



# **Comparativa d'eines de monitorització de sistemes**

**PFC – Xarxes de computadors**

**Sandra González Álvarez**  
Enginyeria Informàtica

**Consultor: Jordi Ceballos Villach**

**Data: 14 de Març de 2011**



**2010**



- Buenos días -dijo el principito.
- Buenos días -dijo el guardaagujas.
- ¿Qué haces aquí? -dijo el principito.
- Clasifico a los viajeros por paquetes de mil -dijo el guardaagujas-. Despacho los trenes que los llevan, tanto hacia la derecha como hacia la izquierda.

Y un rápido iluminado, rugiendo como el trueno, hizo temblar la cabina de las agujas.

- Llevan mucha prisa -dijo el principito-. ¿Qué buscan?
- Hasta el hombre de la locomotora lo ignora -dijo el guardaagujas.

Y un segundo rápido iluminado rugió, en sentido inverso.

- ¿Vuelven ya? -preguntó el principito?
- No son los mismos -dijo el guardaagujas-. Es un cambio.
- ¿No estaban contentos donde estaban?
- Nadie está nunca contento donde está -dijo el guardaagujas.

Y rugió el trueno de un tercer rápido iluminado.

- ¿Persiguen a los primeros viajeros? -preguntó el principito.
- No persiguen absolutamente nada -dijo el guardaagujas-. Ahí dentro duermen o bostezan. Sólo los niños aplastan sus narices contra los vidrios.
- Sólo los niños saben lo que buscan -dijo el principito-. Pierden tiempo por una muñeca de trapo y la muñeca se transforma en algo muy importante, y si se les quita la muñeca, lloran...
- Tienen suerte -dijo el guardaagujas.

“El Principito”  
A. Saint-Exupery

## **Resum**

El següent projecte està estructurat en tres fases, les quals tenen com objectiu la comparació d'eines de monitorització de sistemes.

Una primera fase d'introducció on comentaré la importància de la monitorització de sistemes i de la descripció de com seleccionar la millor eina.

En la segona fase em centraré en l'estudi de cadascuna de les eines.

I per últim una tercera fase de conclusions i les línees obertes del projecte.

## **Resumen**

El siguiente proyecto está estructurado en tres fases, las cuales tienen como objetivo la comparación de herramientas de monitorización de sistemas.

En la primera fase de Introducción donde comentaré la importancia de la monitorización de sistemas i de la descripción de cómo seleccionar la mejor herramienta.

En la segunda fase me centraré en el estudio de las diferentes herramientas.

I per último, una tercera fase de conclusiones i las líneas abiertas del proyecto.

## **Abstract**

The following project is constructed in three phases, which are aimed at the comparison of system monitoring tools.

In the first phases of introduction which comment on the importance of monitoring the systems and the description of how to select the best tool.

In the second phase I will concentrate on the study of the different tools.

And finally, a third phase of conclusions and open lines of the project.

# Índex

|       |   |    |
|-------|---|----|
| 1     | Introducció.....  | 7  |
| 1.1   | Justificació i context del projecte.....                        | 7  |
| 1.2   | Descripció del projecte.....                                    | 7  |
| 1.3   | Requeriments maquinari / programari / documentació / eines..... | 8  |
| 1.4   | Descripció de tasques:.....                                     | 8  |
| 1.5   | Anàlisi de riscos.....  | 10 |
| 2     | Introducció a la monitorització de sistemes.....                | 11 |
| 2.1   | Definició de monitorització de sistemes.....                    | 11 |
| 2.2   | Qui utilitzarà un sistema de monitorització.....                | 12 |
| 2.3   | Com impacta un sistema de monitorització.....                   | 12 |
| 2.4   | Elecció d'un sistema de monitorització.....                     | 12 |
| 2.5   | Selecció de la millor eina.....                                 | 13 |
| 3     | Preparació de l'entorn.....                                     | 14 |
| 3.1   | Elecció i instal·lació del Sistema Operatiu.....                | 14 |
| 3.2   | Descàrrega de les diferents eines de monitorització.....        | 14 |
| 4     | Estudi de l'eina Nagios.....                                    | 15 |
| 4.1   | Què és Nagios?.....   | 15 |
| 4.2   | Objectius i necessitats.....                                    | 15 |
| 4.3   | Característiques generals.....                                  | 15 |
| 4.4   | Què és pot fer amb Nagios.....                                  | 17 |
| 4.5   | Requeriments del sistema.....                                   | 17 |
| 4.6   | Instal·lació bàsica de Nagios.....                              | 19 |
| 4.6.1 | Prerequisits.....   | 19 |
| 4.6.2 | Crear informació de compte d'usuari.....                        | 19 |
| 4.6.3 | Compilar i instal·lar Nagios.....                               | 20 |
| 4.6.4 | Personalitzar la configuració.....                              | 20 |
| 4.6.5 | Configurar la interfície web.....                               | 21 |
| 4.6.6 | Iniciar Nagios.....   | 21 |
| 4.6.7 | Entrar en la interfície Web.....                                | 22 |
| 4.6.8 | Altres configuracions.....                                      | 24 |
| 4.7   | Monitoritzar equips amb Windows.....                            | 25 |
| 4.8   | Monitoritzar equips amb Linux/Unix.....                         | 26 |
| 4.9   | Monitoritzar Routers i Switches.....                            | 27 |
| 4.10  | Exemple de Monitorització.....                                  | 29 |
| 4.11  | Monitoritzar amb Centreon.....                                  | 31 |
| 4.12  | Resum eina.....   | 34 |
| 4.13  | Conclusions.....  | 34 |
| 5     | Estudi de l'eina Pandora FMS.....                               | 35 |
| 5.1   | Què és Pandora FMS?.....  | 35 |
| 5.2   | Objectius i necessitats.....                                    | 36 |
| 5.3   | Característiques generals.....                                  | 37 |
| 5.4   | Què es pot fer amb Pandora FMS.....                             | 39 |
| 5.5   | Requeriments del sistema.....                                   | 39 |

|       |  |    |
|-------|--|----|
| 5.5.1 | Requisits mínims de hardware .....         | 39 |
| 5.5.2 | Requisits mínims de software .....         | 40 |
| 5.6   | Instal·lació bàsica de Pandora FMS.....    | 40 |
| 5.6.1 | Prerequisits:.....                         | 41 |
| 5.6.2 | Instal·lació .....                         | 41 |
| 5.7   | Monitoritzar equips amb Windows .....      | 43 |
| 5.8   | Monitoritzar equips amb Linux / Unix ..... | 43 |
| 5.9   | Monitoritzar Routers i Switches.....       | 43 |
| 5.10  | Reconeixement mapa de xarxa.....           | 43 |
| 5.11  | Exemples de monitoritzacions.....          | 45 |
| 5.12  | Resum eina .....                           | 48 |
| 5.13  | Conclusions .....                          | 48 |
| 6     | Estudi de l'eina i-enable rmf .....        | 49 |
| 6.1   | Què és i-enable rmf? .....                 | 49 |
| 6.2   | Objectius i necessitats.....               | 49 |
| 6.3   | Característiques generals .....            | 50 |
| 6.4   | Que es pot fer amb i-enable rmf.....       | 51 |
| 6.5   | Requeriments del sistema.....              | 52 |
| 6.6   | Pantalles eina .....                       | 53 |
| 6.7   | Resum de l'eina.....                       | 55 |
| 6.8   | Conclusions .....                          | 56 |
| 7     | Estudi de l'eina Zabbix .....              | 57 |
| 7.1   | Què és Zabbix? .....                       | 57 |
| 7.2   | Objectius i necessitats.....               | 57 |
| 7.3   | Característiques generals .....            | 58 |
| 7.4   | Que es pot fer amb Zabbix?.....            | 59 |
| 7.5   | Requeriments del sistema.....              | 59 |
| 7.6   | Pantalles eina .....                       | 60 |
| 7.7   | Resum de l'eina.....                       | 61 |
| 7.8   | Conclusions .....                          | 61 |
| 8     | Comparativa .....                          | 62 |
| 8.1   | Taula comparativa .....                    | 62 |
| 8.2   | Resum de l'anàlisi .....                   | 63 |
| 9     | Conclusions .....                          | 64 |
| 9.1   | Conclusions .....                          | 64 |
| 9.2   | Línees obertes.....                        | 64 |
|       | Bibliografia.....                          | 65 |
|       | Llibres .....                              | 65 |
|       | Internet .....                             | 65 |
|       | Annex 1: Taula comparativa eines .....     | 67 |
|       | Índex de Figures.....                      | 69 |
|       | Índex de Taules .....                      | 71 |

## 1 Introducció

En aquest apartat procedirem realitzar una introducció general al treball, on explicarem la motivació, objectius i la planificació prevista per la realització del projecte.

### 1.1 Justificació i context del projecte

L'àrea d'aquest projecte és Xarxes de Computadors, on m'he intentat especialitzar durant tota l'Enginyeria d'Informàtica (incloent la Tècnica).

El Projecte Final de Carrera és una bona oportunitat (tot i que una miqueta just en el temps) que se'm brinda per tal de poder posar en pràctica els coneixements teòrics adquirits i ampliar-los amb la part pràctica, a més de permetre'm estudiar tres eines que són molt útils per al manteniment d'aquests sistemes.

### 1.2 Descripció del projecte

L'objectiu d'aquest projecte és realitzar una comparativa d'eines de monitorització de sistemes. Per a poder-ho portar a terme hauré d'instal·lar i configurar una xarxa en un servidor Linux(en el meu cas escolliré Ubuntu) per tal de cobrir els requeriments mínims amb els que aquestes eines poden treballar, o bé són més eficients.

Una vegada tinguem preparat l'entorn podrem començar amb l'estudi de cadascuna de les eines i per això s'ha de tenir en compte que alhora d'escollir una eina de monitorització de sistemes s'ha de respondre a aquestes tres preguntes:

- ✓ Com volem veure les dades, alarmes, gràfics, ... tenint en compte que han d'ésser eficients i mostrar els errors fàcilment.
- ✓ Quin tipus de connexió entre equips hi ha (en connexions ràpides però amb molts equips o en connexions lentes hauríem d'utilitzar agents que ens enviïn la informació al servidor central).
- ✓ Quins són els Sistemes Operatius dels equips a monitoritzar.

He intentat programar quatre eines per a fer la comparativa però el calendari no m'ho ha permès, en cas que donés temps afegiria una eina a la comparativa.

Els objectius parcials per assolir-lo són els següents :

- ✓ Preparació de l'entorn
- ✓ Estudi de cadascuna de les eines
- ✓ Preparar un joc de proves per a cada eina
- ✓ Realitzar proves comparatives entre eines
- ✓ Extreure conclusions de les proves comparatives
- ✓ Programar un agent i realitzar proves

### 1.3 Requeriments maquinari / programari / documentació / eines

- ✓ Servidor Ubuntu amb Apache, MySQL, PHP.
- ✓ Eines de monitorització de sistemes (Nagios, Pandora FMS i Zabbix)
- ✓ Equips Windows i Microsoft Office 2007.

### 1.4 Descripció de tasques:

S'ha calculat un calendari de dilluns a divendres amb una horari de 3h diàries i els caps de setmana fer-hi una dedicació de 10 hores, tenint en compte que els diferents lliuraments no es poden modificar. Fent una previsió de 303 hores per la realització del projecte. Aquesta dedicació horària es podrà modificar depenent de les dificultats en les que em vagi trobant durant l'execució del projecte.




























|    |    | Nombre de tarea   | Comienzo     | Fin          | Predecesoras |
|----|---|---|--------------|--------------|--------------|
| 1  |   | [-] <b>Projecte Comparativa d'eines de monitorització de sistemes</b> | mié 02/03/11 | vie 17/06/11 |              |
| 2  |   | [-] <b>0. Definició i Planificació del Projecte</b>                   | mié 02/03/11 | lun 14/03/11 |              |
| 3  |    | 0.1. Definició de l'àmbit del projecte                                | mié 02/03/11 | vie 11/03/11 |              |
| 4  |   | [-] <b>0.2. Planificació</b>  | vie 11/03/11 | lun 14/03/11 |              |
| 5  |    | 0.2.1. Definició de tasques   | vie 11/03/11 | sáb 12/03/11 | 3            |
| 6  |   | 0.2.2. Planificació de les tasques                                    | sáb 12/03/11 | lun 14/03/11 | 5            |
| 7  |    | <b>Lliurament PAC 1</b>   | lun 14/03/11 | lun 14/03/11 | 6            |
| 8  |   | [-] <b>1. Preparació entorn</b>                                       | mar 15/03/11 | vie 18/03/11 |              |
| 9  |  | 1.1. Instal·lar servidor Linux  | mar 15/03/11 | jue 17/03/11 |              |
| 10 |  | 1.2. Descarrega eines monitorització                                  | vie 18/03/11 | vie 18/03/11 | 9            |
| 11 |   | [-] <b>2. Estudi eina Nagios</b>                                      | mar 15/03/11 | lun 21/03/11 |              |
| 12 |  | 2.1. Anàlisi característiques de feina                                | mar 15/03/11 | jue 17/03/11 |              |
| 13 |  | 2.2. Instal·lació de feina  | vie 18/03/11 | vie 18/03/11 | 10;12        |
| 14 |  | 2.3. Aprendre utilitzar eina Nagios                                   | vie 18/03/11 | lun 21/03/11 | 13           |
| 15 |   | [-] <b>3. Estudi eina Pandora FMS</b>                                 | dom 20/03/11 | vie 25/03/11 |              |
| 16 |  | 3.1. Anàlisi característiques de feina                                | dom 20/03/11 | mar 22/03/11 |              |
| 17 |  | 3.2. Instal·lació de feina  | mar 22/03/11 | mar 22/03/11 | 10;16        |
| 18 |  | 3.3. Aprendre utilitzar eina Pandora FMS                              | mar 22/03/11 | vie 25/03/11 | 17           |
| 19 |   | [-] <b>4. Estudi eina Zabbix</b>                                      | vie 25/03/11 | jue 31/03/11 |              |
| 20 |  | 4.1. Anàlisi característiques de feina                                | vie 25/03/11 | dom 27/03/11 |              |
| 21 |  | 4.2. Instal·lació de feina  | lun 28/03/11 | lun 28/03/11 | 10;20        |
| 22 |  | 4.3. Aprendre utilitzar eina Zabbix                                   | lun 28/03/11 | jue 31/03/11 | 21           |
| 23 |  | <b>5. Definició Pla Proves</b>  | mié 30/03/11 | sáb 02/04/11 |              |
| 24 |  | <b>6. Redacció document PAC 2</b>                                     | sáb 02/04/11 | dom 03/04/11 |              |
| 25 |  | <b>Lliurament PAC 2</b>   | lun 04/04/11 | lun 04/04/11 | 24           |
| 26 |   | [-] <b>7. Realització Proves</b>                                      | mar 05/04/11 | lun 18/04/11 |              |
| 27 |  | 7.1. Proves amb eina Nagios   | mar 05/04/11 | sáb 09/04/11 | 23           |
| 28 |  | 7.2. Proves amb eina Pandora FMS                                      | dom 10/04/11 | jue 14/04/11 | 27           |
| 29 |  | 7.3. Proves amb eina Zabbix   | vie 15/04/11 | lun 18/04/11 | 28           |
| 30 |  | <b>8. Estudi Comparacions</b>   | mar 19/04/11 | vie 22/04/11 | 29           |
| 31 |  | <b>9. Extreure Conclusions</b>  | sáb 23/04/11 | dom 24/04/11 | 30           |
| 32 |   | [-] <b>10. Programar un agent</b>                                     | mar 05/04/11 | jue 28/04/11 |              |
| 33 |  | 10.1. Programar agent   | mar 05/04/11 | mar 19/04/11 |              |
| 34 |  | 10.2. Provar agent amb eines  | mié 20/04/11 | jue 28/04/11 | 33           |
| 35 |  | <b>11. Redacció document PAC 3</b>                                    | vie 29/04/11 | mar 03/05/11 | 31;34        |
| 36 |  | <b>Lliurament PAC 3</b>   | mié 04/05/11 | mié 04/05/11 | 35           |
| 37 |   | [-] <b>12. Elaboració lliurament final</b>                            | lun 07/03/11 | dom 29/05/11 |              |
| 38 |  | 12.1 Redacció memòria   | lun 07/03/11 | vie 13/05/11 |              |
| 39 |  | 12.2 Elaboració presentació   | lun 07/03/11 | dom 29/05/11 |              |
| 40 |  | <b>Lliurament Final</b>   | lun 30/05/11 | lun 30/05/11 | 39           |
| 41 |  | <b>Debat Virtual</b>  | lun 13/06/11 | vie 17/06/11 | 40           |

Figura 1: Definició de les tasques



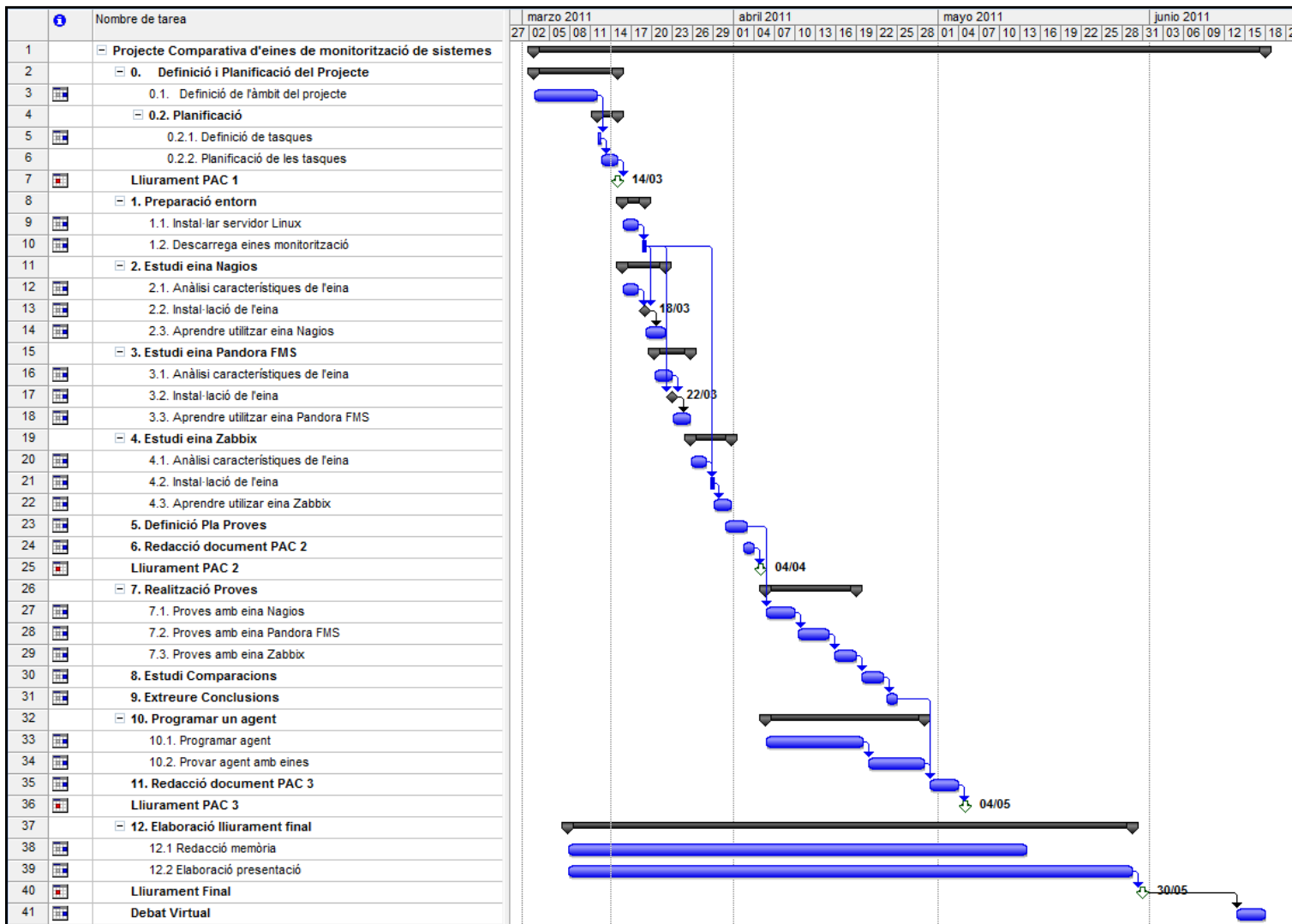


Figura 2: Diagrama de Gantt

### **1.5 Anàlisi de riscos**

Partint de que tinc molt desconeixement del tema del projecte, cosa que ja és un risc en sí, puc afegir que l'ordinador on hagi d'instal·lar el servidor s'espalli, no pugui muntar una xarxa per a provar les eines, etc haig d'afegir que segurament durant aquest semestre m'hauran d'operat d'un quist en el canell dret, fet que em dificultarà molt el treball amb l'ordinador. També s'ha de comptar com a risc el fet que compaginaré la realització del projecte amb una altre assignatura a la UOC, sense comptar la família i la feina.

Per a solucionar els riscos de fallada de programari/maquinari guardaré còpies de seguretat tant del document de memòria, lliuraments parcials, a més d'anar documentant pas a pas per tal de poder reproduir l'escenari abans de la fallada d'una forma ràpida.

El risc de la dificultat del treball amb l'ordinador degut a la operació el resoldré podent-li dedicar més hores diàries, ja que estaré de baixa, per a "recuperar" el temps perdut per haver de treballar amb una sola mà.

## 2 Introducció a la monitorització de sistemes

En aquest apartat definirem la monitorització de sistemes i que hem de tenir en compte per a escollir un bon sistema de monitorització.

### 2.1 Definició de monitorització de sistemes

Per un administrador de sistemes identificar un problema abans que el propi usuari o inclús ser pro actiu, és a dir poder arribar a preveure un incident(per exemple: s'està ocupant el 80% de l'espai de disc), és molt important, sobretot en serveis crítics, per la restauració del sistema, tal i com podem veure en la següent imatge:

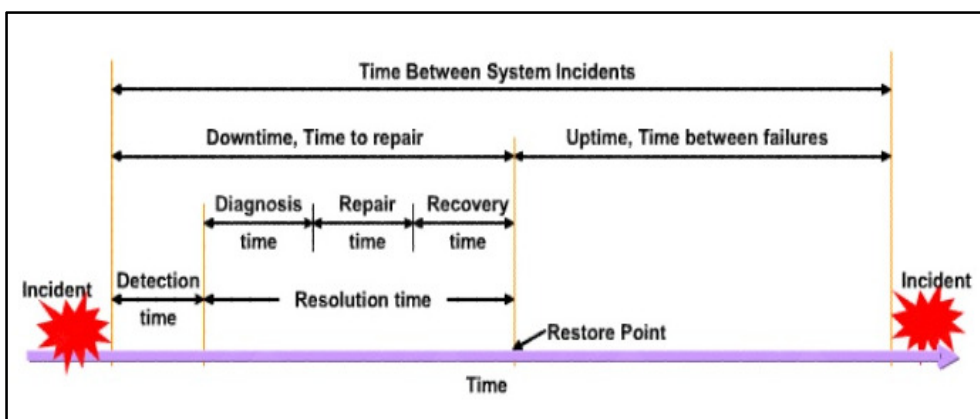


Figura 3: Línia de temps del cicle d'un incident

Per tal de poder reduir al màxim el temps de resolució d'incidents necessitem eines de monitorització de sistemes.

Les eines de monitorització ens permeten estar informats de l'estat dels nostres equips les 24 hores del dia els 365 dies de l'any. Aquests sistemes són cada vegada més complets i amb un alt nivell d'exigència, ja que les xarxes suporten cada vegada més serveis estratègics en les organitzacions. De forma que l'anàlisi i la monitorització de sistemes s'ha convertit en una feina cada vegada més important per tal d'evitar o corregir problemes, ja que ens permet veure l'estat de les nostres màquines (hardware) i serveis (software) que estem monitoritzant mostrant avisos i alarmes en una consola central i/o enviant correus electrònics o missatges instantanis (sms) als responsables dels diferents serveis monitoritzats. L'avantatge principal és la millora de la qualitat.

Aquesta monitorització es fa mitjançant agents i sistemes d'administració que ens permeten inspeccionar i comunicar informació del host.

## **2.2 Qui utilitzarà un sistema de monitorització**

- ✓ Administradors de xarxa
- ✓ Operadors que puguin avisar als administradors per a informar de fallades
- ✓ Equips de desenvolupament

## **2.3 Com impacta un sistema de monitorització**

- ✓ Millora la productivitat
- ✓ Anticipació de problemes
- ✓ Report i avís d'incidents
- ✓ Agilitat en la resolució d'incidents

## **2.4 Elecció d'un sistema de monitorització**

Per a implementar un sistema de monitorització primer s'ha de fer un anàlisi exhaustiu del nostre sistema, per a detectar els sistemes crítics (màquines i serveis) per al bon funcionament de la organització i fer unes polítiques d'actuació davant d'incidències d'aquests sistemes.

Una vegada tenim clar que volem monitoritzar s'ha de fer un pla d'instal·lació i integració del sistema de monitorització en el nostre sistema tenint en compte:

- ✓ S'ha de mantenir la seguretat existent
- ✓ S'ha de minimitzar l'impacte en el sistema
- ✓ S'ha de minimitzar el nombre de sistemes intermedis entre el sistema de monitorització i els sistemes crítics.
- ✓ Com actuar si és el sistema de monitorització el que falla.

Per últim s'ha d'escollir una eina de monitorització de sistemes i per fer-ho s'ha de respondre a aquestes tres preguntes:

- ✓ Com volem veure les dades, alarmes, gràfics, ... tenint en compte que han d'ésser eficients i mostrar els errors fàcilment, ja que es important veure els problemes d'un cop d'ull i ràpidament.
- ✓ Quin tipus de connexió entre equips hi ha (en connexions ràpides però amb molts equips o en connexions lentes hauríem d'utilitzar agents que ens enviïn la informació al servidor central).
- ✓ Quins són els Sistemes Operatius dels equips a monitoritzar (Linux, Windows, ...).

Actualment podem comptar amb eines de llicència lliure (GPL) que són molt competitives com Nagios, Pandora FMS o Zabbix.

## 2.5 Selecció de la millor eina

La definició de criteris ha d'ésser un sistema invariable i estàndard per a qualsevol eina de monitorització de sistemes.

Les característiques les podem agrupar segons les següents categories:

1. Requeriments del sistema
2. Seguretat
3. Suport
4. Facilitat d'ús
5. Administració

Si l'eina disposa d'una característica: 1 punt.

Si l'eina disposa o pot disposar d'una característica però aquesta no es completa o ho és més en altres eines: 0,5 punts

Si l'eina no disposa de la característica 0 punts.

La taula comparativa de característiques resumida amb les puntuacions acumulades per a cada grup de categories és la següent:

| Producte                 | Nagios      | Pandora FMS | Pandora FMS Enterprise | Zabbix    | i-enable rmf |
|--------------------------|-------------|-------------|------------------------|-----------|--------------|
| Versió                   | 3.2.3       | 3.2.1       | 3.2.1                  | 1.8.5     | 2.7          |
| Requeriments sistema (4) | <b>4</b>    | <b>4</b>    | 3,5                    | <b>4</b>  | <b>3</b>     |
| Seguretat (5)            | 2           | 3,5         | <b>5</b>               | 2         | <b>5</b>     |
| Suport (8)               | 5           | 4           | <b>7</b>               | 3         | 4            |
| Facilitat d'ús (5)       | 3           | <b>5</b>    | <b>5</b>               | 3,5       | <b>5</b>     |
| Administració (14)       | 11,5        | <b>14</b>   | <b>14</b>              | 11,5      | 13           |
| <b>Puntuació Total</b>   | <b>25,5</b> | <b>30,5</b> | <b>34,5</b>            | <b>24</b> | <b>30</b>    |

Taula 1: Comparativa característiques eines monitorització sistemes

En negreta s'assenyala l'eina de monitorització que aconsegueix la puntuació més alta en cada categoria. El número que apareix entre parèntesi al costat de cada nom de categoria de criteris indica el nombre de criteris que s'avaluen (la puntuació màxima per categoria).

Per a poder estudiar-les més a fons instal·laré les tres eines de llicència lliure.

### 3 Preparació de l'entorn

En aquest apartat decidirem sobre quin Sistema Operatiu podem treballar l'instal·larem i configurarem per tal de poder portar a terme les proves de les diferents característiques de les eines de monitorització. També les descarregarem.

#### 3.1 Elecció i instal·lació del Sistema Operatiu

Per tal de poder escollir el Sistema Operatiu amb el que treballaré durant la realització del Projecte s'han de mirar els requeriments de sistema de cadascuna de les eines en la seva vessant de Server.

| Eina        | SO                                   | Altres                    |
|-------------|--------------------------------------|---------------------------|
| Nagios      | Linux o Unix                         | Apache 2, PHP, GCC GD     |
| Pandora FMS | Linux recomanat SUSE i Ubuntu/Debian | Apache 2, PHP, MySQL      |
| Zabbix      | Ubuntu / Debian                      | Apache 2, PHP, MySQL, GCC |

Taula 2: *Requeriments de sistema eines monitorització sistemes*

Per tal que la instal·lació de les eines no s'entorpeixin entre si en el moment de fer les diferents proves he decidit crear una màquina virtual per la instal·lació de cadascuna de les eines amb Sistema Operatiu Ubuntu 10.10 desktop i386 ja que és comú a totes les eines.

Les diferents màquines virtuals les he instal·lat sobre el programa VM VirtualBox d'Oracle.

#### 3.2 Descàrrega de les diferents eines de monitorització

Procedeixo a descarregar, de les seves planes oficials, sobre cadascuna de les màquines les diferents eines de monitorització que empremem en aquesta memòria.

- ✓ **Nagios** versió 3.2.3 ([nagios-3.2.3.tar.gz](http://nagios-3.2.3.tar.gz)) i nagios plugins 1.4.15 ([nagios-plugins-1.4.15.tar.gz](http://nagios-plugins-1.4.15.tar.gz))
- ✓ **Pandora FMS** versió 3.2.1 hi ha dues versions: preinstal·lat en una imatge per a virtualbox ([Pandora\\_FMS\\_3.2.1\\_OpenSource.i686-3.2.4.vmx.tar.gz](http://Pandora_FMS_3.2.1_OpenSource.i686-3.2.4.vmx.tar.gz)) o bé els fitxers d'instal·lació per a Debian/Ubuntu (Consola :[pandorafms.console.3.2.1.deb](http://pandorafms.console.3.2.1.deb), Server: [pandorafms.server.3.2.1.deb](http://pandorafms.server.3.2.1.deb) i el pegat publicat el 21 de Març de 2011 :[pandora\\_console.3.2.1\\_March\\_Patch.tar.gz](http://pandora_console.3.2.1_March_Patch.tar.gz)).
- ✓ **Zabbix** versió 1.8.4 ([zabbix-1.8.4.tar.gz](http://zabbix-1.8.4.tar.gz)) o igual que el Pandora, ja pre-instal·lat en una imatge per a virtualbox ([zabbix\\_x86.i686-1.8.4.vmx.tar.gz](http://zabbix_x86.i686-1.8.4.vmx.tar.gz)).

## 4 Estudi de l'eina Nagios

Ens centrarem en l'estudi de l'eina Nagios, definició de les seves característiques i la seva instal·lació, configuració, com monitoritzar diferents equips/serveis, punts febles i forts, la realització d'unes proves i l'extracció de conclusions sobre l'eina.

### 4.1 Què és Nagios?

Nagios és un sistema de monitorització d'equips i serveis de xarxa, escrit en C i sota llicència GNU General Public License versió 2 que ens permet tenir un complet control de la disponibilitat de serveis, processos i recursos d'equips informant a l'administrador dels problemes abans inclús de que els usuaris es donin compte de forma que es pot actuar de forma pro-activa.

Inicialment es va anomenar Netsaint, nom que va haver de canviar per coincidència amb una altre marca, va ser creat i actualment mantingut per Ethan Galstad juntament amb un grup de desenvolupadors de programari que mantenen diversos plugins.

Nagios va ser dissenyat per a ser executat en Linux tot i que també s'executa en diferents variants de Unix.

Durant aquest estudi treballaré amb la versió 3.2.3 (última versió estable des de 3/10/2010) del motor central i 1.4.15 (última versió estable des de 27/07/2010) dels plugins.

### 4.2 Objectius i necessitats

Tal i com hem comentat amb anterioritat l'objectiu principal d'un sistema de monitorització és detectar i informar sobre qualsevol sistema que no funciona correctament, tant aviat com sigui possible, de forma que l'administrador sigui conscient del problema abans que l'usuari.

Realitzar reports amb una configuració personalitzada per a cada cas, fent un testeig de paquets o utilitzant el protocol SNMP que ens permet monitoritzar diferents components de xarxa com switches, routers, servidors, ...

### 4.3 Característiques generals

L'objectiu és conèixer l'estat dels serveis de servidors de diferents sistemes operatius, routers dels que depenen diversos equips. Obtenir informació dels mateixos com l'estat de la xarxa, ports oberts, serveis i processos iniciats, càrrega de la CPU, memòria física, memòria virtual, espai del disc dur, interfaces de xarxa actives.

Nagios no realitza cap revisió de màquines o serveis pel seu compte, utilitza plugins per a realitzar els controls. Això fa que sigui una solució molt flexible i modular per a realitzar comprovacions a les màquines i serveis.

Els objectes que pot supervisar Nagios es divideixen en dues categories:

- ✓ Host: són màquines físiques (servidors, routers, estacions de treball, impressores, etc.)
- ✓ Serveis: són funcions particulars (servidor web, servidor de base de dades, FTP, SSH, servidor de fitxers, servidor LDAP, etc.). Cada servei s'ha d'associar a un host que s'està executant

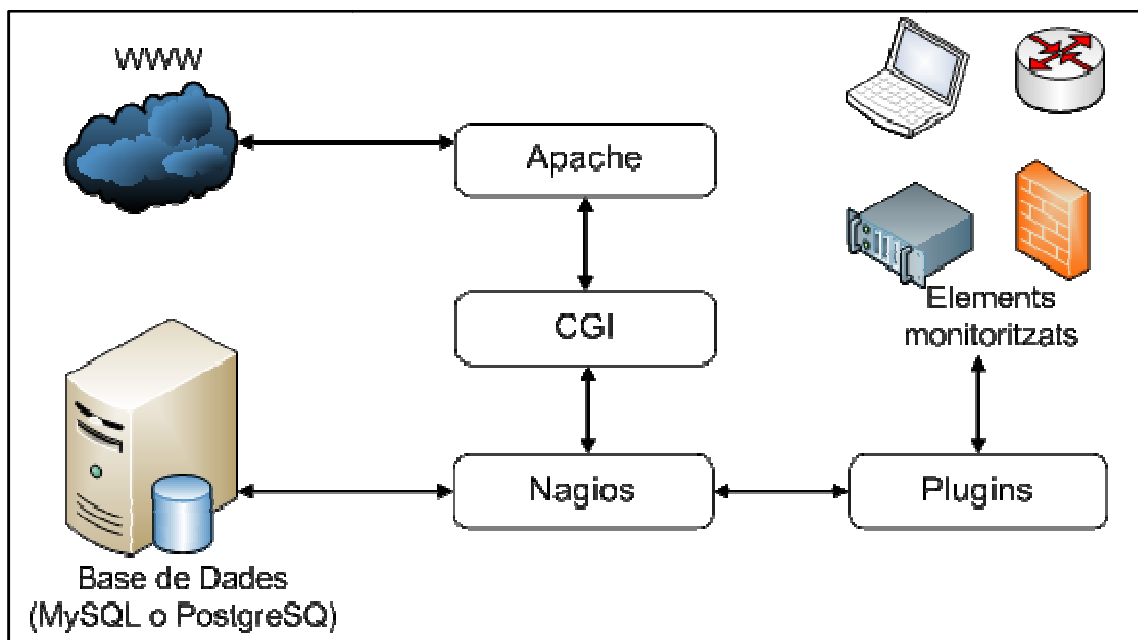


Figura 4: Arquitectura de Nagios

Nagios té dos punts forts importants:

- ✓ Utilitza quatre estats per a descriure l'estat d'un servei o host : OK, WARNING, CRITICAL o UNKNOWN. De forma que pot permetre als administradors centrar-se en els estats WARNING i CRITICAL.
- ✓ La configuració d'informes que ens indiquin com estan els serveis, per exemple els serveis que estan funcionant en els estats de WARNING i CRITICAL, etc.

Nagios permet definir dependències entre els host per tal de poder reflectir la topologia de xarxa real, de forma que si falla un router Nagios no farà els controls de les màquines que depenen del router ja que no serà real el seu error.

Aquestes dependències no només es definiran entre equips físics sinó també es poden definir entre serveis que siguin dependents ja pot ser en el mateix host o en hosts diferents que tindrà el mateix comportament que amb els objectes físics (no realitzarà els controls dels serveis dependents d'un servei caigut).

Nagios és molt flexible alhora de notificar dels serveis o host que no estan funcionant correctament mitjançant correus electrònics a diferents destinataris segons l'objecte. Nagios també permet enviar notificacions a busques, sms, etc.



#### 4.4 Què és pot fer amb Nagios

- ✓ Monitoritzar serveis de xarxa (SMTP, POP3, HTTP, NTP, ICMP, SNMP)
- ✓ Monitoritzar recursos d'un host (càrrega de processador, ús dels discos, logs de sistema) en diferents sistemes operatius, inclús Microsoft Windows amb el plugin adient.
- ✓ Monitorització remota, a través de túnels SSL xifrats o SSH
- ✓ Disseny senzill de plugins, que permet desenvolupar els propis tests de serveis depenent de les necessitats, utilitzant les eines preferides (Bash, C++, Perl, Ruby, Python, PHP, C#, Java, etc.).
- ✓ Revisions de serveis paralitzats
- ✓ Possibilitat de definir la jerarquia de la xarxa, permetent distingir entre hosts caiguts i hosts inaccessibles.
- ✓ Notificacions als contactes (mitjançant correu electrònic, SMS, paper, ...) quan hi ha problemes en serveis o hosts, així com quan aquests es resolen
- ✓ Possibilitat de definir manejadors d'esdeveniments que s'executin al ocórrer un esdeveniment d'un servei o host per resolucions de problemes proactius.
- ✓ Rotació automàtica de l'arxiu de registre (log).
- ✓ Suport per a implementar hosts de monitors redundants.
- ✓ Interfície web opcional, per a observar l'estat de la xarxa actual, notificacions, historial de problemes, arxius de registres, etc.
- ✓ Reports i estadístiques de l'estat cronològic de disponibilitat de serveis i hosts.
- ✓ Accions de recuperació automàtica mitjançant els controladors d'esdeveniments que s'executen quan l'estat d'un servei o host canvia.

#### 4.5 Requeriments del sistema

Els requisits bàsics per al funcionament del sistema són:

| Paquet   | Descripció                                      | Web   |
|----------|---|---|
| Apache 2 | Servidor Web                                    | <a href="http://httpd.apache.org">http://httpd.apache.org</a> |
| GD       | Llibreria per la generació dels formats gràfics | <a href="http://www.libgd.org">http://www.libgd.org</a>       |

Taula 3: Requisits bàsics Nagios

Els paquets necessaris per a poder configurar totes les característiques de Nagios (aquests paquets poden variar depenent de la distribució de Linux que utilitzem)

| Paquet       | Descripció  | Web   |
|--------------|---|---|
| Perl         | Intèrpret per al llenguatge script Perl                                 | <a href="http://www.perl.org">http://www.perl.org</a>   |
| Net::SNMP    | Mòdul de Perl per a consultes SNMP                                      | <a href="http://search.cpan.org/Net-SNMP">http://search.cpan.org/Net-SNMP</a>                                       |
| Crypt::DES   | Mòdul de Perl per a l'encriptació DES, necessari per a consultes SNMPv3 | <a href="http://search.cpan.org/~dparis/Cript-DES/">http://search.cpan.org/~dparis/Cript-DES/</a>                   |
| RDDTool      | Genera gràfiques de xarxa i té un mòdul d'integració amb Perl           | <a href="http://oss.oetiker.ch/rrdtool">http://oss.oetiker.ch/rrdtool</a>   |
| Zlib         | Llibreria de compressió utilitzada per les utilitats gràfiques          | <a href="http://www.gzip.org/zlib/">http://www.gzip.org/zlib/</a>   |
| LibJPEG      | Llibreria per l'exportació jpg  | <a href="http://www.iij.org">http://www.iij.org</a>   |
| LibPNG       | Llibreria per l'exportació png  | <a href="http://www.libpng.org/pub/png">http://www.libpng.org/pub/png</a>   |
| Freetype2    | Llibreria pel processament de les fonts                                 | <a href="http://freetype.org">http://freetype.org</a>   |
| Graphviz     | Utilitzat per la generació dels gràfics                                 | <a href="http://www.graphviz.org">http://www.graphviz.org</a>   |
| XFree86-libs | Llibreries gràfiques generals   | <a href="https://koala.ilog.fr/lehors/xpm.html">https://koala.ilog.fr/lehors/xpm.html</a>                           |
| PHP          | Intèrpret de llenguatge d'script  | <a href="http://www.php.net">http://www.php.net</a>   |
| MySQL        | Sistema de base de dades  | <a href="http://www.mysql.com">http://www.mysql.com</a>   |
| Postfix      | SMTP per a enviar correus electrònics                                   | <a href="http://www.postfix.org">http://www.postfix.org</a>   |
| Nagvis       | Genera diagrames dinàmics   | <a href="http://www.nagvis.org">http://www.nagvis.org</a>   |
| PNP4Nagios   | Genera gràfics estadístics i reports visuals                            | <a href="http://www.pnp4nagios.org">http://www.pnp4nagios.org</a>   |
| NDO          | Connector que connecta Nagios amb MySQL                                 | <a href="http://www.nagios.org">http://www.nagios.org</a>   |
| Plugins      | Plugins de testeig estàndard de Nagios                                  | <a href="http://www.nagios.org">http://www.nagios.org</a>   |
| SNMP Plugins | Plugins per la integració de revisions SNMP de Nagios                   | <a href="http://nagios.manubulon.com">http://nagios.manubulon.com</a>   |
| Nagios       | Lloc de descàrrega oficial  | <a href="http://www.nagios.org">http://www.nagios.org</a>   |
| NagiosQL     | Eina visual de configuració de Nagios mitjançant web                    | <a href="http://www.nagiosql.org/">http://www.nagiosql.org/</a>   |
| Dokuwiki     | Eina de documentació col·laborativa                                     | <a href="http://www.dokuwiki.org/">http://www.dokuwiki.org/</a>   |
| Syslog-Ng    | Connecta els esdeveniments del sistema                                  | <a href="http://www.balabit.com/network-security/syslog-ng/">http://www.balabit.com/network-security/syslog-ng/</a> |

|                |   |   |
|----------------|---|---|
| SNARE          | Agent Syslog per a clients windows  | <a href="http://www.intersectalliance.com/projects/index.html">http://www.intersectalliance.com/projects/index.html</a> |
| MK Liverstatus | Additiu per a obtenir les dades de Nagios mitjançant Socket (útil per deixar d'utilitzar NDO) | <a href="http://mathias-kettner.de/checkmk_liverstatus.html">http://mathias-kettner.de/checkmk_liverstatus.html</a>     |

Taula 4: Requisits per instal·lar totes les característiques de Nagios

## 4.6 Instal·lació bàsica de Nagios

Amb aquesta instal·lació el que aconseguirem es tenir instal·lat el Nagios en Ubuntu amb els seus plugins a /usr/local/nagios, també monitorarà el sistema local (càrrega CPU, us del disc, etc.) i mitjançant la interfície web veurem el resultat del monitoratge.

Per la instal·lació descarreguem els arxius de la pàgina oficial de Nagios, en el nostre cas la versió 3.2.3. Hem de descarregar els paquets:

- ✓ [nagios-3.2.3.tar.gz](#)
- ✓ [nagios-plugins-1.4.15.tar.gz](#)

### 4.6.1 Prerequisits

Per a poder utilitzar totes les funcionalitats de Nagios s'ha d'instal·lar programari addicional:

- ✓ OpenSSL development: són obligatoris pels plugins de Nagios per a comunicar-se a través de SSL. També s'han d'instal·lar les biblioteques de les bases de dades MySQL o PostgreSQL per tal de poder fer plugins per supervisar les bases de dades.
- ✓ Servidor Web: Apache o qualsevol altre que suporti CGI, per a utilitzar la interfície web.
- ✓ Perl ja que els plugins estan escrits en aquest llenguatge. Alguns plugins també necessiten Perl Net::Snmpp per a poder comunicar-se amb dispositius mitjançant el protocol SNMP.
- ✓ Llibreries GD de gràfics per la interfície web per a poder crear el mapa de situació i les tendències de les imatges.

Totes les instal·lacions les farem per línia de comandes (terminal).

### 4.6.2 Crear informació de compte d'usuari

Els processos de Nagios s'executen com usuaris independents per aquesta raó s'ha de crear un usuari i assignar-lo a un grup específic per l'eina.

En el nostre cas s'ha:

- ✓ Creat un nou compte d'usuari "**nagios**" (amb les opcions /bin/bash indiquem l'interpret de comandes utilitzarem)
- ✓ Posat contrasenya (s'ha d'introduir dues vegades) en el nostre cas posarem **nagiospfc**

- ✓ Creat un grup **nagcmd** per a permetre que comandes externes siguin introduïdes mitjançant la interfaç web
- ✓ Introduït l'usuari **nagios** i l'usuari apache **www-data** en el grup **nagcmd** de forma que el servidor web esta funcionant normalment **www-data**

### 4.6.3 Compilar i instal·lar Nagios

Ja tenim els paquets descarregats de la plana oficial de Nagios.

- ✓ Descomprimir el paquet de Nagios
- ✓ Entrar a la carpeta que hem descomprimit
- ✓ Executar l'script de configuració del Nagios amb el nom del grup que hem donat d'alta
 

```
./configure --with-command-group=nagcmd
```
- ✓ Compilar el codi font de Nagios
- ✓ Instal·lar els arxius binaris, l'script d'inici, els fitxers de configuració i el directori de comandes externes respectivament

```
make all
make install
make install-init
make install-config
make install-commandmode
```

El següent pas seria fer la compilació i instal·lació dels plugins de Nagios:

- ✓ Extreure els plugins del arxiu Nagios comprimit
- ✓ Entrem a la carpeta que acabem de descomprimir
- ✓ Compilar els plugins (amb "*with openssl*" habilitem el suport per a SSL i amb "*enable-perl-modules*" habilitem els mòduls de perl per a poder treballar amb perl)

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl=/usr/bin/openssl --enable-perl-modules
```

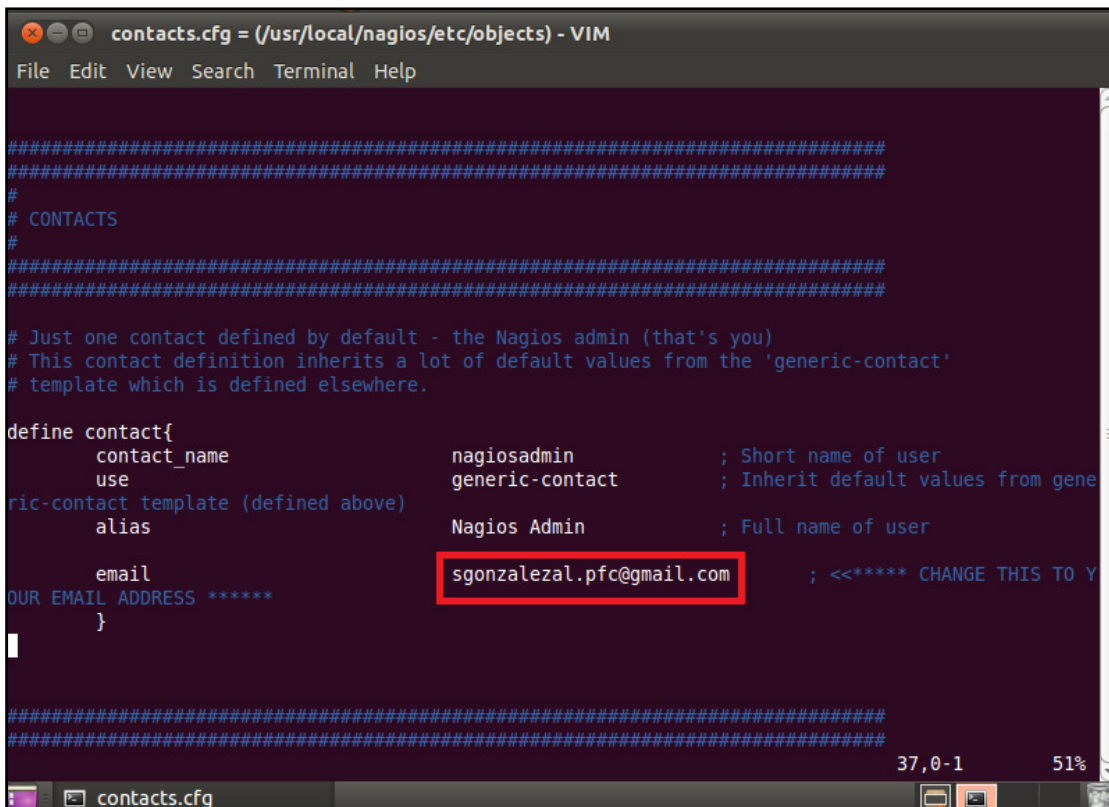
- ✓ Instal·lar

```
make
make install
```

### 4.6.4 Personalitzar la configuració

En el directori `/usr/local/nagios/etc/` tenim els fitxers de configuració de Nagios que haurèm de modificar per a personalitzar la configuració.

Primer de tot, modificarem l'adreça de correu electrònic que s'utilitzarà per a les notificacions de Nagios. Per a poder-ho fer editem l'arxiu `/usr/local/nagios/etc/objects/contacts.cfg` i canviem l'adreça de correu assignada al contacte **nagiosadmin** (concretament a la línia 35). La nostra adreça serà **sgonzalezal.pfc@gmail.com**



```

#####
#####
#
# CONTACTS
#
#####
#####
# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-contact'
# template which is defined elsewhere.

define contact{
    contact_name      nagiosadmin      ; Short name of user
    use                generic-contact  ; Inherit default values from gene
    generic-contact template (defined above)
    alias              Nagios Admin    ; Full name of user
    email              sgonzalezal.pfc@gmail.com ; <<***** CHANGE THIS TO Y
    OUR EMAIL ADDRESS *****
}

#####
#####
37,0-1 51%
contacts.cfg

```

Figura 5: Nagios: Configuració adreça correu notificacions

#### 4.6.5 Configurar la interfície web

Configurem Nagios per a poder accedir mitjançant la interfície web.

- ✓ Instal·lar l'arxiu de configuració de Nagios en el directori conf.d d'Apache
- ✓ Crear un usuari (**nagiosadmin**) que pugui accedir a la interfície web de Nagios.
- ✓ Reiniciem apache per tal que els canvis tinguin efecte

```
/etc/init.d/apache2 reload
```

#### 4.6.6 Iniciar Nagios

- ✓ Configurar Nagios per tal que s'iniciï automàticament quan arrenqui el sistema

```
ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

- ✓ Revisar els arxius de configuració i instal·lació de Nagios són correctes

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

```

root@sandra-HP-Compaq-6730b-GW687AV: ~/Documents/Nagios/nagios-plugins-1.4.15
File Edit View Search Terminal Help
Processing object config file '/usr/local/nagios/etc/objects/localhost.cfg'...
  Read object config files okay...

Running pre-flight check on configuration data...

Checking services...
  Checked 8 services.
Checking hosts...
  Checked 1 hosts.
Checking host groups...
  Checked 1 host groups.
Checking service groups...
  Checked 0 service groups.
Checking contacts...
  Checked 1 contacts.
Checking contact groups...
  Checked 1 contact groups.
Checking service escalations...
  Checked 0 service escalations.
Checking service dependencies...
  Checked 0 service dependencies.
Checking host escalations...
  Checked 0 host escalations.
Checking host dependencies...
  Checked 0 host dependencies.
Checking commands...
  Checked 24 commands.
Checking time periods...
  Checked 5 time periods.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
root@sandra-HP-Compaq-6730b-GW687AV:~/Documents/Nagios/nagios-plugins-1.4.15#

```

Figura 6:Nagios: Pantalla configuració i instal·lació correcta

- ✓ Si no hi ha errors iniciar Nagios
 

```
/etc/init.d/nagios start
```

#### 4.6.7 Entrar en la interfície Web

Ara ja podem entrar a Nagios des de l'explorador Web mitjançant l'adreça <http://localhost/nagios>, ens demanarà el nom d'usuari (**nagiosadmin**) i la contrasenya del punt 4.5.5. (**nagiospfadmin**).

A la plana Services veurem l'estat dels serveis que s'estan executant.

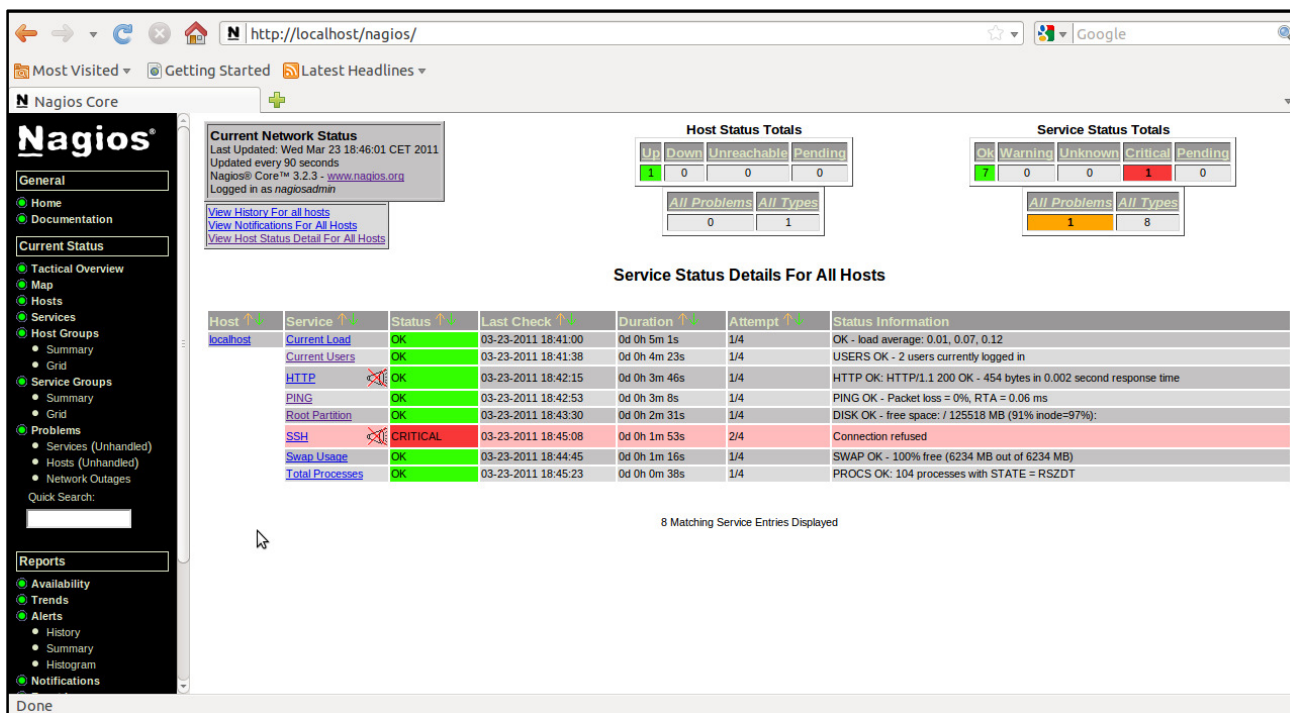


Figura 7:Nagios: Serveis que s'executen amb servei SSH crític

A la imatge podem veure que el servei SSH està amb error crític perquè aquest servei no està instal·lat.

Una vegada instal·lat podem veure com ens canvia l'estat del servei

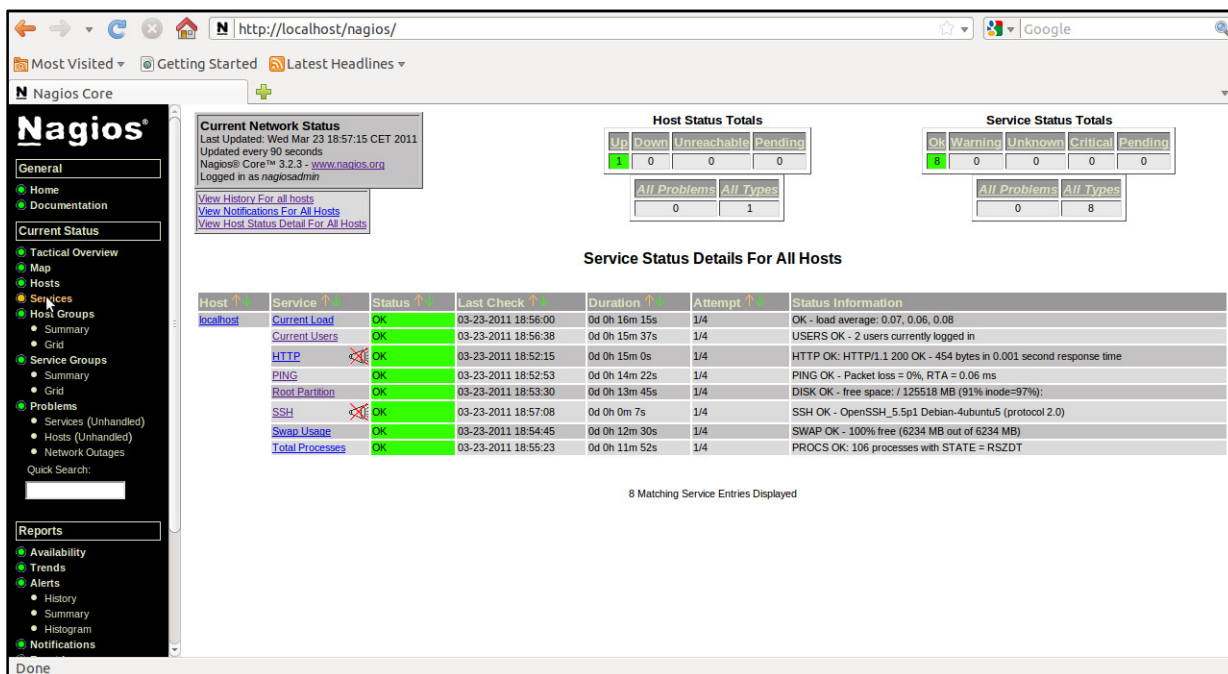


Figura 8:Nagios: Serveis que s'executen amb servei SSH Ok



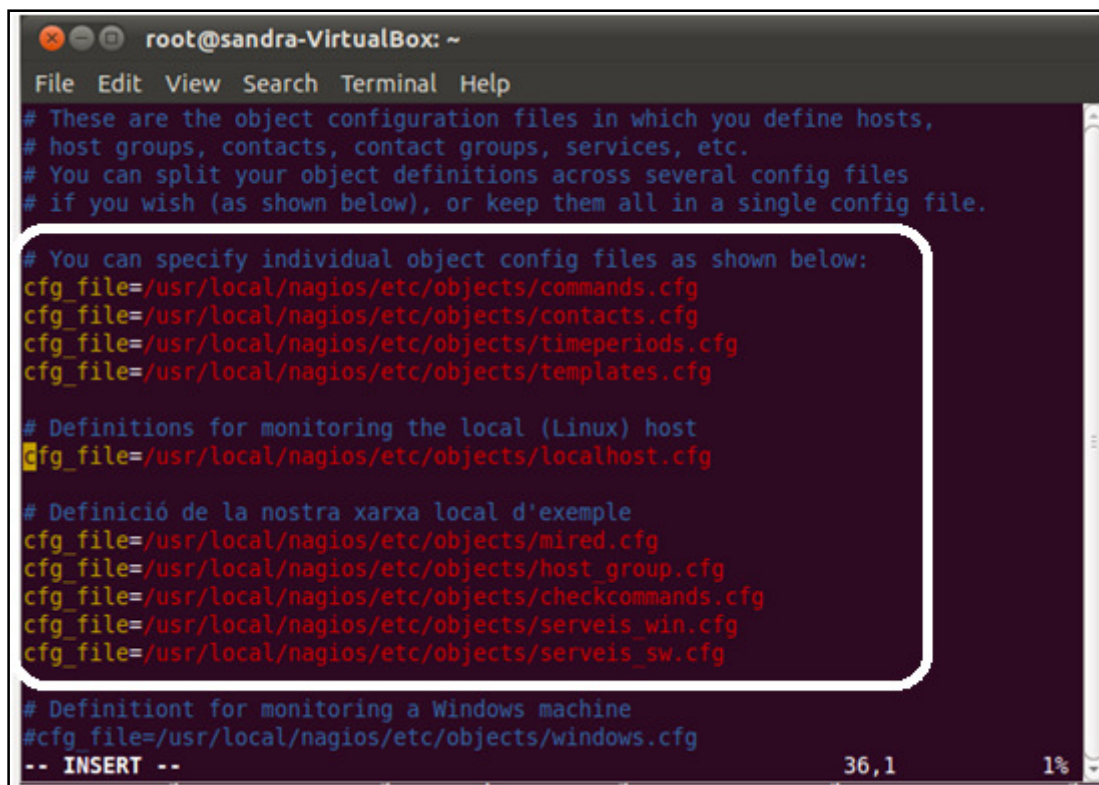
### 4.6.8 Altres configuracions

Per tal de poder rebre les notificacions d'alertes de Nagios per correu electrònic, s'ha d'instal·lar un servidor de correu (Postfix).

Nagios permet definir períodes de temps en els que s'enviaran els missatges d'alerta, franges temporals per dia i hora. També permet definir diferents tipus de contactes per a poder derivar les alertes segons correspongui, per exemple les alertes sobre routers les enviarà als responsables de xarxes, les de SMTP o POP als responsables de sistemes, etc.

Hi ha una eina complementa a Nagios que permet configurar-lo de forma gràfica, extreure gràfics em temps real, realitza informes detallats, interfície multi usuari, etc. Aquesta eina s'anomena Centreon, la veurem en profunditat en el punt "4.11. Monitorització amb Centreon".

Una vegada tenim preparat Nagios hem de dir-li on té els diferents fitxers de configuració i això es fa en el següent fitxer: `/usr/local/nagios/etc/nagios.cfg`, tal i com veiem en la següent imatge:



```
root@sandra-VirtualBox: ~
File Edit View Search Terminal Help
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definició de la nostra xarxa local d'exemple
cfg_file=/usr/local/nagios/etc/objects/mired.cfg
cfg_file=/usr/local/nagios/etc/objects/host_group.cfg
cfg_file=/usr/local/nagios/etc/objects/checkcommands.cfg
cfg_file=/usr/local/nagios/etc/objects/serveis_win.cfg
cfg_file=/usr/local/nagios/etc/objects/serveis_sw.cfg

# Definition for monitoring a Windows machine
#cfg file=/usr/local/nagios/etc/objects/windows.cfg
-- INSERT --
```

Figura 9:Nagios: Definició dels fitxers de Configuracions

Com podem veure en la meua configuració tenim:

- ✓ localhost.cfg: on està la definició de configuració del host i serveis a monitoritzar de la màquina local
- ✓ mired.cfg: està la definició dels diferents hosts
- ✓ host\_group.cfg: està la definició dels diferents grups de hosts.
- ✓ serveis\_win.cfg: està la definició dels diferents serveis a monitoritzar de host Windows
- ✓ serveis\_sw.cfg: està la definició dels diferents serveis a monitoritzar del Router



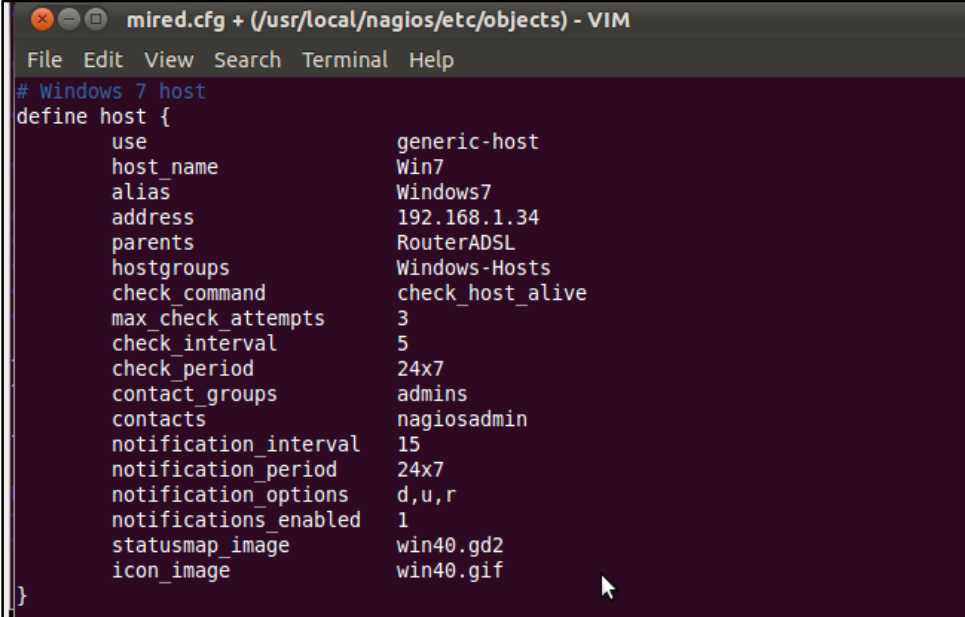
## 4.7 Monitoritzar equips amb Windows

Nagios pot monitoritzar els següents serveis i atributs de màquines Windows:

- ✓ Ús de la memòria
- ✓ Càrrega de la CPU
- ✓ Ús del disc dur
- ✓ Estat en serveis
- ✓ Processos que s'estan executant
- ✓ etc.

Per a poder monitoritzar aquests serveis o atributs en una màquina Windows s'ha d'instal·lar un agent, que actua com a proxy entre el plugging de Nagios que realitza el monitoratge i el servei o atribut de la màquina Windows. Hi ha diversos agents, nosaltres utilitzarem l'**NSClient++** i el plugging de Nagios és **check\_nt**. Una vegada instal·lat l'agent s'ha de configurar el host, el hostgroup i els serveis que volem xequejar. Per fer això s'ha d'adaptar el següent fitxer:

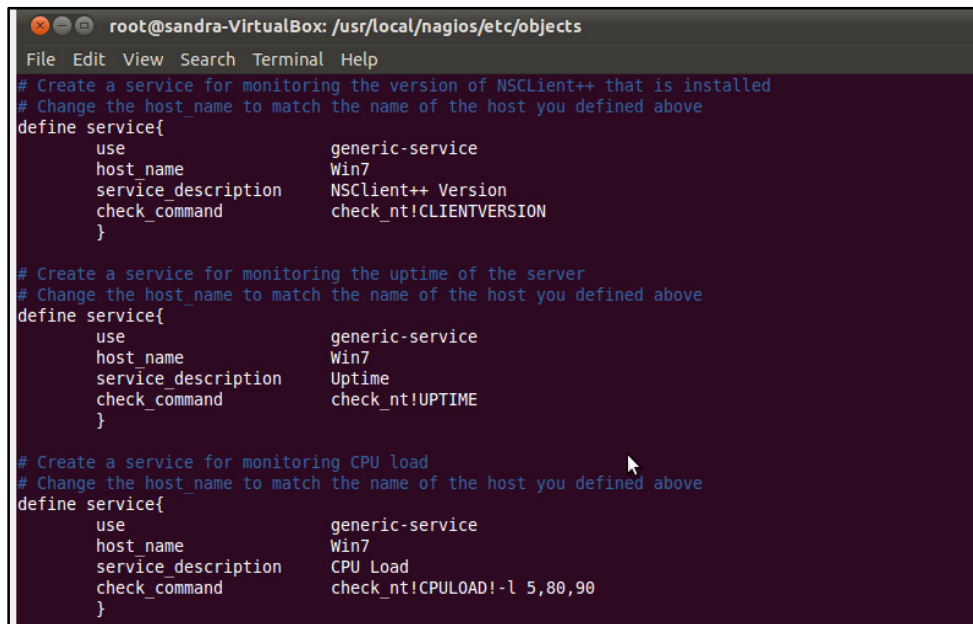
- ✓ /usr/local/nagios/etc/objects/windows.cfg → fitxer d'exemple com definir un host windows i els seus serveis.



```
mired.cfg + (/usr/local/nagios/etc/objects) - VIM
File Edit View Search Terminal Help
# Windows 7 host
define host {
    use                generic-host
    host_name          Win7
    alias              Windows7
    address            192.168.1.34
    parents            RouterADSL
    hostgroups         Windows-Hosts
    check_command      check_host_alive
    max_check_attempts 3
    check_interval     5
    check_period       24x7
    contact groups     admins
    contacts            nagiosadmin
    notification_interval 15
    notification_period 24x7
    notification_options d,u,r
    notifications_enabled 1
    statusmap_image    win40.gd2
    icon_image         win40.gif
}
```

Figura 10: Nagios: Definició host Win7

- ✓ Definició de serveis: /usr/local/nagios/etc/objects/serveis\_win.cfg



```

root@sandra-VirtualBox: /usr/local/nagios/etc/objects
File Edit View Search Terminal Help
# Create a service for monitoring the version of NSClient++ that is installed
# Change the host_name to match the name of the host you defined above
define service{
    use                generic-service
    host_name          Win7
    service_description NSClient++ Version
    check_command      check_nt!CLIENTVERSION
}

# Create a service for monitoring the uptime of the server
# Change the host_name to match the name of the host you defined above
define service{
    use                generic-service
    host_name          Win7
    service_description Uptime
    check_command      check_nt!UPTIME
}

# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above
define service{
    use                generic-service
    host_name          Win7
    service_description CPU Load
    check_command      check_nt!CPULOAD!-l 5,80,90
}

```

Figura 11: Nagios: Exemple definició serveis per a Host Win7

## 4.8 Monitoritzar equips amb Linux/Unix

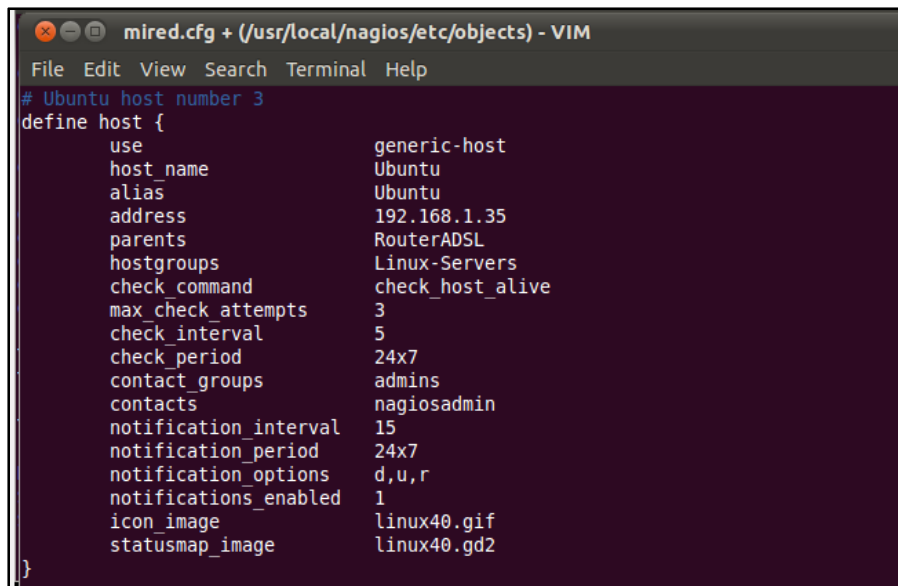
Nagios pot monitoritzar els següents serveis i atributs de màquines Linux/Unix:

- ✓ Ús de la memòria
- ✓ Càrrega de la CPU
- ✓ Ús del disc dur
- ✓ Usuaris signats
- ✓ Processos que s'estan executant
- ✓ etc.

Hi ha diverses formes de monitoritzar els atributs de servidors remots Linux/Unix. Una d'elles és utilitzant claus **SSH compartides** i el plugin **check\_by\_ssh**, aquest mètode pot ser molt útil si es volen monitoritzar milers de serveis. Un altre mètode és utilitzar el complement **NRPE** que permet executar plugins en equips remots Linux/Unix.

Per a configurar el host, el hostgroup i els serveis que volem xequer s'ha d'adaptar el següent fitxer:

- ✓ /usr/local/nagios/etc/objects/localhost.cfg → fitxer d'exemple com definir un host Linux i els seus serveis.



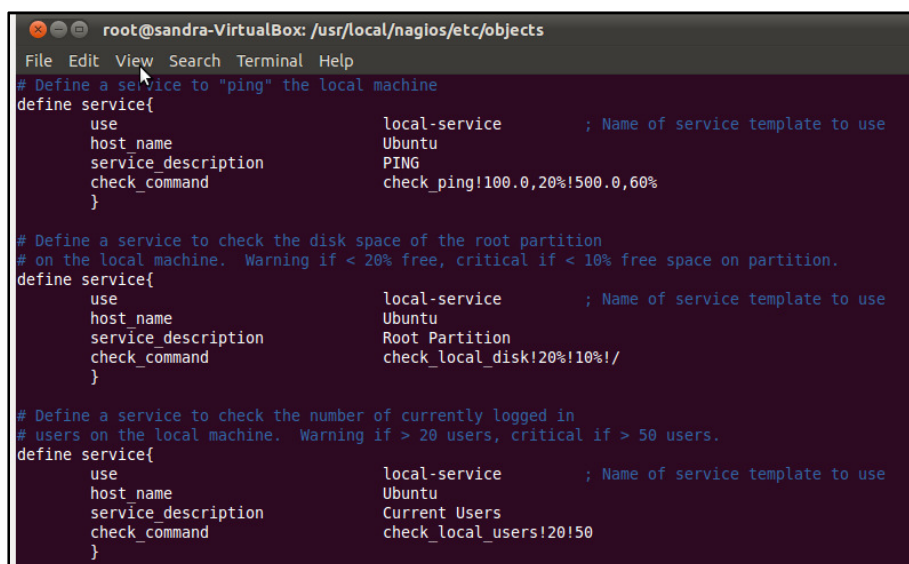
```

# Ubuntu host number 3
define host {
    use                generic-host
    host_name          Ubuntu
    alias              Ubuntu
    address            192.168.1.35
    parents            RouterADSL
    hostgroups         Linux-Servers
    check_command      check_host_alive
    max_check_attempts 3
    check_interval     5
    check_period       24x7
    contact_groups     admins
    contacts           nagiosadmin
    notification_interval 15
    notification_period 24x7
    notification_options d,u,r
    notifications_enabled 1
    icon_image         linux40.gif
    statusmap_image    linux40.gd2
}

```

Figura 12: Nagios: Definició host Ubuntu

- ✓ Definició de serveis: /usr/local/nagios/etc/objects/serveis\_ub.cfg



```

# Define a service to "ping" the local machine
define service{
    use                local-service        ; Name of service template to use
    host_name          Ubuntu
    service_description PING
    check_command      check_ping!100.0,20%!500.0,60%
}

# Define a service to check the disk space of the root partition
# on the local machine. Warning if < 20% free, critical if < 10% free space on partition.
define service{
    use                local-service        ; Name of service template to use
    host_name          Ubuntu
    service_description Root Partition
    check_command      check_local_disk!20%!10%!/
}

# Define a service to check the number of currently logged in
# users on the local machine. Warning if > 20 users, critical if > 50 users.
define service{
    use                local-service        ; Name of service template to use
    host_name          Ubuntu
    service_description Current Users
    check_command      check_local_users!20!50
}

```

Figura 13: Nagios: Definició serveis per a Host Ubuntu

## 4.9 Monitoritzar Routers i Switches

Nagios pot monitoritzar l'estat dels switches i routers de la xarxa. Hi ha alguns switches que no es poden administrar, ja que no tenen una adreça IP, pel que resulten invisibles en la xarxa. Per tal de poder monitoritzar-los s'utilitza **SNMP** per a poder demanar informació sobre el seu estat:

- ✓ Pèrdua de paquets
- ✓ Informació sobre l'estat utilitzant SNMP
- ✓ Amplada de banda / Traça de tràfic

```
mired.cfg + (/usr/local/nagios/etc/objects) - VIM
File Edit View Search Terminal Help
# Router ADSL --> Host number 2
define host {
    use                generic-switch
    host_name          RouterADSL
    alias              RouterADSL
    address            192.168.1.1
    icon_image         router.gif
    statusmap_image    router.gd2
    hostgroups         Routers
    check_command       check_ping!3!200,20%!400,50%
    max_check_attempts 3
    check_interval      5
    check_period        24x7
    contact_groups     admins
    contacts            nagiosadmin
    notification_interval 15
    notification_period 24x7
    notification_options d,u,r
    notifications_enabled 1
}
```

Figura 14: Nagios: Definició host RouterADSL

```
root@sandra-VirtualBox: /usr/local/nagios/etc/objects
File Edit View Search Terminal Help
# Create a service to PING to switch
define service{
    use                generic-service
    host_name          RouterADSL
    service_description PING
    check_command       check_ping!200.0,20%!600.0,60%
    normal_check_interval 5
    retry_check_interval 1
}

# Monitor uptime via SNMP
define service{
    use                generic-service
    host_name          RouterADSL
    service_description Uptime
    check_command       check_snmp!-C public -o sysUpTime.0
}

# Monitor Port 1 status via SNMP
define service{
    use                generic-service
    host_name          RouterADSL
    service_description Port 1 Link Status
    check_command       check_snmp!-C public -o ifOperStatus.1 -r 1 -m RFC1213-MIB
}
```

Figura 15: Nagios: Definició serveis host RouterADSL

### 4.10 Exemple de Monitorització

En el següent mapa es pot veure els diferents equips que s'estan monitoritzant i el seu estat

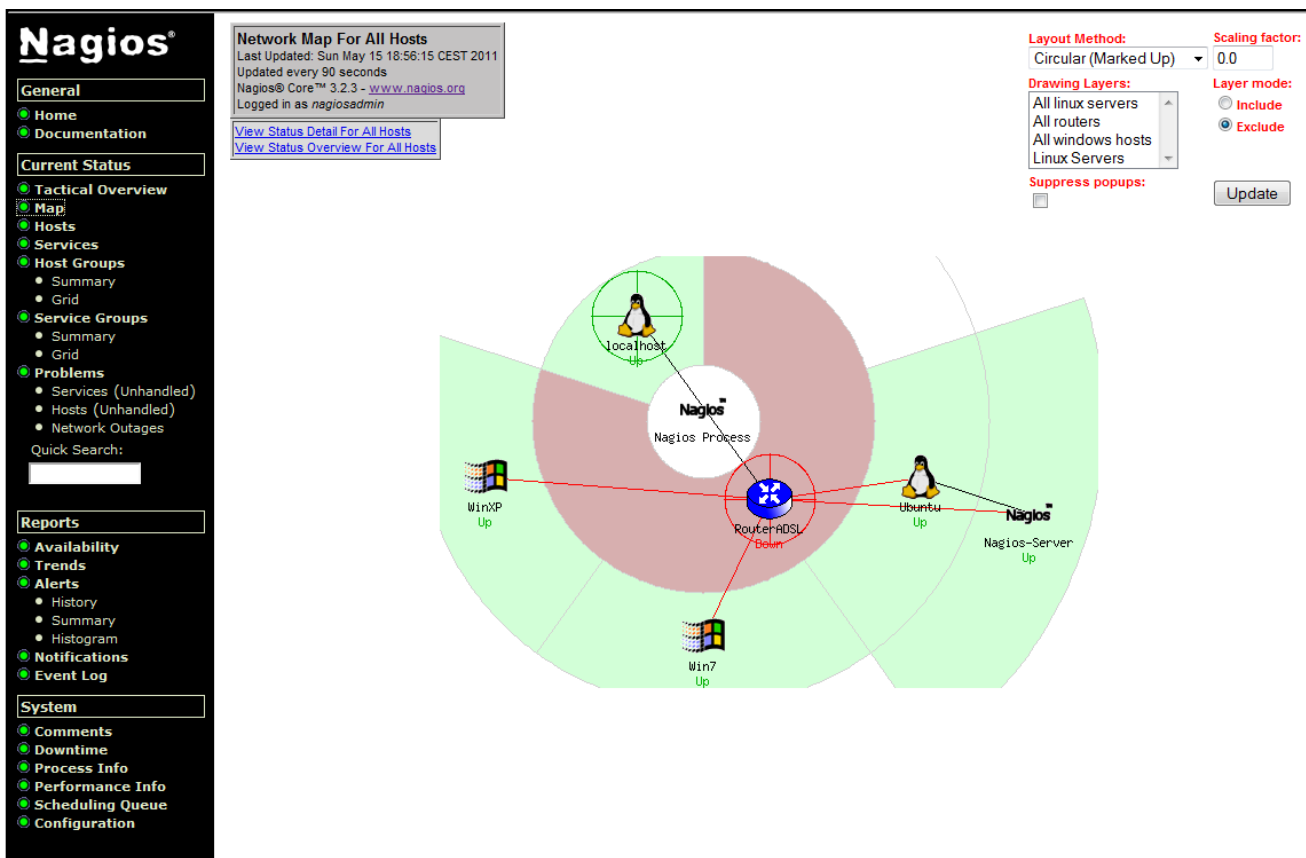


Figura 16: Nagios: Exemple mapa monitorització

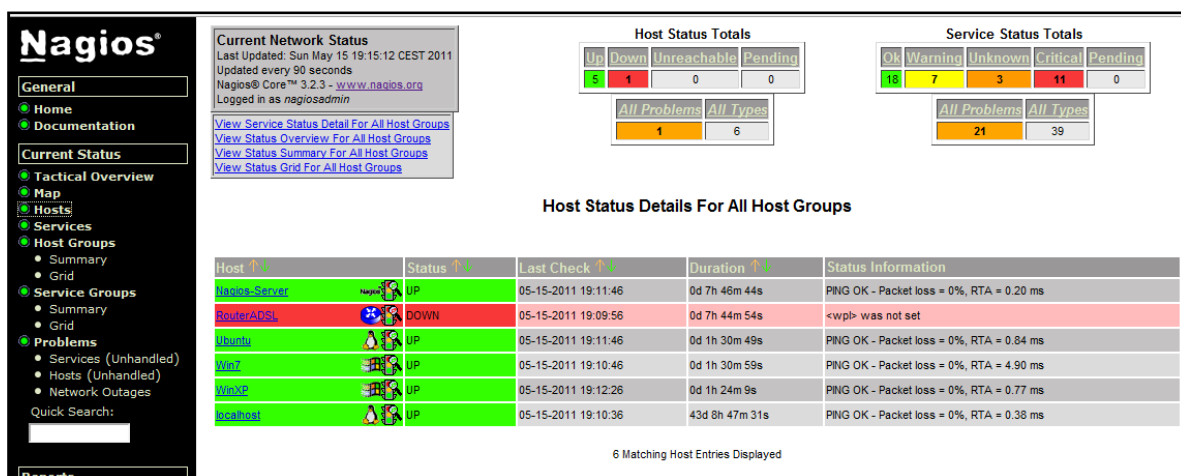


Figura 17: Nagios: Exemple Hosts

The screenshot shows the Nagios web interface with a sidebar on the left containing navigation menus like 'General', 'Current Status', 'Host Groups', 'Reports', and 'System'. The main content area displays a list of monitored hosts and their services with columns for host name, service name, status, last update time, duration, and performance metrics. For example, 'Nagios-Server' has a 'PING' service that is 'OK' with a response time of 1.42 ms. Other services like 'Port 1 Link Status' and 'Uptime' are shown as 'CRITICAL'.

Figura 18: Nagios: Exemple de Serveis

The screenshot displays the 'Hostgroup Availability Report' for 'All Hostgroups' from 05-15-2011 00:00:00 to 05-15-2011 19:20:59. It includes a top navigation bar with filters for 'First assumed host state' and 'First assumed service state'. Below this, there are three tables showing host state breakdowns for different hostgroups:

| Host          | % Time Up         | % Time Down     | % Time Unreachable | % Time Undetermined |
|---------------|-------------------|-----------------|--------------------|---------------------|
| Nagios-Server | 0.000% (0.000%)   | 0.000% (0.000%) | 0.000% (0.000%)    | 100.000%            |
| Ubuntu        | 28.762% (72.696%) | 0.000% (0.000%) | 10.803% (27.304%)  | 60.436%             |
| Average       | 14.381% (36.348%) | 0.000% (0.000%) | 5.401% (13.652%)   | 80.218%             |

| Host       | % Time Up       | % Time Down         | % Time Unreachable | % Time Undetermined |
|------------|-----------------|---------------------|--------------------|---------------------|
| RouterADSL | 0.000% (0.000%) | 100.000% (100.000%) | 0.000% (0.000%)    | 0.000%              |
| Average    | 0.000% (0.000%) | 100.000% (100.000%) | 0.000% (0.000%)    | 0.000%              |

| Host    | % Time Up        | % Time Down     | % Time Unreachable | % Time Undetermined |
|---------|------------------|-----------------|--------------------|---------------------|
| Win7    | 0.000% (0.000%)  | 0.000% (0.000%) | 0.000% (0.000%)    | 100.000%            |
| WinXP   | 7.746% (32.436%) | 0.000% (0.000%) | 16.136% (67.564%)  | 76.118%             |
| Average | 3.873% (16.218%) | 0.000% (0.000%) | 8.068% (33.782%)   | 88.059%             |

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

Figura 19: Nagios: Exemple informe disponibilitat per grups de Hosts

### 4.11 Monitoritzar amb Centreon

Centreon és una eina que està basada en Nagios i el que han fet ha sigut fusionar les noves tecnologies web amb Nagios, millorant així tota la part d'administració, ja que tal i com veurem és on Pandora FMS és millor que Nagios.

Podem veure que Centreon complementa a Nagios convertint-la en:

- ✓ Eina de configuració avançada
- ✓ Interfície Web amb Ajax
- ✓ Gràfics en temps real
- ✓ Informes detallats
- ✓ Interfície multiusuari

Algunes de les pantalles resultants de la configuració de Centreon són:

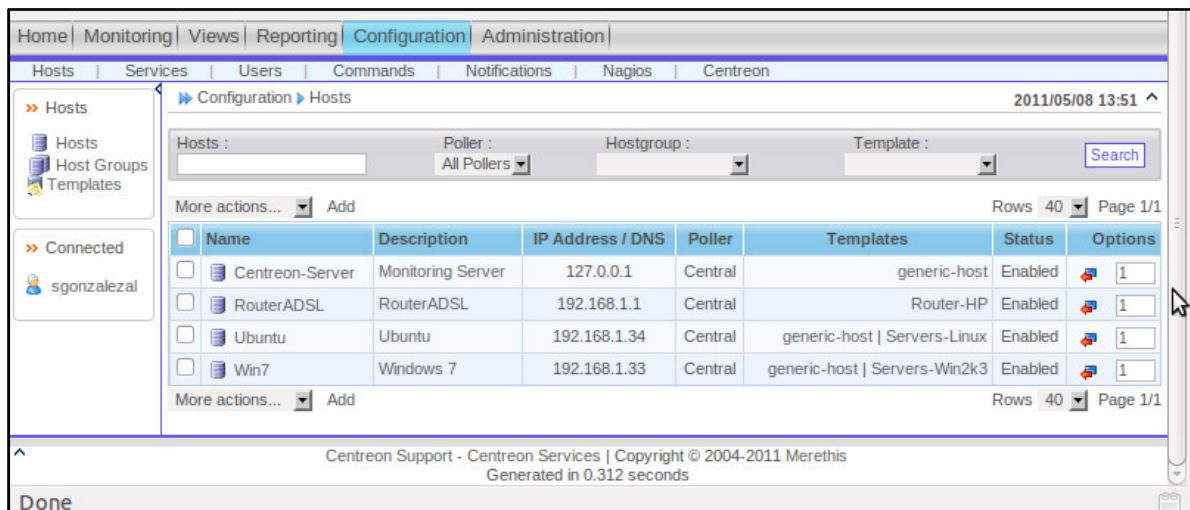


Figura 20: Nagios-Centreon: Configuració de host amb Centreon





Figura 21: Nagios-Centreon: Configuració de Serveis per host amb Centreon

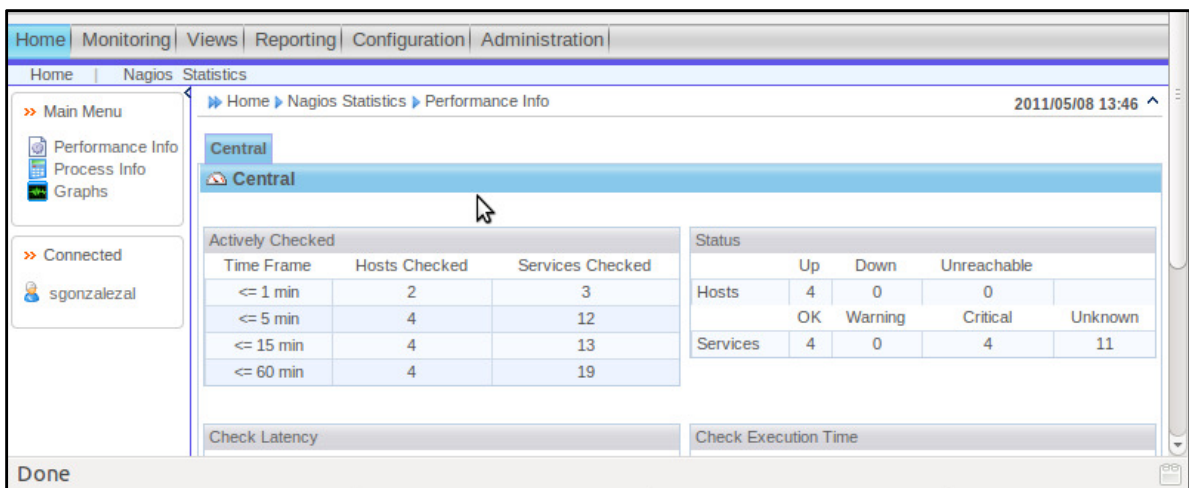


Figura 22: Nagios-Centreon: Estadístiques amb Centreon



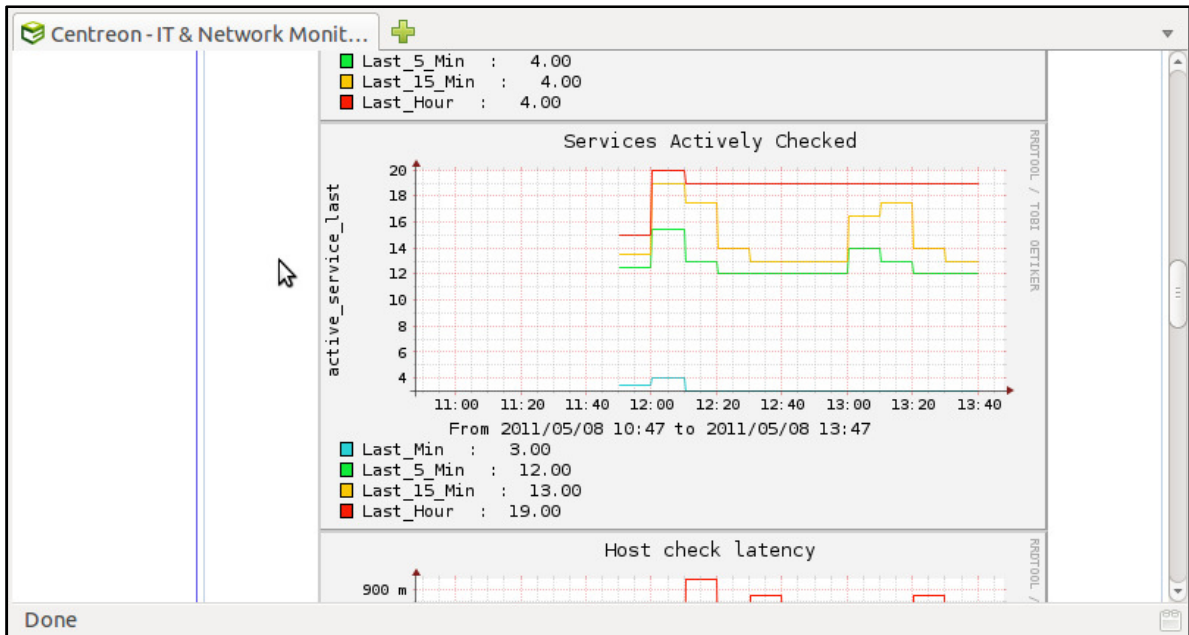


Figura 23: Nagios-Centreon: Exemple estadístiques gràfiques de serveis actius

### 4.12 Resum eina

Nagios és una eina que ens serveix per a monitoritzar els nostres sistemes, és de codi obert.

Entre les eines que són de codi obert és de les més utilitzades, té interfície web, i suporta milers de hosts/serveis

Els seus avantatges són:

- ✓ Utilitza plugins per a connectar diferents tipus de hosts.
  - Fet que fa que la seva arquitectura sigui més senzilla al poder escriure'ls en qualsevol llenguatge.
  - Com que és una eina de codi obert existeixen molts plugins a Internet fets per tercers.
- ✓ Pot fer xequijos en paral·lel.
- ✓ Es pot programar (schedule) els xequijos de forma intel·ligent (buscant càrrega equitativa entre la màquina que executa Nagios i la que s'està xequejant).
- ✓ Utilitza informació per determinar dependències (diferència entre els estats "DOWN" i "UNKNOWN")
- ✓ Permet definir polítiques de notificacions segons contactes, llistes de contactes, dispositius, grups de dispositius i serveis o grups de serveis.
- ✓ Els usuaris poden posar comentaris sobre esdeveniments
- ✓ Permet definir períodes de manteniment per host o grup de hosts
- ✓ Estadístiques de disponibilitat
- ✓ Detecta flappings i treu les notificacions
- ✓ Permet diferents mètodes de notificacions (e-mail, pager, SMS, winpopup, audio, etc.)
- ✓ Definir nivells d'escalatge de notificacions

Els seus inconvenients són:

- ✓ Tota la configuració està basada en codi, fet que dificulta la seva configuració inicial, tot i que porta arxius de configuració (cfg) basats en plantilles. Fet que és millora amb la instal·lació de Centreon.

### 4.13 Conclusions

Nagios és una eina de monitorització de sistemes molt completa i amb molts avantatges, tot i que personalment m'ha costat força la seva configuració.

## 5 Estudi de l'eina Pandora FMS

Ens centrarem en l'estudi de l'eina Pandora FMS, definició de les seves característiques i la seva instal·lació, configuració, com monitoritzar diferents equips/serveis, punts febles i forts, la realització d'unes proves i l'extracció de conclusions sobre l'eina.

### 5.1 Què és Pandora FMS?

Pandora FMS (on FMS ve de Flexible Monitoring System) és un programari de codi obert que monitoritza i mesura qualsevol tipus d'elements. Monitoritza sistemes, aplicacions o dispositius. Permet saber l'estat de cada element.

Pandora FMS està publicat sota llicència GPL2 GNU General Public License i Gnu Lesser Licence v2 (LGPLv2). Pandora FMS és OpenSource, tot i que també disposa de una llicència comercial per a Professionals (Enterprise).

És una eina força nova, ja que la primera versió estable va ser llançada el 14 d'octubre del 2004 sota el nom "Pandoramon". Actualment l'última versió estable es la 3.2 que va ser llançada el 27 de Desembre de 2010.

Durant aquest estudi treballaré amb la versió 3.2.1 (última versió estable des de 23/02/2011) tant per la consola com pel servidor.

## 5.2 Objectius i necessitats

Pandora FMS és una aplicació de monitorització per a vigilar qualsevol tipus de sistemes i aplicacions. Permet conèixer l'estat del hardware, software, aplicacions, Sistema Operatiu, inclús dels moviments de valors del NASDAQ que ens interessin.

Pot recollir informació de qualsevol Sistema Operatiu mitjançant agents específics per a cadascuna de les plataformes (GNU/Linux, AIX, Solaris, HP-UX- BSD/IPSO i Windows 2000, XP i 2003).

Pandora FMS pot mesurar rendiments, comparar valors entre diferents sistemes i establir alertes sobre llindars, també pot monitoritzar qualsevol servei TCP/IP sense necessitat d'instal·lar agents, monitoritzar sistemes de xarxa com balancejadors de càrrega, routers, etc. si es necessita fer de forma remota. També suporta SNMP per a recol·lectar dades o rebre traps.

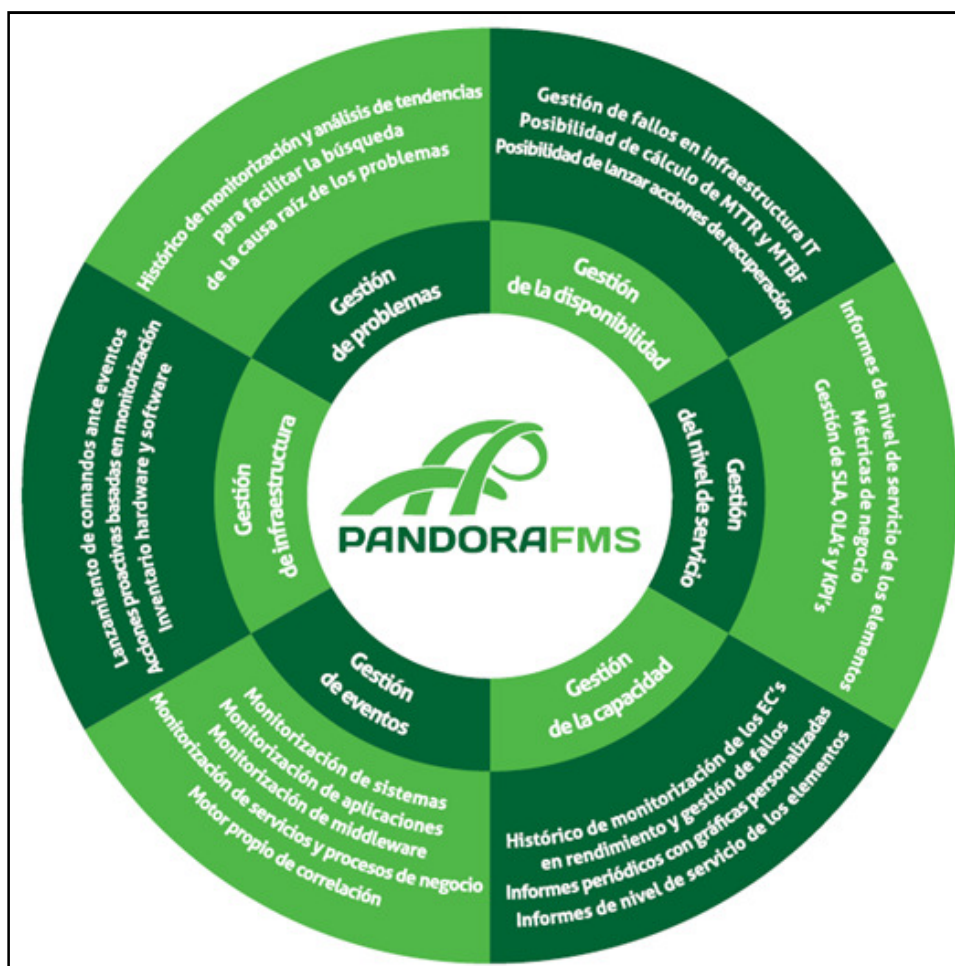


Figura 24: Usos de Pandora FMS

### 5.3 Característiques generals

L'esquema de l'arquitectura global de Pandora FMS és:

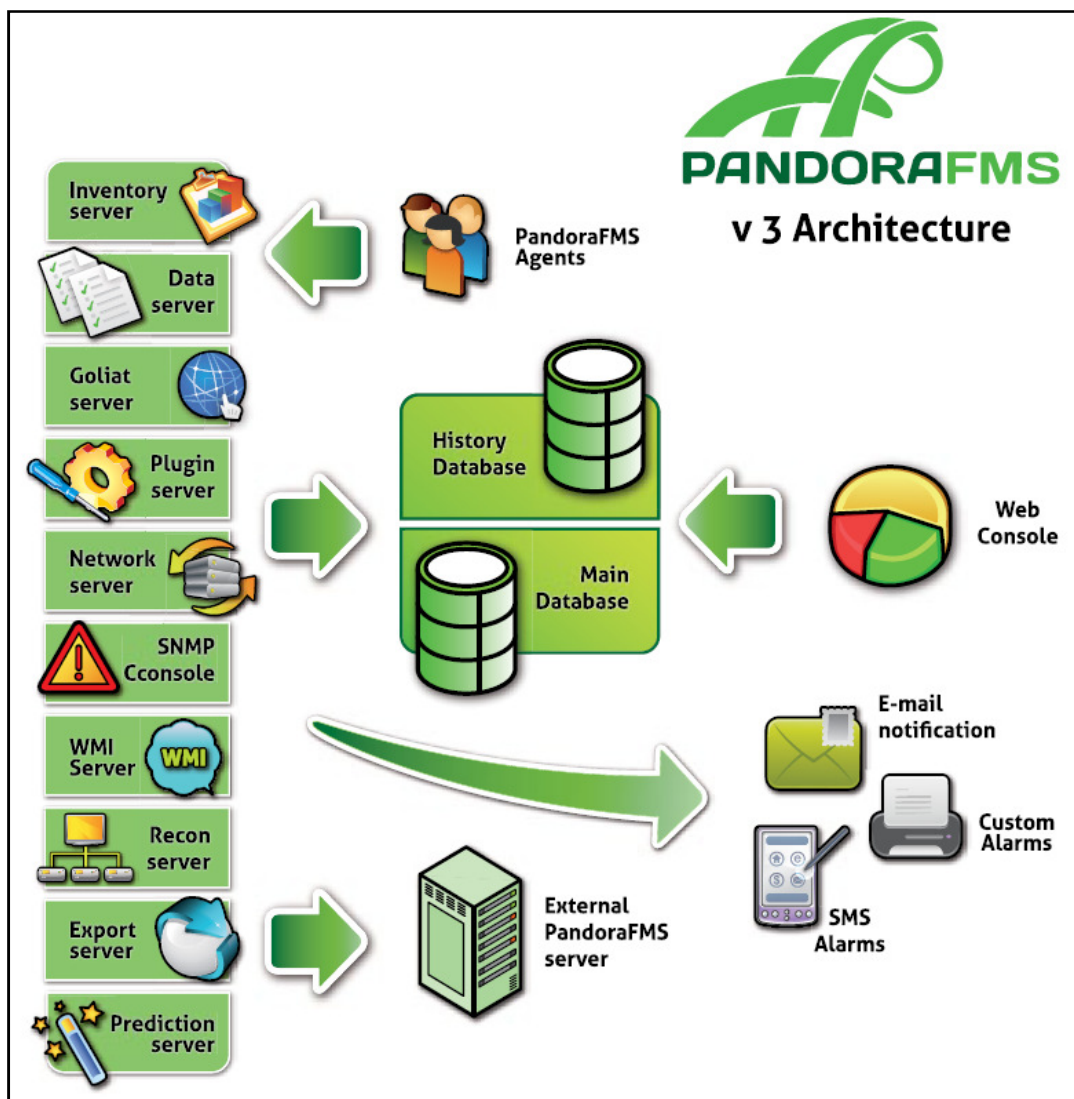


Figura 25: Arquitectura de Pandora FMS

Es pot veure que Pandora FMS és modular i descentralitzat, tot s'emmagatzema en la base de dades (MySQL).

Les característiques de Pandora FMS són:

| Funcionalitat  | OpenSource       | Enterprise        |
|--|------------------|-------------------|
| Llicència d'ús i distribució   | GPL2, LGPL2, BSD | Accés a codi font |
| Suport de l'aplicació  | Foros públics    | Professional, 8x5 |
| Preu   | Gratuït          | Per agent         |
| Auto-descobrimet i detecció de topologia de xarxa i sistemes operatius | Sí               | Sí                |
| Monitorització de rendiment i disponibilitat                           | Sí               | Sí                |
| Gestió d'esdeveniments i fallades                                      | Sí               | Sí                |
| Consola visual (mapes) personalitzable                                 | Sí               | Sí                |
| Agents disponibles per a tots els Sistemes Operatius del mercat        | Sí               | Sí                |
| Alta disponibilitat  | Sí               | Sí                |
| Control d'accés basat en rols: RBAC                                    | Sí               | Sí                |
| Monitorització SNMP i traps SNMP                                       | Sí               | Sí                |
| Monitorització WMI (remot)   | Sí               | Sí                |
| Monitorització Web avançada  | --               | Sí                |
| Escalat a múltiples instàncies   | --               | Sí                |
| Inventari remot i per programari                                       | --               | Sí                |
| Gestió remota d'agents   | --               | Sí                |
| Actualitzacions automàtiques   | --               | Sí                |
| Geolocalització (GIS)  | Sí               | Sí                |
| Monitorització de Serveis  | --               | Sí                |
| API SOA i CLI  | Sí               | Sí                |
| Propietats avançades en informes                                       | --               | Sí                |
| Sistema ACL de grano fino  | --               | Sí                |
| Metaconsola  | --               | Sí                |
| Informes PDF i enviament per correu electrònic                         | --               | Sí                |
| Dashboard  | --               | Sí                |
| BBDD dedicada com a històric   | --               | Sí                |

Taula 5: Característiques Pandora FMS

Quan utilitzar la versió Enterprise i no la OpenSource?

La versió Enterprise reutilitza els conceptes de la versió OpenSource, i les personalitzacions fetes en la versió lliure es poden utilitzar en la versió comercial. Simplifica l'administració remota d'agents, desplegament de configuració per polítiques, etc. Permet la personalització de l'entorn, definició de gràfics, informes configurables per l'usuari i la més important el suport professional.

## 5.4 Què es pot fer amb Pandora FMS

Pandora FMS pot monitoritzar qualsevol procés o sistema que mitjançant una comanda retorni un valor. Alguns exemples d'implementacions existents són:

- ✓ Mitjançant Agents (programari que necessita instal·lació):
  - CPU del sistema: idle, user i system
  - Nombre de processos del sistema
  - Temperatura de la CPU d'un sistema
  - Valor d'un registre de Windows
  - Memòria del sistema (lliure, swap, kernel, cau, etc.)
  - Percentatge d'espai lliure en disc (per particions)
  - Missatges processats per una porta d'enllaç de correu
  - Existència d'una cadena en un arxiu de text
  - Tràfic IP
  - Sessions obertes per servidor VPN
  - etc.
  
- ✓ Monitorització remota
  - Conèixer si un sistema respon a un PING
  - Conèixer el temps d'espera d'un sistema (en milisegons)
  - Ports remots TCP oberts o no
  - Obtenir informació mitjançant SNMP
  - Conèixer si una plana web ha canviat el contingut
  - Pronosticar possibles errors amb el sistema de predicció
  - Consultes a registre de Windows (mitjançant WMI)

## 5.5 Requeriments del sistema

Hi ha dos tipus mínims de requisits el Hardware i el Software i a més també hi ha requisits per a la consola, servidor i agents.

### 5.5.1 Requisits mínims de hardware

Els requisits mínims per hardware són comuns tant per la consola com per al servidor i són:

- ✓ Fins a 500 agents o 5.000 mòduls: 4 Gb de RAM i una CPU d'un sol nucli a 2 GHz de rellotge. Disc dur ràpid, 7200rpm o equivalent.
- ✓ Fins a 2.000 agents o 10.000 mòduls: 8 GB de RAM i una CPU de doble nucli a 2.5GHz de rellotge y disc dur ràpid (7.200 rpm o més)

- ✓ Para més de 4.000 agents: 12GB de RAM, una CPU amb quatre nuclis a 3GHZ y disc dur molt ràpid (15.000 rpm o més).

### 5.5.2 Requisits mínims de software

Els requisits de software depenen de si ho estem instal·lant en un agent, servidor o consola.

- ✓ **Requisits per l'agent:** l'agent es pot executar en qualsevol maquinari que pugui executar el sistema operatiu mínim requerit:
  - Windows 2000 SP3
  - Windows 2003
  - Windows XP
  - Windows Vista
  - Windows 7
  - Windows 2008
  - SUSE Linux 10
  - Ubuntu Linux 8.04
  - Debian Linux
  - AIX 4.3.3
  - HP-UX 11.x
  - Solaris 2.6
- ✓ **Requisits pel servidor:** es recomana i només està suportat sobre Linux sent les versions recomanades SUSE i Ubuntu/Debian. Pandora FMS necessita un servidor MySQL per emmagatzemar la informació, que pot instal·lar-se en qualsevol plataforma suportada per MySQL (Windows, Linux, Solaris, etc.). S'ha d'instal·lar Perl 5.8 més els paquets SNMP i nmap del sistema operatiu, el client binari de WMI per fer consultes WMI contra Windows.
- ✓ **Requisits per la consola:** Igual que pel servidor es recomana sobre sistemes Linux, però com que la interfície web és una aplicació AMP (Apache, MySQL i PHP) es podria treballar sobre qualsevol sistema que ho suporti.

## 5.6 Instal·lació bàsica de Pandora FMS

Amb aquesta instal·lació el que aconseguirem es tenir instal·lat el Pandora FMS en Ubuntu.

És recomanable seguir el següent ordre alhora d'instal·lar Pandora FMS:

- ✓ Instal·lar la consola
- ✓ Instal·lar el servidor

La raó és que la base de dades MySQL que utilitza el servidor es crea en el procés de la configuració inicial de la consola.



Per la instal·lació descarreguem els arxius de la pàgina oficial de Pandora FMS, en el nostre cas la versió 3.2.1. Hem de descarregar els paquets referents a la instal·lació Debian / Ubuntu (.DEB):

- ✓ [pandorafms.console 3.2.1.deb](#)
- ✓ [pandorafms.server 3.2.1.deb](#)

### 5.6.1 Prerequisits:

Les dependències per a Ubuntu/Debian són

#### Servidor

|                             |                    |                       |                    |
|-----------------------------|--------------------|-----------------------|--------------------|
| snmp                        | snmpd              | libtime-format-perl   | libxml-simple-perl |
| libdbi-perl                 | libnetaddr-ip-perl | libhtml-parser-perl   | wmi-client         |
| xprobe                      | nmap               | libmail-sendmail-perl | traceroute         |
| libio-socket-multicast-perl | libhtml-tree-perl  |                       |                    |

Taula 6: Prerequisits de Servidor de Pandora FMS

#### Consola

|           |                     |           |              |
|-----------|---------------------|-----------|--------------|
| php5      | libapache2-mod-php5 | apache2   | mysql-server |
| php5-gd   | php5-mysql          | php-pear  | php5-snmp    |
| php-db    | php-gettext         | graphviz  | mysql-client |
| php5-curl | php5-xmlrpc         | php5-ldap |              |

Taula 7: Prerequisits de Consola de Pandora FMS

Totes les instal·lacions les farem per línia de comandes (terminal).

- ✓ Descarregar i instal·lar:
  - [php-xml-rpc 1.5.2-1\\_all.deb](#)
  - [libnet-traceroute-pureperl-perl 0.10-1\\_all.deb](#)
  - [libnet-traceroute-perl 1.10-1\\_all.deb](#)

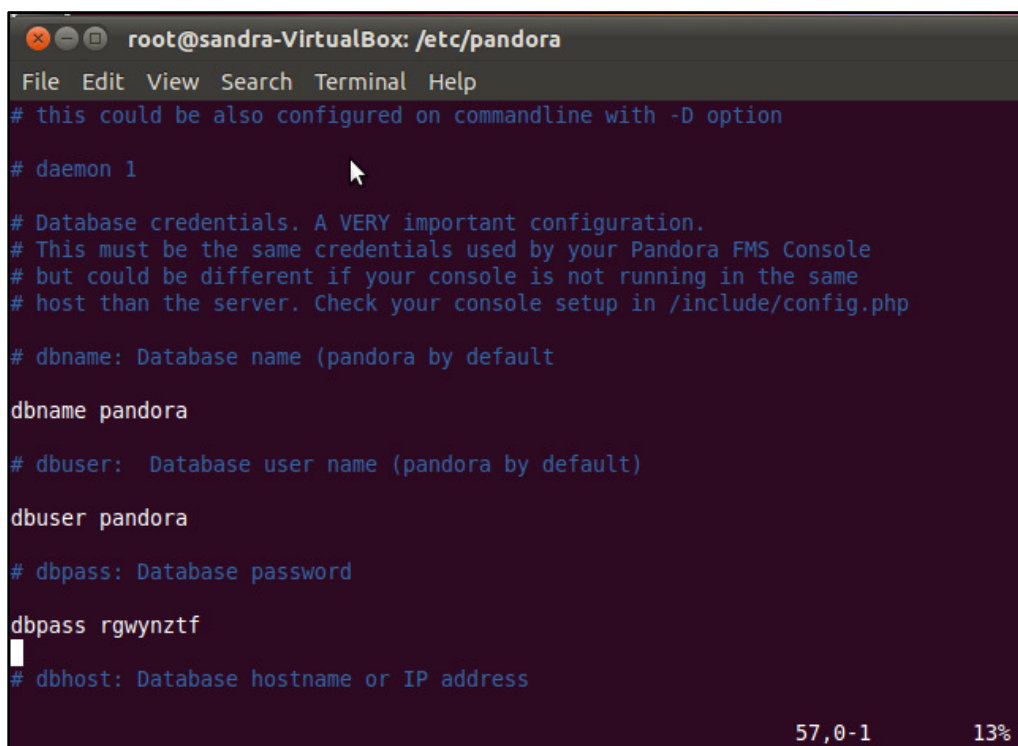
### 5.6.2 Instal·lació

Una vegada s'han descarregat les dependències i s'han instal·lat, s'instal·len els components de Pandora FMS junts.

Durant la instal·lació demana la contrasenya del root del servidor MySQL he posat **adminsqli**

La configuració es fa mitjançant un assistent de sis passes, on s'accepta la llicència, verifica que les dependències estàn correctament instal·lades. S'accepten les dades de la base de dades i la instància web, s'omplen les dades d'un usuari administrador per a crear la base de dades i ens apuntem la contrasenya aleatòria que ens mostra a l'últim pas.

S'ha de modificar el fitxer: `/etc/pandora/pandora_server.conf` i posar la contrasenya que ens ha donat en el paràmetre `dbpass` (veure imatge 26).



```

root@sandra-VirtualBox: /etc/pandora
File Edit View Search Terminal Help
# this could be also configured on commandline with -D option

# daemon 1

# Database credentials. A VERY important configuration.
# This must be the same credentials used by your Pandora FMS Console
# but could be different if your console is not running in the same
# host than the server. Check your console setup in /include/config.php

# dbname: Database name (pandora by default)

dbname pandora

# dbuser: Database user name (pandora by default)

dbuser pandora

# dbpass: Database password

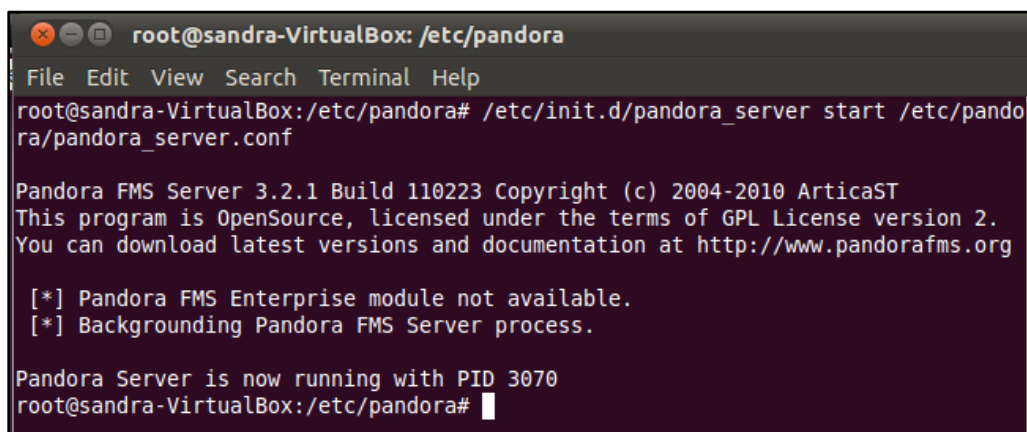
dbpass rgwynztf
# dbhost: Database hostname or IP address

57,0-1 13%

```

Figura 26: Assignació contrasenya Pandora FMS

Una vegada hem modificat la contrasenya al fitxer `pandora_server.conf` passem a arrencar el procés de servidor de Pandora FMS.



```

root@sandra-VirtualBox: /etc/pandora
File Edit View Search Terminal Help
root@sandra-VirtualBox:/etc/pandora# /etc/init.d/pandora_server start /etc/pandora/pandora_server.conf

Pandora FMS Server 3.2.1 Build 110223 Copyright (c) 2004-2010 ArticaST
This program is OpenSource, licensed under the terms of GPL License version 2.
You can download latest versions and documentation at http://www.pandorafms.org

[*] Pandora FMS Enterprise module not available.
[*] Backgrounding Pandora FMS Server process.

Pandora Server is now running with PID 3070
root@sandra-VirtualBox:/etc/pandora#

```

Figura 27: Arrencar Pandora FMS

El nom d'usuari i la contrasenya que crea per defecte són **admin** i **pandora** respectivament.

Per a accedir a administrar Pandora FMS accedim al nostre navegador i escrivim [http://localhost/pandora\\_console](http://localhost/pandora_console) o bé des d'una altre màquina [http://<ip\\_servidor\\_pandora>/pandora\\_console](http://<ip_servidor_pandora>/pandora_console).

### **5.7 Monitoritzar equips amb Windows**

Per a poder monitoritzar equips amb Windows primer hem d'instal·lar un agent en l'equip a monitoritzar i automàticament el servidor Pandora FMS el donarà d'alta.

L'agent que hem de descarregar és: [Pandora FMS Windows Agent v3.2.1-Setup.exe](#)

Aquest agent es un instal·lador molt senzill, en el que bàsicament s'ha de seguir l'assistent on primerament ens demanarà l'idioma, acceptar la llicència, ruta on volem instal·lar l'agent, comprovar dades són correctes, s'instal·len els fitxers, ip del servidor Pandora FMS que ha de rebre les dades de l'agent i per últim pregunta si vols arrencar els serveis agent de Pandora FMS per a Windows. Si es vol modificar qualsevol dels paràmetres es pot editar amb el fitxer *pandora\_agent.conf*.

### **5.8 Monitoritzar equips amb Linux / Unix**

Per a monitoritzar equips amb Linux en principi no fa falta instal·lar cap agent, doncs el propi Pandora FMS al fer un reconeixement de mapa de xarxa els detecta sense cap problema, igualment existeix un agent per a màquines Unix: [pandorafms.agent\\_unix\\_3.2.1.deb](#) .

### **5.9 Monitoritzar Routers i Switches**

El propi Pandora FMS al fer un reconeixement de mapa de xarxa detecta aquells que es poden administrar.

### **5.10 Reconeixement mapa de xarxa**

Per tal de que Pandora FMS ens reconegui els servidors, routers, etc. de forma automàtica podem fer que Pandora FMS faci una tasca de reconeixement i automàticament ens crearà un mapa de la nostra xarxa.

Per a fer aquesta tasca en el menú a la part d'Administració, despleguem l'opció de "Gestionar Servidors" i fem una tasca de reconeixement on li hem de dir quina es la nostre xarxa.

Quan ha acabat el reconeixement ens crea el mapa de la nostra xarxa, veure imatge:

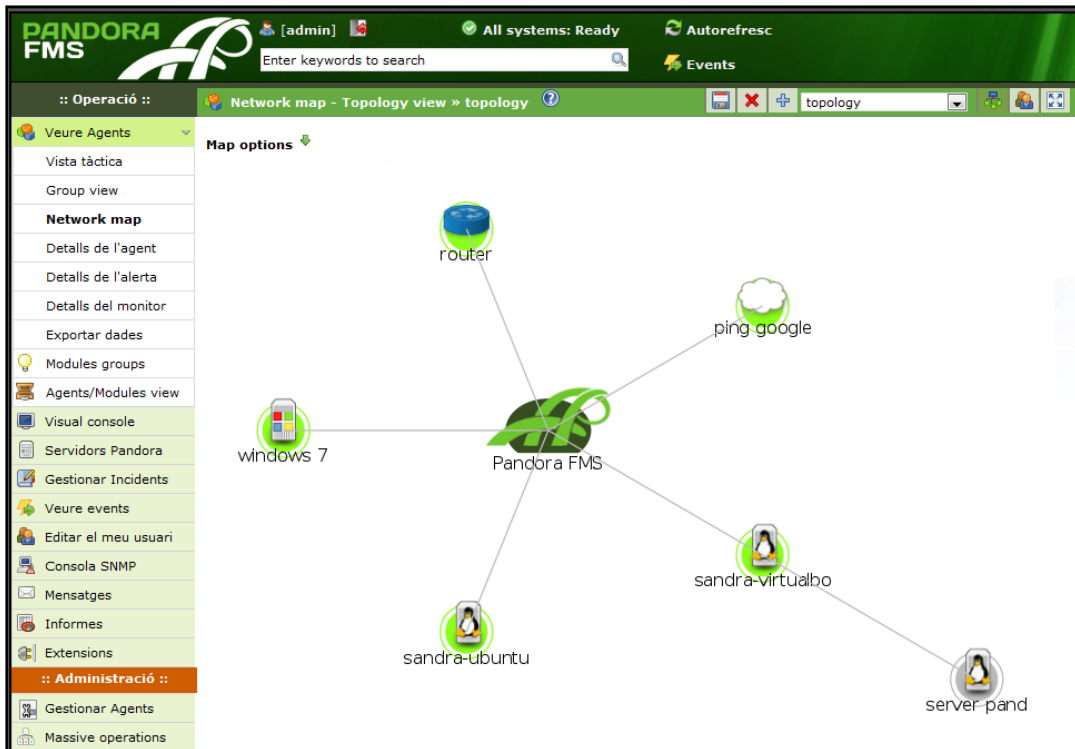


Figura 28: Pandora FMS: Mapa de xarxa amb la vista Topology

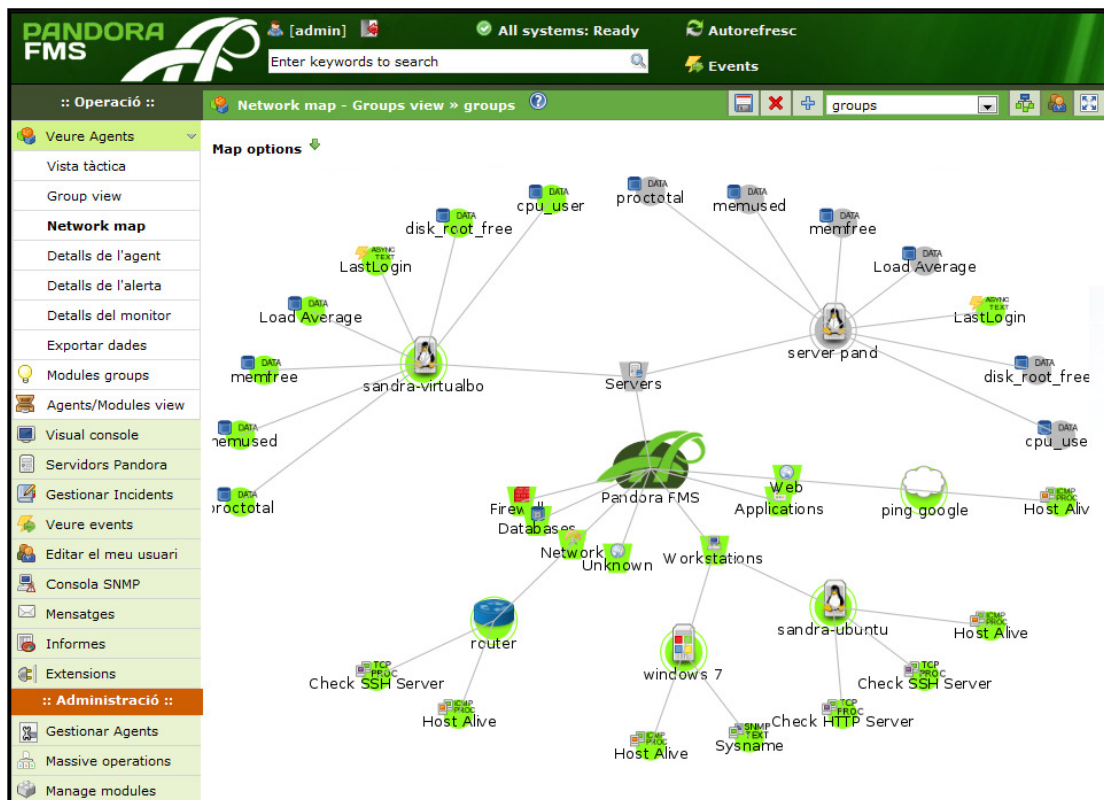


Figura 29: Pandora FMS: Mapa de xarxa amb la vista Groups

### 5.11 Exemples de monitoritzacions

Aquestes són algunes de les pantalles de monitorització:

The screenshot displays the Pandora FMS tactical view interface. At the top, it shows the user 'admin', system status 'All systems: Ready', and a search bar. The main content is divided into several sections:

- Global health:** Includes 'Monitor health' and 'Module sanity' with progress bars.
- Alert level:** Shows the current alert level.
- Monitor checks:** A summary of monitoring metrics:
  - Monitor checks: 25
  - Monitors critical: -
  - Monitors warning: -
  - Monitors normal: 16
  - Monitors unknown: 6
  - Monitors not init: 3
  - Alerts defined: 7
  - Alertes activades: -
- Server performance:** Shows local and remote module rates:
  - Local modules rate: 0.1
  - Remote modules rate: 0.0
  - Local modules: 14
- Latest events:** A table listing recent system events.
 

| V. | S. | Tipus | Nom de l'event                             | Nom de l'Agent | Identificador d'usuari | Segell de temps |
|----|----|-------|--|----------------|------------------------|-----------------|
| ◆  | ●  | ●     | sandra-VirtualBox dataserver going UP      | Sistema        |                        | 3 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox networkserver going UP   | Sistema        |                        | 3 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox reconserver going UP     | Sistema        |                        | 3 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox snmpconsole going UP     | Sistema        |                        | 3 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox dataserver going UP      | Sistema        |                        | 4 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox networkserver going UP   | Sistema        |                        | 4 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox reconserver going UP     | Sistema        |                        | 4 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox snmpconsole going UP     | Sistema        |                        | 4 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox dataserver going DOWN    | Sistema        |                        | 4 dies          |
| ◆  | ●  | ●     | sandra-VirtualBox networkserver going DOWN | Sistema        |                        | 4 dies          |
- Tactical server information:** A table showing server status and performance.
 

| Nom               | Tipus     | Estat | Load  | Lag           |
|-------------------|-----------|-------|-------|---------------|
| sandra-VirtualBox | (Data)    | ●     | 100 % | - / 0         |
| sandra-VirtualBox | (Network) | ●     | 100 % | - / 0         |
| sandra-VirtualBox | (Snmp)    | ●     |       | No disponible |
| sandra-VirtualBox | (Recon)   | ●     | 100 % | No disponible |

Figura 30: Pandora FMS: Vista tàctica

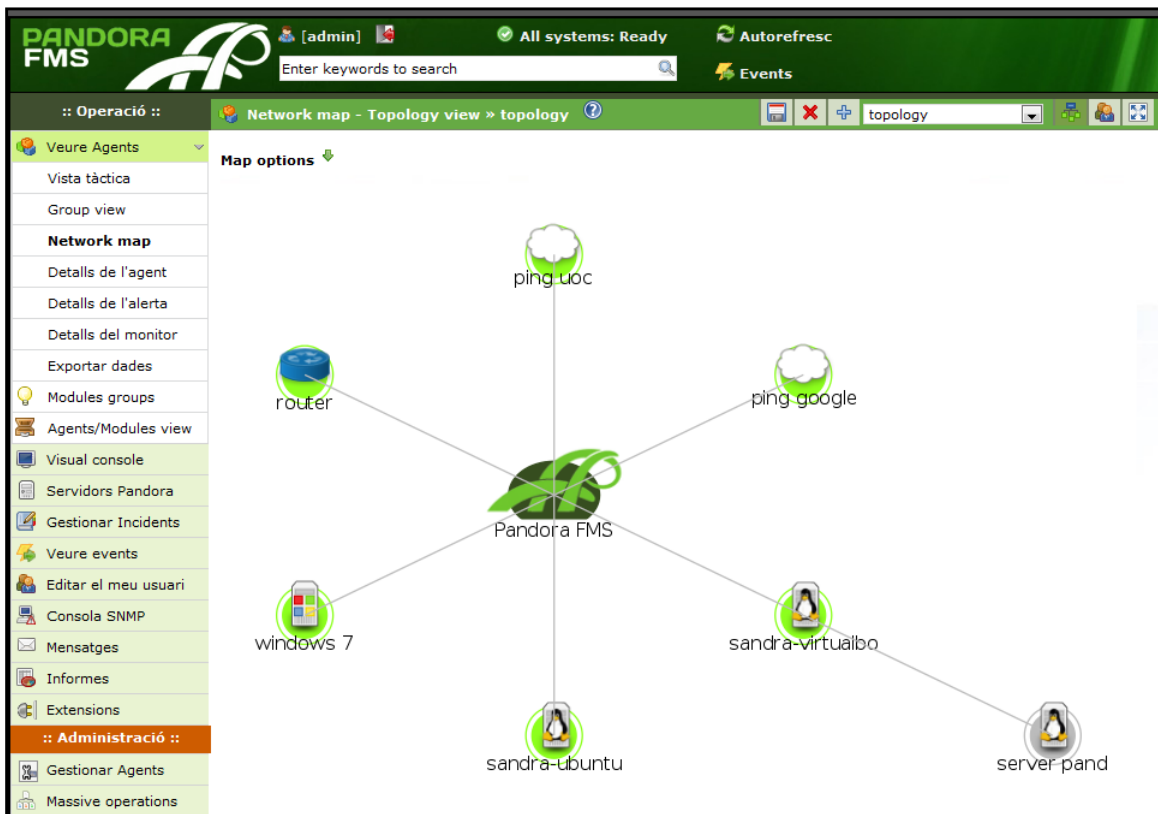


Figura 31: Pandora FMS: Mapa de xarxa

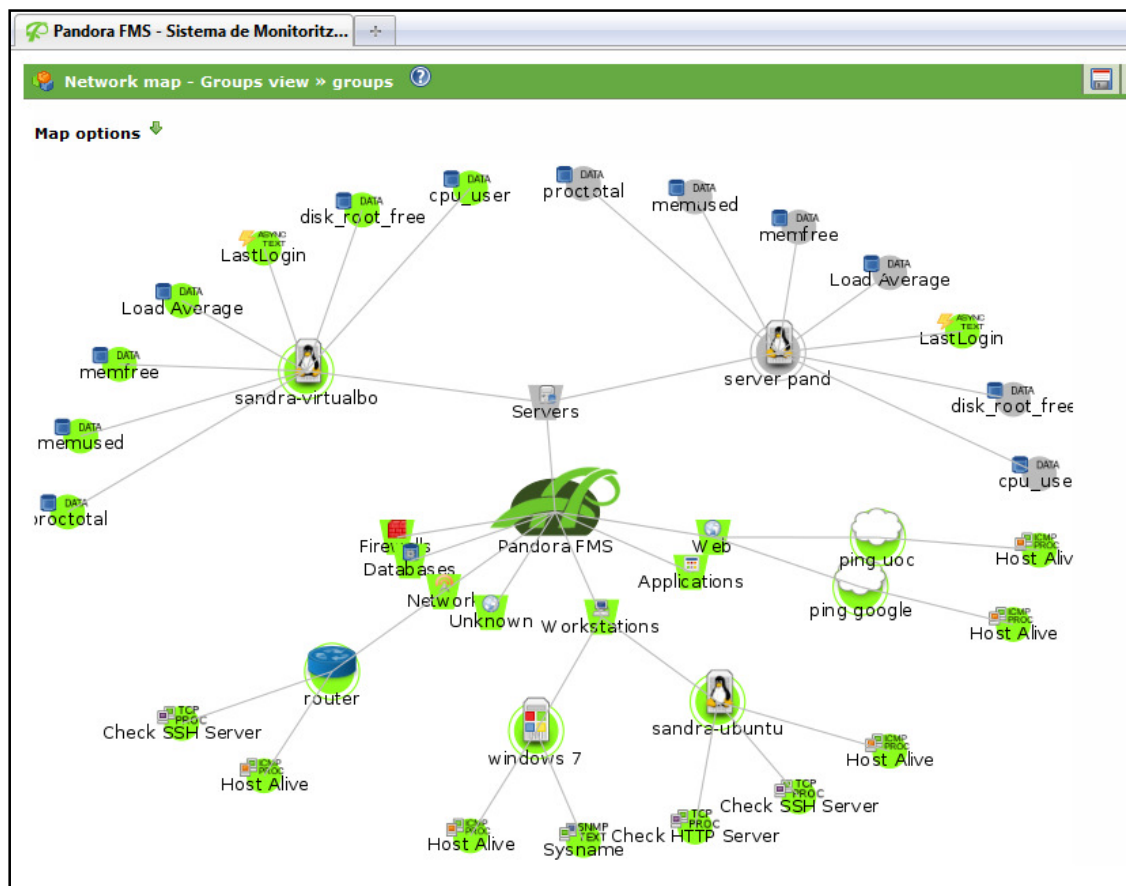


Figura 32: Pandora FMS: Mapa de xarxa per grups



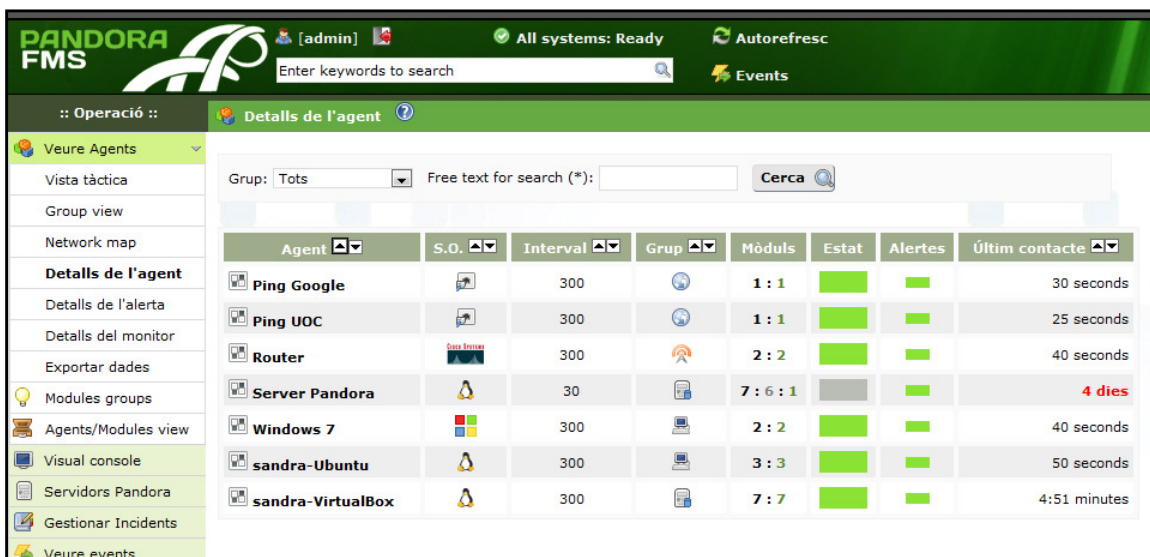


Figura 33: Pandora FMS: Detalls de l'agent

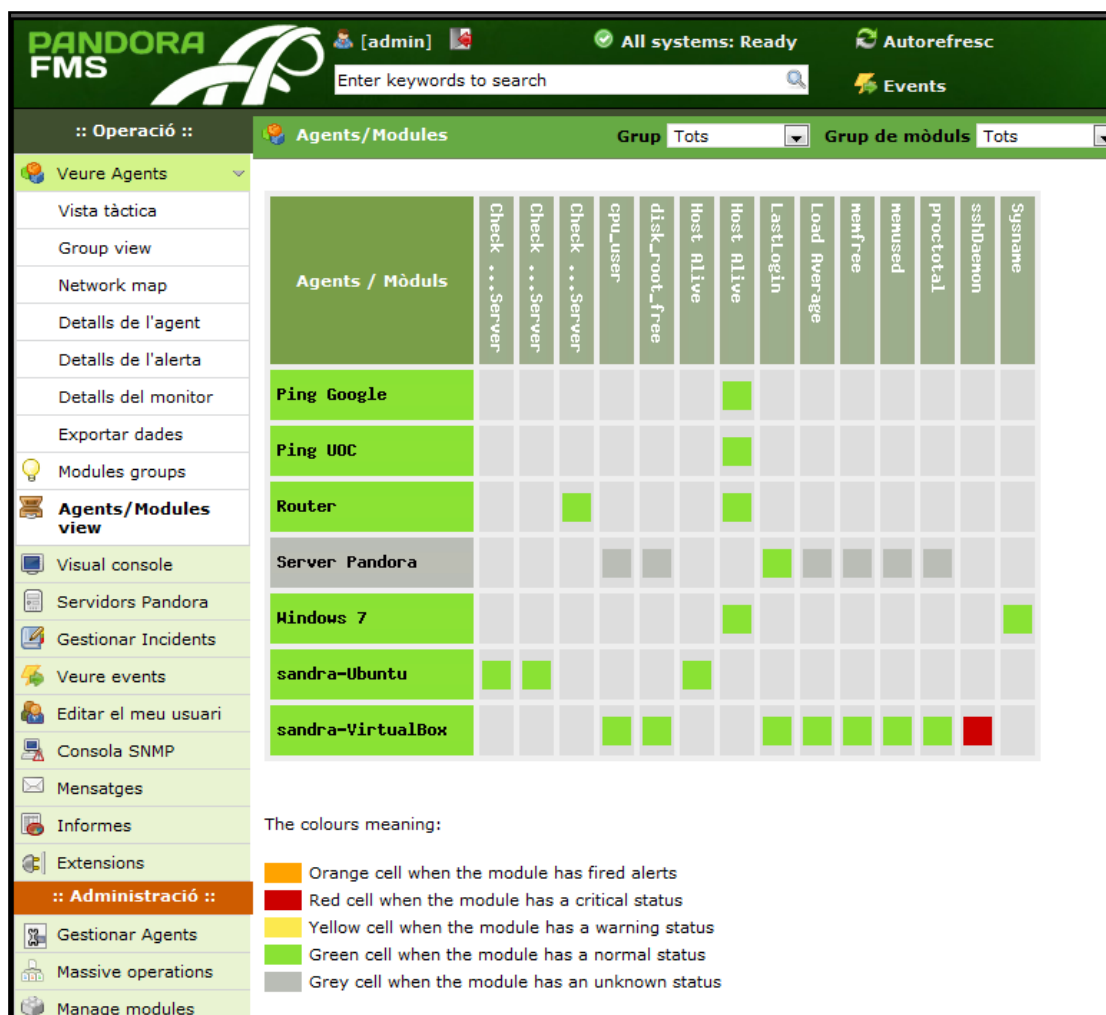


Figura 34: Pandora FMS: Vista d'Agents i Mòduls

### **5.12 Resum eina**

Pandora FMS és una eina que ens serveix per a monitoritzar els nostres sistemes, aplicacions o dispositius, és de codi obert es distribueix sota llicència GPL2 tot i que també disposa d'una llicència comercial on dona més valor afegit a l'eina com el suport d'experts, actualitzacions automàtiques, etc.

Els seus avantatges són:

- ✓ Reconeixement automàtic del mapa de xarxa
- ✓ Ràpid desplegament de comprovacions i nous servidors
- ✓ Mesura rendiments, comparar valors i establir alertes sobre llindars
- ✓ Monitoritza serveis TCP/IP sense necessitat d'instal·lar agents
- ✓ Suporta SNMP per recol·lectar dades o rebre traps
- ✓ Diferents tipus d'usuaris segons els nivells d'accessos
- ✓ Control total amb la interfície Web, no s'ha d'Administrar l'eina des de diversos llocs
- ✓ Interfície Web multi-llenguatge (podem posar la interfície fins i tot en català)

L'inconvenient que l'he trobat és:

- ✓ Algunes opcions interessants estan només a la versió comercial, com l'escalatge a múltiples instàncies, monitorització web avançada, gestió remota d'agents, enviament dels informes per correu electrònic, etc.

### **5.13 Conclusions**

Pandora FMS té molts avantatges com a eina de monitorització de sistemes, però el que haig de remarcar és la seva simplicitat en la configuració inicial, és a dir ràpidament es pot començar a fer una monitorització senzilla de la xarxa.



## 6 Estudi de l'eina i-enable rmf

Ens centrarem en l'estudi de l'eina i-enable rmf on definirem l'eina, les seves característiques punts febles i forts i finalment extraurem unes conclusions sobre l'eina.

### 6.1 Què és i-enable rmf?

I-enable rmf (on rmf vé de Remote Monitoring Framework) és un programari que ens serveix per a controlar els components de la infraestructura de TI, ens proporciona l'estat i el rendiment tant de hardware com de software que conformen la nostra xarxa.

I-enable rmf és de llicència comercial distribuït per l'empresa 3i infotech.

### 6.2 Objectius i necessitats

I-enable rmf és una aplicació de monitorització que permet supervisar i proporcionar visibilitat de tots els components de la nostra infraestructura de TI incloent xarxes, servidors, sistemes operatius, aplicacions de base de dades i emmagatzematge permetent així respondre amb rapidesa i gestionar proactivament les condicions que poden interrompre els serveis crítics.

S'executa 24x7 en un equip basat en Windows dins de la xarxa a monitoritzar, registra els paràmetres d'ús de la xarxa i la gestió de les dades registrats que s'emmagatzema en una base de dades històrica.

### 6.3 Característiques generals

L'arquitectura de i-enable rmf es pot classificar en:

- ✓ Arquitectura de Desenvolupament
- ✓ Arquitectura d'Eines

L'arquitectura d'implementació de l'eina és:

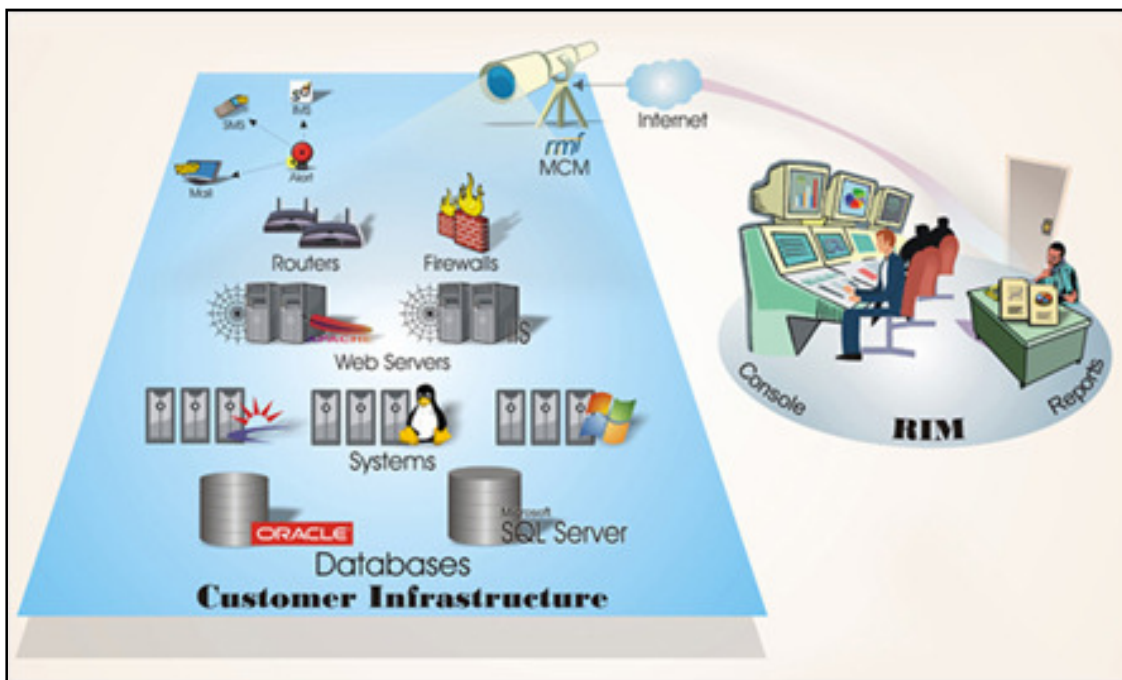


Figura 35: Arquitectura de desenvolupament de i-enable rmf

L'arquitectura d'eines representa la visió completa de les comandes.

- ✓ Customer Infrastructure: és la infraestructura de TI que s'ha de monitoritzar
- ✓ Detect: detecta esdeveniments en els elements de control relacionats amb la disponibilitat d'estat i el rendiment
- ✓ Interpret: informa sobre els esdeveniments mitjançant el correu electrònic o SMS
- ✓ Visibility Engine (VE): VE constitueix la interfície d'usuari, anàlisi de tendències i representació gràfica de les dades.



Figura 36: Arquitectura d'eines de i-enable rmf

#### 6.4 Que es pot fer amb i-enable rmf

i-enable rmf supervisa i proporciona visibilitat en tots els aspectes de l'entorn de TI, incloent xarxes, servidors, sistemes operatius, aplicacions, bases de dades i emmagatzematge.

Les seves característiques són:

- ✓ Interfície gràfica d'usuari:
  - Interfície amigable i fàcil d'utilitzar
  - Interfície d'usuari Web, s'analitza les dades per a poder crear informes
  - Entorns multiusuari
- ✓ Escalable:
  - Dissenyat per a proporcionar suport
  - Arquitectura multi-thread que permet garantir la escalabilitat i el rendiment
- ✓ Segur:
  - Encripta la comunicació entre el programari d'administració i l'agregador
- ✓ Vigilància:
  - Ràpida identificació de problemes amb lo que es redueix el temps de fallada, permet la notificació per correu electrònic i SMS
- ✓ Detecció automàtica:
  - Monitoritza adreces IP en una xarxa i genera les alertes sobre la base de temps de resposta

- La detecció automàtica per explorar i descobrir els dispositius de la infraestructura
- ✓ Mapes:
  - Dibuixa els mapes de la infraestructura per a una millor visibilitat de la vigilància
  - Provisió per a afegir en Google Maps per a una vigilància basada en la ubicació
- ✓ Informes:
  - Ofereix vistes gràfiques de les estadístiques de seguiment
  - Parcel·les de temps real de gràfics de rendiment
  - Les exportacions dels informes en format PDF
- ✓ Notificacions:
  - Alertes i notificacions configurables per disponibilitat, mètriques de rendiment i esdeveniments de registre
  - Notificacions basades en correu electrònic
  - Suporta alertes SMS
- ✓ Integració:
  - Capacitat d'integració amb l'eina d'administració d'incidentes (i-enable sd (service desk))

## 6.5 *Requeriments del sistema*

Els requeriments del sistema són:

- ✓ Plataforma .....Processador Intel o AMD
- ✓ Sistema Operatiu .....Windows 2003 o superior
- ✓ Base de Dades .....MySQL 5.0 o superior
- ✓ Requisits de navegador .....Internet Explorer 6 o superior

Especificacions mínimes de hardware

- ✓ 2 GB de RAM o més
- ✓ 2.0 GHz i superiors
- ✓ 80 GB de disc dur

### 6.6 Pantalles eina



Figura 37: i-enable rmf: pantalla inicial amb estat global

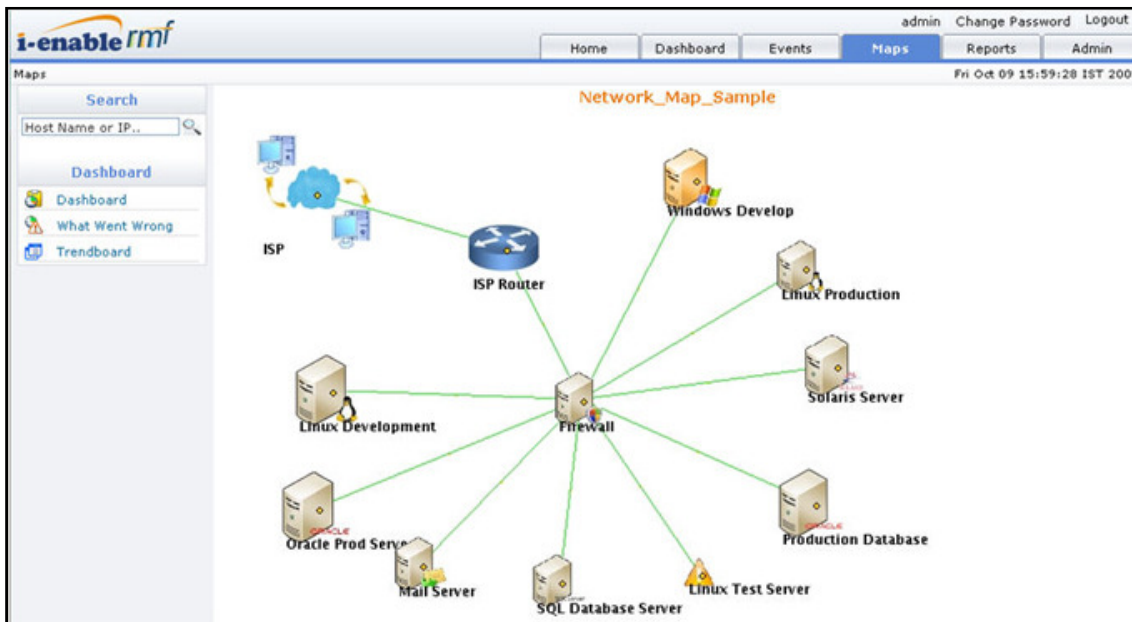


Figura 38: i-enable rmf: mapa de la xarxa

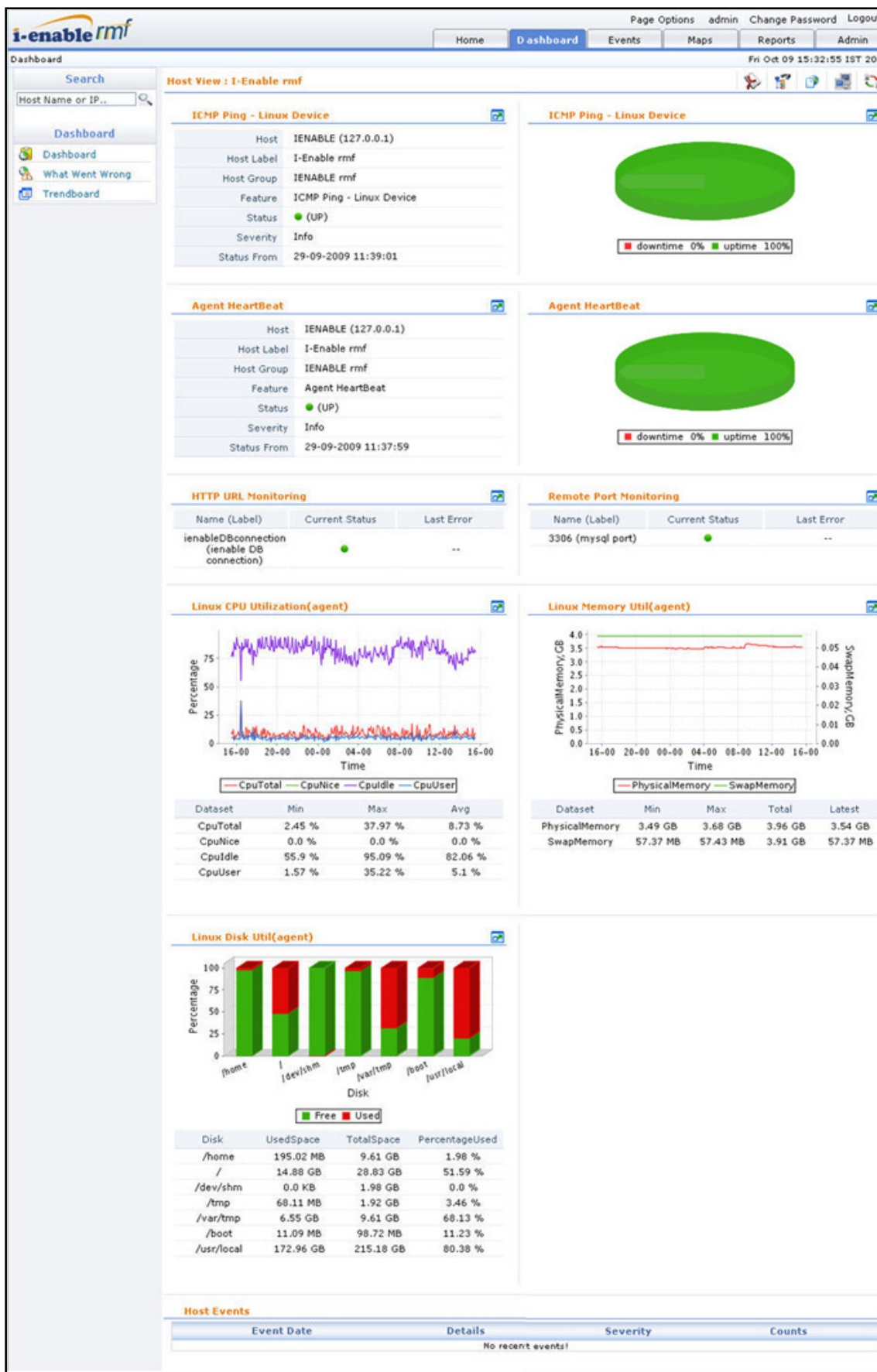


Figura 39: I-enable rmf: estat de la xarxa



## 6.7 Resum de l'eina

i-enable rmf és una arquitectura de sistemes distribuïts de monitorització de xarxes distribuïdes geogràficament, amb escalabilitat i control del disseny del procés de supervisió.

Les avantatges del control distribuït són:

- ✓ Utilització reduïda d'amplada de banda en els enllaços WAN ja que té instal·lat agents entre cada LAN i les comunicacions amb l'agregador instal·lat en l'oficina central o central de dades.
- ✓ Comunicació segura SSL entre els administradors i l'agregador
- ✓ Centralització de la notificació i gestió d'incidents dels indicadors monitoritzats

Els avantatges de l'eina són:

- ✓ Arquitectura basada en Web 100 % i amb una interfície d'usuari personalitzada
- ✓ Servidor de RMF que només gestiona l'estat de disponibilitat i rendiment dels servidors, routers, switches, dispositius d'emmagatzematge, etc.
- ✓ Identificació dels colls d'ampolla en la infraestructura de TI fent que sigui més ràpida
- ✓ Garanteix un alt temps d'activitat mitjançant la identificació de problemes de forma ràpida i precisa mitjançant la interfície Web
- ✓ Facilita la integració de dues vies amb i-enable sd (service desk) per al registre automàtic d'incidents
- ✓ Sistema automatitzat basant en les notificacions per correu electrònic i alertes SMS
- ✓ Proporciona informes que permeten un ràpid anàlisi en temps real
- ✓ Monitorització en temps real mitjançant quadres de comandament
- ✓ Descobriments LAN de forma automàtica o manual
- ✓ Compliment de les normes de seguretat més recents
- ✓ Creació de vistes de negoci personalitzades mitjançant l'agrupació de sistemes i aplicacions, per exemple:
  - Integració de vista de la infraestructura en una única consola
  - WAN de la xarxa (routers, firewalls)
  - Punt de vista del servidor (Windows, Unix)
  - Aplicacions (bases de dades, serveis, aplicacions personalitzades)
- ✓ Ús òptim dels recursos
- ✓ Augment de l'eficiència operativa
- ✓ Minimitzar el temps d'inactivitat maximitzant així la confiança dels clients

Inconvenients:

- ✓ Poca documentació sobre l'eina, pel que estàs lligat al distribuïdor
- ✓ No funciona el link per baixar la versió trial pel que no he pogut testear-la

## **6.8 Conclusions**

Per les seves característiques aquesta és una bona eina de monitorització, ja que detecta automàticament la xarxa, en cas que tinguem diverses seus, fa els mapes segons les seus i les seves infraestructures cosa que ens permet identificar millor l'abast d'una caiguda de servei, té la possibilitat d'integrar-se amb l'eina de service desk (i-enable sd) fent que automàticament es creïn els incidents, etc.

Cap remarcar que aquesta eina es comercial.

Personalment no he pogut testear-la ja que el link de la web del distribuïdor no funciona i no m'han respost al correu amb petició d'informació.



## 7 Estudi de l'eina Zabbix

Ens centrarem en l'estudi de l'eina Zabbix, definirem l'eina, les seves característiques, la instal·lació, configuració, com monitoritzar diferents equips/serveis, punts febles i forts, la realització d'unes proves i finalment extraurem unes conclusions sobre l'eina.

### 7.1 Què és Zabbix?

Zabbix és un sistema de gestió de xarxes creat per Alexei Vladishev. La seva principal funció és monitoritzar i rastrejar l'estat de serveis de xarxes i servidors de xarxes. Està escrit en C i la seva interfície web en PHP.

Zabbix permet fer controls simples que permeten comprovar la disponibilitat i la capacitat de resposta dels serveis estàndards, com SMTP o HTTP sense necessitat d'instal·lar més programari en el host monitoritzat.

Un Agent de Zabbix es pot instal·lar tant un Unix com en Windows per a supervisar les estadístiques, així com les càrregues de CPU, utilització de la xarxa, espai en disc, etc. Com a alternativa a la instal·lació d'un agent, Zabbix, inclou un suport per a monitoratge mitjançant SNMP, TCP e ICMP.

Zabbix es distribueix sota els termes de la versió 2 de la GNU General Public License.

Zabbix va començar com un projecte de programari intern en el 1998, no es però fins el 2001 que fou lliberat al públic sota llicència GPL, es van necessitar 3 anys més fins que va sortir la primera versió estable (2004). La última versió estable és 1.8.5.

### 7.2 Objectius i necessitats

Els objectius de Zabbix són:

- ✓ Ser fàcil d'utilitzar
- ✓ Una menor utilització de recursos en el processament de la informació
- ✓ Permetre reaccionar amb rapidesa
- ✓ Documentar cada aspecte del programari

### 7.3 Característiques generals

Zabbix és un sistema de monitoratge semi-distribuït amb administració centralitzada, permet la utilització de nodes de monitoratge remot, es basa en la instal·lació d'un agent en el client.

Té les següents característiques:

- ✓ Pot monitorar dispositius SNMP
- ✓ Pot monitorar dispositius amb interfícies IPMI
- ✓ Permet monitorar sense agent ni SNMP, per exemple fer un ping a un servidor o que estigui disponible un port TCP o UDP
- ✓ Permet monitorar planes web, URLs
- ✓ Permet la utilització de plantilles per facilitar el modelament de dispositius a monitorar
- ✓ Les notificacions o alertes permeten configurar nivell d'escalament, es poden enviar alertes per correu electrònic, SMS

Zabbix està integrat per tres components:

- ✓ Base de dades
- ✓ Interfície web
- ✓ El servei o daemon Zabbix

Aquesta arquitectura permet que Zabbix pugui gestionar instal·lacions grans i complexes.

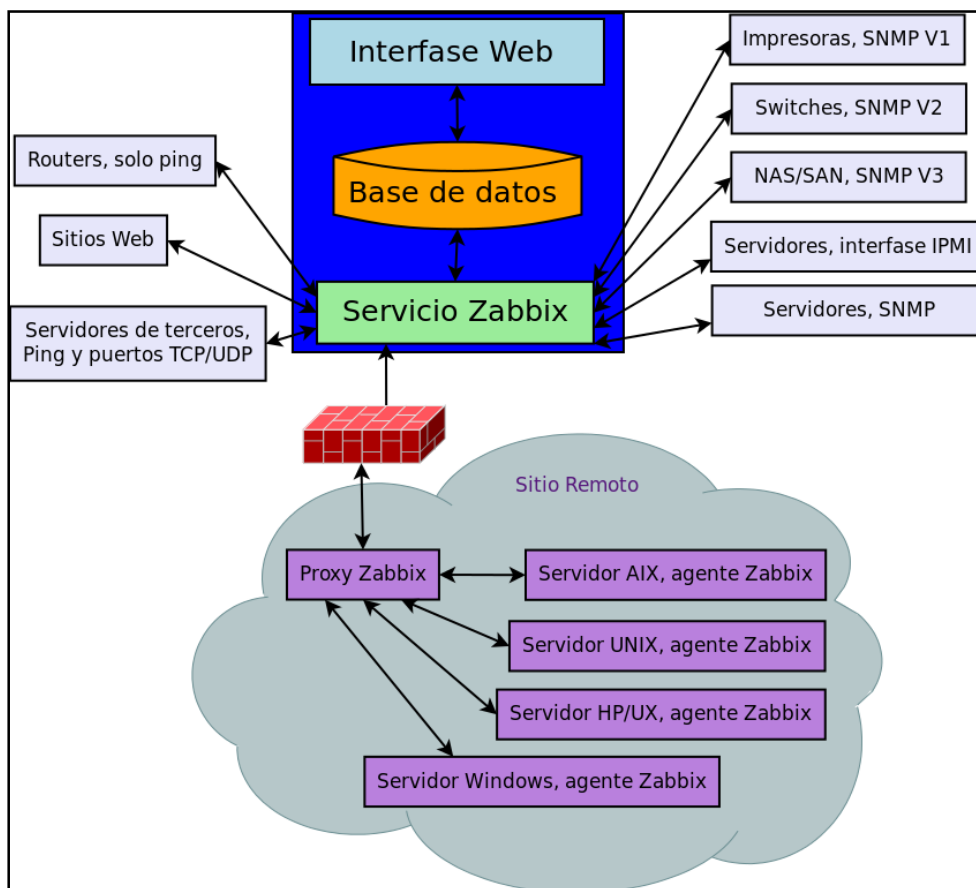


Figura 40: Arquitectura Zabbix

## 7.4 *Que es pot fer amb Zabbix?*

Zabbix ofereix:

- ✓ Detectar automàticament els servidors i dispositius de xarxa
- ✓ Interfície basada en web
- ✓ Monitoritzacions distribuïdes amb administració centralitzada mitjançant Web
- ✓ Suport per a sondejar la xarxa i mecanismes de captura
- ✓ Programari de servidor per a Linux, Solaris, HP-UX, AIX, BSD Lliures, BSD Open OS X
- ✓ Agents per a Linux, Solaris, HP-UX, AIX, BSD lliures, BSD Open, US X, Tru64/OSF1, Windows NT 4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista
- ✓ No té agents de vigilància
- ✓ Autenticació d'usuari segura
- ✓ Permisos d'usuaris flexibles
- ✓ Notificacions flexibles per correu electrònic

## 7.5 *Requeriments del sistema*

Els requisits mínims de programari són:

- ✓ GCC
- ✓ Automake
- ✓ MySQL
- ✓ Zlib-devel
- ✓ Mysql-devel (per al suport de MySQL)
- ✓ Glibc-devel
- ✓ Curl-devel (monitoratge web)
- ✓ Libidn-devel (curl-devel podria dependre d'ella)
- ✓ Openssl-devel (curl-devel podria dependre d'ella)
- ✓ Net-SNMP-devel (suport SNMP)
- ✓ Popt-devel (Net-SNMP-devel pot dependre d'ella)
- ✓ Rpm-devel (Net-SNMP-devel pot dependre d'ella)
- ✓ OpenIPMI-devel (suport de IPMI)
- ✓ Libssh2-devel (checks SSH)

### 7.6 Pantalles eina

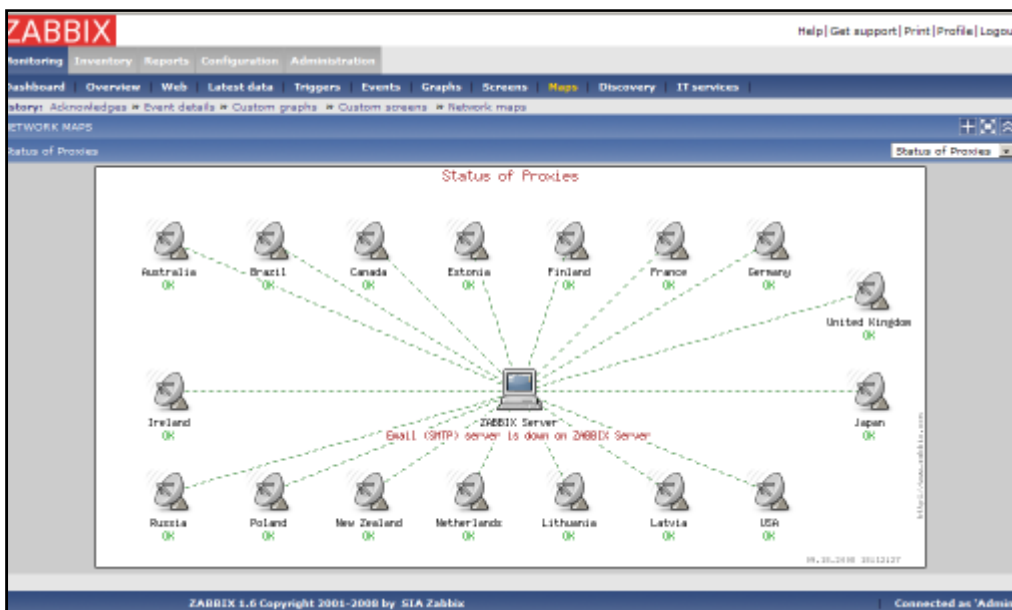


Figura 41: Zabbix: Mapa mostra l'estat de les connexions

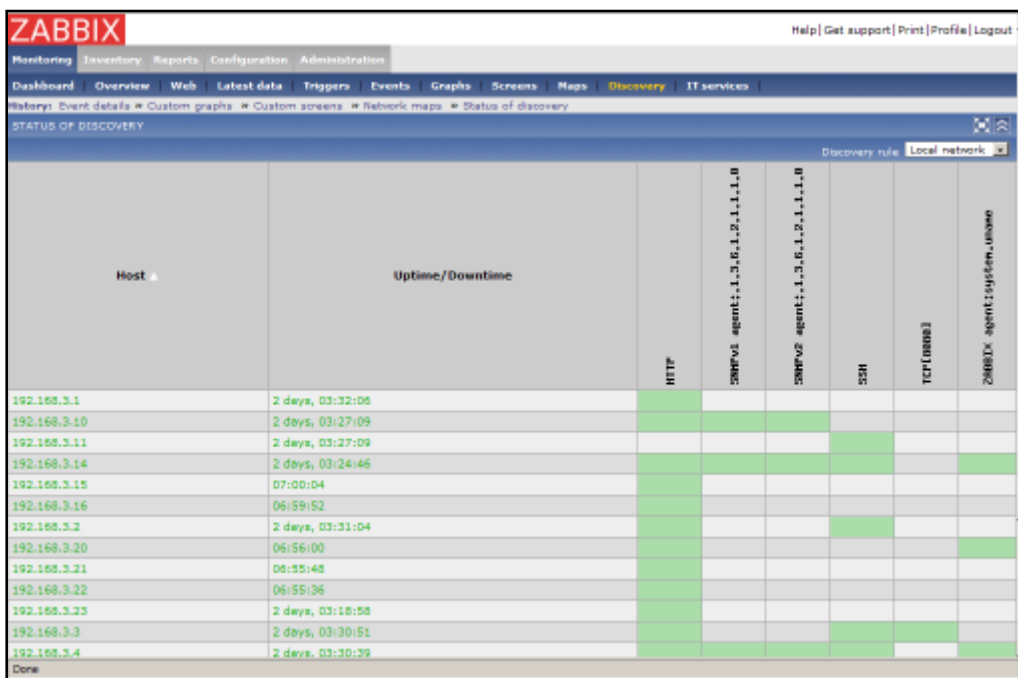


Figura 42: Zabbix: pantalla mostra l'estat dels serveis

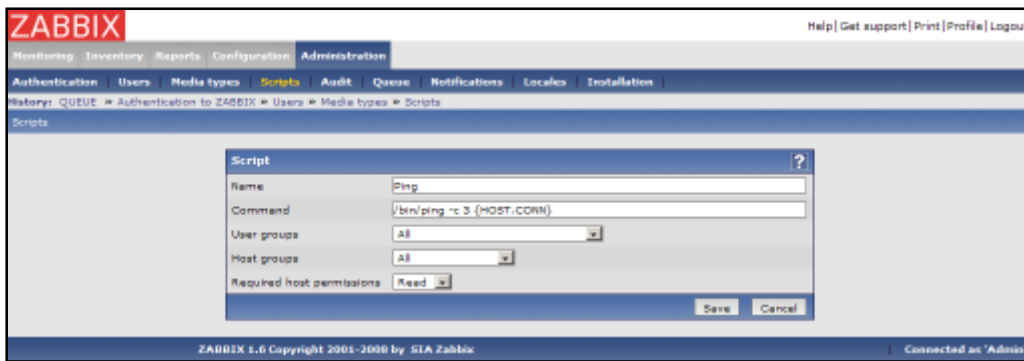


Figura 43: Zabbix: configuració d'un Ping

## 7.7 Resum de l'eina

Zabbix és una eina que ens permet monitoritzar i rastrear l'estat de serveis i servidors de xarxes, permet fer controls simples que ens comproven la disponibilitat de serveis estàndards o controls més complexos mitjançant agents. És distribuïda sota llicència GPL.

Els seus avantatges són:

- ✓ Reconeixement automàtic de servidors i dispositius de xarxa
- ✓ Interfície basada en web
- ✓ Monitoritzacions distribuïdes
- ✓ Sense agents de vigilància
- ✓ Autenticació d'usuari segura

L'inconvenient que l'he trobat és:

- ✓ No he tingut temps de comprovar l'eina ja que m'ha donat problemes la instal·lació.

## 7.8 Conclusions

Zabbix segons les seves característiques és una bona eina de monitorització, però personalment no he pogut testear-la per manca de temps.

## 8 Comparativa

Ens centrarem en explicar en que m'he basat per a fer la comparativa de les diferents eines.

### 8.1 Taula comparativa

La taula comparativa de característiques resumida amb les puntuacions acumulades per a cada grup de categories és la següent:

| Producte                 | Nagios      | Pandora FMS | Pandora FMS Enterprise | Zabbix    | i-enable rmf |
|--------------------------|-------------|-------------|------------------------|-----------|--------------|
| Versió                   | 3.2.3       | 3.2.1       | 3.2.1                  | 1.8.5     | 2.7          |
| Requeriments sistema (4) | <b>4</b>    | <b>4</b>    | 3,5                    | <b>4</b>  | 3            |
| Seguretat (5)            | 2           | 3,5         | <b>5</b>               | 2         | <b>5</b>     |
| Suport (8)               | 5           | 4           | <b>7</b>               | 3         | 4            |
| Facilitat d'ús (5)       | 3           | <b>5</b>    | <b>5</b>               | 3,5       | <b>5</b>     |
| Administració (14)       | 11,5        | <b>14</b>   | <b>14</b>              | 11,5      | 13           |
| <b>Puntuació Total</b>   | <b>25,5</b> | <b>30,5</b> | <b>34,5</b>            | <b>24</b> | <b>30</b>    |

Taula 8: Comparativa característiques eines monitorització sistemes

En negreta s'assenyala l'eina de monitorització que aconsegueix la puntuació més alta en cada categoria. El número que apareix entre parèntesi al costat de cada nom de categoria de criteris indica el nombre de criteris que s'avaluen (la puntuació màxima per categoria).

A l'Annex 1 podem veure aquesta taula completa.

## 8.2 Resum de l'anàlisi

En aquest apartat analitzaré cadascuna de les categories per a cadascun dels productes:

- ✓ **Requeriments del Sistema:** en aquest apartat valoraré el sistema operatiu (1 punt Linux, 0,5 Windows per ser comercial), si necessita Servidor Web, Base de dades i el tipus de llicència (1 punt GPL i 0,5 Comercial). Es per aquesta raó que tenim com a puntuació més alta Nagios, Pandora FMS i Zabbix, les que són amb llicència GPL.
- ✓ **Seguretat:** en aquest apartat valoraré el control de versions de l'eina (1 punt si és automàtic i 0,5 si s'ha d'anar comprovant manualment a la web), si té auditories, gestió de sessions, administració en línia (1 punt si es control total i 0,5 si és només visualització). En aquest apartat tenim com a major puntuació les comercials ja que tenen un control de versions automàtic, seguiment d'auditories. La gestió de sessions juntament amb l'administració en línia han sigut dos punts que han resultat pel posicionament de Pandora FMS.
- ✓ **Suport:** és valora si té suport, aprenentatge comercial, si existeixen foros públics, comunitat de desenvolupadors, manuals comercials, ajuda en línia, serveis professional si el desenvolupament de tercers. En aquesta categoria torna a tenir millor puntuació Pandora FMS en la seva versió comercial ja que té característiques que la fan millorar com a eina comercial però alhora es beneficia de la seva part lliure.
- ✓ **Facilitat d'ús:** en aquest apartat es valora la facilitat d'ús de l'eina, si té autodescobriment de la xarxa (detecta automàticament els diferents elements que formen la xarxa), si treu gràfics i informes, si informa d'incompliment de les SLA's, si hi ha diferents perfils d'usuaris. Aquí ha marcat la diferència dos característiques l'autodescobriment de la xarxa i que l'aplicació web tingui control total.
- ✓ **Administració:** valoro la creació de grups lògics de treball, l'extracció d'estadístiques i la seva predicció, necessitat de treballar o no amb agents (Pandora FMS, Pandora FMS Enterprise i i-enable rmf poden treballar tant amb agents com sense per això tenen 1 punt i la resta Nagios i Zabbix 0,5 ja que només poden treballar amb agents), SNMP (si necessita plugin 0,5 punts i en cas que no necessiti plugins 1 punt), pot rebre o notificar logs de sistema, té capacitat d'executar scripts fets pels usuaris, existeixen complements oficials (plugins), si es poden crear nous plugins (en aquest apartat hem valorat la dificultat fàcil 1 punt i mitjana 0,5), disposa d'alertes, mapes de xarxa (1 punt si són automàtics), distribució de la càrrega en la monitorització de la xarxa. Els elements diferenciadors han sigut que hi ha eines que poden treballar amb i sense agents (Pandora FMS, Pandora FMS Enterprise i i-enable rmf), si es necessita o no d'un plugin per a poder extreure estadístiques d'SNMP, la dificultat en la creació de complements i la creació automàtica dels Mapes.

Hem vist que en la puntuació total ha guanyat la versió comercial de Pandora FMS Enterprise, seguida de la seva versió lliure.

## 9 Conclusions

En aquest apartat farem unes conclusions per eina i una conclusió general. Per finalitzar posaré les línies que han quedat obertes en el projecte.

### 9.1 Conclusions

**Nagios** és una eina de monitorització de sistemes molt completa i amb molts avantatges, tot i que amb una configuració complexa.

**Pandora FMS** té molts avantatges com a eina de monitorització, però haig de remarcar un i és la seva simplicitat en fer una configuració inicial.

**i-enable rmf** segons les seves característiques és una bona eina de monitorització, però personalment no he pogut testear-la ja que el link de la web del distribuïdor no funciona i no m'han respost al correu amb petició d'informació.

**Zabbix** segons les seves característiques és una bona eina de monitorització, però personalment no he pogut testear-la per manca de temps.

Segons la meua experiència Pandora FMS és la millor eina de monitorització de sistemes de les que he comparat. Aquesta conclusió coincideix amb l'anàlisi fet a l'eina.

### 9.2 Línies obertes

Les línies que he deixat obertes per falta de temps són:

- ✓ Aprofundiment l'eina Zabbix.
- ✓ Instal·lar i-enable-rmf per a poder comparar-la amb més informació
- ✓ Crear un agent per a cadascuna de les eines i veure el seu funcionament



## Bibliografia

### *Libres*

- ✓ **Títol:** Learning Nagios 3.0
  - **Autor:** Wojciech Kocjan
  - **Editorial:** Packt Publishing
  
- ✓ **Títol:** Zabbix 1.8 Network Monitoring
  - **Autor:** Rihards Olups
  - **Editorial:** Packt Publishing

### *Internet*

Moltes cerques s'han fet amb el cercador <http://www.google.es>

- ✓ General
  - <http://doc.ubuntu-es.org/Comparativa>
  - [http://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n de sistemas de monitorizaci%C3%B3n de redes](http://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes)
  
- ✓ Linux
  - <http://www.ubuntu.com/>
  - <http://www.ubuntu-es.org/node/142690>
  - <http://www.ubuntu-es.org/index.php?q=node/35946>
  
- ✓ Nagios
  - <http://www.nagios.org/>
  - <http://es.wikipedia.org/wiki/Nagios>
  - <http://www.centreon.com/Centreon/product-overview.html>
  - <http://www.slideshare.net/xoroz/presetacion-nagios-centreon>
  
- ✓ Pandora FMS
  - <http://pandorafms.org/>
  - <http://pandorafms.com/index.php?sec=pandora&lng=es>
  - [http://pandorafms.com/downloads/pandora\\_product\\_detail\\_es.pdf](http://pandorafms.com/downloads/pandora_product_detail_es.pdf)
  - [http://www.openideas.info/wiki/index.php?title=Pandora\\_3.0:Documentation](http://www.openideas.info/wiki/index.php?title=Pandora_3.0:Documentation)
  - [http://es.wikipedia.org/wiki/Pandora\\_FMS](http://es.wikipedia.org/wiki/Pandora_FMS)

## Bibliografia

---

- ✓ I-enable rmf (Remote Monitoring Framework)
  - [http://www.3i-infotech.com/content/IT\\_infrastructure/ienablermf\\_overview.aspx](http://www.3i-infotech.com/content/IT_infrastructure/ienablermf_overview.aspx)
- ✓ Zabbix
  - <http://www.zabbix.com/>
  - <http://www.zabbix.com/wiki/doku.php>
  - <http://zabbix-es.blogspot.com/>

## Annex 1: Taula comparativa eines

| Versió                              | Nagios<br>3.2.3 | Pandora FMS<br>3.2.1 | Pandora FMS<br>Enterprise<br>3.2.1 | Zabbix<br>1.8.5 | i-enable rmf<br>2.7 |
|-------------------------------------|-----------------|----------------------|------------------------------------|-----------------|---------------------|
| <b>Requeriments del sistema (4)</b> | <b>4</b>        | <b>4</b>             | <b>3,5</b>                         | <b>4</b>        | <b>3</b>            |
| Sistema Operatiu                    | 1               | 1                    | 1                                  | 1               | 0,5                 |
| Servidor Web                        | 1               | 1                    | 1                                  | 1               | 1                   |
| Base de dades                       | 1               | 1                    | 1                                  | 1               | 1                   |
| Llicència                           | 1               | 1                    | 0,5                                | 1               | 0,5                 |
| <b>Seguretat (5)</b>                | <b>2</b>        | <b>3,5</b>           | <b>5</b>                           | <b>2</b>        | <b>5</b>            |
| Control de versions                 | 0,5             | 0,5                  | 1                                  | 0,5             | 1                   |
| Seguiment d'auditoria               | 0               | 0                    | 1                                  | 0               | 1                   |
| Gestió de Sessions                  | 0               | 1                    | 1                                  | 0               | 1                   |
| Verificació de correu electrònic    | 1               | 1                    | 1                                  | 1               | 1                   |
| Administració en Línea              | 0,5             | 1                    | 1                                  | 0,5             | 1                   |
| <b>Suport (8)</b>                   | <b>5</b>        | <b>4</b>             | <b>7</b>                           | <b>3</b>        | <b>4</b>            |
| Suport comercial                    | 0               | 0                    | 1                                  | 0               | 1                   |
| Aprenentatge comercial              | 0               | 0                    | 1                                  | 0               | 1                   |
| Foro Públic                         | 1               | 1                    | 1                                  | 0,5             | 0                   |
| Comunitat de desenvolupadors        | 1               | 1                    | 1                                  | 0,5             | 0                   |
| Manuais Comercials                  | 1               | 0                    | 0                                  | 1               | 1                   |
| Ayuda en línia                      | 1               | 1                    | 1                                  | 0,5             | 0                   |
| Serveis professionals               | 0               | 0                    | 1                                  | 0               | 1                   |
| Desenvolupament de tercers          | 1               | 1                    | 1                                  | 0,5             | 0                   |
| <b>Facilitat d'ús (5)</b>           | <b>3</b>        | <b>5</b>             | <b>5</b>                           | <b>3,5</b>      | <b>5</b>            |
| Autodescobrimet xarxa               | 0,5             | 1                    | 1                                  | 0,5             | 1                   |
| Perfils intefície usuari            | 0               | 1                    | 1                                  | 0               | 1                   |
| Gràfics i informes                  | 1               | 1                    | 1                                  | 1               | 1                   |
| Informar compliment SLA's           | 1               | 1                    | 1                                  | 1               | 1                   |
| Aplicació Web                       | 0,5             | 1                    | 1                                  | 1               | 1                   |

|                            |             |             |             |             |           |
|----------------------------|-------------|-------------|-------------|-------------|-----------|
| <b>Administració (14)</b>  | <b>11,5</b> | <b>14</b>   | <b>14</b>   | <b>11,5</b> | <b>13</b> |
| Grups Lògics de treball    | 1           | 1           | 1           | 0           | 1         |
| Estadístiques              | 1           | 1           | 1           | 1           | 1         |
| Predicció d'Estadístiques  | 1           | 1           | 1           | 1           | 1         |
| Agents                     | 0,5         | 1           | 1           | 0,5         | 1         |
| SNMP                       | 0,5         | 1           | 1           | 1           | 1         |
| Syslog                     | 1           | 1           | 1           | 1           | 1         |
| Scripts Externs            | 1           | 1           | 1           | 1           | 1         |
| Complements (plugins)      | 1           | 1           | 1           | 1           | 1         |
| Creació complements        | 0,5         | 1           | 1           | 1           | 1         |
| Alertes                    | 1           | 1           | 1           | 1           | 1         |
| Mapes                      | 0,5         | 1           | 1           | 0,5         | 0,5       |
| Seguretat                  | 0,5         | 1           | 1           | 0,5         | 0,5       |
| Esdeveniments              | 1           | 1           | 1           | 1           | 1         |
| Monitorització distribuïda | 1           | 1           | 1           | 1           | 1         |
| <b>Puntuació Total</b>     | <b>25,5</b> | <b>30,5</b> | <b>34,5</b> | <b>24</b>   | <b>30</b> |

Taula 9: Taula completa comparativa eines monitorització sistemes

## Índex de Figures

|            |  |    |
|------------|--|----|
| Figura 1:  | Definició de les tasques.....  | 8  |
| Figura 2:  | Diagrama de Gantt .....  | 9  |
| Figura 3:  | Línia de temps del cicle d'un incident.....                              | 11 |
| Figura 4:  | Arquitectura de Nagios .....   | 16 |
| Figura 5:  | Nagios: Configuració adreça correu notificacions .....                   | 21 |
| Figura 6:  | Nagios: Pantalla configuració i instal·lació correcta.....               | 22 |
| Figura 7:  | Nagios: Serveis que s'executen amb servei SSH crític .....               | 23 |
| Figura 8:  | Nagios: Serveis que s'executen amb servei SSH Ok .....                   | 23 |
| Figura 9:  | Nagios: Definició dels fitxers de Configuracions .....                   | 24 |
| Figura 10: | Nagios: Definició host Win7 .....  | 25 |
| Figura 11: | Nagios: Exemple definició serveis per a Host Win7.....                   | 26 |
| Figura 12: | Nagios: Definició host Ubuntu .....                                      | 27 |
| Figura 13: | Nagios: Definició serveis per a Host Ubuntu.....                         | 27 |
| Figura 14: | Nagios: Definició host RouterADSL .....                                  | 28 |
| Figura 15: | Nagios: Definició serveis host RouterADSL.....                           | 28 |
| Figura 16: | Nagios: Exemple mapa monitorització .....                                | 29 |
| Figura 17: | Nagios: Exemple Hosts .....  | 29 |
| Figura 18: | Nagios: Exemple de Serveis .....   | 30 |
| Figura 19: | Nagios: Exemple informe disponibilitat per grups de Hosts.....           | 30 |
| Figura 20: | Nagios-Centreon: Configuració de host amb Centreon .....                 | 31 |
| Figura 21: | Nagios-Centreon: Configuració de Serveis per host amb Centreon.....      | 32 |
| Figura 22: | Nagios-Centreon: Estadístiques amb Centreon.....                         | 32 |
| Figura 23: | Nagios-Centreon: Exemple estadístiques gràfiques de serveis actius ..... | 33 |
| Figura 24: | Usos de Pandora FMS .....  | 36 |
| Figura 25: | Arquitectura de Pandora FMS.....   | 37 |
| Figura 26: | Assignació contrasenya Pandora FMS .....                                 | 42 |
| Figura 27: | Arrencar Pandora FMS.....  | 42 |
| Figura 28: | Pandora FMS: Mapa de xarxa amb la vista Topology .....                   | 44 |
| Figura 29: | Pandora FMS: Mapa de xarxa amb la vista Groups .....                     | 44 |
| Figura 30: | Pandora FMS: Vista tàctica.....  | 45 |
| Figura 31: | Pandora FMS: Mapa de xarxa .....   | 46 |
| Figura 32: | Pandora FMS: Mapa de xarxa per grups .....                               | 46 |
| Figura 33: | Pandora FMS: Detalls de l'agent.....                                     | 47 |
| Figura 34: | Pandora FMS: Vista d'Agents i Mòduls.....                                | 47 |
| Figura 35: | Arquitectura de desenvolupament de i-enable rmf .....                    | 50 |
| Figura 36: | Arquitectura d'eines de i-enable rmf.....                                | 51 |
| Figura 37: | I-enable rmf: pantalla inicial amb estat global .....                    | 53 |

## Índex de Figures

---

|            |   |    |
|------------|---|----|
| Figura 38: | I-enable rmf: mapa de la xarxa.....                 | 53 |
| Figura 39: | I-enable rmf: estat de la xarxa .....               | 54 |
| Figura 40: | Arquitectura Zabbix .....                           | 58 |
| Figura 41: | Zabbix: Mapa mostra l'estat de les connexions ..... | 60 |
| Figura 42: | Zabbix: pantalla mostra l'estat dels serveis.....   | 60 |
| Figura 43: | Zabbix: configuració d'un Ping .....                | 61 |

## Índex de Taules

|          |  |    |
|----------|--|----|
| Taula 1: | Comparativa característiques eines monitorització sistemes .....   | 13 |
| Taula 2: | Requeriments de sistema eines monitorització sistemes .....        | 14 |
| Taula 3: | Requisits bàsics Nagios .....                                      | 17 |
| Taula 4: | Requisits per instal·lar totes les característiques de Nagios..... | 19 |
| Taula 5: | Característiques Pandora FMS .....                                 | 38 |
| Taula 6: | Prerequisits de Servidor de Pandora FMS.....                       | 41 |
| Taula 7: | Prerequisits de Consola de Pandora FMS.....                        | 41 |
| Taula 8: | Comparativa característiques eines monitorització sistemes .....   | 62 |
| Taula 9: | Taula completa comparativa eines monitorització sistemes .....     | 68 |