Comparativa d'eines de monitorització

Eduard Espallargas Sánchez
Consultor: Jordi Ceballos Villach
Juny 2011

Índex de continguts

Índex de figures

1. Introducció

Les empreses treballen dins d'un mercat global, competitiu, exigent i marcat per la crisi econòmica, han d'oferir bons serveis/productes, amb alta qualitat i baix cost. Dins d'aquest marc la informàtica ens ajuda a controlar tots els processos, els productes i els serveis, així la monitorització, que pertany a l'àrea de xarxes de computadors, permet supervisar tots els elements de l'empresa, mesurar les variables dels sistemes per determinar les variacions de comportament i actuar en cas de detecció de problemes o de preveure'ls.

Aquest projecte mostra com hi han moltes possibilitats de programari Open Source que cobreixen les necessitats empresarials. El primer pas era cercar les eines de monitorització utilitzant Internet i definir quines característiques han de tenir per cobrir les necessitats de les empreses. Les eines s'han comparat en un entorn de proves envers de fer-ho dels seus manuals, pel que s'ha seguit aquest mètode: al principi s'ha definit les tècniques que fan servir aquestes eines per a aconseguir informació dels dispositius remots, s'ha seleccionat tres eines basant-nos en el nombre de descàrregues i la valoració per organitzacions independents i s'han definit les característiques que es demanen a una eina d'aquest tipus utilitzant la metodologia de les enquestes. Al final s'ha intentat validar si aquestes eines cobrien les necessitats demandades i classificar-les en tres nivells per comparar cadascuna.

El treball està estructurat en quatre apartats: la descripció del pla de treball, les eines de monitorització, l'entorn de proves de les tres eines escollides i la valoració.

- Al pla de treball es descriu la motivació, els objectius i la preparació del projecte.
- L'apartat d'eines de monitorització inclou les definicions dels sistemes estandarditzats i la metodologia per la selecció dels sistemes de supervisió. Es descriu els protocols ICMP i SNMP i l'estructura de dades WMI. La comanda *ping,* que fa servir el protocol ICMP, és la utilitat més bàsica, SNMP és el protocol que dóna més informació dels dispositius remots i WMI implementa en una base de dades tota la configuració del sistema operatiu Windows. Al finalitzar aquest bloc es selecciona tres sistemes de monitorització entre les consultes a Internet i es descriu les característiques que s'analitzaran en aquestes eines.
- A l'entorn de proves s'utilitza ordinadors amb diferents sistemes operatius, un encaminador com a equip de la xarxa, diferents webs accessibles des d'Internet i s'ha fet ús dels mecanismes de monitorització descrits a l'anterior apartat. S'ha analitzat Nagios, Pandorafms i Zenoss i per cadascuna s'ha fet una breu descripció del sistema de supervisió i de l'entorn de proves, el detall de tasques principals fetes durant les proves, el desenvolupament d'agents per la monitorització i el comportament que té el programari en cada punt a comparar.
- Per la valoració s'ha utilitzat la puntuació de les característiques feta per un grup de tècnics informàtics amb experiència amb eines de monitorització.

2. Pla de treball

2.1. Abast

L'abast avarca les eines de monitorització que es trobin per Internet, essent eines que permeti la supervisió de l'estat tant dels dispositius físics de xarxa, ordinadors, servidors i els altres elements amb adreça IP, així com dels seus serveis.

2.2. Objectius

L'objectiu és fer una comparativa entre una selecció de les diferents eines de monitorització de sistemes de programari lliure, analitzant les seves característiques, avantatges i inconvenients.

Es crearà un entorn de proves per a analitzar tres eines de programari lliure escollides, que inclou fer el desenvolupament d'un agent per cadascuna.

2.3. Fites

Dins del projecte s'identifiquen 5 fites abans d'assolir l'objectiu i aporten com a resultat un lliurable que s'integra dins del document del projecte.

Fites		
Activitat / Tasca	**Data**	**Lliurable**
Descripció dels punts a avaluar	10/04/2011	document amb els punts que s'avaluaran
Proves amb eina1	21/04/2011	document amb els resultats de cada punt
Proves amb eina2	09/05/2011	document amb els resultats de cada punt
Proves amb eina3	24/05/2011	document amb els resultats de cada punt
Tancament	30/05/2011	vídeo explicatiu

Taula 1 fites del projecte

2.4. Activitats

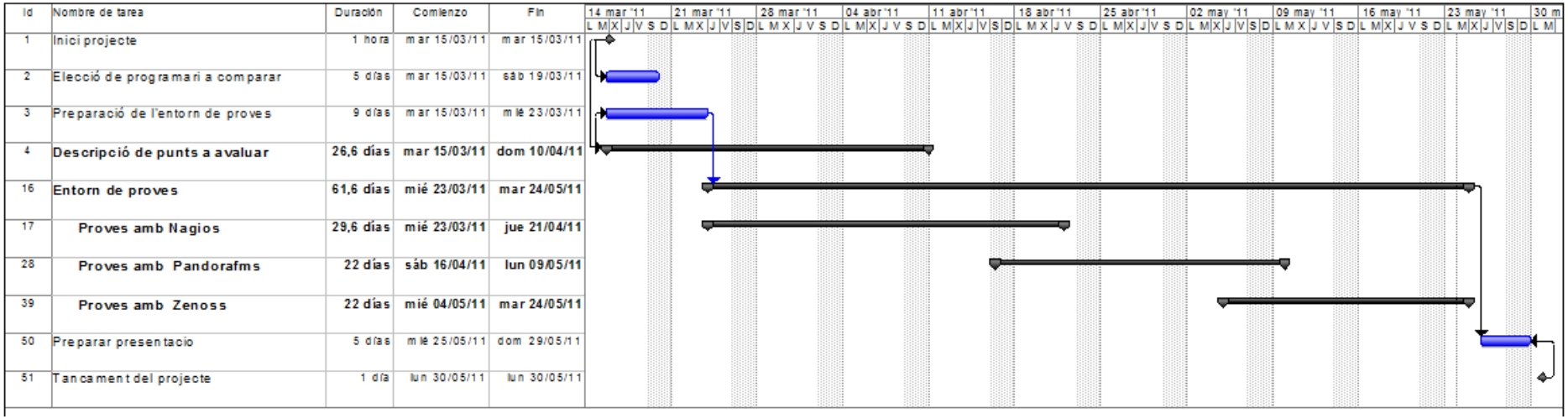
El projecte es descompon en onze tasques més petites, també anomenades EDT o estructures de distribució del treball, que tenen un lliurable final.

Activitats		
Activitat / Tasca	**Data prevista d'inici**	**Data prevista de fi**
Inici projecte	15/03/2011	15/03/2011
Elecció de programari a avaluar	15/03/2011	19/03/2011
Preparació de l'entorn de proves	15/03/2011	23/03/2011
Descripció de punts a comparar	15/03/2011	10/04/2011
Entorn de proves	23/03/2011	24/05/2011
Proves amb Nagios	23/03/2011	24/05/2011
Proves amb Pandorafms	16/04/2011	09/05/2011
Proves amb Zenoss	04/05/2011	24/05/2011
Preparar presentació	25/05/2011	29/05/2011
Tancament del projecte	30/05/2011	30/05/2011

Taula 2 activitats del projecte

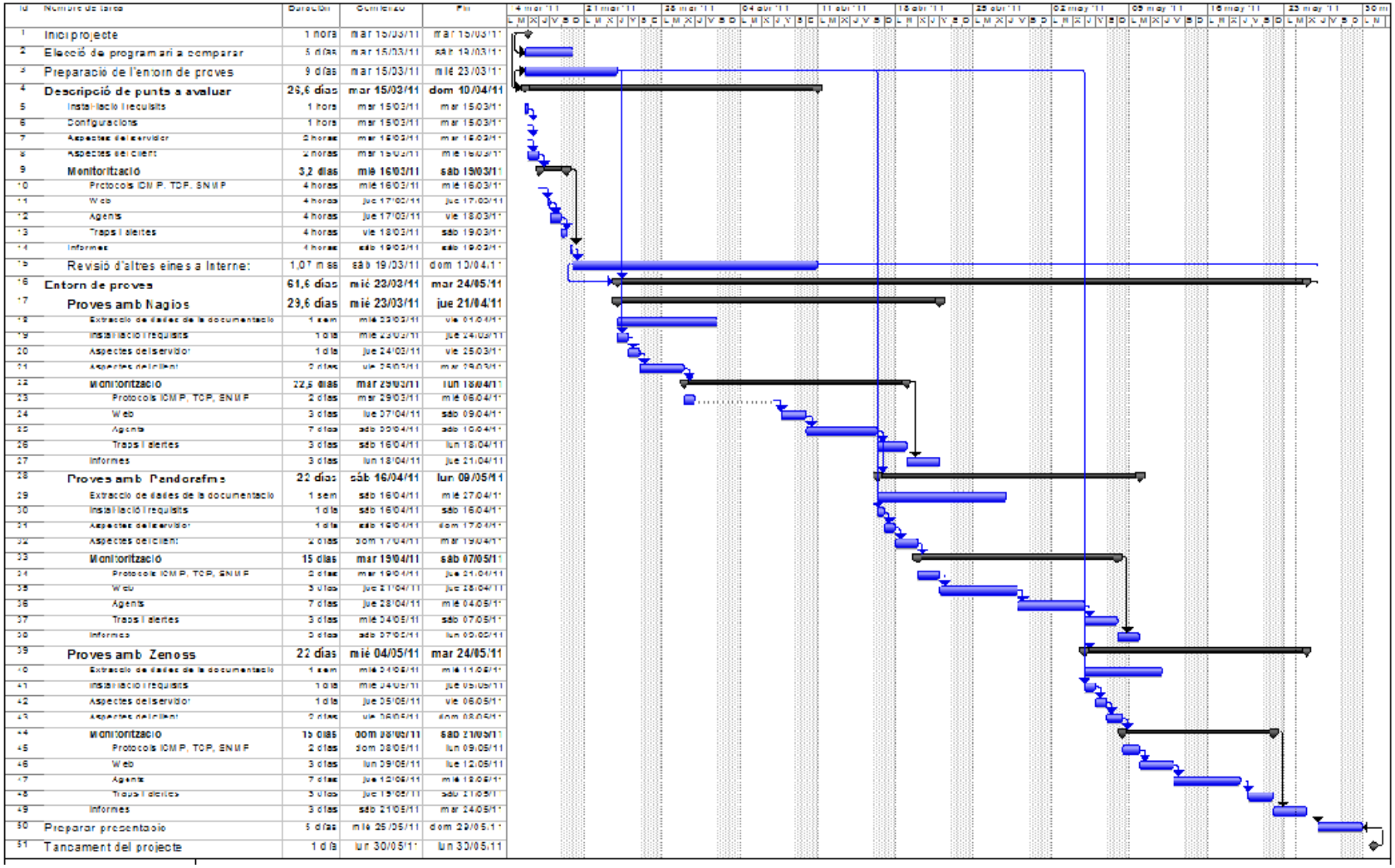
2.5. Cronograma de tasques principals

Es representa el camí que s'ha de seguir per aconseguir l'objectiu del projecte



Id	Nombre de tarea	Duración	Comienzo	Fin
1	Inici projecte	1 hora	mar 15/03/11	mar 15/03/11
2	Elecció de programari a comparar	5 días	mar 15/03/11	sáb 19/03/11
3	Preparació de l'entorn de proves	9 días	mar 15/03/11	mié 23/03/11
4	**Descripció de punts a avaluar**	**26,6 días**	**mar 15/03/11**	**dom 10/04/11**
16	**Entorn de proves**	**61,6 días**	**mié 23/03/11**	**mar 24/05/11**
17	**Proves amb Nagios**	**29,6 días**	**mié 23/03/11**	**jue 21/04/11**
28	**Proves amb Pandorafms**	**22 días**	**sáb 16/04/11**	**lun 09/05/11**
39	**Proves amb Zenoss**	**22 días**	**mié 04/05/11**	**mar 24/05/11**
50	Preparar presentacio	5 días	mié 25/05/11	dom 29/05/11
51	Tancament del projecte	1 día	lun 30/05/11	lun 30/05/11

2.6. Cronograma



	Nombre de tarea	Duración	Comienzo	Fin
1	Inici projecte	1 hora	mar 15/03/11	mar 15/03/11
2	Elecció de programari a comparar	5 días	mar 15/03/11	sáb 19/03/11
3	Preparació de l'entorn de proves	9 días	mar 15/03/11	mié 23/03/11
4	**Descripció de punts a avaluar**	**26,6 días**	**mar 15/03/11**	**dom 10/04/11**
5	Instal·lació i requisits	1 hora	mar 15/03/11	mar 15/03/11
6	Configuracions	1 hora	mar 15/03/11	mar 15/03/11
7	Aspectes del servidor	2 horas	mar 15/03/11	mar 15/03/11
8	Aspectes del client	2 horas	mar 15/03/11	mié 16/03/11
9	**Monitorització**	**3,2 días**	**mié 16/03/11**	**sáb 19/03/11**
10	Protocols ICMP, TCP, SNMP	4 horas	mié 16/03/11	mié 16/03/11
11	Web	4 horas	jue 17/03/11	jue 17/03/11
12	Agents	4 horas	jue 17/03/11	vie 18/03/11
13	Traps i alertes	4 horas	vie 18/03/11	sáb 19/03/11
14	Informes	4 horas	sáb 19/03/11	sáb 19/03/11
15	Revisió d'altres eines a interne:	1,07 mes	sáb 19/03/11	dom 10/04/11
16	**Entorn de proves**	**61,6 días**	**mié 23/03/11**	**mar 24/05/11**
17	**Proves amb Nagios**	**29,6 días**	**mié 23/03/11**	**jue 21/04/11**
18	Extracció de dades de la documentació	1 sem	mié 23/03/11	vie 01/04/11
19	Instal·lació i requisits	1 día	mié 23/03/11	jue 24/03/11
20	Aspectes del servidor	1 día	jue 24/03/11	vie 25/03/11
21	Aspectes del client	5 días	vie 25/03/11	mar 29/03/11
22	**Monitorització**	**22,6 días**	**mar 29/03/11**	**lun 18/04/11**
23	Protocols ICMP, TCP, SNMP	2 días	mar 29/03/11	mié 06/04/11
24	Web	3 días	jue 07/04/11	sáb 09/04/11
25	Agents	7 días	sáb 09/04/11	sáb 16/04/11
26	Traps i alertes	3 días	sáb 16/04/11	lun 18/04/11
27	Informes	3 días	lun 18/04/11	jue 21/04/11
28	**Proves amb Pandorafms**	**22 días**	**sáb 16/04/11**	**lun 09/05/11**
29	Extracció de dades de la documentació	1 sem	sáb 16/04/11	mié 27/04/11
30	Instal·lació i requisits	1 día	sáb 16/04/11	sáb 16/04/11
31	Aspectes del servidor	1 día	sáb 16/04/11	dom 17/04/11
32	Aspectes del client	2 días	dom 17/04/11	mar 19/04/11
33	**Monitorització**	**15 días**	**mar 19/04/11**	**sáb 07/05/11**
34	Protocols ICMP, TCP, SNMP	2 días	mar 19/04/11	jue 21/04/11
35	Web	3 días	jue 21/04/11	jue 28/04/11
36	Agents	7 días	jue 28/04/11	mié 04/05/11
37	Traps i alertes	3 días	mié 04/05/11	sáb 07/05/11
38	Informes	3 días	sáb 07/05/11	lun 09/05/11
39	**Proves amb Zenoss**	**22 días**	**mié 04/05/11**	**mar 24/05/11**
40	Extracció de dades de la documentació	1 sem	mié 04/05/11	mié 11/05/11
41	Instal·lació i requisits	1 día	mié 04/05/11	jue 05/05/11
42	Aspectes del servidor	1 día	jue 05/05/11	vie 06/05/11
43	Aspectes del client	2 días	vie 06/05/11	dom 08/05/11
44	**Monitorització**	**15 días**	**dom 08/05/11**	**sáb 21/05/11**
45	Protocols ICMP, TCP, SNMP	2 días	dom 08/05/11	lun 09/05/11
46	Web	3 días	lun 09/05/11	lue 12/05/11
47	Agents	7 días	jue 12/05/11	mié 18/05/11
48	Traps i alertes	3 días	jue 19/05/11	sáb 21/05/11
49	Informes	3 días	sáb 21/05/11	mar 24/05/11
50	Preparar presentació	5 días	mié 25/05/11	dom 29/05/11
51	Tancament del projecte	1 día	lun 30/05/11	lun 30/05/11

3. Eines de monitorització

Per la supervisió o monitorització s'utilitzen sistemes que mitjançant eines estàndards o agents específics permeten la detecció de comportaments anòmals en els elements connectats a una xarxa informàtica i interactuar amb ells per a resoldre'ls.

La informàtica ha evolucionat seguint dos recorreguts a destacar: primer el pas de ser l'eina que facilita i accelerar els processos habituals a ser el cor dels propis processos, o sigui ha arribat a ser imprescindible per a elaborar un document, per controlar la producció o per definir els circuits de funcionament intern; el segon és la implantació de les TIC que han estès les xarxes fora dels àmbits locals. Aquests dos fets han produït que aspectes com la gestió, el control i la supervisió dels sistemes informàtics esdevinguin una necessitat estratègica per les organitzacions que volen aconseguir una millor qualitat en els seus productes i/o serveis sense incrementar el cost. Aquests canvis també han propiciat l'aparició d'empreses que ofereixen un NOC o *Network Operation Center*, per a donar serveis de monitorització de 24x7 des d'una infraestructura externa a les xarxes dels clients o implantant el servei dintre d'aquestes.

Els sistemes de monitorització també han evolucionat, al principi eren distribuïts pels fabricants de dispositius i es feia la supervisió dels dispositius de la xarxa d'àmbit local, al final, controlen qualsevol element connectat a la xarxa per que són sistemes heterogenis o multifabricants i aprofiten l'estandardització de protocols com l'SNMP o l'ICMP.

Les actuals eines de monitorització prenen importància per millorar la disponibilitat, el rendiment i la efectivitat dels sistemes informàtics i agrupen funcionalitats per a la configuració dels dispositius, avaluar el tràfic, supervisar els sistemes, detectar errors, millorar la seguretat, controlar les operacions diàries, inventari, seguiment dels registres i elaborar informes.

3.1. Elements de la monitorització

El funcionament es basa en una estructura simple de comunicació entre dos elements: l'emissor o servidor de la pròpia eina, el receptor o dispositiu connectat a la xarxa i un medi comú de comunicació per a interactuar, tot i que en les dos primeres es fa el desplegament del sistema de monitorització. La comunicació és de 1 a N o la més habitual de N a N, doncs sempre es supervisen diferents equips i es solen crear servidors per a gestionar diferents àmbits, el que simplifica, facilita l'escalabilitat, la modificabilitat i l'extensibilitat d'aquestes eines.

En aquest estudi s'han avaluat dos blocs: les característiques comunes de les eines de supervisió que les fan adaptables a les necessitats de l'usuari i els mecanismes per a monitoritzar que fan la recol·lecció de la informació.

En el primer apartat s'agrupen als servidors, la interfície dels administradors per a gestionar l'eina, la base de dades i el seus processos. La recol·lecció de la

informació es fa sobre una base de dades que permet la seva manipulació per a resoldre les peticions demanades al sistema de monitorització. Aquestes dades tenen com a característica especial la temporalitat, ja que la informació que proporciona és correcte en un moment determinat, i la variabilitat segons canviïn, així podria ser estàtica si no canvia en un temps, per exemple l'equipament de inventari, o dinàmica si canvia constantment, per exemple l'ample de banda dels dispositius.

En el segon apartat els mecanismes de monitorització fan servir diferent eines per a obtenir les dades:

- els protocols de xarxa, estan desenvolupat en el punt 3.2.1 i fan servir tècniques de mostreig o *polling* als dispositius a controlar amb protocols estàndards, com SNMP, ICMP i HTTP.
- la recepció d'esdeveniments, anomenats *traps*, que són enviats des dels dispositius remots quan detecten una anomalia.
- instal·lant agents en els dispositius a monitorar, un programari allotjat en el dispositiu supervisat que recull dades que poden ser enviades o consultades per l'eina de monitorització. Requereixen del desenvolupament d'un programari específic pel sistema on estan instal·lades i provoquen un consum de recursos.
- amb maquinari específic, anomenat sondes, que recull la informació per la que s'ha programat. Són molt habituals per a mesurar el tràfic de xarxa i com sensors de temperatura, humitat, tensió elèctrica,... .

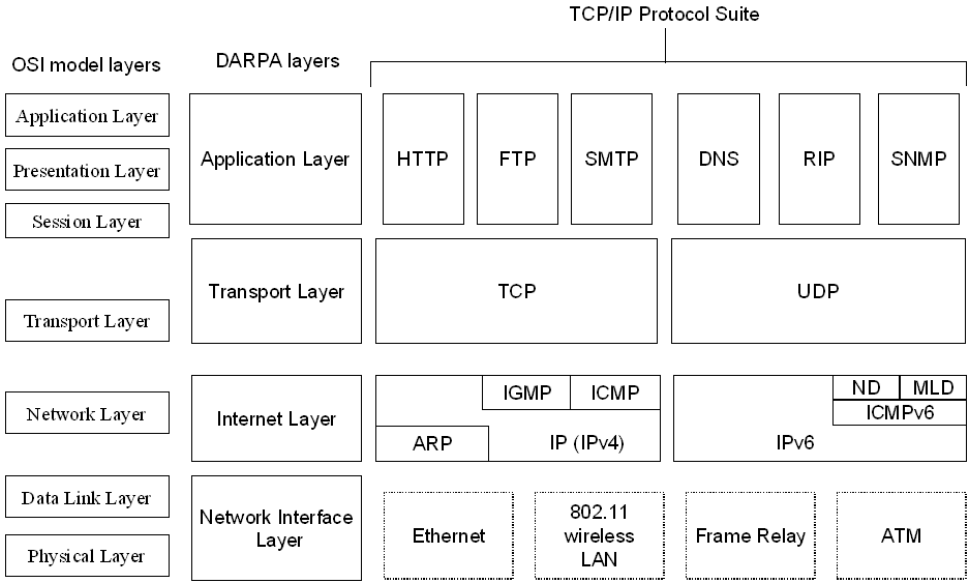
3.2. Mecanismes per a monitoritzar

De totes les eines de monitorització destaquen les basades en els protocols de xarxa TCP/IP, sobretot l'ICMP i l'SNMP, i l'eina WMI que incorpora una base de dades per la consulta i la gestió dels components del sistema operatiu Windows.

3.2.1. Protocols de xarxa

Són protocols estàndards que han impulsat l'aparició dels sistemes de monitorització. El més habitual és utilitzar el protocol SNMP, que dóna més informació que la resta, Ping per determinar si un element està connectat, HTTP per provar planes web, Telnet per la gestió i SSH per establir connexions remotament. També hi han eines com NMAP o Portscaner per fer un test dels ports TCP/UDP, el que aporta més funcionalitats.

En el següent dibuix estan representats els protocols més habituals i la seva correspondència del model OSI i del model TCP/IP o *DARPA Layers*



Il·lustració 1 esquema de protocols TCP/IP

L' il·lustració mostra les arquitectures per les comunicacions, Model OSI i DARPA, amb els protocols distribuïts en capes. Cal destacar dos protocols: ICMP/PING per la seva senzillesa i SNMP per l'aportació d'informació.

3.2.1.1. ICMP

La utilitat o comanda basada en el protocol ICMP més coneguda és el PING, també es considera l'eina més bàsica per la monitorització. La comanda envia un paquet a un equip destí, aquest retorna un paquet de resposta i es calcula el temps transcorregut, això ens indica si un equip està actiu o no (és típic escoltar l'expressió "està viu" o " no està viu") i la latència o temps que triga el paquet en anar al destí i torna a l'origen.

La comanda té el format *ping adreça_destí,* essent una adreça_destí una expressió de 4 xifres o un nom reconegut als DNS).

```
C:\Users\provençals>ping www.gmx.com

Haciendo ping a www.gmx.com [213.165.64.202] con 32 bytes de
datos:
Respuesta desde 213.165.64.202: bytes=32 tiempo=82ms TTL=50
Respuesta desde 213.165.64.202: bytes=32 tiempo=88ms TTL=50
Respuesta desde 213.165.64.202: bytes=32 tiempo=82ms TTL=50
Respuesta desde 213.165.64.202: bytes=32 tiempo=87ms TTL=50

Estadísticas de ping para 213.165.64.202:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 82ms, Máximo = 88ms, Media = 84ms
```

Il·lustració 2 exemple del protocol ICMP

En l'exemple ens dóna la següent informació útil per una eina de monitorització: hi ha connectivitat fins els destí per que s'han rebut les respostes, el temps de resposta mig de 84 milisegons, l'adreça de destí és 213.165.64.202 (dada obtinguda després de resoldre el nom als DNS) i el percentatge de paquets perduts.

Un altre paràmetre utilitzable, si es prepara correctament, és el valor TTL que indica el nombre de xarxes o d'encaminadors per les que ha circulat el paquet i serveix com indicador per rebutjar-lo com a tràfic obsolet. El seu funcionament és: al formar la comanda es guarda el valor d'aquest camp, en aquest cas s'ha consultat que és 128 en la variable del registre de windows *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters*, i és descompta un 1 per cada encaminador que passa fins arribar al destí. S'ha de tenir en compte que el valor del camp es carrega al retornar el paquet, pel que és important conèixer aquest nou valor per poder extreure informació del retorn (en el nostre exemple 50 no indica res, si no coneixem quin valor de TTL té el servidor gmx), i que si arriba a 0 els encaminadors el rebutjaran per eliminar tràfic innecessari.

En les eines de monitorització al detectar la pèrdua de la resposta o al superar el llindar del temps de resposta predefinit es genera una alarma per a indicar una possible incidència.

3.2.1.2. SNMP (Simple Network Management Protocol)

Aquest protocol és el més rellevant per les eines de monitorització. Va ser desenvolupat per l'IETF (*Internet Engineering Task Force*) amb la intenció d'aconseguir un protocol de gestió per la xarxa Internet i des de llavors ha evolucionat per la versió 1, la versió 2 i la versió 3 que estan descrits als RFC 2271 al 2275 i del 2570 al 2575, respectivament.

SNMP v2 incorpora l'obligació d'una clau en les funcions d'escriptura, sistemes de control en la transferència de grans volum de dades i millores en l'enviament d'esdeveniments des de l'agent. SNMMP v3 es centra en millores en la seguretat: xifrat de comunicació i de les claus d'autentificació, incorpora mecanismes que controlen el temps de les peticions per evitar repeticions i millores en l'autentificació dels agents.

Característiques

El protocol es basa en dos elements: els Administradors o *Management Stations* que correspondria als servidors de les eines de monitorització, que són els encarregats de gestionar tota la informació, i els Agents o *Network Agents* situats als dispositius a supervisar. Els administradors tenen funcions per a enviar peticions de consulta als agents, de rebre les respostes, per tractar la informació que reben i per notificar. Els agents tenen les funcions d'enviar les respostes a les peticions que l'arribaven i enviar una informació concreta, quan succeïa un esdeveniment.

La base del protocol és la consulta d'informació molt concreta emmagatzemada en l'agent anomenada OID i que està dins d'una estructura d'arbre anomenada MIB, la què veurem en més profunditat en el següent apartat.

Pels fluxos TCP o missatges entre els dos elements es fa servir el port 161 UDP, protocol no orientat a la connexió, per les comandes SNMP des del gestor i el port 162 UDP per enviar els traps des de l'agent.

Les *comunity* o claus permeten l'accés als nivells de lectura (RO) i al de escriptura (RW). La seguretat del sistemes supervisats està limitada pel nivell de seguretat d'aquestes claus i el xifrat de la comunicació.

Funcionalitats
Es una eina simple, fàcil i flexible per a gestionar la xarxa i s'utilitza per a:

- En el nivell d'escriptura pot configurar equips amb les limitacions del protocol.
- supervisar diferents paràmetres de rendiment de la xarxa, amples de banda, identificar tendències o comportaments habituals,.. .
- detectar errors en les transmissions i en els equips.
- generar avisos quan succeeix un esdeveniment o per superar uns llindars que han estat programats als agents i els avisos són programats i poden ser per SMS, correu, sonors, plana web,.. .
- auditories de l'ús de la xarxa per equips o usuaris, ja que les consultes poden ser programades en seqüències de temps curts (dependrà del nombre de dispositius a consultar i del espai en disc per emmagatzemar la informació).

Missatges
Es basa en la comunicació entre els Administradors i els Agents i destaquen els següents missatges:

- *GetRequest*: fa una sol·licitud de consulta de les MIB.
- *GetNextRequest:* demana el següent paràmetre que ocupa la posició seqüencial de la MIB.
- *GetResponse:* respon la petició que ha rebut abans pel gestor.
- *Set request (SetRequest):* es demana la modificació d'un valor en la MIB del dispositiu que té instal·lat l'agent.
- *Trap:* envia una notificació quan es produeix un esdeveniment o un canvi i el seu sentit és des de l'agent al gestor.
- *GetBulkRequest:* és un missatge usat per les versions 2 i 3 que fa la mateixa funció de *getNextRequest.*
- *InformRequest*: és un missatge usat per les versions 2 i 3 per a intercanvi d'informació entre gestors sobre objectes supervisats.

Inconvenients
Sobretot és l'excés de tràfic que es pot generar al fer consultes molt esteses o fer-les periòdiques amb poc temps i la seguretat, ja que la versió 2 és la més estesa i existeix la possibilitat de capturar la *community* sense xifrar durant la consulta.

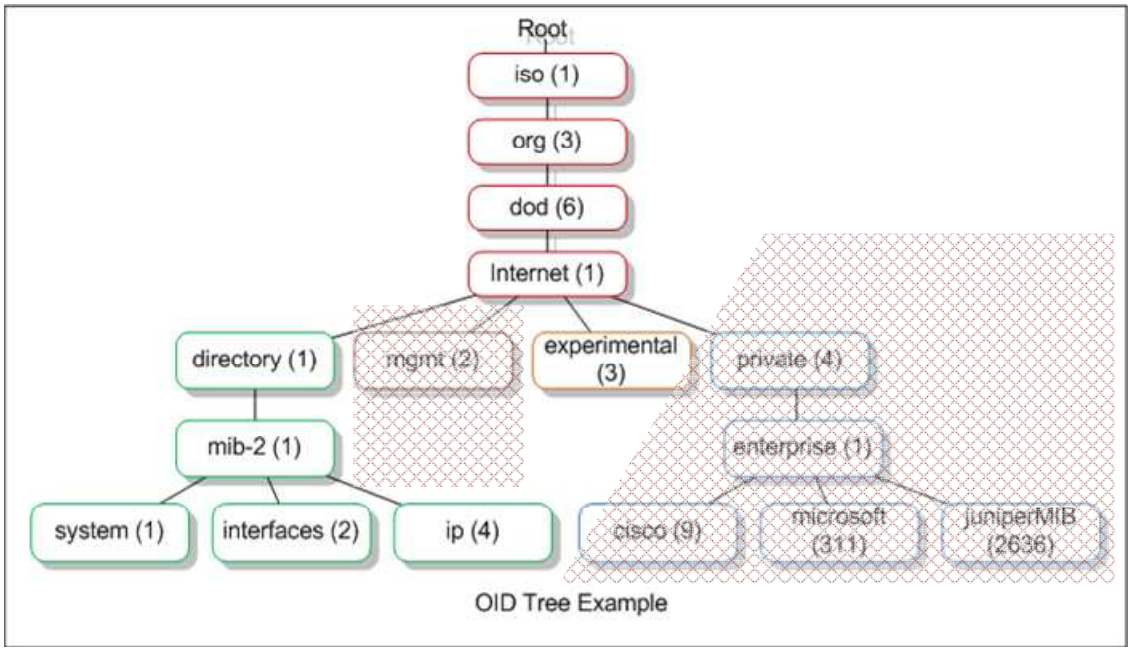
MIB (*Management Information Base*) i OID (*Object Identifier*)
Destaquem aquests dos conceptes per la importància en el protocol SNMP. La MIB és similar a una base de dades estructurada en forma d'arbre i que es descompon en branques o nodes estructurals i fulles o nodes d'informació. Els primers descriuen el camí per arribar a les fulles i els segons són els extrems de l'estructura que contenen els objectes, anomenats OID, per gestionar-los i consultar-los.

L'administrador del protocol SNMP té localment la referència dels elements consultables en la MIB del dispositiu, el que li permet fer-li la consulta d'objectes o OID que proporcionen informació concreta.

L'arbre té una estructura igual per tots els dispositius i la diferència es troba sota el node d'"internet" (MIB 1.3.6.1), on hi ha quatre subnodes:

- directory: reservat per l'OSI directory (X.500), estandardització futura de l'estructura de directoris.
- mgmt: reservat per a objectes de la IAB, que corresponen als objectes estàndards de les MIB-I i MIB-II.
- experimental: reservat per a objectes experimentals.
- private: reservat per que les empreses afegeixin els seus OID.

Esquema de la MIB[1]:



Il·lustració 3 esquema MIB per a qualsevol dispositiu

Els nodes de les estructures de "mgmt" i "private" són els més consultats. Poden representar-se en format numèric o en format de text, per exemple:

text: iso.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOcte
numèric: 1.3.6.1.2.1.2.2.1.10

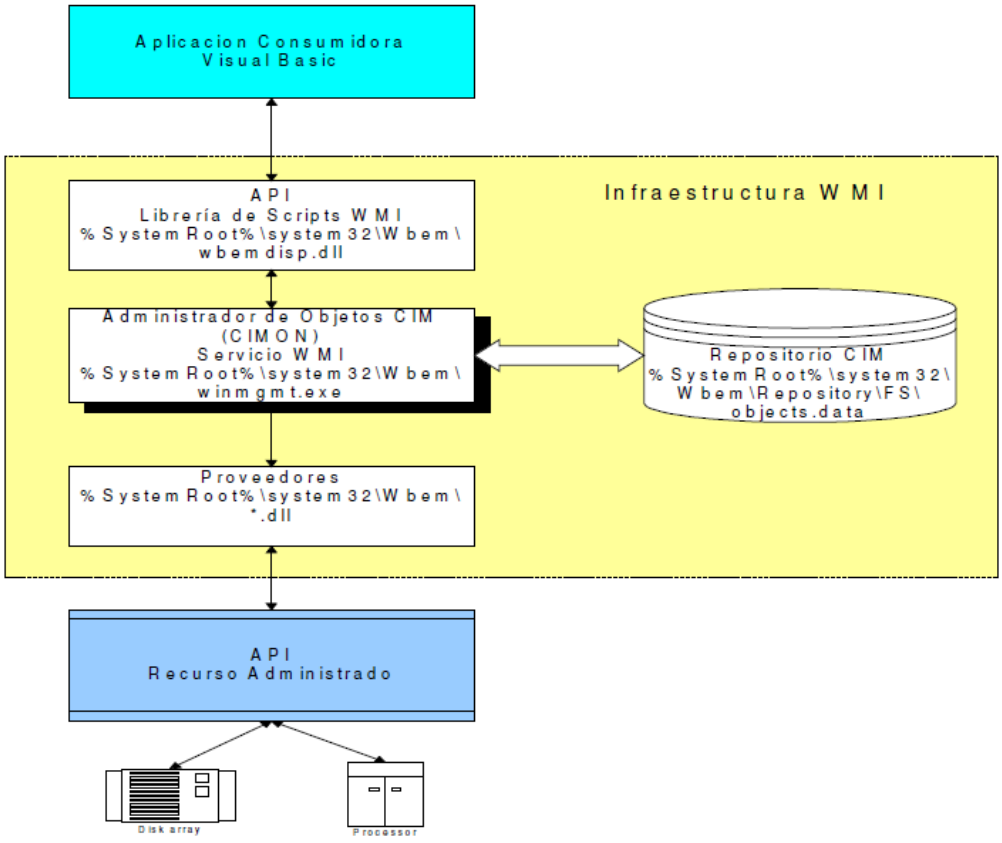
Així, per exemple, la MIB que dóna la CPU d'un encaminador de l'empresa CISCO en els últim 5 segons és 1.3.6.1.4.1.9.9.109.1.1.1.1.6. i el resultat obtingut és l'OID.

[1] http://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics

Les MIB són proporcionades pel fabricant i existeix dues versions, MIB-I i MIB-II, totalment compatibles respecte al seu ús. Per la consulta de les MIB dels fabricants es pot fer servir eines específiques per extreure les dades de l'equip o anar a les adreces http://www.oidview.com/mibs/detail.html i http://www.mibsearch.com/.

3.2.2.WMI

"Instrumental d'administración de Windows (WMI, *Windows Management Instrumentation*) és la implementació de Microsoft de WBEM, una iniciativa que pretén establir normes estàndards per a tenir accés i compartir la informació d'administració a través de la xarxa d'una empresa."[2] L'estàndard WBEM és una arquitectura que integrar l'administració de sistemes, formada per objectes que permeten administrar els recursos d'un ordinador que té un sistema operatiu Windows. Està estructurat en una base de dades SQL que emmagatzema informació sobre el proveïdor, el maquinari, el programari i el sistema operatiu de l'equip i és accessible local o remotament amb drets de lectura o escriptura per a permetre la configuració remotament.



Il·lustració 4 estructura WMI[3]

La infraestructura de WMI té quatre components:

- una API interfície per tramitar els accessos

[2] http://technet.microsoft.com/es-es/library/cc787057(WS.10).aspx

[3] Dibuix extret de http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/886/5/T10391CAP2.pdf

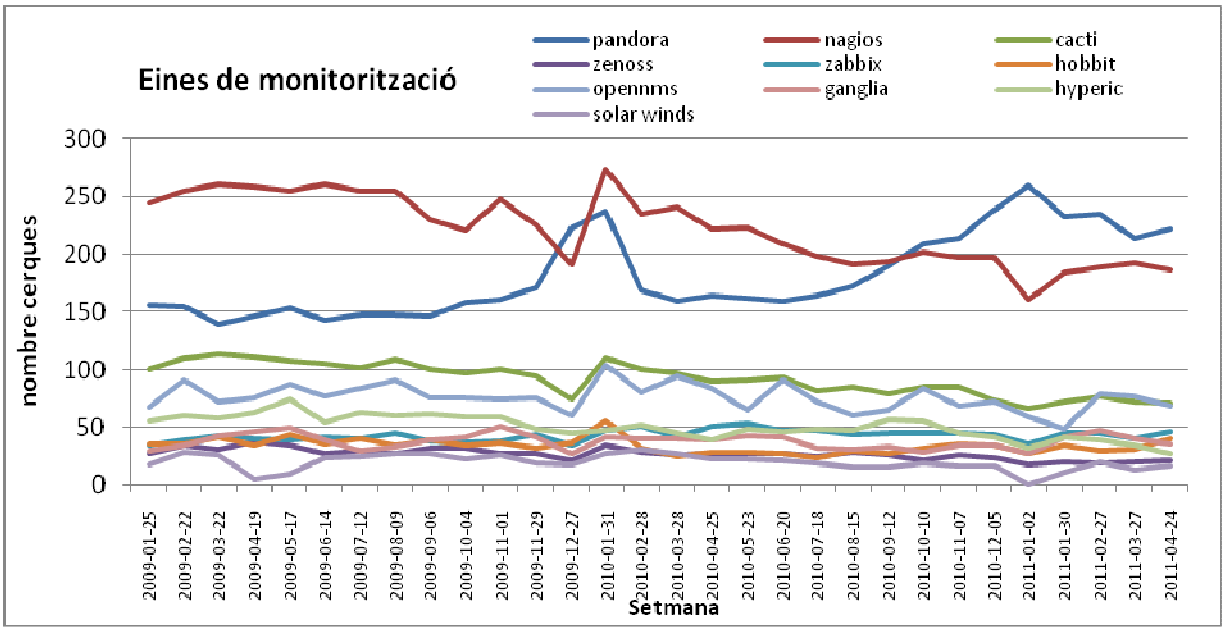
- CIMON o l'administrador d'objectes que implementa la seguretat, gestiona els accessos entre la resta de components i és la interfície per accedir a WMI.
- el repositori CIM emmagatzema la informació per localitzar els objectes en una estructura d'arbre on els nodes s'anomenen *namespace*, aquests serà un dels paràmetres a configurar durant les proves amb WMI.
- els proveïdors és la interfície per adreçar la petició a l'API proporcionada pel fabricant.

La informació es consultable amb una eina especialitzada com "WMI Explorer".

3.3. Selecció de les eines de monitorització

Per a escollir les eines s'ha fet una recerca per Internet d'eines Open Source a partir de les paraules: "eines de monitoritzacio", "herramientas de monitorizacion", "Network Manager" i "monitoring system". Els programaris recollits són Nagios, Hyperic, Zabbix, Server Eye, OpenNMS, Hobbit, Nimsoft, Solar Winds, Zyrion, Munin, Cacti, GroundWork, Zenoss, Ganglia, Nedi, Osimus, Argus, Pandorafms, Intermapper, Wormly, PacketTrap.

Per fer la selecció entre aquestes eines s'ha fet servir la plana de Google http://www.google.com/insights/search/?hl=ca# per extreure estadístiques del nombre de cerques. S'ha escollit les 10 eines amb els valors més alts i els resultats es poden veure a la següent gràfica, que indica el nombre de consultes fetes a les paraules clau (representat a l'eix vertical) per períodes de 4 setmanes i des de l'any 2009 anys (eix horitzontal). La gràfica resultat és:



Il·lustració 5 gràfica de cerques a Google

Les paraules han estat manipulades per centrar els resultats en les eines de monitorització que s'estan comparant. Per validar els resultats es pot verificar a la taula 3 les paraules clau (amb el signe menys són les paraules excloses) i les cerques més freqüents a Google per a aquestes paraules:

Paraules clau	**Cerques principals**	
nagios	Centreon nagios centos nagios centreon nagios ubuntu nagios vmware	nagios 3 nagios exchange zabbix nagios cacti cacti
pandora -psp -ipod -iphone -splinter -radio -recovery -mobile -hearts -tv -firefox -app -battery -player -music	pandora download pandora mac pc pandora proxy pandora open pandora	pandora linux pandora installer pandora software pandora ubuntu pandora one
zabbix	zabbix agent zabbix install zabbix mysql zabbix server zabbix ubuntu	zabbix windows nagios nagios zabbix zabbix snmp zabbix monitoring
cacti	cacti plugin ubuntu cacti install cacti nagios nagios cacti	cacti server cacti template cacti cisco cacti mysql cacti windows
zenoss	download zenoss install zenoss ubuntu zenoss zabbix zenoss core	zenoss monitoring zenoss nagios zenoss snmp zenoss vmware zenoss windows
hobbit	hobbit client hobbit monitor hobbit monitoring hobbit server	hobbit snmp linux hobbit xymon
OpenNMS	opennms centos opennms configuration opennms port opennms ubuntu opennms vmware	opennms vs nagios opennms windows zabbix zenoss opennms nagios
Ganglia	ganglia aix ganglia centos ganglia download ganglia gmond ganglia install	ganglia monitor ganglia nagios ganglia rpm ganglia windows
Hyperic	hyperic agent hyperic download hyperic hq hyperic monitoring hyperic nagios	hyperic open source hyperic plugin hyperic snmp hyperic ubuntu

		hyperic vmware
Solar Winds	free tftp server solar winds calculator solar winds ftp solar winds monitoring	solar winds orion solar winds snmp solarwinds

Taula 3 taula de paraules clau per les cerques a Google

En general destaca el lideratge de Nagos i Pandora, així com la distancia respecte a les altres eines, Cacti i OpenNMS fa un anys que té un lleuger descens però estan al voltant de les 70 descàrregues i per sobre de la resta. Un comportament curiós de les dues eines més consultades que no puc justificar, és l'intercanvi de posicions sobre l'agost passat i el comportament oposat, una puja l'altre baixa i a l'inrevés, durant tota la gràfica.

Eines seleccionades

Nagios, Pandorafms per que són les eines de monitorització líders. La tercera és Zenoss per que va ser escollida per Gartner, al desembre del 2010, entre les eines d'anàlisi i correlació d'esdeveniments per avaluar, quedant situada al quadrant de les empreses visionaries. Al document de Gartner es fa aquesta valoració de les empreses del *Magic Quadrant for IT Event Correlation and Analysis* que "*Zenoss ha tingut èxit amb un creixement en un període relativament curt de temps pels clients de Gartner i proveïdors referents que destaquen els preus, la velocitat de desplegament i la funcionalitat (sobretot per a la gestió d'entorns virtuals) com les principals raons per a l'elecció de Zenoss. No obstant això, la notificació i presentació de la informació eren vistos com àrees que necessiten millores.*" [4]

Llavors les escollides per l'entorn de proves són Nagios, Pandorafms i Zenoss sobretot per que cobreixen les necessitats per a gestionar xarxes i sistemes informàtics amb diferents sistemes per a recollir dades, maneguen la informació recol·lectada, la possibilitat d'incorporar agents i per ser les més descarregades. Totes tenen una versió comercial de baix cost però les proves i l'avaluació es fa sobre la versió Open Source.

- Nagios: va ser creat i encara el manté *Ethan Galstad,* es va convertir en l'estàndard, la comunitat és molt activa i és la més estesa. Es pot trobar informació a www.nagios.org.
- Pandorafms: desenvolupat per l'empresa espanyola Artica, en llenguatge *Perl*, fa servir els mecanismes estàndards i agents que tenen implementats mòduls per facilitar les ampliacions fetes per personal especialitzat. Es pot trobar informació a http://pandorafms.org.
- Zenoss: funciona sobre Linux o Windows sobre *VMWare Player*, permet la migració dels *pluggins* d'un sistema Nagios a Zenoss i en comptes d'agents remots fa servir SSH en els entorns Linux, SNMP i WMI als Windows. Es pot trobat informació a http://www.zenoss.com/.

[4] Enllaç de Gartner (cal validació)
http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&resId=1492516&ref=g_portalfromdoc&content=html
Enllaç d'HP accessible:
http://h30501.www3.hp.com/hpsws/attachments/hpsws/161/305/1/HP_vol3-art4.pdf

3.4. Característiques a valorar

Les característiques de les eines de monitorització s'han escollit segons la documentació trobada a Internet i s'han ampliat després de fer una enquesta a tècnics informàtics que han aportat la seva experiència.

3.4.1. Enquesta per a seleccionar i valorar les característiques d'una eina de monitorització

Per fer l'enquesta s'ha consultat a 5 persones que treballen com a informàtics, dels quals dos, FGR i JGC, gestionen eines de monitoratge i la resta són usuaris passius del producte o la relació és limita a rebre notificacions, informes i sol·licitud per a afegir dispositius. Als participants se'ls ha facilitat una relació inicial de característiques, en dues rondes han creat el llistat definitiu amb els aspectes més rellevants i al final han afegit un pes a cadascuna fins a repartir 100 punts segons la importància.

El resultat és una taula que consta d'una part on es descriu el perfil dels usuaris i un llistat dels aspectes a destacar d'una eina de supervisió amb el seu pes. Al final s'han retirat les característiques valorades com a zero i s'ha afegit una columna amb la ponderació dels pesos valorats a les característiques.

PERFIL (descripció de la persona que omple el formulari)					
Inicials del nom	JGC	JFM	MRS	JCM	FGR
Àrea de treball	Explotació	Xarxes	Sistemes	Sistemes i Plataformes	Explotació
Anys d'experiència	24	10	>5	6	13

CONCEPTE		**PUNTS**					**PES**
Característiques generals	Instal·lació	1	2	4	0	3	2,00%
	Manual i ajuda	2	9	6	5	8	6,00%
	Seguretat	9	5	6	8	5	6,60%
	Integració amb altres eines	1	6	2	10	6	5,00%
	Base de dades	6	6	5	0	3	4,00%
	Còpies de seguretat i restauració	2	5	4	0	4	3,00%
	Codi obert	1	2	2	0	2	1,40%
	Nivell d'ús	5	5	5	0	8	4,60%
	Personalització	2	8	6	0	5	4,20%
	Gestió SLA	2	1	5	5	6	3,80%
	Gestió de pressupostos	2	1	1	0	0	0,80%
	Gestió ITL	2	1	2	5	1	2,20%
	Instal·lar clients	0	0	1	2	4	1,40%
	Generació automatitzada d'informes	5	3	0	15	1	4,80%

Mecanismes per a recol·lectar la informació	Descobriment automàtic de dispositius	3	6	2	0	2	2,60%
	Detecció de caigudes	9	4	4	10	6	6,60%
	Programació de llindars	6	4	3	10	7	6,00%
	Correlació d'esdeveniments	8	4	7	5	2	5,20%
	Recepció d'esdeveniments	9	5	4	10	5	6,60%
	Prediccions	3	2	7	0	3	3,00%
	Accions automàtiques per esdeveniments	4	2	5	0	4	3,00%
	Eines per actuar als dispositius	5	2	5	0	2	2,80%
	Filtratge d'esdeveniments	2	4	6	5	7	4,80%
	Suportar IP, IPX,IPv6	4	4	6	0	4	3,60%
	Eines de suport a MIB	4	4	2	10	1	4,20%
	Inventari	3	5	0	0	1	1,80%

Taula 4 valoració característiques d'una eina de monitorització

Totes les característiques han obtingut una puntuació. Els aspectes més valorats són la seguretat, la notificació d'esdeveniments i la detecció de les caigudes, seguits per poder programar els llindars i la documentació. La pitjor puntuació ha estat per la gestió de pressupostos. La característica del "codi obert" que permet fer modificacions no l'hauríem de tenir en compte per que totes són eines Open Source, es manté com a característica per no modificar els punts que han assignat cada participant en l'enquesta i per que no afectarà al resultat final.

3.4.2. Característiques generals

- **Instal·lació**: si la documentació que ens proporciona el desenvolupador del producte és comprensible i ens permet fer la instal·lació sense problemes.
- **Manual i ajuda**: si la informació que dóna és complerta, comprensible i ens permet resoldre els entrebancs sorgits durant la configuració per les proves.
- **Seguretat**: es tindrà en compte els apartats:
  - Mètodes d'accés segur: es valorarà si implementa sistemes segurs per l'accés a l'eina, a la base de dades i per la comunicació amb els dispositius a monitoritzar. També si es recomana o si s'obliga a utilitzar normes per a millorar les claus d'accés, per exemple barrejar números i lletres, fer servir majúscules,.. .
  - Possibilitat d'auditories: si permet fer un seguiment posterior de les accions dels usuaris.
- **Integració amb altres eines**: si té o permet incorporar altres eines, la senzillesa per manegar-les i el nivell d'integració, el que suposaria gestionar-les des de l'eina de monitorització i aprofitar les funcionalitats i les dades que obté, com per exemple integrar l'eina Cacti per extreure la informació consultada per les seves gràfiques.
- **Base de dades**: identifica el tipus de base de dades, si és gestionada des de l'eina o externament i si és estàndard per integrar-la amb altres sistemes.
- **Còpies de seguretat i restauració**: si disposa d'un sistema per a fer les còpies de seguretat de les dades i per recuperar-les.
- **Codi obert**: poder modificar el codi del programari per adaptar-lo a les nostres necessitats.

- **Nivell d'ús**: la usabilitat, si és intuïtiva i les funcions bàsiques són accessibles.
- **Personalització**: si l'eina es pot adaptar per cada usuari o a cada entorn de treball.
- **Gestió SLA**: si permet o no la gestió de SLA automàticament.
- **Gestió de pressupostos**: si disposa d'eines per fer control i seguiment de la gestió financera.
- **Gestió ITIL**: si els informes ajuden a seguir la normativa ITIL.
- **Instal·lació de client**: si cal un programari en el dispositiu a supervisar per a obtenir les dades.
- **Generació automàtica d'informes**: si podem programar informes per a ser generats i enviats a uns destinataris concrets automàticament.

3.4.3. Mecanismes per a recol·lectar la informació

- **Descobriment automàtic de dispositius**: si permet funcions per descobrir automàticament els elements amb connectivitat IP.
- **Detecció de caigudes**: si detecta la pèrdua de connexió amb els dispositius, és habitual fer servir el protocol ICMP. També es valorarà si permet la detecció d'alertes complexes o en cascada des d'un dispositiu principal, com per exemple detectar que si l'encaminador d'una xarxa cau els dispositius que estiguin connectats darrere no donin alarmes.
- **Programació de llindars**: si permet la programació de llindars pels diferents estats de les alarmes que generin accions com l'enviament d'avisos remotes i locals.
- **Recepció d'esdeveniments**: si permet al recepció d'esdeveniments o alarmes des del dispositius remots en el moment que es produeixen. S'ha de diferenciar que una l'alarma es detecta al fer la consulta però existeix la possibilitat de rebre un avís en el moment que es detecta des del dispositiu supervisat.
- **Prediccions**: pot analitzar el comportament d'una consulta després d'un temps i generar una línia base per poder predir una possible alarma segons el valor de la consulta d'un instant.
- **Accions automàtiques per esdeveniments**: si permet executar accions al detectar un esdeveniment, com per exemple si es detecta un ús excessiu de la sortida a Internet fer la captura del tràfic de la interfície de sortida de l'encaminador.
- **Eines per actuar als dispositius** : si disposa d'eines integrades de configuració de dispositius remots.
- **Correlació d'esdeveniments**: si permet fer correlació d'esdeveniments per fer el seguiment de problemes complexes, per exemple es podria crear una regla per detectar la caiguda de la web publicada a Internet i si després hi ha intents d'accés a la BBDD es podria generar una alerta per possible intent d'accés.
- **Filtratge d'esdeveniments**: si té eines de filtratge o cerca per a trobar alarmes que facilitin el seguiment de les incidències.
- **Suportar IP, IPX i IPv6**: si suporta altres protocols, inclòs el protocol IPv6.
- **Eines de suport a MIB**: si disposa de mecanismes per facilitar la interpretació de les MIB.

- **Inventari**: si pot extreure un inventari d'equips connectats i de les seves configuracions.

4. Entorn de proves

Amb l'entorn de proves es validarà les característiques de les eines Open Source Nagios, Pandorafms i Zenoss.

4.1. Maqueta de proves

Per a fer les proves s'ha preparat una maqueta amb els següents recursos disponibles:

- Portàtil: Intel Core2 T5500 1,66Ghz i 4Gb amb Ubuntu 10.10 Server Edition.
- Portàtil: Intel Core2 P8600 2,4Ghz i 4 Gb amb Ubuntu 10.10 Server Edition.
- Ordinador sobretaula: Intel Pentium (R) D 3,4Ghz i 2Gb amb Windows 7 Ultimate.
- Router Zyxel amb port ADSL, 4 ports ethernet i WIFI.
- Adreces d'Internet: per consultes HTTP www.gmx.com, www.badalona.org i www.Cwazy.net per a consultes HTTP, SNMP i POP3.

4.2. Nagios

Per aquesta prova s'ha utilitzat les següents versions:

- Nagios Core 3.2.3,
- versió de plugin del servidor 1.4.15,
- plugin per a sistema operatiu Windows nsclient 201
- plugin per a sistema operatiu Linux nrpe 212

4.2.1. Eina de monitorització

Iniciat al 1999 per Ethan Galstad, qui va crear la comanda de MSDOS *ping,* va canviar el nom de Netsaint a projecte Nagios al 2002 i avui la versió *Open Source* s'anomena Nagios Core i la versió comercial Nagios Fusion. El projecte Nagios és l'eina de codi font obert o *Open Source* més popular per a la monitorització de sistemes informàtics. És un sistema estable, escalable i extensible, que permet la supervisió de qualsevol dispositiu connectat a la xarxa.

Tenim la possibilitat d'escollir que el servidor treballi en els sistemes operatius Windows o Linux i de fer les consultes als dispositius remots. Utilitza agents remots (fa servir NSClient ++ per a entorns Windows i NRPE per a Linux), SNMP, WMI per a Windows i els protocols de TCP/IP. Així, pot controlar host amb diferents sistemes operatius (Sistemes Windows, Sistemas Linux/Unix, Sistemes MAC/OS), dispositius

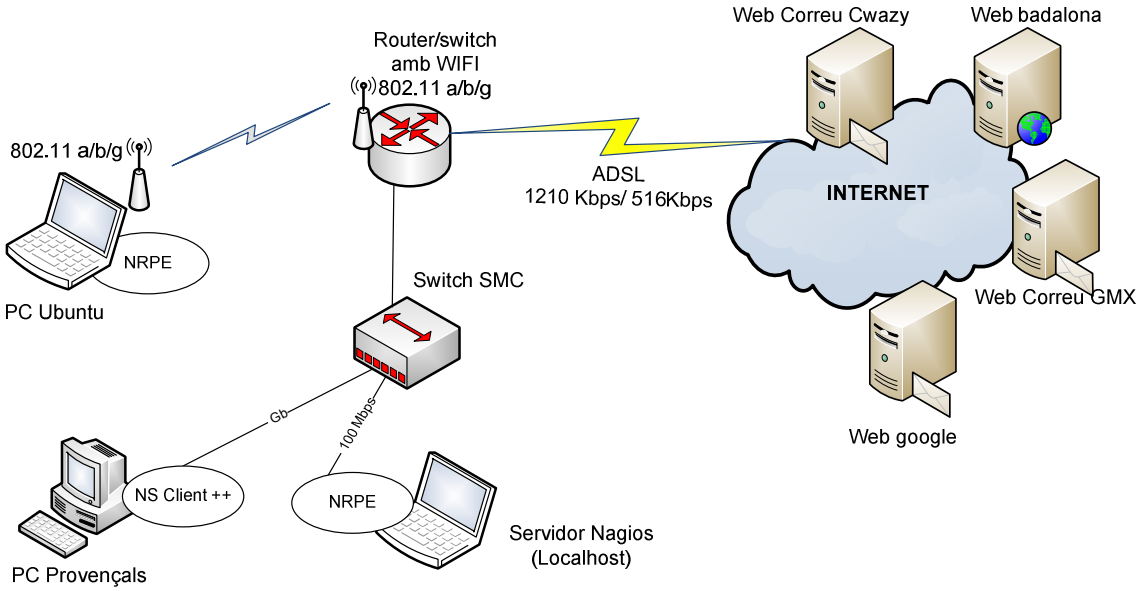
de xarxa com encaminadors o commutadors, elements de seguretat com tallafocs, aplicacions, serveis com SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH i d'altres equips connectat a la xarxa com impressores o càmeres.

A l'utilitzar la consola veiem el potencial que dóna la comunitat amb informació i moltes d'aplicacions per afegir a Nagios, però també ens fixem que la configuració de l'eina és amb fitxers de text, les pantalles web són poc atractives i manquen estadístiques més atractives visualment, amb gràfics.

S'han pogut fer totes les proves que permet l'eina i només a l'instal·lar una programari addicional per a facilitar la gestió de la configuració s'ha perdut la gestió de l'eina, pel que s'ha tornat a instal·lar la còpia del programari.

4.2.2. Descripció de l'entorn de proves

Per aquesta avaluació s'han fet servir tres ordinadors, un encaminador o router i la xarxa Internet per a accedir a quatre servidors web, l'esquema és el següent:



Il·lustració 6 esquema de l'entorn de proves de Nagios

4.2.3. Tasques fetes per la preparació de l'entorn de proves

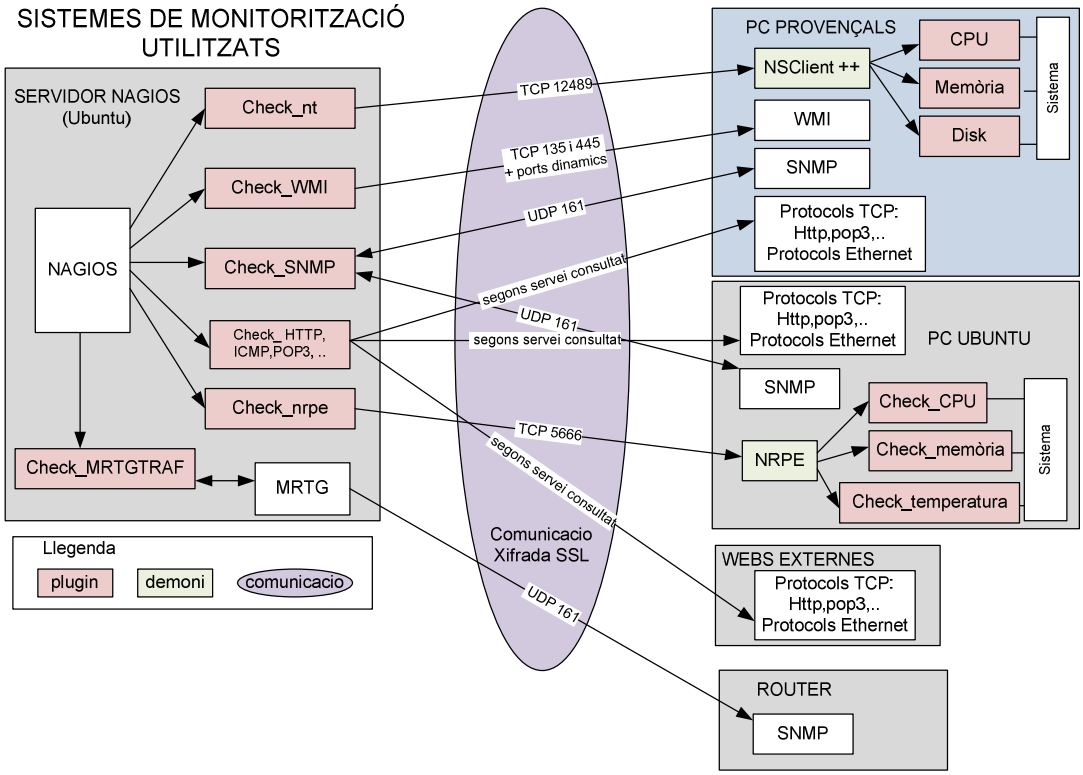
4.2.3.1. Configuracions als equips

- Al Servidor Nagios s'ha instal·lat la part servidor del programari, un client de NRPE per a Linux i s'ha afegit els següents mòduls: snmpd per rebre els traps, Postfix per l'enviament de correu, SSH per la connexió als dispositius, PHP com a llenguatge de programació, la llibreria gd2 per crear els gràfics i Apache2 per la interfície web. La base de dades MySQL i Perl estan integrats i s'instal·len amb el servidor Nagios. El programari MRTG s'ha instal·lat per les consultes dels interfícies de l'encaminador.

- Al PC Ubuntu amb sistema operatiu Linux s'ha instal·lat SNMP, SSH i SSL per la connexió amb el servidor.
- Al PC Provençals amb Windows 7 s'ha activat el protocol SNMP amb una clau o *community*, s'ha donat permisos a WMI de lectura al servidor Nagios i s'ha configurat el tallafoc per a permetre les comunicacions amb l'adreça IP del servidor Nagios, ja que és difícil de determinar els ports necessaris.
- Al router s'ha configurat SNMP amb la *community* i la IP on enviar els traps.

4.2.3.2. Definició dels sistemes de monitorització

La comunicació entre el servidor i els dispositius a monitoritzar fa servir el següent esquema[5]:



Il·lustració 7 esquema de comunicacions de Nagios

S'han creat les comandes al servidor i agents:

- A traves de l'agent per a Windows NSC, al PC Provençals es consulta el temps que porta encesa l'ordinador, anomenat Uptime. S'ha habilitat WMI per a comprovar si el procés del firewall "MsPgEng.exe" està actiu i per validar la comunicació s'ha consultat la configuració local amb l'eina "WMI explorer". S'ha activat SNMP v2 amb clau per poder llegir les variables.
- S'ha instal·lat l'agent Linux NRPE, en el Servidor Nagios i PC Ubuntu i a traves d'aquest s'ha programat la consulta de la temperatura de la CPU, l'ocupació de la memòria i de les unitats de discos.

[5] Extretes de les dades de http://nagios.sourceforge.net/docs/3_0/quickstart.html

- S'ha activat el protocol SNMP a l'encaminador per a consultar el temps des de que està funcionant i per fer consultes amb l'eina MRTG que està instal·lada al servidor.
- A les webs externes s'utilitzen eines TCP/IP: ICMP, HTTP, POP3, ..
    1. ICMP a totes les màquines
    2. HTTP a les 4 webs
    3. POP3 i IMAP a Web Cwazy

En totes les consultes s'han definit diferents llindars d'alertes per a identificar els diferents estats (ok, warning i critical) i, en cas de produir-se una alerta de nivell warning o critical s'envia una notificació per correu electrònic.

Com a recolzament s'ha utilitzat les eines "MIB tools" i "snmpwalk" per a extreure abans de tot les dades del dispositiu.

4.2.3.3. Configuració de l'eina

Fitxers de configuració:

L'eina es basa en una estructura de fitxers per la configuració del sistema, ubicats al directori /usr/local/nagios/etc/objects, així hem modificat els següents fitxers:

- Nagios.cfg: és el fitxer base on es configura els paràmetres genèrics de l'eina i inclou les crides a la resta de fitxers. S'ha afegit els enllaços a dos fitxers nous d'objectes o *hosts* per les webs i pel PC Ubuntu amb Linux.
- WebExternes.cfg: per definir els objectes consultats per Internet i quins paràmetres són supervisats remotament.
- Linux.cfg: per definir l'objecte Linux, PC Ubuntu, i s'ha afegit una imatge amb format .png pel host.
- Switch.cfg: té la definició de l'encaminador de la prova i s'han afegit les consultes per SNMP i a l'eina MRGT.
- Contacts.cfg: per definir diferents usuaris per a accedir i els seus paràmetres: nom, adreça, el correu electrònic per rebre les alarmes,... . Hem creat els usuaris nagiosadmin, administrador1 i administrador2 per a provar la personalització de l'eina.
- Commands.cfg: es defineixen els scripts, els plugins, les comandes externes,.. per a fer les consultes als dispositius remots. Hem fet servir check_nrpe per l'agent de windows, check_wmi per les consultes WMI a Windows, check_nt per les consultes a l'agent Linux, check_mrgt per integrar l'eina MRTG i fer consultes a l'encaminador, ...
- Timeperiods.cfg: per indicar els horaris i dies que és fa la monitorització i les notificacions per alertes, també es defineix els dies festius, .. . Nosaltres hem fet servir un període de temps de 24h pels 7 dies de la setmana (24x7).
- Templates.cfg: per definir les plantilles dels objectes, contactes i dels serveis que faciliten la configuració de nous elements a Nagios. Hem afegit les plantilles "windows" pel PC Provençals i els *templates* "web" i "web_services" pels objectes que es consulten a través d'Internet (GMX, Cwazy, Google i Badalona).

Dispositius remots:

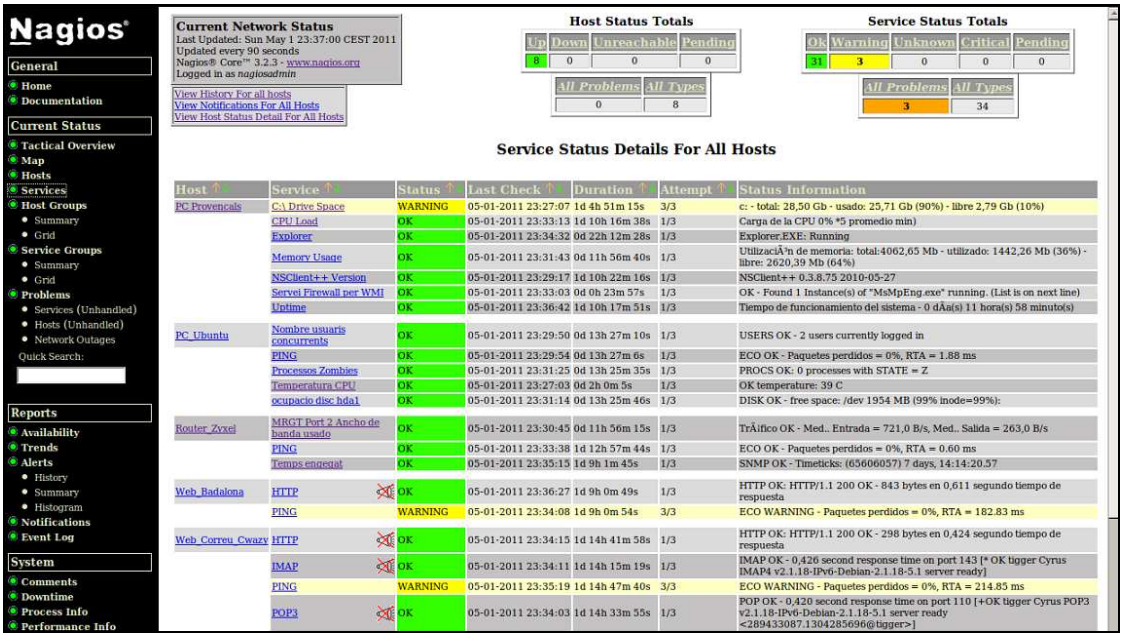
- Al PC Ubuntu amb sistema operatiu Linux s'ha instal·lat i configurat l'agent NRPE com a dimoni i SSL per fer segura la connexió amb el servidor.
- Al PC Provençals s'ha instal·lat i configurat l'agent NSClient++.

4.2.3.4. Plugins

S'ha fet servir els plugins: check_ping, check_http, chek_pop3, check_snmp, check_users, etc... Per la seva importància destaquen:

- check_mrtgtraf: monitoritza els fitxers generats per l'eina MRTG que fa consultes per SNMP a un dispositiu i per extreure dades de CPU, tràfic, memòria,... i presenta aquesta informació en gràfiques. En aquest cas es comprova el tràfic de les interfícies del router.
- check_nrpe: fa la consulta remotament a NRPE i aquest executa la consulta local. NRPE gestiona la comunicació entre els dos equips i les dades són extretes pels plugins per una consultes locals, com seria la consulta dels usuaris connectats amb check_users o a dispositius remots com si fos un equip intermediari. Llavors són les mateixes consultes que es poden utilitzar des del servidor Nagios.
- check_nt: funciona igual que l'anterior i consulta la informació que l'agent NSClient++ ha extret d'un dispositiu Windows.
- Check_temperatura: que s'ha desenvolupat per aquest projecte i fa la consulta de la temperatura del portàtil amb Ubuntu, informació que dóna l'API ACPI en equips HP.

En les imatges es pot veure dos visions de tots els dispositius amb els seus plugins i on es veu els avisos pel disc del PC Provençals que té un percentatge d'ocupació molt alt i la latència de dos webs externes que superen el llindar de 100 ms en la resposta, la mateixa consulta en altres dispositius no genera l'estat Warning per que donen un temps inferior. També és rellevant el resum de les alarmes dels equips i dels serveis i el camp "*Status information*" que dóna el valor de la resposta i l'estat.



Il·lustració 8 llistat de consultes a l'entorn de proves

4.2.3.5. Estats

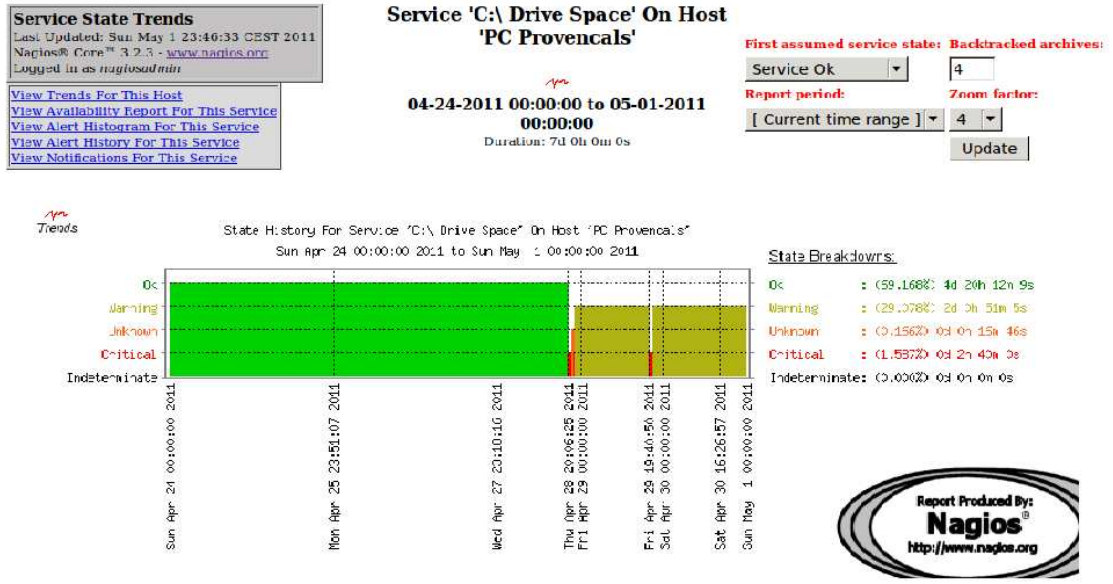
Els dispositius supervisats poden estar en diferents estats per a cada consulta que és faci: Up si està connectat, Down si està caigut, unreachable si està connectat però no podem fer-li consultes i Pending quan estem esperant fer la primera consulta després d'una configuració.

Els serveis tenen un comportament similar i poden estar: Up, Critical o Warning segons els llindars definits a la consulta per l'usuari, Unreachable i Pending

4.2.3.6. Elaboració d'informes

Per a cada host, servei o agrupació d'ells, Nagios pot generar informes, gràfics, històrics de disponibilitat, alertes o notificacions durant un període de temps.

L'informe de disponibilitat del disc dur PC Provençals indica en quin moment ha hagut els canvis d'estat produïts, ja que ha estat sense connectivitat dues hora i per la variació de l'ocupació que ha creat alarmes de *Warning* que estan indicades en color verd oliva.

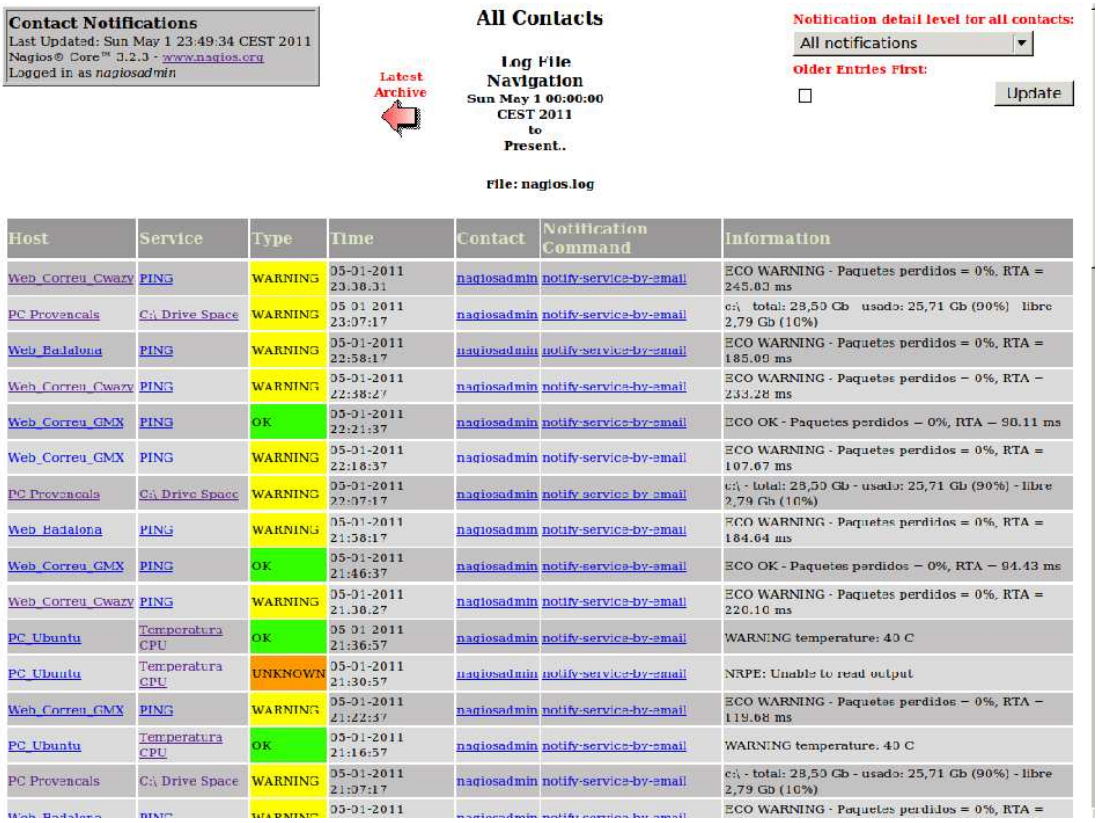


Il·lustració 9 informe de disponibilitat del disc dur

4.2.3.7. Notificacions

S'ha configurat que qualsevol alerta es generi un correu electrònic al responsable per a indicar el canvi d'estat. Els missatges indiquen aquests estats i poden ser: Critical si està caigut, unreachable, Recovery (OK) quan es recupera la connexió o Flapping quan els valors consultats canvien de valor, aquest estat ha d'estar configurat al definir el dispositiu.

L'eina permet generar un informe de les notificacions com el d'aquesta imatge, es pot veure les dades de l'equip, el servei afectat, l'hora, a qui s'avisa i les dades de la consulta que han motivat aquesta notificació.



Contact Notifications
Last Updated: Sun May 1 23:49:34 CEST 2011
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as *nagiosadmin*

All Contacts

Latest Archive

Log File Navigation
Sun May 1 00:00:00 CEST 2011 to Present..

File: nagios.log

Notification detail level for all contacts: All notifications
Older Entries First: ☐ Update

Host	Service	Type	Time	Contact	Notification Command	Information
Web_Correu_Cwazy	PING	WARNING	05-01-2011 23:38:31	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA = 245.03 ms
PC Provencals	C:\ Drive Space	WARNING	05-01-2011 23:07:17	nagiosadmin	notify-service-by-email	c:\ total: 28,50 Gb usado: 25,71 Gb (90%) libre 2,79 Gb (10%)
Web_Badalona	PING	WARNING	05-01-2011 22:58:17	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA = 185.09 ms
Web_Correu_Cwazy	PING	WARNING	05-01-2011 22:38:27	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA = 233.28 ms
Web_Correu_GMX	PING	OK	05-01-2011 22:21:37	nagiosadmin	notify-service-by-email	ECO OK - Paquetes perdidos = 0%, RTA = 90.11 ms
Web_Correu_GMX	PING	WARNING	05-01-2011 22:18:37	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA = 107.07 ms
PC Provencals	C:\ Drive Space	WARNING	05-01-2011 22:07:17	nagiosadmin	notify-service-by-email	c:\ - total: 28,50 Gb - usado: 25,71 Gb (90%) - libre 2,79 Gb (10%)
Web_Badalona	PING	WARNING	05-01-2011 21:58:17	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA = 184.64 ms
Web_Correu_GMX	PING	OK	05-01-2011 21:46:37	nagiosadmin	notify-service-by-email	ECO OK - Paquetes perdidos = 0%, RTA = 94.43 ms
Web_Correu_Cwazy	PING	WARNING	05-01-2011 21:38:27	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA = 220.10 ms
PC_Ubuntu	Temperatura CPU	OK	05-01-2011 21:36:57	nagiosadmin	notify-service-by-email	WARNING temperature: 40 C
PC_Ubuntu	Temperatura CPU	UNKNOWN	05-01-2011 21:30:57	nagiosadmin	notify-service-by-email	NRPE: Unable to read output
Web_Correu_GMX	PING	WARNING	05-01-2011 21:22:37	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA = 119.68 ms
PC_Ubuntu	Temperatura CPU	OK	05-01-2011 21:16:57	nagiosadmin	notify-service-by-email	WARNING temperature: 40 C
PC Provencals	C:\ Drive Space	WARNING	05-01-2011 21:07:17	nagiosadmin	notify-service-by-email	c:\ - total: 28,50 Gb - usado: 25,71 Gb (90%) - libre 2,79 Gb (10%)
Web_Badalona	PING	WARNING	05-01-2011	nagiosadmin	notify-service-by-email	ECO WARNING - Paquetes perdidos = 0%, RTA =

Il·lustració 10 informe amb les notificacions enviades per correu

4.2.3.8. Funcionalitats ampliables

La comunitat del projecte Nagios ofereix un ampli assortiment de plugins i addons que complementen les seves funcionalitats, entre els que destaquem:

- gestió de SLA amb el plugin check_csl o amb un addon NetMySLA
- entorn gràfic per simplificar la gestió amb addon com Centreon, Nagios QL o NagVis
- incorporar eines per la gestió dels dispositius supervisats amb addons nmap2nagios, ScanToNag
- clúster de servidors Nagios amb NDOUtils
- instal·lar un client de Nagios a un Iphone, s'anomena INag
- consultar la llista *blacklist* d'un proveïdor de serveis antiSpam o filtre antiinundació amb el plugin check_rdl, també estan disponibles plugins per fer consultes a bases de dades com Oracle, als equips que formen una xarxa SAN amb connexions *fiberchannels* dels fabricants Broacade o EMC,... .

4.2.4. Desenvolupament d'agents

S'han fet tres agents: per controlar la temperatura de la CPU d'un equip Linux, controlar el servei Firewall d'un equip Windows i integrar l'eina MRTG per a controlar per SNMP la interfície ADSL d'un encaminador.

4.2.4.1. Plugin Temperatura

FITXER LINUX.CFG (en Servidor Nagios)

```
define service{
        use                     generic-service; plantilla utilitzada pel servei
        host_name               PC_Ubuntu; nom del host que s'aplica
        service_description     Temperatura CPU; descripció del servei
        check_command           check_nrpe!check_temp; consulta per cridar a NRPE del dispositiu Linux i executar la comanda check_hda1 (per a veure l'espai en disc)
}
```

FITXER NRPE.CFG (en PC Ubuntu)

```
command[check_temp]=/usr/local/nagios/libexec/check_temperatura -w 60 -c 80; ubicació del fitxer executable i els llindars de la consulta check_temperatura
```

FITXER CHECK_TEMPERATURA.SH (en PC Ubuntu)

```
# S'ha d'instal·lar ACPI per identificar les característiques físiques de l'ordinador

#!/usr/bin/perl; identifica el fitxer com a script fet en Perl

use strict;

my $STATE_WARNING= $ARGV[1];  pas per paràmetres del llindar
my $STATE_CRITICAL=$ARGV[3]; pas per paràmetres del llindar
my $STATE_UNKNOWN=0; defineix llindar  per detectar errors

my $VALOR = ""; inicialització de les variables
my $TEMP = 0;
my $VALOR_TEMP = "";

$VALOR_TEMP = `cat /proc/acpi/thermal_zone/CPUZ/temperature | awk '{ print $2 }'`; es guarda en una variable la temperatura (el format és: temperatura xx C)
$TEMP = substr($VALOR_TEMP,12); s'identifica el valor XX
$TEMP = int($TEMP||0); es converteix en numèric
if ($TEMP >= $STATE_CRITICAL) {$VALOR = "CRITICAL " . $VALOR_TEMP; }
  elsif ($TEMP >= $STATE_WARNING) { $VALOR = "WARNING " . $VALOR_TEMP; }
  elsif ($TEMP == 0) {$VALOR = "ERROR " . $VALOR_TEMP;}
        else  {$VALOR = "OK " . $VALOR_TEMP;} ;s'identifica entre quins llindars està i es genera la sortida

print $VALOR; s'imprimeix, només serveis per fer un seguiment des de la línia de comandes
exit($VALOR) ; retorna el resultat
```

4.2.4.2. Plugin WMI Servei Firewall

FITXER WINDOWS.CFG (en Servidor Nagios)

```
define service{
        use                     generic-service; plantilla utilitzada pel servei
        host_name               PC Provencals; nom del host que s'aplica
        service_description     Servei Firewall per WMI; descripció del servei
```

check_command
check_wmi_proces!provençals!coyote!MsMpEng.exe; comanda per WMI passant els paràmetres de usuari/clau per a consultar si el procés del Firewall de Windows està actiu
}

FITXER COMMANDS.CFG (en Servidor Nagios)
define command{
command_name check_wmi_proces ; nom de la comanda
command_line $USER1$/check_wmi_plus -H $HOSTADDRESS$ -u $ARG1$ -p $ARG2$ -m checkprocess -a $ARG3$; comanda amb els paràmetres –H adreça, -u usuari amb drets per llegir WMI –p clau –m nom de la comanda (WMI_plus té altres comandes implementades) –a nom del procés
}

4.2.4.3. Plugin amb consulta MRTG

FITXER SWITCH.CFG
define service{
use senseflap-service ; deshabilita el flapping
host_name Router_Zyxel ; nom encaminador
service_description MRGT Port 2 Ample de banda utilitzat; descripció del servei
check_command
check_local_mrtgtraf!/var/www/mrtg/192.168.1.1_2.log!AVG!1000000,1000000!5000000,5000000!10 ; consulta per llegir els valors de MRTG que ha generat un fitxer del port 2 del router 192.168.11. (192.168.1.1_2), que obté el valor mig (AVG), els llindars són 10Mb per a Warning i 50Mb per a Critical i si en 10 minuts no s'ha actualitzat les dades genera una alarma Critical
}

FITXER COMMANDS.CFG
define command{
command_name check_local_mrtgtraf ; nom de la comanda
command_line $USER1$/check_mrtgtraf -F $ARG1$ -a $ARG2$ -w $ARG3$ -c $ARG4$ -e $ARG5$; comanda amb els paràmetres –F ubicació del fitxer, -a valor a llegir –w llindra per considerar l'alarma Warning –c llindar per considerar l'alarma Critica –e temps sense modificar el fitxer
}

4.2.5. Comparativa

S'han agrupat en característiques generals i les relacionades amb els mètodes de monitorització.

4.2.5.1. Característiques general

- **Instal·lació**: amb la documentació de la web és pot instal·lar tant el servidor com l'agent per a Linux i Windows sense problemes.
- **Manual i ajuda**: està molt accessible des de la plana web oficial i des de l'eina. Les ajudes són senzilles i estan esteses per totes els apartats de l'eina, al visualitzar el mapa podem veure els icones de cada dispositiu supervisat i al situar-nos sobre la icona podem veure les dades necessàries

per saber l'estat de l'equip i les seves característiques. La informació es pot descarregar a http://www.nagios.org/documentation.

- **Seguretat**: totes les claus no tenen cap recomanació. BBDD només permet posar una clau a l'usuari administrador i és accessible des de fora de l'eina. Per l'accés al programari es poden crear perfils amb permisos diferents, el que permet limitar l'accés a certes funcionalitats segons l'usuari. Les modificacions dels administradors no queden registrades sinó fas servir una eina gràfica per a gestionar Nagios. La comunicació des del servidor fins l'agent es fa servir el protocol SSL que es considerat segur.
- **Integració amb altres eines**: no disposa de cap funcionalitat implementada però existeix addons per incorporar-les, per exemple nmap2nagios i ScanToNag.
- **Base de dades**: només pot ser MySQL i no permet cap gestió afegida a les permeses per una BBDD, per obtenir més funcionalitats es pot carregar l'addon NDOUtils per a manegar les dades i integrar-la amb altres programaris.
- **Còpies de seguretat i restauració**: no disposa de cap funcionalitat per poder fer una còpia de seguretat, encara que només caldria fer-la dels fitxer de configuració.
- **Codi obert**: s'ofereix amb llicència *Open Source* que permet modificar el programari.
- **Nivell d'ús**: la configuració és complicada per que es fa per comandes que s'afegeixen a diferents fitxers, encara que és possible afegir una interfície web per facilitar-la.
  Dins del sistema la interfície web és fàcil de manegar, intuïtiva i té totes les funcionalitats ubicades en el lateral esquerra, que es manté en totes les pantalles. La plana inicial, *Tactical Overview,* dóna un resum de l'estat actual de tots els serveis i equips, el nombre d'alertes segons els nivells i s'identifiquen en colors diferents per veure d'un cop d'ull l'estat general. Aquesta característica es troba a la resta del sistema, els colors verd, groc o vermell com a element visual per identificar amb rapidesa com està l'equip o el servei. Les estadístiques estan basades en taules de dades i són poc visuals.
- **Personalització**: és poc adaptable a cada usuari ja que només es pot modificar la pàgina inicial, afegir mapes aportats per l'usuari, que inclou la utilització de Googlemaps i es pot modificar els icones dels elements supervisats. Els informes es poden configurar pel temps a visualitzar però estan restringits a les opcions que ens proporciona l'eina.
- **Gestió SLA**: es pot gestionar els SLA amb un plugin (check_csl).
- **Gestió ITL**: té un addon per a registrar els temps d'una incidència segons les definicions d'ITIL per facilitar el seguiment.
- **Gestió de pressupostos**: no té cap referència.
- **Instal·lació de client**: per a poder consultar detalls de l'equipament fa falta instal·lar agents en els ordinadors.
- **Generació automàtica d'informes**: no ho permet, cal generar-los en el mateix moment per l'usuari i enviar-los als destinataris.

4.2.5.2. Mecanismes per a recol·lectar la informació

- **Descobriment automàtic de dispositius**: només la versió comercial disposa d'una eina per fer la cerca automàtica d'equips.

- **Detecció de caigudes**: té definit com a funcionalitat bàsica "Host Alive" per saber si el dispositiu està connectat a la xarxa. A la plana *Hosts* podem veure per cada equip l'estat, l'hora de la última i la següent comprovació, el retorn de la consulta i accedir a tota la informació. No detecta caigudes complexes.
- **Programació de llindars**: cada comanda permet la configuració de dos llindars per a delimitar els tres nivells d'alarmes (OK, Warning i Critical) i el nombre de repeticions de la consulta abans de indicar aquest nivell. Les alarmes poden executar l'enviament SMS, de correu electrònic o una identificació visual o sonora en la mateixa aplicació.
- **Recepció d'esdeveniments**: per poder rebre els traps i interpretar-los cal un addon específic anomenat NSCA.
- **Prediccions**: no ofereix aquesta funcionalitat.
- **Accions automàtiques per esdeveniments**: no permet iniciar cap acció.
- **Eines per actuar als dispositius** : no té cap eina integrada.
- **Correlació d'esdeveniments**: l'eina pot carregar l'addon per configurar *Splunk*, com a eina de correlació d'esdeveniments, s'encarrega de recollir tots els registres i permet crear patrons per a trobar coincidències.
- **Filtratge d'esdeveniments**: permet classificar i filtrar esdeveniments per diferents paràmetres.
- **Suportar IP, IPX oIPv6**: està preparat per a treballar amb IPv6 i no suporta IPX.
- **Eines de suport a MIB**: es poden integrar eines de Linux com "snmpwalk" però no ofereix cap ajuda des del seu sistema.
- **Inventari**: només es pot fer inventari amb la versió Nagios Enterprise.

4.3. Pandorafms

Per aquesta prova s'ha utilitzat la versió de Pandorafms 3.2.1 i els plugins de Windows i Linux versió 3.2.1. A l'entorn de proves s'ha fet servir la versió més estable encara que el manual oficial de Pandorafms és d'una altre versió http://www.openideas.info/wiki/index.php?title=Pandora_3.0:Documentation.

4.3.1. Eina de monitorització

Pandora FMS és un projecte del 2003, liderat per l'empresa Artica, que ofereix una versió Open Source i una comercial Enterprise, per a consultar les funcionalitats del sistema de monitorització i les diferències entre la versió Open Source i comercial es poden consultar a http://pandorafms.com/index.php?sec=pandora&sec2=features&lng=es. Entre les característiques que van motivar el projecte destaquen que és codi lliure, distribuït, escalable i extensible, els mètodes de supervisió i la facilitat en l'ús.

El motor del sistema s'implementa en servidors independents per controlar diferents funcionalitats i poden instal·lar-se en una màquina o en diferents, aquest disseny facilita l'escalabilitat i les aplicacions de millores. Els mètodes per monitoritzar són: agents que recullen dades localment per a enviar-les al servidor i són específics per als diferents sistemes operatius (Linux, AIX, SUN Solaris, HP-UX, BSD / IPSO de Nokia i de Windows 2000 fins a Windows 7); el protocol SNMP

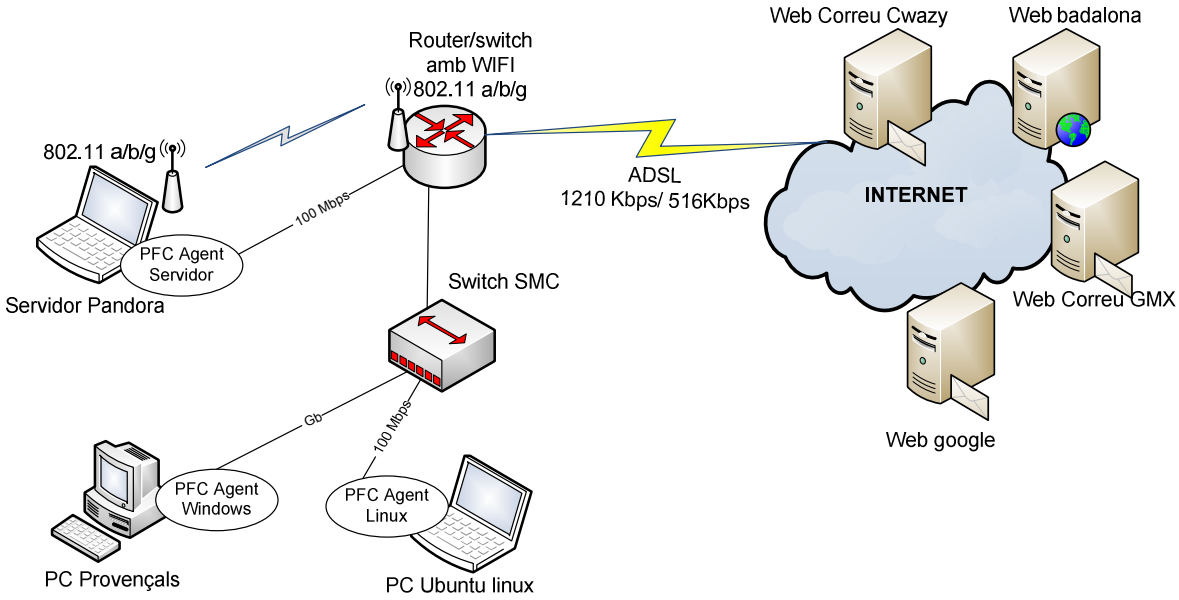
permet recol·lectar dades en remot o rebre els traps des dels dispositius a supervisar; eines basades en TCP/IP per a monitoritzar els elements dels sistemes, com balancejadors de càrrega, encaminadors, commutadors, sistemes operatius, aplicacions, ordinadors o impressores; i el desenvolupador ofereix la possibilitat d'incorporar agents físics d'altres fabricants per a supervisar paràmetres externs, com són la temperatura d'una sala d'ordinadors o un detector d'obertura de portes.

De la consola destaca les possibilitat per agrupar els equips supervisats segons els criteris definits pels gestors, la representació dels dispositius amb les seves connexions gràficament per que sigui més comprensible pels administradors (connectar dos encaminadors entre si i darrera de cadascun estan les seves xarxes), incorporar l'accés a utilitats com VNC o SSH, incorporar un servidor per rebre els traps d'SNMP i la incorporació de les dades consultades a les gràfiques. Aquestes últimes s'utilitzen per a generar informes, fer el seguiment de les incidències, obtenir la disponibilitat d'equips o serveis i presentar l'evolució dels SLA, el rendiment, errors i alertes. Els informes d'incidències reflecteixen la normativa ITIL v3 en la descripció dels temps, els estats i dels conceptes.

Durant les proves no s'ha pogut fer ús de WMI remotament per problemes de incompatibilitat de la comanda *wmic* que incorpora Pandorafms amb Windows 7, alguns canvis s'han actualitzat correctament després de reiniciar l'ordinador, el servidor de prediccions i alguns dels mòduls oficials no funcionaven, encara que la documentació ha ajudat molt a fer la instal·lació i a resoldre altres problemes. S'ha produït major lentitud a l'eina després de carregar el Googlemaps però sense cap pèrdua de servei. Les notificacions per correu no han funcionat per que necessitaven d'una compte a un servidor de correu que no teníem, però al registre es veia els tràfic rebutjat.

4.3.2. Descripció de l'entorn de proves

Per aquesta avaluació s'han fet servir tres ordinadors, un encaminador o router i quatre servidors web, l'esquema és el següent:



Il·lustració 11 esquema de l'entorn de proves de Pandorafms

4.3.3. Tasques fetes per la preparació de l'entorn de proves

4.3.3.1. Configuracions als equips

- El servidor es comunica per una connexió amb o sense fils sense cap problema. S'ha instal·lat tots els servidors del sistema Pandorafms, un client de pandora i s'ha afegit els següents mòduls a l'Ubuntu Server per a fer servir les eines del sistema: MySQL com a base de dades, snmpd per rebre els traps, xprobe per a rebre informació pel protocol ICMP, Postfix per enviar correu, SSH per a connectar-nos als dispositius i Tentacle i SSL per la comunicació entre el Servidor i els agents.
- Al PC Provençals amb Windows 7 s'ha instal·lat i configurat l'agent, s'ha activat el protocol SNMP amb una clau o community, s'ha donat permisos a WMI de lectura a l'agent i al Servidor Pandora i s'ha configurat al Firewall per a permetre les comunicacions d'entrada i sortida amb Pandora.
- Al router s'ha configurat SNMP amb la community i l'IP on enviar els traps.
- Al PC Ubuntu i al Servidor Pandora s'ha instal·lat i configurat l'agent linux amb el protocol SSL i Tentacle i, també, s'ha activat el protocol SNMP amb la clau i la configuració dels traps.

4.3.3.2. Definició de sistemes de monitorització

S'han creat els diferents agents amb els seus mòduls, segons la terminologia de Pandora:

- Consultes amb eines TCP/IP: ICMP, HTTP, POP3, ..
  - ICMP a totes les màquines
  - HTTP a les 4 webs
  - POP3 a Web correu Cwazy
- Consultes amb SNMP a router i PC Provençals (Windows). S'ha fet servir les eines "MIB tools" i "snmpwalk" per a extreure a l'inici les dades o OID del dispositiu a supervisar.
- El sistema ofereix agents per diferents sistemes operatius que s'han d'instal·lar en l'equip a supervisar, incorporen mòduls per a fer diferents consultes locals o remotes. En aquest cas hem fet servir l'agent Windows i Linux (en Servidor Pandora i PC Ubuntu), llavors en total s'han desplegat 3 agents: s'han descarregat les darreres versions, programat i afegit noves funcionalitats, que es descriuen més endavant.
- Per validar localment la configuració WMI del PC Provençals s'ha instal·lat l'eina "WMI explorer"[6] en el mateix ordinador i l'eina "wmic" al servidor Pandora per les comprovacions remotes. Per problemes d'incompatibilitat de versions s'ha abandonat aquest mecanisme de monitorització.

4.3.3.3. Configuració de l'eina

Entre les tasques més significatives:

- Per a simplificar la tasca de la gestió d'altes de dispositius a monitoritzar s'han creat plantilles o templates per a facilitar aquesta tasca, com per

[6] http://www.ks-soft.net/hostmon.eng/wmi/index.htm

exemple qualsevol nou agent definit amb la plantilla anomenada "Web" s'inclou els mòduls de ICMP: "host latency" i "host alive".

- S'ha instal·lat un mapa amb la ubicació d'un dispositiu a un sistema GIS, en aquest cas amb googlemaps, per a localitzar geogràficament als agents, Ha estat necessari generar la clau amb l'API de google i definir el centre del mapa per defecte.
- S'ha activat la consola SNMP al servidor per a rebre els traps dels dispositius remots.
- S'ha generat una recerca d'equips dins d'un rang de classe C (192.168.1.0/24) amb 254 adreces per assignar a dispositius

4.3.3.4. Mòduls (plugins)

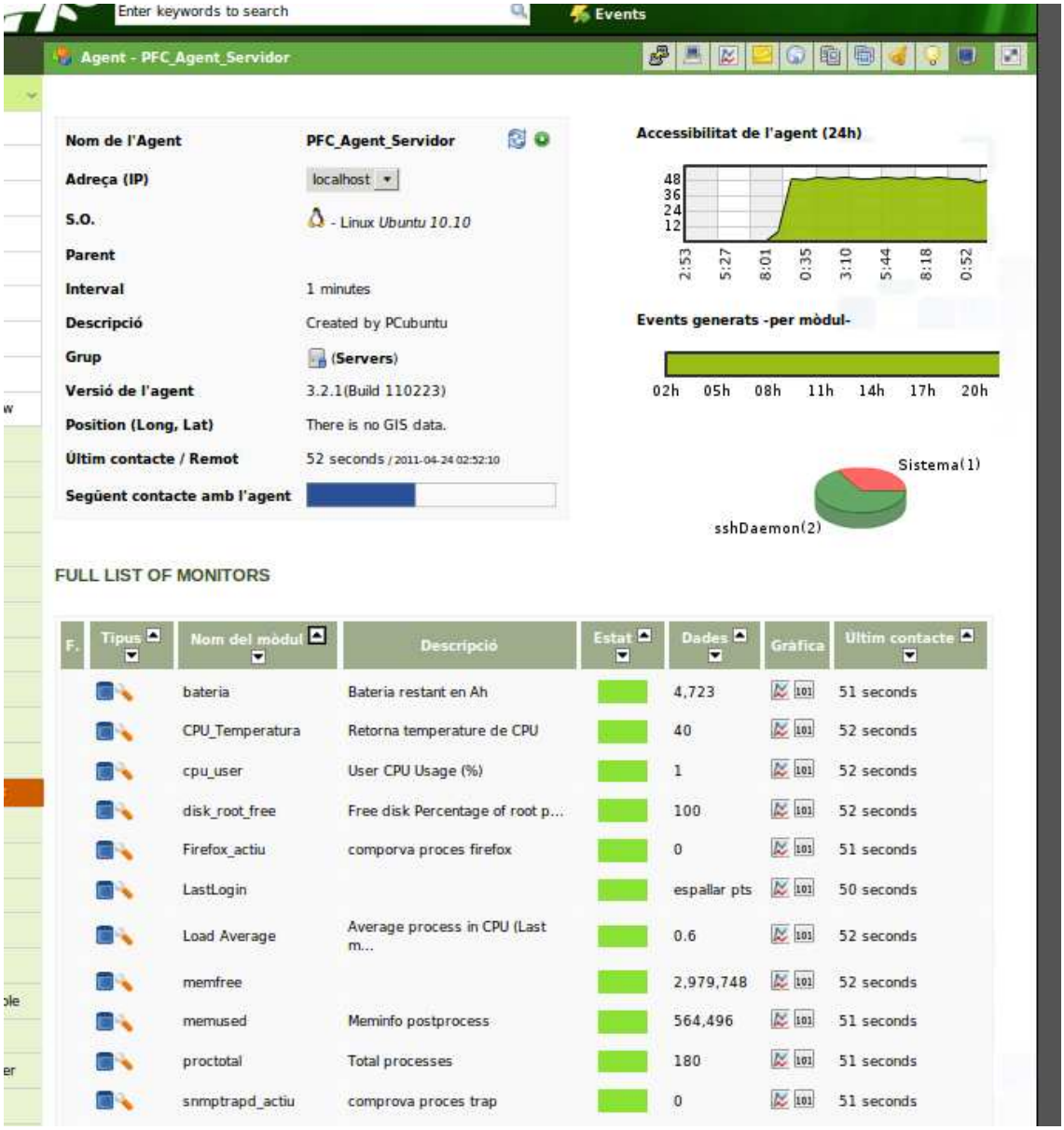
S'han desenvolupat diferents mòduls en l'agent Windows:

- "Tràfic" que consulta els bytes transmesos i rebuts pel dispositiu amb la comanda netstat i els suma.
- Service_FW que comprova que el servei del tallafocs, anomenat "MpsSvc", està iniciat. Per detectar immediatament la caiguda del servei s'incorpora la comanda "module_async yes" per enviar una notificació al servidor i per completar la supervisió s'ha configurat "module_watchdog yes" per aixecar el servei automàticament.
- Test del router que comprova des del PC Provençals si el port TCP 80 de l'encaminador està actiu. És una mostra del que Pandora anomena Agent Proxy o agent que fa d'intermediari entre el dispositiu supervisat i el servidor Pandorafms.

Per l'agent Linux s'han desenvolupat aquests mòduls:

- CPU_Temperatura que comprova la temperatura de la CPU que dóna l'API ACPI o Advanced Configuration and Power Interface, instal·lada abans en l'equip.
- Bateria que fa servir la mateixa API i dóna la càrrega restant en Amperis/hora o AH de la bateria del portàtil.
- Firefox_actiu i snmptrapd_actiu comproven que els processos respectius estiguin actius.

L'agent al Servidor ens dóna en la part superior informació de l'agent i gràfiques de la disponibilitat, esdeveniments i alertes; en la part inferior informació dels mòduls que supervisa, el seu estat, quins valors retorna i quan ha estat l'última consulta. En aquest moment la temperatura de la CPU és de 40 ºC, la bateria té una càrrega de 4,723 Ah, firefox està actiu i el snmp està inactiu.



F.	Tipus	Nom del mòdul	Descripció	Estat	Dades	Gràfica	Últim contacte
		bateria	Bateria restant en Ah		4,723		51 seconds
		CPU_Temperatura	Retorna temperature de CPU		40		52 seconds
		cpu_user	User CPU Usage (%)		1		52 seconds
		disk_root_free	Free disk Percentage of root p...		100		52 seconds
		Firefox_actiu	comporva proces firefox		0		51 seconds
		LastLogin			espallar pts		50 seconds
		Load Average	Average process in CPU (Last m...		0.6		52 seconds
		memfree			2,979,748		52 seconds
		memused	Meminfo postprocess		564,496		51 seconds
		proctotal	Total processes		180		51 seconds
		snmptrapd_actiu	comprova proces trap		0		51 seconds

Il·lustració 12 dades proporcionades per l'agent del servidor

4.3.3.5. Gestió d'alertes, esdeveniments i incidents

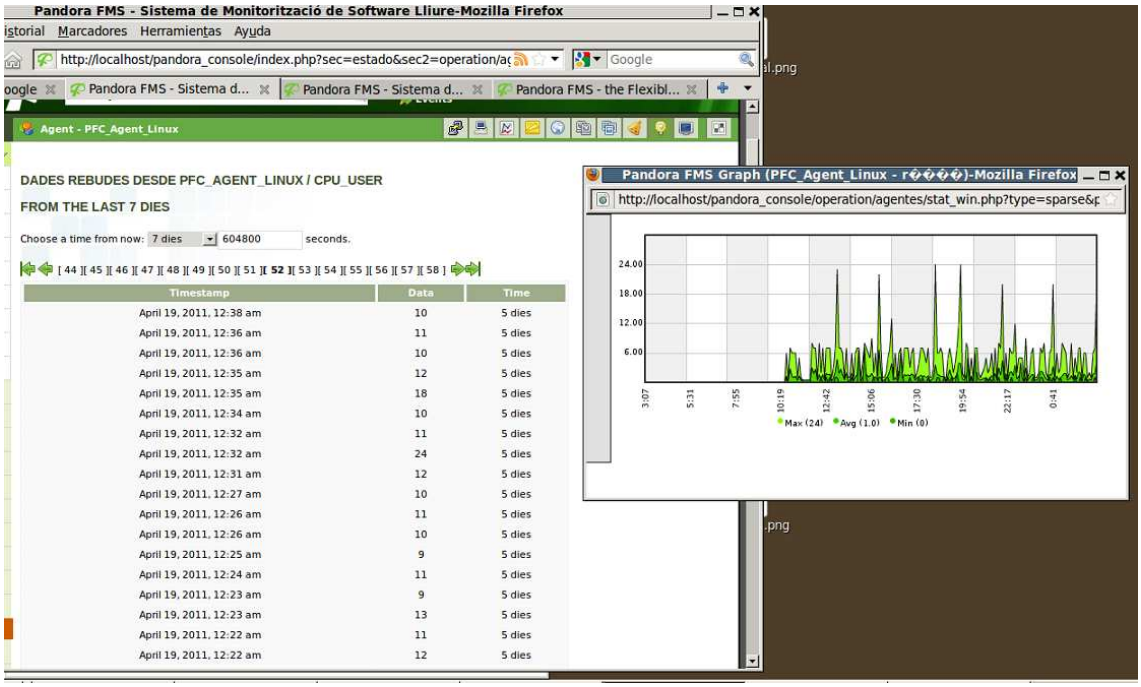
S'han creat alertes que poden crear esdeveniments, enviar de correu, reinici de l'agent i iniciar el cicle pel seguiment d'una incidència. En aquest apartat s'ha generat una alerta correlada:

S'anomena "Error d'accés a Internet" i està assignada a la "Web de Badalona" i es crearà un incident quan es detecta que l'encaminador no respon a ICMP o a SNMP

4.3.3.6. Elaboració d'informes

Hi ha diferents opcions pels informes i s'accedeix des de l'eina de gestió, en concret s'han generat tres informes pel grup de servidors, el grup de webs i l'encaminador. Una altre opció és, al veure l'estat de cada agent, consultar el gràfic que indica l'evolució dels valors de la consulta en el temps.

En aquest exemple es pot veure les dades i la gràfica de l'ús de la CPU que proporciona l'agent Linux del PC Ubuntu.



Il·lustració 13 informe d'agent Linux

4.3.3.7. Notificacions

S'ha configurat que les alertes crítiques d'ICMP generin un correu electrònic al responsable i al fitxer *log* es pot consultar els error en els missatges per que el destinatari no acceptava l'origen del correu.

4.3.3.8. Funcionalitats ampliables

El projecte pandorafms ofereix ampliacions per a:

- Agent per a dispositius Android que es pot descarregar des del *Market Android,* i amb la integració amb Googlemaps es pot localitzar la ubicació geogràfica dels dispositius.
- *Monitorització transaccional web avançada*: mesura els temps de resposta de cada element d'una web monitoritzada i pot introduir dades en un formulari per provar el funcionament.
- Supervisió d'equipament virtualitzat, tipus VMWare.
- Disposa d'un *plugin* per a entorns virtualitzats i *cloud* com Amazon Elastic Compute Cloud o Amazon EC2.

4.3.4. Desenvolupament d'agents

S'han fet modificacions l'agent Windows per a extreure el tràfic de la interfície de xarxa, comprovar que el servei Firewall està actiu i provar la connectivitat entre l'equip Windows i l'encaminador. A l'agent Linux es fa la consulta de la temperatura de la CPU i la càrrega de la bateria del portàtil.

4.3.4.1. Mòduls agent Windows

```
# Bytes enviats i rebuts per la interfície de xarxa
module_begin #inici del mòdul
module_name Trafic #nom del mòdul
module_type generic_data # tipus de dada, en aquest cas un valor numèric
# executa 'netstat –e', fa una recerca del valor "bytes" i fa la suma del segon i el
# tercer paràmetre, el que correspon als bytes totals: emesos i els rebuts
module_exec netstat -e| grep  "Bytes " | gawk "{ print ($2 +$3) }"
module_description tràfic en Bytes #la descripció del mòdul
module_end #final del mòdul

# Veure si el servei Firewall Windows està actiu i sinó aixecar-lo
module_begin
module_name Service_FW
module_type generic_proc #tipus de dada, retorna un 1 si esta actiu o un 0
module_service MpsSvc # nom del servei de tallafocs de Windows
module_description Service FW Windows
module_async yes #permet l'enviament de traps al Servidor
module_watchdog  yes  # aixeca el procés MpsSvc que correspon al servei de tallafocs
module_end

# Utilitzar l'agent com a pont fins un altre punt de mesura
# Veure si el router té actiu el port 80
module_begin
module_name Test del router
module_type generic_data #retorna el temps de resposta
module_tcpcheck 192.168.1.1 #executa l'script tcpcheck per fer un test al router
module_port 80 #volem provar que està actiu el port HTTP
module_timeout 5 #temps màxim per la resposta
module_end
```

4.3.4.2. Mòduls agent Linux

```
# Mòdul per a obtenir la temperatura de la CPU, cal instal·lar abans l'ACPI o Advanced Configuration and Power Interface
module_begin
module_name CPU_Temperatura # Nom  del mòdul
module_type generic_data # Retorna un número
module_exec cat /proc/acpi/thermal_zone/CPUZ/temperature | awk '{ print $2 }'# Crida a un fitxer que emmagatzema el valor de la temperatura i extreu només aquest valor
module_description Retorna temperature de CPU
module_end

# Comprova si el l'estat de la bateria cal instal·lar abans l'ACPI o Advanced Configuration and Power Interface
module_begin
module_name bateria# Nom  del mòdul
module_type generic_data_string # Retorna una cadena de text
```

```
module_exec cat /proc/acpi/battery/BAT0/state | grep remaining | awk '{ print $3 }'# retorna el valor de la bateria en Ah
module_description Bateria restant
module_end
```

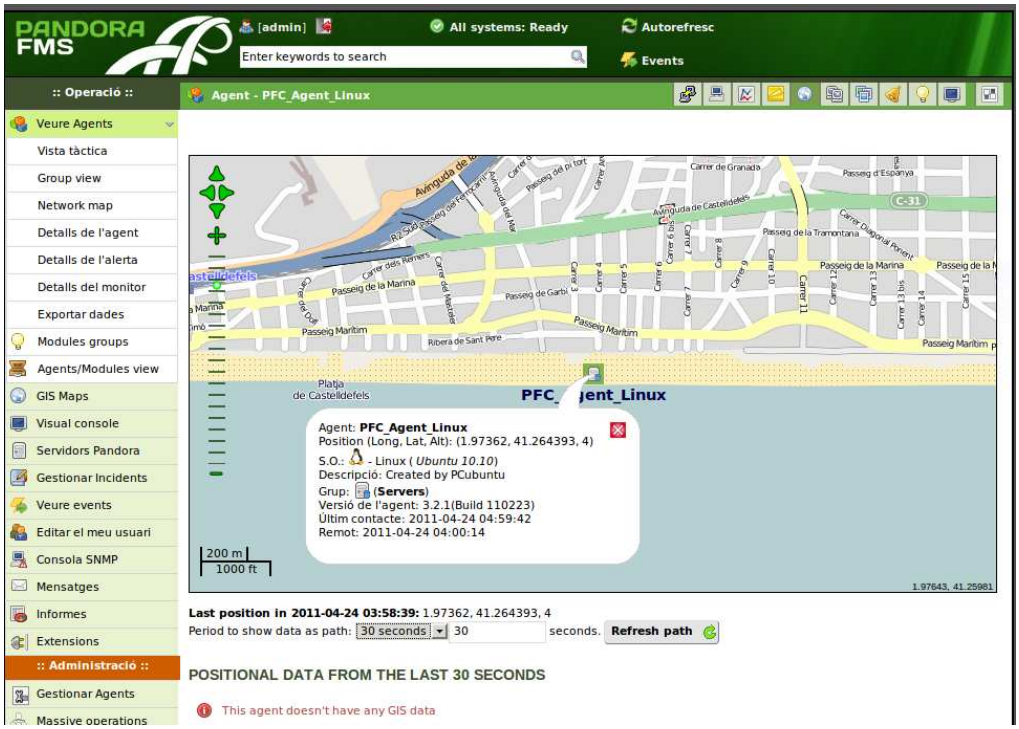
4.3.5. Comparativa

S'han agrupat en característiques generals i les relacionades amb els mètodes de monitorització.

4.3.5.1. Característiques generals

- **Instal·lació**: seguint els passos de la documentació és pot instal·lar tant el servidor com l'agent per a Linux i Windows sense problemes.
- **Manual i ajuda**: la informació és comprensible i força complerta per a poder resoldre els problemes més comuns que puguin sorgir, a part cal destacar la bona documentació de les FAQ, qüestions més freqüents, i les guies ràpides que són accessibles des de la web de la comunitat. La web del desenvolupador http://artica.es/ o del producte http://pandorafms.com/ no ofereixen la documentació de Pandorafms, cal anar a la web de la comunitat http://pandorafms.org/.
  L'ajuda del programari és la necessària per a poder interpretar les funcionalitats que ens ofereix sempre que partim d'un coneixement bàsic de l'eina
- **Seguretat**: les claus no tenen cap recomanació. L'accés al programari és amb usuari/clau, es poden crear diferents perfils el que permet limitar l'accés a certes funcionalitats, com per exemple accés de lectura o escriptura, o també pot limitar la gestió a una part dels elements supervisats, com per exemple per a compartir l'eina amb els departaments de sistemes i els gestors de la xarxa que tenen rols diferents. L'accés a la BBDD: hi ha dos usuaris per a accedir a la base de dades que es configuren a la fase d'instal·lació, l'usuari root que ens demana la clau d'accés i l'usuari de Pandora que el mateix programa genera una clau aleatòria amb un nivell mig de seguretat.
  La comunicació des del servidor fins l'agent es fa servir Tentacle o SSH o FTP i es pot xifrat l'intercanvi de dades amb el protocol SSL.
  Es poden fer auditories dels usuaris, sempre que s'hagin habilitat durant l'alta de l'usuari.
- **Integració amb altres eines**: incorpora l'ús de SSH i VNC, però és la versió Enterprise qui té un plugin per afegir les més estàndards.
- **Base de dades**: només pot ser MySQL i pot estar configurat en mode clúster, amb diferents servidors que poden treballar actiu/passiu o actiu/actiu, en funció de si poden rebre les dades al mateix moment. No té cap manteniment i només es controla el nombre de dies per eliminar les dades i quan es poden compactar per reduir espai físic.
  Per a solucionar la possibilitat de consultar dades més antigues existeix la possibilitat de generar una segona base dades MySQL com a històric independent de la descrita abans.
- **Còpies de seguretat i restauració**: l'eina facilita un *script* extern a la consola molt fàcil d'utilitzar per a fer les còpies de seguretat i la restauració amb diferents opcions.
- **Codi obert**: el codi és accessible i modificable.

- **Nivell d'ús**: la gestió es fa amb una aplicació web, no necessita instal·lar cap component, és fàcil d'utilitzar i té totes les funcionalitats molt accessibles doncs estan representades en quatre zones fixes a totes les pantalles: la capçalera i en tres menús en la part esquerra de la pantalla.
- **Personalització**: en la versió *Open Source* aquesta modificació ens obliga a aplicar-la a tots els usuaris i en la versió *Enterprise* es pot adaptar per a cadascun dels usuaris.
  Es pot afegir mapes aportats per l'usuari o un sistema GIS (Sistema d'informació geogràfica) amb les dades de altitud, latitud i longitud, es pot modificar els icones dels elements supervisats i es pot modificar la pantalla inicial. En aquesta imatge es pot veure la integració amb Googlemaps per la localització geogràfica dels dispositius, en aquesta imatge l'agent Linux indica que el dispositiu està actiu pel color verd de la icona i obre una finestra amb les seves dades.

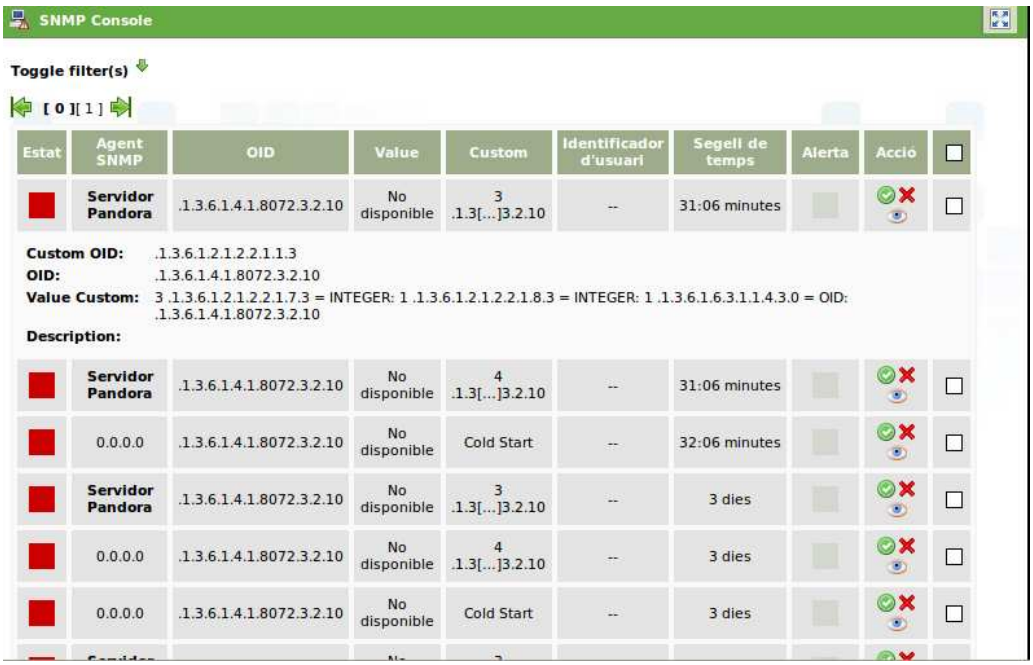


Il·lustració 14 integració amb Googlemaps

- **Gestió SLA**: podem configurar els paràmetres dels SLA i extreure el seu compliment amb un informe específic, tant pels elements supervisats com per un grup d'aquests. La configuració és laboriosa per que implica la parametrització de cadascun dels SLA.
- **Gestió ITL**: ofereix eines per aplicar les definicions dels paràmetres reconeguts a ITIL v3 en els processos per la resolució d'incidències i fer un seguiment amb informes programats, similar al punt anterior.
- **Gestió de pressupostos**: no està suportat.
- **Instal·lació de client**: als ordinadors cal un agent per a poder enviar les dades detallades de l'equip.
- **Generació automàtica d'informes**: no permet la creació de tasques automàtiques per la generació o l'envio d'informes.

4.3.5.2. Mecanismes per a recol·lectar la informació

- **Descobriment automàtic de dispositius**: fa servir el servidor Redcon del sistema Pandorafms per a descobrir els dispositius connectats a la xarxa, segons diferents paràmetres: rang d'IPs, sistemes operatiu o ports TCP o UDP oberts. També permet l'ús d'*scripts* creats per l'usuari, un exemple seria el descobriment i la creació automàtica dels elements connectats amb el port SNMP activat amb la plantilla que incorpora l'agent adient. Aquesta funcionalitat es pot fer servir per a descobrir els dispositius que tenen oberts ports considerats insegurs, extreure un llistat els equips que tenen desactualitzat el sistema operatiu,... . El descobriment d'una classe C triga uns 40 segons i al representar els dispositius descoberts no sempre surten al lloc correcte, pel que s'han de revisar la ubicació en el mapa.
- **Detecció de caigudes**: té definit com a funcionalitat bàsica "Host Alive" i "Host latency" per a fer consultes amb el protocol ICMP.
  No permet la detecció d'alertes en cascada des d'un dispositiu principal, com per exemple detectar que si l'encaminador d'una xarxa cau els dispositius que estiguin connectats darrere no donin alarmes.
- **Programació de llindars**: cada mòdul dels dispositius a supervisar permet la configuració de dos paràmetres: els llindars per a classificar els tres nivells d'alarmes i el nombre de repeticions de la consulta abans de situar l'alerta en aquest nivell. Les alertes poden iniciar diferents accions: enviar SMS o correu, alarma sonora, enviar informació a un Syslog, ...
- **Recepció d'esdeveniments**: es poden rebre pel protocol SNMP traps asíncrons, de qualsevol dispositiu que tingui configurada la IP del servidor Pandora com a receptor del servei. Es poden consultar per la consola de recepció de traps, com es veu a la següent imatge, però les eines per a facilitar la interpretació del missatge i per la generació automàtica de mòduls de supervisió estan implementats a la versió *Enterprise.*



Il·lustració 15 consola de recepció de traps

- **Prediccions**: té un servidor dedicat per aquesta funció i permet crear una línia base generada amb la informació, recomanen un mes com a mínim per

a predir el comportament del dispositiu a supervisar i si s'obtenen resultats per sota d'aquesta línia generar una alerta. No ha funcionat correctament a l'entorn de prova.

- **Accions automàtiques per esdeveniments**: no permet la interacció automàtica amb altres eines. La versió Enterprise permet executar altres eines i registrar cada esdeveniment.
- **Eines per actuar als dispositius** : proporciona programari per la gestió amb SSH i per incorporar altres eines caldrà fer un desenvolupament propi.
- **Correlació d'esdeveniments**: permet crear alarmes complexes relacionades amb altres alarmes, s'ha provat la creació d'una alarma associada al dispositiu "web badalona" quan es detecta el tràfic a la interfície de l'ADSL de l'encaminador baixa a un llindar.
- **Filtratge d'esdeveniments**: permet el filtratge d'esdeveniments fent cerques per diferents paràmetres i la creació d'alarmes per a registrar-los i fer seguiment.
- **Suportar IP i IPv6**: està preparat per a treballar amb IPv6 i amb plataformes Linux, Windows, HP-UX, AIX, Solaris, Android i Nokia IPSO, no suporta MacOS.
- **Eines de suport a MIB**: incorpora la comanda *snmpwalk* durant la creació dels agents, però a la versió Enterprise s'ofereixen eines per interpretar les consultes de les MIB.
- **Inventari**: està disponible per la versió Enterprise i disposaria d'un servidor dedicat a extreure l'inventari de les xarxes que necessiten d'agents específics per aquesta funció, què s'entreguen per a cada sistema operatiu suportat

4.4. Zenoss

Per aquesta prova s'ha utilitzat les següents versions:

- Zenoss Core 3.1.0,
- Zenpack de Zenoss HTTP monitor 2.6, Linux monitor 2.6 i RPC monitor 2.6,
- Zenpack de Blake Drager fping 2.6.

4.4.1. Eina de monitorització

Avui està la versió Zenoss Core com a Open Source i la versió comercial Enterprise. El projecte Open Source per desenvolupar una eina de monitorització i gestió per a dispositius remots es va iniciar l'any 2005, està fet en llenguatge Phyton. El desenvolupament està centralitzat en la seva comunitat, des d'on es poden descarregar els Zenpacks i els paquets per complementar la versió Open Source. Estan agrupades per la seva utilitat i pel dispositiu a monitoritzar, en els anomenats zenpacks. En general tot el sistema és escalable per que permet incorporar servidors o Zenpacks desenvolupats externament.

El nucli es basa en independents servidors que gestionen aspectes diferents del sistema i estan preparats per a treballar en entorns Linux i MAC OS, però també amb Windows sobre VMPlayer. Utilitza un servidor per incorporar mapes GIS o Googlemaps que permet la localització dels dispositius mòbils. Té integrat un servidor Syslog o recol·lector d'esdeveniments, només ens cal configurar l'adreça del servidor Zenoss en la configuració dels traps SNMP dels dispositius a

monitoritzar L'eina incorpora un client web per la gestió dels servidors i per supervisar-los. està basada en la web orientat a objectes Zope.

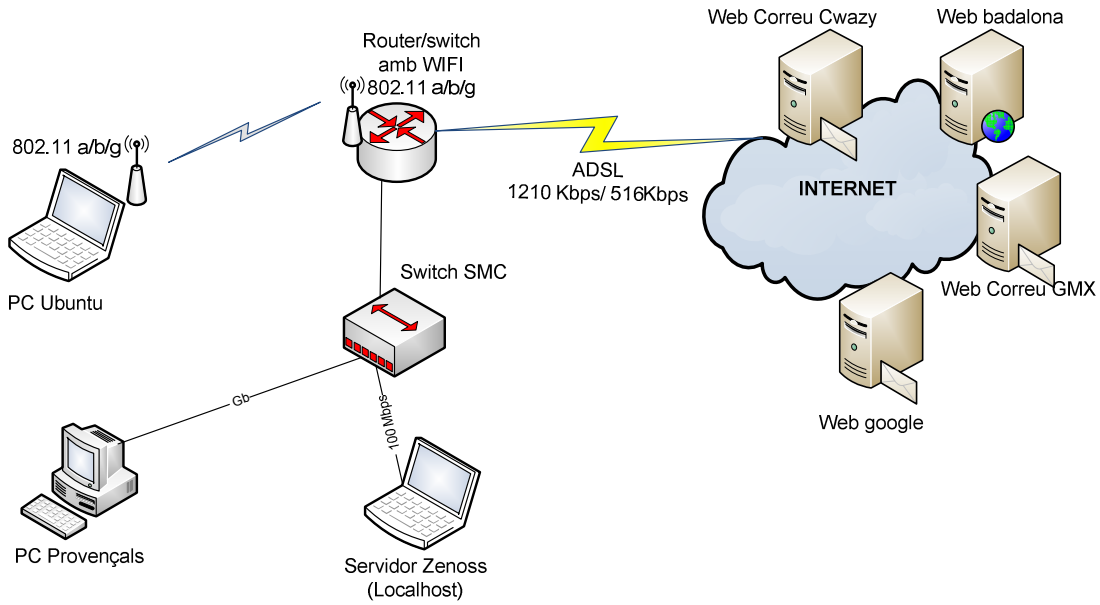
Per la monitorització fa servir els protocols SNMP, WMI per a Windows, ICM, SSH i Telnet, integra eines complementaries com RRDTools o NET-SNMP i incorpora eines com NMAP, IPScan i snmpwalk. Els anteriors protocols els té implementats dins de l'eina i són els mètodes per a fer els consultes remotes, apart es poden afegir altres funcionalitats amb mòduls addicionals anomenats Zenpacks. Les consultes s'emmagatzemen en una BBDD MySQL, i proporciona eines bàsiques per extreure o modificar la informació.

Els millors punts de la consola són l'aprofitament dels mecanismes de supervisió per extreure la major quantitat d'informació possible, l'alta de dispositius és molt fàcil amb les plantilles o *template* segons el tipus d'equip que podem fer noves o modificar-les, l'ampliació de funcionalitats és molt fàcil tenint en compte que només cal el ratolí, integra altres eines i ofereix una amplia varietat de gràfiques. Pel nombre de valors la parametrització es pot complicar i és lenta de manegar.

És una eina complicada de configurar però per la gestió dels dispositius es simplifica. La integració de Googlemaps només serveix per localitzar dispositius mòbil. Utilitza els *plugins* de Nagios, per exemple al veure el fitxer que executa les consultes RPC es llegeix les referències a la web de Nagios. En aquesta prova les consultes WMI si han funcionat.

4.4.2. Descripció de l'entorn de proves

Per aquesta avaluació s'han fet servir tres ordinadors, un encaminador o router, i la xarxa Internet per a accedir a quatre servidors web, l'esquema és el següent:



Il·lustració 16 esquema de l'entorn de proves de Zenoss

4.4.3. Tasques fetes per la preparació de l'entorn de proves

4.4.3.1. Configuracions als equips

- El servidor no te cap requeriment per configurar
- Al PC Provençals amb Windows 7 s'ha instal·lat i configurat l'agent, s'ha activat el protocol SNMP amb una clau o community, s'ha donat permisos a WMI de lectura a l'agent i al Servidor Pandora i s'ha configurat al Firewall per a permetre les comunicacions d'entrada i sortida amb Pandora. S'ha instal·lat el plugin "SNMP informant"[7], versió estàndard, per completar la informació que proporciona el protocol SNMP.
- Al router, PC Ubuntu i Servidor Pandora s'ha activat el protocol SNMP amb la clau i la configuració dels traps.

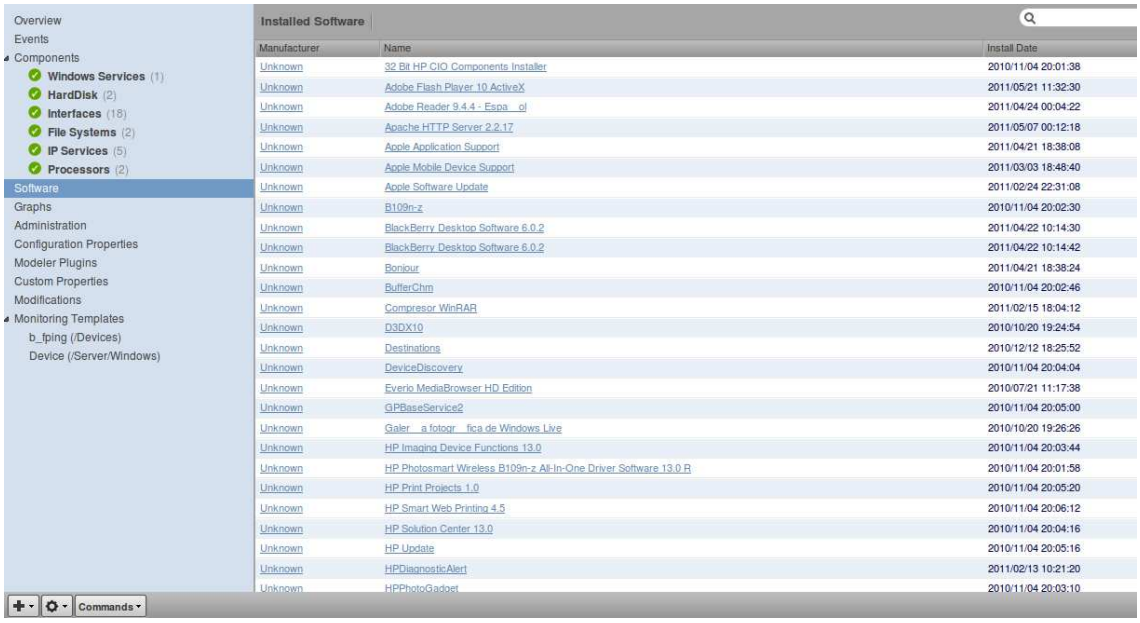
4.4.3.2. Definició de sistemes de monitorització

L'activació d'un servei es limita a crear el dispositiu, a assignar-li una plantilla i configurar, a les propietats de cada dispositiu, l'usuari i la clau de cadascun dels sistemes per accedir. Per aquest accés es poden utilitzar tres sistemes: protocol SNMP, comanda SSH o Telnet i protocol WMI per a entorns Windows. Quan s'ha establert el contacte es poden consultar els paràmetres dels plugins que té assignats a la plantilla inicial: interfícies, CPU, memòria, programari que està instal·lat,... . També pot fer servir eines del protocol TCP/IP. Així utilitza:

- protocol SNMP fa servir el port UDP 162, només requereix tenir el servei actiu als dos extrems i configurat la community. També podem configurar els traps als equips remots per enviar els esdeveniments al servidor.
- comanda SSH o Telnet permeten connectar als dispositius i consultar les dades del seu estat mitjançant comandes.
- protocol WMI s'ha configurat al servidor l'usuari, la clau i el domini on es vol consultar per accedir a WMI, a l'equip amb sistema operatiu Windows.
- Eines TCP, podem fer servir el protocol ICMP o ping per consultar l'estat i la latència, també poden fer una anàlisi de ports amb la comanda nmap.

Un exemple de la informació que pot treure per WMI és un llistat del software instal·lat d'un ordinador amb el nom de fabricant i la data d'instal·lació. Aquesta funcionalitat s'aprofita per poder fer descobriments de dispositius que tinguin un programari concret, per exemple serviria per extreure un llistat dels equips que tenen una versió desactualitzada del programari de comptabilitat.

[7] Veure http://www.snmp-informant.com/index.htm



Il·lustració 17 exemple de dades consultades per WMI

4.4.3.3. Configuració de l'eina

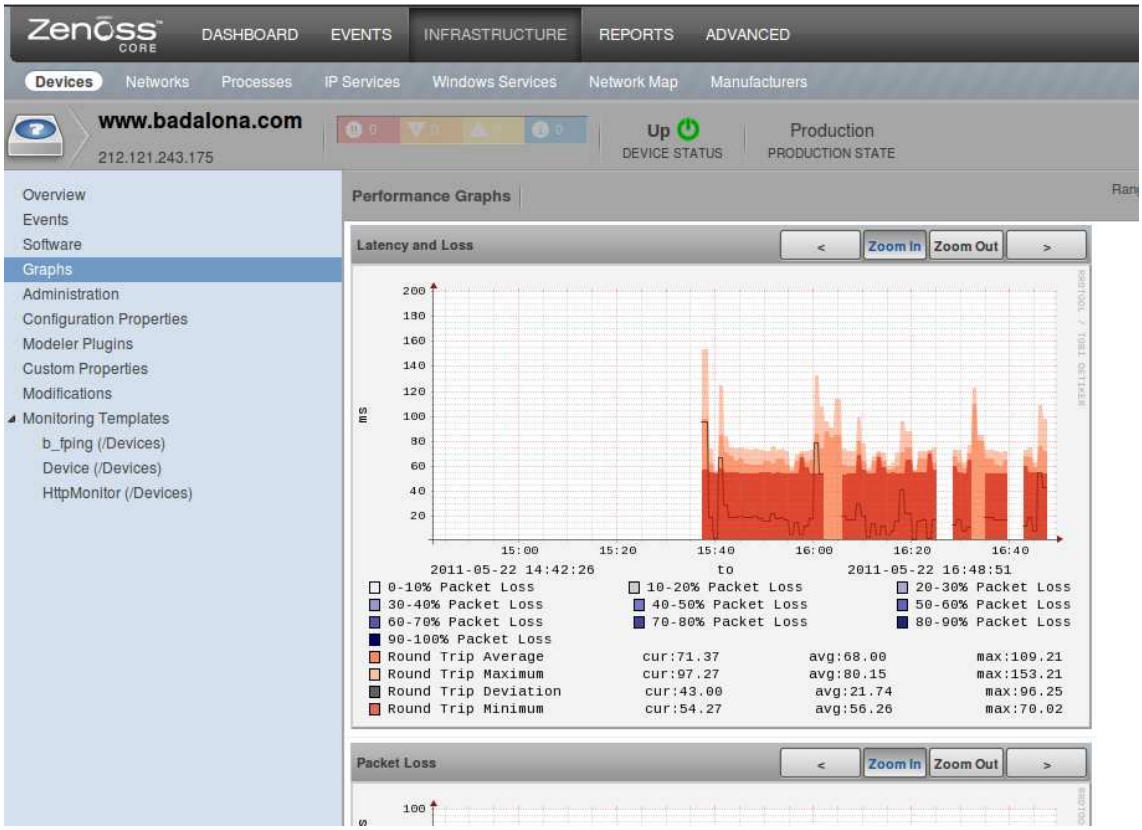
Configurar el sistema bàsic és molt senzill: a l'entrar a Zenoss per primer cop ofereix la possibilitat de fer un escaneig per incorporar els dispositius o fer-ho manualment. Si escollim el sistema automàtic ens preguntarà al finalitzar el tipus de plantilla a fer servir pel l'equip, si es fa manual ens caldrà configurar algun paràmetre més. Per posar-ho en marxa, el que ens queda es configurar l'usuari i la clau de cadascun dels protocol o eina que farem servir per a monitoritzar-lo.

Les funcionalitats més habituals per monitoritzar dispositius estan implementades pel programari. Un exemple és l'estructura d'arbre de les plantilles, on cada branca hereta les característiques de la seva predecessora i en el cas de repetir-la s'escull la última. En aquesta prova s'ha creat una plantilla o template per facilitar generar els dispositius que s'accedeixen per Internet que incorpora la consulta "host alive". Les plantilles estan agrupades pel tipus de dispositiu a supervisar i pel mètode en comunicar-nos, així un template Server/Linux/SSH és una plantilla per un servidor Linux que es connectarà per l'eina SSH.

4.4.3.4. Plugins i Zenpacks

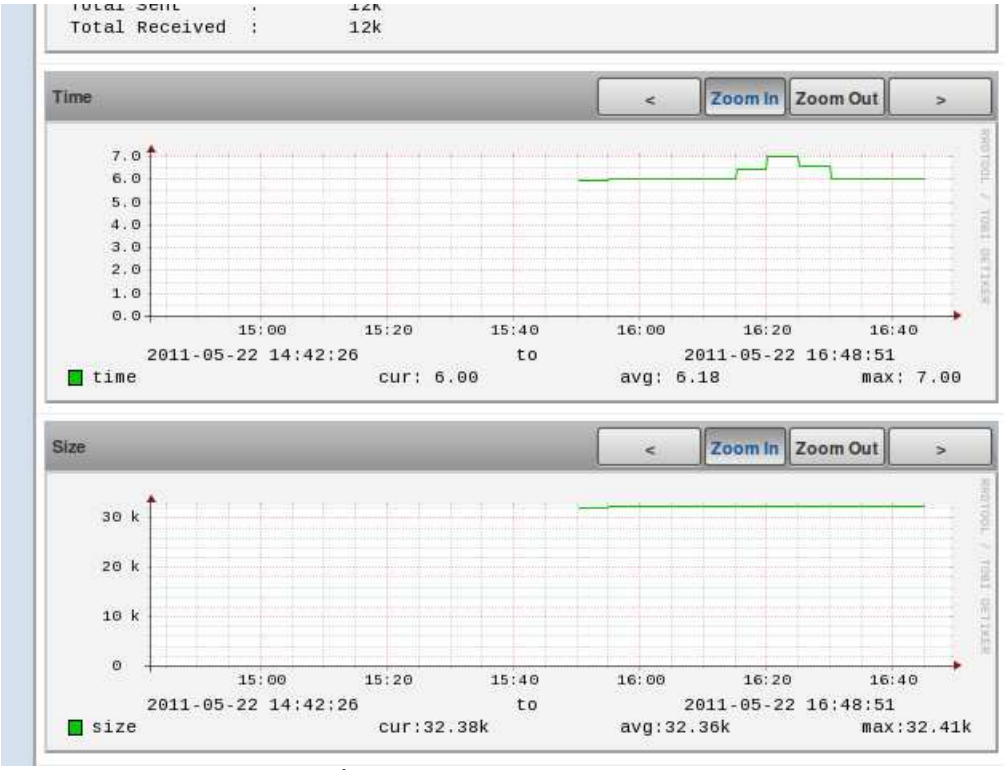
La comunitat del projecte Zenoss ofereix un ampli assortit de plugins i zenpacks que complementen les seves funcionalitats. Els primer són comandes associades a un dels sistema de monitoritzar i el segon són paquets que poden incloure plugins, gràfics o comandes. Es pot utilitzar els plugin de Nagios per a Zenoss. S'han instal·lat els zenpacks:

- Des de la comunitat, "fping", que genera una gràfica del temps de resposta del dispositiu que ho tingui configurat.
  A la següent imatge es pot veure latència de www.badalona.com que ens proporciona l'eina *fping*, ens dóna les valors mitjos de 68 ms. La informació aportada pel zenpack es consulta en l'apartat de gràfics del dispositiu.



Il·lustració 18 latència web badalona

- Des de Zenoss, "HTTP monitor", per a incorporar gràfiques de les consultes a servidors externs i "Linux monitor" per millorar les gràfiques dels servidors Linux. Amb "HTTP monitor" podem veure el temps en descarregar la plana principal i la seva mida.



Il·lustració 19 resposta HTTP de la web de badalona

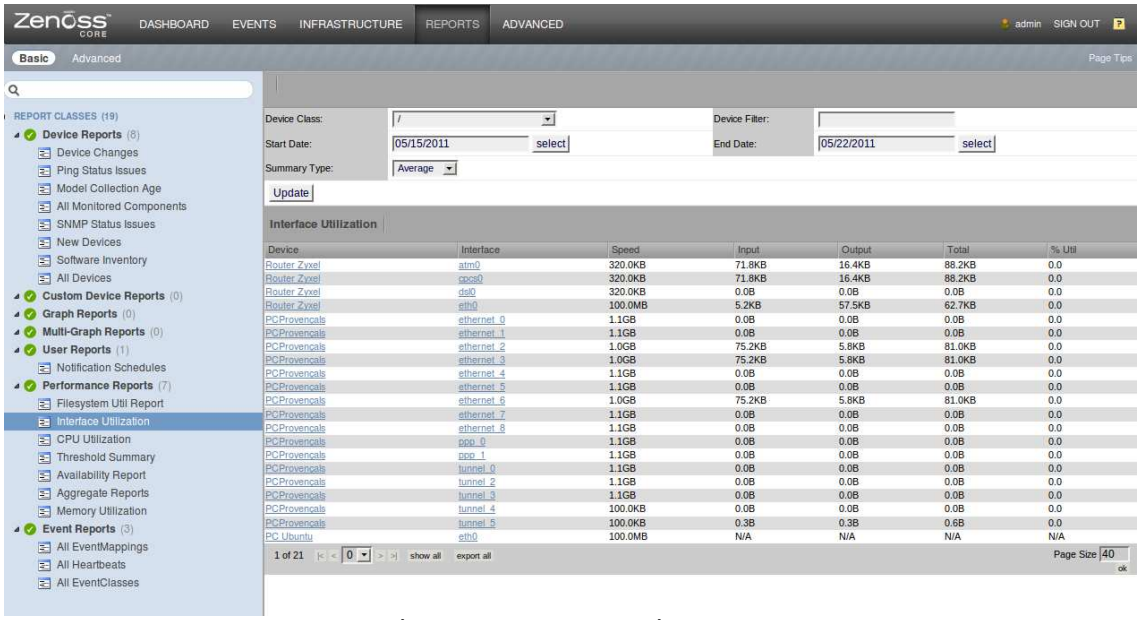
4.4.3.5. Estats

Els dispositius tenen tres estats: OK si està correcte, Critical si falla algun mòdul i Warning si supera uns llindars que pot configurar l'usuari. Els esdeveniments tenen 7 nivells de severitat: Critical, Error, Warning i Info per identificar les consultes dels equips, Debug i Clear per indicar les funcions noves que s'han activat.

4.4.3.6. Elaboració d'informes

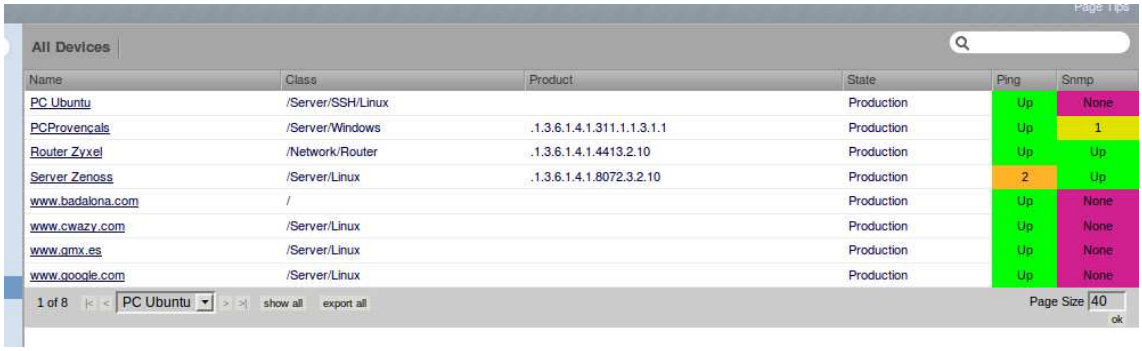
Té una gran varietat definits des de CPU, memòria, disponibilitat, SNMP, discos,.. i la possibilitat de crear de nous. Per les representació gràfica fa servir MRTG, que a l'estar integrat permet la manipulació de les gràfiques amb el ratolí, o sigui limitar en el temps i ampliar.

L'eina té moltes opcions per generar informes, pel que mostrarem diferents exemples: el primer és un informe amb tots els interfícies dels equips supervisats on surt les dades del consum dels amples de banda de cadascun, es veu com el tràfic que surt per la interfície *atm* de l'encaminador (correspon a la sortida ADSL i és de 88,2 KB) el fa servir el PC Provençals (genera un tràfic de 81 KB). També ens mostrarà a la part dreta els diferents informes que ofereix l'eina.



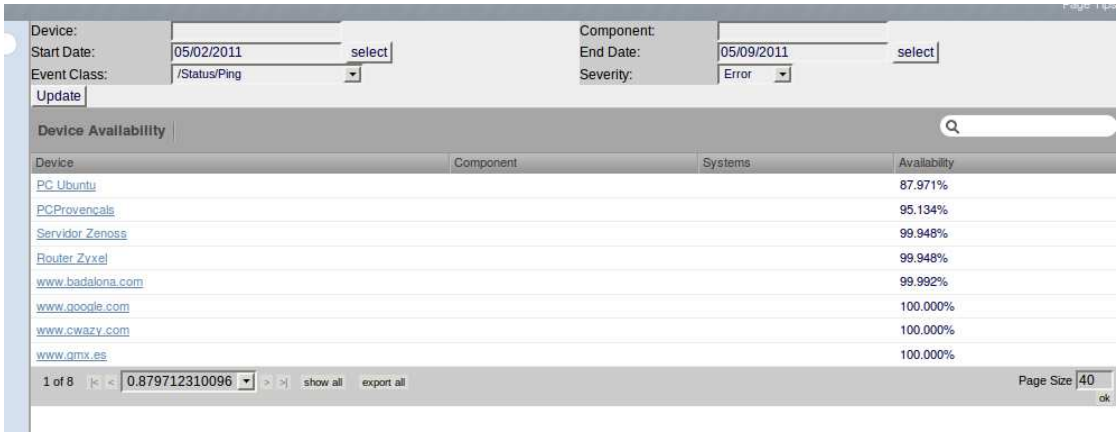
Il·lustració 20 informe d les interfícies supervisades

En aquesta imatge es veu la classificació de cada dispositiu, quines consultes SNMP te actives, el tipus de connexió que fa servir: SSH, SNMP, o Ping i l'estat de les dues últimes amb el nombre d'alarmes,



Il·lustració 21 informe dels dispositius

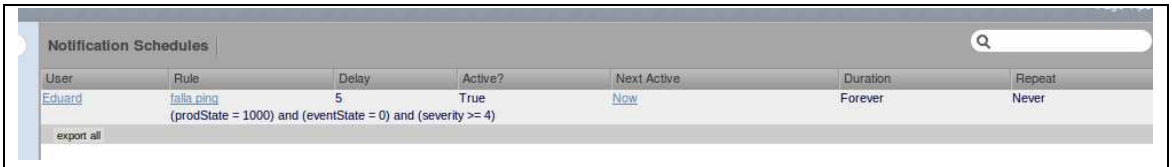
Es un informe de disponibilitat dels equips que estan monitoritzats.



Il·lustració 22 informe de disponibilitat

4.4.3.7. Notificacions

Es genera un correu electrònic a l'usuari definit quan s'arriba l'alerta. En l'exemple s'envia el missatge després de 5 segons de rebre l'alerta, la regla no té caducitat i no cal tornar a enviar la mateixa alerta si no s'havia recuperat abans. En el missatge es veu el nombre d'enllaços per a aconseguir informació de l'avís.



De: "zenossuser_admin@localhost6.localdomain6"
<zenossuser_admin@localhost6.localdomain6>
Para: espallargasse@yahoo.es
Enviado: vie,27 mayo, 2011 00:08
Asunto: [PFC amb zenoss] Server Zenoss ip 192.168.1.35 is down

Device: Server Zenoss
Component:
Severity: Critical
Time: 2011/05/27 00:08:08.000
Message:
ip 192.168.1.35 is down
Event Detail:

http://localhost6.localdomain6:8080/zport/dmd/Devices/Server/Linux/devices/Server%20Zenoss/viewDetail?evid=345d2ef4-7a89-4f45-99b6-c6984acfa92b
Acknowledge:
http://localhost6.localdomain6:8080/zport/dmd/Devices/Server/Linux/devices/Server%20Zenoss/manage_ackEvents?evids=345d2ef4-7a89-4f45-99b6-c6984acfa92b&zenScreenName=viewEvents
Delete:
http://localhost6.localdomain6:8080/zport/dmd/Devices/Server/Linux/devices/Server%20Zenoss/manage_deleteEvents?evids=345d2ef4-7a89-4f45-99b6-c6984acfa92b&zenScreenName=viewHistoryEvents
Device Events:
http://localhost6.localdomain6:8080/zport/dmd/Devices/Server/Linux/devices/Server%20Zenoss/viewEvents

Il·lustració 23 regla i exemple de notificació per alerta PING

4.4.3.8. Funcionalitats ampliables

- Ofereix la possibilitat de gestionar i generar informes de sistemes d'emmagatzematge amb Zenpack HP EVA monitor.
- Pot incorpora les eines cfengine per la gestió de fitxers de configuració i Subversion per la gestió de versions d'aquests.
- Incloure sistemes de control per detectar i notificar de qualsevol canvi sobre dels equips supervisats, ja sigui de programari o maquinari. És un sistema per controlar les modificacions no autoritzades en els sistemes informàtics.
- Localització remota per que permet la integració amb tecnologia mòbil per a fer un seguiment i registre dels moviments del dispositiu.
- Té Zenpack per la gestió de les bases de dades Oracle, Nginx o servidor intermediari de codi obert.
- És una eina orientada a la supervisió en entorns tipus *cloud* com la monitorització dels serveis d'allotjament oferts per l'empresa Amazon al núvol o Amazon Web Services (EC2), control de les aplicacions que ofereix Google a la seva estructura o Google App Engine i la integració les eines de supervisió de serveis en el núvol com Ganglis de l'empresa OpenNebula.
- Permet la instal·lació en una màquina virtual, la versió Windows dins d'una VMWare, i supervisa sistemes virtuals en el núvol o *cloud.*

4.4.4. Comparativa

S'han agrupat en característiques generals i les relacionades amb els mètodes de monitorització.

4.4.4.1. Característiques generals

- **Instal·lació**: és molt senzilla per que només cal instal·lar MySQL i executar una instrucció, el manual només s'ha consultat per la comanda d'instal·lació.
- **Manual i ajuda**: la web està molt bé estructurada per localitzar documentació però l'ajuda de l'aplicació no té aquest nivell i et remet a la informació d'Internet.
- **Seguretat**: no fa cap recomanació sobre les claus però les claus de la BBDD estan xifrades per evitar que siguin accessibles. Per entrar a la consola es poden crear perfils per limitar l'accés a certes funcionalitats segons l'usuari.

- **Integració amb altres eines**: integra ping, snmpwalk, traceroute, DNS reverse i DNS forward, també permet la incorporació d'altres comandes a través de Zenpacks.
- **Base de dades**: és MySQL, es poden afegir mòduls per gestionar-la i permet fer còpies de seguretat amb les eines que fan la còpia de tot el sistema.
- **Còpies de seguretat i restauració**: té una eina incorporada per fer còpies de seguretat i recuperacions amb molta facilitat.
- **Codi obert**: el codi es modificable per la versió Zenoss Core.
- **Nivell d'ús**: és fàcil d'utilitzar el menú principal per trobar les funcions bàsiques però és difícil d'entendre les funcions de configuració per la quantitat d'opcions i finestres. Podem crear incidents, alertes, els llindars de les alertes, incloure MIB, definir els paràmetres que no reconegui l'eina i modificar les comandes que s'han afegit però per crear estadístiques cal crear un Zenpack específic.
- **Personalització**: és poc adaptable a cada usuari ja que només es pot configurar la pàgina inicial i afegir mapes com Googlemaps o els aportats per l'usuari. Els informes no es poden adaptar a l'usuari.
- **Gestió SLA**: es pot gestionar els SLA amb un paquet específic per a treure les gràfiques de funcionament, anomenat ZenPacks.ipSLA.SLADevice-2.0.1-py2.6.egg
- **Gestió ITIL**: permet la gestió dels paràmetres d'ITIL, inclòs el propi sistema té una CMDB o base de dades adaptada a aqueta normativa.
- **Gestió de pressupostos**: no està suportat.
- **Instal·lació de client**: no calen agents als equips a supervisar.
- **Generació automàtica d'informes**: no ho permet, cal generar-los en el mateix moment per l'usuari.

4.4.4.2. Mecanismes per a recol·lectar la informació

- **Descobriment automàtic de dispositius**: té implementat la cercar de dispositius segons rangs d'adreces, segons ports actius, segons programari,.. .
- **Detecció de caigudes**: té definit com a funcionalitat bàsica "Host Alive" per a fer consultes amb el protocol ICMP. No es poden encadenar els dispositius per només identificar la caiguda de l'equip principal.
- **Programació de llindars**: cada plugin té incorporat el seus llindars i poden ser modificats per l'usuari. Permet enviar SMS, correu electrònic o identificació visual.
- **Recepció d'esdeveniments**: té un dimoni per rebre les notificacions amb el servidor Zentraps, per cada alarma té eines per fer la consulta dels valors que s'han enviat.
- **Prediccions**: ofereix aquesta funcionalitat en la llicència comercial.
- **Accions automàtiques per esdeveniments**: no està implementat.
- **Eines per actuar als dispositius** : incorpora eines per gestionar dispositius com SSH, permet incorporar informació de fabricants per detectar les MIB d'un equip.
- **Correlació d'esdeveniments**: té un zenpack per integrar *Splunk* a Zenoss, com a eina de correlació d'esdeveniments.
- **Filtratge d'esdeveniments**: facilita moltes opcions per filtrar-los, severitat o nivell d'alarma, estat, data, tipus d'esdeveniment, dispositiu,.. .

- **Suportar IP, IPX o IPv6**: està preparat per a treballar amb IPv6 i en MacOS.
- **Eines de suport a MIB**: es poden integrar eines incorporades amb Zenpacks per a interpretar les MIB i fer servir les que ofereix snmpwalk.
- **Inventari**: es pot fer servir com inventari d'equipament, inclús de programari.

4.5. Valoracions de l'entorn de proves

Durant l'elecció de les característiques d'una eina de monitorització Open Source s'ha demanat repartir un pes de 100 entre les diferents aspectes, veure el punt 3.3.2.1, i en l'entorn de proves s'ha descrit el comportament de l'eina per cadascun d'ells, llavors en aquest apartat s'ha puntuat cada característica amb aquest barem:

- 0 si no compleix o si només compleix la versió comercial
- 0,5 si compleix en part la descripció de la característica
- 1 si compleix la descripció de la característica

El resultat de multiplicar el valor del pes per la puntuació que ha obtingut segons aquets criteris, així situarem en una posició a cada eina segons les característiques valorades. També s'ha indicat en color l'opció que està millor situada per a superar aquella característica, per exemple en l'aspecte de la seguretat a diferència de la resta Zenoss xifra la comunicació entre l'eina i la BBDD.

CONCEPTE		PES	Nagios		Pandorafms		Zenoss	
			Punts	total	Punts	total	Punts	total
Característiques generals	Instal·lació	2,00	1	2	1	2	1	2
	Manual i ajuda	6,00	1	6	1	6	0,5	3
	Seguretat	6,60	0,5	3,3	0,5	3,3	0,5	3,3
	Integració amb altres eines	5,00	0,5	2,5	0	0	1	5
	Base de dades	4,00	1	4	1	4	1	4
	Còpies de seguretat i restauració	3,00	0,5	1,5	1	3	1	3
	Codi obert	1,40	1	1,4	1	1,4	1	1,4
	Nivell d'ús	4,60	0,5	2,3	1	4,6	0,5	2,3
	Personalització	4,20	0	0	0	0	0	0
	Gestió SLA	3,80	1	3,8	1	3,8	1	3,8
	Gestió de pressupostos	0,80	0	0	0	0	0	0
	Gestió ITL	2,20	0,5	1,1	0,5	1,1	0,5	1,1
	Instal·lar clients	1,40	0	0	0	0	1	1,4
	Generació automatitzada d'informes	4,80	0	0	0	0	0	0

Mecanismes per a recol·lectar la informació	Descobriment automàtic de dispositius	2,60	0	0	1	2,6	1	2,6
	Detecció de caigudes	6,60	0,5	3,3	0,5	3,3	0,5	3,3
	Programació de llindars	6,00	1	6	1	6	1	6
	Recepció d'esdeveniments	6,60	1	6,6	0,5	3,3	1	6,6
	Prediccions	3,00	0	0	0	0	0	0
	Accions automàtiques per esdeveniments	3,00	0	0	0	0	1	3
	Eines per actuar als dispositius	2,80	0	0	0,5	1,4	0,5	1,4
	Correlació d'esdeveniments	5,20	1	5,2	0,5	2,6	1	5,2
	Filtratge d'esdeveniments	4,80	1	4,8	1	4,8	1	4,8
	Suportar IP, IPX,IPv6	3,60	1	3,6	1	3,6	1	3,6
	Eines de suport a MIB	4,20	0,5	2,1	0	0	0,5	2,1
	Inventari	1,80	0	0	0	0	1	1,8
			59,5		56,8		70,7	

Taula 5 valoracions de l'entorn de proves

A la següent taula s'ha extret un resum del compliment de les característiques i de les més fàcilment millorables, així ens permet preveure quines possibilitats hi ha de creixement.

Resum compliment	Nagios	Pandorafms	Zenoss
Característiques no compleix	9	9	4
Característiques compleix a mitges	7	6	7
Característiques que compleix	10	11	15
Característiques millorables		2 (amb 0) 1 (amb 0,5)	4 (amb 0,5)

Taula 6 compliment de les característiques a valorar

En la següent taula s'han extret les característiques que les tres eines compleixen i les que no compleixen cap. A les primeres s'hauria de qüestionar si aporten alguna cosa ja que no tenen cap impacte entre aquestes eines. De les segones s'ha confirmat que són assequibles per aquest tipus d'eines, per que eines comercials com HPOpenView ofereixen aquestes característiques.

Característiques que compleix tots	**Característiques que cap compleix**
Instal·lació Base de dades Codi obert Gestió SLA Programació de llindars Filtratge d'esdeveniments Suportar IP, IPX,IPv6	Gestió de pressupostos Generació automatitzada d'informes Prediccions

Taula 7 característiques que compleixen tots o cap

L'eina que obté una millor valoració és Zenoss i les altres dues estarien més igualades, encara que Pandora compleix amb més característiques és Nagios qui té

s'adequa millor als aspectes més valorats. Senoss torna a anar davant de les eines que tenen possibilitat de millora, seguit per Pandora i Nagios, encara que amb aquest sistema de valoració no es té en compte el potencial de la comunitat de Nagios. Entre les característiques destaca que la "generació automatitzada d'informes", les "prediccions" i la "gestió de pressupostos" ningú aconsegueix cap puntuació i que set tots tenen el valor màxim.

5. Conclusions

El resultat ha estat satisfactori i ha assolit l'objectiu proposat, sobre la metodologia crec que es podria ampliar el nombre de persones i de diferents àmbits que participen per determinar les característiques de les eines de monitorització amb la intenció de obtenir un llistat més adaptat a totes les parts afectades.

En general totes les eines cobreixen les possibilitats mínimes i utilitzen els mecanismes per consultar informació descrits en aquets projecte, només Zenoss també incorpora les comandes SSH o Telnet.

En la meva opinió Nagios és l'estàndard que tothom ha seguit i té moltes aportacions de la comunitat en plugins i millores, segurament pel temps que funciona, però el seu entorn de treball amb fitxers és ferragós de manegar, els informes gràfics són pobres i també la seva interfície gràfica, hi ha entorn gràfics que milloren aquests aspectes però durant les proves he fet servir Centreon que han finalitat en dues instal·lacions de la còpia de seguretat. És l'eina perfecte per monitoritzar amb personal informàtic o especialitzat per aprofitar tot el que ofereix la seva comunitat i no ser massa exigent a l'aspecte dels informes.

Pandora cobreix totes les necessitats bàsiques per la supervisió sense cap problema, l'ús és molt intuïtiu, senzill i per afegir supervisions als agents incorpora un llenguatge molt fàcil, però sembla tenir una comunitat menys activa i ha estat l'eina que he tingut més problemes durant la instal·lació: s'ha bloquejat dues vegades, el correu no funcionava encara que es veien al fitxer de log, el protocol WMI no funcionava des de el programari i amb la càrrega de Googlemaps es va alentir tota l'aplicació. És una eina molt bona per qui vulgui complicar-se poc, tenir les eines per monitoritzar i extreure informes detallats i visuals.

En la primera visió Zenoss era una eina complicada però aquesta opinió ha anat canviat, sorprèn l'aprofitament que fa de cada mètode de monitorització per obtenir informació, la documentació està molt bé estructurada, l'eina és lenta per a treballar pel que caldria validar si aquest comportament empitjora amb molts dispositius per supervisar i preocupa veure que els Zenpacks anteriors necessiten validar el seu funcionament a la nova versió. Caldria saber el nivell de dependència amb Nagios per que podria ser un problema, encara que sembla aprofitar el gran desplegament que ofereix l'altre. És l'eina que recomanaria a qui vulgui molta informació i tingui intenció de dedicar-li temps per que té moltes possibilitats, és molt interessant el control de serveis en el núvol si es té intenció d'utilitzar-lo a mig termini.

La valoració final s'hauria de prendre com una referència entre eines i no com un valor quantitatiu. És més important el mètode que el resultat final, per que si ens calgués fer una valoració similar hauríem de començar identificant les característiques particulars del client i després seguir la metodologia descrita. S'ha de mencionar que les valoracions obliguen a fer una reflexió de la metodologia emprada, sobretot a l'escollir les característiques, doncs destapa 10 (aproximadament un 40%) que no aporten res, pel que caldria plantejar-nos si són massa obvies o si no aporten res a l'estudi (un exemple, que no aporta res, és valorar "codi obert" en eines Open Source).

Per futurs projectes crec que seria interessant:

- incorporar a la comparativa versions de prova de les eines comercials d'aquests productes, inclòs, si es disposa de medi tècnics, es podria incloure eines líders del mercat com HPOpenView o Tivoli.
- escollir les eines Open Source que poden aportar alguna novetat en aquest camp i que no siguin conegudes, per donar-li una empenta.
- fer les proves sobre entorns més actuals: VMWare, serveis web, cloud,.., encara que s'hauria d'anar en compte si són serveis en producció.
- millorar la selecció de les característiques fent participar a persones amb experiència en altres aspectes de la monitorització, un lloc on trobar-los és a l'UOC.

6. Glossari

ACPI (Advanced Configuration and Power Interface): especificació que permet gestionar la energia del maquinari amb els sistemes operatius.
ADDON: (a Nagios) aplicació per ampliar funcionalitats a Nagios.
CENTREON: addon per incorporar una interfície web per la configuració de Nagios.
COMMUNITY: clau per protegir l'accés a un dispositiu en xarxa per SNMP.
CLOUD o *cloud computing:* model per oferir serveis distribuïts en una xarxa mallada en forma de núvol.
DNS reverse: servei UDP que associa IP a adreces d'Internet.
DNS forward: servei UDP que associa adreces d'Internet a IP.
ESDEVENIMENT: qualsevol notificació o successos d'un sistema.
GARTNER: empresa dedicada a l'anàlisi i l'assessorament en tecnologies de la informació
HOST ALIVE: consulta per ICMP per saber si un dispositiu està actiu.
HOST LATENCY: consulta per ICMP per saber la latència fins un dispositiu.
HTTP: protocol per la transferència d'informació per una xarxa IP.
ICMP: (Internet Control Message Protocol): protocol de la capa de xarxa dissenyat pel control de dispositius connectats en xarxes IP.
IP/IPX/IPV6: protocols equivalents de la capa de xarxa
IPSCAN: eina Open Source per fer cerques d'IP i de ports.
ITIL v3: normativa de bones practiques per la gestió de serveis de tecnologies de la informació
LATÈNCIA: temps en recorre la distancia entre dos dispositius en xarxa.
MIB: base de dades estructura en forma d'arbre dels dispositius.
MIB tools:eina Windows per la consulta de la MIB d'un dispositiu.

MÒDUL: (a Pandora) és la implementació d'una consulta.
MRTG: eina Open Source per la consulta de paràmetres SNMP i representa la resposta en una gràfica.
MWIC: eina de Linux per la consulta WMIC a sistemes operatius Windows.
MYSQL: és un sistema de gestió de base de dades relacionals Open Source.
NETSTAT: eina que proporciona l'estat de les connexions TCP i UPD actives en un dispositiu.
NET-SNMP: conjunt d'aplicacions per la gestió remota que utilitzen el protocol SNMP.
NMAP: eina per la consulta dels ports obert d'una IP concreta
NOC (Network Operation Center): servei per la gestió de xarxa remotes.
NRPE: (a Pandora) agent Linux on estan definits els mòduls del sistema on s'allotja.
NSCLIENT++: (a Pandora) agent Windows on estan definits els mòduls del sistema on s'allotja.
OPEN SOURCE: programari que el codi està disponible per modificar-lo.
PING: eina que utilitza el protocol ICMP per enviar un paquet al destinatari.
PLUGIN: (a Nagios) és la implementació d'una consulta.
POLLING: sistema per a consultar a un grup d'adreces.
POP3: protocol per l'enviament de missatges.
RDDTOOLS: és un sistema per emmagatzemar dades en una base de dades circulars.
ROUTER: equip de xarxa que s'encarrega de les comunicacions a nivell de xarxa.
SCRIPT: llenguatge de programació per l'execució d'ordres.
SLA: Acord de nivell de servei o temps acordat per tenir un servei funcionant.
SNMP: protocol per la gestió dels dispositius connectats a una xarxa IP.
SNMPWALK: eina de Linux per la consulta pel protocol SNMP.
SNMP informant: aplicació Open Source que recull els esdeveniments d'un sistema Windows.
SPLUNK: eina Open Source per gestionar molta informació que es fa servir per relacionar esdeveniments.
SSH: eina per la gestió remota de dispositiu.
SSL: protocol per encriptar les dades d'una comunicació.
SUBVERSION: és una aplicació Open Source per controlar versions de documents, programari,..
SYSLOG: estàndard per l'enviament d'esdeveniments.
TCP/IP: conjunt de protocols que formen la torre OSI per la comunicació entre dispositius.
TELNET: eina per la gestió remota de dispositiu.
TEMPLATE: (a Nagios i Zenoss) plantilla que incorpora les característiques generals d'un dispositiu.
TRACEROUTE:
TRAPS: notificacions que envia un dispositiu pel protocol SNMP a la IP de destí configurada.
VMWARE: empresa dedicada a la virtualització de maquinari.
WMI: base de dades que emmagatzema tota la informació per la configuració d'un sistema operatiu Windows.
WMI explorer:
ZENPACK: (a Zenoss) aplicació per ampliar funcionalitats en Zenoss.
ZOPE: programari open Source per un servidor web d'objectes.

Bibliografia

SNMP:
http://www.snmp.com
http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol
http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?objectInput=snmpTrapAddress&translate=Translate&submitValue=SUBMIT
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa5.shtml
http://www.ulpgc.es/otros/tutoriales/tcpip/3376c414.html
MIB:
http://www.coit.es/publicac/publbit/bit102/quees.htm
http://www.networkmanagementsoftware.com/
WMI:
http://technet.microsoft.com/es-es/library/cc787057(WS.10).aspx
http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/886/5/T10391CAP2.pdf
Nagios:
http://www.nagios.org/
http://nagios.sourceforge.net/docs/nagioscore/3/en/toc.html
Plugins i addon de Nagios
http://exchange.nagios.org/
http://nagiosplugins.org/
Plugin SNMP: http://nagios.manubulon.com/
Plugin NRPE:
http://anotherhost.homelinux.com/nrpe-nagios-remote-plugin-executor/
http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf
Plugin NSClient++: http://nsclient.org/nscp/
ACPI:
http://www.acpi.info/spec.htm
Pandorafms:
http://pandorafms.org/index.php?lang=es
http://pandorafms.com/
http://openideas.info/wiki/index.php?title=Pandora_2.0:Documentation_es:Introduccion
http://deset.es/es/index.php/esp/pandora-para-sap/descripcion-de-pandora-fms-for-sap.html
Zenoss:
http://www.zenoss.com/
http://community.zenoss.org/index.jspa
Zenpack Fping
http://community.zenoss.org/docs/DOC-3467
Consultes SNMP del visor de logs de Windows
http://www.snmp-informant.com/index.htm
http://syslogserver.com/download.html