Retour d'expérience sur Nagios 3

Christophe Sahut <christophe.sahut@sgs.com>

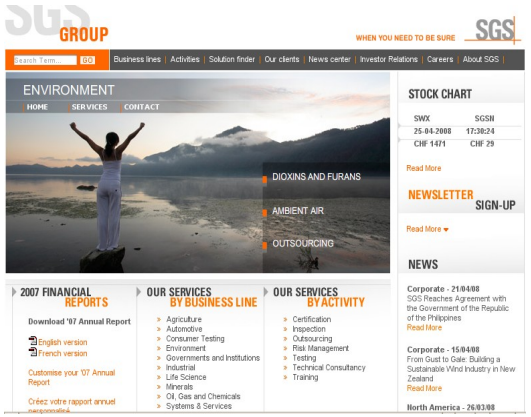
WHEN YOU NEED TO BE SURE

SGS

Introduction

- SGS : Société Générale de Surveillance
  - Activités

    Inspection,verification,test,certification
  - Clients
  - IT à la SGS



- Pourquoi cette présentation

Présentation du contexte

Contexte

- Historique de la supervision à la SGS
  - Big Brother
  - Nagios 2.x
  - Nagios 3.x

Contexte

- Plateforme utilisée : Hardware
  - VMWare ESX en cluster HA
  - Machine virtuelle
    - 2 CPU Xeon 2.66Ghz
    - 512MB de RAM

pour ~ 270 hosts et 1200 services

Contexte

- Plateforme utilisée : Software
  - RedHat EL (4&5)
  - RPMs Nagios (SGS)
  - PNP4nagios

Contexte

- Environnement à monitorer
  - Serveurs
    - Linux, Windows, VMware
  - Routeurs, switchs
  - Filers NetAPP, load balancers BigIP
  - Beaucoup d'applications

Installation et Administration de Nagios

Installation

- Serveur Nagios
  - RPM vs Sources : RPMs
- Scripts de réinstallation : « Disaster Recovery »
  - Réinstallation d'un OS standard
  - Application d'un script
  - Nagios « up and running »

Administration

- Avec rpm/yum tout simplement
  - Mise à jour via miroir local
- Etant sur une plateforme ESX, on profite des snapshots
  - Retour en arrière très simple en cas de gros problème (?)

Configuration

- Plusieurs méthodes :
  - Fichier texte
    - Beaucoup de manières de s'organiser !
  - Interface graphiques
    - Fruity
    - Monarch
    - Centreon
    - ...

Configuration

- Notre choix : par fichier texte : K.I.S.S.
  - Facile à modifier (bash/vim/sed/awk...)
  - Facile à backuper
  - Facile à restaurer
- Example :

  - Génération automatique avec Vim

Configuration

- Configuration de Nagios
  - Avantages : très flexible
  - Inconvénients : très flexible
- La configuration peut être très simple comme très compliquée

Configuration

- Configuration classique
  - Définition d'un host
  - Définition de services, appliqué à ce host
  - Définition de contactgroups pour ce host et ses services
    - Exemple : configuration par défaut
- Difficile à maintenir à grande echelle
- Nagios 3 apporte beaucoup de facilités

Configuration

- Nos choix (Nagios 3) :
  - Utilisation massive de « templates » imbriqués
    - Pour les machines
    - Pour les services
    - Pour les contacts
  - Utilisation massive de hostgroups
  - Exemple

SGS

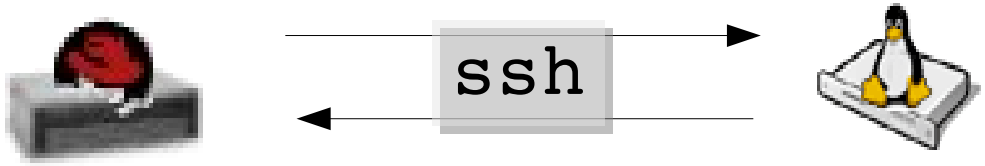
Supervision avec Nagios

Supervision Linux

- Dans notre cas, RedHat uniquement
  - On déploie les agents par ssh via un script, ce en fonction de la version de RedHat
  - Contient les « nagios-plugins » officiels
  - Tout ce qui est test spécifique est gardé dans la mesure du possible centralisé sur le serveur Nagios

Supervision Linux

- Comment : plusieurs méthodes :
  - NRPE
  - checkbyssh
  - SNMP
  - ...
- Nous n'utilisons que *checkbyssh*




```
nagios-plugins
- check_load
- check_swap
- check_disk
- ...
```

Serveur Nagios

Serveur distant

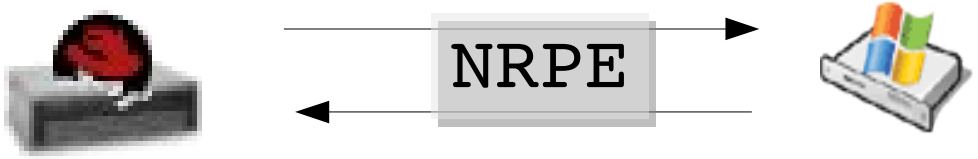
Supervision Linux

- En standard, nous monitorons :
  - Le charge du processeur
  - La mémoire (swap)
  - L'utilisation des disques

Host	Service	Status	Last Check	Duration	Attempt	Status Information
[redacted]	Disk	OK	04-16-2008 09:33:50	4d 21h 18m 8s	1/3	DISK OK - free space: / 13497 MB (21% inode=98%): /boot 70 MB (75% inode=99%): /dev/shm 3988 MB (100% inode=99%):
	Hardware	OK	04-16-2008 09:32:17	76d 15h 26m 46s	1/1	OK
	Load	OK	04-16-2008 09:31:21	54d 5h 39m 1s	1/3	OK - load average: 1.02, 1.03, 1.00
	Ping	OK	04-16-2008 09:34:22	122d 17h 53m 3s	1/3	OK - [redacted] rta 0.290ms, lost 0%
	Swap	OK	04-16-2008 09:34:31	1d 22h 15m 54s	1/3	SWAP OK - 100% free (1983 MB out of 1983 MB)
	[redacted] login	OK	04-16-2008 09:31:35	1d 11h 13m 42s	1/3	WebInject OK - All tests passed successfully in 1.235 seconds

Supervision Windows

- Nous utilisons le plugin NSClient++
  - Archive avec la configuration pour notre environnement
  - Déployé manuellement (pour l'instant)
    - Possibilité de le faire via AD
  - Service sous Windows




```
NSClient++
- CheckSystem.dll
- CheckDisk.dll
- CheckWMI.dll
- ...
```

Serveur Nagios

Serveur distant

Supervision Windows

- En standard, nous monitorons :
  - Le processeur
  - La mémoire
  - L'utilisation des disques

Host	Service	Status	Last Check	Duration	Attempt	Status Information
[redacted]	Check CPU	OK	04-16-2008 09:34:21	42d 0h 4m 30s	1/3	OK CPU Load ok.
	Check Event Log	OK	04-16-2008 09:34:54	68d 20h 54m 57s	1/3	Eventlog check ok
	Check Local Drives	OK	04-16-2008 09:30:44	33d 12h 41m 47s	1/3	OK: All drives within bounds.
	Check Memory	OK	04-16-2008 09:31:45	42d 0h 4m 30s	1/3	OK: page file: 1.29G
	HTTP	OK	04-16-2008 09:34:56	4d 16h 23m 29s	1/3	HTTP OK HTTP/1.1 200 OK - 0.247 second response time
	Hardware	OK	04-16-2008 09:34:06	76d 14h 7m 13s	1/1	OK
	Ping	OK	04-16-2008 09:34:52	13d 23h 59m 11s	1/3	OK - [redacted]: rta 2.566ms, lost 0%

Supervision Windows

- Possible :
  - Etat d'un service ou d'un processus
  - Vérification de logs
  - Taille de fichier etc...
- Non limité à NSClient++ en lui-même
  - Possibilité d'extension avec WMI/WSH/VBScript

Supervision Windows

- En évaluation :
  - Performance counters
  - Supervision de clusters Microsoft

Divers

- Exemple pour les NAS NetApp
  - Utilisation de check_netapp.pl, modifié pour nos besoins
  - Basé sur du SNMP

SNMP Traps

- Principe
  - Les équipements envoient des messages de type SNMPTrap à Nagios en cas de dysfonctionnement
  - Nagios gère les alertes et contacte les personnes conçernées
- Intérêt :
  - On évite beaucoup de trafic réseau inutile

SNMP Traps

- Cartes RSA IBM
  - On reçoit des alertes de type :
    - **Critical alerts :** Hard disk drive,Multiple fan failure,Power failure,Tamper,Temperature,Voltage,VRM failure
    - **Warning alerts :** Single fan failure, Temperature, Voltage, Redundant power supply
    - **System alerts :** Boot failure, Loader timeout, OS timeout, PFA, POST timeout, Power off, Power on, Partition Configuration, Event Log

SNMP Traps

- De nombreux équipements savent envoyer des SNMPTraps :
  - Aruba Wireless AP
  - BigIPs
  - Cisco switches (modifications de la configuration , link up, link down etc...)
  - Vmware (Etat des machines (powered off, powered on, pause state etc...)
  - Netapps

Supervision passive

- Principe : « push » des résultats des tests au lieu de « pull »
- Utile pour des évènements irréguliers
  - Vérification du statut d'un backup
- Utilisation de NSCA pour ceci
  - Egalement utilisé dans des environnements distribués, ou des architectures avec firewalls

Spécifique

- Webinject : utilisation de scénario
  - Connexion sur une page web
  - Entrée d'un login
  - Réalisation de quelques opérations
  - Déconnexion
- Si tout s'est bien passé => statut OK

Notifications

- Envoi d'email 24x7 pour tout le monde
  - Possibilité de plages horaire, de rotation d'équipes « OnCall Teams »
  - Possibilité d' « Escalation process »

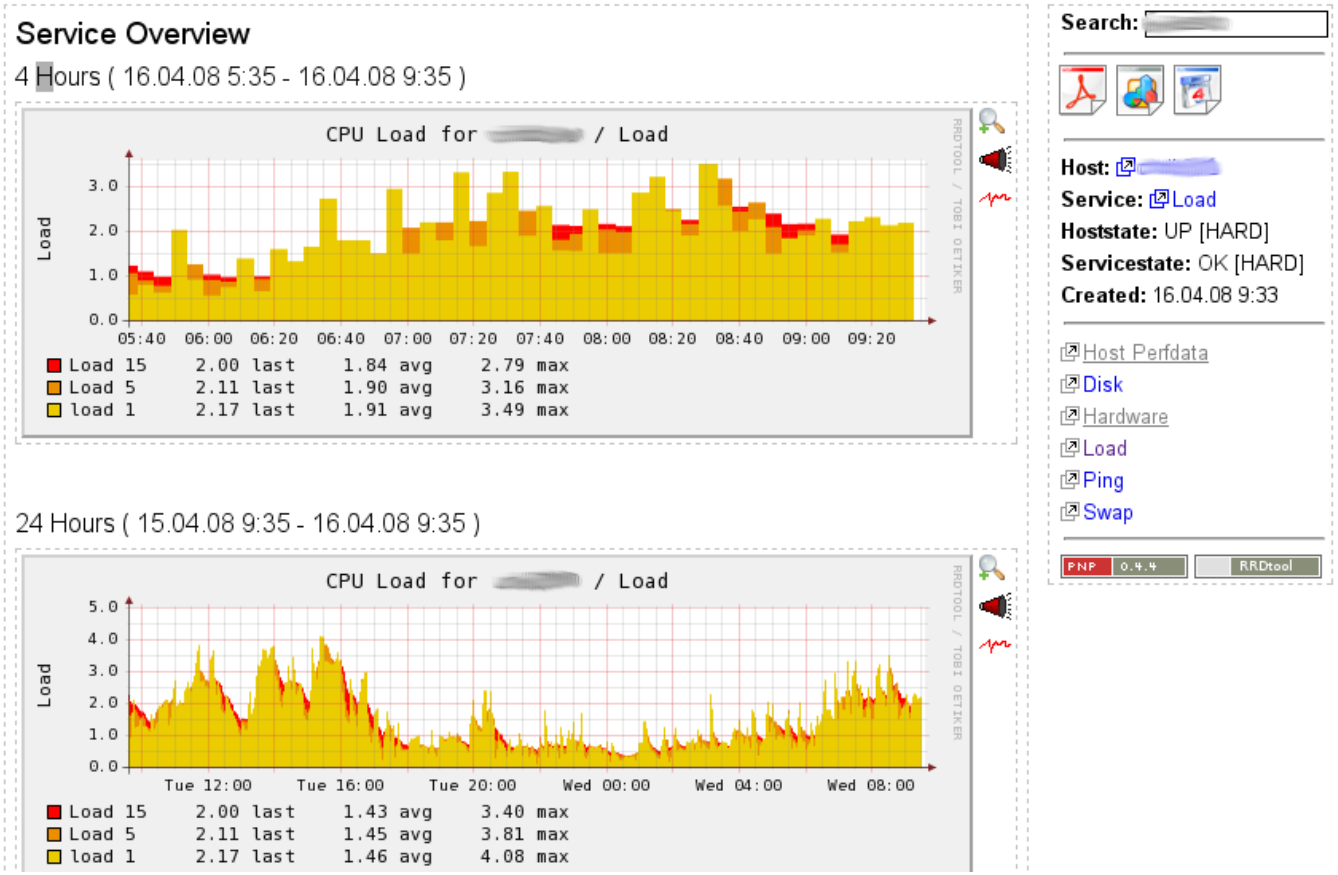
Notifications

- Et si les emails ne fonctionnent pas ?
  - Envoi de SMS si le système de messagerie est défaillant
    - Modem iTegno 3000 sous Linux avec gnokii
- Et si Nagios ne fonctionne pas ?
  - Supervision du serveur Nagios par un autre serveur Nagios

Graphes avec Nagios

Graphes

- Plusieurs solutions, une seule retenue : PNP4Nagios



Graphes

- Très simple, très peu intrusif
- Utilise les résultats de Nagios pour faire des graphes
- Utilisé uniquement pour avoir les évolutions

Graphes

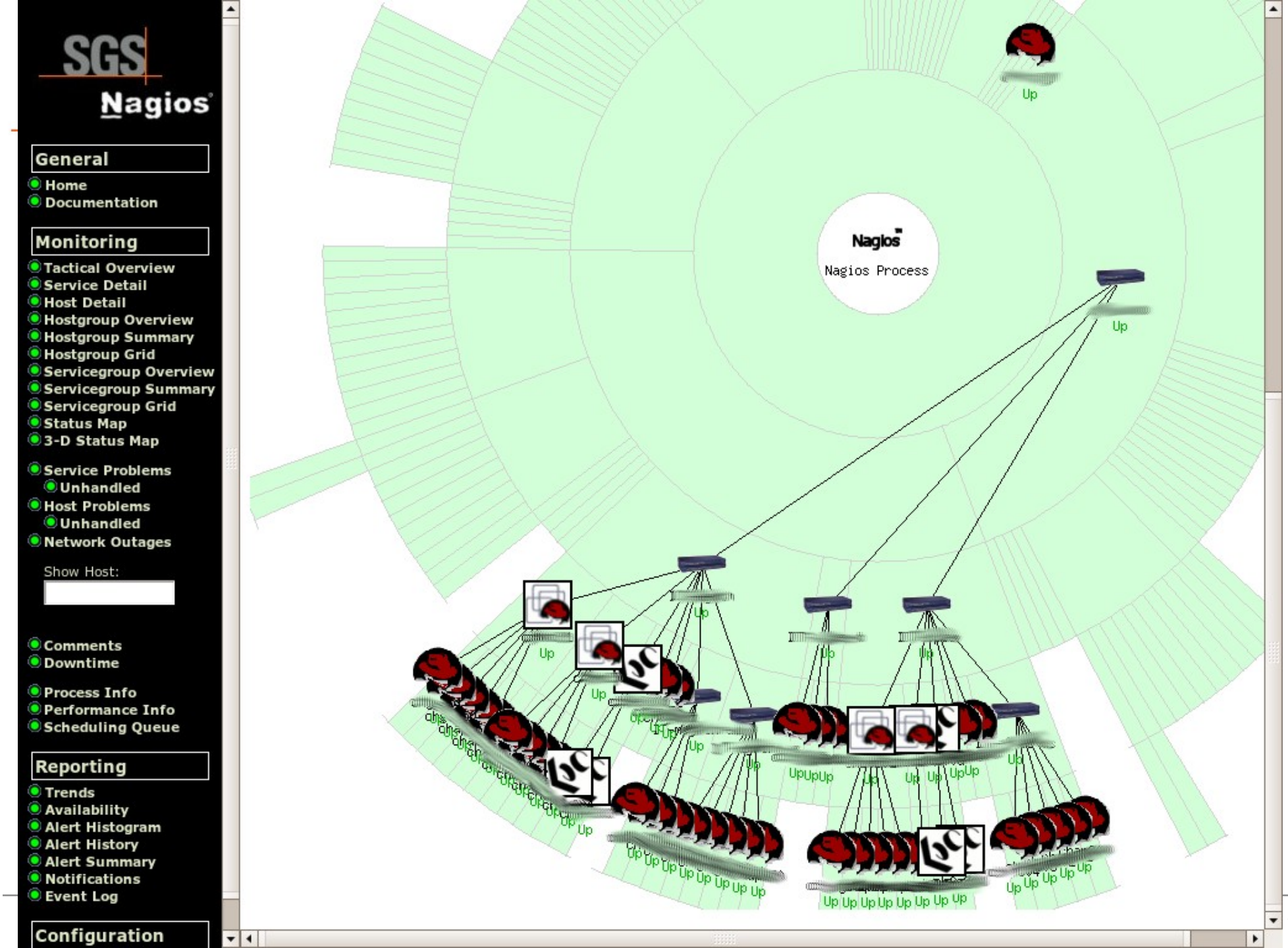
- Outil sympathique
  - Recherche Ajax
  - Calendrier
  - Zoom « à la Cacti »
  - Export PDF
- Example

Intégration avec l'existant

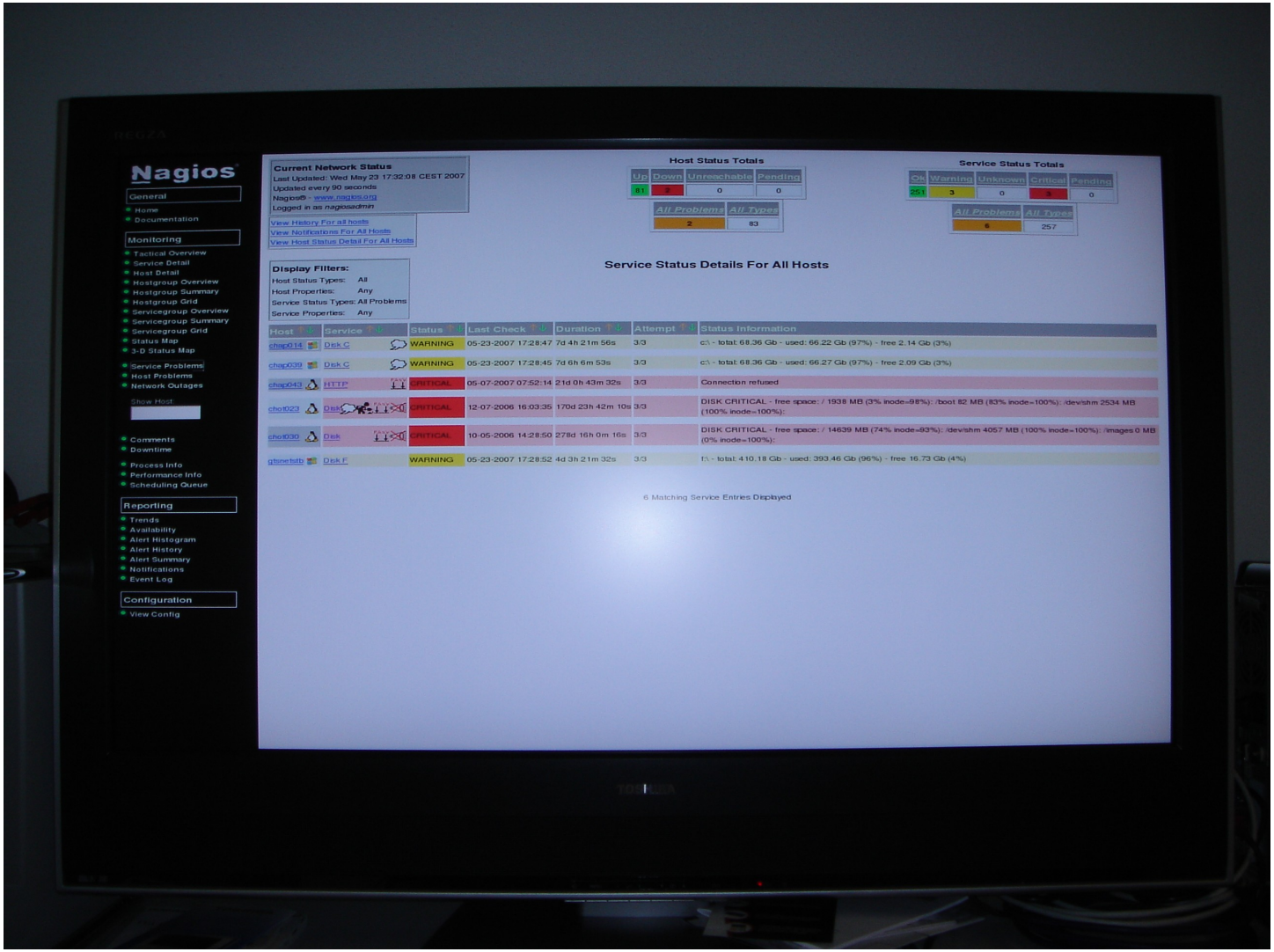
Authentification AD

Authentification AD

- Utilisateurs autorisés
  - Un groupe AD
  - Un utilisateur pour l'écran de supervision Genève : accès à toute l'infrastructure
  - Un utilisateur pour l'écran de supervision Manille : accès à leur partie


SGS
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Service Problems
Unhandled
Host Problems
Unhandled
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
Nagios
Nagios Process
Up

Authentification AD

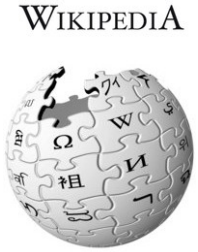


Authentification AD

- Configuration d'Apache
  - Redirection HTTP -> HTTPS
    - HTTPS systématique
  - Configuration de l'authentification AD
    - Lien vers le Global Catalog AD
    - Connexion avec un compte de service
    - Vérification d'appartenance à un groupe AD

Intégration

- Intégration avec l'infrastructure existante
  - Wiki
    - Démo
  - Gestionnaire de ticket
    - En cours d'intégration



Intégration

- D'autres outils sont utilisés en complément :
  - Cacti pour le réseau
  - Ganglia pour les clusters
  - TTL (basé sur rrdtool, développement spécifique pour une application)
  - SmokePing : debugging réseau

Utilisation avec les équipes de support

Support 24x7

- Equipe à Manille 24x7 GIMS
  - *Global Infrastructure Management Services*
  - Une dizaine de personnes (sys & dba)
  - Support niveau 1 & 2 infrastructure
  - Accès à une partie restreinte de l'infrastructure

Support 24x7

- Besoin de communiquer lors d'incidents
  - Fait via des fonctionnalités de Nagios
  - « Scheduled Downtime »
  - « Acknowledgement »

Interconnexion de serveurs

Nagios

Interconnexion

Interconnexion

- Usage habituel
  - Un nagios maître qui a l'interface web et qui envoie les alertes
  - Plusieurs Nagios esclaves qui font la supervision « local » et qui envoient les résultats au serveur central
  - Configuration assez lourde

Interconnexion

- De part la configuration IT de SGS :
  - Plusieurs Nagios indépendants par pays
  - Des accès au Nagios des applications globales par les équipes de support
  - Une configuration de base commune à tous
  - Nous maintenons en un seul endroit la référence de configuration

Remarques / Astuces / Divers

Divers

- Demander des feedbacks des admins
- DNS vs IP dans la configuration
- Thresolds de charge sur les systèmes
- Enable notification / dev_null contact
- Plugin Firefox
- Génération de bookmarks
- Curiosité : Googlemap dans Nagios

Contributions

- SGS et le libre :

  - Contribution d'un serveur quadcore à Ethan Gstaad, auteur de Nagios
  - Bug reports / RFE sur Nagios
  - Membre « grande entreprise » du GULL
  - Evangélisation ;-)

Conclusion

- Nagios, c'est très bien.

Questions