

Outils de supervision

Nagios

Bianco Jean-François

A quoi sert la supervision ?

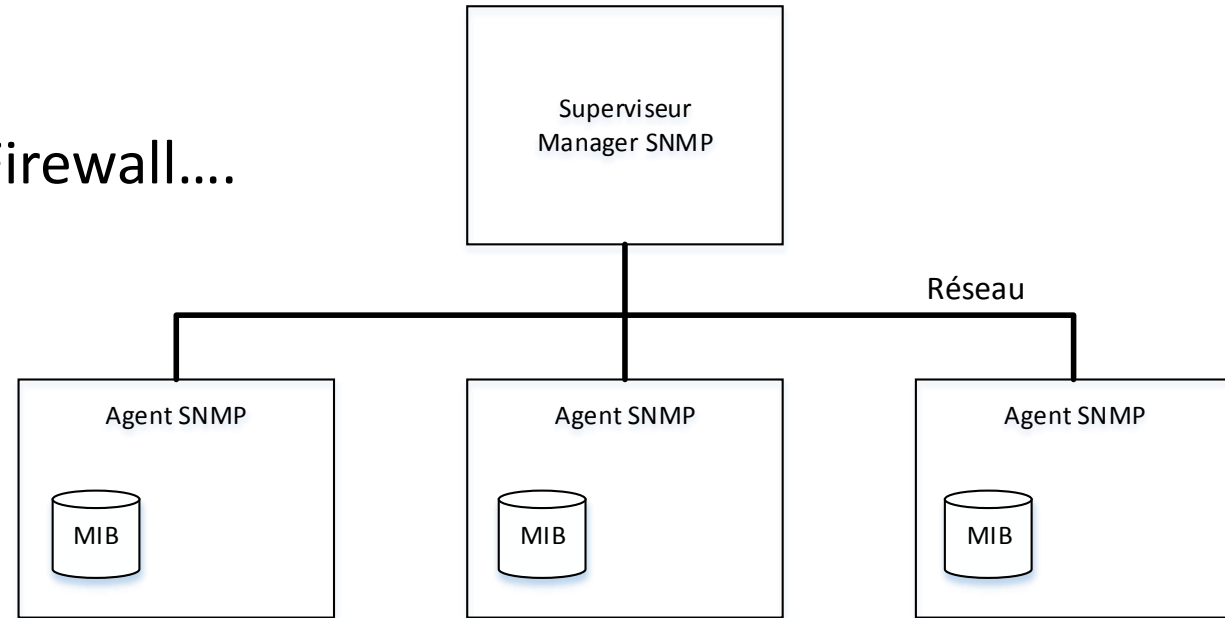
- Permet d'avoir une vue d'ensemble d'une plateforme
- Analyser son fonctionnement
- Prévenir d'éventuel problèmes avant qu'ils ne surviennent
- Avertir en cas de problèmes

Comment ?

- Analyse des logs serveurs
- Exécution de commande sur les machines
- Utilisation de SNMP

Simple Network Management Protocol

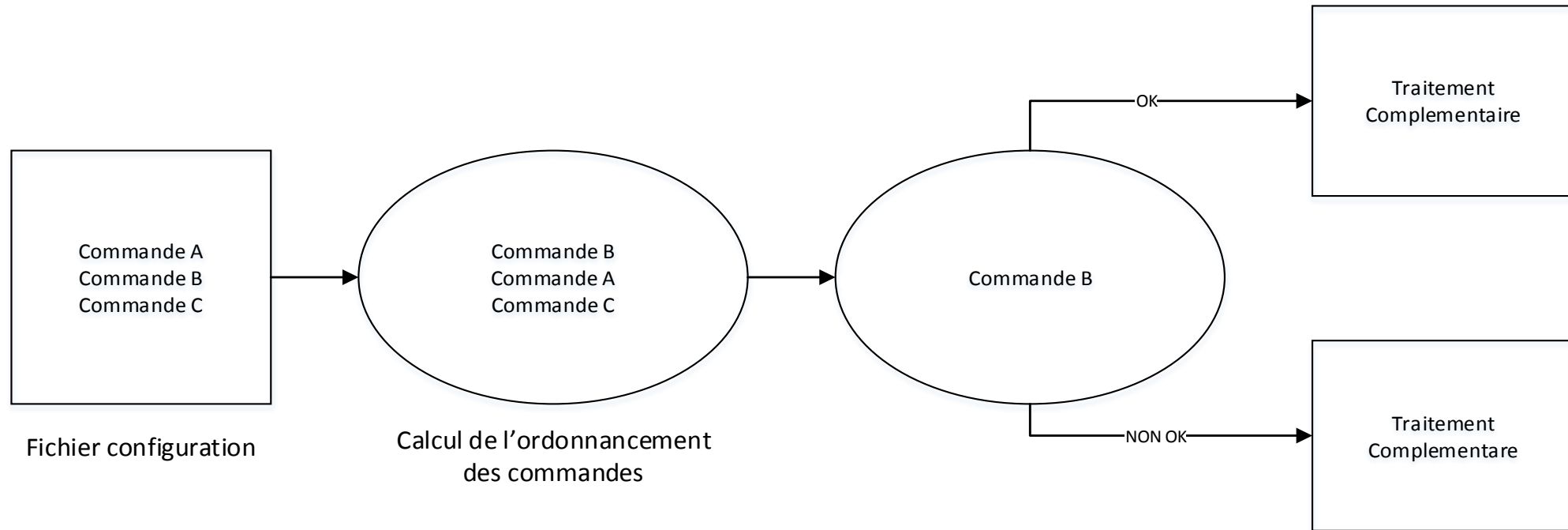
- Agent SNMP
 - Serveur, Routeur, Switch, Firewall....
- Manager SNMP
 - Serveur Nagios
- Requête UDP



Qu'est ce que Nagios ?

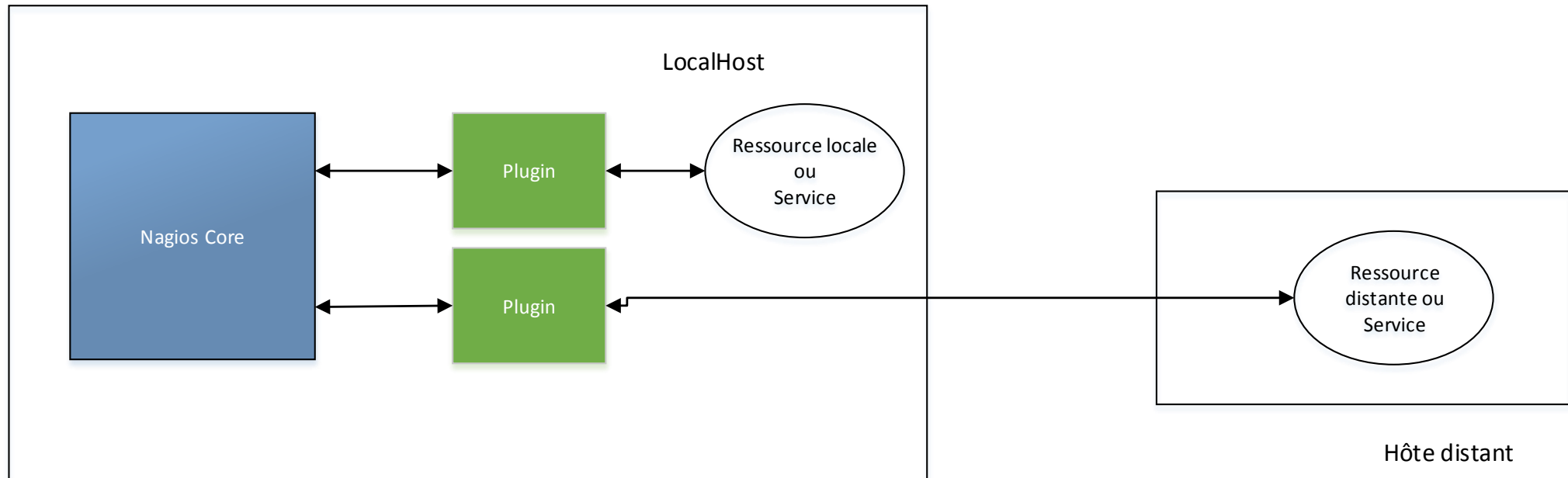
- Nagios permet :
 - La surveillance des services réseaux (SMTP, POP3, HTTP, NTP, PING, etc.)
 - La surveillance des ressources des hôtes (charge processeur, utilisation des disques, etc.)
 - Un système simple de plugins
 - Des notifications quand un hôte ou un service a un problème
 - Des gestionnaires d'événements
 - Le support pour mettre en œuvre des serveurs de supervision redondants
 - Une interface web permettant de voir l'état courant du réseau, l'historique des notifications et problèmes, le fichier journal, etc.

Nagios Core



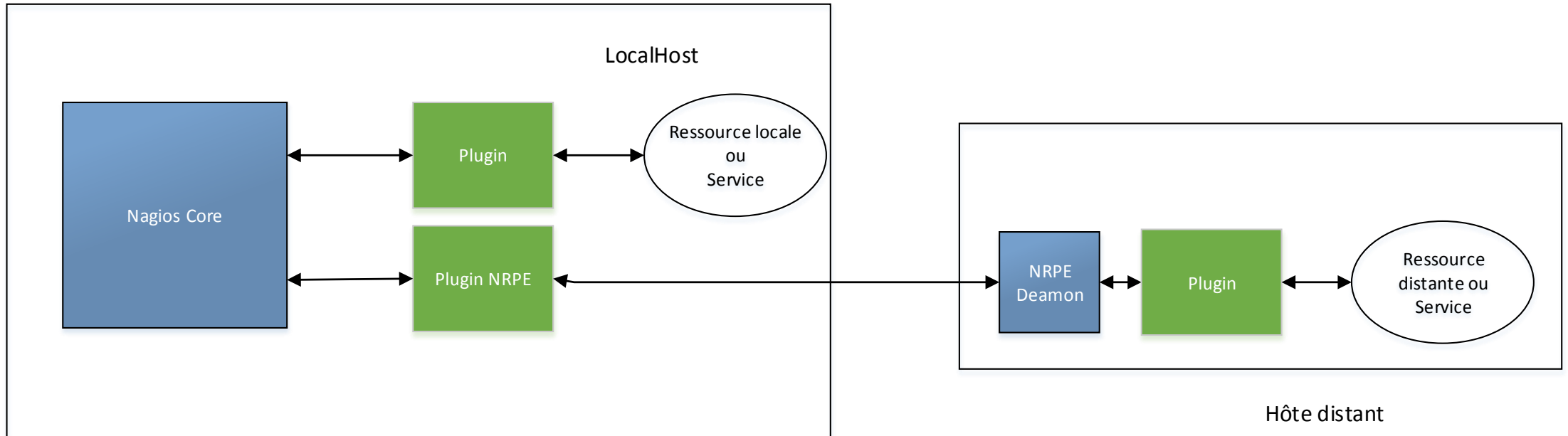
Architecture de Nagios

Version centralisée



Architecture de Nagios

Version décentralisée




Démonstration

- Mes rapports
- Rapports planifiés
- Rapports disponibles
 - Résumé
 - Disponibilité
 - Histoire État
 - Top des producteurs d'alerte
 - Alerte Histogramme
 - Notifications
 - Journal des événements
 - D'utilisation de bande passante
 - Planification de la capacité
- Les visualisations de données
 - Alerte Heatmap
 - Alerte Nuage
 - Alerte flux
 - Alerte timeline
 - Network Replay
- Rapports existants

Journal des événements

Période: Dernières 24 h À partir de: à: Go

Recherche ...    

À partir de: 2013-10-09 16:43:04 À: 2013-10-10 16:43:04
Projection 1-25 de 27 nombre total d'enregistrements

- 2013-10-10 16:32:32 SERVICE NOTIFICATION: nagiosadmin;www.twitter.com;DNS IP Match;ACKNOWLEDGEMENT (CRITICAL);notify-service-by-email;DNS CRITICAL - expected 199.59.148.10,199.59.150.39,199.59.150.7 but got 199.59.149.198,199.59.149.230,199.59.150.7;Nagios Admin;ztztututuz
- 2013-10-10 16:32:32 SERVICE NOTIFICATION: advanced;www.twitter.com;DNS IP Match;ACKNOWLEDGEMENT (CRITICAL);xi_service_notification_handler;DNS CRITICAL - expected 199.59.148.10,199.59.150.39,199.59.150.7 but got 199.59.149.198,199.59.149.230,199.59.150.7;Nagios Admin;ztztutu
- 2013-10-10 16:32:30 SERVICE NOTIFICATION: readonly;www.twitter.com;DNS IP Match;ACKNOWLEDGEMENT (CRITICAL);xi_service_notification_handler;DNS CRITICAL - expected 199.59.148.10,199.59.150.39,199.59.150.7 but got 199.59.149.198,199.59.149.230,199.59.150.7;Nagios Admin;ztztutu
- 2013-10-10 16:29:51 SERVICE ALERT: www.nagios.com;SNMP Traps;OK;HARD;1;Waiting for trap...
- 2013-10-10 16:29:41 Finished daemonizing... (New PID=7117)
- 2013-10-10 16:29:41 Warning: Host 'NOAA' has no default contacts or contactgroups defined!
- 2013-10-10 16:29:41 Event broker module '/usr/local/nagios/bin/ndomod.o' initialized successfully.
- 2013-10-10 16:29:41 Successfully shutdown... (PID=20758)
- 2013-10-10 16:29:41 Caught SIGTERM, shutting down...
- 2013-10-10 16:26:50 SERVICE ALERT: NOAA;Weather Carteret North Carolina;OK;SOFT;2;Weather OK: No watches or warnings currently apply to your area.
- 2013-10-10 16:25:50 SERVICE ALERT: NOAA;Weather Carteret North Carolina;CRITICAL;SOFT;1;(Service Check Timed Out)
- 2013-10-10 16:23:20 SERVICE FLAPPING ALERT: NOAA;Auroral Activity;STOPPED; Service appears to have stopped flapping (3.9% change < 5.0% threshold)
- 2013-10-10 16:09:10 SERVICE NOTIFICATION: nagiosadmin;www.twitter.com;DNS IP Match;CRITICAL;notify-service-by-email;DNS CRITICAL - expected 199.59.148.10,199.59.150.39,199.59.150.7 but got 199.59.148.82,199.59.149.230,199.59.150.39
- 2013-10-10 16:09:10 SERVICE NOTIFICATION: advanced;www.twitter.com;DNS IP Match;CRITICAL;xi_service_notification_handler;DNS CRITICAL - expected 199.59.148.10,199.59.150.39,199.59.150.7 but got 199.59.148.82,199.59.149.230,199.59.150.39
- 2013-10-10 16:09:10 SERVICE NOTIFICATION: readonly;www.twitter.com;DNS IP Match;CRITICAL;xi_service_notification_handler;DNS CRITICAL - expected 199.59.148.10,199.59.150.39,199.59.150.7 but got 199.59.148.82,199.59.149.230,199.59.150.39
- 2013-10-10 16:05:41 SERVICE NOTIFICATION: nagiosadmin;secure.nagios.com;Web Page Content;CRITICAL;notify-service-by-email;HTTP CRITICAL - string not found
- 2013-10-10 16:05:40 SERVICE NOTIFICATION: readonly;secure.nagios.com;Web Page Content;CRITICAL;xi_service_notification_handler;HTTP CRITICAL - string not found
- 2013-10-10 16:05:40 SERVICE NOTIFICATION: jdoe;secure.nagios.com;Web Page Content;CRITICAL;xi_service_notification_handler;HTTP CRITICAL - string not found
- 2013-10-10 16:05:40 SERVICE NOTIFICATION: advanced;secure.nagios.com;Web Page Content;CRITICAL;xi_service_notification_handler;HTTP CRITICAL - string not found
- 2013-10-10 16:04:01 SERVICE NOTIFICATION: nagiosadmin;secure.nagios.com;SSL Certificate;CRITICAL;notify-service-by-email;CRITICAL - Certificate expired on 01/11/2011 13:05.
- 2013-10-10 16:04:00 SERVICE NOTIFICATION: readonly;secure.nagios.com;SSL Certificate;CRITICAL;xi_service_notification_handler;CRITICAL - Certificate expired on 01/11/2011 13:05.
- 2013-10-10 16:04:00 SERVICE NOTIFICATION: jdoe;secure.nagios.com;SSL Certificate;CRITICAL;xi_service_notification_handler;CRITICAL - Certificate expired on 01/11/2011 13:05.
- 2013-10-10 16:04:00 SERVICE NOTIFICATION: advanced;secure.nagios.com;SSL Certificate;CRITICAL;xi_service_notification_handler;CRITICAL - Certificate expired on 01/11/2011 13:05.
- 2013-10-10 16:03:30 SERVICE ALERT: NOAA;Weather San Bernardino California;OK;HARD;3;Weather OK: No watches or warnings currently apply to your area.
- 2013-10-10 16:01:40 Finished daemonizing... (New PID=20758)

Sources

- Documentation Nagios Core

<http://www.nagios.org/>

- Cours Outils de supervision

Erwan Ben Souiden - Université Paris XVIII

- Les outils d'administration et de supervision réseau

Thierry Briche, Matthieu Voland (Université de Pau)

- Protocole SNMP

Wikipedia et Site de Christian Caleca (<http://irp.nain-t.net/>)

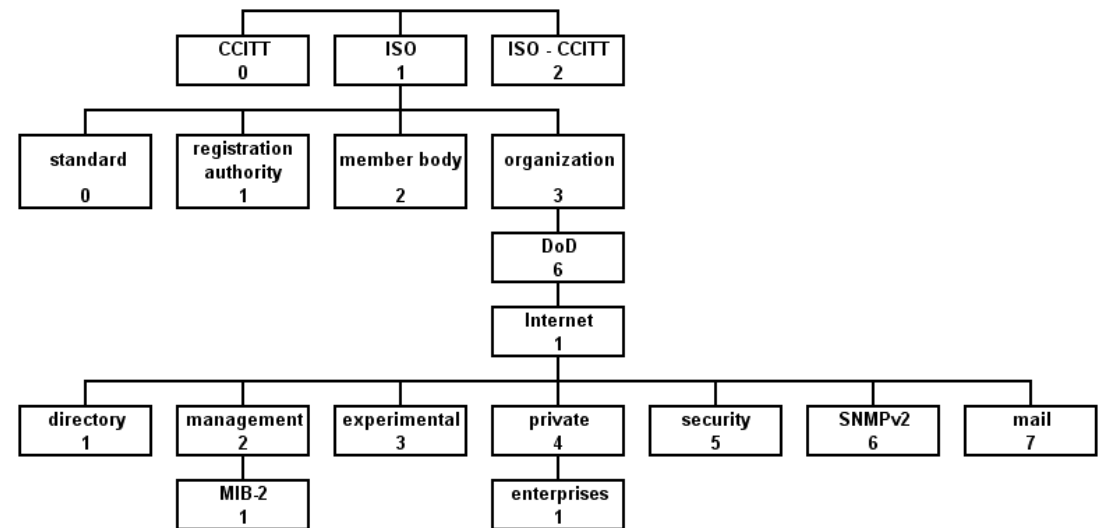
Détails MIB

adslLineMib

Fq Name :

iso.org.dod.internet.mgmt.mib2.transmission.adslMIB.adslLineMib

{ adslMIB 1 } (1.3.6.1.2.1.10.94.1.)



Simple Network Management Protocol

Commande	Action
get-request	Le Manager SNMP demande une information à un agent SNMP
get-next-request	Le Manager SNMP demande l'information suivante à l'agent SNMP
set-request	Le Manager SNMP met à jour une information sur un agent SNMP
get-reponse	L'agent SNMP répond à un get-request ou a un set-request
trap	L'agent SNMP envoie une alarme au Manager

Outils utilisant Nagios

