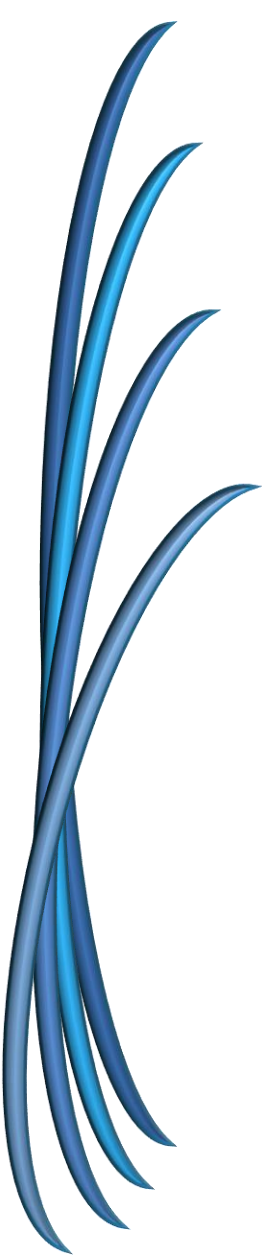


# La supervision

Un monde transverse





- SNMP
- Cacti
- Ecosystème Nagios
- Zabbix



[Cette photo](#) par Auteur inconnu est soumis à la licence [CC BY-SA-NC](#)



[Cette photo](#) par Auteur inconnu est soumis à la licence [CC BY-SA](#)

# SNMP

- Configurer votre agent SNMP sur Linux selon les URL suivantes, mais en adaptant les paramétrages à votre contexte (mot de passe, ... )
  - <https://blog.cedrictemple.net/341-configuration-avancee-de-snmp-sur-linux-snmpv3/>
  - <http://www.bortzmeyer.org/snmp-v3-inciga-cacti.html>
  - <http://wiki.linuxwall.info/doku.php/fr:ressources:dossiers:supervision:snmpv3>



# /etc/snmp/snmpd.conf

- Directives :
  - rouser <utilisateur> priv
  - createUser <utilisateur> SHA <supermotdepasse> AES <superpassphrase>
  - syslocation Paris, France
  - syscontact adresse@email.com



# snmpwalk ou snmpget

- `snmpwalk -v3 -l <noAuthNoPriv|authNoPriv|authPriv> -u <username> [-a <MD5|SHA>] [-A <authphrase>] [-x DES] [-X <privaphrase>] <ipaddress>[:<dest_port>][oid]`

Exemple:

- `snmpwalk -v3 -l authPriv -u snmpadmin -a MD5 -A PaSSword -x DES -X PRlVPassWord 127.0.0.1:161 system`

```
$ snmpwalk -v 3 -u <utilisateur> -l authPriv -a SHA -A <supermotdepasse> -x AES -X <superpassphrase> 127.0.0.1
```

```
$ snmpget -v 3 -u <utilisateur> -l authPriv -a SHA -A <supermotdepasse> -x AES -X <superpassphrase> 127.0.0.1 sysUpTime.0
```

*DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (107614) 0:17:56.14*

```
$ snmpget -v 3 -u <utilisateur> -l authPriv -a SHA -A <supermotdepasse> -x AES -X <superpassphrase> 127.0.0.1 sysUpTime.0
```

*DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (107614) 0:17:56.14*



# Analyse de configuration

rouser test priv system

rouser youpi noauth system

createUser test SHA testmotdepasse AES testpassphrase

createUser youpi

syslocation Paris, France

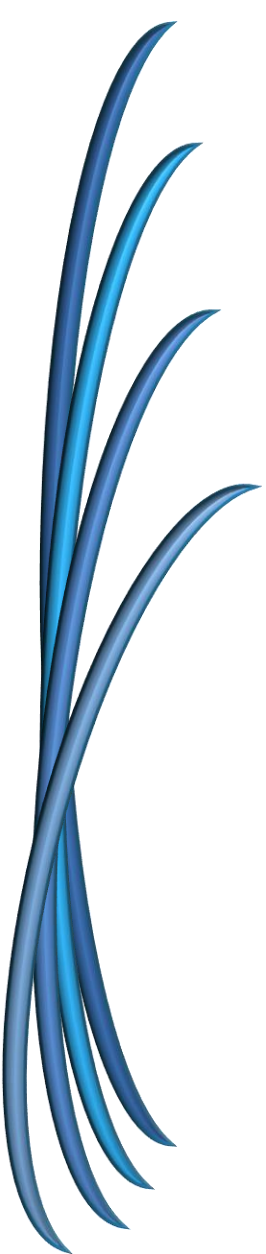
syscontact adresse@email.com



# Travaux pratiques

- Configurer votre agent SNMP sur équipement Linux
- Tester avec les commandes snmpwalk et snmpget le bon fonctionnement





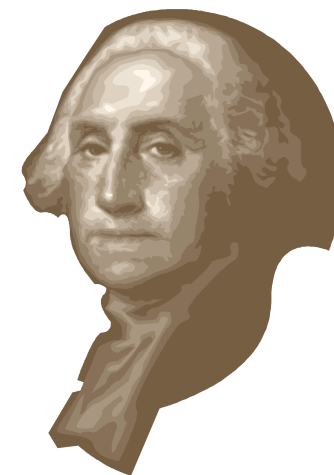
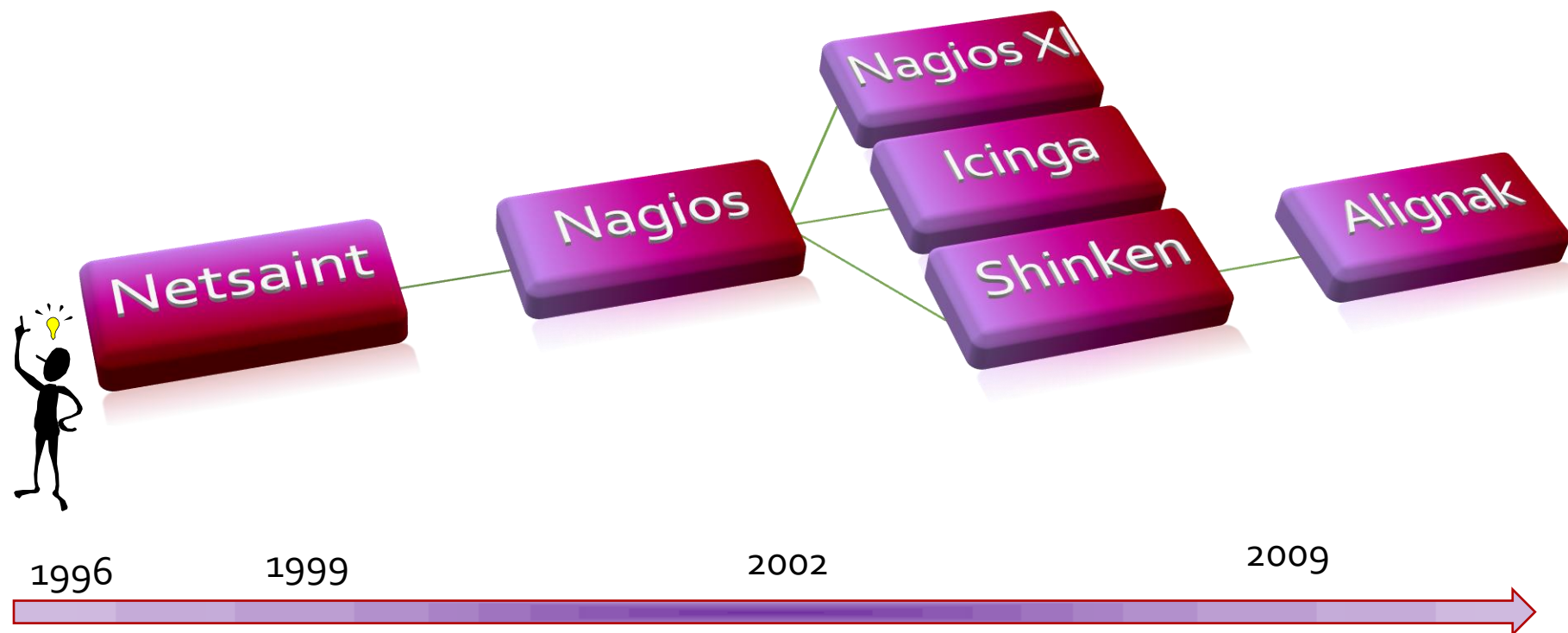
# Bref historique

Eco-système Nagios



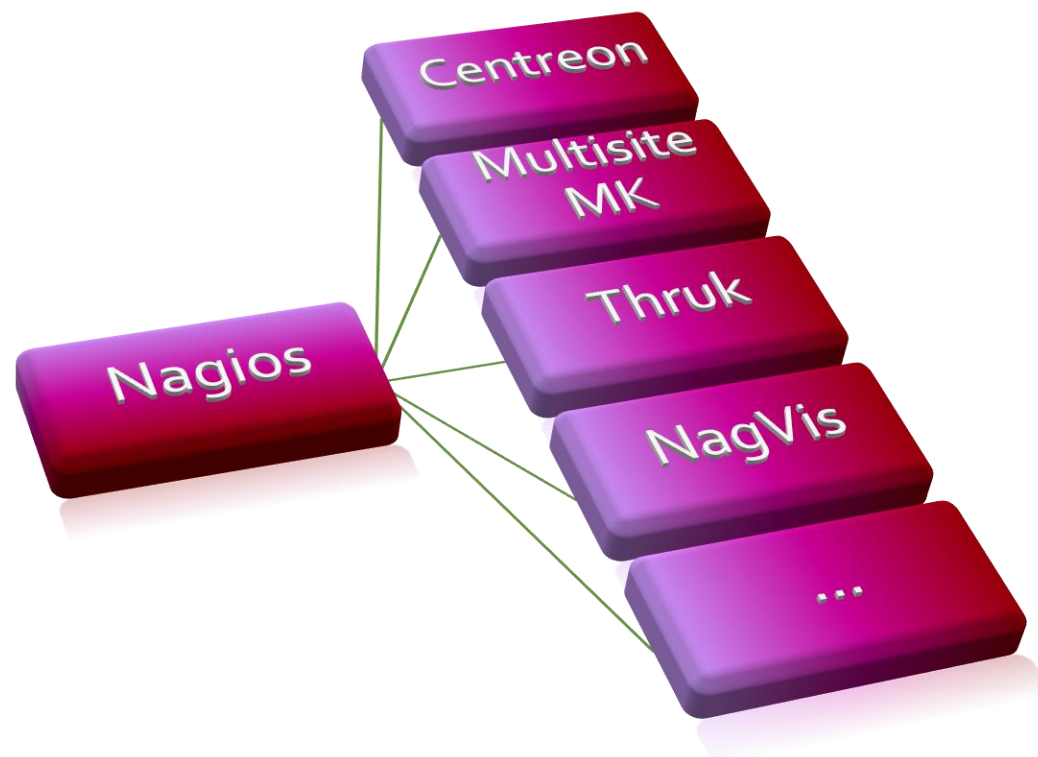


# D'où je viens ? Dans quel état j'erre ?

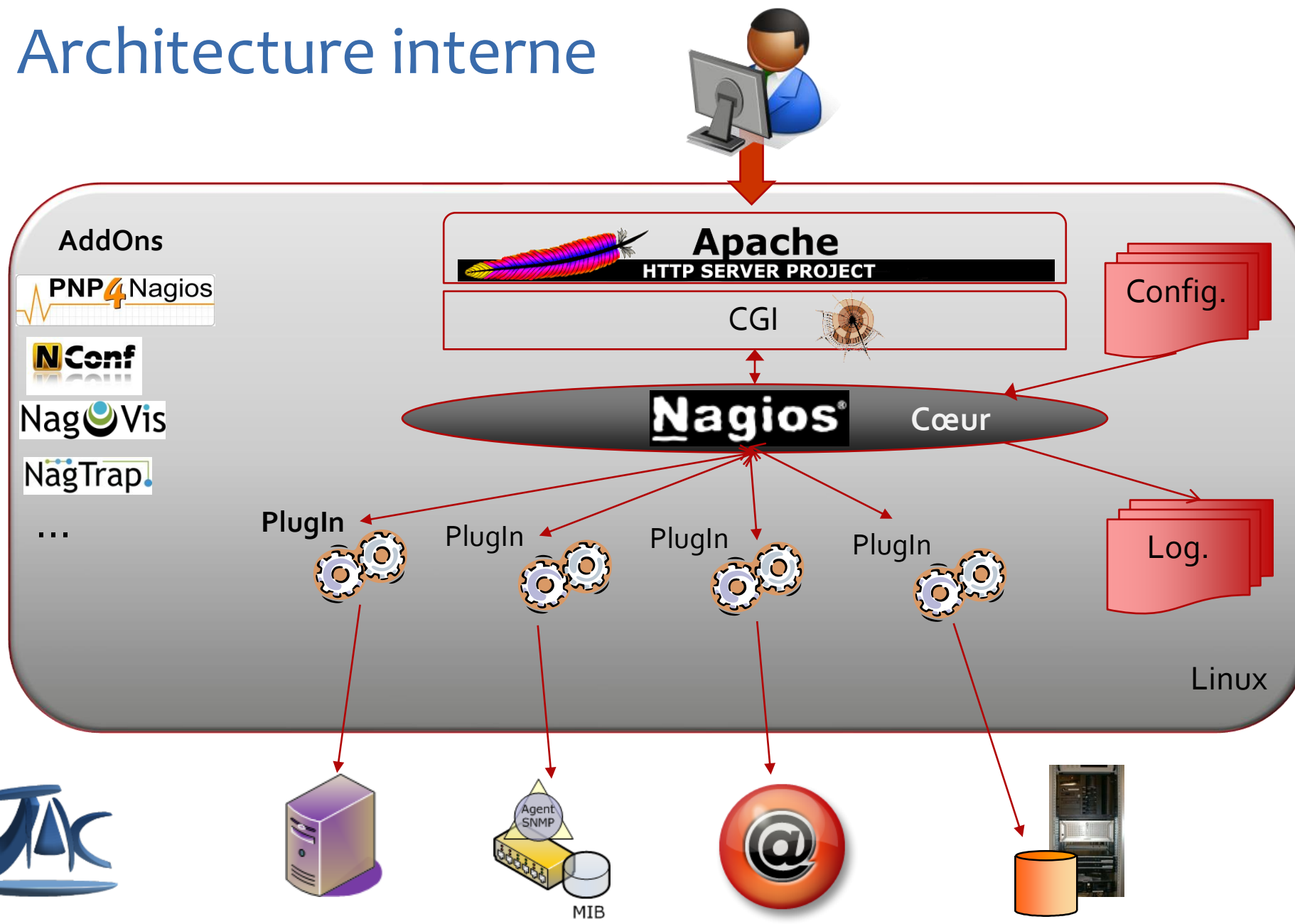


# Greffons

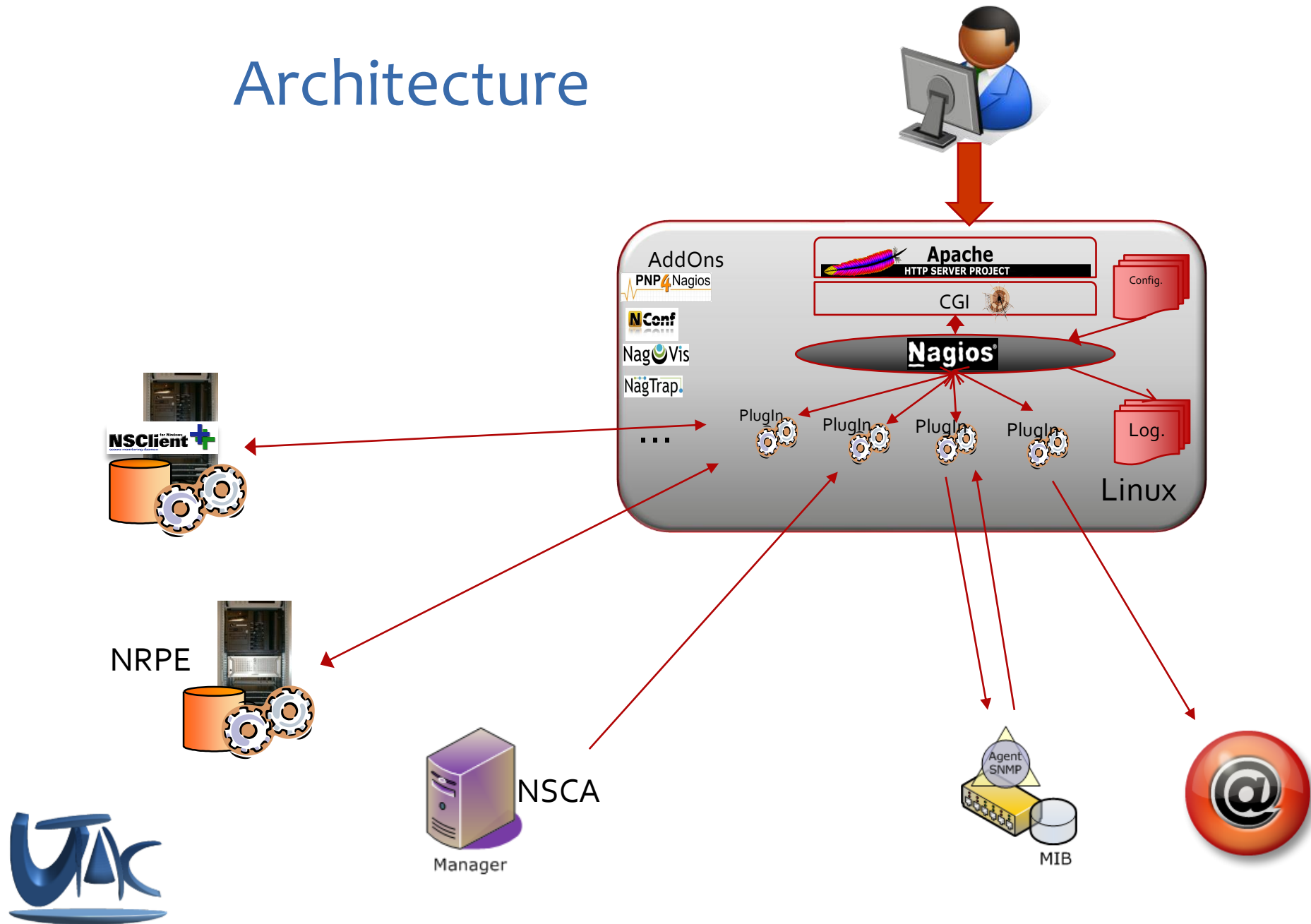
- IHM
  - L'influence de certaines fonctions masque ensuite le cœur



# Architecture interne



# Architecture



# Notion de PlugIn (1)

- Modules externes
  - Rôle :
    - effectuer une surveillance spécifique
    - Interface standardisée avec Nagios
      - Code retour + texte
      - Fournissent de + en + des informations de performances (optionnelles)
  - Langages : Perl, Shell, Python, C compilé, ...
- La distribution d'accompagnement standard  
<http://www.nagios.org/download/plugins>



# Notion de PlugIn (2)

- Plusieurs catégorisations
  - Contrôle des ressources locales
    - Ressources système (CPU, charge, mémoire, pagination, espace disque, les io disques...)
      - ✓ check\_load, check\_cpu, check\_swap, check\_mem, check\_disk, check\_io, ...
    - Contrôle de la présence d'un fichier, de la taille d'un fichier ou d'un répertoire, du nombre de fichier dans un répertoire, ...
      - ✓ check\_file , check\_file\_age, check\_file\_size, check\_dirsize, CheckFileCount
  - Contrôle des ressources matérielles
    - souvent lié à l'interfaçage avec les logiciels constructeurs (HP Insight Manager, Dell Open Manager, IBM Netfinity, ...)
      - ✓ check\_openmanage, check\_sun\_raidctl, check\_ccis, ...
  - Contrôle des applications locales
    - Surveillance des processus, du contenu des fichiers de journalisation, ...
      - ✓ check\_procs, check\_logs2, check\_log\_windows, ...





# Notion de PlugIn (3)

- Contrôles des services distants
  - Service ftp, smtp, pop, dhcp, dns, ...
    - ✓ check\_tcp, check\_udp, check\_dhcp, check\_smtp, check\_http, ...
  - Service distant pour les bases de données
    - ✓ check\_oracle, check\_mysql, check\_pgsql, ...
- Contrôle des équipements à distance
  - Contrôle générique
    - ✓ check\_icmp, check\_fping, check\_ping, check\_snmp, ...
  - Contrôle plus spécifique à distance
    - ✓ Imprimantes HP
      - check\_hpjd
    - ✓ Ressources systèmes
      - check\_snmp\_load, check\_snmp\_mem, check\_snmp\_storage
    - ✓ Partage réseau
      - check\_smb
    - ✓ Processus / Services (au sens Windows)
      - check\_snmp\_win, check\_win\_process, check\_process\_by\_ssh



## Notion de PlugIn (4)

- Problématique : identifier, intégrer les bons plug-ins, ... voire développer
- Une référence :



<http://exchange.nagios.org/directory/Plugins>





# Notion de greffon (« Add-On »)

- Avec la distribution officielle
  - <http://www.nagios.org/download/addons>
    - L'agent NRPE
    - L'agent NSCA
    - Le socle et les utilitaires NDOUtils
- Les add-ons ou greffons apportent à Nagios
  - NagVis : Une cartographie Web 2.0
  - NagTrap : Une gestion des traps SNMP
  - PnP : Une gestion des graphes de performance
  - Nconf : Une gestion graphique de la configuration
  - NagiosBP : Une gestion des « Business View »
  - NaReTo : Une gestion de la performance et des alarmes
  - ...
  - Bref, tout comme pour les PlugIns, une multitude de fonctionnalités, parfois redondantes...
  - ... il faut également faire son tri.

<http://exchange.nagios.org/directory/Addons>



# Hôtes, Services, Regroupement

- Au sein de Nagios, on définit :
  - Les hôtes (« hosts »), c'est-à-dire les machines à surveiller
  - Les services (« services »), sont les points de contrôle qui seront effectués sur les différents hôtes.
- Notion de regroupement :
  - Groupe d'hôtes (« hostgroups »)
  - Groupe de services (« servicegroups »)
  - Facilite l'exploitation en synthétisant la représentation
  - Facilité l'administration en évitant les duplications de configuration



# Surveillance active/passive

- 2 concepts sont également importants à connaître :
  - Surveillance active :
    - le mécanisme de surveillance fait partie intégrante de Nagios et de son paramétrage. L'architecture de supervision Nagios est à l'initiative du contrôle.
    - La surveillance peut être :
      - ✓ directe
      - ✓ avec rebond (ou proxy)
  - Surveillance passive :
    - Nagios reste dans ce cas à l'écoute d'éventuels événements
      - ✓ Événements SNMP
      - ✓ Événements NSCA



# Surveillance active

- « check\_command »
  - Nagios définit en son sein des commandes de contrôle nommées « check\_command »
  - Les « check\_command » font le lien avec les Plugins
  - Ils renvoient un code retour permettant de déterminer l'état du composant surveillé

**Nagios**<sup>®</sup>

check\_command

Plugins

- Exemples :
  - « check\_ping » fait partie de la surveillance active
  - Le rôle de Nagios : planifier l'exécution du contrôle



# Surveillance passive



- Exemple :

- Les sauvegardes :

- lorsque l'on veut contrôler la bonne réalisation des sauvegardes, il pourrait être choisi, fonction des aléas de durée des sauvegardes, que l'envoi de l'événement de fin de réalisation de la sauvegarde (bon ou mauvais) soit à l'initiative du logiciel de sauvegarde.

Cette photo par  
Auteur inconnu  
est soumise à la  
licence [CC BY-SA](#)

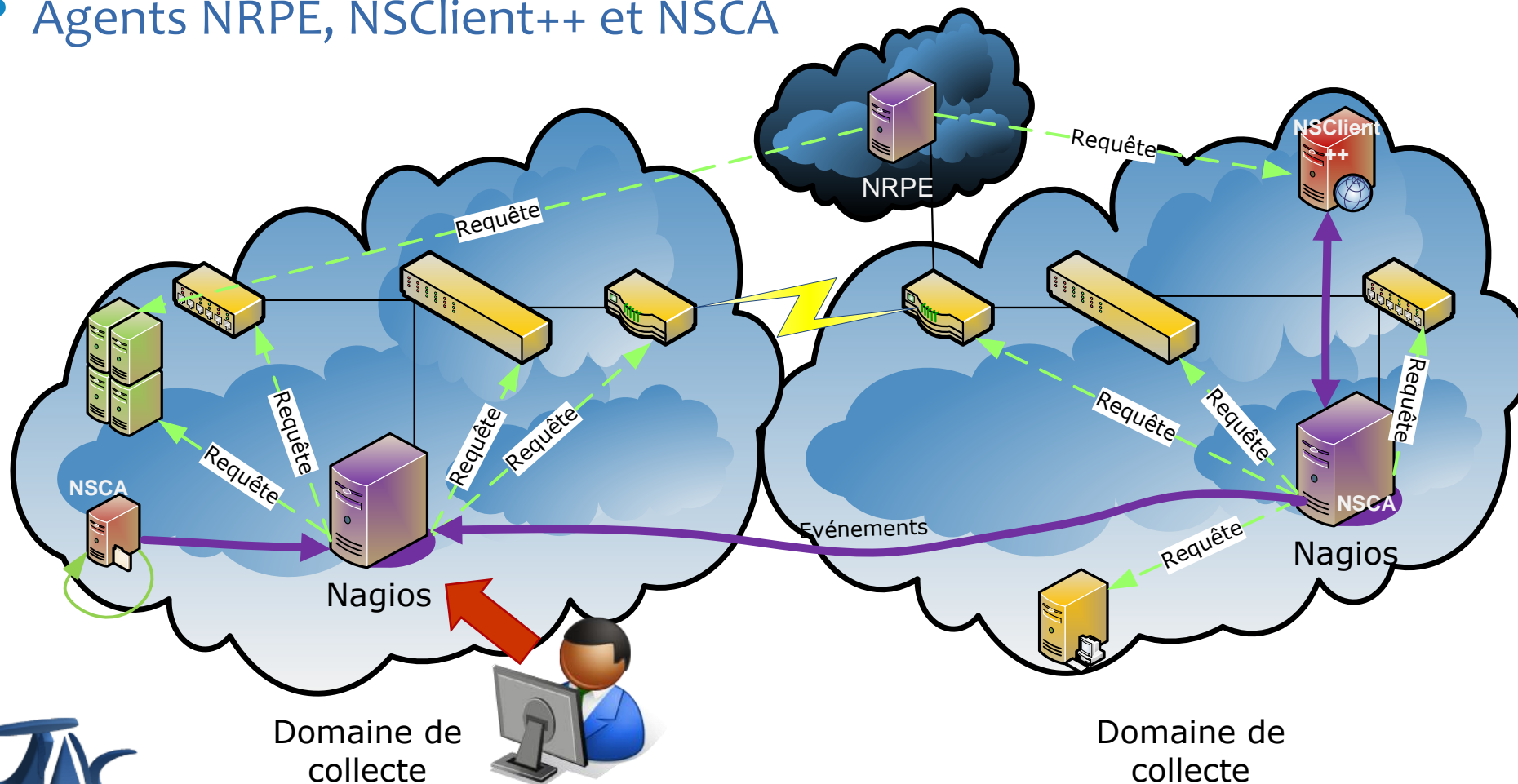
- L'ordonnancement et la planification

- La surveillance passive est souvent également présente dans les processus de production informatique, car celle-ci est de plus en plus événementiel. Si l'outil de supervision est fédérateur des événements, il peut se mettre à l'écoute des événements en provenance des chaînes de traitement, sans pour cela être ou remplacer l'outil de planification et d'ordonnancement.



# Surveillance « distribuée »

- Agents NRPE, NSClient++ et NSCA



# Les notifications

- Nagios
  - est un gestionnaire d'état
  - n'est pas un gestionnaire d'événements (pas de gestion du cycle d'un événement avec des notions d'appropriation, d'acquittement, ...)
- Notifications
  - d'où la présence des notifications
  - Interface avec :
    - la gestion des événements
    - la gestion des incidents
    - la gestion des astreintes



[Cette photo](#) par  
Auteur inconnu est  
soumis à la licence [CC](#)  
[BY-SA](#)





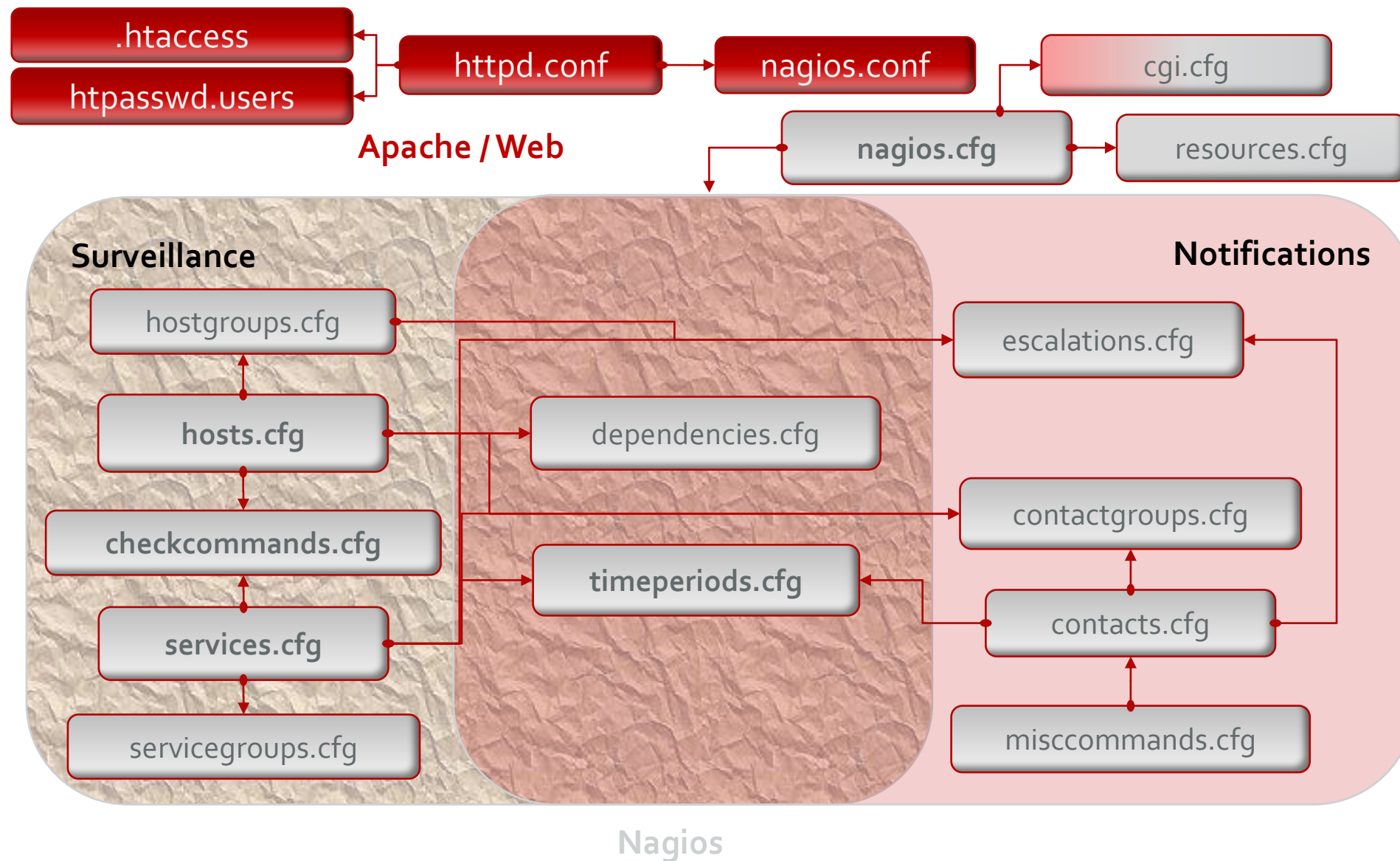
# Vue d'ensemble

- 2 gestions de configurations
  - Configuration du service Web Apache pour la sécurisation des accès
  - Configuration de Nagios, pour les politiques de surveillance et de notification et précision pour les permissions d'accès à certaines fonctions
- Configuration de Nagios
  - Pour des petites configurations
    - Tout peut être décrit dans « nagios.cfg »
  - Pour les configurations plus importantes et la structuration
    - Gestion de plusieurs fichiers de configuration





# Vue d'ensemble



# Les fichiers

- Que se passe-t-il si je définis plusieurs fois la même chose dans mon arborescence de fichier ?
  - L'exécution de « nagios » ne pourra s'effectuer
  - La méthode est de contrôler en amont la conformité de ma configuration

« nagios -v <RepInstallNagios>/etc/nagios.cfg »



# Le fichier principal

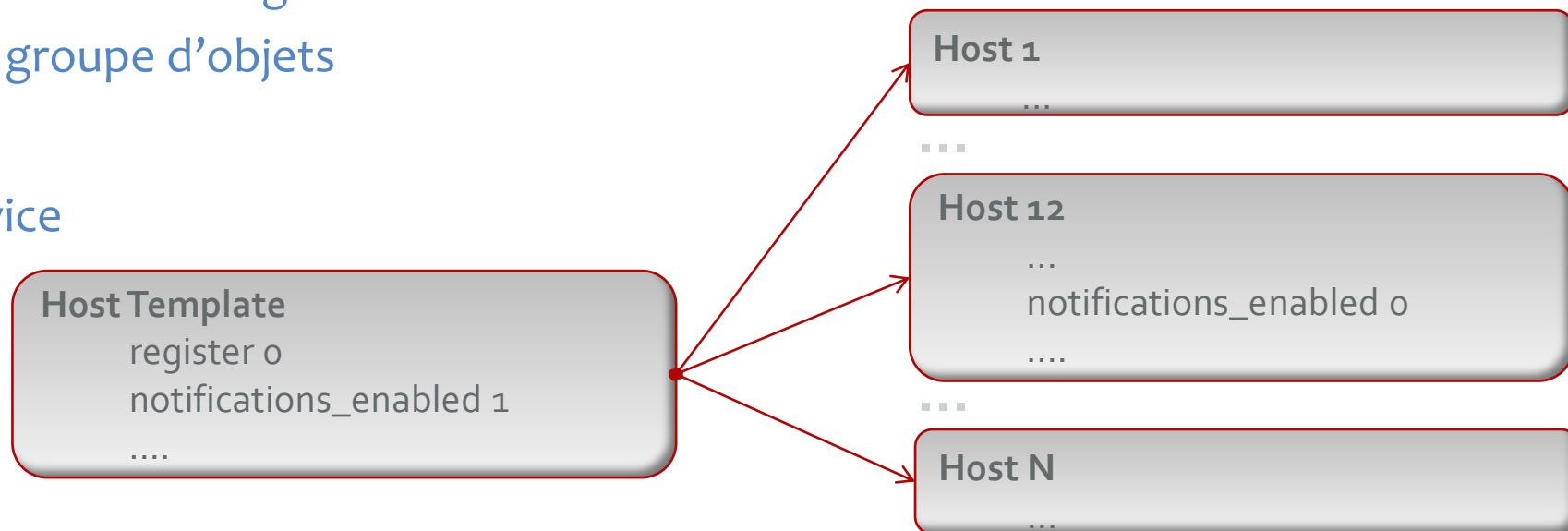
- « nagios.cfg »
  - Fichier principal, car c'est par défaut ce fichier que le processus « nagios » va aller lire
  - Il définit
    - les autres fichiers de configuration à prendre en compte
      - ✓ Variables « cfg\_dir » et « cfg\_file »
        - cfg\_dir=/usr/local/nagios/etc/global
        - cfg\_file=/usr/local/nagios/etc/objects/contacts.cfg
    - les paramètres globaux
      - ✓ La définition des fichiers de journalisation, d'archives, de cache, de statut, les comptes de soumission, fichier de « lock », temporaire, ...
        - log\_file=/usr/local/nagios/var/nagios/nagios.log
        - status\_file=/usr/local/nagios/var/status.dat
        - nagios\_user=nagios
        - nagios\_group=nagios

# nagios.cfg



# Les modèles (« templates »)

- Principe
  - Mutualisation de directive commune
  - Héritage sur les objets fils
- Intérêt
  - Simplification de la configuration
  - Gestion par groupe d'objets
- Application
  - Hôte & Service
- Exemple



# Formalisme des définitions

- Pour l'ensemble des objets définis, le principe syntaxique est :

```
define <Type d'objet>{  
    directive1 valeur  
    directive2 valeur    ; Commentaire  
    ...  
}
```

Exemple :

```
define command{  
    command_name <commandname>  
    command_line    <commandline>  
}
```



# Objet « command »

- « Command »
  - C'est donc la base, la référence à la commande qui sera appelée pour effectuer le contrôle
  - Fournit en standard, nous avons des plugins auxquels nous pouvons faire référence
    - Exemple : contrôle snmp avec le plugin check\_snmp

```
define command {  
    command_name check_snmp  
    command_line $USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$  
}
```

- La ligne de commande fait référence à des macros
  - Celles-ci sont valorisées avant le lancement de la commande
  - Exemple : \$USER<n> \$HOSTADDRESS\$ \$HOSTNAME\$ \$ARG<n>\$

**checkcommands.cfg**



# La définition d'un hôte (1)

- On rappelle que la syntaxe permet de définir un hôte ou un modèle d'hôte (« host\_template »)

```
define host{  
    host_name      host_name  
    alias          alias  
    address        address  
    check_command  check-host-alive  
    max_check_attempts #  
    check_period   timeperiod_name  
    [contact|contact_groups] [contact|contact_groups]  
    notification_interval #  
    notification_period  timeperiod_name  
    notification_options [d,u,r,f]  
}
```

hosts.cfg





# La définition d'un hôte (2)

```
define host {  
    host_name      www.matrics.fr  
    alias          Internet_ICS  
    address        193.33.79.70  
    check_command  check-host-alive  
    notification_interval 15  
    notification_options d,u,r  
    max_check_attempts 3  
    active_checks_enabled 1  
    passive_checks_enabled 0  
    notifications_enabled 1  
    check_period      24x7  
    notification_period 24x7  
    parents           cisco_800  
    use               Default_monitor_server  
    contact_groups    admins  
}
```





# La définition d'un service (1)

- Dans le même esprit que l'hôte :

```
define service{  
    host_name                host_name  
    service_description      service_description  
    check_command             command_name  
    max_check_attempts        #  
    normal_check_interval     #  
    retry_check_interval      #  
    check_period              timeperiod_name  
    notification_interval     #  
    notification_period       timeperiod_name  
    notification_options      [w,u,c,r,f]  
    contact_groups            contact_groups  
}
```

**services.cfg**



# La définition d'un service (2)

```
define service {  
    service_description      check_snmp  
    check_command            check_snmp!-C public -o sysUpTime.o  
    host_name                ncypher  
    check_period             24x7  
    notification_period      24x7  
    event_handler_enabled    0  
    notification_interval    15  
    notification_options      w,u,c,r  
    max_check_attempts       3  
    check_interval           5  
    retry_interval           1  
    active_checks_enabled    1  
    passive_checks_enabled   0  
    notifications_enabled    1  
    check_freshness          0  
    freshness_threshold       86400  
    contact_groups            admins  
}
```



# Les groupes

- Groupe d'hôtes

```
define hostgroup {  
    hostgroup_name hostgroup_name  
    alias           Nom long  
    members         Liste des hôtes membres séparés par le caractère « , »  
}
```

- Groupe de services

```
define servicegroup {  
    servicegroup_name servicegroup_name  
    alias             Nom long  
    members           Liste des services membres séparés par le caractère « , »  
}
```

- Exemple

```
define hostgroup {  
    hostgroup_name switches  
    alias          Network Switches  
    members        switch_Dell,switch_des3526  
}
```

hostgroups.cfg

servicegroups.cfg



# Calendrier (« timeperiod »)

- On définit des calendriers tant pour
  - gérer et optimiser les périodes de contrôle ;
  - gérer et optimiser les périodes de notification.

```
define timeperiod {  
    timeperiod_name workhours  
    alias           Normal Work Hours  
    monday         09:00-12:00,14:00-18:00  
    tuesday        09:00-12:00, 14:00-18:00  
    wednesday      09:00-12:00, 14:00-18:00  
    thursday       09:00-12:00, 14:00-18:00  
    friday         09:00-12:00, 14:00-18:00  
}
```

**timeperiods.cfg**





# Contact

- Personne susceptible d'être contacté pour le traitement d'un événement.

```
define contact{  
    contact_name          contact_name  
    alias                  alias  
    contactgroups          contactgroup_names  
    host_notifications_enabled [0/1]  
    service_notifications_enabled [0/1]  
    host_notification_period      timeperiod_name  
    service_notification_period  timeperiod_name  
    host_notification_options    [d,u,r,f,s,n]  
    service_notification_options [w,u,c,r,f,s,n]  
    host_notification_commands  command_name  
    service_notification_commands  command_name  
}
```

**contacts.cfg**



# Groupe de contact

- Définition d'un ensemble de contact
  - La définition peut se faire par
    - niveau
    - technologie
    - combiné les 2
  - Elle est souvent très associée à l'organisation humaine exploitant les événements, incidents et problèmes.

**contactgroups.cfg**

```
define contactgroup{  
    contactgroup_name    contactgroup_name  
    alias                alias  
    members              contacts  
    contactgroup_members contactgroups  
}
```



# Travaux pratiques

- But
  - Faire une première configuration simple
- Lab
  - Editer Nagios.cfg et créer la structure des fichiers de configuration
  - Définir (ou trouver) la commande pour la surveillance par ping
  - Définir un Host pour la machine locale
  - Définir un Service pour surveiller Sntp (Port TCP 25)
  - Définir un contact et groupe de contacts pour notifier à root
  - Vérifier la configuration : `nagios -v nagios.cfg`
  - Lancer Nagios et consulter le résultat via l'interface Web
  - Arrêter Sendmail et vérifier la notification



# Les agents

- Surveillance active avec agent passif
  - Cible Unix : NRPE
  - Cible Windows : NSClient++
- Surveillance passive
  - NSCA : configuration



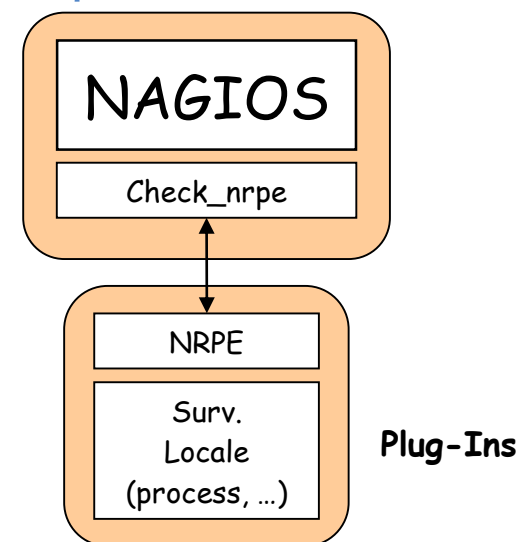


# NRPE : configuration

- Principe

- Passage de commande par Nagios via check\_nrpe
- Nrpe active le plug-in localement et renvoie la réponse
- Configuration

- Générale : communication  
check\_nrpe / nrpe
- Commandes sur le système  
distant nrpe
- Commandes sur le serveur Nagios



# NRPE : configuration générale

- Configuration générale : nrpe.cfg
  - server\_port=5666
  - allowed\_hosts=127.0.0.1 ; Serveurs Nagios
  - nrpe\_user=nagios
  - nrpe\_group=nagios
  - dont\_blame\_nrpe=1 ; Autorise le passage d'arg.
  - debug=0
  - command\_timeout=60
  - include=nrpe\_commands.cfg
- Chiffrement : codé en dur dans le fichier dh.h utilisé à la compilation ...



# NRPE : configuration générale

- Lancement par xinetd : /etc/xinetd.d/nrpe

```
service nrpe
{
    flags      = REUSE
    type       = UNLISTED
    port       = 5666
    socket_type = stream
    wait       = no
    user       = nagios
    group      = nagios
    server      = /usr/sbin/nrpe
    server_args = -c /etc/nagios/nrpe.cfg --inetd
    log_on_failure += USERID
    disable    = no
    only_from  = 127.0.0.1
}
```



# NRPE : commandes NRPE

- Commandes sur le système NRPE
- Syntaxe différente des commandes Nagios
- Deux cas
  - `dont_blame_nrpe=0` : pas de passage d'arguments  
`command[check_disk]=/usr/lib/nagios/plugins/check_disk -w 20 -c 10 -p /`
  - `dont_blame_nrpe=1` : passage autorisé d'arguments  
`command[check_disk]=/usr/lib/nagios/plugins/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$`
- Que faire ?
  - Autoriser le passage d'arguments pour centraliser la configuration
  - Sauf impératifs spécifiques de sécurité



# NRPE : commandes Nagios

- Commandes sur le serveur Nagios

# 'check\_nrpe\_disk' command definition

```
define command{
```

```
    command_name          check_nrpe_disk
```

```
    command_line          $USER1$/check_nrpe -H $HOSTADDRESS$ -t 60 -c check_disk -a $ARG1$  
                          $ARG2$ $ARG3$
```

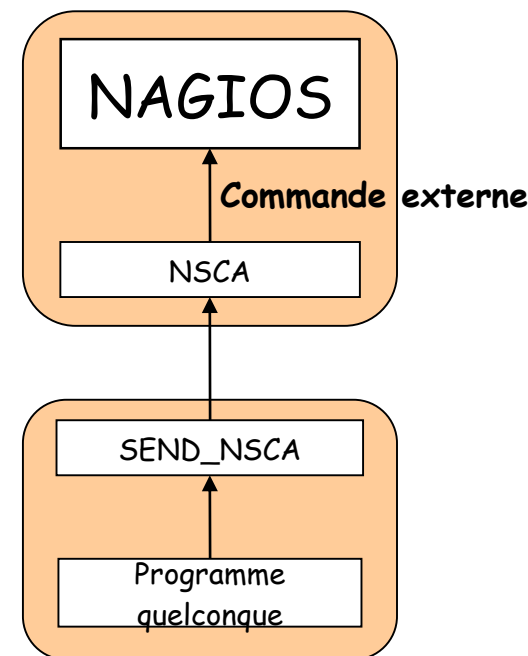
```
}
```



# NSCA : configuration

- Principe

- Passage de commande par `send_nsca` sur le système distant
- NSCA réceptionne la commande et la passe à Nagios via les commandes externes.
- Configuration
  - Générale : communication  
`send_nsca / nsca`



# NSCA : configuration générale

- Configuration générale : nsca.cfg
  - server\_port=5667
  - allowed\_hosts=127.0.0.1 ; Serveurs Nagios
  - nsca\_user=nagios
  - nsca\_group=nagios
  - debug=0
  - command\_file=/var/log/nagios/rw/nagios.cmd
  - password=matrice ; clé commune
  - decryption\_method=3 ; Algorithme





# NSCA : configuration générale

- Lancement par xinetd : /etc/xinetd.d/nsca

```
service nrpe
{
    flags      = REUSE
    type       = UNLISTED
    port       = 5667
    socket_type = stream
    wait       = no
    user       = nagios
    group      = nagios
    server     = /usr/sbin/nsca
    server_args = -c /etc/nagios/nsca.cfg -inetd
    log_on_failure += USERID
    disable    = no
    only_from  = 127.0.0.1
}
```



# NSCA : configuration send\_nsca

- Configuration de send\_nsca : /etc/nagios/send\_nsca.cfg
  - password=matrics ; clé commune
  - decryption\_method=3 ; Algorithme
- Mêmes valeurs que dans nsca.cfg sur le serveur Nagios ...
- Passage de commandes :
  - Service Check :  
<host\_name>[tab]<svc\_description>[tab]<return\_code>[tab]<plugin\_output>[newline]
  - Host Check : <host\_name>[tab]<return\_code>[tab]<plugin\_output>[newline]



# NSCA : exemple send\_nsca

- Soumission de Service Check

```
echo -e "chene\tRoot Partition\t2\tTest nsca\n" | send_nsca -H chene  
-c /etc/nagios/send_nsca.cfg
```

- Soumission de Host Check

```
echo -e "chene\t1\tTest nsca\n" | send_nsca -H chene -c  
/etc/nagios/send_nsca.cfg
```



# Travaux Pratiques



- But
  - Configurer NRPE et NSCA
  - Faire fonctionner une commande simple
- TP
  - Faire la configuration de base de NRPE
  - Intégrer une commande de vérification de disque de bout en bout
  - Faire la configuration de base de NSCA et send\_nsca
  - Tester le passage de commandes et vérifier sur l'interface graphique
- Recherche
  - Effectuer une recherche pour savoir s'il existe un autre agent que les agents précités



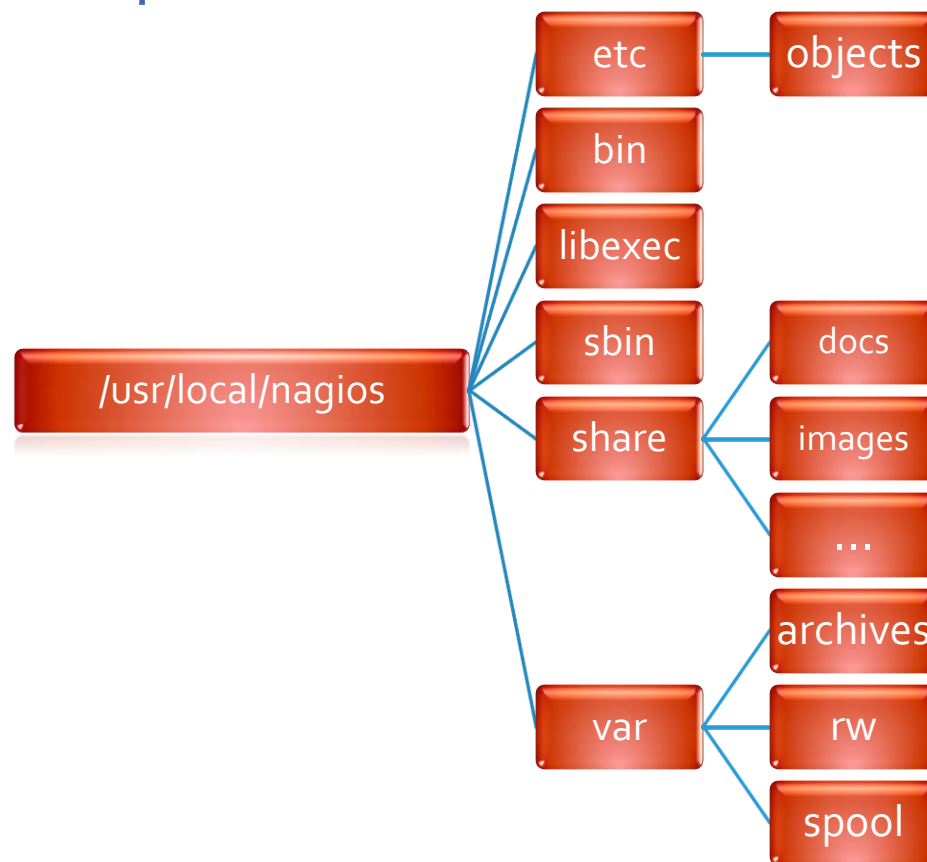
# Installation

- <https://djibril.developpez.com/tutoriels/linux/nagios-pour-debutant/>



# Répertoires et fichiers

- Dans une distribution compilée



# /usr/local/nagios/var

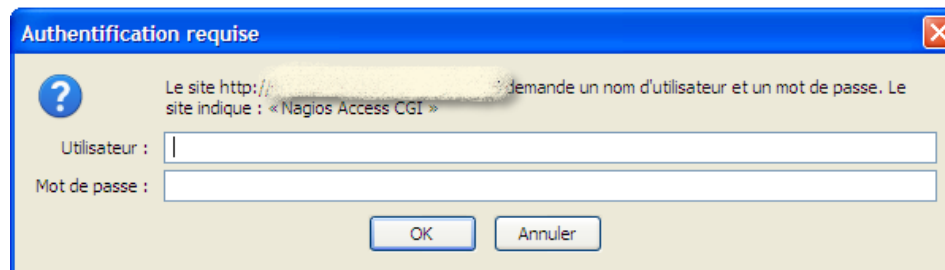
- Fichier de journalisation
  - « nagios.log »
- Fichiers de fonctionnement
  - « retention.dat » : fichier de conservation des données lors d'un crash ou d'un arrêt de Nagios
  - « status.dat » : fichier de stockage des états de Nagios et des données complémentaires
  - « spool/checkresults » recueille le résultat des différents contrôles.





# Pour y accéder

- Interface Full Web d'exploitation
- En configuration standard, cela peut dépendre du système d'exploitation
  - RedHat / Ubuntu
    - `http://<NomServeur|@IP>/nagios`
  - Debian
    - `http://<NomServeur|@IP>/nagios2`
- En configuration spécifique
  - Cela peut être ce que l'installateur a décidé
- Authentification
  - Active ou non active




The screenshot shows a standard Windows-style dialog box titled "Authentification requise". It contains a question mark icon and a message in French: "Le site http://... demande un nom d'utilisateur et un mot de passe. Le site indique : « Nagios Access CGI »". Below the message are two input fields labeled "Utilisateur :" and "Mot de passe :". At the bottom right, there are two buttons: "OK" and "Annuler".



# Vision générale

- Une page d'accueil et un menu général découpé en 4 sections



**General**

- Home
- Documentation
- NagTrap
- NagVis
- NConf
- Cacti
- PNP

**Current Status**

- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
  - Services (Unhandled)
  - Hosts (Unhandled)
  - Network Outages

Quick Search:

**Reports**

- Availability
- Trends
- Alerts
  - History
  - Summary
  - Histogram
- Notifications
- Event Log

**System**

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

**General**

- Home
- Documentation
- NagTrap
- NagVis
- NConf
- Cacti
- PNP

**Current Status**

- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
  - Services (Unhandled)
  - Hosts (Unhandled)
  - Network Outages

Quick Search:

# Nagios®

Nagios® Core™  
Version 3.2.0

August 12, 2009

[Check for updates](#)

[Read what's new in Nagios Core 3](#)

A new version of Nagios is available!

Visit [nagios.org](#) to download Nagios 3.2.1.

Copyright © 2009 Nagios Core Development Team and Community Contributors.  
Copyright © 1999-2009 Ethan Galstad.  
See the THANKS file for more information on contributors.

Nagios Core is licensed under the GNU General Public License and is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Nagios Core and the Nagios logo are trademarks, servicemarks, registered trademarks or registered servicemarks owned by Nagios Enterprises, Inc. Nagios marks are governed by our [trademark policy](#).

Nagios®  
Enterprises

MONITORED BY  
Nagios®  
NAGIOS CORE

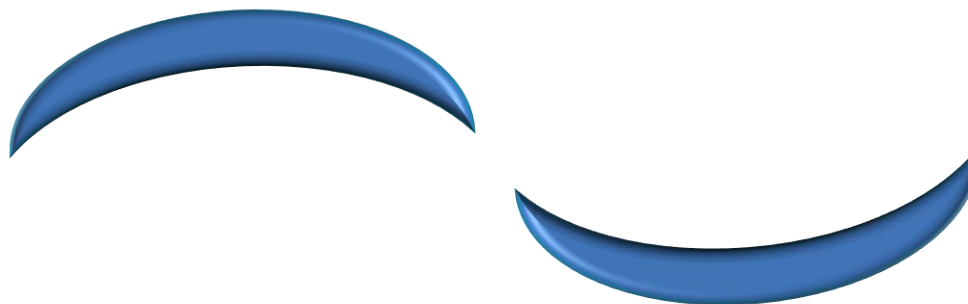
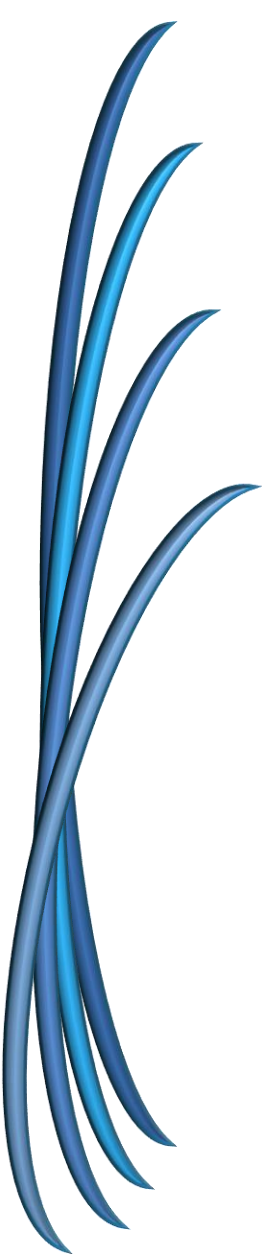
SOURCEFORGE.NET

**Reports**

- Availability
- Trends
- Alerts
  - History
  - Summary
  - Histogram
- Notifications
- Event Log

**System**

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration



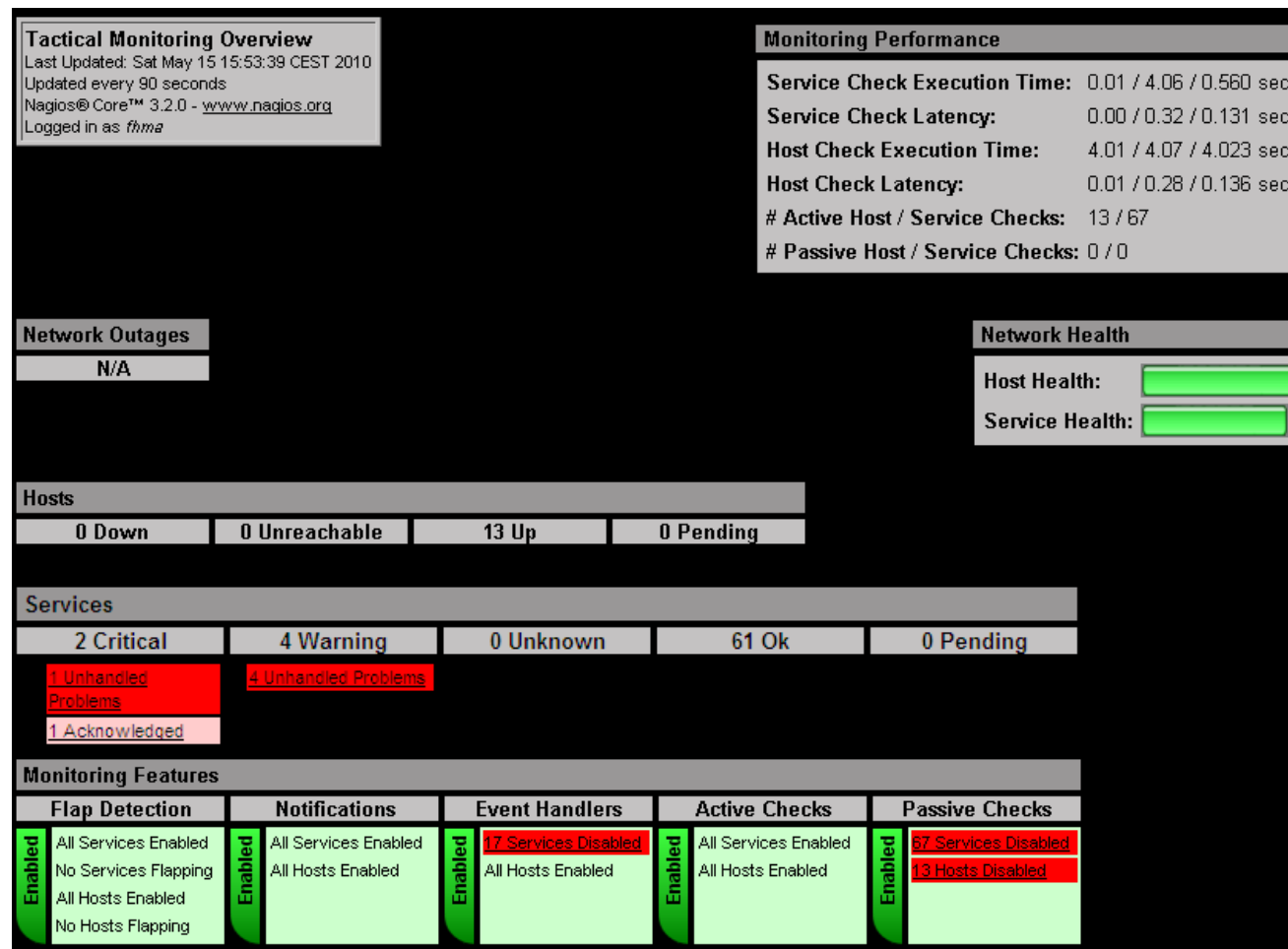
# Exploitation

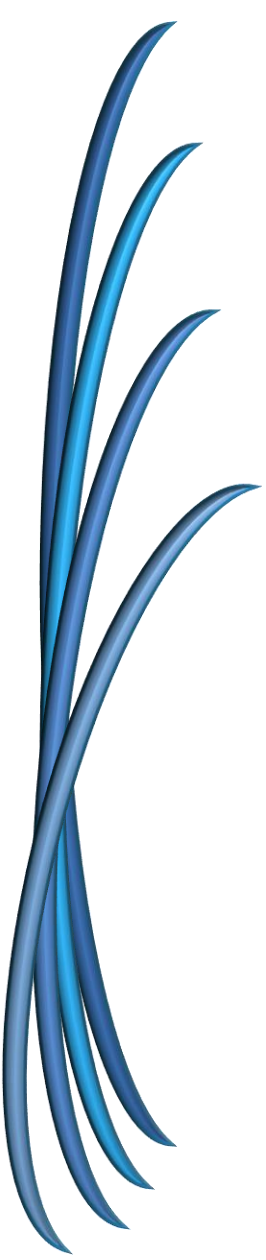
Interface graphique



# Vue d'ensemble ou tactique de la surveillance

- « Tactical Overview »





# Les états des hôtes

- « Tactical Overview »

- Chaque hôte supervisé peut prendre 4 états

1. « Up » : opérationnel
2. « Down » : non opérationnel
3. « Unreachable » : inaccessible
4. « Pending » : cas rare où l'hôte vient d'être déclaré et son statut n'a pas pu encore être contrôlé

Hosts			
0 Down	0 Unreachable	13 Up	0 Pending



# Les états des services (1)

- « Tactical Overview »
  - Les services ont également plusieurs états
    1. « Critical » : le service est sensé être dans un état critique
    2. « Warning » : le service est dans un état d'avertissement.
    3. « Unknown » : le programme n'a pas pu obtenir les éléments pour vérifier l'état du service. Il est donc inconnu.
    4. « Ok » : opérationnel
    5. « Pending » : cas où le service venant d'être déclaré n'a pas encore été contrôlé. On est donc en attente du contrôle.



Attention :

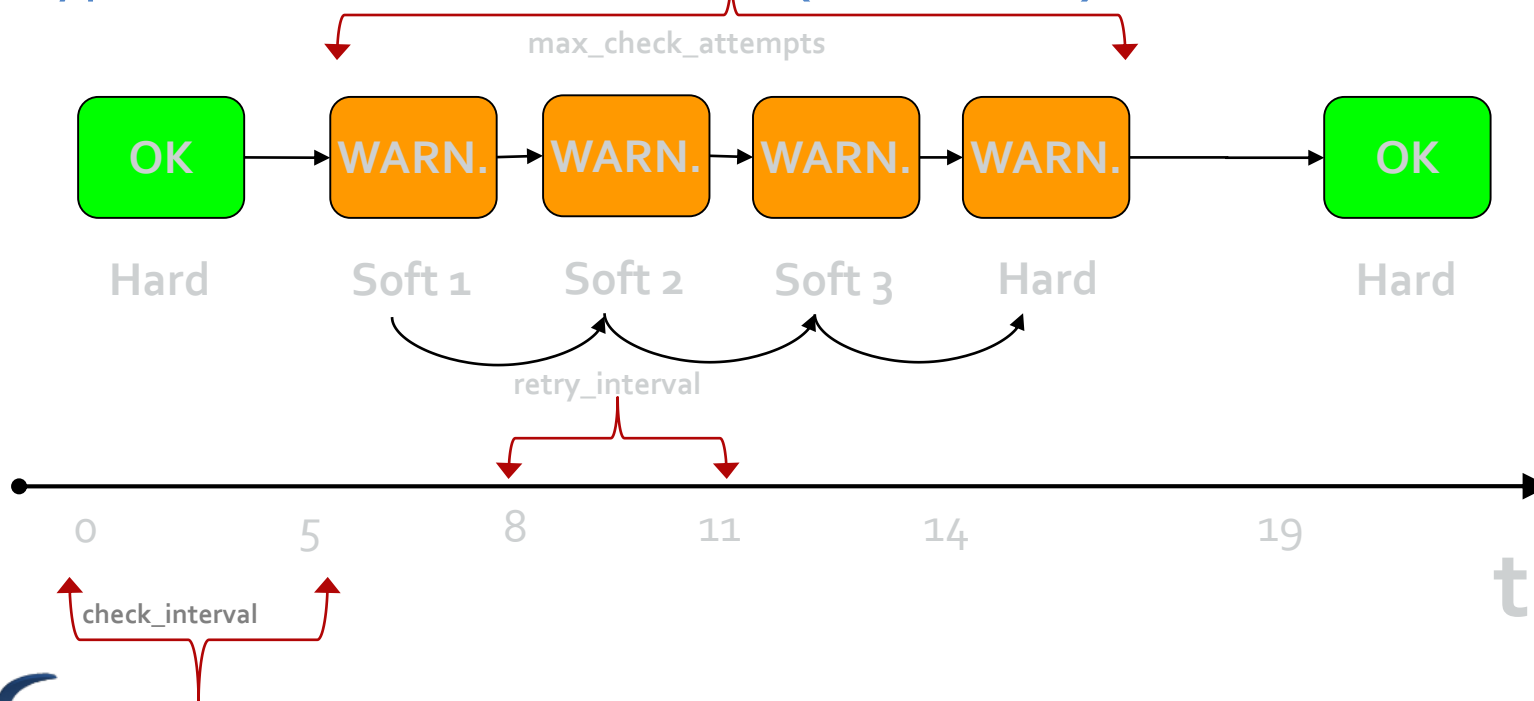
Les états dépendent de la manière dont a été écrit le programme effectuant le contrôle du service.





## Les états des services (2)

- De plus, les états peuvent être de 2 types :
  - Type Soft "S" : état intermédiaire non confirmé
  - Type Hard "H" : état stable (« ferme »)



# Les différentes options

- « Tactical Overview »
  - « Flap Detection » : Détection du bagotement
  - « Notifications » : Résumé des notifications externes
  - « Event Handlers » : Synthèse de l'activation des actions associées aux événements en provenance des services et des hôtes
  - « Active Checks » : Synthèse de l'activation des contrôles
  - « Passive Checks » : Synthèse de l'activation des contrôles

Monitoring Features					
Flap Detection		Notifications		Event Handlers	
Active Checks		Passive Checks			
Enabled	All Services Enabled No Services Flapping All Hosts Enabled No Hosts Flapping	Enabled	All Services Enabled All Hosts Enabled	Enabled	17 Services Disabled All Hosts Enabled
Enabled	All Services Enabled All Hosts Enabled	Enabled	67 Services Disabled 13 Hosts Disabled		



# Cartographie

- « Map »
  - Une vue basique adaptée au petite infrastructure

**Network Map For All Hosts**  
Last Updated: Mon May 17 23:12:57 CEST 2010  
Updated every 90 seconds  
Nagios® 3.1.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *fhma*

[View Status Detail For All Hosts](#)  
[View Status Overview For All Hosts](#)


**Layout Method:**  
Circular (Marked Up) ▼

**Scaling factor:**  
0.0

**Drawing Layers:**  
Equipements externes ▲  
Linux Servers ▲  
Network Printers ▼  
Network Switches ▼

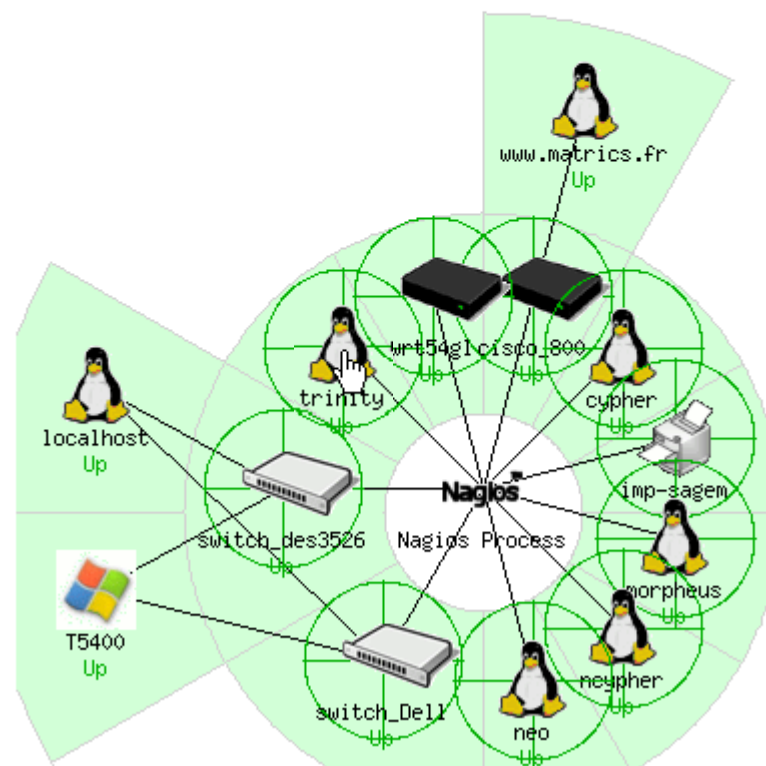
**Layer mode:**  
☐ Include  
☒ Exclude

**Suppress popups:**  
☐

 **Linux**

**Name:** trinity  
**Alias:** trinity  
**Address:** 192.168.3.69  
**State:** Up  
**Status Information:** PING OK - Packet loss = 0%, RTA = 0.39 ms  
**State Duration:** 14d 12h 6m 0s  
**Last Status Check:** 17-05-2010 23:23:43  
**Last State Change:** 03-05-2010 11:20:51  
**Parent Host(s):** None (This is a root host)  
**Immediate Child Hosts:** 0

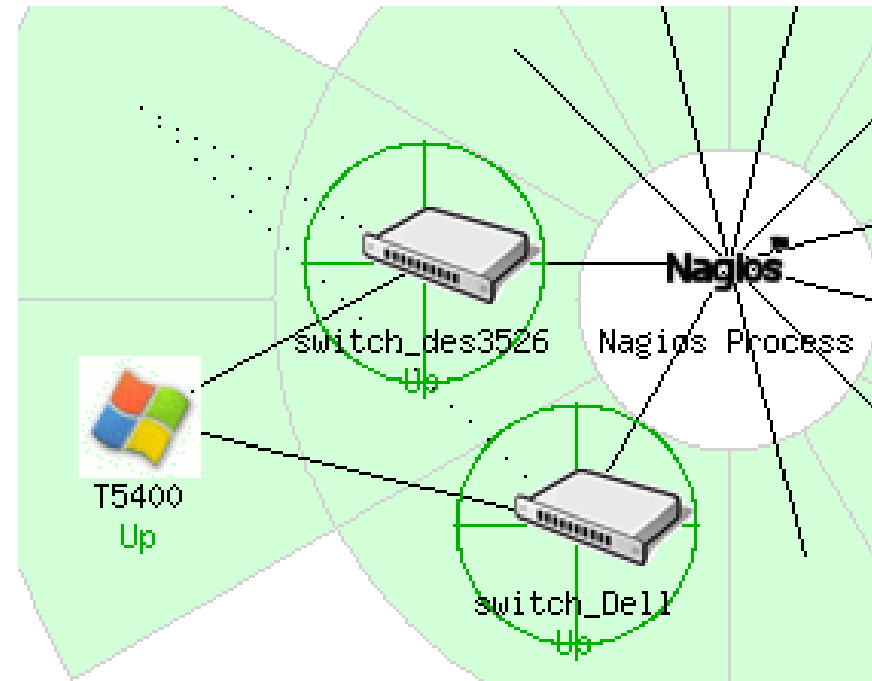
**Services:**  
- 7 ok



# Cartographie

- Dépendance

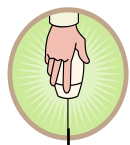
- La cartographie présente les informations de dépendances ; en effet, dans le cas où les 2 switchs sont indisponibles (état « down »), le T5400 sera dans l'état injoignable (« unreachable »)
- Les dépendances discutées sont des dépendances entre hôtes, mais il est également envisageable de mettre en œuvre des dépendances entre services.



# La vue des états des hôtes

**Current Network Status**  
Last Updated: Mon May 17 23:41:06 CEST 2010  
Updated every 90 seconds  
Nagios® Core™ 3.2.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *fhma*

[View Service Status Detail For All Host Groups](#)  
[View Status Overview For All Host Groups](#)  
[View Status Summary For All Host Groups](#)  
[View Status Grid For All Host Groups](#)



Host Status Totals			
Up	Down	Unreachable	Pending
13	0	0	0
All Problems		All Types	
0		13	

Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
61	4	0	2	0
All Problems		All Types		
6		67		

Host Status Details For All Host Groups

Host ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Status Information
<a href="#">TS400</a>	UP	18-05-2010 06:23:43	14d 19h 26m 59s	PING OK - Packet loss = 0%, RTA = 0.17 ms
<a href="#">cisco_800</a>	UP	18-05-2010 06:21:53	14d 19h 20m 19s	PING OK - Packet loss = 0%, RTA = 0.95 ms
<a href="#">cypher</a>	UP	18-05-2010 06:19:23	14d 19h 19m 9s	PING OK - Packet loss = 0%, RTA = 0.62 ms
<a href="#">imp-sagem</a>	UP	18-05-2010 06:19:47	14d 19h 20m 9s	PING OK - Packet loss = 0%, RTA = 1.76 ms
<a href="#">localhost</a>	UP	03-05-2010 13:41:31	16d 10h 38m 29s	PING OK - Packet loss = 0%, RTA = 0.04 ms
<a href="#">morpheus</a>	UP	18-05-2010 06:20:23	14d 19h 19m 59s	PING OK - Packet loss = 0%, RTA = 0.28 ms
<a href="#">ncypher</a>	UP	18-05-2010 06:20:53	14d 19h 19m 39s	PING OK - Packet loss = 0%, RTA = 0.30 ms
<a href="#">neo</a>	UP	18-05-2010 06:21:13	14d 19h 19m 39s	PING OK - Packet loss = 0%, RTA = 0.35 ms
<a href="#">switch_Dell</a>	UP	18-05-2010 06:21:33	14d 19h 18m 59s	PING OK - Packet loss = 0%, RTA = 0.91 ms
<a href="#">switch_des3525</a>	UP	18-05-2010 06:22:03	14d 19h 18m 9s	PING OK - Packet loss = 0%, RTA = 1.57 ms
<a href="#">trinity</a>	UP	18-05-2010 06:22:13	14d 19h 3m 9s	PING OK - Packet loss = 0%, RTA = 0.35 ms
<a href="#">wrt54gl</a>	UP	18-05-2010 06:22:43	14d 19h 20m 9s	PING OK - Packet loss = 0%, RTA = 0.91 ms
<a href="#">www.matrics.fr</a>	UP	18-05-2010 06:20:23	0d 16h 56m 7s	PING OK - Packet loss = 0%, RTA = 42.06 ms

13 Matching Host Entries Displayed

**Display Filters:**

Host Status Types: All problems  
Host Properties: Any  
Service Status Types: All  
Service Properties: Any



Host ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Status Information
---------	-----------	---------------	-------------	--------------------

0 Matching Host Entries Displayed

# Un hôte dans le détail (1)

- En cliquant sur l'icône représentatif du type d'équipement, on obtient :

**Host Information**  
Last Updated: Tue May 18 11:53:29 CEST 2010  
Updated every 90 seconds  
Nagios® Core™ 3.2.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *fhma*

[View Status Detail For This Host](#)  
[View Alert History For This Host](#)  
[View Availability Report For This Host](#)  
[View Notifications For This Host](#)

Host  
**T5400**  
(T5400)

Parents:  
[switch\\_des3526](#)  
[switch\\_Dell](#)

Member of  
[windows-servers](#)

192.168.3.133



## Host State Information

Host Status: **UP** (for 15d 0h 58m 2s)  
Status Information: PING OK - Packet loss = 0%, RTA = 1.47 ms  
Performance Data: rta=1.471000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0  
Current Attempt: 1/3 (HARD state)  
Last Check Time: 18-05-2010 11:54:23  
Check Type: ACTIVE  
Check Latency / Duration: 0.096 / 4.018 seconds  
Next Scheduled Active Check: 18-05-2010 11:59:33  
Last State Change: 03-05-2010 10:57:01  
Last Notification: N/A (notification 0)  
Is This Host Flapping? **NO** (0.00% state change)  
In Scheduled Downtime? **NO**  
Last Update: 18-05-2010 11:55:03 ( 0d 0h 0m 0s ago)

Active Checks: **ENABLED**  
Passive Checks: **DISABLED**  
Obsessing: **ENABLED**  
Notifications: **ENABLED**  
Event Handler: **ENABLED**  
Flap Detection: **ENABLED**

## Host Commands

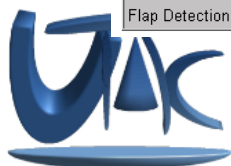
☒ [Disable active checks of this host](#)  
☒ [Re-schedule the next check of this host](#)  
☒ [Start accepting passive checks for this host](#)  
☒ [Stop obsessing over this host](#)  
☒ [Disable notifications for this host](#)  
☒ [Send custom host notification](#)  
☒ [Schedule downtime for this host](#)  
☒ [Disable notifications for all services on this host](#)  
☒ [Enable notifications for all services on this host](#)  
☒ [Schedule a check of all services on this host](#)  
☒ [Disable checks of all services on this host](#)  
☒ [Enable checks of all services on this host](#)  
☒ [Disable event handler for this host](#)  
☒ [Disable flap detection for this host](#)

## Host Comments

 [Add a new comment](#)  [Delete all comments](#)

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
------------	--------	---------	------------	------------	------	---------	---------

This host has no comments associated with it



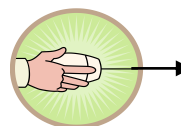


# Un hôte dans le détail (2)

- Les commandes associées à un hôte nous permettent
  - de suspendre ou d'activer les contrôles actifs ou pour tous les services hébergés par l'hôte ;
  - de replanifier le prochain contrôle pour l'hôte ou pour tous les services hébergés par l'hôte ;
  - de suspendre ou d'activer les contrôles passifs ;
  - d'arrêter le transfert hiérarchique ;
  - de suspendre ou d'activer les notifications pour l'hôte ou tous les services hébergés par l'hôte ;
  - d'envoyer à la volée une notification spécifique ;
  - de planifier une plage de maintenance ;
  - de suspendre ou d'activer les actions correctives ou de diagnostic ;
  - de suspendre ou d'activer la détection du bagotement

## Host Commands

- ✗ [Disable active checks of this host](#)
- 🕒 [Re-schedule the next check of this host](#)
- ✓ [Start accepting passive checks for this host](#)
- ✗ [Stop obsessing over this host](#)
- ✗ [Disable notifications for this host](#)
- 📢 [Send custom host notification](#)
- 🕒 [Schedule downtime for this host](#)
- ✗ [Disable notifications for all services on this host](#)
- ✓ [Enable notifications for all services on this host](#)
- 🕒 [Schedule a check of all services on this host](#)
- ✗ [Disable checks of all services on this host](#)
- ✓ [Enable checks of all services on this host](#)
- ✗ [Disable event handler for this host](#)
- ✗ [Disable flap detection for this host](#)





# Un hôte dans le détail (3)

- Mise en œuvre d'une plage de maintenance

## External Command Interface

Last Updated: Tue May 18 19:43:46 CEST 2010  
Nagios® Core™ 3.2.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *fhma*

You are requesting to schedule downtime for a particular host

## Command Options

Host Name: T5400  
Author (Your Name): françois-hugues  
Comment: de fonctionnement de la plage de planification  
Triggered By: N/A  
Start Time: 18-05-2010 19:43:46  
End Time: 18-05-2010 20:00:00  
Type: Fixed  
If Flexible, Duration: 0 Hours 45 Minutes  
Child Hosts: Do nothing with child hosts  
Commit Reset

## Command Description

This command is used to schedule downtime for a particular host. During the specified downtime, Nagios will not send notifications out about the host. When the scheduled downtime expires, Nagios will send out notifications for this host as it normally would. Scheduled downtimes are preserved across program shutdowns and restarts. Both the start and end times should be specified in the following format: **mm/dd/yyyy hh:mm:ss**. If you select the *fixed* option, the downtime will be in effect between the start and end times you specify. If you do not select the *fixed* option, Nagios will treat this as "flexible" downtime. Flexible downtime starts when the host goes down or becomes unreachable (sometime between the start and end times you specified) and lasts as long as the duration of time you enter. The duration fields do not apply for fixed downtime.

Your command request was successfully submitted to Nagios for processing.

Note: It may take a while before the command is actually processed.

[Done](#)

Please enter all required information before committing the command.

Required fields are marked in red.

Failure to supply all required values will result in an error.



# La vue des états des services

## Current Network Status

Last Updated: Tue May 18 06:42:08 CEST 2010  
Updated every 90 seconds  
Nagios® Core™ 3.2.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *fhma*

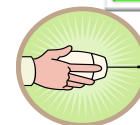
[View History For all hosts](#)  
[View Notifications For All Hosts](#)  
[View Host Status Detail For All Hosts](#)

## Host Status Totals

Up	Down	Unreachable	Pending
13	0	0	0
All Problems		All Types	
0		13	

## Service Status Totals

Ok	Warning	Unknown	Critical	Pending
61	4	0	2	0
All Problems		All Types		
6		67		



## Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
<a href="#">T5400</a>	<a href="#">check_nt</a>	OK	18-05-2010 06:40:26	14d 19h 43m 42s	1/3	NSClient++ 0.3.6.818 2009-06-14
	<a href="#">check_nt_cpuload</a>	OK	18-05-2010 06:36:25	14d 19h 43m 49s	1/3	CPU Load 4% (5 min average)
	<a href="#">check_nt_dskspace</a>	CRITICAL	18-05-2010 06:37:14	16d 11h 29m 9s	3/3	c: - total: 31.87 Gb - used: 30.77 Gb (97%) - free 1.11 Gb (3%)
	<a href="#">check_nt_memload</a>	OK	18-05-2010 06:40:07	5d 17h 30m 30s	1/3	Memory usage: total:5208.27 Mb - used: 3667.19 Mb (70%) - free: 1541.08 Mb (30%)
	<a href="#">check_snmptrap</a>	OK	18-05-2010 06:39:01	47d 18h 46m 29s	1/3	OK - No warning Traps and no critical traps in the database
<a href="#">cisco_800</a>	<a href="#">check_ping</a>	OK	18-05-2010 06:39:57	1d 22h 20m 40s	1/3	PING OK - Packet loss = 0%, RTA = 1.05 ms
	<a href="#">check_snmptrap</a>	OK	18-05-2010 06:40:31	47d 18h 45m 39s	1/3	OK - No warning Traps and no critical traps in the database
<a href="#">cypher</a>	<a href="#">check_ping</a>	OK	18-05-2010 06:36:26	14d 19h 36m 8s	1/3	PING OK - Packet loss = 0%, RTA = 1.44 ms
	<a href="#">check_smtp</a>	CRITICAL	18-05-2010 06:37:18	112d 14h 2m 44s	3/3	Connection refused
	<a href="#">check_snmp</a>	OK	18-05-2010 06:38:12	14d 19h 35m 17s	1/3	SNMP OK - Timeticks: (186899965) 21 days, 15:09:59.65
	<a href="#">check_snmptrap</a>	OK	18-05-2010 06:39:07	47d 18h 44m 49s	1/3	OK - No warning Traps and no critical traps in the database
	<a href="#">check_ssh</a>	OK	18-05-2010 06:39:59	14d 19h 32m 30s	1/3	SSH OK - OpenSSH_3.6.1p2 (protocol 1.99)
<a href="#">imp-sagem</a>	<a href="#">check_http</a>	OK	18-05-2010 06:35:35	14d 19h 34m 13s	1/3	Status: OK
	<a href="#">check_ping</a>	OK	18-05-2010 06:36:29	14d 19h 33m 59s	1/3	PING OK - Packet loss = 0%, RTA = 0.67 ms
	<a href="#">check_snmptrap</a>	OK	18-05-2010 06:37:27	47d 18h 43m 9s	1/3	OK - No warning Traps and no critical traps in the database

## Display Filters:

Host Status Types: All  
Host Properties: Any  
Service Status Types: All Problems  
Service Properties: Any

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
<a href="#">T5400</a>	<a href="#">check_nt_dskspace</a>	CRITICAL	18-05-2010 06:42:14	16d 11h 35m 50s	3/3	c: - total: 31.87 Gb - used: 30.77 Gb (97%) - free 1.11 Gb (3%)
<a href="#">cypher</a>	<a href="#">check_smtp</a>	CRITICAL	18-05-2010 06:42:18	112d 14h 9m 25s	3/3	Connection refused
<a href="#">morpheus</a>	<a href="#">check_ping</a>	WARNING	18-05-2010 06:43:47	33d 21h 46m 7s	3/3	FPING WARNING - 192.168.3.87
<a href="#">ncypher</a>	<a href="#">check_http_internet</a>	WARNING	18-05-2010 06:43:30	19d 13h 11m 40s	3/3	Status: WARNING (500 Can't connect to www.matrics.fr:80 (connect: Connection refused))
<a href="#">switch_Dell</a>	<a href="#">check_snmptrap</a>	WARNING	18-05-2010 06:44:37	47d 13h 35m 36s	3/3	WARNING - 143 warning Traps and no critical traps in the database
<a href="#">switch_des3526</a>	<a href="#">check_snmptrap</a>	WARNING	18-05-2010 06:47:00	70d 20h 16m 21s	3/3	WARNING - 416 warning Traps and no critical traps in the database

7 Matching Service Entries Displayed



# Un service dans le détail (1)

- On retrouve des éléments similaires aux hôtes

## Service State Information

Current Status: **CRITICAL** (for 114d 1h 55m 32s)  
Status Information: Connection refused  
SMTP CRITICAL - 0.001 sec. response time  
Performance Data: time=0.000516s;;;0.000000  
Current Attempt: 3/3 (HARD state)  
Last Check Time: 19-05-2010 18:32:18  
Check Type: ACTIVE  
Check Latency / Duration: 0.156 / 0.012 seconds  
Next Scheduled Check: 19-05-2010 18:37:18  
Last State Change: 25-01-2010 15:37:53  
Last Notification: 19-05-2010 18:22:20 (notification 10647)  
Is This Service Flapping? **NO** (0.00% state change)  
In Scheduled Downtime? **NO**  
Last Update: 19-05-2010 18:33:20 ( 0d 0h 0m 5s ago)

Active Checks: **ENABLED**  
Passive Checks: **DISABLED**  
Obsessing: **ENABLED**  
Notifications: **ENABLED**  
Event Handler: **ENABLED**  
Flap Detection: **ENABLED**

Service  
**check\_smtp**  
On Host  
**cypher**  
([cypher](#))

Member of  
**No servicegroups.**

192.168.3.6

## Service Commands

- [Disable active checks of this service](#)
- [Re-schedule the next check of this service](#)
- [Start accepting passive checks for this service](#)
- [Stop obsessing over this service](#)
- [Acknowledge this service problem](#)
- [Disable notifications for this service](#)
- [Delay next service notification](#)
- [Send custom service notification](#)
- [Schedule downtime for this service](#)
- [Disable event handler for this service](#)
- [Disable flap detection for this service](#)

## Service Comments

[Add a new comment](#) [Delete all comments](#)

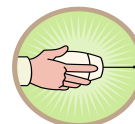
Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This service has no comments associated with it							














# Un service dans le détail (2)

- L'acquittement

TS400		check_nt	OK
		check_nt_cpuload	OK
		check_nt_dskspace	CRITICAL



## Service Commands

-  [Disable active checks of this service](#)
-  [Re-schedule the next check of this service](#)
-  [Start accepting passive checks for this service](#)
-  [Stop obsessing over this service](#)
-  [Acknowledge this service problem](#)
-  [Disable notifications for this service](#)
-  [Delay next service notification](#)
-  [Send custom service notification](#)
-  [Schedule downtime for this service](#)
-  [Disable event handler for this service](#)
-  [Disable flap detection for this service](#)

You are requesting to acknowledge a service problem

## Command Options

Host Name:	TS400
Service:	check_nt_dskspace
Sticky Acknowledgement:	<input checked="" type="checkbox"/>
Send Notification:	<input checked="" type="checkbox"/>
Persistent Comment:	<input type="checkbox"/>
Author (Your Name):	françois-hugues
Comment:	Acquittement en attendant l'achat d'un disque
	<input type="button" value="Commit"/> <input type="button" value="Reset"/>

## Command Description

This command is used to acknowledge a service problem. When a service problem is acknowledged, future notifications about problems are temporarily disabled until the service changes from its current state. If you want acknowledgement to disable notifications until the service recovers, check the 'Sticky Acknowledgement' checkbox. Contacts for this service will receive a notification about the acknowledgement, so they are aware that someone is working on the problem. Additionally, a comment will also be added to the service. Make sure to enter your name and fill in a brief description of what you are doing in the comment field. If you would like the service comment to remain once the acknowledgement is removed, check the 'Persistent Comment' checkbox. If you do not want an acknowledgement notification sent out to the appropriate contacts, uncheck the 'Send Notification' checkbox.

Please enter all required information before committing the command.



Required fields are marked in red.

Failure to supply all required values will result in an error.

TS400		check_nt	OK
		check_nt_cpuload	OK
		check_nt_dskspace	CRITICAL

## Service Comments

 [Add a new comment](#)  [Delete all comments](#)

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
18-05-2010 22:36:07	françois-hugues	Acquittement en attendant l'achat d'un disque	78	No	Acknowledgement	N/A	
18-05-2010 17:02:54	françois-hugues	Un disque supplémentaire est à provisionner	76	Yes	User	N/A	



# Vues de synthèse par groupe d'hôtes













- Amélioration de la lisibilité
  - 3 types de vue (Overview/Summary/Grid)
- Facilitation de l'exploitation

## Service Overview For All Host Groups



[Equipements externes \(Eqpts\\_externes\)](#)

Host	Status	Services	Actions
<a href="#">www.matrics.fr</a>	UP	2 OK	 





[Linux Servers \(linux-servers\)](#)

Host	Status	Services	Actions
<a href="#">cypher</a>	UP	4 OK 1 CRITICAL	 
<a href="#">localhost</a>	UP	7 OK	 
<a href="#">morpheus</a>	UP	9 OK 1 WARNING	 
<a href="#">ncypher</a>	UP	10 OK 1 WARNING	 
<a href="#">neo</a>	UP	7 OK	 
<a href="#">trinity</a>	UP	7 OK	 



[Network Printers \(network-printers\)](#)

Host	Status	Services	Actions
<a href="#">imp-sagem</a>	UP	3 OK	 

[Network Switches \(switches\)](#)

Host	Status	Services	Actions
<a href="#">switch_Dell</a>	UP	2 OK 1 WARNING	 
<a href="#">switch_des3526</a>	UP	2 OK 1 WARNING	 

[Windows Servers \(windows-servers\)](#)

Host	Status	Services	Actions
<a href="#">T5400</a>	UP	4 OK 1 CRITICAL	 





# Vues de synthèse par groupe de services

- Dans le même esprit que les vues par groupe d'hôtes
  - 3 types de vue (Overview/Summary/Grid)

## Service Overview For All Service Groups

<a href="#">Web Services (web-services)</a>			
Host	Status	Services	Actions
<a href="#">localhost</a>	 UP	1 OK	  

<a href="#">Services Web externes (web_external_services)</a>			
Host	Status	Services	Actions
<a href="#">www.matrics.fr</a>	 UP	1 OK	  

## Status Summary For All Service Groups

Service Group	Host Status Summary	Service Status Summary
<a href="#">Web Services (web-services)</a>	1 UP	1 OK
<a href="#">Services Web externes (web_external_services)</a>	1 UP	1 OK

## Status Grid For All Service Groups

<a href="#">Web Services (web-services)</a>		
Host	Services	Actions
<a href="#">localhost</a>	check http	  

<a href="#">Services Web externes (web_external_services)</a>		
Host	Services	Actions
<a href="#">www.matrics.fr</a>	check http	  



# Vues par exception

- L'ensemble des problèmes



**Display Filters:**  
Host Status Types: All  
Host Properties: Any  
Service Status Types: All Problems  
Service Properties: Any

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
<a href="#">T5400</a>	<a href="#">check_nt_dskspace</a>	CRITICAL	18-05-2010 22:42:14	17d 3h 34m 18s	3/3	c: - total: 31.87 Gb - used: 30.81 Gb (97%) - free 1.07 Gb (3%)
<a href="#">cypher</a>	<a href="#">check_smtp</a>	CRITICAL	18-05-2010 22:42:18	113d 6h 7m 53s	3/3	Connection refused
<a href="#">morpheus</a>	<a href="#">check_fping</a>	WARNING	18-05-2010 22:43:47	34d 13h 44m 35s	3/3	FPING WARNING - 192.168.3.87
<a href="#">ncypher</a>	<a href="#">check_http_internet</a>	WARNING	18-05-2010 22:43:30	20d 5h 10m 8s	3/3	Status: WARNING (500 Can't connect to www.matrics.fr:80 (connect: Connection refused))
<a href="#">switch_Dell</a>	<a href="#">check_snmptrap</a>	WARNING	18-05-2010 22:44:37	48d 5h 34m 4s	3/3	WARNING - 143 warning Traps and no critical traps in the database
<a href="#">switch_des3526</a>	<a href="#">check_snmptrap</a>	WARNING	18-05-2010 22:42:00	71d 12h 14m 49s	3/3	WARNING - 416 warning Traps and no critical traps in the database

- Uniquement les problèmes non pris en compte (« unhandled »)



Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
<a href="#">cypher</a>	<a href="#">check_smtp</a>	CRITICAL	18-05-2010 22:47:18	113d 6h 12m 53s	3/3	Connection refused
<a href="#">morpheus</a>	<a href="#">check_fping</a>	WARNING	18-05-2010 22:48:47	34d 13h 49m 35s	3/3	FPING WARNING - 192.168.3.87
<a href="#">ncypher</a>	<a href="#">check_http_internet</a>	WARNING	18-05-2010 22:48:30	20d 5h 15m 8s	3/3	Status: WARNING (500 Can't connect to www.matrics.fr:80 (connect: Connection refused))
<a href="#">switch_Dell</a>	<a href="#">check_snmptrap</a>	WARNING	18-05-2010 22:49:37	48d 5h 39m 4s	3/3	WARNING - 143 warning Traps and no critical traps in the database
<a href="#">switch_des3526</a>	<a href="#">check_snmptrap</a>	WARNING	18-05-2010 22:47:00	71d 12h 19m 49s	3/3	WARNING - 416 warning Traps and no critical traps in the database



# Vues par exception

- « Network Outage »

**Blocking Outages**

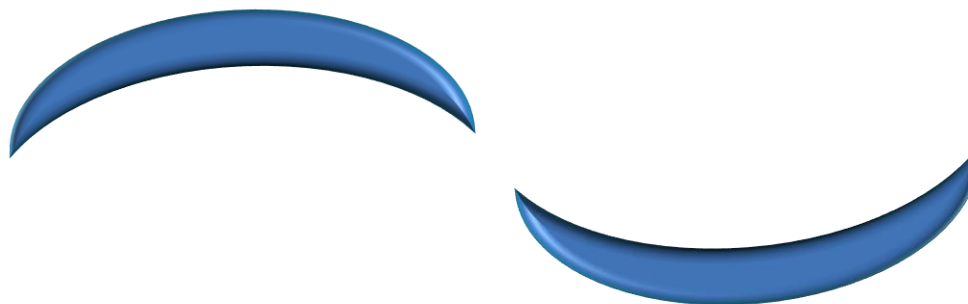
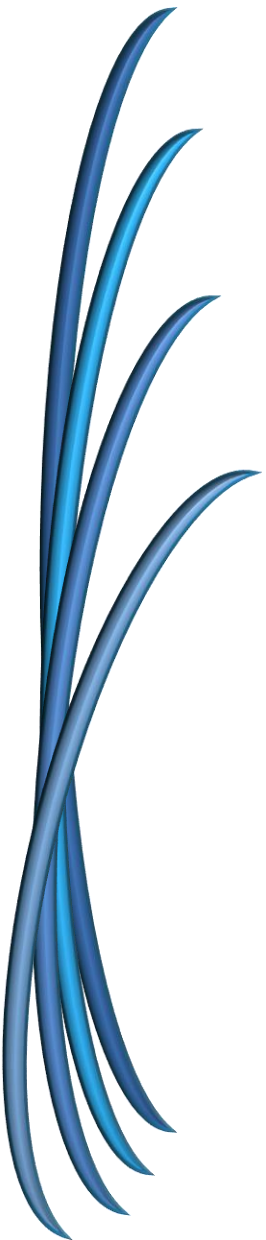
Severity	Host	State	Notes	State Duration	# Hosts Affected	# Services Affected	Actions
3	<a href="#">switch</a>	DOWN	N/A	0d 0h 6m 47s	2	4	

Annotations:

- Sévérité : dépend du nombre de Hosts et Services impactés
- Host source du problème
- État du Host
- Durée de l'état actuel
- Hosts et Services impactés
- Actions : Status Detail, Maps, Trends, Alert History, Notifications







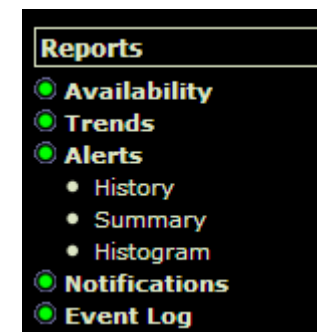
# Rapports

Interface graphique



# Les rapports

- En synthèse
  - « Availability » : Taux de disponibilité en % de temps passé par état
  - « Trends » : Historique temporel des états
  - « Alert »
    - « History » : Consultation des journaux de l'historique des événements
    - « Summary » : Rapport d'événements filtré
    - « Histogram » : Graphe des événements par périodicité horaire
  - « Notifications » : Consultation des journaux de notifications
  - « Event Log » : Journaux bruts des événements (Alertes, Notifications, ...)
- Les rapports peuvent être filtrés suivants le profil utilisateur



# Rapports de disponibilité

## Step 1: Select Report Type

Type:

- Servicegroup(s)
- Hostgroup(s)
- Host(s)
- Servicegroup(s)
- Service(s)

## Step 2: Select Servicegroup

Servicegroup(s):

- ALL SERVICE
- web-services
- web\_external\_s

## Step 3: Select Report Options

Report Period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Report time Period:

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Host State:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

Create Availability Report!

## All Servicegroups

13-05-2010 09:33:20 to 20-05-2010 09:33:20  
Duration: 7d 0h 0m 0s

[ Availability report completed in 0 min 0 sec ]

### Servicegroup 'web-services' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
localhost	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

### Servicegroup 'web-services' Service State Breakdowns:

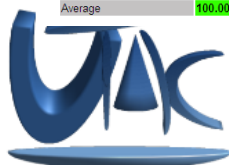
Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
localhost	check_http	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average		100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

### Servicegroup 'web\_external\_services' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
www.matrics.fr	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

### Servicegroup 'web\_external\_services' Service State Breakdowns:

Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
www.matrics.fr	check_http	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average		100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%



# Graphe de performance

## Step 3: Select Report Options

Report period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

Suppress image map: ☐

Suppress popups: ☐

**Service State Trends**  
Last Updated: Mon Sep 19 17:03:46 CEST 2005  
Nagios® - [www.nagios.org](http://www.nagios.org)  
Logged in as: nagios

[View Trends For This Host](#)  
[View Availability Report For This Service](#)  
[View Alert Histogram For This Service](#)  
[View Alert History This Service](#)  
[View Notifications For This Service](#)

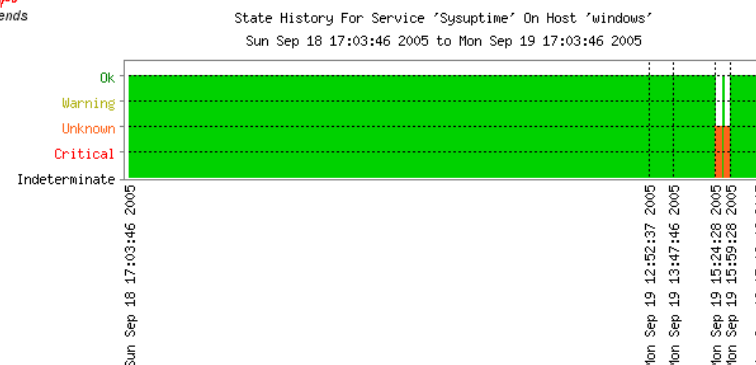
## Service 'Sysuptime' On Host 'windows'

18-09-2005 17:03:46 to 19-09-2005 17:03:46  
Duration: 1d 0h 0m 0s

First assumed service state: Backtracked

Report period:  Zoom factor:

Trends



## State Breakdowns:

Ok : (97.709%) 0d 23h 27m 1s  
Warning : (0.000%) 0d 0h 0m 0s  
Unknown : (2.291%) 0d 0h 32m 59s  
Critical : (0.000%) 0d 0h 0m 0s  
Indeterminate: (0.000%) 0d 0h 0m 0s



# Rapport sur les alertes - histogramme

## Service Alert Histogram

Last Updated: Mon Sep 19 17:15:58 CEST 2005

Nagios® - [www.nagios.org](http://www.nagios.org)

Logged in as *nagios*

[View Trends For This Service](#)

[View Availability Report For This Service](#)

[View History This Service](#)

[View Notifications For This Service](#)

## Service 'Sysuptime' On Host 'windows'

12-09-2005 17:15:58 to 19-09-2005 17:15:58

Duration: 7d 0h 0m 0s

### Report period:

Last 7 Days

### Assume state retention:

yes

### Breakdown type:

Hour of the Day

### Initial states logged:

no

### Events to graph:

All service events

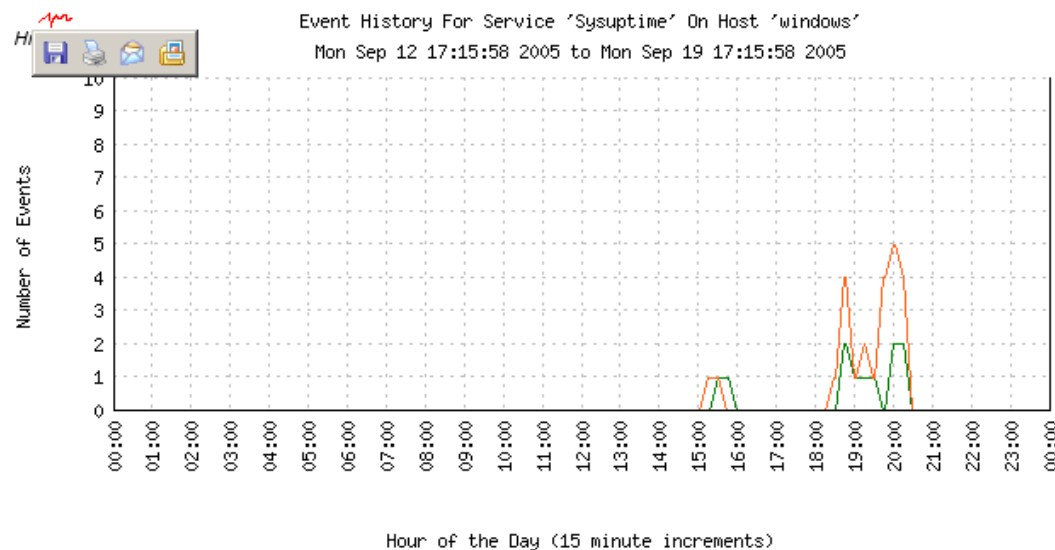
### Ignore repeated states:

no

### State types to graph:

Hard and soft states

Update



EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Ok):	0	2	11	0.11
Warning:	0	0	0	0.00
Unknown:	0	5	24	0.25
Critical:	0	0	0	0.00



# Rapports sur les alertes – historique et synthèse

## Alert History

Last Updated: Thu May 20 11:18:19 CEST 2010  
Nagios® Core™ 3.2.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *fhma*

[View Status Detail For All Hosts](#)  
[View Notifications For All Hosts](#)

## All Hosts and Services

Latest Archive



Log File Navigation  
Thu May 20 00:00:00 CEST 2010  
to  
Present..

File: nagios.log

### State type options:

All state types ▾

### History detail level for all hosts:

All alerts ▾

- ☐ Hide Flapping Alerts
- ☐ Hide Downtime Alerts
- ☐ Hide Process Messages
- ☐ Older Entries First

Update

May 20, 2010 08:00

OK [20-05-2010 08:07:00] SERVICE ALERT: trinity;check\_ux\_totalprocs;OK;HARD;3;PROCS OK: 149 processes

May 20, 2010 07:00

! [20-05-2010 07:27:00] SERVICE ALERT: trinity;check\_ux\_totalprocs;WARNING;HARD;3;PROCS WARNING: 154 processes

! [20-05-2010 07:26:00] SERVICE ALERT: trinity;check\_ux\_totalprocs;WARNING;SOFT;2;PROCS WARNING: 154 processes

! [20-05-2010 07:25:00] SERVICE ALERT: trinity;check\_ux\_totalprocs;WARNING;SOFT;1;PROCS WARNING: 154 processes





# Rapport sommaire sur les alertes

- 2 types de rapports
  - Rapport de type « Top N »

## Report Options Summary:

Alert Types: Host & Service Alerts

State Types: Hard States

Host States: Up, Down, Unreachable

Service States: Ok, Warning, Unknown, Critical

[Generate New Report](#)

type «

## Most Recent Alerts

13-05-2010 14:07:19 to 20-05-2010 14:07:19

Duration: 7d 0h 0m 0s

Displaying all 24 matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
20-05-2010 08:07:00	Service Alert	trinity	check_ux_totalprocs	OK	HARD	PROCS OK: 149 processes
20-05-2010 07:27:00	Service Alert	trinity	check_ux_totalprocs	WARNING	HARD	PROCS WARNING: 154 processes
19-05-2010 15:52:10	Service Alert	T5400	check_nt_memload	OK	HARD	Memory usage: total:5208.27 Mb - used: 4037.21
19-05-2010 15:37:10	Service Alert	T5400	check_nt_memload	WARNING	HARD	Memory usage: total:5208.27 Mb - used: 4216.03
19-05-2010 13:22:10	Service Alert	cisco_800	check_ping	OK	HARD	PING OK - Packet loss = 0%, RTA = 1.07 ms
19-05-2010 13:17:10	Service Alert	cisco_800	check_ping	CRITICAL	HARD	CRITICAL - Plugin timed out after 10 seconds
19-05-2010 11:14:10	Service Alert	T5400	check_nt_memload	OK	HARD	Memory usage: total:5208.27 Mb - used: 4012.99
19-05-2010 11:04:10	Service Alert	T5400	check_nt_memload	WARNING	HARD	Memory usage: total:5208.27 Mb - used: 4175.22
19-05-2010 10:52:10	Service Alert	T5400	check_nt_memload	OK	HARD	Memory usage: total:5208.27 Mb - used: 4033.49
19-05-2010 10:22:10	Service Alert	T5400	check_nt_memload	WARNING	HARD	Memory usage: total:5208.27 Mb - used: 4201.36
19-05-2010 07:55:03	Service Alert	trinity	check_ux_totalprocs	OK	HARD	PROCS OK: 147 processes
19-05-2010 07:25:03	Service Alert	trinity	check_ux_totalprocs	WARNING	HARD	PROCS WARNING: 152 processes
18-05-2010 10:22:03	Service Alert	cisco_800	check_ping	OK	HARD	PING OK - Packet loss = 0%, RTA = 1.13 ms
18-05-2010 10:17:13	Service Alert	cisco_800	check_ping	CRITICAL	HARD	CRITICAL - Plugin timed out after 10 seconds
18-05-2010 07:38:03	Service Alert	trinity	check_ux_totalprocs	OK	HARD	PROCS OK: 146 processes
18-05-2010 07:28:03	Service Alert	trinity	check_ux_totalprocs	WARNING	HARD	PROCS WARNING: 151 processes
17-05-2010 07:46:03	Service Alert	trinity	check_ux_totalprocs	OK	HARD	PROCS OK: 146 processes
17-05-2010 07:26:03	Service Alert	trinity	check_ux_totalprocs	WARNING	HARD	PROCS WARNING: 151 processes
16-05-2010 07:54:03	Service Alert	trinity	check_ux_totalprocs	OK	HARD	PROCS OK: 147 processes
16-05-2010 07:29:03	Service Alert	trinity	check_ux_totalprocs	WARNING	HARD	PROCS WARNING: 151 processes
15-05-2010 07:42:03	Service Alert	trinity	check_ux_totalprocs	OK	HARD	PROCS OK: 147 processes
15-05-2010 07:27:03	Service Alert	trinity	check_ux_totalprocs	WARNING	HARD	PROCS WARNING: 151 processes
14-05-2010 07:50:03	Service Alert	trinity	check_ux_totalprocs	OK	HARD	PROCS OK: 146 processes
14-05-2010 07:30:03	Service Alert	trinity	check_ux_totalprocs	WARNING	HARD	PROCS WARNING: 151 processes

## Standard Reports:

Report Type: 25 Most Recent Hard Alerts

[Create Summary Report!](#)

## Custom Report Options:

Report Type: Most Recent Alerts

Report Period: Last 7 Days

If Custom Report Period...

Start Date (Inclusive): May 1 2010

End Date (Inclusive): May 20 2010

Limit To Hostgroup: \*\* ALL HOSTGROUPS \*\*

Limit To Servicegroup: \*\* ALL SERVICEGROUPS \*\*

Limit To Host: \*\* ALL HOSTS \*\*

Alert Types: Host and Service Alerts

State Types: Hard and Soft States

Host States: All Host States

Service States: All Service States

Max List Items: 25

[Create Summary Report!](#)

# Rapport sommaire sur les alertes

- Exemple de rapport personnalisé :
  - Rapport de type TopN pour les hôtes les plus verbeux sur les alertes confirmées du mois dernier

**Custom Report Options:**

Report Type:

Report Period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Limit To Hostgroup:

Limit To Servicegroup:

Limit To Host:

Alert Types:

State Types:

Host States:

Service States:

Max List Items:

## Top Alert Producers

01-04-2010 00:00:00 to 01-05-2010 00:00:00  
Duration: 30d 0h 0m 0s

## Report Options Summary:

Alert Types: *Host Alerts*

State Types: *Hard States*

Host States: *Up, Down, Unreachable*

Service States: *Ok, Warning, Unknown, Critical*

## Displaying all 12 matching alert producers

Rank	Producer Type	Host	Service	Total Alerts
#1	Host	<a href="#">morpheus</a>	N/A	19
#2	Host	<a href="#">www.matrics.fr</a>	N/A	12
#3	Host	<a href="#">imp-sagem</a>	N/A	10
#4	Host	<a href="#">trinity</a>	N/A	7
#5	Host	<a href="#">wrt54gl</a>	N/A	6
#6	Host	<a href="#">switch_Dell</a>	N/A	6
#7	Host	<a href="#">ncvpher</a>	N/A	6
#8	Host	<a href="#">neo</a>	N/A	6
#9	Host	<a href="#">T5400</a>	N/A	4
#10	Host	<a href="#">switch_des3526</a>	N/A	4
#11	Host	<a href="#">cisco_800</a>	N/A	4
#12	Host	<a href="#">cvpher</a>	N/A	4





# Rapports sur les notifications

## All Contacts

Latest Archive



Log File Navigation  
Thu May 20 00:00:00 CEST 2010  
to  
Present..

File: nagios.log

Notification detail level for all contacts:

- All notifications
- All notifications
- All service notifications
- All host notifications
- Service custom
- Service acknowledgements
- Service warning
- Service unknown
- Service critical
- Service recovery
- Service flapping
- Host custom
- Host acknowledgements
- Host down
- Host unreachable
- Host recovery
- Host flapping

Update

Host	Service	Type	Time	Contact	Notification Command	Information
<a href="#">switch_Dell</a>	<a href="#">check_snmptrap</a>	WARNING	20-05-2010 14:54:40	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	WARNING - 143 warning
<a href="#">morpheus</a>	<a href="#">check_fping</a>	WARNING	20-05-2010 14:53:50	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	FPING WARNING - 192.168.3.87
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:52:24	<a href="#">icde</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:52:24	<a href="#">cmei</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:52:24	<a href="#">afra</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:52:20	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	Connection refused
<a href="#">switch_Dell</a>	<a href="#">check_snmptrap</a>	WARNING	20-05-2010 14:39:40	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	WARNING - 143 warning Traps and no critical traps in the database
<a href="#">morpheus</a>	<a href="#">check_fping</a>	WARNING	20-05-2010 14:38:50	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	FPING WARNING - 192.168.3.87
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:37:24	<a href="#">icde</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:37:24	<a href="#">cmei</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:37:24	<a href="#">afra</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:37:20	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	Connection refused
<a href="#">switch_Dell</a>	<a href="#">check_snmptrap</a>	WARNING	20-05-2010 14:24:40	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	WARNING - 143 warning Traps and no critical traps in the database
<a href="#">morpheus</a>	<a href="#">check_fping</a>	WARNING	20-05-2010 14:23:50	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	FPING WARNING - 192.168.3.87
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:22:24	<a href="#">icde</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:22:24	<a href="#">cmei</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:22:24	<a href="#">afra</a>	<a href="#">notify-service-by-email</a>	Connection refused
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:22:20	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	Connection refused
<a href="#">switch_Dell</a>	<a href="#">check_snmptrap</a>	WARNING	20-05-2010 14:09:40	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	WARNING - 143 warning Traps and no critical traps in the database
<a href="#">morpheus</a>	<a href="#">check_fping</a>	WARNING	20-05-2010 14:08:50	<a href="#">lcor</a>	<a href="#">check-host-alive</a>	FPING WARNING - 192.168.3.87
<a href="#">cvpher</a>	<a href="#">check_smtp</a>	CRITICAL	20-05-2010 14:07:24	<a href="#">icde</a>	<a href="#">notify-service-by-email</a>	Connection refused



# Rapports sur les journaux d'événements

- Événement =  
(alerte et notification, événement Nagios)

May 20, 2010 15:00

```
[20-05-2010 15:24:52] ndomod: Still unable to connect to data sink. 893 items lost, 5000 queued items to flush.
[20-05-2010 15:24:48] SERVICE NOTIFICATION: lcor;morpheus;check_fping;WARNING;check-host-alive;FPING WARNING - 192.168.3.87
[20-05-2010 15:24:36] ndomod: Still unable to connect to data sink. 789 items lost, 5000 queued items to flush.
[20-05-2010 15:24:20] ndomod: Still unable to connect to data sink. 689 items lost, 5000 queued items to flush.
[20-05-2010 15:24:04] ndomod: Still unable to connect to data sink. 578 items lost, 5000 queued items to flush.
[20-05-2010 15:23:48] Finished daemonizing... (New PID=20401)
[20-05-2010 15:23:48] Event broker module '/usr/local/nagios/bin/ndomod.o' initialized successfully.
[20-05-2010 15:23:48] ndomod: Could not open data sink! I'll keep trying, but some output may get lost...
[20-05-2010 15:23:48] ndomod: NDOMOD 1.4b9 (10-27-2009) Copyright (c) 2009 Nagios Core Development Team and Community Contributors
[20-05-2010 15:23:48] LOG VERSION: 2.0
[20-05-2010 15:23:48] Local time is Thu May 20 15:23:48 CEST 2010
[20-05-2010 15:23:48] Nagios 3.2.0 starting... (PID=20400)
[20-05-2010 15:23:47] Event broker module '/usr/local/nagios/bin/ndomod.o' deinitialized successfully.
[20-05-2010 15:23:46] ndomod: Shutdown complete.
[20-05-2010 15:23:46] Successfully shutdown... (PID=4699)
[20-05-2010 15:23:46] Caught SIGTERM, shutting down...
[20-05-2010 15:23:36] ndomod: Still unable to connect to data sink. 790823 items lost, 5000 queued items to flush.
[20-05-2010 15:23:20] ndomod: Still unable to connect to data sink. 790707 items lost, 5000 queued items to flush.
[20-05-2010 15:23:04] ndomod: Still unable to connect to data sink. 790614 items lost, 5000 queued items to flush.
[20-05-2010 15:22:48] ndomod: Still unable to connect to data sink. 790499 items lost, 5000 queued items to flush.
[20-05-2010 15:22:32] ndomod: Still unable to connect to data sink. 790379 items lost, 5000 queued items to flush.
[20-05-2010 15:22:24] Warning: Attempting to execute the command "/usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: PROBLEM\n\nServ
15:22:24 CEST 2010\n\nAdditional Info:\n\nConnection refused" | /bin/mail -s "*** PROBLEM Service Alert: cypher/check_smtp is CRITICAL ***" jcdc@
actually exists...
[20-05-2010 15:22:24] SERVICE NOTIFICATION: jcdc;cypher;check_smtp;CRITICAL;notify-service-by-email;Connection refused
```



# Informations étendues des objets

Configuration avancée



# Les informations étendues (hôtes)

- Anciennement
- Dorénavant (v3), c'est directement dans la définition d'un hôte
- Par exemple, pour l'ergonomie

```
define host{  
    ...  
    host_name      chene  
    notes          Note : Serveur de Management  
    notes_url      http://chene/NotesChene.html  
    action_url     http://chene/ActionsChene.html  
    icon_image     linux40.png  
    icon_image_alt Fedora Core 3  
    vrmf_image     linux40.png  
    statusmap_image linux40.gd2  
    2d_coords      100,250  
    3d_coords      100.0,50.0,75.0  
}
```

~~hostextra.info.cfg~~

Host  
**chene : serveur de supervision  
(chene)**

Member of  
[HG\\_Management](#), [HG\\_Servers](#)

127.0.0.1



( Fedora Core 3 )

Note : Serveur de Management



Extra Host Actions



Extra Host Notes



# Les informations étendues (services)

- Le principe est similaire pour les services
- Par exemple, pour l'ergonomie  
define service{

```
...  
display_name      display_name  
notes             string  
notes_url         url  
action_url        number_timeperiod  
icon_image        number_timeperiod  
icon_image_alt    [0|1]  
}
```

~~servicee>info.cfg~~



# Les contrôles et états

- Spécifier des fréquences particulières
  - *check\_interval* *number\_timeperiod*
  - *retry\_interval* *number\_timeperiod*
- Indiquer globalement le On/Off des types de surveillance
  - *active\_checks\_enabled* *[0|1]*
  - *passive\_checks\_enabled* *[0|1]*
- définir dans quel état Nagios considère l'hôte avant même de l'avoir interrogé
  - *initial\_state* *[o|d|u]*
- dans quelle mesure doit on relayer cet état à un autre Nagios
  - *obsess\_over\_host* *[0|1]*





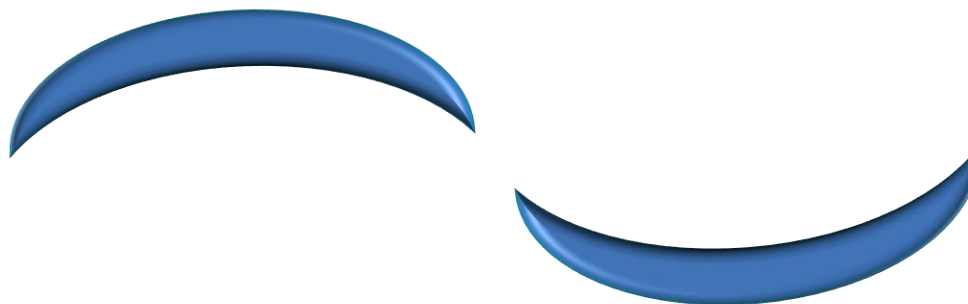
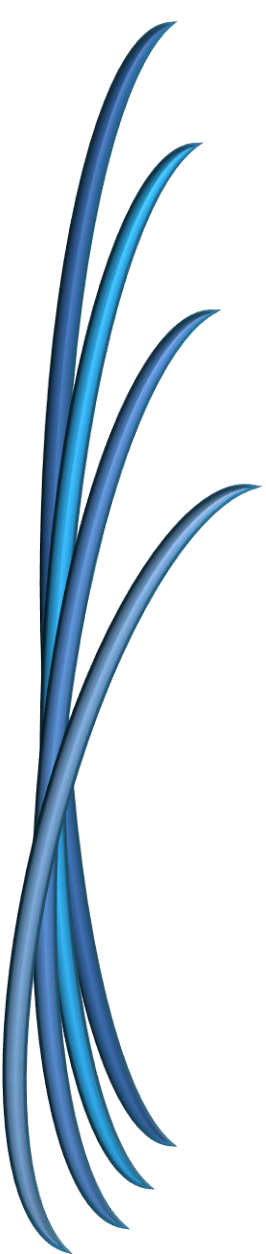
# Le contrôle du rafraichissement

- Vérification d'arrivée de données
    - Contrôles basés uniquement sur du passif
      - envoie-t-on un signe de vie par heure ?
        - ✓ Oui ?
- dans ce cas, on peut mettre en place le contrôle du rafraichissement



```
define host{  
    ...  
    check_freshness      [0|1]  
    freshness_threshold  #  
    ...  
}
```





# Le bagotement

Configuration avancée





# Le bagotement

- Détection du bagotement

- Nagios conserve pour chaque élément ces 21 derniers états

- Calcul du taux de variation

$$Taux = \frac{\sum Chgt * Poids}{20}$$

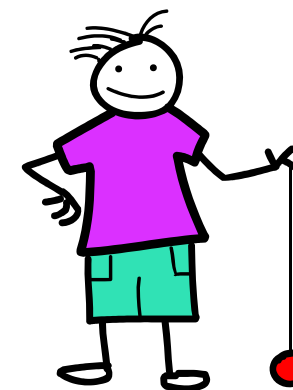
- par rapport au changement d'état de type « HARD »
    - fonction de l'ancienneté des changements d'états (poids)
    - aux états définis dans le paramètre « flap\_detection\_options »

- Détection

- Si Taux > « high\_flap\_detection »

- Retour à la normale

- Si Taux < « low\_flap\_detection »



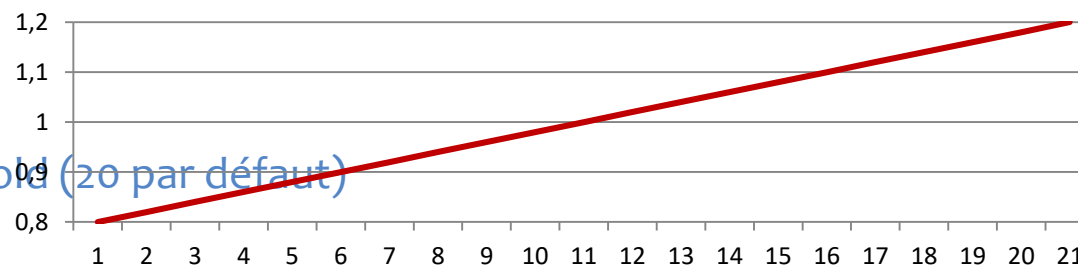
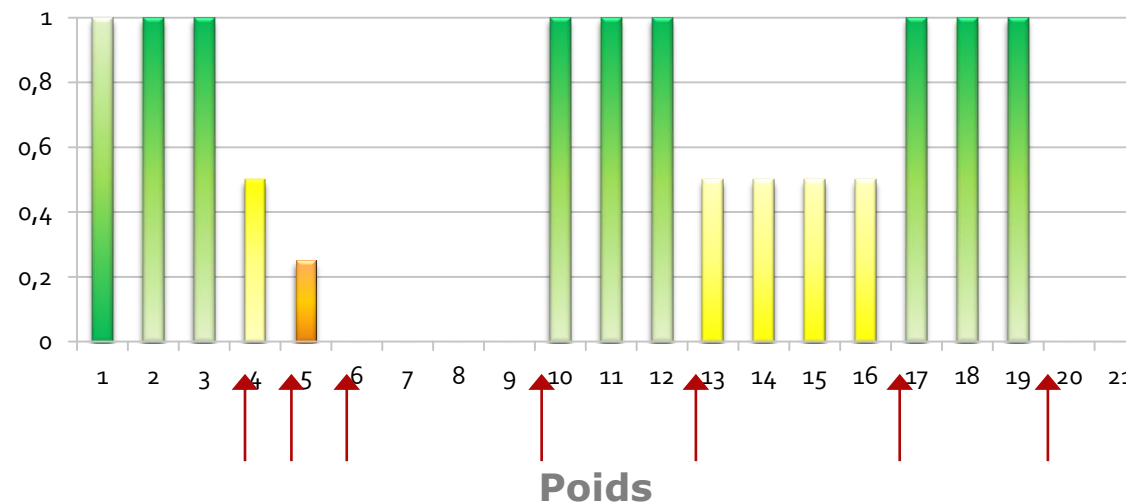
# Le bagotement (2)

Variation des états

- Exemple
  - 7 changements d'états
  - $7/20 = 35\%$

On applique la pondération  
 $6,96/20 = 34,8\%$

$34,8\% > \text{high\_service\_flap\_threshold (20 par défaut)}$   
⇒ Détection d'un bagotement



# Performance

- Le traitement des données de performance

process\_perf\_data [0|1]



- Dépendance des directives principales

- Nagios seul  $\Rightarrow$  pas de traitement
- Nagios avec greffon  $\Rightarrow$  possibilité de traitement

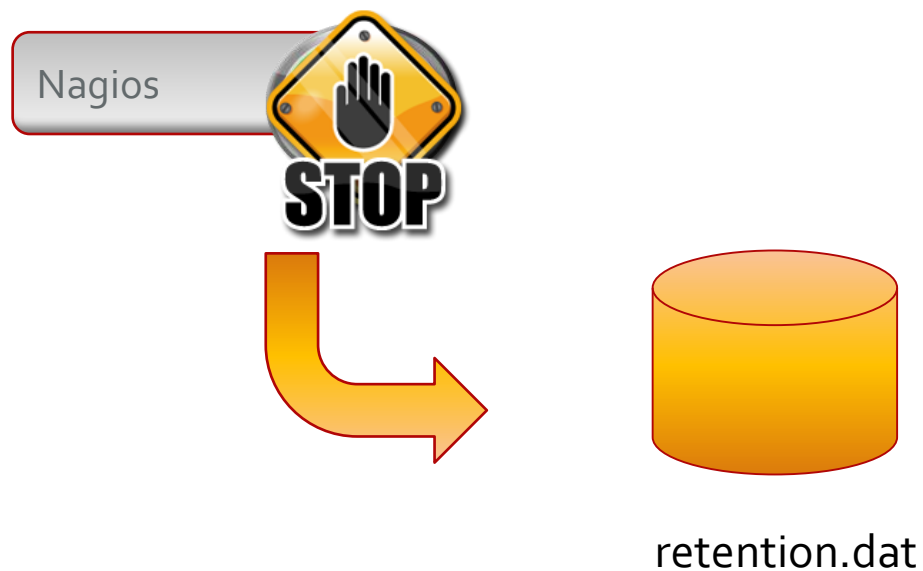


# Statistique et état

- Stockage des états lors de l'arrêt de Nagios

retain\_status\_information [o|d|u]

retain\_nonstatus\_information number\_timeperiod



# Les contacts et la notification

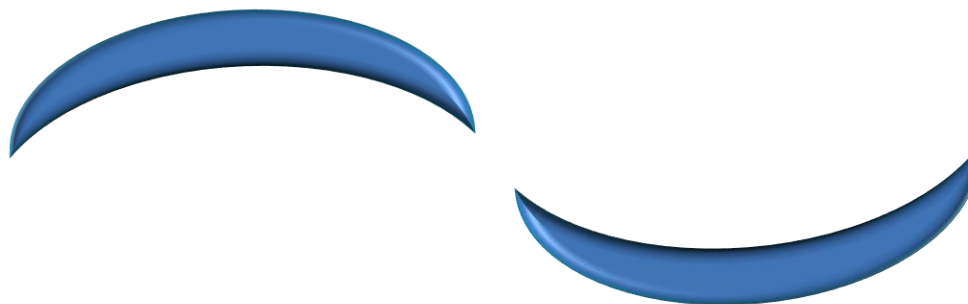
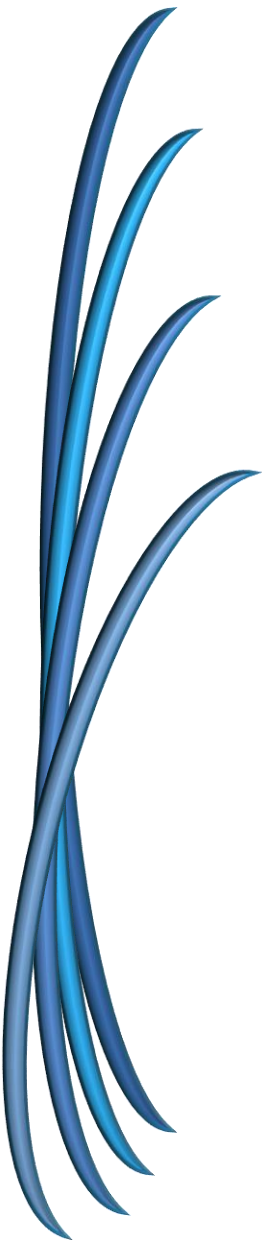
- Contact

- Par défaut, nous avons précisé que la directive « `contact_groups` » était la plus souvent utilisé
- L'obligation est de définir au moins une des 2 directives
  - `contacts`
  - `contact_groups`

- Notification

<code>notification_interval</code>	<code>#</code>
<code>notification_period</code>	<code>timeperiod</code>
<code>notification_option</code>	<code>[d u r f]</code>
<code>first_notification_delay</code>	<code>#</code>
<code>notifications_enabled</code>	<code>[0 1]</code>





# les actions

Configuration avancée



# Introduction au macro

**resources.cfg**

- Définition des macros
  - \$USERx\$ avec x = [0-32]
- En standard
  - \$USER1\$ est le chemin d'accès aux plugins de surveillance (scripts & exécutables de contrôle)
    - /usr/local/nagios/libexec
  - \$USER2\$ est le chemin d'accès aux commandes externes (inhibé par défaut)
    - /usr/local/nagios/libexec/eventhandlers



# Les réactions sur événement

- Fonction
  - Résoudre automatiquement
  - Obtenir des diagnostics complémentaires au moment de la détection d'un événement particulier
- Associé aux hôtes et aux services
  - event\_handler            command\_name
  - event\_handler\_enabled   [0/1]
- Directive principale
  - « enable\_event\_handlers » dans « nagios.cfg » prime sur toute autre directive locale !





# Exemple d'actions

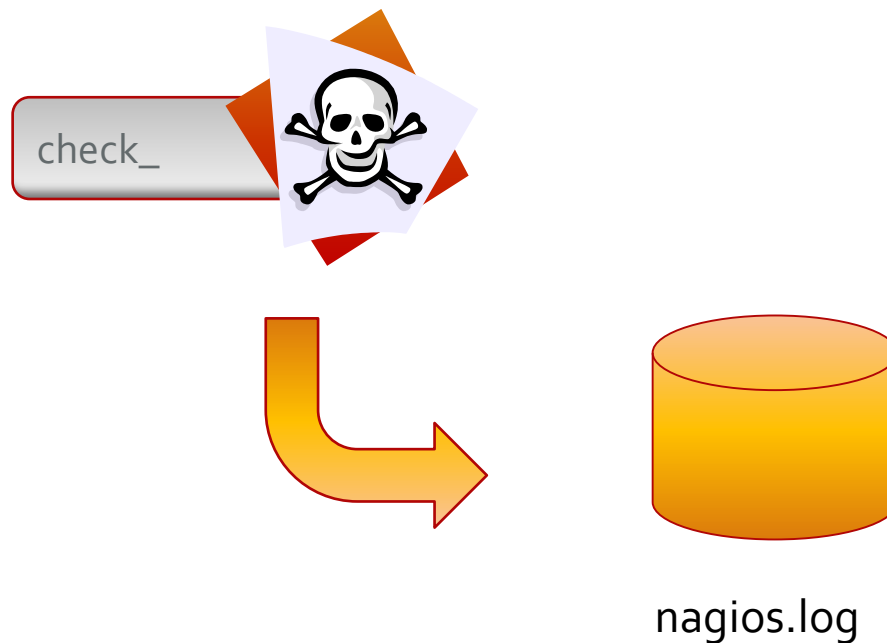
```
define service{  
    host_name          SrvWeb  
    service_description Site institutionnel  
    max_check_attempts 3  
    event_handler       restart-local-httpd  
    [...]                
}
```

```
define command{  
    command_name restart-local-httpd  
    command_line sudo $USER1$/eventhandlers/restart-httpd $SERVICESTATE$ $SERVICESTATETYPE$  
                  $SERVICEATTEMPT$  
}
```



# L'enregistrement dans le journal

- Analyse à posteriori
  - Une dernière directive commune aux services et aux hôtes  
stalking\_options [[o|d|u]][[o|w|c|u]]



# Les spécificités pour les services : la volatilité

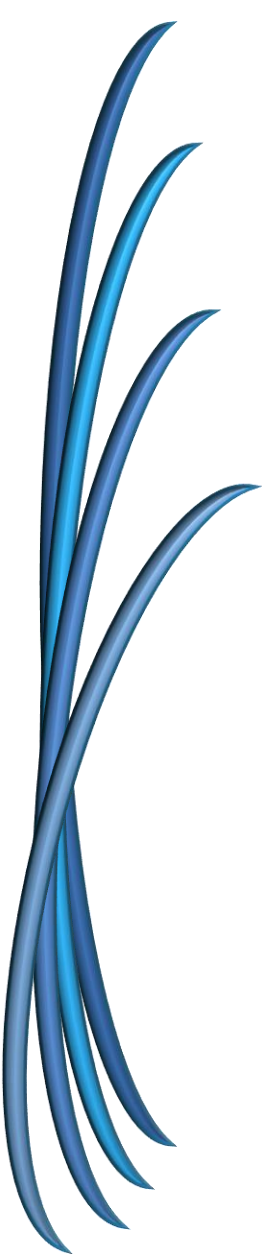
- La surveillance ou chaque changement d'état est indispensable

- is\_volatile[0|1]

- Exemple de définition pour un service de contrôle de fichier

```
define host{  
    ...  
    check_attempts      1  
    is_volatile         1  
    notification_options w,c  
    ...  
}
```





# Les dépendances

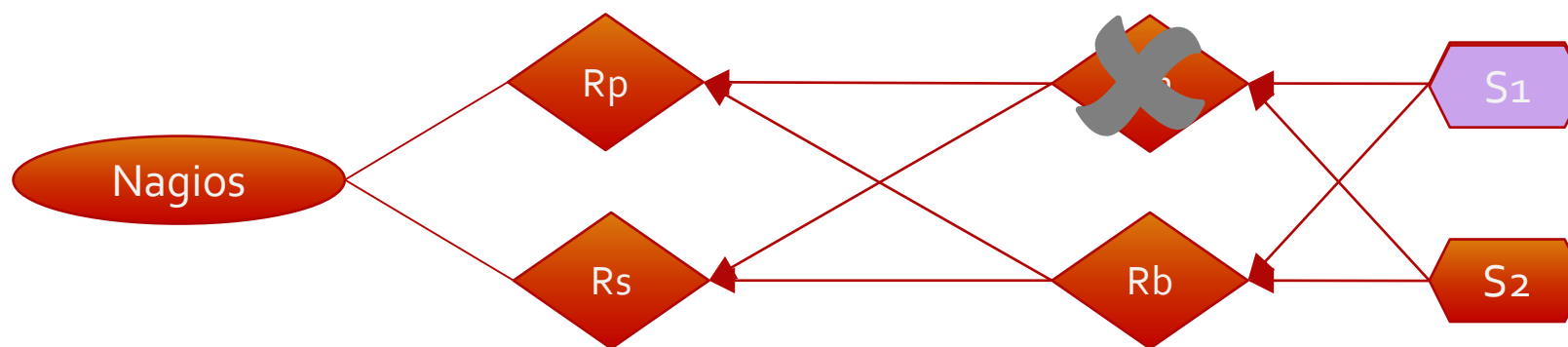
Configuration avancée



# Les dépendances topologiques

- dépendances topologiques
  - dépendances définis au travers des directives présentes dans la définition des hôtes

```
define host{  
    host_name    S1  
    parents      Rn  
}
```

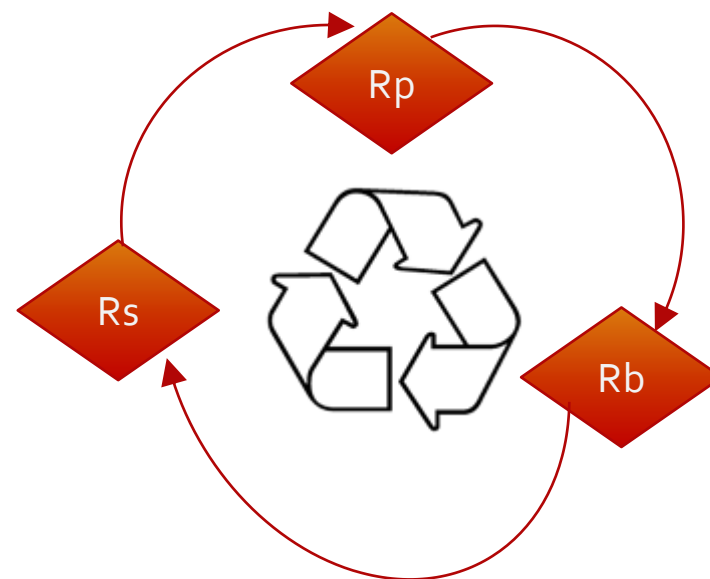




# Les dépendances topologiques

- Attention au(x) boucle(s)

```
define host{  
    host_name    Rp  
    parents    Rb  
}  
define host{  
    host_name    Rb  
    parents    Rs  
}  
define host{  
    host_name    Rs  
    parents    Rp  
}
```



# Les dépendances fonctionnelles

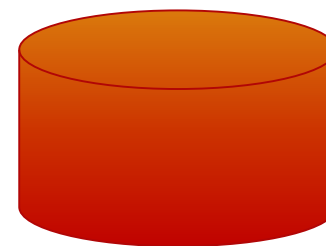
## dependencies.cfg

- dépendances fonctionnelles
  - dépendances définis au travers des directives présentes dans un fichier de configuration dédié

```
define servicedependency{  
    dependent_host_name      HBDD  
    dependent_service_description  SBDD  
    host_name                HSW  
    service_description      SW1  
    execution_failure_criteria c  
    notification_failure_criteria  n  
}
```



Service Web (SW1)  
Hôte HSW



Base de données (SBDD)  
Hôte HBDD



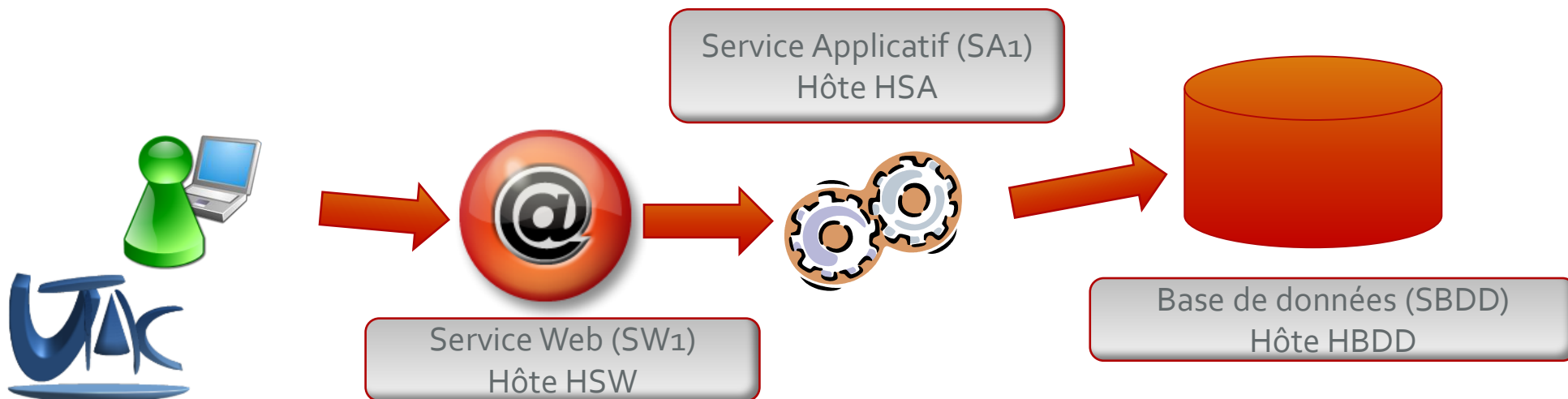
# Les dépendances fonctionnelles

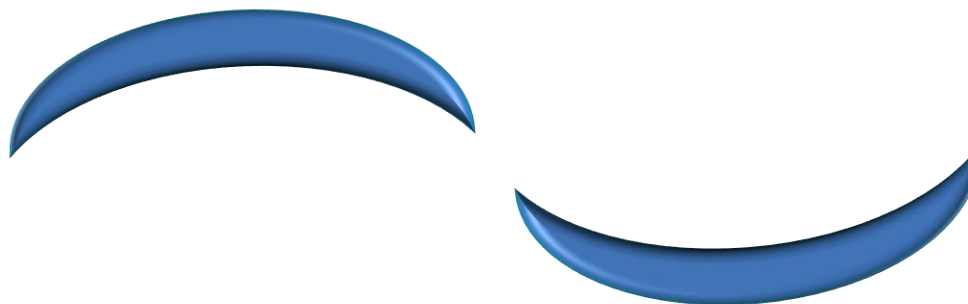
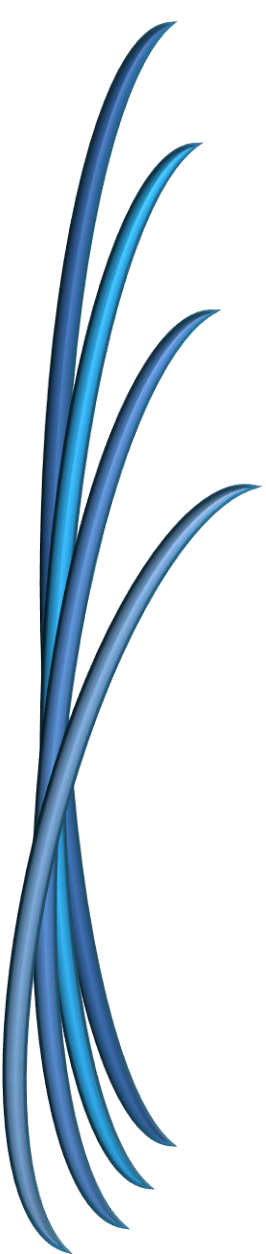
- Héritage des dépendances

- « inherits\_parent » directive positionnée à 1 pour la 1<sup>ère</sup> dépendance, à savoir SW1 ⇒ SA1 qui hérite de fait de la dépendance SA1 ⇒ SBDD

- Conclusion :

- Si SBDD est en warning ou critique ou si SA1 est en critique,
      - ✓ les contrôles sur SW1 sont suspendus
      - ✓ les notifications sur SW1 sont suspendus sauf si SBDD n'est que Warning





# Les escalades

Configuration avancée



# Les contacts

- Les directives complémentaires des contacts

```
define contact{  
    contact_name          contact_name  
    ...  
    email                 email_address  
    pager                 pager_number or pager_email_gateway  
    addressx              additional_contact_address  
    can_submit_commands [0/1]  
    retain_status_information [0/1]  
    retain_nonstatus_information [0/1]  
}
```



# Les escalades

**escalations.cfg**

- Problématique
  - Les événements remontent
  - Les notifications partent
  - Le problème persiste !
- Notification d'un niveau d'intervention plus fort
  - Nous sommes typiquement dans une problématique de gestion d'incidents et d'organisation de traitements
  - Attention aux effets de bords : le niveau 1 doit être au courant du fonctionnement
- « escalations.cfg »
  - Mise en place de la définition « serviceescalation »



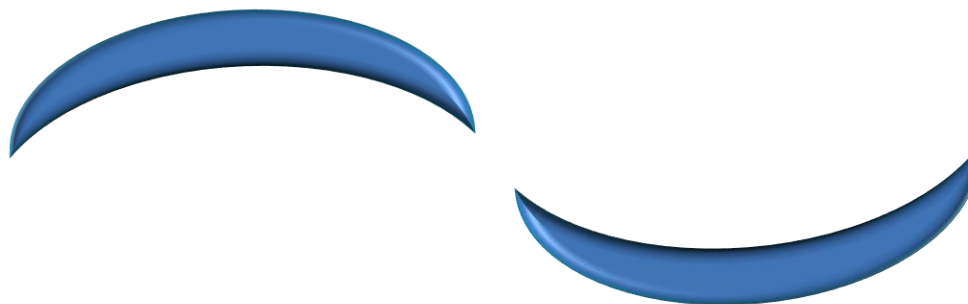
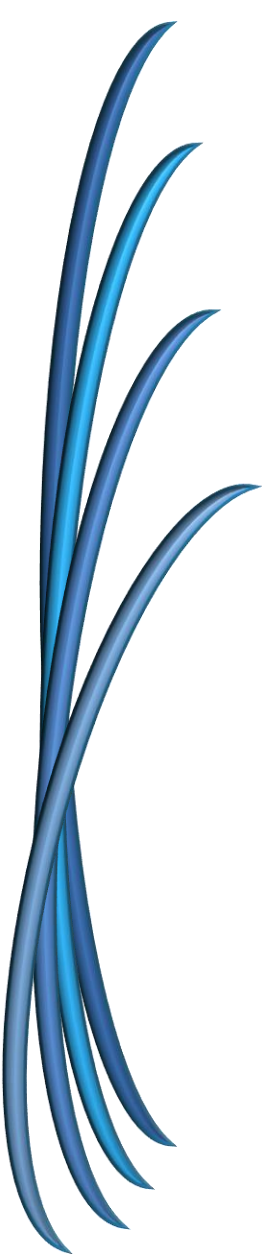
# Les escalades par l'exemple

```
define serviceescalation{
    host_name hostname
    hostgroup_name hostgrpname
    service_description svcdescr
    contacts contacts
    contact_groups ctctgrpname
    first_notification #
    last_notification #
    notification_interval #
    escalation_period timeperiod
    escalation_options [w,u,c,r]
}
```

```
define serviceescalation{
    host_name SW1
    service_description Http
    first_notification 3
    last_notification 4
    notification_interval 30
}

define serviceescalation{
    host_name SW1
    service_description Http
    first_notification 5
    last_notification 0
    notification_interval 60
    contact_groups support-level3
}
```





# Commandes externes

Configuration avancée



# Les commandes externes

- Des directives principales dans « nagios.cfg »
  - « check\_external\_commands » [0|1]
  - « command\_check\_interval » [-1|NbrePeriod]
  - « command\_file » <CheminFichier>

## Host Commands

- ✗ [Disable active checks of this host](#)
- 👤 [Re-schedule the next check of this host](#)
- ✓ [Start accepting passive checks for this host](#)
- ✗ [Stop obsessing over this host](#)
- 👤 [Acknowledge this host problem](#)
- ✗ [Disable notifications for this host](#)
- 👤 [Send custom host notification](#)
- 👤 [Delay next host notification](#)
- 👤 [Schedule downtime for this host](#)
- ✗ [Disable notifications for all services on this host](#)
- ✓ [Enable notifications for all services on this host](#)
- 👤 [Schedule a check of all services on this host](#)
- ✗ [Disable checks of all services on this host](#)
- ✓ [Enable checks of all services on this host](#)
- ✗ [Disable event handler for this host](#)
- ✗ [Disable flap detection for this host](#)

## External Command Interface

Last Updated: Tue Jun 29 18:18:07 CEST 2010  
Nagios® Core™ 3.2.0 - [www.nagios.org](http://www.nagios.org)  
Logged in as *fhma*

You are requesting to schedule downtime for a particular host

Command Options	Command Description
<p>Host Name: <input type="text" value="switch_001"/></p> <p>Author (Your Name): <input type="text" value="frank@fos-hugues"/></p> <p>Comment: <input type="text"/></p> <p>Triggered By: <input type="text" value="10.4"/></p> <p>Start Time: 29-06-2010 18:18:07</p> <p>End Time: 29-06-2010 20:18:07</p> <p>Type: <input type="text" value="Fixed"/></p> <p>If Flexible, Duration: <input type="text" value="2"/> Hours <input type="text" value="0"/> Minutes</p> <p>Child Hosts: <input type="text" value="Do nothing with child hosts"/></p> <p><input type="button" value="Commit"/> <input type="button" value="Reset"/></p>	<p>This command is used to schedule downtime for a particular host. During the specified downtime, Nagios will not send notifications out about the host. When the scheduled downtime expires, Nagios will send out notifications for the host as it normally would. Scheduled downtimes are processed across program invocations and reports. Both the start and end times should be specified in the following format: mmddyyyy HH:mm:ss. If you specify the end date, the downtime will be in effect between the start and end times you specify. If you do not specify the end date, Nagios will treat this as a "flexible" downtime. Flexible downtime starts when the host goes down or becomes unreachable (between the start and end times you specified) and lasts as long as the duration of time you enter. The duration fields do not apply for fixed downtime.</p>

Please enter all required information before committing the command.  
Required fields are marked in red.  
Failure to supply all required values will result in an error.

Your command request was successfully submitted to Nagios for processing.

Note: It may take a while before the command is actually processed.

[Done](#)



# Exemple : mise en maintenance d'un hôte

- Le format attendu par Nagios est :
  - `SCHEDULE_HOST_DOWNTIME;<host_name>;<start_time>;<end_time>;<fixed>;<trigger_id>;<duration>;<author>;<comment>`
  - `/bin/printf "[%lu]\n"`  
`SCHEDULE_HOST_DOWNTIME;Switch01;1110741500;1110748700;0;0;7200;FHMA;Livraison microcode attendue\n" $now > $commandfile`



# Utilisation pour les contrôles passifs

- Le mécanisme précédemment décrit est la base des contrôles passifs
  - Une application externe vérifie le fonctionnement d'un service
  - L'application écrit le résultat dans le processus de lecture des commandes externes
  - Nagios lit les arrivées des commandes externes et place les résultats dans une file d'attente des contrôles passifs pour traitement
  - Nagios scrute régulièrement cette file d'attente, fait le rapprochement avec les services et hôtes surveillés de manière passive et alimente la base de contrôle en fonction des résultats.

