

Seguretat i Administració de Xarxes

SEAX

Monitorització amb Nagios

Curs 2023-2024



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú



Pràctica 3 - Nagios

Índex

- Objectius
- Encaix en l'escenari de la pràctica 3
- Monitorització amb Nagios
 - Elements, objectes i plugins
 - Exemple
- Software: servidor & agent & plugins
- Bibliografia

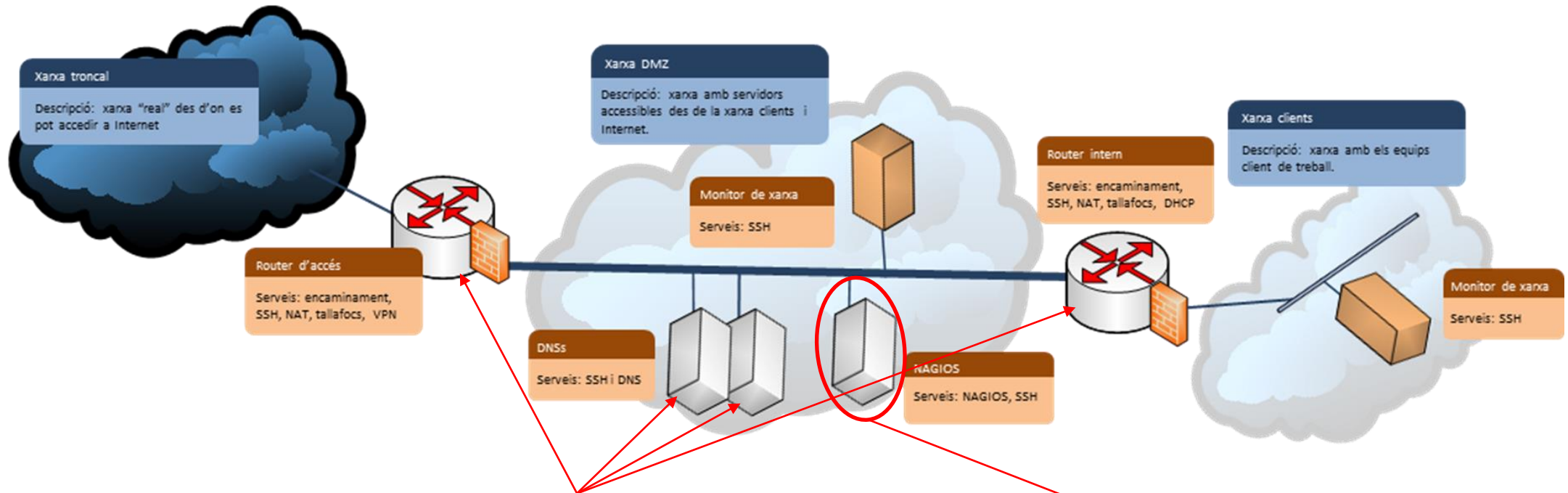
Nagios

Objectius

- ✓ Monitoritzar els elements que formen la nostra xarxa (i algun servei extern)
- ✓ Paràmetres d'interès (varien en funció de la màquina):
 - ✓ Càrrega, ocupació disc dur (partició de root) i RAM utilitzada
 - ✓ Connectivitat
 - ✓ Disponibilitat de serveis: SSH, HTTP, DNS i DHCP
 - ✓ Opcional: trànsit per interfície de xarxa
- ✓ Protegir el servidor Nagios

Monitorització amb Nagios

Encaix en l'escenari de la pràctica 3



Màquines monitoritzades
(+ serveis externs)

Servidor Nagios

Monitorització amb Nagios

Encaix en l'escenari de la pràctica 3

- ✓ **Servidor Nagios**
 - ✓ Ubicat a la xarxa de servidors
 - ✓ Veure equip i IP a la sessió 1 i 2
 - ✓ Ofereix una interfície Web
 - ✓ Accés amb login/password
 - ✓ Accessible només des dels monitors

Important

Cal utilitzar les següent
credencials per la compta
d'administrador de
Nagios
User: nagiosadmin
Password: seax2024

Monitorització amb Nagios

Encaix en l'escenari de la pràctica 3

- ✓ **Màquines monitoritzades** (+ serveis externs):
 - ✓ El propi servidor
 - ✓ Servidors DNS
 - ✓ Routers
- ✓ Cal instal·lar un software (agent) per a que puguin ser monitoritzades des del servidor Nagios

Monitorització amb Nagios

Encaix en l'escenari de la pràctica 3

- ✓ Introduir el servidor Nagios
- ✓ Comprovar que podem monitoritzar el propi servidor i després els serveis públics que es troben a Internet
- ✓ Comprovar que té connectivitat amb la resta de màquines a monitoritzar
- ✓ Comprovar que el servidor pot comunicar-se amb els agents d'aquestes màquines
- ✓ Comproveu des de la UI del servidor que la monitorització de les màquines amb agents funciona correctament

En aquest punt, podeu garantir que podeu monitoritzar tots els elements de la xarxa i els serveis públics que s'han indicat

Monitorització amb Nagios

Per què Nagios?
Comunitat d'usuaris
Capacitat de
customització

Introducció

No confondre:
Nagios Core: open
source
Nagios XI: pagament

- ✓ Monitoritzar no és administrar equips. Volem:
 - ✓ Veure les constants vitals
 - ✓ Reportar esdeveniments, recopilar logs, generar avisos,...
- ✓ Hi ha forces eines open source:

Nagios®

ZABBIX



Monit



checkmk



LibreNMS



Prometheus

cacti

openNMS®
group



icinga



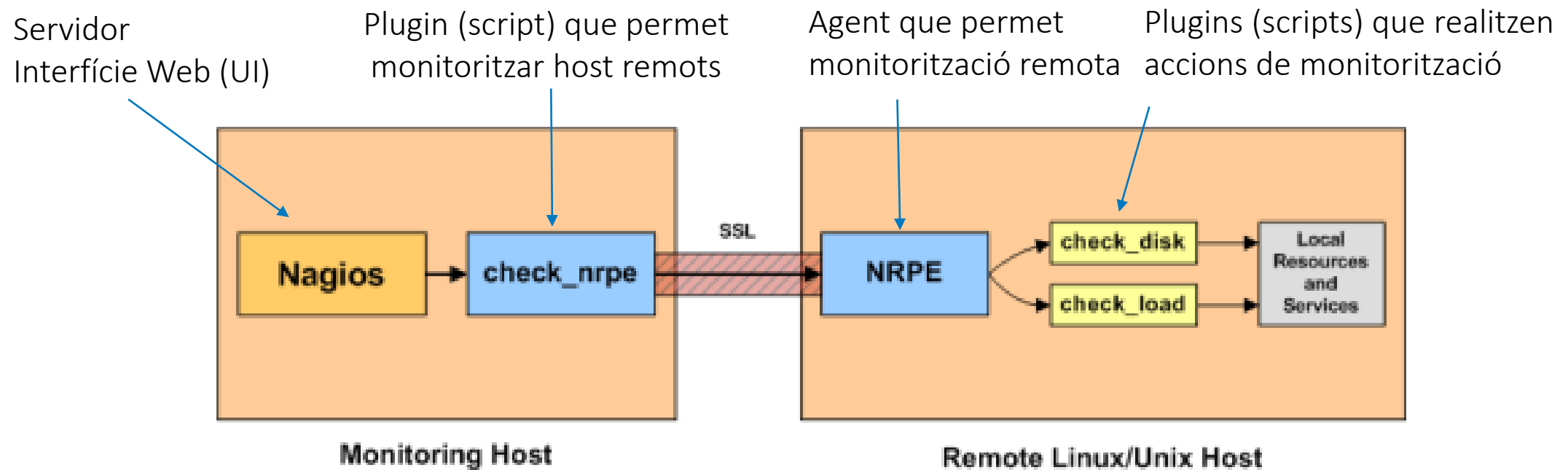
NETDATA



Grafana

Monitorització amb Nagios

Elements



Altres possibilitats: màquines Windows amb l'agent ncpa; monitorització de dispositius de xarxa (per ex. routers, switch, impressores) amb SNMP enlloc d'agents; monitorització de serveis públics (per ex. DNSs, pàgines Web o servidors de correu) accedint als seus ports, iniciant algun diàleg o fent-los pings


Monitorització amb Nagios

Objectes

- ✓ Definicions que permeten configurar el sistema
 - ✓ Veure fitxers *.cfg a `/usr/local/nagios/etc/`
 - ✓ `nagios.cfg`: fitxer on cal declarar tots els altres
 - ✓ Subdirectori `objects`: fitxers d'exemple
 - ✓ Sintaxi basada en directives (parelles variable-valor)
 - ✓ Orientat a objectes (herència)

Monitorització amb Nagios

Objectes (II)

- ✓ Necessaris per aquesta pràctica:
- 
Host. Un per cada màquina a monitoritzar i també pel servidor
 - ✓ Veure llista a l'enunciat de la sessió
 - Host groups.** N'haureu de definir 3, de nom:
 - ✓ routers, dns i servidors-externs
 - ✓ Veure contingut a l'enunciat de la sessió

Important



Per claredat, utilitzeu un fitxer per cada Host o com a mínim per a cada grup de hosts

Monitorització amb Nagios

Important

A la declaració d'un servei podeu fer constar més d'un host o tot un grup de hosts

Objectes (III)

- ✓ Necessaris per aquest pràctica:
- 
 - ✓ **Service.** Acció de monitorització (veure plugins) que es realitzarà per un Host en particular
 - ✓ Es declaren al fitxer `.cfg` on s'ha declarat el Host
- 
 - ✓ **Command.** Mapeig entre una acció declarada a `Service` i la seva comanda, ie. crida a l'script (veure plugins).
 - ✓ Es declaren a
 - `/etc/local/nagios/etc/objects/commands.cfg` o
 - `/etc/local/host/nagios/etc/nrpe.cfg` (veure plugins)

Monitorització amb Nagios

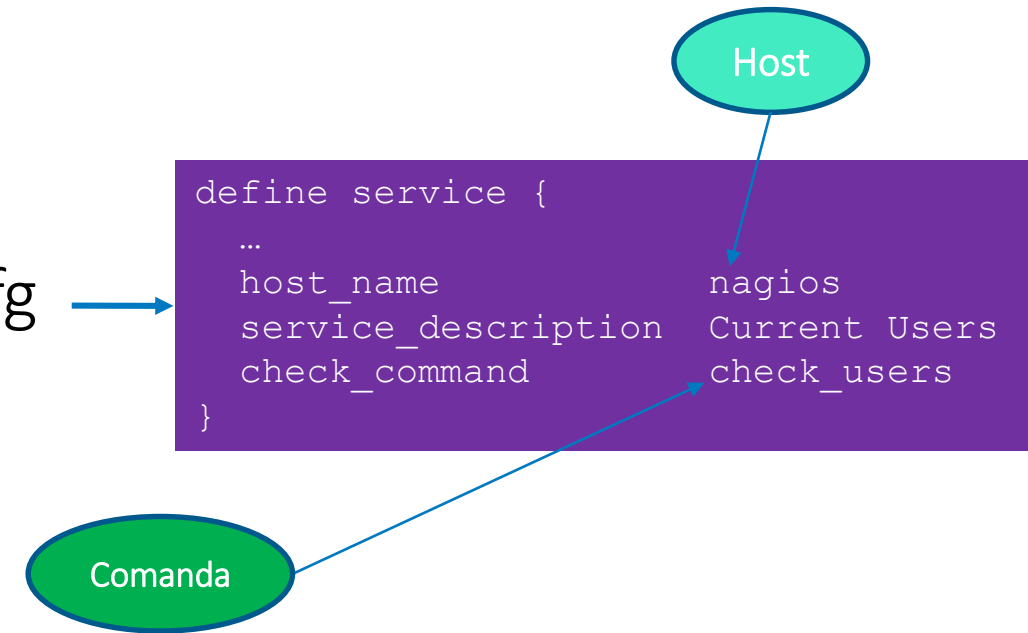
Plugins

- ✓ Scripts que s'executaran per a realitzar una determinada acció de monitorització
 - ✓ Per ex., un ping per fer un test de connectivitat
- ✓ Diferenciarem
 - ✓ Paquet de plugins oficial (veure bibliografia)
 - ✓ Plugins de tercers
 - ✓ Instal·larem quan no trobem la funció desitjada en el paquet oficial
 - ✓ Fixar-se en: compatibilitat amb versió de Nagios, llenguatge (bash) i instruccions ús

Monitorització amb Nagios

Plugins (II)

- ✓ Execució en el servidor: per a monitoritzar el propi servidor o serveis públics
- 1. Copiar l'script a
 /usr/local/nagios/libexec
- 2. Declarar-lo com a servei al fitxer *.cfg
 corresponent
- 3. Associar-lo a una comanda al fitxer
 command.cfg



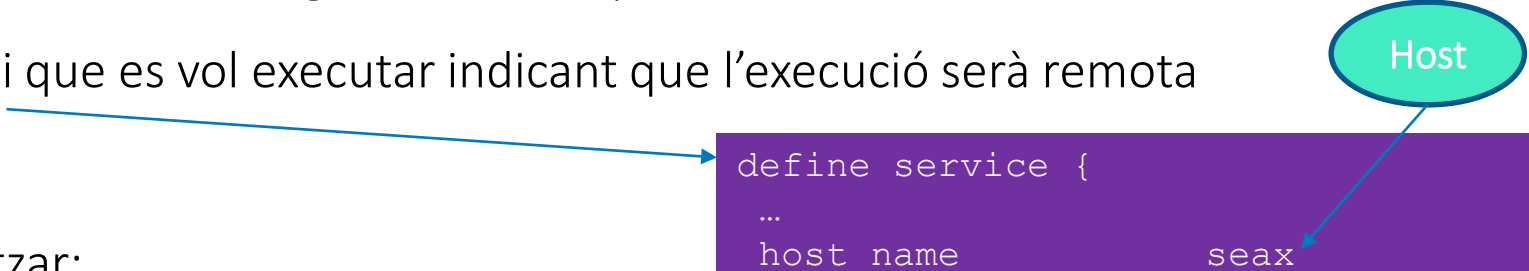
Monitorització amb Nagios

Plugins (II)

- ✓ Execució en l'agent: per a monitoritzar màquines remotament
- ✓ Al servidor:
 - ✓ Cal instal·lar i declarar com a comanda el plugin **check_nrpe**
 - ✓ Estableix comunicació amb l'agent, li indica que cal executar i en recull el resultat
 - ✓ Cal declarar el servei que es vol executar indicant que l'execució serà remota

- ✓ A la màquina a monitoritzar:

- ✓ Instal·lar l'agent nrpe
- ✓ Instal·lar l'script a `/usr/local/nagios/libexec`
- ✓ Declarar la comanda al fitxer `/etc/local/host/nagios/etc/nrpe.cfg`



```

define service {
    ...
    host_name          seax
    service_description Current Users
    check_command check_nrpe!check_users
}
  
```

Monitorització amb Nagios

Plugins (IV)

- ✓ Declaració de comandes. Pas de paràmetres:
 - ✓ Scripts inclouen `-h` per indicar opcions possibles
 - ✓ És poden utilitzar macros. Per ex. `$USER1$`, `$HOSTADDRESS$`, `$ARG1$` o `$ARG2$`
 - ✓ Per claredat i seguretat es recomana definir comandes amb paràmetres *hard coded*
 - ✓ Menys flexible
 - ✓ Permet assegurar (a l'agent) com s'executarà la comanda

```
define command {
  command_name check-host-alive
  command_line $USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100% -p 5
}
```

Declarat al
Servei

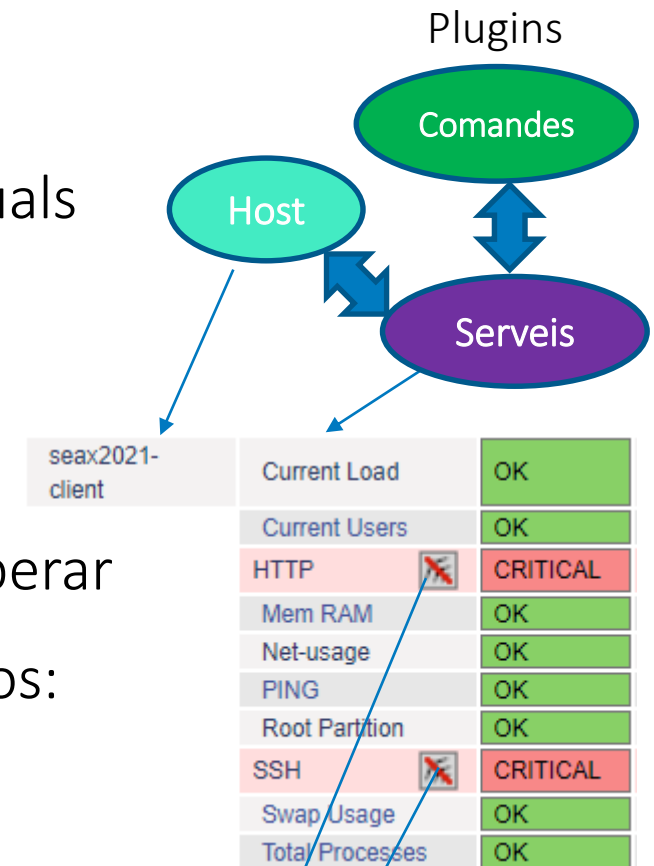
Paràmetres hard coded

Paràmetres passats amb macros

Monitorització amb Nagios

Plugins (V)

- ✓ Permeten definir llindars (***thresholds***), valors a partir dels quals es genera un avís:
 - ✓ Warning (-w): defineix un nivell que es considera perillós/significatiu sobrepassar
 - ✓ Critical (-c): defineix un nivell que es considera crític superar
- ✓ Facilita identificació ràpida estat servei/host a la UI de Nagios:
 - ✓ Verd: OK
 - ✓ Groc: warning
 - ✓ Vermell: crític



Indica notificacions deshabilitades
 Només si no es volen guardar els avisos

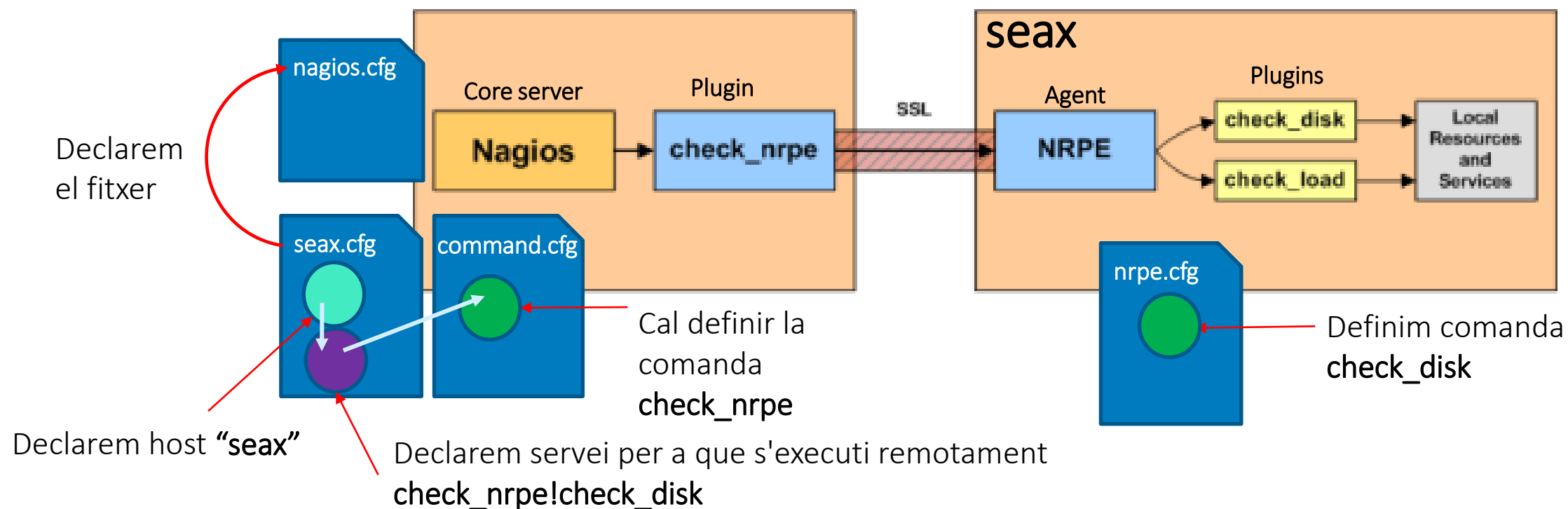
Monitorització amb Nagios

Important

Consulteu fitxers d'exemple i bibliografia sobre NRPE per veure exemples de sintaxis

Exemple

- ✓ Monitorització espai lliure del disc dur màquina "seax"



Nagios

Software

- ✓ Nagios core
 - ✓ Servidor Nagios
- ✓ NRPE
 - ✓ Agent nrpe
- ✓ Nagios Plugins
 - ✓ Plugins per defecte
- ✓ Plugin nrpe
 - ✓ Plugin per executar scripts en màquines remotes

Nagios®

Nagios

Software – Servidor Nagios

- ✓ En aquest ordre (entre []) nº enllaç de la part d'instal·lació de la bibliografia):
 1. Nagios core [1]
 2. Nagios Plugins [2]
 3. Plugin nrpe [3]
 4. Altres plugins per cobrir necessitats específiques

Avís

La instal·lació de Nagios Core amb apt-get no funciona al 100% i utilitza directoris diferents.

No la feu servir

Si heu fet la instal·lació bé hauríeu de veure això

Nagios®

General

[Home](#)
[Documentation](#)

Current Status

[Tactical Overview](#)
[Map \(Legacy\)](#)
[Hosts](#)
[Services](#)
[Host Groups](#)
 [Summary](#)
 [Grid](#)
[Service Groups](#)
 [Summary](#)
 [Grid](#)
[Problems](#)
 [Services \(Unhandled\)](#)
 [Hosts \(Unhandled\)](#)
 [Network Outages](#)

Quick Search:

Reports

[Availability](#)
[Trends \(Legacy\)](#)
[Alerts](#)
 [History](#)
 [Summary](#)
 [Histogram \(Legacy\)](#)
[Notifications](#)
[Event Log](#)

System

[Comments](#)
[Downtime](#)
[Process Info](#)
[Performance Info](#)
[Scheduling Queue](#)
[Configuration](#)

Nagios® Core™

✓ Daemon running with PID 1041

Nagios® Core™
Version 4.4.14

August 01, 2023
[Check for updates](#)

Get Started

- [Start monitoring your infrastructure](#)
- [Change the look and feel of Nagios](#)
- [Extend Nagios with hundreds of addons](#)
- [Get support](#)
- [Get training](#)
- [Get certified](#)

Quick Links

- [Nagios Library](#) (tutorials and docs)
- [Nagios Labs](#) (development blog)
- [Nagios Exchange](#) (plugins and addons)
- [Nagios Support](#) (tech support)
- [Nagios.com](#) (company)
- [Nagios.org](#) (project)

Latest News

Don't Miss...

Copyright © 2010-2023 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, Nagios Core and the Nagios logo are trademarks, servicemarks, registered trademarks or registered servicemarks owned by Nagios Enterprises, LLC. Use of the Nagios marks is governed by the [trademark use restrictions](#).



Nagios

Software – Màquines a monitoritzar

- ✓ En aquest ordre (entre [] n^o enllaç de la part d'instal·lació de la bibliografia):
 1. NRPE [3]
 2. Nagios Plugins [2]
 3. Altres plugins per cobrir necessitats específiques

Recomanació

Podeu estalviar temps instal·lant els paquets corresponents amb apt-get



Atenció

Els directoris canvien:
configuració ara és
`/usr/local/` i els plugins són
a `/usr/lib/nagios/plugins`

Nagios

Bibliografia (II)

- ✓ Instal·lació
 1. Servidor: <https://support.nagios.com/kb/article/nagios-core-installing-nagios-core-from-source-96.html#Debian>
 2. Plugins per defecte: <https://support.nagios.com/kb/article/nagios-plugins-installing-nagios-plugins-from-source-569.html>
 3. Agent nrpe: <https://support.nagios.com/kb/article.php?id=515>
 4. Requeriments per instal·lar els plugins (alguns en tenen):
<https://support.nagios.com/kb/article/nagios-plugins-installing-nagios-plugins-from-source-569.html#Debian>
 5. Plugin check_nrpe: veure «Install the check_nrpe Plugin» a «Utilització de l'agent NRPE».
<https://support.nagios.com/kb/article.php?id=515#Debian> Utilitzeu però la darrera versió publicada: <https://github.com/NagiosEnterprises/nrpe/releases/tag/nrpe-4.1.0>

Nagios

Bibliografia

- ✓ General
 - ✓ Documentació Nagios Core 4: <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/>
 - ✓ Utilització de l'agent NRPE: <https://assets.nagios.com/downloads/nagioscore/docs/nrpe/NRPE.pdf>
- ✓ Configuració
 - ✓ Objectes: <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/objectdefinitions.html>
 - ✓ Sintaxis crides serveis i comandes (macros):
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/macros.html>
- ✓ Plugins
 - ✓ Oficials <http://nagios-plugins.org/doc/man/index.html>
 - ✓ De tercers: <https://exchange.nagios.org/directory/Plugins>
 - ✓ Com crear-ne: <https://nagios-plugins.org/doc/guidelines.html> &
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/pluginapi.html>

Seguretat i Administració de Xarxes



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

