORMATION (DMZ_FORMATION)', 'DMZ LAN (DMZ_LAN)', and 'DMZ PERF (DMZ_PERF)'. Each group's table lists the host name, its status, and the status of its services. Summary panels on the right offer a consolidated view of the overall host group health.

Dashboard :

Nagios XI permet de créer des tableaux de bords personnalisés d'exploitation et offre de nombreuses possibilités de configuration.

Exemple de dashboard :



The screenshot displays the Nagios XI dashboard interface. The top navigation bar includes Home, Views, Dashboards, Reports, Configure, Tools, Help, and Admin. The dashboard is divided into several sections:

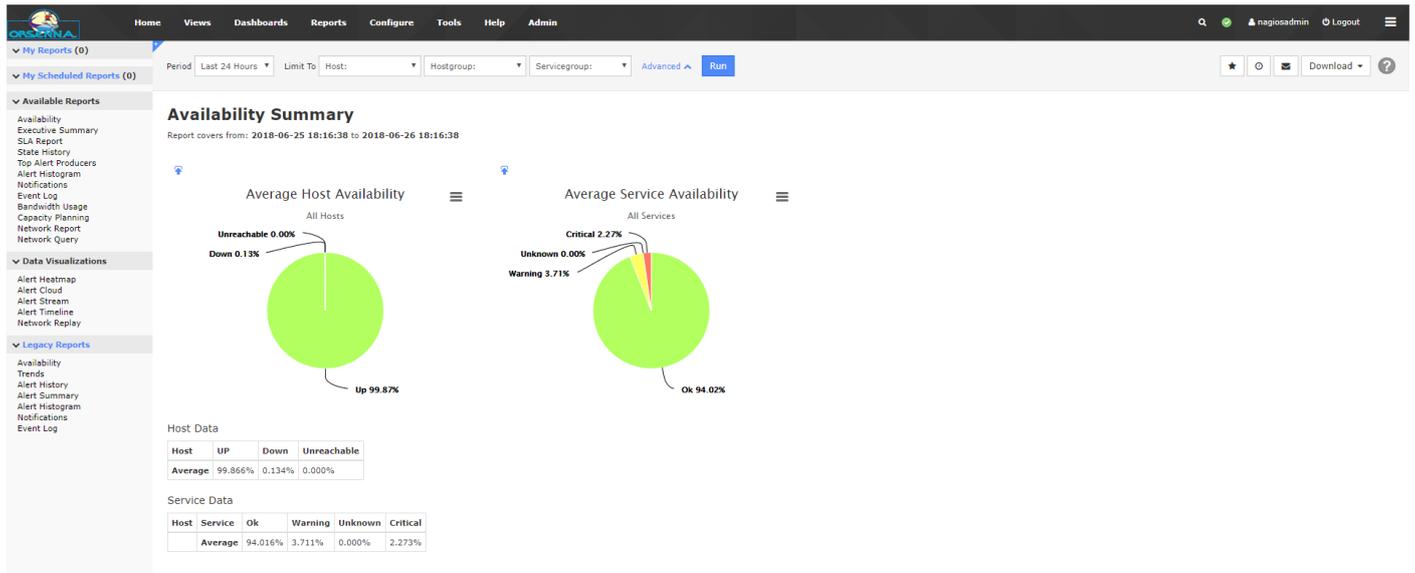
- Server Statistics:** A table showing metrics for Load (1-min, 5-min, 15-min), CPU Stats (User, Nice, System, I/O Wait, Steal, Idle), Memory (Total, Used, Free, Shared, Buffers, Cached, Swap), and Swap (Total, Used, Free). Each metric includes a value and a progress bar.
- XI System Component Status:** A table listing various system components (Monitoring Engine, Performance Grapher, Database Backend, Database Maintenance, Command Subsystem, Event Manager, Feed Processor, Report Engine, Cleaner, Nonstop Operations Manager, System Statistics) with their status (green checkmark) and an action icon.
- Monitoring Engine:** A table showing process information (State, Process Start, Time, Total Running Time, Process ID) and process settings (Active, Passive, Service Checks, Active Host Checks, Passive Host Checks, Notifications, Event Handlers, Flap Detection, Performance Data, Service Obsession, Host Obsession) with their status (green checkmark or red X).
- Monitoring Engine Performance:** A table showing performance metrics for Host Check Latency, Host Check Execution Time, Service Check Latency, and Service Check Execution Time, including Min, Max, and Avg values.
- Monitoring Engine Event Queue:** A section titled "Scheduled Events Over Time" with a small bar chart showing event frequency over a 5-minute period.

The footer of the dashboard includes "Nagios XI 5.4.13 • Check for Updates" and "About | Legal | Copyright © 2008-2018 Nagios Enterprises, LLC".

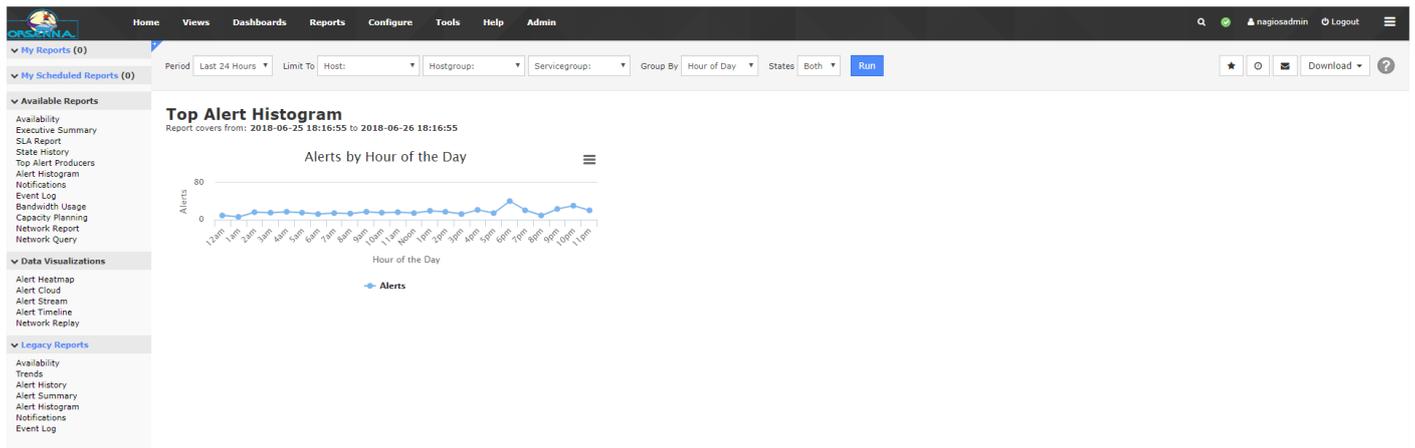
3.5.15. Rapports

Des rapports de performances sur les indicateurs sont disponibles et permettent de disposer des historiques de valeurs collectées. Aucun rapport sur les modifications apportées par les utilisateurs sur Nagios XI. Les rapports sont actualisés automatiquement lors de modifications sur les groupes.

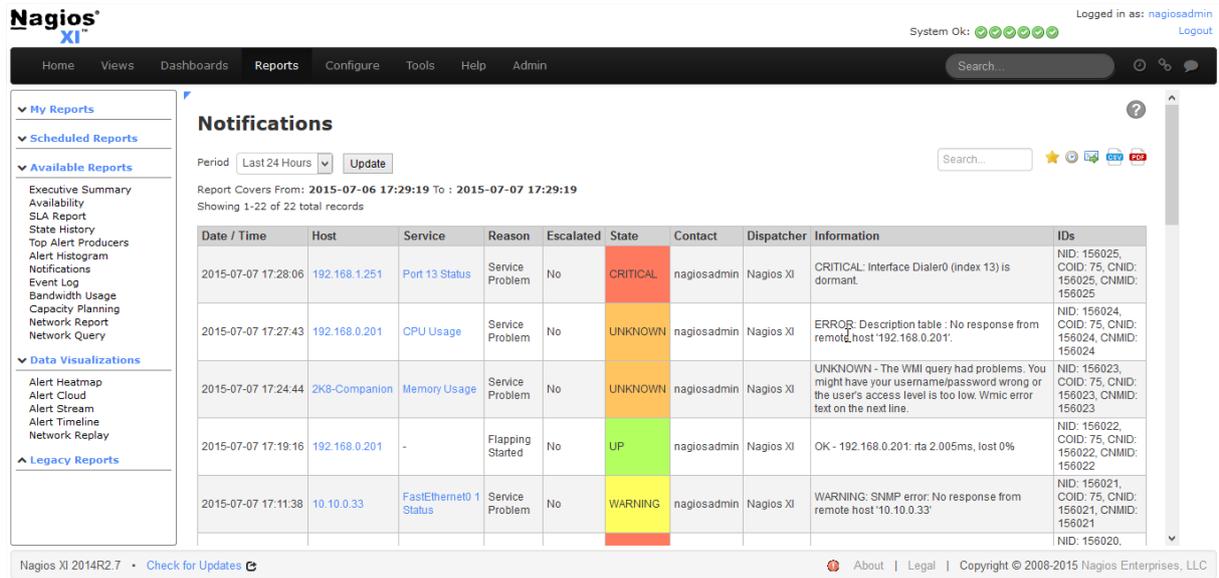
Rapports sur la disponibilité des hôtes et services :



Journal d'alertes :



Notifications :



The screenshot shows the Nagios XI interface with the 'Notifications' page selected. The page displays a table of recent alerts for the period of 2015-07-06 17:29:19 to 2015-07-07 17:29:19. The table includes columns for Date/Time, Host, Service, Reason, Escalated, State, Contact, Dispatcher, Information, and IDs. The states shown are CRITICAL, UNKNOWN, UP, and WARNING.

Date / Time	Host	Service	Reason	Escalated	State	Contact	Dispatcher	Information	IDs
2015-07-07 17:28:06	192.168.1.251	Port 13 Status	Service Problem	No	CRITICAL	nagiosadmin	Nagios XI	CRITICAL: Interface Dialer0 (index 13) is dormant.	NID: 156025, COID: 75, CNID: 156025, CNMID: 156025
2015-07-07 17:27:43	192.168.0.201	CPU Usage	Service Problem	No	UNKNOWN	nagiosadmin	Nagios XI	ERROR: Description table : No response from remote host '192.168.0.201'.	NID: 156024, COID: 75, CNID: 156024, CNMID: 156024
2015-07-07 17:24:44	2K8-Companion	Memory Usage	Service Problem	No	UNKNOWN	nagiosadmin	Nagios XI	UNKNOWN - The WMI query had problems. You might have your username/password wrong or the user's access level is too low. Wmic error text on the next line.	NID: 156023, COID: 75, CNID: 156023, CNMID: 156023
2015-07-07 17:19:16	192.168.0.201	-	Flapping Started	No	UP	nagiosadmin	Nagios XI	OK - 192.168.0.201: rta 2.005ms, lost 0%	NID: 156022, COID: 75, CNID: 156022, CNMID: 156022
2015-07-07 17:11:38	10.10.0.33	FastEthernet0/1 Status	Service Problem	No	WARNING	nagiosadmin	Nagios XI	WARNING: SNMP error: No response from remote host '10.10.0.33'	NID: 156021, COID: 75, CNID: 156021, CNMID: 156021

Tous les rapports peuvent être mis en favoris, ou bien exportés aux formats CSV ou PDF.

3.5.16. Authentication LDAP

Nagios XI peut importer les comptes utilisateurs LDAP qui ont été créés sur les serveurs d'authentification.

LDAP / Active Directory Integration Configuration

LDAP/AD Authentication Servers

Authentication servers can be used to authenticate users over on login. Once a server has been added you can [import users](#).

[Add Authentication Server](#)

Server(s)	Type	Encryption	Associated Users	Actions
There are currently no LDAP or AD servers to authenticate against.				

Certificate Authority Management

For connecting over SSL/TLS using self-signed certificates you will need to add the certificate(s) of the domain controller(s) to the local certificate authority so they are trusted. If any certificate was signed by a host other than itself, that certificate authority/host certificate needs to be added.

[Add Certificate](#)

Hostname	Issuer (CA)	Expires On	Actions
You have not added any CA certificates through the web interface			

Authentication Server Settings

Enable this authentication server

Connection Method: Active Directory
Use either LDAP or Active Directory settings to connect.

Base DN:
The LDAP-format starting object (distinguished name) that your users are defined below, such as **DC=nagios,DC=com**.

Account Suffix:
The part of the full user identification after the username, such as **@nagios.com**.

Domain Controllers:
A comma-separated list of domain controllers on your network.

Security: None
The type of security (if any) to use for the connection to the server(s).

[Save Server](#) [Cancel](#)

3.5.17. Core Config Manager

Le core config manager permet de monitorer manuellement les équipements, les contacts, etc.

Dans cette partie, Nagios XI nous permet de réaliser des migrations de configuration d'un autre Nagios XI ou d'un Nagios d'une version plus ancienne, de créer des groupes d'équipements, des groupes de services qui sont modifiables à tout instant par l'utilisateur (Groupe Dynamique).

CCM Core Config Manager

- Quick Tools
 - Core Config Manager
 - Apply Configuration
 - Configuration Snapshots
 - Monitoring Plugins
 - Configuration Wizards
- Monitoring
 - Hosts
 - Services
 - Host Groups
 - Service Groups
- Alerting
 - Contacts
 - Contact Groups
 - Time Periods
 - Host Escalations
 - Service Escalations
- Templates
- Commands
- Advanced
- Tools
- CCM Admin

CCM Object Summary

2 Hosts	2 Host Groups
14 Services	0 Service Groups
1 Contacts	2 Contact Groups
128 Commands	0 Host Dependencies
0 Service Dependencies	

Recent Snapshots

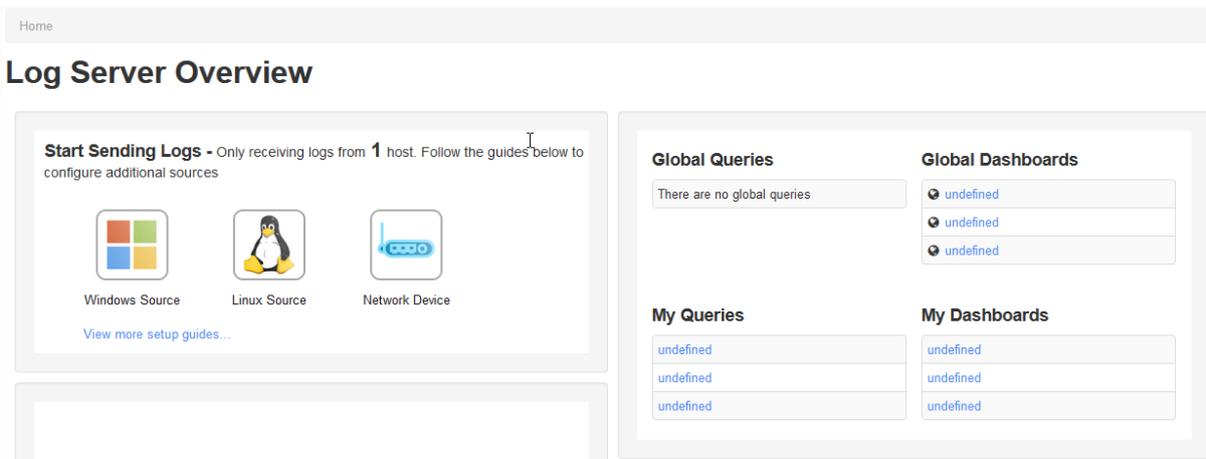
Date	Snapshot Result	Actions
2017-06-29 10:40:05	Config Ok	  
2017-06-28 10:39:03	Config Ok	  
2017-06-27 10:38:04	Config Ok	  
2017-06-26 17:35:41	Config Ok	  
2017-06-26 17:34:44	Config Ok	  
2017-06-26 17:33:24	Config Ok	  
2017-06-26 10:37:07	Config Ok	  
2017-04-25 22:25:09	Config Ok	  

3.6. Complément Gestion de logs

Nagios Log Server permet de réaliser la collecte d'évènements via des agents pour :

- Les serveurs Linux
- Les serveurs Windows
- Les logs spécifiques Apache / IIS

Les logs Traps SNMP et Syslog peuvent être collectés directement depuis le serveur également.



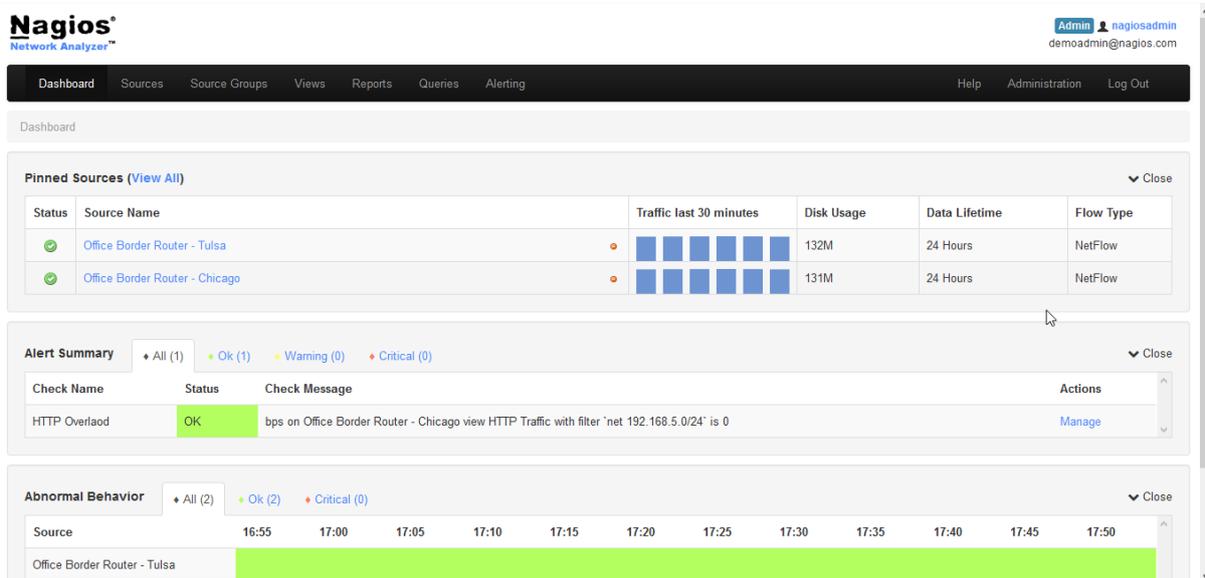
Des tableaux de bords dédiés sont ensuite proposés, ainsi qu'un mécanisme de détection de logs critiques et un système d'alerting.

Les filtres peuvent ensuite être interfacés avec NagiosXI.



3.7. Complément NetFlow

Un analyseur NetFlow est également intégré dans la console de supervision NagiosXI. Les tableaux de bords dédiés permettront d'identifier les applications, protocoles et adresses IP les plus consommatrices en termes de bandes passantes.



Nagios Network Analyzer | Admin | nagiosadmin | demoadmin@nagios.com

Dashboard | Sources | Source Groups | Views | Reports | Queries | Alerting | Help | Administration | Log Out

Dashboard

Pinned Sources (View All) | Close

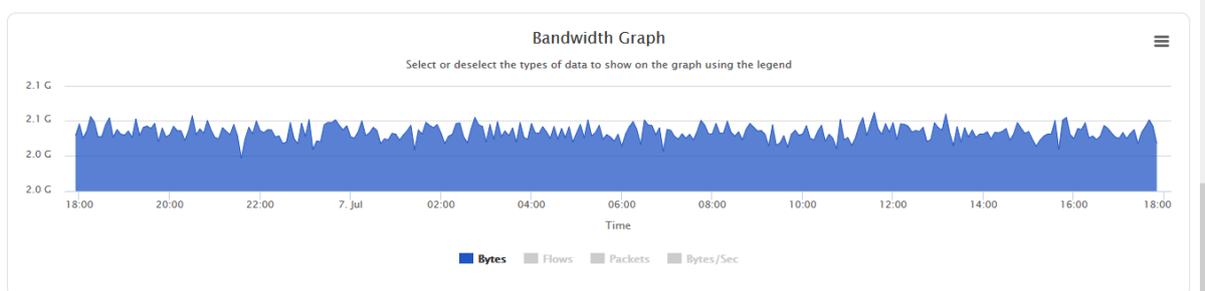
Status	Source Name	Traffic last 30 minutes	Disk Usage	Data Lifetime	Flow Type
OK	Office Border Router - Tulsa		132M	24 Hours	NetFlow
OK	Office Border Router - Chicago		131M	24 Hours	NetFlow

Alert Summary | All (1) | Ok (1) | Warning (0) | Critical (0) | Close

Check Name	Status	Check Message	Actions
HTTP Overload	OK	bps on Office Border Router - Chicago view HTTP Traffic with filter 'net 192.168.5.0/24' is 0	Manage

Abnormal Behavior | All (2) | Ok (2) | Critical (0) | Close

Source	16:55	17:00	17:05	17:10	17:15	17:20	17:25	17:30	17:35	17:40	17:45	17:50
Office Border Router - Tulsa												



Top 5 Talkers

Destination IP	% Bytes	Source IP	% Bytes	Dest. Port	% Bytes	Src. Port	% Bytes
192.168.1.223	0.4	172.12.3.47	0.4	80	40.4	31131	0.5
192.168.1.118	0.4	172.12.3.170	0.4	22	10.1	31060	0.5
192.168.1.193	0.4	172.12.3.104	0.4	53	5.1	31165	0.5
192.168.1.54	0.4	172.12.3.187	0.4	139	5.1	31127	0.5
192.168.1.125	0.4	172.12.3.95	0.4	3306	5.1	31090	0.5

3.8. Options : Appliance SMS

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

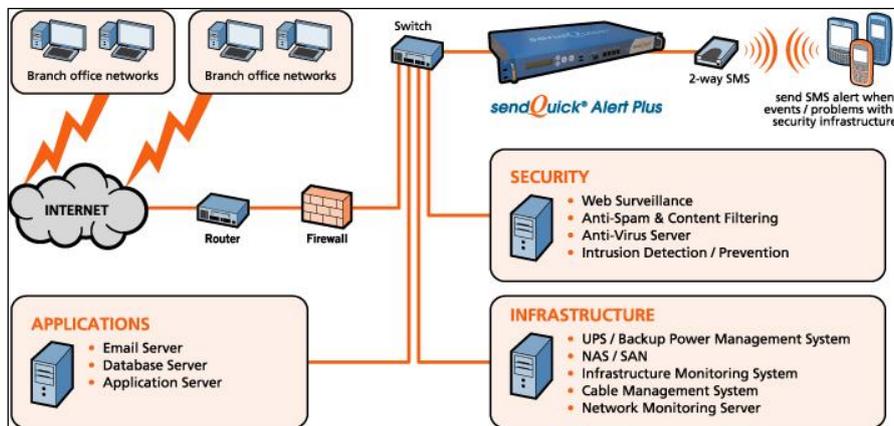
Ces appliances permettent de diffuser des SMS à partir d'un envoi d'email, d'envoi de traps SNMP ou de messages SYSLOG.

3.8.1. SendQuick – Talariax

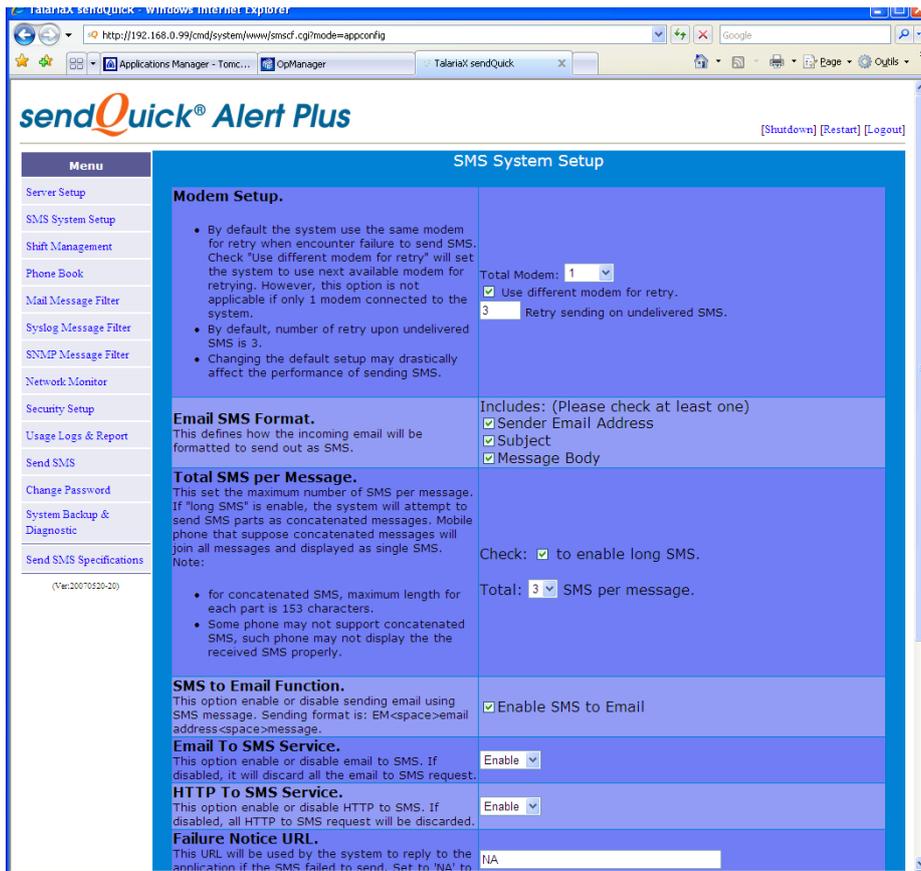
Cette appliance sous Linux dispose de nombreuses fonctionnalités :

- Gestion d'un planning d'astreinte
- Annuaire
- 4 ports réseaux indépendants (Gestion de DMZ)
- Gestion des acquittements
- Mode multi opérateur

Architecture Appliance SMS



Interface appliance



3.8.2. SMSEagle – SMSEAGLE

Cette appliance est plus basique et permet de disposer d'un modem GSM disposant de fonctions évoluées.



Interface appliance



3.9. Option : MiniFlowProbe

La sonde MiniFlowProbe est un Agent Netflow installé sur un mini PC, celle-ci peut être configurée et utilisée avec collecteur (WhatsUp Gold, ORION, PRTG, NagiosXI, FlowMon, Scrutinizer, ...)

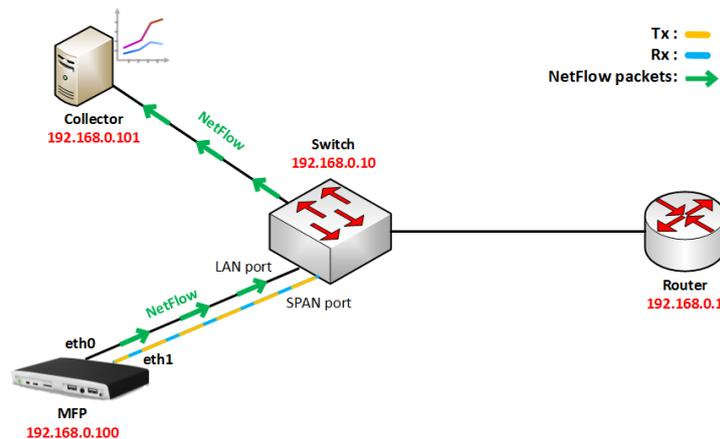
Les avantages principaux du MiniFlowProbe sont :

- Faible coût,
- Appliance petite et compacte,
- Simple et rapide :
 - Gigabit Ethernet ports x 2
 - µSD card 8 GB
 - Dual Core 1 GHz CPU
 - 2 GB RAM

MiniFlowProbe appliance



Architecture Appliance MiniFlowProbe



4. Conclusion

4.1. Bilan

4.1.1. Bilan Analyse

Afin de mettre en place une surveillance principalement non intrusive basée essentiellement sur du polling et sur la réception d'évènements on peut analyser les besoin comme suit :

- Polling SNMP
- Réception de traps SNMP
- Polling NRPE
- Polling WMI

4.1.2. Bilan logiciel

Le logiciel de base est constitué par la console Nagios XI et des plugins associés (en option). Dans le cadre d'un projet, on prévoit de disposer des outils complémentaires suivant :

- Nagvis (cartographie).

4.2. Pré-requis Environnement Serveur

4.2.1. Recommandations éditeur

L'environnement recommandé par l'éditeur Nagios est :

- RedHat 6.0 32 bits ou plus, ou CentOS 6.0 32 bits ou plus
- Machine avec processeur de 2 GHz, 2 GB RAM, 32 GB HD, Raid 5 Drive Configuration

4.2.2. Recommandations Orsenna

L'environnement recommandé est un serveur CentOS 6.3 avec 2 processeurs et 2 G de RAM.

Cet environnement supportera les logiciels installés : Nagios XI et ses plugins.

La machine NagiosXI peut être virtualisée, soit sous environnement VMware ou Windows. Nagios XI est disponible en téléchargement au format VMware Workstation convertible pour ESX, ainsi qu'au format Windows Virtual PC, Virtual Server. Cette machine n'a toutefois pas été validée pour Windows Hyper-V. Il est toutefois possible d'installer NagiosXI sous Hyper-V, en virtualisant un serveur CentOS 6.3, et en installant les sources NagiosXI manuellement.

4.2.3. Environnement de supervision

Afin de mettre en place les paramètres à superviser, il est nécessaire au préalable de disposer d'un accès sur l'ensemble des équipements sur la base des éléments suivants :

- Accès SNMP en lecture sur les équipements
- Accès SSH sur les environnements Linux
- Création d'un compte de supervision sous Windows (accès WMI)
- Création d'une boîte aux lettres destinée à la supervision (Tests email)
- Accès SSH sur les appliances (FW, ..)
- Comptes d'accès aux bases de données

5. Mise en œuvre – Mode Projet

Dans le cadre de la mise en œuvre nous proposons une mise en place de la solution sur 3 modes distincts :

- **Mode Projet** - planning de travail classique
- Mode Assistance - prestation de mise en œuvre et transfert de compétence.
- Mode POC (Proof Of Concept) – Maquette spécifique

Ce chapitre décrit les modalités du mode projet

Afin de présenter le déroulement d'un mode projet nous décrivons une mise en place classique de la solution de supervision sur la base d'un planning de travail suivant :

5.1. Présentation de la démarche méthodologique pour la réalisation de la prestation

La mise en œuvre du projet comprend les phases suivantes :

- Phase 1 : Initialisation du projet,
- Phase 2 : Spécifications Générales,
- Phase 3 : Spécifications détaillées et Conception,
- Phase 4 : Maquette,
- Phase 5 : Mise en œuvre
- Phase 6 : Recettes et Pré-production
- Phase 7 : Formation et Transfert de Compétences.

5.2. Phase 1 : Initialisation du projet

5.2.1. Description

La première phase du projet est une **phase d'initialisation**, qui est une phase de prévision et d'organisation de l'ensemble des actions à mener pendant le déroulement du projet pour atteindre les objectifs assignés. Il s'agit essentiellement de définir et mettre en place les moyens nécessaires, en particulier définir :

- Le rôle des participants du groupe de projet devant intervenir au cours de la phase,
- Les modalités de travail,
- Les objectifs poursuivis,
- Les moyens matériels et logiciels nécessaires au maquetage - prototypage.

Cette étape, importante pour cadrer le projet, sera réalisée en partie sous la forme d'une réunion de lancement prévue au démarrage des travaux.

Tâches

- Définition de l'équipe projet : les différents intervenants, leurs rôles et responsabilités,
- Déterminer le mode de communication pendant le déroulement du projet,
- Planning,
- Préciser les trames des livrables,
- Préciser le mode de fonctionnement avec le client et les règles d'arbitrage,
- Détailler finement le planning du projet et positionner les différents jalons,
- Répartir les tâches par collaborateur,
- Préciser les normes et méthodes utilisées,

5.2.2. Points d'entrée

- Cahier des charges CLIENT,
- La Proposition Technique et Financière d'Orsenna,

5.3. Phase 2 : Spécifications Générales

5.3.1. Description

Cette phase permet d'élaborer le Dossier de Spécifications Générales (Choix de concepts) et le Document d'Architecture, selon le plan défini dans la phase précédente, comprenant :

- La confirmation du choix et la justification de l'architecture matérielle,
- La confirmation du choix des outils,
- La confirmation du choix et la justification de l'architecture logicielle,
- Le descriptif fonctionnel,

5.3.2. Points d'entrée

- Cahier des charges CLIENT,
- La Proposition Technique et Financière d'Orsenna,

5.3.3. Fournitures et revues

- Dossier de Spécifications Générales approuvé par le CLIENT,
- Document d'Architecture approuvé par le CLIENT,
- Approvisionnement des logiciels de base pour la prestation

5.4. Phase 3 : Spécifications Détaillées

5.4.1. Description

Cette phase a pour objectif de détailler et de valider le champ fonctionnel, conceptuel et technique avant passage en phase de réalisation.

Elle permet d'élaborer le document de Spécifications Détaillées comprenant :

- L'analyse fonctionnelle détaillée,
- L'architecture détaillée des logiciels et des communications,
- La liste des matériels mis en œuvre dans la surveillance
- La définition détaillée des états et valeurs attendues
- La définition des rapports attendus
- La définition de la cartographie
- La définition de l'interface Web
- Les pré-requis de déploiement (Politique SNMP, ACL,..)
- La définition du cahier de recette

5.4.2. Points d'entrée

- Cahier des charges CLIENT,
- La Proposition Technique et Financière d'Orsenna,
- Spécifications Générales
- Document d'Architecture

5.4.3. Fournitures et revues

- Dossier de Spécifications Détaillées approuvé par le CLIENT,
- Le Cahier de recettes approuvé par le CLIENT

5.5. Phase 4 : Maquette

5.5.1. Description

Cette phase permet de valider l'accès à l'environnement et la mise en place de règles de monitoring qui seront appliqués à l'ensemble du périmètre à partir d'un périmètre restreint.

Ceci permet notamment de vérifier l'accessibilité et de compléter le document spécifiant les prérequis détaillés pour le déploiement.

Le CLIENT fournit une aide pour accéder aux environnements (notamment en cas de problème technique dû aux règles de sécurité et de filtrage).

Cette phase permet de réaliser les opérations suivantes :

- Installation des composants logiciels
- Validation de l'accessibilité des composants sur site de production et compléments d'information (prérequis)
- Mise en place d'une collecte d'informations sur une dizaine d'équipements types (Routeur, Switch, Appliance, Serveur 2K3, Linux, VM, SAN)
- Mise en place des politiques de rapports
- Mise en place des politiques d'alarmes
- Mise en place d'une cartographie sur le périmètre restreint

Lors de la validation de l'accessibilité des équipements, il est possible que des points techniques restent à résoudre. Pour minimiser les temps de résolutions de ces points il est impératif de pouvoir travailler à distance sur le sujet (temps de réponse des éditeurs, tests internes,...).

5.5.2. Points d'entrée

- Cahier des charges CLIENT,
- La Proposition Technique et Financière d'Orsenna,
- Spécifications Générales
- Spécifications Détaillées
- Document d'Architecture

5.5.3. Fournitures et revues

- Mise à jour des spécifications détaillées notamment sur les pré-requis de déploiement
- Documentation d'installation (PRA), destiné aux administrateurs

5.6. Phase 5 : Mise en œuvre

5.6.1. Description

Cette phase permet en complément à la phase de maquette d'étendre la surveillance à l'ensemble des équipements. Ce déploiement est effectué en collaboration avec les équipes du client.

Les procédures d'administration et d'exploitation sont mises en œuvre à cette occasion.

Le client fournit une aide pour accéder aux environnements (notamment en cas de problème technique dû aux règles de sécurité et de filtrage).

Cette phase permet de réaliser les opérations suivantes :

- **Validation Monitoring** : Validation de l'accessibilité des équipements et des paramètres sur site de production au niveau SNMP, SSH, Telnet
- **Cartographie – Périmètre fonctionnel** : Organisation de la cartographie : cartes physiques & fonctionnelles :
- **Validation résultats** : Validation rapports, analyse des historiques et ajustement des seuils de déclenchement sur site
- Mise en place des procédures d'**exploitation** (Sauvegarde, gestion de la base)

5.6.2. Points d'entrée

- Cahier des charges CLIENT,
- La Proposition Technique et Financière d'Orsenna,
- Spécifications Générales
- Spécifications Détaillées
- Document d'Architecture

5.6.3. Fournitures et revues

- Documentation d'Exploitation, destiné aux administrateurs

5.7. Phase 6 : Recette et Pré-production

5.7.1. Description

Cette phase de recette a pour objectif de valider sur une période plus importante la mise en œuvre de la solution.

Cette phase représente l'acceptation finale de la prestation par le CLIENT.

La durée de cette phase est d'un maximum de 2 semaines.

Cette phase permet de réaliser les opérations suivantes :

- Exploitation de l'environnement de pré-production:
 - Identification des problèmes éventuels
 - Consignation des remarques et des demandes d'informations complémentaires
- Analyse de l'environnement de pré-production.
 - Consignation des problèmes éventuels
- Prise en compte des demandes d'informations complémentaires et des remarques

5.7.2. Points d'entrée

- Cahier des charges CLIENT,
- La Proposition Technique et Financière d'Orsenna,
- Spécifications Générales
- Spécifications Détaillées
- Document d'Architecture

5.7.3. Fournitures et revues

- Cahier de recettes rempli et approuvé par le CLIENT

5.8. Phase 7 Formation et transfert de compétence

Nous disposons d'un canevas standard de formation pour les utilisateurs et les Administrateurs sur l'environnement proposé.

Celui-ci inclus un plan de formation sur 3 jours qui reste néanmoins adaptable à vos besoins.

5.9. Livrables et documentation

Les livrables fournis dans le cadre du projet sont les suivants :

- Dossier de Spécifications Générales
- Document d'Architecture
- Dossier de Spécifications Détaillées,
- Le Cahier de recette
- Documentation d'installation (PRA)
- Documentation d'Exploitation

Les prestations s'effectuent en fonction des besoins dans les locaux du client ou dans les locaux d'Orsenna.

Les prestations de documentation s'effectuent systématiquement dans les locaux d'Orsenna.

6. Mise en œuvre – Mode Assistance

Dans le cadre de la mise en œuvre nous proposons une mise en place de la solution sur 3 modes distincts :

- Mode Projet - planning de travail classique
- **Mode Assistance** - prestation de mise en œuvre et transfert de compétence.
- Mode POC (Proof Of Concept) – Maquette spécifique

Ce chapitre décrit les modalités du mode assistance

En mode assistance, il est proposé de réaliser au minimum les étapes suivantes :

- Installation de l'environnement
- Mise en place des surveillances de base sur l'ensemble des équipements
- Présentation des fonctionnalités principales de l'outil
- Documentation d'installation

En complément, cette assistance peut être étendu pour :

- La prise en compte d'équipements nécessitant une surveillance spécifique
- Présentation des fonctionnalités spécifiques de l'outil (Customisation)
- Documentation d'administration, d'exploitation et d'architecture

7. Mise en œuvre – Mode POC

Dans le cadre de la mise en œuvre nous proposons une mise en place de la solution sur 3 modes distincts :

- Mode Projet - planning de travail classique
- Mode Assistance - prestation de mise en œuvre et transfert de compétence.
- **Mode POC (Proof Of Concept)** – Maquette spécifique

Ce chapitre décrit les modalités du mode POC

Le but du POC est d'intégrer les différents équipements dans le logiciel NCM, d'associer les templates à chaque type d'équipements (voir les créer s'ils n'existent pas), de créer les scripts si besoin, de scheduler les sauvegardes et surtout d'avoir une visibilité dans le logiciel des différents backup (test présence fichier reçu en ftp, test script externe, etc...)

Il est proposé de réaliser au minimum les étapes suivantes :

- Installation de l'environnement
- Mise en place d'une collecte des configurations sur les familles d'équipements listés dans le POC
- Réalisation des scripts et templates spécifiques
- Présentation des fonctionnalités principales de l'outil

En complément, cette assistance peut être étendu pour :

- La prise en compte d'autres équipements nécessitant un modèle spécifique
- Documentation d'installation et d'exploitation

8. Charges

8.1. Tableau de charge de travail - Mode Projet

Ce mode est le mode choisi dans le cadre de la proposition.

Phase	Tâche	Charge de travail	Détails de la tâche
1- Initialisation	Réunion de lancement	0,5J	Réunion lancement du projet avec CLIENT
2 -3 Spécifications	Documentation	1J	Doc d'Architecture 0,25J Doc Spécifications Détaillés 0,75J
4 -5 Maquette & Mise en œuvre	Intégration des équipements dans Nagios XI	2J-3J	Création des Equipements Création des Monitors
4 -5 Maquette & Mise en œuvre	Cartographie	1J	Création des Cartes (Siège, Agences)
4 -5 Maquette & Mise en œuvre	Politiques d'alerte, Actions, Interface Web	1,5J	Création des actions, définition des informations envoyées Création des politiques d'action Customisation de l'interface Web Gestion des vues
4 -5 Maquette & Mise en œuvre	Passive Monitors	1 J	Définition des Traps à traiter Corrélation des évènements
4 -5 Maquette & Mise en œuvre	Documentation	2 J	Doc d'Installation 0,5J Doc d'Exploitation 1J Cahier de recette 0,5J
6 – Recette & Pré-production	Validation et mise en œuvre des remarques	1 J	
	Formation	2 J	Formation Nagios XI
	Total	12-13 J	

La charge de travail estimée classique est donc de 12 à 13 jours dont 2 jours de formation.

8.2. Charges – Mode Assistance

La charge d'assistance initiale est la suivante :

Phase	Tâche	Charge de travail	Détails de la tâche
Initialisation	Réunion de lancement, vérification de la mise en œuvre des prérequis (SNMP, WMI, SSH)	0,5J	Réunion et validation technique
Maquette & Mise en œuvre	Intégration des équipements dans Nagios XI	2J – 3J	Création des Equipements Création des Monitors
Maquette & Mise en œuvre	Cartographie Politiques d'alerte, Actions, Interface Web	1,5J-	Création des Cartes Création des actions, définition des informations envoyées Création des politiques d'action Customisation de l'interface Web Gestion des vues
Maquette & Mise en œuvre	Gestions journaux & Passive Monitors & Rapports	1 J	Définition des Traps à traiter, compléments , rapports
Maquette & Mise en œuvre	Compléments Plugins	1 J	Mise en œuvre WhatsUp Companion et plugins associés
Maquette & Mise en œuvre	Documentation	0,5 J	Doc d'Installation 0,5J
Recette & Pré-production	Validation et mise en œuvre des remarques	0,5 J	
	Total	7J - 8J	

8.3. Charges – Mode POC

La charge est la suivante :

Tâche	Charge de travail	Détails de la tâche
Installation de l'environnement Et pré requis initiaux	0,5 J	
Mise en place des équipements	2 J	Intégration Equipements
Ajustement pré-requis	1 J	SNMP, WMI, SSH
Intégration détaillés d'équipements - Utilisation de l'ensemble des plugins	1,5 J	Intégration autres équipements et fonctionnalités complémentaires
Intégration fonctionnalités de base	1 J	Création des politiques d'alertes Customisation de l'interface Web Ajustement
OPTION : Documentation	2 J	Doc d'Installation & Doc d'Exploitation
Total sans option	6 J	

9. Prestations complémentaires

9.1. Maintenance

Une prestation de maintenance est assurée par Orsenna sur les bases suivantes :

- Hotline téléphonique et email 08h30-18h30 (Jours ouvrés) (Un maximum de 10 incidents)
- Veille technologique sur les composants logiciels,
- Relais auprès des supports techniques des éditeurs,
- Aide à l'installation des mises à jour logicielles.
- Intervention préventive sur site de 1 jour/an

L'objectif des interventions préventives est, notamment, de valider les évolutions de la plateforme, d'analyser les bases de données d'évènements et d'assurer tout conseil sur une problématique cliente.

Cette prestation est effectuée sur la base d'une enveloppe budgétaire de 2 Hommes/jours.

9.2. Assistance, expertise et formation

Des prestations complémentaires d'assistance, d'expertise ou de formation peuvent être mises en place sur demande de la société CLIENT.

10. Conclusion

Notre proposition s'appuie sur les points forts suivants :

- Connaissance du marché de la supervision
- Forte expérience de mise en œuvre de solutions
- Une expertise reconnue par les éditeurs et intégrateurs
- Une capacité de développement
- Indépendance vis-à-vis des éditeurs