### Supervision Réseau Avec

# Nagios

Réalisé par : Hajar SEBTI Reda GHANEMI Mohamed QOBAYLI Encadré par ;

Mme BOUBAKRI

## Semmaire

Introduction	4
I. Cahier des charges	5
1. Réseau à superviser	5
2. Règles sur le réseau	5
II. Fonctionnement et installation de Nagios	6
1. Présentation de Nagios	6
2. Fonctionnement de Nagios	6
III. Les plugins	8
1. Plugins principaux	8
2. Plugins retenus	9
A. Check_nt	9
B. Check_nrpe	10
C. Check_snmp	10
D. Check_ping	10
IV. INSTALLATION DE NAGIOS SUR FEDORA	10
V. Installation et configuration NSClient++	19
1. Installation	20
2. Configurer NSClient + +	20
Conclusion	24

### Introduction

Actuellement aucune entreprise ne peut se passer d'outils informatiques, et très souvent un réseau informatique de taille plus ou moins importante est mis en oeuvre. Le nombre des machines dans ces réseaux peut parfois devenir extrêmement élevé; La maintenance ainsi que la gestion de ces parcs informatiques deviennent alors des enjeux cruciaux, d'autant plus qu'une panne du réseau peut parfois avoir des conséquences catastrophiques.

C'est pourquoi les administrateurs réseau font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Grâce à un tel système, les délais d'interventions sont fortement réduits..

Plusieurs logiciels réalisent ces taches, comme par exemple Websense, Tivoli, Observer, Hp Openview, Ciscoworks, Patrol et d'autres, mais certains sont payants.

Dans ce domaine, un logiciel fait office de référence: Nagios. En effet Nagios est très performant et possède une prise en main assez intuitive. Il s'installe sur une machine possédant un système d'exploitation Linux, mais peut superviser aussi bien des machines

Linux que Windows. Cet outil permet également une supervision des équipements réseaux (routeur, switch), ce qui est primordial pour l'utilisation que l'on va en faire.

De plus, Nagios est un outil Open source: Chaque société peut l'adapter comme elle lui semble. Puis, la société ne payera pas de licence: Elle ne payera que les frais de formation, d'installation et de maintenance.

Enfin un autre avantage: Une grosse communauté est réunie autour de ce logiciel, ce qui facilite les recherches de documentations et de réponses à nos questions. Notre projet consiste donc à superviser un réseau grâce à l'outil Nagios. Ce rapport résumera les trois étapes de notre projet : Compréhension, installation, et utilisation de Nagios.

#### I. Cahier des charges

#### 1. Réseau à superviser

Le réseau que nous devons superviser est celui-ci :



Il sera composé :

- D'un serveur "Windows Server 2003" qui permettra la gestion des utilisateurs du réseau :
- Stockage des données et identifications des utilisateurs
- D'un serveur "Nagios" qui s'occupera de la supervision du réseau, de la centralisation et de l'analyse des informations du réseau
- D'un poste client "Windows XP"
- D'un poste client "Linux"
- D'un routeur "Cisco" qui permettra de relier les différents équipements du réseau et d'être relié au réseau extérieur (à Internet).
- 2. Règles sur le réseau

Sur le routeur, un firewall sera configuré grâce à des ACL (Access Control List) permettant l'autorisation ou le refus de certaines connections.

Le firewall devra:

- Autoriser le protocole SMTP (pour l'envoi de mail) sortant mais pas entrant
- Autoriser le protocole IMAP (pour la réception de mail) entrant et sortant
- Autoriser le protocole HTTP entrant et sortant (pour le web)
- Autoriser le protocole ICMP entrant et sortant (pour l'envoi et la réception de PING)
- Refuser tous les autres protocoles dans les deux sens

#### Pour résumer :



#### II. Fonctionnement et installation de Nagios

#### 1. Présentation de Nagios

Nagios est un logiciel de supervision de réseau libre sous licence GPL qui fonctionne sous Linux.

Il a pour fonction de surveiller les hôtes et services spécifiés, alertant l'administrateur des états des machines et équipements présents sur le réseau.

Bien qu'il fonctionne dans un environnement Linux, ce logiciel est capable de superviser toutes sortes de systèmes d'exploitation (Windows XP, Windows 2000, Windows 2003 Server, Linux, Mac OS entre autres) et également des équipements réseaux grâce au protocole SNMP.

Cette polyvalence permet d'utiliser Nagios dans toutes sortes d'entreprises, quelque soit la topologie du réseau et les systèmes d'exploitation utilisés au sein de l'entreprise.

Ce logiciel est composé de trois parties:

-Le moteur de l'application, qui gère et ordonnance les supervisions des différents équipements

-Les Plugins qui servent d'intermédiaire entre les ressources que l'on souhaite superviser et le moteur de Nagios. Il faut bien noter que pour accéder à une certaine ressource sur un hôte, il faut un plugin coté Nagios et un autre coté hôte administré.

-L'interface web qui permet d'avoir une vue d'ensemble des états de chaque machine du parc informatique supervisé et ainsi pouvoir intervenir le plus rapidement possible en ciblant la bonne panne.

#### 2. Fonctionnement de Nagios

Le principe de supervision de Nagios repose sur l'utilisation de plugins, l'un installé sur la machine qui supporte Nagios, et l'autre sur la machine que l'on souhaite superviser. Un plugin est un programme modifiable, qui peut être écrit dans plusieurs langages possibles, selon les besoins, et qui servent à récupérer les informations souhaitées.

Nagios, par l'intermédiaire de son plugin, contact l'hôte souhaité et l'informe des informations qu'il souhaite recevoir.

Le plugin correspondant installé sur la machine concernée reçoit la requête envoyée par Nagios et ensuite va chercher dans le système de sa machine les informations demandées.

Il renvoi sa réponse au plugin Nagios, qui ensuite le transmet au moteur de Nagios afin d'analyser le résultat obtenu et ainsi mettre à jour l'interface web.

Il existe deux types de récupération d'informations: La récupération active et la récupération passive.

La différence entre les deux types est l'initiative de la récupération. Dans le premier type, à savoir le type actif, c'est Nagios qui a toujours cette initiative. C'est lui qui décide quand il envoie une requête lorsqu'il veut récupérer une information.

Alors que lors d'une récupération passive, l'envoi d'information est planifié en local, soi à partir d'une date, soit en réaction à un événement qui se déroule sur la machine administrée.

Pour notre projet, nous avons décidé d'utiliser le type de récupération active, c'est-àdire que Nagios prend l'initiative d'envoyer une requête pour obtenir des informations. Ceci évite donc de configurer les postes à superviser.

La demande d'informations se fait grâce à l'exécution d'une commande de la part de Nagios. Une commande doit obligatoirement comporter des arguments afin de pouvoir chercher les bonnes informations sur les bonnes machines.

Ces arguments sont l'adresse IP de l'hôte sur lequel aller chercher l'information, la limite de la valeur de l'information recherchée pour laquelle l'état 'attention' sera décidé, idem pour la valeur 'critique', et enfin d'autres options qui varient selon le plugin utilisé.

Pour ne pas devoir à créer une commande par machine supervisée et par information recherchée, nous pouvons remplacer les arguments par des variables, et ainsi réutiliser la commande plusieurs fois, en remplaçant la bonne variable. Nous avons alors la possibilité de travailler avec des services. Lors de la création d'un service, il faut l'associer à un ou plusieurs hôtes puis à une commande.

Ensuite Nagios remplace automatiquement la variable de l'adresse IP dans la commande, grâce à la liste d'hôtes associée au service.

Puis on doit définir manuellement dans le service les autres variables nécessaires à la commande.



Un fois que Nagios à reçu les informations dont il avait besoin sur l'état des hôtes, celui-ci peut construire des notifications sur l'état du réseau, afin d'en informer l'administrateur.

Lorsque Nagios effectue une notification, il attribut des états aux hôtes, ainsi qu'aux services.

Un hôte peut avoir les états suivants:

- Up : en fonctionnement
- Down : éteint
- Inaccessible
- En attente

Les différents états d'un service sont:

- OK
- Attention
- Critique
- En attente
- Inconnu



#### III. Les plugins

#### 1. Plugins principaux

Nagios possède une importante communauté sur Internet. Grâce à celle-ci, de nombreux utilisateurs ont crées des plugins permettant à Nagios d'aller récupérer des informations sur des équipements du réseau (PC, routeurs, serveurs, ...)

Les plugins n'utilisent pas tous le même protocole pour échanger les informations. Le protocole utilisé est dans la plupart des cas un facteur décisif sur le choix des plugins à utiliser.

Un seul plugin Nagios ne peut pas aller chercher toutes les informations sur les équipements du réseau: En effet, chaque plugin n'a accès qu'à certaines informations (exemple: un plugin peut aller chercher l'occupation du disque dur, et un autre l'occupation du processeur d'un PC). Pour superviser un parc informatique, il est donc nécessaire de mettre en place plusieurs plugins.

De plus, certains plugins peuvent aller chercher des informations sur des clients uniquement sur certains systèmes d'exploitation (c'est le cas du plugin check\_nt qui peut chercher des informations uniquement sur des équipements Windows).

Les principaux plugins utilisés par nagios sont :

- check\_disk : Vérifie l'espace occupé d'un disque dur
- check\_http : Vérifie le service "http" d'un hôte
- check\_ftp : Vérifie le service "ftp" d'un hôte
- check\_mysql : Vérifie l'état d'une base de données MYSQL
- check\_nt : Vérifie différentes informations (disque dur, processeur ...) sur un système d'exploitation Windows
- check\_nrpe: Permet de récupérer différentes informations sur les hôtes
- check\_ping: Vérifie la présence d'un équipement, ainsi que sa durée de réponse
- check\_pop: Vérifie l'état d'un service POP (serveur mail)
- check\_snmp : Récupère divers informations sur un équipement grâce au protocole SNMP (Simple Network Management Protocol)

Il est possible de créer son propre plugin. Dans ce cas, il faudra les créer de la sorte que celui renvoie à nagios :

- L'état du résultat (OK, CRITICAL, DOWN, UP, ...)
- Une chaine de caractères (pour donner le détail du résultat)

#### 2. Plugins retenus

Après avoir consulté les différents plugins existants, nous avons choisi ceux qui correspondaient à notre cahier des charges.

Nous avons retenus les plugins suivants :

- check\_nt
- check\_nrpe
- check\_snmp
- check\_ping

#### A. Check\_nt

Le plugin Check\_nt est un plugin récent qui permet de superviser très facilement des PC dont le système d'exploitation est Windows.

Check\_nt permet de récupérer sur un système Windows les informations suivantes :

L'espace occupé sur le disque dur, le temps depuis le démrrage de l'ordinateur, la version du plugin NsClient ++ (voir ci-dessous), occupation du processeur, occupation de la mémoire, état d'un service.

#### B. Check\_nrpe

Le plugin Check\_nrpe est un plugin qui permet de superviser des PC dont le système d'exploitation est Windows ou Linux.

Check\_nrpe utilise une connexion SSL (Secure Socket Layout) pour aller chercher les informations sur les postes. Ceci permet de crypter les trames d'échanges.

#### C. Check\_snmp

Le plugin Check\_snmp est un plugin qui permet de superviser tous les équipements. En revanche, il est très instable pour superviser les PC.

Dans notre projet, nous utiliserons check\_snmp pour superviser le routeur.

#### **D.** Check\_ping

Le plugin Check\_ping est un plugin qui permet de vérifier qu'un hôte est bien joignable. Usage : Pour vérifier qu'un hôte est joignable, Nagios exécute une commande ayant la syntaxe suivante :

check\_ping -H <adresse de l'hote> -w <temps maxi de reponse>,<Pourcentage de réussite des pings> -c <temps maxi de reponse>,<Pourcentage de réussite des pings>

Avec:

-w : Seuil pour lequel le résultat est considéré comme une alerte

-c : Seuil pour lequel le résultat est considéré comme critique

Pour notre projet, on testera la présence du routeur RT (192.168.104.5). En effet, ci celuici ne répond plus, on peut considérer que l'on est plus connecté à Internet.

#### IV. INSTALLATION DE NAGIOS SUR FEDORA

On commence par l'installation de Nagios et des différents plugins.

# yum -y install nagios # yum -y install nagios-plugins # yum -y install nagios-plugins-ping nagios-plugins-tcp nagios-plugins-udp nagios-plugins-http nagios-plugins-dns nagios-plugins-smtp nagios-plugins-ldap nagios-pluginspgsql nagios-plugins-mysql Vient ensuite la configuration du serveur web (Apache dans notre exemple, mais on peut en utiliser un autre). On doit pour cela modifier le fichier nagios.conf dans /etc/httpd/conf.d/ pour autoriser l'accès depuis toutes les sources.



On doit également générer un couple login/password pour accéder à l'interface Web d'administration. Pour cela, il faut:

[root@reda reda]# htpasswd -c /etc/passwd admin New password: Re-type new password: Adding password for user admin [root@reda reda]# Greer Un Mot de aser/passw JROMP) Production (19) NV-V(PI

Dans ma configuration il a aussi fallu que je passe ma Fedora en mode SELINUX permissive, sinon les scripts CGI de Nagios ne s'exécutaient pas.

# This file controls the state of SELinux on the system. # SELINUX= can take one of these three values: enforcing - SELinux security policy is enforced. # permissive - SELinux prints warnings instead of enforcing. # disabled - No SELinux policy is loaded. # SELINUX=disabled SELINUXTYPE= can take one of these two values: # # targeted - Targeted processes are protected, # mls - Multi Level Security protection. SELINUXTYPE=targeted



On active le service par la commande :

# service nagios start

Après en redémarre le système par la commande :

# reboot

Et enfin on teste le nagios





Groupes d'hôtes Descriptif de Nagios

000			Nagios	
4 + 6 + 6				Coogle
00	10	10		
	North Build	ng Switches (north switches	South Building Switches (south, switches	hes) Windows Domain Servers (win domain servers)
Nagios	Haret Status Se	reione Actions	Hust Status Services Action	m Blatten Services Actions
General	ND.35483.1 UP	205 9 9 8	20-2040.1 UP 205 Q S	
Home	N1.3588.1 UP	200 Q B A	11-1548-1 ··· 2.08 ··· 2.08	
Montheday	N1.2548.2 UP	105 Q B	SEAMER W ELEMANOVES Q 5	
Tactical Overview	N1.3545.3 0P	X0K Q 64.7	105 TO 10	A Carlos A C
Service Detail Host Detail	522548.1 UP	105 Q B-2	ETUNON A	
<ul> <li>Hostgroup Overview</li> <li>Hostgroup Summary</li> </ul>	52.2548.2 OP	MARNING Q BA	ELINOICINI Q IS	
Heatgroup Grid     Servicegroup Overview	N2-3548-3 UP	105 Q 84.34	52-3548-4 🦛 🛛 104 🖬 🔍 🐉	
Servicegroup Summary Servicegroup Grid	ND-3548-1 UP	205 9 8.5.	22-2548-1 🤲 I BOH 🔍 💱	
3-D Status Map	1	MARNING CO. CO.	52-3542.2 P	
Service Problems	53.254E.2 0P	MARNING Q DAG	54-3548-1 W	N. 74
Network Outenes	544.3346-1 UP	205 Q B	54 3545 2 W 205 Q	
Show Host:	NA 3548-2 UP	105 Q BA	10.30451 W 3.08 Q.F	
	Herstein Martin		15.3549.2 P 3.08 Q	
Commente	A second second	N DEMONSTRATION	Conservation of the Conser	
Downtime     Docess Tafe	Window	As Servers (wit_servers)	Xaerves (xaervea)	1
Performance Info	arter La I	SON QBA	STOR 9.8.3	
Burnetten	armite Las I	105 9 B.A.		
Trends	the UP	108 9 BA		
Availability Alert Histogram	thesized GP 1	105 Q 5 3		
Alert History Alert Summary	coccer LP	10K Q B.A.		
Notifications     Event Log	etuenten an	AGE Q DAR		
Configuration	1			
View Config	and the second s	100 Q 50 R		
	Contraction of Contra	A G G A		
	visit LP	10K 9 19 7		
		SOK 9 19 2		
	coth Law	10K 9 6 8		
		SDR Q BAR		

Les services Descriptif de Nagios

000				Nagios		8
▲ ► C + 6						• Q- Google
m						
ана О	0	O Navias				
····	·	© Nagios				
Nagios	xserve01	<u>ComputerSysID</u>	ок	02-28-2007 13:38:57 11d 19h 56m 02-28-2007 13:39:09 10d 18h 15m	23s 1/5 30s 1/5	2 process matching AppleFieServer :> 0: OK SNMP OK - "Darwin xserve01. 8.8.0 Darwin Kernel Version 8.8.0: Fri Sep 8 17:18:57 DD 2006: rootxnu, 22:12 6 obi-10EFIEASE_PPC Power Macintosh"
General		ComputerSysInfo	ок	02-28-2007 13:39:09 5d 2h 59m 48	s 1/5	SNMP OK - "xserve01
Home		Currentilisere	OK	02-28-2007 13:36:14 12d 1b 49m 4	8e 1/5	LISERS OK - 1 years currently logged in
Ocumentation		KDCRunning	OK	02-28-2007 13:40:08 11d 20h 8m 3	1s 1/5	1 process matching krb5kdc : > 0 ; OK
Monitoring		LDAPRunning	ОК	02-28-2007 13:39:26 28d 4h 55m 5	7s 1/5	1 process matching slapd : > 0 : OK
Monitoring		LocalLoad	ОК	02-28-2007 13:39:21 33d 0h 30m 2	9s 1/5	OK - load average: 0.59, 0.92, 0.90
Tactical Overview     Service Detail		MacShare FreeSpace	ОК	02-28-2007 13:38:25 28d 4h 55m 5	7s 1/5	/Volumes/MacShare : 85 %left (2038067Mb/2384544Mb) (> 20) : OK
Host Detail		PING	ОК	02-28-2007 13:36:43 5d 10h 52m 4	4s 1/5	PING OK - Packet loss = 0%, RTA = 0.29 ms
Hostgroup Overview		RetroServerRunning	ОК	02-28-2007 13:40:08 11d 20h 8m 3	1s 1/5	1 process matching RetroRun : > 0 : OK
Hostgroup Summary		SMBdRunning	ок	02-28-2007 13:39:26 28d 4h 55m 5	7s 1/5	3 process matching smbd : > 0 : OK
Hostgroup Grid		SSH	ок	02-28-2007 13:39:08 28d 20h 45m	18s 1/5	SSH OK - OpenSSH_4.2 (protocol 2.0)
Servicegroup Summary		Unix Root FreeSpace	OK	02-28-2007 13:38:58 28d 4h 54m 4	5s 1/5	/:68 %left (120102Mb/176700Mb) (>20): OK
Servicegroup Grid		Xserveu1LDAP	UK	02-28-2007 13:39:08 10d 20h 39m	4/S 1/5	LDAP OK - 0.045 seconds response time
Status Map	xserve02	AFPdRunning	ОК	02-28-2007 13:40:09 10d 20h 10m	19s 1/5	2 process matching AppleFileServer : > 0 : OK
<ul> <li>3-D Status Map</li> <li>Cacti Home</li> </ul>		ComputerSysID	ок	02-28-2007 13:39:25 1d 1h 36m 51	s 1/5	SNMP OK - "Darwin xserve02. 8.8.0 Darwin Kernel Version 8.8.0: Fri Sep 8 17:18:57 PDT 2006: root:xnu-792.12.6.obj~1/RELEASE_PPC Power Macintosh"
Service Problems Host Problems		ComputerSysInfo	ок	02-28-2007 13:39:09 1d 20h 45m 4	s 1/5	SNMP OK - " OID: NET-SNMP-TC::unknown Timeticks: (17449421) 2 days, 0:28:14.21 "\"PC Server Room\""
Network Outages		CurrentUsers	OK	02-28-2007 13:38:25 10d 19h 39m	375 1/5	USERS OK - 1 users currently logged in
Show Host:		HTTP Local and	OK	02-28-2007 13:40:08 11d 17h 11m	455 1/5 3c 1/5	OK - load average: 0.53, 1.01, 0.92
Show Host.		Nanine ServerProce	OK	02-28-2007 13:40:08 4d 23h 25m 2	s 1/5	PROCS OK: 92 processes
		NaciosServerZombieProcs	OK	02-28-2007 13:39:08 4d 5h 30m 12	s 1/5	PROCS OK: 44 processes with STATE = RSDTIUs+>
		PING	ОК	02-28-2007 13:36:43 5d 3h 5m 39s	1/5	PING OK - Packet loss = 0%, RTA = 0.06 ms
Comments		SMBdRunning	ОК	02-28-2007 13:40:09 10d 20h 10m	19s 1/5	3 process matching smbd : > 0 : OK
Owntime		SSH	OK	02-28-2007 13:38:25 12d 15h 24m	28s 1/5	SSH OK - OpenSSH_4.2 (protocol 1.99)
Process Info		Unix Root FreeSpace	ОК	02-28-2007 13:38:25 10d 20h 13m	19s 1/5	/: 51 %left (79240Mb/156830Mb) (> 20) : OK
Performance Info	xserveraid1s1	AppleBaseStationID	ОК	02-28-2007 13:39:09 4d 4h 14m 29	s 1/5	SNMP OK - "Xserve RAID V1.5"
Scheduling Queue		AppleBaseStationInfo	ок	02-28-2007 13:40:27 1d 15h 16m 6	s 1/5	SNMP OK - "xserveraid01" Timeticks: (66413893) 7 days, 16:28:58.93 "PC Server Room, under Xserve01"
Reporting		XserveRaidStatus	ОК	02-28-2007 13:37:27 1d 1h 30m 38	s 1/5	OK - Ihs.array1 optimal, rhs.array1 optimal
Trends	xserveraid1s2	AppleBaseStationID	ОК	02-28-2007 13:40:27 4d 11h 14m 4	6s 1/5	SNMP OK - "Xserve RAID V1.5"
Availability		Anala Daga Station Info	OK	02 29 2007 42/20/00 4d 45h 46m 6	4/6	SNMP OK - "xserveraid01-2" Timeticks: (66400601) 7 days, 16:26:46.01
Alert History		Applebasestationinto	UK	02-28-2007 13:39:09 10 150 1600 6	s 1/5	"PC Server Room, under Xserve01"
Alert Summary		XserveRaidStatus	ОК	02-28-2007 13:39:48 0d 23h 1m 29	s 1/5	OK - Ihs.array1 optimal, rhs.array1 optimal
<ul> <li>Notifications</li> <li>Event Log</li> </ul>	<u>yellow</u>	ComputerSysID	ок	02-28-2007 13:40:27 3d 23h 23m 3	5s 1/5	SNMP OK - "Hardware: x86 Family 6 Model 7 Stepping 3 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)"
Configuration		ComputerSysInfo	ок	02-28-2007 13:39:25 1d 15h 16m 6	s 1/5	SNMP OK - "YELLOW" OID: MSFT-MIB::dc Timeticks: (93781048) 10 days, 20:30:10.48 ' "PC Server Room"
View Config		CurrentUsers	ОК	02-28-2007 13:36:14 10d 19h 28m	19s 1/5	USERS OK - 1 users currently logged in
		PING	ок	02-28-2007 13:38:18 2d 13h 41m 5	5s 1/5	PING OK - Packet loss = 0%, RTA = 0.31 ms
		WindowsLDAP	ок	02-28-2007 13:36:31 10d 20h 28m	1s 1/5	LDAP OK - 0.075 seconds response time
		Windows C FreeSpace	ок	02-28-2007 13:40:09 6d 8h 56m 51	s 1/5	C:\Label:Local Disk Serial Number 24a13aaa : 61 %left (5268Mb/8699Mb) (> 20) : OK
	zinc	ComputerSysID	ок	02-28-2007 13:39:08 0d 10h 25m 1	7s 1/5	SNMP OK - "Hardware: x86 Family 15 Model 4 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Multiprocessor Free)"
		ComputerSysInfo	ок	02-28-2007 13:40:08 0d 10h 25m 4	7s 1/5	SNMP OK - "ZINC" OID: MSFT-MIB::server Timeticks: (294227628) 34 days, 1:17:56.28 "server Room"
		CurrentUsers	ок	02-28-2007 13:39:21 1d 15h 28m 7	s 1/5	USERS OK - 1 users currently logged in
		PING	OK	02-28-2007 13:36:43 10d 20h 23m	5s 1/5	PING OK - Packet loss = 0%, RTA = 0.23 ms
		Windows C FreeSpace	OK	02-28-2007 13:38:25 0d 10h 25m 4	7s 1/5	C:\ Label: Serial Number 40034dtd : 91 %left (63659Mb/69994Mb) (> 20) : OK

Hôte problème Descriptif de Nagios

$\Theta \Theta \Theta$				Nagios				-
							^ Q- Google	*
m								>>
Narios								
Rugios								
<u>N</u> agios	Current Network St Last Updated: Thu Mar Updated every 90 secon Nagios® - www.nagios.c	tatus 1 08:58:35 CST 2007 nds 279		Up Do 60	wn Unreachabl	e Pending 0	Ok Warning Unknown Critical Pending 259 6 4 2 0	
General	View History For all host	•		A	II Problems All	Types	All Problems All Types	
Documentation	View Notifications For Al View Host Status Detail	Hosts For All Hosts			2	62	12 262	2
	(Hen Host oldes bolan							
Monitoring	Display Filters:			Servic	e Status Detai	Is For All Ho	sts	
Tactical Overview     Service Detail	Host Status Types: A	NI						
Host Detail	Service Status Types: A	VI Problems						
Hostgroup Overview	Service Properties: A	Any						
Hostgroup Summary	Host 🔨	Service 1	Status 🐴	Last Check	Duration 1	Attempt 1	Status Information	
Hostgroup Grid Servicegroup Overview	N2-3548-1	PING	WARNING	03-01-2007 08:54:53	0d 0h 7m 58s	5/5	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 4.20 ms	
Servicegroup Summary	N2-3548-2	PING	WARNING	03-01-2007 08:54:53	0d 0h 7m 58s	5/5	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 3.54 ms	
Servicegroup Grid	NO 2640 0	DINC	WADNING	03 04 2007 08-64-62	Od Ob 7m ERs	E/E	DING WADNING DUDU CATES FOUND Desired lass = 0% DTA = 5.10 ms	
Status Map	143-3040-2	PING	WARMING	03-01-2007 08:54:53	od on 7m Ses	5/5	PING WARNING - DUPLICATES FOUND: Packet loss - 0%, RTA - 5.10 his	
Cacti Home	<u>S2-3548-1</u>	PING	WARNING	03-01-2007 08:54:37	0d 0h 8m 19s	5/5	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 0.96 ms	
Service Problems	<u>S2-3548-2</u>	PING	WARNING	03-01-2007 08:54:49	0d 0h 33m 6s	5/5	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 0.81 ms	
Host Problems	<u>84-3548-1</u>	PING	WARNING	03-01-2007 08:53:58	0d 0h 29m 10s	5/5	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 15.07 ms	
Network Outages		Nata and Base Station ID	LINKA KOMAN	02.01.2007.00.56.22	224 105 47- 52-	6/E	Child assistant. Ma data spectrum from host	
Show Host:		NetgearBaseStationID		03-01-2007 08:58:32	330 19h 47m 32s	1/5	CNMP protein - No data received from host	
		nergearbaseStationinic		03-01-2007 08:57:30	330 19h 33h 27s	1/5	CDITICAL Diversity freed and after 10 accession	
		<u>PING</u> 9	CHINCAL	03-01-2007 08:56:32	00 10h 2m 56s	1/5	CRITICAL - Plugin timed out after 10 seconds	
Comments	) <u>an2</u> 🕺	NetgearBaseStationID	UNKNOWN	03-01-2007 08:54:10	33d 19h 47m 50s	1/5	SNMP problem - No data received from host	
Sowname		NetgearBaseStationInfo	UNKNOWN	03-01-2007 08:54:10	33d 19h 45m 17s	1/5	SNMP problem - No data received from host	
Process Info     Derformance Info		PING ¢		03-01-2007 08:57:30	1d 20h 50m 12s	1/5	CRITICAL - Plugin timed out after 10 seconds	
Scheduling Queue								
Reporting Trends				12	Matching Service E	intries Displayed		

#### L'information sur le rendement de Nagios

$\Theta \Theta \Theta$		Nagio	os	
				↑ Q- Google
<u> </u>				
Nagios				
Nagios <sup>®</sup> General ® Home © Documentation	Performance Information Last Updated: Thu Mar 1 08:00:24 CST 2007 Updated every 90 seconds Nagios0 - www.nagios.org Logged in as	Progra	m-Wide Performanc	e Information
Monitoring © Tactical Overview © Service Detail © Host Detail © Hostgroup Overview © Hostgroup Summary © Hostgroup Summary © Hostgroup Summary	Active Service Checks:	Time Frame <= 1 minute: <= 5 minutes: <= 1 minutes: <= 1 hour: Since program start:	Checks Completed           12 (4.6%)           258 (98.5%)           262 (100.0%)           262 (100.0%)           262 (100.0%)	Metric         Min.         Max.         Average           Check Execution Time:         0.02 sec         1.02 sec         1.615 sec           Check Latency:         0.00 sec         15.97 sec         1.284 sec           Percent State Change:         0.00%         17.30%         0.34%
Servicegroup Sumary     Servicegroup Grid     Status Map     Cacti Home     Service Problems     Host Problems	Passive Service Checks:	Timo Framo <= 1 minute: <= 5 minutes: <= 15 minutes: <= 1 hour: Since program start:	Checks Completed           0 (0.0%)           0 (0.0%)           0 (0.0%)           0 (0.0%)           0 (0.0%)           0 (0.0%)	Metric         Min.         Max.         Average           Percent State Change:         0.00%         0.00%         0.00%
Comments     Downtime     Process Info	Active Host Checks:	Time Frame <= 1 minute: <= 5 minutes: <= 15 minutes: <= 1 hour: Since program start:	Checks Completed 6 (9.7%) 13 (21.0%) 17 (27.4%) 33 (53.2%) 56 (90.3%)	Metric         Min.         Max.         Average           Check Execution Time:         0.02 sec         10.02 sec         0.350 sec           Check Latency:         0.00 sec         0.00 sec         0.00 sec           Percent State Change:         0.00%         0.00%         0.00%
Performance Info     Scheduling Queue      Reporting     Trends     Availability     Alert Histogram     Alert Histogram     Alert Summary     Notifications	Passive Host Checks:	Time Frame <= 1 minute: <= 5 minutes: <= 15 minutes: <= 1 hour: Since program start:	Chocks Completed           0 (0.0%)           0 (0.0%)           0 (0.0%)           0 (0.0%)           0 (0.0%)           0 (0.0%)	Metric Min. Max. [Average] Percent State Change: 0.00% 0.00% 0.00%

#### L'information de processus de Nagios



#### Les Checkcommands Nagios

$\Theta \Theta \Theta$		Nagios					
	▲ ► C + A A						
Address Book - Bonjo	our - Gmail My Blogs - PC News Feed	ls▼ Mac News Sites▼ Security Sites (15)▼ LiveJournal▼ Site Status Feeds▼ Apple Tech Feeds▼ >>>					
Nagios							
	Logged in as	Update					
<u>N</u> agios <sup>®</sup>		@ Ť					
General		-					
Home		Commands					
Documentation	Command Name	Command Line					
Monitoring	check-host-alive	SUSER15/check_ping -H \$HOSTADDRESS\$ -w 3000.0,80% -c 5000.0,100% -p 1					
Tactical Overview	check_afp_process_via_snmp	\$USER1\$/check_snmp_process.pl -H \$HOSTADDRESS\$ -C \$USER3\$ -n \$USER8\$					
Service Detail	check_airport_version	\$USER1\$/check_snmp -H \$HOSTADDRESS\$ -0 .1.3.6.1.4.1.63.501.3.1.5.0 -C \$USER15\$ -P 2c					
O Host Detail	check_airport_wireless_client_MAC_addresses	SUSERT\$/check_snmp-H_SHOSTADDRESS\$-0.1.3.6.1.4.1.63.501.3.2.2.1.0.23.242.72.157.17 -C \$USER15\$-P 2c					
Hostgroup Overview	check_airport_wreless_client_count	SUSERVISCHEDK_SIMP -H SHOSTADDRESSS -0 .1.3.0.1.4.1.03.001.3.2.1.0 -0 SUSERVIS6 -P 20 SUSERVISCHEDK_SIMP strange strange of uH SHOSTADDRESS -0 SUSERVIS6 -P 20					
Hostgroup Summary	check dos	SUSERI/herk drs - Huwy vaho com - \$HOSTADDESSS					
Hostgroup Grid	check ftp	SUSER1\$/check ftp -H \$HOSTADDRESS\$					
Servicegroup Overview	check hpid	SUSER1\$/check hold -H \$HOSTADDRESS\$ -C kclife					
Servicegroup Summary	check_http	\$USER1\$/check_http-H \$HOSTADDRESS\$					
Servicegroup Grid	check_kdc_process_via_snmp	\$USER1\$/check_snmp_process.pl -H \$HOSTADDRESS\$ -C \$USER3\$ -n \$USER9\$					
Status Map	check_ldap	\$USER1\$/check_Idap -H \$HOSTADDRESS\$ -b \$USER12\$ -3					
Casti Hama	check_ldap_process_via_snmp	\$USER1\$/check_snmp_process.pl -H \$HOSTADDRESS\$ -C \$USER3\$ -n \$USER11\$					
Caco Home	check_local_disk	\$USER1\$/check_disk -w \$ARG1\$ -c \$ARG2\$ -p \$ARG3\$					
Service Problems	check_local_load	\$USER1\$/check_load -w \$ARG1\$ -c \$ARG2\$					
Host Problems	check_local_procs	SUSERIS/check_procs-w SARGIS-c-SARG2S					
Network Outages	check_local_users	SUSERTS/Check_USERS -W SARGTS -C SARGZS					
Show Host:	check_nntp	SUSERIS/Check_Inter + SHOTADDESSS # \$APC15 - \$APC25 - 5					
Show Hose.	check pop	SUSERIS/check poor + SHOSTADDRESSS					
	check retrospect process via snmp	SUSERIS/check simp process.pl -H SHOSTADDRESSS -C SUSERIS -n SUSERIOS					
	check_smb	\$USER1\$/check_disk_smb-H \$HOSTADDRESS\$ -s MacShare -W \$USER4\$					
Comments	check_smb_process_via_snmp	\$USER1\$/check_snmp_process.pl -H \$HOSTADDRESS\$ -C \$USER3\$ -n \$USER7\$					
O Downtime	check_smtp	\$USER1\$/check_smtp -H \$HOSTADDRESS\$					
Process Info	check_snmp_abs_sysID	\$USER1\$/check_snmp -H \$HOSTADDRESS\$ -C \$USER15\$ -o system.sysDescr.0					
Performance Info	check_snmp_abs_sysinfo	SUSER1\$/check_snmp-H_SHOSTADDRESS3-C_SUSER155-m_ALL-co- system sysName_0_system system system sysContact 0_system sysLocation_0_					
Scheduling Queue	check snmp astaro svsID	SUSER1\$/check_snmp-H_SHOSTADDRESS\$-C \$USER17\$-o system.sysDescr.0					
	check_snmp_astaro_sysinfo	\$USER1\$/check_snmp -H \$HOSTADDRESS\$ -C \$USER17\$ -m ALL -o system.sysName.0,system.sysUpTime.0					
Reporting	check_snmp_computer_sysid	\$USER1\$/check_snmp -H \$HOSTADDRESS\$ -C \$USER3\$ -o system.sysDescr.0					
Trends	check_snmp_computer_sysinfo	SUSER1\$/check_snmpH_SHOSTADDRESS\$-C_SUSER3\$-m_ALLo system system sys					
Availability	check snmp netgear sysID	SUSERIS/check snnp - H \$HOSTADDRESS - C \$USERIE\$ - o system.sysDescr.0					
Alert Histogram	check_snmp_netgear_sysinfo	\$USER1\$/check_snmp -H \$HOSTADDRESS\$ -C \$USER16\$ -m ALL -o system.sysName.0.system.sysUpTime.0					
Alert History	check_snmp_netgear_wireless_client_IP_addresses	\$USER1\$/check_snmpwalk -H \$HOSTADDRESS\$ -C \$USER16\$ -0 .1.3.6.1.4.1.4526.4.3.2.6.1.3.1					
Notifications	check_snmp_netgear_wireless_client_MAC_addresses	\$USER1\$/check_snmpwalk -H \$HOSTADDRESS\$ -C \$USER16\$ -0 .1.3.6.1.4.1.4526.4.3.2.5.1.2.1					
Event Log	check_snmp_switch_sysid	SUSER13/check_snmp -H SHOSTADDRESS\$ -C SUSER6\$ -o system.sysDescr.0					
	check_snmp_switch_sysinfo	subservargenex_snmp -H sHUSIADURESSS -C SUSERSS -m ALL -o system.sysName.0.system.sysObjectID.0.system.sysUbTime.0.system.sysContact.0.system.sysLocation.0					
Configuration	check_ssh_tiger	\$USER1\$/check_ssh -4 -1 30 -r OpenS8H_4.2 -H \$HOSTADDRESS\$					
View Config	check_top	\$USER1\$/check_top -H \$HOSTADDRESS\$ -p \$ARG1\$					
	check_teinet	\$USER1\$/check_tcp -H \$HOSTADDRESS\$ -p 23					
	check_udp	\$USER1\$/check_udp -H \$HOSTADDRESS\$ -p \$ARG1\$					
	check_windows_Idap	\$USER1\$/check_ldap -H \$HOSTADDRESS\$ -b \$USER5\$					
	check_xserve_raid	SUSERTS/check_xserve_raidaddress SHOSTADDRESSS					
	cneck_zomble_procs	SUSERIA/CITELE_JPOUS -M APRO 19 -C SARGES -S SARGES - NOTEICATIONTYDESINHAEL SHOETNAMESINGIata: SHOETNATESINGIAT					
	host-notify-by-email	Danomiphinin yau "unindenication type: alconnection reasonal shows showed and a showed the showed the showed and the showed an					
	host-notify-by-epager	/usr/bin/pnntt "xb" "Host "sHOSTALIASS" is SHOSTSTATE\$\\intc: \$HOSTOUTPUT\$\\nTime: \$LONGDATETIME\$"  /usr/bin/mail -s "\$NOTIFICATIONTYPES alert - Host \$HOSTNAME\$ is \$HOSTSTATE\$" \$CONTACTPAGER\$					
	notify-by-email	usrbiniprinti "%b" **********************************					
	notify-by-epager	Jus/bin/printf "%6" "Service: SSERVICEDESCSInHost: \$HOSTNAME\$InAddress: \$HOSTADDRESSInState: SSERVICESTATE\$InInfo: \$SERVICEOUTPUT\$InDate: \$LONGDATETIME\$"   /usr/bin/mail -s "\$NOTIFICATIONTYPE\$: \$HOSTALIAS\$/\$SERVICEDESC\$ is \$SERVICESTATE\$" \$CONTACTPAGER\$					
	process-service-perfdata	echo '\$HOSTNAME\$1:\$SERVICEDESC\$\t\$SERVICEOUTPUT\$\t\$SERVICEPERFDATA\$\n'   nc -u -w 3 localhost 5667					
		T					

#### 2-D Carte de Nagios



Le menu Host Detail :Cette page résume l'état global des machines de votre réseau, avec leurs états (ACTIF, EN PANNE ...)

<b>Dagios</b> <b>General</b> <b>®</b> Home <b>®</b> Documentation <b>Monitoring</b> <b>®</b> Tactical Overview <b>®</b> Service Detail <b>®</b> <u>Host Detail</u> <b>®</b> Status Overview <b>®</b> Status Summary	Current Netw Last Updated: Wed h Updated every 90 see Napose 9 - www seek Logged in as napose View Service Status View Status Onerview View Status Control For	ork Statu fay 11 16:48 os.org imin Detail For All # For All Host For All Host Gro	IS 27 CEST 2005 Host Groups 6 Groups 6 Groups 9 Groups 9 Groups 9 Groups 9 Groups	Host Sta	Host Status 7 Down Unreacha 2 0 All Problems A 2 1 Atus Details For	Totals ble Pending 0 11 Types 13 • All Host Groups	Service Status Totals           Ok         Warning         Unknown         Critical         Pending           17         0         1         1         2           All Problems         All Types         2         21
Status Grid	Host↑↓		Status ᠰ	Last Check 🔨	Duration ᠰ	Status Information	
Status Map 3-D Status Man	<u>fw2.alex.fr</u>	08	UP	11-05-2005 16:10:49	0d 1h 25m 20s	(Host assumed to be up)	
Corriso Broblome	printer1	28	DOWN	11-05-2005 16:43:19	5d 6h 19m 3s	Timeout: No Response from 1	192.168.0.1. : Timeout from host 192.168.0.1
<ul> <li>Service Problems</li> <li>Host Problems</li> </ul>	srv1.alex.fr	*	UP	11-05-2005 16:11:03	5d 20h 1m 22s	(Host assumed to be up)	
Network Outages	srv12.alex.fr	01	DOWN	11-05-2005 16:46:46	0d 0h 36m 50s	Share volume not specified	
<ul> <li>Comments</li> <li>Downtime</li> </ul>	srv2.alex.fr	۵ß	UP	11-05-2005 16:11:44	0d 1h 22m 0s	(Host assumed to be up)	
Process Info	<u>srv3.dmz.alex.fr</u>	- # <b>B</b>	UP	11-05-2005 16:11:57	0d 1h 23m 5s	(Host assumed to be up)	
Performance Info	srv4.dmz.alex.fr	08	UP	11-05-2005 16:12:12	0d 1h 23m 5s	(Host assumed to be up)	
Scheduling Queue	srv5.alex.fr	08	UP	11-05-2005 16:12:24	2d 3h 31m 56s	(Host assumed to be up)	
Reporting	srv6.alex.fr	_ <u>∆</u> {₿	UP	11-05-2005 16:12:38	0d 1h 23m 0s	(Host assumed to be up)	
Trends Availability	<u>srv7.alex.fr</u>	_ <u>∆</u> ®	UP	11-05-2005 16:12:41	2d 3h 29m 4s	(Host assumed to be up)	
Alert Histogram	<u>srv9.dmz.alex.fr</u>	08	UP	11-05-2005 16:11:51	5d 18h 43m 7s	(Host assumed to be up)	
Alert History Alert Summary	switch1		UP	11-05-2005 16:11:37	5d 20h 2m 15s	PING OK - Paquets perdus =	0%, RTA = 0.05 ms
Notifications     Event Log	switch2	-8	UP	11-05-2005 16:13:05	5d 5h 25m 14s	(Host assumed to be up)	
Configuration • View Config					13 Matching Host Entri	ies Displayed	

Le menu Status Overview :Cette page affiche tous les hôtes par groupes, cela permet une vue rapide sur un sous-ensemble de votre parc



#### Le menu Status Map :

Cette page représente l'implantation de vos hôtes sous plusieurs



formes graphiques. Vous avez un aprecu de la topologie de vos hôtes en 2D ou en 3D pour le fun (installez un plugin VRML)



Le menu Scheduling Queue :Cette page liste les services qui vont être testés prochainement. C'est ici que vous pouvez demander le test d'un service manuellement (l'icone montre au poignet), suite à une modification de votre configuration par exemple

	Logged in as <i>nagiosadmin</i>					
Nagios		Entries sorte	ed by <b>next check ti</b>	<b>me</b> (ascending)		
Guera	Host $\uparrow \downarrow$	Service ↑↓	Last Check ᠰ	Next Check ᠰ	Active Checks	Actions
<ul> <li>Documentation</li> </ul>	switch1	<u>Ping du switch LOC</u>	11-05-2005 16: 45: 21	11-05-2005 16: 50: 21	ENABLED	XX
Monitoring	srv3.dmz.alex	fr Connexions SMTP	11-05-2005 16:47:27	11-05-2005 16: 50: 27	ENABLED	X
Tactical Overview     Germine Detail	fw2. alex. fr	Requetes TCP	11-05-2005 16: 45: 49	11-05-2005 16: 50: 49	ENABLED	X
• Service Detail	srv1.alex.fr	Requetes DNS	11-05-2005 16: 46: 03	11-05-2005 16: 51: 03	ENABLED	X 🕅
Status Overview Status Summary	srv12.alex.fr	<u>Usage Disque dur par SNMP</u>	11-05-2005 16: 46: 41	11-05-2005 16: 51: 41	ENABLED	X
<ul> <li>Status Grid</li> <li>Status Map</li> </ul>	srv2.alex.fr	Connexions LDAP	11-05-2005 16: 46: 44	11-05-2005 16: 51: 44	ENABLED	XX
3-D Status Map	srv3.dmz.alex	fr Connexions POP3	11-05-2005 16: 46: 57	11-05-2005 16: 51: 57	ENABLED	XX
Service Problems Host Problems	srv4. dmz. alex	fr <u>Requetes vers le Proxy</u>	11-05-2005 16: 50: 13	11-05-2005 16: 52: 13	ENABLED	X
Network Outages	srv5.alex.fr	<u>Requetes web</u>	11-05-2005 16:47:24	11-05-2005 16: 52: 24	ENABLED	X
© Comments © Downtime	<u>srv6. alex. fr</u>	Requetes TCP SMB	11-05-2005 16:47:38	11-05-2005 16: 52: 38	ENABLED	XX
Process Info	srv7.alex.fr	CUPS	11-05-2005 16:47:41	11-05-2005 16: 52: 41	ENABLED	XX
Performance Info Scheduling Queue	switch2	<u>Ping du switch DMZ</u>	11-05-2005 16: 48: 05	11-05-2005 16: 53: 05	ENABLED	XX
Reporting	printer1	printer1	11-05-2005 16: 48: 19	11-05-2005 16: 53: 19	ENABLED	XX
• Trends	srv12.alex.fr	Connexion NFS	11-05-2005 16: 48: 19	11-05-2005 16: 53: 19	ENABLED	XX
Availability Alert Histogram	srv12.alex.fr	Espace disque dur par SMB	11-05-2005 16: 48: 46	11-05-2005 16: 53: 46	ENABLED	XX
Alert History	<u>srv2. alex. fr</u>	Requetes TCP SMB	11-05-2005 16: 49: 13	11-05-2005 16: 54: 13	ENABLED	XX
Notifications	<u>srv5. alex. fr</u>	Requetes DNS	11-05-2005 16: 49: 40	11-05-2005 16: 54: 40	ENABLED	XX
• Event Log	<u>srv6. alex. fr</u>	Connexions LDAP	11-05-2005 16: 49: 54	11-05-2005 16: 54: 54	ENABLED	X 🕅
Configuration	<u>srv12. alex. fr</u>	Charge CPU par SNMP	N/A	11-05-2005 17:00:00	ENABLED	XX
• view config	<u>srv12. alex. fr</u>	Utilisation RAM par SNMP	N/A	11-05-2005 17:00:00	ENABLED	XX
	srv9. dmz. alex	fr <u>Usage Disque dur par SNM</u> F	11-05-2005 16: 11: 51	11-05-2005 17:00:00	ENABLED	X 🕅

#### V. Installation et configuration N\$Client++

La supervision des machines Windows se fait grâce à l'agent NSClient++ qui doit être installé sur la machine distante à superviser.

"NSClient++" se base sur une architecture client/serveur. La partie cliente (nommée check\_nt), doit être disponible sur le serveur Nagios. La partie serveur (NSClient++) doit être installée sur chacune des machines Windows à surveiller.

#### 1. Installation

hercher 😥 [		
hercher 🏀 L		
	Jossiers View View View View View View View View	
Fichiers actu	I NSClient++ (Win32) Setun	
	End-User License Agreement	
15	Please read the following license agreement carefully	I.
NSClient++-0.		
	GNU GENERAL PUBLIC LICENSE	-
	Version 2, June 1991	
	Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St. Fifth Floor, Boston, MA, 02110-1301	
	Everyone is permitted to copy and distribute verbatim copies	
	or mis license document, but changing it is not allowed.	
	Preamble	
	The licenses for most software are designed to take away your	
	$\overline{arphi}$ I accept the terms in the License Agreement	
	Print Back Next	Cance
Old con	Figuration was not Found!	C
Î	nados server lol	
N	Schert exempted (only used via chark of):	
	And a best and fault and up a part of the	
100	Modules to load:	
	Enable common check plugins	
	Enable risdient server (check_nt)	
	Enable MRPE server (check_nrpe)	
	Enable NSCA client (dont enable unless you really use NSCA)	
	Enable WMI checks	
l		
l	Back Have Car	-

On saisit l'adresse ip de serveur nagios dans la case Aloowedhost .

On termine l'installation par start service et finish

#### 2. Configurer NSClient + +

Pour autoriser le service intégrer au bureau on passe a outils d'administration via panneau de configuration on sur services puis nsclient++

Double click et on activer

Nom 🛆	Description	État
🏶 Extensions du pilot	Fournit des informations de gestion du systèm	
🏶 Fournisseur de la p…	Assure la sécurité des programmes RPC (appel	
🍓 Gestion d'applications	Fournit des services d'installation de logiciels t	Démarré
🍓 Gestionnaire de co…	Stocke les informations de sécurité pour les co	Démarré
🍓 Gestionnaire de co	Crée une connexion vers un réseau distant à c	
🍓 Gestionnaire de co	Crée une connexion réseau.	
🍓 Gestionnaire de dis	Détecte et analyse de nouveaux lecteurs de di	Démarré
🍓 Gestionnaire de l'Al	Active le Gestionnaire de l'Album afin de stock	
🍓 Gestionnaire de ses	Gère et contrôle l'assistance à distance. Si ce s	
🍓 Horloge Windows	Conserve la synchronisation de la date et de l'	Démarré
🆓 Hôte de périphériq	Offre la prise en charge des périphériques hôt	
🆓 HTTP SSL	Ce service implémente le protocole sécurisé HT	
🍓 Infrastructure de g	Fournit une interface commune et un modèle o	Démarré
🆏 Journal des événe	Active les messages d'événements émis par le	Démarré
🆓 Journaux et alertes	Collecte les données de performances des ordi	
🆓 Lanceur de process	Fournit la fonctionnalité de lancement des serv	Démarré
🏶 Localisateur d'appel	Gère la base de données du service de nom RPC.	
🆓 Mises à jour autom	Active le téléchargement et l'installation des mi	Démarré
🆓 MS Software Shado	Gère les copies logicielles de clichés instantané	
🆏 NLA (Network Loca	Recueille et stocke les informations de configur	Démarré
🏶 Notification d'évén	Scrute les événements système tels que les ou	Démarré
🍓 NSClient++ (Win32)	Monitoring agent for nagios (and others) used	Démarré
🆏 Onduleur	Gère un onduleur connecté à l'ordinateur.	
🍓 Ouverture de sessi	Prend en charge l'authentification directe des	
🍓 Pare-feu Windows	Assure la traduction d'adresses de réseau, l'ad	Démarré

Éditez le fichier NSC.INIfile (situé dans le répertoire C:\NSClient++) et effectuez les changements suivants :

Décommentez tous les modules listés dans la section [modules], exceptés CheckWMI.dll et RemoteConfiguration.dll

Exigez optionnellement un mot de passe des clients en remplaçant l'option password dans la Section

Décommentez l'option allowed\_hosts dans la section [Settings]. Ajoutez l'adresse IP du serveur Nagios à cette ligne, ou laisser vide pour autoriser n'importe quel hôte à se connecter.

Assurez-vous que l'option port dans la section [NSClient] soit décommentée

Configurer le Pare-feu Windows pour permettre NSClient + + d'accès:

Exception à ajouter sur le pare-feu Windows pour autoriser l'accès à NSClient ++

📴 Pare-feu Windows	×
Général Exceptions Avancé	
Le Pare-feu Windows est désactivé. Votre ordinateur encourt des risques d'attaques et d'intrusions depuis des sources extérieures telles qu'Internet. Nous vous recommandons de cliquer sur l'onglet Général et de sélectionner Activé. Programmes et services :	
Nom	
Assistance à distance	
Bureau à distance	
Diagnostics du réseau pour Windows XP	
Infrastructure UPnP	
Rothage de fichiere et d'imprimentes	
Ajouter un programme Ajouter un port Modifier Supprimer	
Quels sont les risques liés à l'autorisation des exceptions ?	
OK Annuler	

On passe au serveur nagios de terminer la configuration

Ouvrez le fichier windows.cfg pour édition

#### Fedora: # vi /usr/local/nagios/etc/objects/windows.cfg

Ajouter une nouvelle définition d'hôte pour la machine Windows que vous souhaitez superviser. Si c'est la « première » que vous supervisez, vous pouvez simplement modifier l'exemple de définition d'hôte dans windows.cfg. Remplacez les champs host\_name, alias, et adressé par les valeurs appropriées pour votre machine Windows.



Maintenant vous pouvez ajouter quelques définitions de services (dans le même fichier de configuration) pour indiquer à Nagios de superviser différents aspects de la machine Windows.

Ajoutez la définition de service suivante pour contrôler la version de l'addonNSClient++ tournant sur le serveur Windows. Cela devient utile quand il s'agit de mettre à jour des serveurs Windows vers une nouvelle version de l'addon, en vous permettant de déterminer quelles sont les machines Windows nécessitant une mise à jour vers la dernière version de NSClient++.

# Create a service for monitori	ing the version of NSCLient++ that is installed
# Change the host_name to match	h the name of the host you defined above
define service{ use host_name service_description check_command }	generic-service winserver NSClient++ Version check_nt!CLIENTVERSION

Ajoutez la définition de service suivante pour superviser le temps écoulé depuis le dernier re/démarrage du serveur Windows.



Ajoutez la définition de service suivante pour superviser la charge CPU du serveur Windows et générer une alerte CRITICAL si la charge CPU des 5 dernières minutes est égale à 90% ou plus ou une alerte WARNING si la charge CPU des 5 dernières minutes est égale à 80% ou plus.

```
# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above
define service{
    use generic-service
    host_name winserver
    service_description CPU Load
    check_command check_nt!CPULOAD!-l 5,80,90
```

Voilà pour le moment. On a ajouté des services simples qui devraient être supervisés sur les machines Windows. Enregistrez le fichier de configuration.

Maintenant, il faut enregistrer le fichier et vérifier s'il n'a pas des erreurs avec la commande :

linux:~ # /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Pius redémarrer Nagios



Conclusion

Un logiciel de supervision de réseau comme Nagios est indispensable pour un administrateur lorsque le réseau devient complexe. Cela lui permet d'avoir une vue globale et en temps réel sur tout le parc informatique.

Mais cela nécessite une configuration qui devient elle aussi assez complexe en fonction du niveau de supervision que l'administrateur souhaite mettre en place. En effet, dans Nagios, il n'y a pas d'outils de simplification de la configuration, qui s'effectue entièrement par modification manuelle des fichiers de configuration.

Malheureusement nous avons estimé que la difficulté de configuration de Nagios n'était pas compensée par le service rendu à l'administrateur. Nous avons alors effectué des recherches pour savoir s'il existait des outils qui pourraient simplifier cette configuration.

Pour conclure, un projet comme celui-ci se révèle être une solution très intéressante au sein d'une entreprise, mais il ne doit pas être réalisée par n'importe qui, et ne constitue qu'un outil de travail pour un administrateur réseau. Il ne remplace en aucun cas celui-ci...