Monitorització Ambiental d'un CPD basat en codi obert.

Agustí Capdevila Alabart

ETIS

Manel Mendoza Flores

10 de Gener de 2013

TFC - Administració de Xarxes i Sistemes Operatius

Monitorització Ambiental d'un CPD basat en codi obert

Agustí Capdevila Alabart

ETIS

Estudis d'Informàtica i Multimèdia

UOC
Universitat Oberta de Catalunya

Dedicatòries

A la meva dona Anna, amb la que sense la seva ajuda i amor no hauria estat posible arribar fins aquí.

Als meus fills Gerard i Albert, dels que aquest projecte s'ha endut part de la meva dedicació a ells.

A la meva mare pel seu interès i recolzament incondicional.

Al meu pare en particular, que em va deixar fa uns pocs anys (que en pau descansi), i sé que li hauria fet il.lusió veure finalitzada la meva carrera.

Agraïments

A tots els companys que s'han anat creuant i acompanyant en aquest llarg camí.

A tots els professors, consultors i tutors que amb el seu coneixement i dedicació m'han anat resolent els dubtes.

Resum

Els avanços tecnològics han facilitat el desenvolupament de les Tecnologies de la informació i les Comunicacions, que s'han integrat perfectament en molts àmbits com l'empresarial, educatiu i científic.

En un àmbit empresarial, moltes organitzacions disposen de sistemes informàtics i de centres de processament de dades centralitzats, que cada vegada més poden estar compartits entre varies empreses. Per tant, aquests centres poden estar físicament separats dels punts de suport informàtic propis de cada empresa, però amb necessitats de treballar conjuntament.

També l'elevat grau de dependència tecnològica, suposa que les organitzacions tinguin condicionada la seva gestió del negoci amb el correcte funcionament dels equips informàtics i de comunicació, per tal de poder garantir les seves dades.

Amb la monitorització podem detectar quan es produeix una incidència o una degradació en qualsevol equipament informàtic o de comunicacions i notificar-la a la persona responsable, per tal de prendre les accions correctives de forma proactiva i evitar així qualsevol problema major.

Les eines de monitorització permeten controlar una gran varietat processos com l'estat dels serveis en la xarxa i de paràmetres ambientals, com la temperatura, humitat, etc.

El present TFC està enfocat en la implementació d'un Sistema de Monitorització Ambiental en Centres de Processament de Dades (CPD) basat en maquinari compatible i programari obert. La solució té com a objectiu definir els trets bàsics i la viabilitat d'aquests sistemes, perquè qualsevol organització tingui les nocions bàsiques per l'aquisició d'un sistema de monitorització adaptat al seu CPD.

Per arribar a aquest objectiu caldrà:

- Fer un estudi de mercat del programari obert disponible i les seves versions. Definir les seves característiques i funcionament principals. Determinar la millor opció, amb un análisis comparatiu de les eines estudiades.
- Avaluar els principals paràmetres ambientals a monitoritzar en un CPD, quins estàndars o protocols tenen aquest sensors i conèixer les principals característiques dels sensors ambientals.
- Definir les característiques, funcions, configuració i els requisits d'instal.lació de la plataforma de monitorització escollida.
- Definir els conceptes bàsics, principis de funcionament, tipus i implementació dels principals sensors per monitorització ambiental i dels seus dispositius recol.lectors de dades.
- Avaluar els costos econòmics en base a proveïdors especialitzats en monitorització ambiental i determinar la viabilitat de la solució.

Índex

Índex de Continguts

Resum 3
Índex 4
Índex de Continguts 4
Índex de Figures 5
1 Introducció 6
1.1 Justificació del TFC i context 7
1.2 Objetius del TFC 7
1.3 Enfocament i mètode a seguir 7
1.4 Planificació del projecte 8
1.4.1 Calendari i dates clau 8
1.4.2 Desglossament de tasques a realitzar 8
1.4.3 Diagrama de Gantt: 9
1.5 Anàlisis de riscos 10
1.6 Productes obtinguts 10
2 Cos de la Memòria 11
2.1 Marc Tecnològic 11
2.1.1 Antecedents i estat de l'art 11
2.1.2 Introducció a la monitorització de sistemes. 12
2.1.3 Introducció als sensors de variables ambientals. 21
2.1.4 Protocol SNMP 24
2.2 NAGIOS com a plataforma de Monitorització. 26
2.2.1 Estructura del sistema 27
2.2.2 Funcionament 28
2.2.3 Configuració 29
2.2.4 Preparació de l'entorn 30
2.2.5 Instal.lació bàsica de Nagios. 31
2.2.6 Monitorització de serveis i equips. 38
2.2.7 Altres eines associades a Nagios. 41
2.3 Sensors Ambientals 43
2.3.1 Sensors de Temperatura 43
2.3.2 Sensors d'Humitat 45
2.3.3 Sensors per detecció d'aigua 47
2.3.4 Sensors per detecció de fum 48
2.3.5 Altres sensors 49
2.3.6 Recollida i monitorització dades 50
2.3.7 Solució de monitorització ambiental 51
2.4 Valoracions econòmiques 54
3 Conclusions 56
Glosari 57
Bibliografía i Refèrencies 59
Annexos 61
Annex A – Detall equipament monitor Room Alert 24E 61
Annex B – Detall equipament monitor TempPageR 3E 62
Annex C – Scripts d'exemple configuració sensors en Nagios 63

Índex de Figures

Figura 1: Diagrama de Gantt 9
Figura 2: Comparativa gràfica de plataformes de monitorització. 20
Figura 3: Esquema funcionament del protocol SNMP. 25
Figura 4: Arquitectura de Nagios 27
Figura 5: Estructura arxius configuració de Nagios 29
Figura 6: Pantalles dels entorns màquina VirtualBox i Sistema Operatiu Ubuntu 30
Figura 7: Captura de configuració personalitzada de l'arxiu contacts.cfg 33
Figura 8: Captura del fitxer de verificació d'errors 35
Figura 9: Captura de la interface Web de Nagios 36
Figura 10: Captura dels serveis en curs de Nagios amb warning SSH 36
Figura 11: Captura dels serveis en curs de Nagios sense warnings 37
Figura 12: Captura del fitxer de configuració nagios.cfg 38
Figura 13: Definició host Ubuntu 39
Figura 14: Definició serveis Ubuntu 39
Figura 15: Definició host RouterADSL 40
Figura 16: Definició serveis RouterADSL 40
Figura 17: Exemple de monitorització amb Nagios 41
Figura 18: Arquitectura N2RRD 42
Figura 19: Esquema d'un termoparell 43
Figura 20: Circuit excitació d'una RTD 44
Figura 21: Circuit excitació d'un termistor 44
Figura 22: Principi del Sensor Humitat capacitiu. 45
Figura 23: Sensor Humitat resistiu 46
Figura 24: Detall Detector de líquids tipus puntual 47
Figura 25: Detall Cable Detector de líquids 47
Figura 26: Principi del detector de fum fotoelèctric 48
Figura 27: Detector de fallada d'energia 49
Figura 28: Arquitectura Monitorització Distribuida 50
Figura 29: Especificacions i detall del sensor Temperatura AVTECH 51
Figura 30: Especificacions i detall del sensor Temperatura i Humitat AVTECH 51
Figura 31: Especificacions i detall del sensor d' inundació AVTECH 51
Figura 32: Especificacions i detall del sensor de fum AVTECH 51
Figura 33: Especificacions i detall del Power Sensor AVTECH 52
Figura 34: Especificacions i detall del Room Entry Sensor AVTECH 52
Figura 35: Especificacions i detall del Monitor Room Alert 24E AVTECH 52
Figura 36: Especificacions i detall del TempPageR 3ER AVTECH 52
Figura 37: Esquema distribució sensors i monitors ambientals en un CPD 53
Figura 38: Taula valoració econòmica Sistema Monitorització 54

1 Introducció

Cada vegada més, les empreses i organitzacions conscients de la importància de la informació i que aquesta és subsistència, han derivat les seves dades cap els Centres de Processament de Dades, en endavant CPD.

Així doncs, un CPD (en anglès "*Data Center*") és bàsicament un edifici que conté una gran quantitat d'equipament electrònic, com Servidors, Sistemes d'emmagatzematge de dades, equips de comunicacions, etc.

Aquest són creats i mantinguts per organitzacions, on la principal motivació és guardar i mantenir aquesta informació, que en molts casos és crítica, i oferir una protecció física de la infraestructura informàtica.

Per això, hi ha disponible actualment molta normativa i estàndards de disseny d'aquests CPD, on el més emprat i que valora alhora el seu nivell de disponibilitat és el TIA-942. Aquest estàndard inclou també quatre nivells TIER per determinar el grau de disponibilitat en la infraestructura de les instal·lacions del CPD.

Amb tot però, un CPD ha de tenir en compte també altres factors, com la seva fiabilitat i seguretat, que sigui modular, escalable i ecològic. Per tot això i basat en els estàndars abans indicats, es doten els CPD d'equips redundants de climatització, sistemes d'alimentació ininterrompuda i distribució d'energia redundants, control d'accessos i seguretat física, sistemes de videovigilància etc.

Però què passa dins d'un CPD malgrat tota la infraestructura indicada?. Qui controla la temperatura dins d'un CPD, la humitat, si ha fum, si es produeixen possibles inundacions d'aigua, les pertorbacions elèctriques dels servidors i altres paràmetres ambientals?

La disponibilitat de la infraestructura d'un CPD és un dels requisits bàsics dels processos diaris de les empreses i organitzacions. La seva seguretat comença en cada un dels armaris de servidors, continua en tot el CPD i s'acaba monitoritzant en una sala segura, de manera que així es garanteixi un desenvolupament segur i regulat del processos, apart de la seva optimització i estalvi energètic.

Per tant, si analitzem l'evolució que els darrers anys han tingut les infraestructures tecnològiques i en base al seu creixement, és de vital importància tenir cura de les instal·lacions tècniques que ofereixin les condicions necessàries per el correcte funcionament del maquinari, a la vegada que tinguin en compte aspectes tan importants com la disponibilitat dels serveis del CPD.

Per aconseguir aquest objectiu, una de les possibles solucions o així com els aspectes estratègics sobre les instal·lacions tècniques o infraestructures IT a tenir en compte, són **la monitorització de l'eficiència i les condicions ambientals**.

1.1 Justificació del TFC i context

Per al creixement expansiu dels serveis tecnològics i les necessitats de garantir les dades de les empreses, els CPD han evolucionat de manera exponencial i estant recolzats per molts estàndards i normes relacionades amb el seu disseny i en funció de la seva mida.

També s'ha donat molta importància als sistemes de climatització, protecció física, sistemes contra incendis, etc, però realment n'hi ha prou? Cal esperar que un servidor es cremi davant d'un problema en el sistema de climatització, si podem evitar un desenllaç fatal per la infraestructura IT sent més proactius amb un sistema de monitorització?.

Probablement tindrem encara molts CPD que els hi falta un sistema de monitorització ambiental, que pugui controlar i gestionar la salut dels servidors, discos, bases de dades i aplicacions abans que pugui haver una caiguda integral del mateix.

Per tant és aquí on entren en acció els sensors ambientals que permeten monitoritzar la temperatura, la humitat, possibles riscos d'inundació, falles d'alimentació, etc., a més d'un ampli ventall d'eines i software de monitorització que permeten la seva gestió, creació d'alarmes, gràfics de tendències i altres avisos que puguin evitar un desastre en el CPD i pèrdua d'informació critica.

La solució és conèixer tots aquest sistemes de monitorització per tal que les organitzacions que encara no disposen d'aquests, puguin tenir una idea de com implementar-ho i establir noves estratègies que puguin garantir la seguretat de les seves dades.

1.2 Objetius del TFC

Els objectius principals desitjats per complir en la realització d'aquest TFC són:

- ✓ Obtenir els coneixements necessaris sobre les plataformes de monitorització ambiental existents i fer un anàlisis per escollir la més adequada.
- ✓ Obtenir els coneixements necessaris de l'entorn tecnològic sobre sensors i monitors ambientals, les seves funcionalitats, protocols, distribuïdors e implementació.
- ✓ Definir totes les parts i fases necessàries per la implantació dels dispositus de monitorització, perquè puguin orientar a una organització o empresa a escollir la solució més adaptable a les seves necessitats, complint criteris d'escalabilitat, flexibilitat, compatibilitat, etc.
- ✓ Definir una possible solució per comprovar la viabilitat de la mateixa, per tal de garantir en tot moment i com objectiu més prioritari, que la implantació d'aquests sistemes sigui el més adequat i rentable possible sense costos addicionals per l'empresa. És a dir, que la despesa econòmica en aquesta inversió sigui la mínima. Per cobrir aquest requisit s'intentarà la utilització de codi lliure i sensors compatibles amb els estàndards de facto.

1.3 Enfocament i mètode a seguir

El cicle de vida escollit és en cascada, on les etapes que formen el projecte s'organitzaran de manera que no comenci una fins que no hagi finalitzar l'anterior.

En principi les fases del cicle de vida bàsiques seran la definició del treball que volem realitzar, la planificació del mateix, la seva execució, revisió i finalització.

Per a assolir els objectius, el projecte es subdivideix en una sèrie de tasques que segueixen el cicle de vida esmentat en base a una temporització marcada en un calendari de treball. Aquest calendari té unes dates clau, o fites, en les quals s'han de fer lliuraments parcials del treball (o PAC's).

1.4 Planificació del projecte

Una vegada definits els objectius del TFC i el mètode a seguir per aconseguir el seu desenvolupament, es definiran les activitats previstes per arribar a la solució final.

1.4.1 Calendari i dates clau

Les dates claus per la realització del TFC estan relacionades amb les previstes en la temporització de l'assignatura i són les següents :

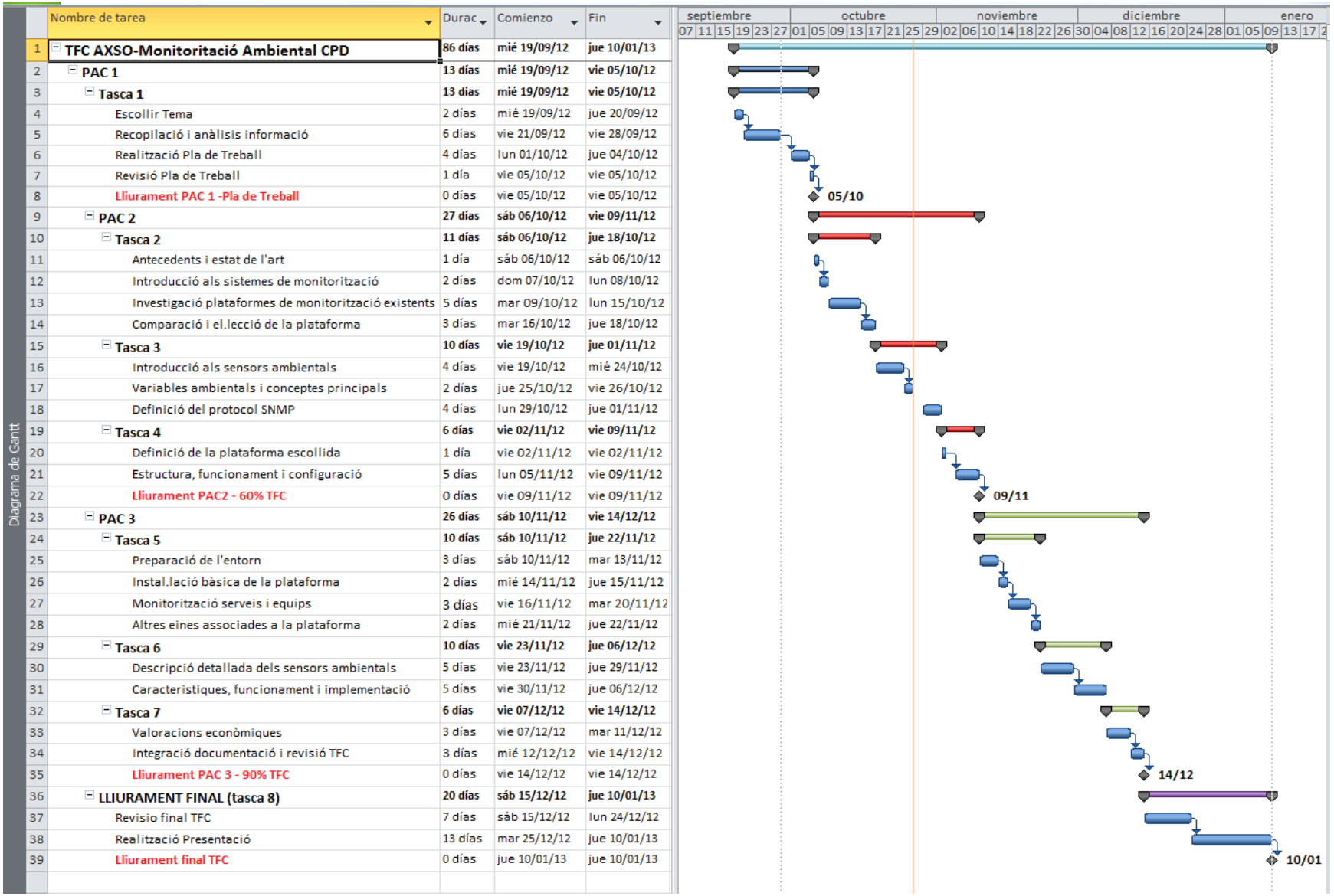
Resum Dates Clau		
Descripció	***Activitat Acadèmica***	***Data planificada***
Data Inici TFC		19/09/2012
Lliurament Pla de Treball	PAC 1	05/10/2012
Lliurament TFC en avançament del 50%	PAC 2	09/11/2012
Lliurament TFC en avançament del 90%	PAC 3	14/12/2012
Entrega Memòria i Presentació TFC	ENTREGA FINAL	10/01/2013

1.4.2 Desglossament de tasques a realitzar

En resum, les tasques a realitzar seran les següents :

- **Tasca 1**:
  - Elecció i recopilació d'informació del tema seleccionat.
  - Anàlisi del treball a realitzar i planificació de les activitats a desenvolupar.
  - Realització Pla de Treball i entrega PAC1
- **Tasca 2**:
  - Definició dels antecedents i estat de l'art.
  - Introducció als sistemes de monitorització ambiental
  - Investigació plataformes de monitorització existents.
  - Comparació d'aquests sistemes de monitorització i el.lecció de la plataforma
- **Tasca 3**:
  - Introducció als sensors ambientals.
  - Variables ambientals i conceptes principals.
  - Definició del protocol SNMP.
- **Tasca 4**:
  - Definició de la plataforma de monitorització ambiental a utilitzar.
  - Estructura, funcionament i configuració.
  - Revisió i entrega PAC2
- **Tasca 5**:
  - Preparació de l'entorn.
  - Instal.lació bàsica de la plataforma.
  - Monitorització serveis i equips.
  - Altres eines associades a la plataforma
- **Tasca 6**:
  - Descripció detallada del sensors ambientals.
  - Característiques, principis de funcionament i implementació de la solució.
- **Tasca 7**:
  - Valoracions econòmiques.
  - Finalització memòria, integració i estructuració de tota la documentació disponible.
  - Maquetació, revisió final i entrega PAC3
- **Tasca 8**:
  - Elaboració de la Presentació, revisió Memòria i entrega final TFC.

1.4.3 Diagrama de Gantt:



	Nombre de tarea	Durac	Comienzo	Fin
1	**TFC AXSO-Monitoritació Ambiental CPD**	**86 días**	**mié 19/09/12**	**jue 10/01/13**
2	**PAC 1**	**13 días**	**mié 19/09/12**	**vie 05/10/12**
3	**Tasca 1**	**13 días**	**mié 19/09/12**	**vie 05/10/12**
4	Escollir Tema	2 días	mié 19/09/12	jue 20/09/12
5	Recopilació i anàlisis informació	6 días	vie 21/09/12	vie 28/09/12
6	Realització Pla de Treball	4 días	lun 01/10/12	jue 04/10/12
7	Revisió Pla de Treball	1 día	vie 05/10/12	vie 05/10/12
8	Lliurament PAC 1 -Pla de Treball	0 días	vie 05/10/12	vie 05/10/12
9	**PAC 2**	**27 días**	**sáb 06/10/12**	**vie 09/11/12**
10	**Tasca 2**	**11 días**	**sáb 06/10/12**	**jue 18/10/12**
11	Antecedents i estat de l'art	1 día	sáb 06/10/12	sáb 06/10/12
12	Introducció als sistemes de monitorització	2 días	dom 07/10/12	lun 08/10/12
13	Investigació plataformes de monitorització existents	5 días	mar 09/10/12	lun 15/10/12
14	Comparació i el.lecció de la plataforma	3 días	mar 16/10/12	jue 18/10/12
15	**Tasca 3**	**10 días**	**vie 19/10/12**	**jue 01/11/12**
16	Introducció als sensors ambientals	4 días	vie 19/10/12	mié 24/10/12
17	Variables ambientals i conceptes principals	2 días	jue 25/10/12	vie 26/10/12
18	Definició del protocol SNMP	4 días	lun 29/10/12	jue 01/11/12
19	**Tasca 4**	**6 días**	**vie 02/11/12**	**vie 09/11/12**
20	Definició de la plataforma escollida	1 día	vie 02/11/12	vie 02/11/12
21	Estructura, funcionament i configuració	5 días	lun 05/11/12	vie 09/11/12
22	Lliurament PAC2 - 60% TFC	0 días	vie 09/11/12	vie 09/11/12
23	**PAC 3**	**26 días**	**sáb 10/11/12**	**vie 14/12/12**
24	**Tasca 5**	**10 días**	**sáb 10/11/12**	**jue 22/11/12**
25	Preparació de l'entorn	3 días	sáb 10/11/12	mar 13/11/12
26	Instal.lació bàsica de la plataforma	2 días	mié 14/11/12	jue 15/11/12
27	Monitorització serveis i equips	3 días	vie 16/11/12	mar 20/11/12
28	Altres eines associades a la plataforma	2 días	mié 21/11/12	jue 22/11/12
29	**Tasca 6**	**10 días**	**vie 23/11/12**	**jue 06/12/12**
30	Descripció detallada dels sensors ambientals	5 días	vie 23/11/12	jue 29/11/12
31	Caracteristiques, funcionament i implementació	5 días	vie 30/11/12	jue 06/12/12
32	**Tasca 7**	**6 días**	**vie 07/12/12**	**vie 14/12/12**
33	Valoracions econòmiques	3 días	vie 07/12/12	mar 11/12/12
34	Integració documentació i revisió TFC	3 días	mié 12/12/12	vie 14/12/12
35	Lliurament PAC 3 - 90% TFC	0 días	vie 14/12/12	vie 14/12/12
36	**LLIURAMENT FINAL (tasca 8)**	**20 días**	**sáb 15/12/12**	**jue 10/01/13**
37	Revisio final TFC	7 días	sáb 15/12/12	lun 24/12/12
38	Realització Presentació	13 días	mar 25/12/12	jue 10/01/13
39	Lliurament final TFC	0 días	jue 10/01/13	jue 10/01/13

Figura 1: Diagrama de Gantt

1.5 Anàlisis de riscos

És habitual en tot projecte fer un anàlisis i mesurar possibles riscos. En aquest apartat voldria avaluar algunes possibles incidències que podrien sorgir al llarg de la realització del TFC i establir si cal algunes possibles solucions.

- ***Motius de salut*:** seria una contingència imprevista, donat que en principi al meu historial clínic no hi ha factors de risc. Una malaltia o accident, serien el màxim risc que podria afectar la realització del meu TFC i que en funció de la gravetat clínica que pogués sorgir, malgrat tot, intentaria donar prioritat al TFC dins de les meves possibilitats i de la meva recuperació física òptima.
- ***Motius laborals:*** en principi no presenta cap risc la meva compatibilitat laboral amb la realització del TFC, ja que en tota la meva carrera he efectuat els meus estudis en aquestes condicions, amb l'únic impacte del temps de dedicació que ha influït proporcionalment en el termini de la mateixa. En el meu cas personal i com a responsable de projectes d'automatització, és habitual que tingui que efectuar desplaçaments fora de la meva residència habitual i en mols casos desplaçaments prolongats a l'estranger.

  Malgrat aquesta situació, no seria inconvenient poder seguir treballant amb el TFC donades les circumstàncies, gràcies a la metodologia d'estudi a distància de l'UOC que ho facilita, però crec que cal avaluar el risc, donat que en aquest cas seria una falta de dedicació temporal i perfectament recuperable.
- ***Incidències del punt de treball***: Un altre factor de risc podria ser la fallada del meu punt de treball (un PC de sobretaula) per motius d'avaria del disc, virus o altra defecte de maquinari. Aquest factor és força previsible i no seria la primera vegada que la he patit. Per aquest motiu disposo d'un PC portàtil, del que tinc rèplica idèntica del meu treball, a més de còpies de seguretat en un disc extern. Així doncs un error en qualsevol dels dos equips, no suposaria la pèrdua total del treball.

1.6 Productes obtinguts

Els entregables que formen part d'aquest Treball Final de Carrera seran els seguents:

- El Pla de Treball, que recull la planificación y estimació de les activitats necesaries per arribar als objectius indicats.
- La present Memòria, que és el document que detallará el treball realitzat. Inclourà tota la información necessaria per comprendre la solució plantejada.
- La Presentació, que resumirá de manera clara i sintètica el treball realitzat i els resultats obtinguts.

2 Cos de la Memòria

2.1 Marc Tecnològic

En el present capítol es presenta la base teòrica i entorn tecnològic més actual dels sistemes de monitorització ambiental. Es definiran les plataformes de monitorització existents, els protocols emprats i les tecnologies més habituals en sensors per la mesura de variables ambientals.

2.1.1 Antecedents i estat de l'art

La monitorització ha tingut aquests darrers anys un fort creixement gràcies a la necessitat de controlar la infraestructura informàtica i sobretot una eina enfocada als administradors de sistemes amb la finalitat de poder fer una gestió proactiva i evitar possibles riscos d'un incident que pugui malmetre els equips informàtics o de comunicacions.

Per tal de reduir el temps de resolució d'incidents, calen eines de monitorització de sistemes de manera que aquestes ens permetin estar informats de l'estat dels equips informàtics les 24 hores del dia durant 365 dias del any.

Les xarxes cada vegada més suporten serveis estratègics i els servidors guarden dades crítiques que cal salvar davant de qualsevol incidència. Per aquest fet, els sistemes de monitorització han de ser cada vegada més complerts i amb un alt nivell d'exigència, per poder detectar i corregir problemes en el maquinari i programari, i poder enviar avisos, crear alarmes i definir gràfics que permetin a l'administrador de sistemes actuar en conseqüència.

Les plataformes de monitorització conjuntament amb els sensors ambientals conformaran els elements clau per garantir la qualitat de la infraestructura informàtica, com a principal avantatge d'aquests sistemes.

Actualment hi ha disponible una gran varietat de programari de monitorització, entre els que cal diferenciar entre els de programari lliure i programari comercial.

- **Programari Lliure**: són eines de lliure distribució i en general de disponibilitat gratuïta, malgrat que no sempre està garantirà la seva gratuïtat condicionada a distribucions més complertes. L'autor del programari pot establir també una llicència pel producte, doncs no significa que sigui de domini públic. Com principals avantatges són el seu baix cost d'adquisició i la innovació i correcció d'errors per part de qualsevol usuari. D'aquest programari hi han les següents plataformes: Pandora FMS, Nagios, Hyperic, Zabbix, Zenoss, Ganglia, OpenNMS, Cacti, Munin, etc.
- **Programari Comercial** : són eines conegudes també com a programari propietari o privat i de les que l'usuari té un ús limitat en quant a modificació i redistribució. El propietari del programari té els drets d'autor i pot restringir els drets de l'usuari, emprant la seva utilització amb finalitats productives i de benefici, establint un accord o contracte amb el client. Entre el programari privat tenim les següents plataformes: BMC Patrol, HP Open View, IBM Tivoli , OpManager.

En quant als sensors, ni han de molts tipus tant per mesurar variables ambientals, elèctriques, de seguretat,etc., així com un un ampli ventall de fabricants.

Entre les principals tecnologies, hi trobem dos grups disponibles de sensors: els intel·ligents plug-and-play amb cablejat tradicional o bé amb tecnologia inal.làmbrica, ambdós connectats a controladors o passarel·les per tal de tractar la seva senyal i que suporten el protocol de facto SNMP.

2.1.2 Introducció a la monitorització de sistemes

En aquest apartat definirem la monitorització de sistemes i quins conceptes cal tenir en compte per poder escollir un sistema de monitorització, a més d'evaluar les principals plataformes de monitorització existents per treuren conclusions i optar per la més óptima.

2.1.2.1 Definició d'un sistema de monitorització

Per monitorització podríem entendre tot tipus d'anàlisis de manera periòdica d'un sistema, del que poguem extreuren dades del seu estat actual, es a dir fer un escaneig d'un sistema cada cert interval de temps.

Dit d'altra manera, la monitorització és un cas particular de la interpretació, que consisteix en la comparació contínua dels valors de les senyals o dades d' entrada i uns valors que actúen com a criteri de normalitat o estándars.

En un àmbit de manteniment predictiu, els sistemes de monitorització s'utilizen també com eines de diagnóstic. Es tracta d'un programari que pugui determinar en cada moment el estat de funcionament de sistemes informàtics més simples als més complexes, avançant-se en les possibles incidències que puguin sorgir.

Quant en una monitorització tenim que el sistema a analitzar està a una certa distància s'està parlant del concepte de remot.

2.1.2.2 Impactes d'un sistema de monitorització ambiental

Un sistema de monitorització pot tenir els següents impactes:

- Millora de la productivitat
- Eficiència energètica.
- Anticipació de problemes.
- Detecció i avís d'incidents.

2.1.2.3 Conceptes per la implementació d'un sistema de monitorització

Per a implementar un sistema de monitorització primer s'ha de fer un anàlisi detallat de la infraestructura informática que volem monitoritzar i així detectar els sistemes crítics de manera que es puguin establir les polítiques d'actuació davant les incidències d'aquests sistemes.

Una vegada es tingui clar que és el que volem monitoritzar, s'ha de fer un pla d'instal·lació i integració del nostre sistema tenint en compte que cal mantenir la seguretat existent, minimitzar l'impacte en el sistema i com actuar si és el sistema de monitorització el que falla.

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

- Com volem veure les dades, alarmes, gràfics,... per tenir en compte que han de ser eficients i mostrar els errors fàcilment.
- Quin tipus de connexió entre equips hi ha: com connexions ràpides o connexions lentes on caldria utilitzar agents que ens enviïn la informació al servidor central.
- Quin's són els Sistemes Operatius dels equips a monitoritzar: Linux, Windows,etc.
- Quines són les plataformes de monitorització i amb quin tipus de programari volem treballar, és a dir amb codi obert o amb programari comercial?

2.1.2.4 Estudi i evaluació de les principals plataformes de monitorització

A continuació evaluarem algunes de les principals plataformes de monitorització definint les seves prestacións i principals funcionalitats. Comencerem per les de ***codi lliure***:

- ***Pandora FMS :***

Pandora FMS (on FMS és l'acrònim de Flexible Monitoring System) és un programari de codi obert que monitoritza sistemes, aplicacions o dispositius. Està publicat sota llicència GPL2 GNU General Public License i és OpenSource, tot i que també disposa de una llicència comercial per a Professionals (FMS Enterprise).

És una eina força nova, ja que la primera versió estable va ser llençada el 14 d'octubre del 2004 sota el nom "Pandoramon". Actualment l'última versió és la 4.2 .Pot recollir informació de qualsevol Sistema Operatiu mitjançant agents específics per a cadascuna de les plataformes (GNU/Linux, AIX, Solaris, HP-UX- BSD/IPSO i Windows 2000, XP i 2003).

Serveix per vigilar i analitzar de forma visual tot tipus de sistemes, utilitzant una interfície o entorn web a través del nostre navegador. És una eina modular i flexible, orientada a dades. Pot supervisar tot tipus de paràmetres o serveis, mitjançant agents específics que recullen informació, fins i tot sensors (per exemple: humitat, lluminositat, moviment), electrònica de xarxa, etc.

L'arqitectura de Pandora FMS és modular i descentralitzada, tot s'emmagatzema en una base dades MySQL.

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

Els seus avantatges de Pandora FMS són:

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

Entre els inconvenients que podem trovar són:

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

- ***Zabbix :***

ZABBIX

Zabbix és un sistema de gestió de xarxes creat per Alexei Vladishev. La seva principal funció és monitoritzar i rastrejar l'estat de serveis de xarxes i servidors de xarxes. Està escrit en C i la seva interfície web en PHP. Zabbix es distribueix sota els termes de la versió 2 de la GNU General Public License.

Aquesta eina va començar com un projecte de programari intern en el 1998, però no és fins el 2001 que fou lliberat al públic sota llicència GPL, i es van necessitar 3 anys més fins que va sortir la primera versió estable (2004). La última versió és la 2.0 i és un sistema de monitoratge semi-distribuït amb administració centralitzada que permet l'utilització de nodes de monitoratge remot, i es basa en la instal·lació d'un agent en el client.

Està integrat per tres components: Base de dades, Interfície web i el servei o daemon Zabbix

Té les següents característiques:

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

Entre els avantages tenim :

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

Així com també alguns inconvenients:

- ✓ Potencia o capacitat del programari limitades.
- ✓ Al no tenir una versió Entreprise repercuteix que no tingui un desenvolupament apropiat i poca popularitat entre clients importants asociats als sistemes de monitoriztació.

- ***Zenoss :***

Una altra plataforma de gestió de xarxa i servidors OpenSource és Zenoss Core Versió 3.2.1. El projecte de creació de Zenoss començar el 2005 i va ser iniciat per Erik Dahl i Bill Karpovich, els quals van formar la companyia Zennos Inc. Aquesta empresa és patrocinadora del nucli Zenoss i proporciona suport, manteniment i desenvolupament de productes.

També disposa de dues versions comercials basades en la versió bàsica: Zenoss Service Dynamics Enterprise i Zennos Professional, que inclou funcionalitats addicionals com la supervisió en temps real d'accions programades en aplicacions web, bases de dades o correu electrònic, llindars de predicció, gestió completa de VMware VI3, panells de controls globals, etc. Aquestes versions a més poden oferir suport i manteniment als seus clients i permet la descàrrega d'una versió de proves.

Zenoss Core és un producte de vigilància i seguiment per a una xarxa informàtica i de supervisió d'infraestructures IT. Pot gestionar la configuració, salut, rendiment de dispositius, servidors i aplicacions. Tot això a través d'un únic paquet de integrat de programari. Ofereix monitorització de dispositius i serveis a la xarxa (SNMP, HTTP, POP3, etc.), recursos de maquinari i detecta automàticament nous recursos a la xarxa i canvis en la seva configuració.

Realitza notificacions i alertes basades en un conjunt de regles. És un producte multiplataforma per a suport a clients, incloent: Windows Server (2000, 2003, 2008), XP, Vista, 7, GNU / Linux , Tomcat i servidors Java / JMX.

Zenoss utilitza una tecnologia sense agents (SNMP, SSH, Telnet i WMI) i s'inicia amb una CMBD (Base de dades de la Gestió de Configuració), la qual conté detalls rellevants de cada element, notificacions, alertes i tasques de remediació a fallades. A més, conté un ampli inventari de cada recurs. Quan es descobreix la infraestructura, comença a monitoritzar el rendiment de cada dispositiu. Posteriorment, ofereix la gestió d'esdeveniments, automatització d'alarmes i informes.

L'arquitectura del sistema esta separada i escalonada en quatre parts principals : una capa d'usuari, un altra capa de dades, una de procés i una darrera de col.lecció.

Com avantatges d'aquesta plataforma tenim:

- ✓ Fàcil installació d'extensions o paquets ZenPacks des de la consola web.
- ✓ Suporta i pot per tant executar plugins de Nagios i de Cacti.

Entre els inconvenients:

- ✓ Al no utilitzar tecnologia amb agents en els clients, requereix una configuració prèvia en la instal·lació del protocol SNMP en cada una de les màquines a monitoritzar seguint un procediment diferent segons la versió o tipus de sistema operatiu.
- ✓ Necessita la instal·lació d'altres paquets ZenPacks per monitorització de serveis bàsics com HTTP o FTP, informació del sistema operatiu i alguns recursos maquinari com obtenir informació de la CPU. Amb la qual cosa, la instal·lació pot no arribar a ser suficient, i necessita una actualització per complir funcionalitats bàsiques.
- ✓ La instal·lació de l'eina de l'amfitrió és ràpida, però no cada configuració del client des de la consola web. Per exemple, cal assignar-li una plantilla o template adequada o personalitzada perquè monitoritzi el que necessitem d'aquest dispositiu.
- ✓ Necessita de l'aplicació externa VMplayer per funcionar en sistemes operatius de Microsoft Windows.

➢ ***Nagios :***

Nagios

Nagios Core Versió 3.x és el principal programari lliure orientat al monitoratge des de fa molt temps. És una eina Open Source i està dissenyat i mantingut per Ethan Galstad, autor del programari, juntament amb un grup de desenvolupadors que mantenen diversos plugins. Segons diu el seu propi autor, el significat del seu nom, Nagios, és un acrònim recursiu: "Nagios Ain't Gonna Insist On Sainthood". És una referència a l'encarnació original del programari sota el nom de Netsaint.

Està llicenciat sota la GPL Version 2 publicada per al Programari Fundation. També té una llicència comercial Nagios PoweredTM la qual posa a disposició dels seus clients dos programaris: Nagios XI i OpMon. El primer d'ells, es pot obtenir en base al volum del nostre sistema: entre 50-100 nodes o per nodes il·limitats, i representa la versió de Nagios comercial. El segon, és una solució de govern IT i gestió de processos empresarials i és compatible amb Nagios.

Quant a la seva arquitectura i definició, és un sistema de monitorització monolític i orientat a esdeveniments que vigila els equips, tant del maquinari com programari, alertant quan el comportament dels mateixos no és l'adequat. Pot monitoritzar serveis de xarxa, recursos hosts i pot programar plugins específics per a nous sistemes.

El control remot és emprat a través de túnels SSH o SSL xifrat. Va ser dissenyat per a sistemes GNU / Linux però també funciona en variants Unix.

Està basat en una estructura mestre-esclau on el mestre és el servidor dedicat per Nagios i els esclaus les màquines a monitoritzar.

En cada un dels esclaus o clients a monitoritzar es configuren els plugins o scripts que seran executats per revisar un determinat servei. Aquests scripts poden estar desenvolupats en diferents llenguatges o tecnologies: Perl, C / C + + / C #, Expect / TCL, Bash, Ruby, Python, o PHP. Encara Nagios té opcionalment un intèrpret embegut de Perl que accelera l'execució d'aquests scripts.

Al mestre s'executa una eina de connexió remota, la més habitual és el NRPE, amb la qual el servidor accedeix als plugins o scripts de mesura disponibles i configurats en les màquines remotes o esclaus.

Algunes de les seves principals característiques o funcions poden ser:

- ✓ Supervisió dels serveis xarxa (SMTP, POP3, HTTP, NNTP, PING, etc).
- ✓ Monitorització dels recursos (càrrega de processador, espai en disc, etc).
- ✓ Capacitat per definir una jerarquia de servidors a la xarxa, el que permet la detecció de hosts 'down' o inabastables.
- ✓ Notificació d'errors quan hi ha problemes i quan són resolts mitjançant correu electrònic, buscapersones, SMS, etc.
- ✓ Registre automàtic de rotació de logs.
- ✓ Interfície web per visualitzar l'estat actual de la xarxa amb la possibilitat de generar informes i gràfiques.
- ✓ La seva finalitat principal és el tractament de dades temporals i dades serials com temperatures, transferències en xarxes, càrregues del processador, etc.

Avantatges:

- ✓ És un programari popularment conegut i consolidat, ja que posseeix una gran quantitat de connectors de la comunitat (més de 200) per estendre les seves funcionalitats a través d'innombrables llocs web, que fins i tot són facilitats en el seu manual oficial. Encara que, hi ha etapes de la seva història en la que aquesta comunitat ha estat poc activa pel que fa al desenvolupament de nous avenços sobre el producte.
- ✓ La seva fama ha incentivat noves eines de monitorització que contenen un nucli basat en Nagios, com ara: Opsview o Shinkem.
- ✓ Hi ha bona documentació molt treballada fins i tot en detalls i facilitada per la comunitat.
- ✓ Permet diferenciar entre hosts caiguts o inaccessibles.
- ✓ Posseeix una ordre que revisa i valida els fitxers de text de configuració modificats abans de reiniciar el sistema.
- ✓ Pot acoblar amb una altra aplicació anomenada Centreon per a la gestió i control de qualsevol aspecte de l'eina des d'una interfície web, evitant les modificacions sobre fitxers i per línia d'ordres.

Inconvenients:

- ✓ La instal·lació, configuració i els complements (plugins) està basada en text, la qual cosa implica una dificultat mitjana, inversió de temps i requereix un grau de coneixement tècnic, a més pot resultar una mica tediós. Quan en realitat, la majoria d'aquestes funcions, al voltant del 90% ja són possibles a partir del protocol SNMP.
- ✓ Qualsevol modificació en la configuració requereix un reinici complet del sistema, ja que per exemple, no és capaç d'auto-descobrir nodes nous que s'inclouen al sistema.
- ✓ La seva interfície web només serveix per visualitzar els esdeveniments. Qualsevol canvi s'ha de fer manualment des del servidor de Nagios.
- ✓ No suporta cap gestor de base de dades que treballi sota SQL.
- ✓ No està disponible o no funciona en tots els sistemes operatius, per exemple, en sistemes Microsoft Windows, és a dir, només està disponible per a sistemes GNU Linux i altres unicode. Necessita una eina auxiliar per monitoritzar aquests sistemes que serveixi de proxy o intermediari, per exemple, NSClient + +.
- ✓ Aporta molta informació, però de vegades és poc exhaustiu, ja que no localitza el problema i requereix una interacció propera amb l'eina. A part, que l'històric de dades tampoc és molt recomanable, ja que no utilitza cap tipus de recol·lector de dades per al rendiment.
- ✓ Disposa d'una consola d'esdeveniments molt feble, ja que per exemple no permet configurar accions automàtiques davant nous esdeveniments en el sistema.

- ***OpenNMS :***

OpenNMS és una eina de monitoratge de programari lliure, publicada actualment sota la llicència GPL versió 3 (GNU Public License), de les més antigues que existeixen juntament amb Nagios i coneguda com un dels pares d'aquest tipus d'eines, ja que és un projecte que es va iniciar el 1999 per Steve Giles, Brian Weaver i Luke Rindfuss i la seva empresa PlatformWorks. Actualment s'encarrega del projecte la fundació The Order of the Green Polo (OGP) fundada el 2004 per administrar el projecte, al costat de The OpenNMS Group. Aquesta eina ha estat premiada també amb diversos guardons.

L'última versió de l'eina disponible estable i en producció és la versió 1.8.16, a més segueixen desenvolupant noves versions gràcies a la comunitat, que li permet seguir oferint noves característiques al seu producte.

No disposen d'altres versions diferents de la OpenSource, és a dir, que no disposen d'una versió Enterprise o comercial del seu producte.

És una eina escrita en el llenguatge de programació Java, i per tant, funciona sobre qualsevol plataforma amb suport per a una versió de Java SDK 1.5 o superior. També hi ha paquets binaris precompilats per a Linux, Windows, Solaris o Mac OS X.

OpenNMS va ser dissenyat per oferir disponibilitat i escalabilitat a desenes de milers de nodes i per oferir solucions a empreses.

Entre les funcionalitats de OpenNMS podem destacar que és una eina capaç de:

- ✓ Autodescrubrir dels serveis a la xarxa en la qual està funcionant.
- ✓ Es pot utilitzar la interfície web d'usuari o crear arxius personalitzables de configuració en XML.
- ✓ L'aprovisionament dels processos és asíncron per l'escalabilitat.
- ✓ Pot generar esdeveniments i notificacions o fins i tot rebre de fonts externes, com per exemple, SNMP, syslog o TL / 1.
- ✓ Pot processar 125.000 missatges de syslog per minut de forma contínua i enviar aquestes notificacions mitjançant correu electrònic, XMPP, SMS
- ✓ Podent generar informes detallats i representacions gràfiques sobre la disponibilitat d'aquests serveis i configurar els temps d'inactivitat, a partir de les dades recollides a la base de dades, la qual cosa ajuda a identificar els problemes dins de la xarxa.

Avantatges:

- ✓ Disposa d'un sistema de notificacions molt flexible, ja que pot gestionar i enviar fins i tot a una eina exterior (JIRA, OTRS, etc.) centralitzant així tot el mecanisme de processos ITIL.
- ✓ Suporta i executa plugins dissenyats inicialment per Nagios.
- ✓ Té una interfície web com demo per poder visualitzar el seu funcionament sense necessitat d'instal · lar i tenir una idea del producte: demo.opennms.org /.

Inconvenients:

- ✓ Només pot utilitzar com a gestor de base de dades PostgreSQL.
- ✓ Té una posada a punt per optimitzar el rendiment del sistema que requereix un nivell molt elevat de coneixement que comporta una sèrie de modificacions i tunnings a la instal · lació a nivell de configuració, maquinari, base de dades, sistema operatiu, etc.
- ✓ Té una interfície web que de vegades no deixa clar l'avaluació de les dades mostrades. Tampoc funciona correctament amb alguns navegadors com ara Mozilla Firefox.

Per finalitzar aquesta evaluació i no extendrens molt, ja que encara ens faltarien moltes altres plataformes existents no menys importants de les indicades, farem una breu evaluació d'una eina de **programari comercial** o privat.

- ***IBM Tivoli :***

Tivoli Software és una família de productes de programari per a l'administració d'infraestructura d'IT (tecnologia de la informació) pertanyent a IBM (International Business Machines) empresa multinacional nord-americana que comercialitza maquinari i programari i ofereix serveis en una àmplia gamma d'àrees relacionades amb la informàtica.

Malgrat que ha estat descrita com una empresa orientada a les vendes, actualment està sent un defensor principal en el moviment de OpenSource invertint milers de milions de dòlars en serveis i programari basats en Linux.

Ofereix eines orientades a l'administració del rendiment i la disponibilitat dels sistemes i serveis. Entre les quals destaquem IBM Tivoli Monitoring (ITM) amb llicència comercial i és la solució més innovadora d'IBM en monitorització de rendiment, disponibilitat per a la supervisió i vigilància de sistemes operatius, aplicacions, bases de dades i serveis de negocis en entorns distribuïts i de hosts. Es troba disponible per a diverses plataformes que inclouen Linux, UNIX (AIX, Solaris, HP-UX), Windows ®, iz / OS.

Utilitza el protocol SNMP per a la recol·lecció de dades que després emmagatzema i processa. Disposa d'una arquitectura amb o sense agents i permet la configuració d'una resposta programada davant una alarma ja sigui local o funcional. Produeix informes i gràfics en varies tecnologies (XML, HTML, CSV) personalitzats basats en l'historial o mètriques recollides pels agents.

Ajuda a identificar i arreglar interrupcions que amenacen aplicacions clau abans que afectin directament els usuaris. Supervisa de manera proactiva els recursos del sistema per detectar problemes potencials i respon automàticament a esdeveniments. Proporciona un llindar dinàmic i anàlisi de rendiment per millorar la prevenció de riscos. Millora la mitjana de temps de recuperació gràcies a la visualització i la recerca històrica ràpida d'incidents. Recull dades que pot utilitzar per dirigir les activitats de rendiment i planificació de la capacitat a temps i així evitar interrupcions degudes a l'excés d'ús de recursos.

És un producte altament escalable amb una àmplia gamma d'opcions de personalització i d'integració. Hi ha diversos mòduls disponibles per Tivoli Monitoring que s'estenen les capacitats de monitorització als sistemes més complexos, com ara les aplicacions. NET, bases de dades o AMW (Amazon Web Services).

Avantatges:

- ✓ Té una àmplia varietat de productes comercials que fan en conjunt una gestió senzilla d'una infraestructura IT, fins i tot amb un suport total a la instal·lació, actualització i manteniment.

Inconvenients:

- ✓ No és un producte de programari lliure i presenta un preu elevat per la seva llicència comercial amb una durada limitada a 12 mesos i se li ha de sumar un cost extra per cada agent que es desitgi instal·lar als nodes a monitoritzar.
- ✓ El fet d'haver de contractar diverses llicències diferents per a diversos productes o programari encareix encara més la compra d'un producte sòlid que sigui capaç de complir totes les expectatives del client, sense esmentar que la facturació més costosa és el posterior servei i manteniment que haurà de realitzar aquesta empresa multinacional.
- ✓ Trobem fàcilment per la web diversos forats de seguretat remesos i publicats per la pròpia empresa com vulnerabilitats davant atacs per l'execució de codi arbitrari causats per desbordament del buffer en processar cadenes massa grans.

2.1.2.5 Selecció de la millor plataforma

Després de conèixer i detallar algunes de les eines de monitoratge més reconegudes, realitzarem una comparació entre totes les solucions plantejades d'acord amb uns factors globals, de competències o especificacions contingudes en aquests factors, els quals descriurem a continuació.

- ***Funcionalitat***:
  - Monitoritzar serveis, maquinari i sistema operatiu.
  - Multiplataforma a client.
  - Generar gràfiques, informes i estadístiques.
  - Enviar alarmes i notificacions, etc.
- ***Facilitat d' ús***:
  - Interfície o consola web amb control total sobre l'aplicació.
  - Personalització de la interfície.
  - Extensió del sistema (plugins).
  - Instal·lació, configuració i posada en marxa, etc.
- ***Arquitectura***:
  - Consum i requisits previs acceptables (maquinari, programari, etc.)
  - Sistema amb agents que treballen en cada client o node.
  - Possibilitat de monitoritzar gran quantitat nombre de nodes (diversos milers).
  - Estabilitat a canvis de configuració (reinicis del sistema), etc.
- ***Qualitat del Suport***:
  - Desenvolupament de noves millores i revisions en l'aplicació per a la correcció d'errors.
  - Activitat al fòrum i wiki davant preguntes i resolució de problemes o peticions d'usuaris.
  - Disponibilitat d'una versió Enterprise de la seva eina.
  - Idiomes de la documentació disponible, etc.

La figura 2 mostra una taula comparativa resum amb els factors indicats

Sistema de Monitorització	Funcionalitat	Fàcilitat d'ús	Arquitectura	Suport	Programari Lliure
Pandora FMS	√	√	√	√	√
Zabbix	√	√	✗	√	√
Zennos	√	✗	✗	√	√
Nagios	√	✗	✗	√	√
Open NMS	√	✗	√	√	√
IBM Tivoli	√	√	√	✗	✗

Figura 2: Comparativa gràfica de plataformes de monitorització.

Amb tot i a la vista de la comparativa anterior, la plataforma PandoraFMS sembla complir tots els factors, ens decantarem per la plataforma NAGIOS, principalment pel seu suport e informació disponibles.

2.1.3 Introducció als sensors de variables ambientals.

En aquest apartat farem una introducció als sensors, les seves característiques i conceptes principals.

2.1.3.1 Definició de sensors

- ***Que és un Sensor* :**

Un sensor és un dispositiu capaç de detectar magnituds físiques o químiques, anomenades variables d'instrumentació, i transformar-les en variables elèctriques. Les variables d'instrumentació poden ser per exemple: temperatura, intensitat lumínica, distància, acceleració, inclinació, desplaçament, pressió, força, torsió, humitat, pH, etc. Una magnitud elèctrica pot ser una resistència elèctrica (com en una RTD), una capacitat elèctrica (com en un sensor d'humitat), una Tensió elèctrica (com en un termoparell), un corrent elèctric (com en un fototransistor), etc.

Un sensor es diferència d'un transductor en què el sensor està sempre en contacte amb la variable d'instrumentació, amb el que es pot dir també que és un dispositiu que aprofita una de les seves propietats per tal d'adaptar el senyal que mesura perquè la pugui interpretar un altre dispositiu. Un sensor també pot dir-se que és un dispositiu que converteix una forma d'energia en una altra.

- ***Caracteristiques dels Sensors :***
  - **Rang de mesura**: domini en la magnitud mesurada en el qual es pot aplicar el sensor.
  - **Precisió**: és l'error de mesura màxim esperat.
  - **Offset o desviació de zero**: valor de la variable de sortida quan la variable d'entrada és nul·la. Si el rang de mesura no arriba a valors nuls de la variable d'entrada, habitualment s'estableix un altre punt de referència per definir el offset.
  - **Linealitat o correlació lineal**.
  - **Sensibilitat d'un sensor**: suposant que és d'entrada a sortida i la variació de la magnitud d'entrada.
  - **Resolució**: mínima variació de la magnitud d'entrada que pot apreciar-se a la sortida.
  - **Rapidesa de resposta**: pot ser un temps fix o dependre de quant variï la magnitud a mesurar. Depèn de la capacitat del sistema per seguir les variacions de la magnitud d'entrada.
  - **Derives**: són altres magnituds, a part de la mesura com a magnitud d'entrada, que influeixen en la variable de sortida. Per exemple, poden ser condicions ambientals, com la humitat, la temperatura o altres com l'envelliment (oxidació, desgast, etc.) del sensor.
  - **Repetitivitat**: error esperat en repetir diverses vegades la mateixa mesura.

En funció del tipus de senyal de sortida, un sensor pot ser **analògic o digital**. Els sensors analògics lliuren com a sortida un voltatge o un corrent continu i variable dins un camp de mesura especificat. Els rangs de voltaje de sortida són molt variats, sent els més usuals +10 V, +1 V, ± 10V, +-5V i ± 1V.

Els rangs de corrent de sortida més estandarditzats actualment és el de 4 a 20 mA, on 4 mA correspon a zero en la variable mesura i 20 mA a plena escala.

Els sensors digitals lliuren com a sortida un voltatge o un corrent variable enforma de salts o passos discrets de manera codificada, és a dir amb el seu valor representat en algun format de polsos o paraules, diguem PWM (Modulació de Ample de Pols) o binari.

En general, el senyal de sortida d'aquests sensors no és apta per a la seva lectura directa i de vegades tampoc per al seu processat, pel que s'usa un circuit de condicionament, com per exemple un pont de Wheatstone, amplificadors i filtres electrònics que adapten la senyal als nivells apropiats per a la resta dels circuits.

2.1.3.2 Conceptes per la implementació de sensors.

Una solució de monitorització d'altes prestacions, no només hauria de permetre ampliar fàcilment els sistemes de control, sinó també servir com a unitat central de gestió de les variables físiques més variades recollides per el sistemes de sensors.

Els següents conceptes indiquen les principals prestacions que haurien de tenir un sistema de sensors:

- ✓ **Modularitat / Escalabilitat**: amb el principi modular d'un sistema de sensors, aquests podrien ajustar-se a les necessitats inicials i ampliar-se (escalabilitat) en funció del creixement del CPD.

- ✓ **Rendibilitat:** Els sensors s'haurien de poder muntar de forma fàcil mitjançant la tecnologia plug & play o tecnologia sense fils. Amb aquest darrer concepte, podem reduir al mínim els costos d'instal·lació i configuració del sistema.

- ✓ **Compatibilitat:** els sensors haurien de permetre la gestió de seguretat mitjançant diferents protocols: Ethernet, SNMP, TCP/IP, Telnet, Web, FTP, etc. També caldria que aquest sensors poguessin integrar-se en sistemes de monitorització de xarxes convencionals (Nagios, HP Open View, ...).

- ✓ **Robustesa:** La xarxa de sensors tindria que poder utilitzar-se en racks, files de racks, sales TI, edificis, centres de producció, magatzems, instal·lacions industrials o en espais exteriors. D'aquesta manera és possible la seva utilització en aplicacions per a diversos sectors amb total seguretat.

- ✓ **Seguretat:** En el cas de sensors sense fil, haurien de suportar una encriptació de dades per oferir una protecció adequada contra l'escolta no autoritzada de la transmissió.

- ✓ **Flexibilitat:** L'aplicació de sensors sense fil és recomanable quan no es pot o no es vol fer un cablejat directe entre el sensor i la unitat de sensors. Per exemple en cablejats al aire lliure o punts inaccessibles del rack per servidors o dins de la infraestructura de CPDs

- ✓ **Durabilitat:** Els sensors en principi han d'estar dissenyats per durar, ser autònoms i sense bateries. Els sensors sense fils però necessiten en canvi una bateria de liti de 3,6 V d'alta capacitat i llarga vida. Segons el tipus de sensor, la aplicació i temperatura ambient s'aconsegueix una durada de la bateria de fins a 5 anys.

Entre els posibles modes d'implementació dels sensors, tenim básicament dues topologies de connexió:

- ✓ ***Connexió cablatje tradicional***: el cablejat tradicional dels sensors consisteix bàsicament en una connexió plug&play a un dispositiu d'acondicionament de la señal o controlador i que facilita la comunicación al sistema de monitorització mitjançant la xarxa TCP/IP. El tipus de cable podría ser de Cat 3 o Cat.5 amb connexions RJ45 o RJ11.

- ✓ ***Connexió Inalàmbrica***: les noves solucions de monitorització ambiental són els sensors inalambrics, que per general són menys costoses que les solucions de cablejat tradicional, doncs no hi han cables per instal.lar ni mantenir. També es poden afegir nous sensors sense preocupar-se del cablejat. Aques sensors han d'estar normalitzats per el estándar IEEE 802.15.4 i ZigBee.

Els sensors, tant els de tipus de connexió convencional com els de connexió inal.lambrica, requereixen de maquinari de monitorització o recol.lector de dades, per adaptar les senyals del sensors i procesar-la a una señal que pugui ser enviada a través de la xarxa. Aquest maquinari normalment són adaptadors, amplificadors o gateways, que són adaptables tant per instal.lació en els mateixos Racks, com de tipus mural. El protocol estándar més emprat per la transferencia d'aquestes dades és el **SNMP**.

2.1.3.3 Variables Ambientals

Els sensors permeten la mesura de moltes variables entre les que podriem agrupar les següents en un Centre de Procesament de Dades:

- ✓ ***Variables Electriques***: per mesurar el voltatge trifàsic, bifàsic o monofàsic. La corrent elèctrica AC de Baixa i mithana tensió. El voltatge i la corrent DC d'un banc de bateries. El consum electric en VA,W, Var i la qualitat d'energia i el factor de potència.
- ✓ ***Variables Ambientals*** : per mesurar la humitat i temperatura ambiental, la detecció d'aigua sota els fals terra. La detecció del fluxe d'aire, detecció de fum, detecció de CO2, i la medició de pressió ambiental en sales blanques o presuritzades.
- ✓ ***Detecció per la seguretat***: per detecció de trencament de vidres, detecció d'apertura de portes, detecció d'aigua, detecció del flux d'aire, detecció de fum, detecció d'anomalies per equips via contacte sec.

Per la nostra solució però, ens centrarem principalment en les **variables ambientals**, de les que definirem a continuació els principals tipus de variables a mesurar i dels espais físics crítics dels que es recomanable fer aquestes mesures per detectar les principals amenaces d'un CPD:

- ✓ ***Temperatura:*** Hi ha molts llocs en un CPD on la temperatura és critica:
  - Temperatura de l'aire en els espais físics elevats i lluny dels aparells de climatització.
  - Temperatura de l'aire en front dels armaris situats en els passadissos freds, o de l'aire d'admisió per els servidors dins dels racks.
  - Temperatura de l'aire dels equips TI en els racks, en particular si aquest estan completament tancats.
- ✓ ***Humitat:*** En un CPD, la humitat es susceptible de tenir moltes variacions de les seves condicions, en las que pot tenir una incidència o riscos següents:
  - Risc per condicions de baixa humitat, que podrien provocar descargas electrostàtiques i malmetre seriosament els equips informàtics i/o de comunicacions.
  - Risc per condicions d'alta humitat, que podrien provocar condensacions.
- ✓ ***Fum*** : El sistemes de detecció de fum són especialment recomanats en CPDs per l'elevat risc d'incendi ocasionats per els nivells elevats d'energia que dissipen els circuits electronics, i possibles sobreescalfaments del cablejat. La detecció de fum depèn de tres factors: la cobertura o situació del sistema de detecció, la concentració o densitat de punts de detecció i la sensibilitat.
- ✓ ***Fuites de líquid o aigua*** : aquestes són també un altra risc dins dels CPDs o motiu de preocupació pel fet que molts sistemes utilitzen líquids o aigua per la refrigeració dels equips e climatitació. Sobretot en l'impacte sobre els sistemes electronics i de cablejats que es troben en els fals terra dels CPD's.
- ✓ ***Posició de les portes***: la posició de les portes té especial rellevància en la climatització i fuites d'aire d'un CPD's i en la gestió de la eficiència climàtica. L'oblit de tancament d'un porta pot provocar pèrdues d'aire del CPC, apart de la seguretat i detecció d'accés per personal no autoritzat. També la apertura de portes dels armaris pot condicionar fluxes d'aire innecessaris que podrien malmetre els equips informàtics.
- ✓ ***Falta d'aire dels equips de climatització :*** no tots els equips de climatització en CPD's són redundants o tenen la capacitat de ser monitoritzats via xarxa i gestionar el tractament d'aire o la seva supervisió. Per tant, a un nivell bàsic caldria poder controlar el seu estat i evitar fallas en les unitast de climatització, amb la detecció mitjançant contactes secs.
- ✓ ***Control d'energia:*** darrerament un dels paràmetres de monitorització força importants, són la detecció de fallades d'energia, control de la corrent, tensió i potència dels equips distribuïdors d'alimentació electrica als dispositus i infraestructura TI. El control d'aquestes variables repercuteixen en la eficiència energètica del CPD.

2.1.4 Protocol SNMP

En un sistema de monitorització ambiental, la transferència de dades entre els equips de monitorització i els sistemes de gestió utilitzen el protocol SNMP (Simple Network Management Protocol) per obtenir la informació necessària. Definirem alguns conceptes per entendre el seu funcionament.

2.1.4.1 Definició i origen

El protocol SNMP és part de la família de protocols TCP/IP i facilita l'intercanvi d'informació d'administració entre dispositius de xarxa i permet supervisar el funcionament dels equips i buscar i resoldre possibles problemes.

La idea és que SNMP sigui un component integral i essencial de tots els sistemes TCP/IP, per això, tots els protocols per sota del nivell d'aplicació tenen els seus components SNMP.

SNMP també s'ha estès per cobrir equips no TCP/IP i alguns protocols propietaris, constituint-se en l'estàndard més àmpliament utilitzat per a la recollida de informació de gestió de xarxa.Va ser publicat inicialment el 1989 però les primeres aplicacions no van aparèixer fins 1990.

S'han definit tres versions del protocol. Les versions 1 i 2 són les més utilitzades i la versió 3, tot i que inclou millores en quant a aspectes de seguretat, no ha estat tant ampliament acceptada per la industria.

2.1.4.2 Conceptes bàsics

SNMP utilitza un servei no orientat a connexió (UDP) per enviar missatges entre administradors i agents.

Un sistema administrat mitjançant SNMP disposa de tres componens bàsics:

- **Dispositius administrats**: aquest són normalment maquinari conectat a una xarxa i que contenen un agent SNMP que es troben en una xarxa administrada. Aquests dispositius recullen i guarden informació d'administració, que es posa a disposició dels **NMS**'s utilitant SNMP.
- **Agents** : els agents són mòduls programari d'administració de xarxa que resideixen en els dispositius administrats. Un agent disposa d'un coneixement local d'informació d'administració que és traduïda a un format compatible com el SNMP i organitzada en jerarquies.
- **Sistema administrador de xarxa (NMS)** : executa aplicacions que supervisen i controlan als dispositus administrats. Els NMS's proporcionen els recursos de processament i memòria requerits per l'administrador de xarxa.

Tindrem també un programari en l'element de xarxa monitoritzat que es denominarà agent i la funció és, d'una banda, recollir informació dels esdeveniments que es produeixen en el dispositiu, i per un altre comunicar-se amb el gestor.

La comunicació pot produir de dues maneres:

1. El gestor pot preguntar a l'agent sobre el valor d'alguna variable

2. L'agent pot informar el gestor sobre algun fet important.

El gestor, a més de poder llegir el contingut de les variables de l'agent, pot modificar el seu valor.

Els dispositius administrats són supervisats i controlats usant quatre comandaments SNMP bàsics: lectura, escriptura, notificació i operacions transversals.

2.1.4.3 Funcionament SNMP

Per funcionar SNMP consta de tres elements principals:

1. ***La base d'Informació de gestió (MIB - Management Information Bases)*** : És un base de dades distribuïda, a través de la qual es té accés a la informació per a la seva gestió i continguda en la memòria interna del dispositiu en qüestió. Aquesta base és una col·lecció d'informació que està organitzada jeràrquicament i té una estructura en arbre, adequada per gestionar diversos grups d'objectes (informació sobre variables o valors que es poden adoptar), i amb identificadors exclusius per a cada objecte.

2. ***L'estructura de gestió de la informació (SMI- Structure of Management Information)***: Bàsicament tracta de definir la sintaxis emprada per especificar la MIB. S'indicaran aquí els aspectes de quin tipus de dades podrà allotjar la MIB, com representar i anomenar els recursos a la MIB, etc. En definitiva, són les regles per a la definició de la MIB.

3. ***El protocol de gestió de xarxa simple (SNMP):*** És el protocol utilitzat entre el gestor i l'element de xarxa. Hi ha dos maneres d'obtenir la informació amb SNMP: utilitzant notificacions o ***Traps*** , o bé fent consultes.

2.1.4.4 Missatges SNMP

SNMP proporciona un mecanisme per accedir als objectes de MIB de manera que puguin ser consultats i modificats, a més de permetre que els dispositius connectats a la xarxa envien correu brossa a una estació de gestió SNMP per indicar que s'ha produït una certa condició.

SNMP Defineix cinc tipus de missatges d'intercanvi entre gestor i agent que es denominen PDUs (Unitat de dades de Protocol): Get-request , Get-next-request , Response, Set-request i Trap.

SNMP fa ús de dos ports UDP: el 161 i el 162, per a la recepció en l'agent i el gestor respectivament, d'aquesta manera és possible que en una estació operin simultàniament el programari de gestor i agent. El gestor implementa un esquema de temporització i retransmissió per contemplar el fet de la pèrdua dels missatges i solucionar la manca de fiabilitat d'UDP.

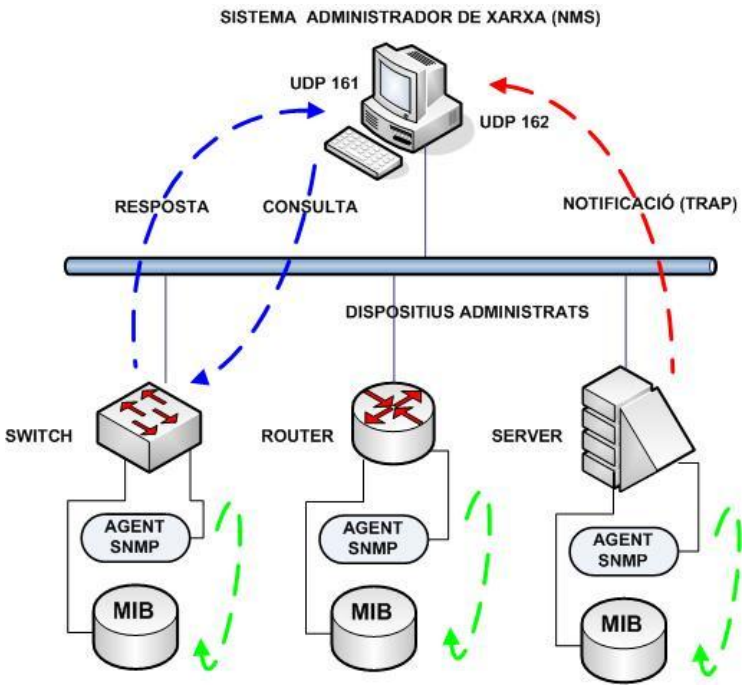


Figura 3: Esquema funcionament del protocol SNMP.

2.2 NAGIOS com a plataforma de Monitorització

Com ja haviem esmentat en l'apartat Introducció a la Monitorització de Sistemes i com a resultat de la comparativa realitzada, NAGIOS és la plataforma escollida. Aquesta sel.lecció bé donada que Nagios és una de les eines més conegudes en projectes de monitorització de sistemes i també amb un bon suport, malgrat la seva configuració no és sencilla.

En els següents apartats definirem algunes de les seves característiques, funcionalitat i configuració, tot i que no és l'objectiu entrar en detall, doncs hi ha molta informació disponible a la mateixa pàgina web de Nagios..

Nagios és un sistema open source de monitorització de xarxes molt ampliament utilitzat, que vigila equips (maquinari) i serveis (programari) que se l'hi especifiquin, avisant quant el comportament d'aquests no sigui el desitjat i poder actuar de manera proactiva

Aquesta eina també proporciona una gran versatilitat per consultar pràcticament qualsevol parametre d'interés d'un sistema i generar alertes, que poden ser rebudes per els responsables corresponents mitjançant correu electronic o missatges SMS, quant aquest paràmetres passin dels llindars o marges establerts per els administradors de la xarxa.

Inicialment Nagios es va anomenar Netsaint, nom que va haver de canviar per coincidir amb un altra marca comercial, i va ser creat i mantingut actualment per Ethen Galstad juntament amb un grup de desenvolupadors de programari que mantenen també els seus components.

Nagios està escrit en C i originalment dissenyat per ser executat en un entorn GNU/Linux, tot i que pot ser executat amb altres variants d'Unix. Està llicenciat per GNU General Public License Version 2 publicada per la Free Software Fundation.

Que podem fer amb Nagios?. Entre algunes de les característiques que ja havia descrit anteriorment, tenim les següents:

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

Per tots aquest motius doncs hem considerat a Nagios com una de les plataformes ideals per formar el que seria el nucli del sistema de monitorització.

2.2.1 Estructura del sistema

L'estructura interna de NAGIOS està formada de quatre mòduls :

- **Nucli o *kernel***. El nucli conté el programari necessari per realitzar la monitorització, el control dels processos, la gestió dels serveis i de les màquines de la xarxa. Utilitza diversos components ja inclosos amb l'aplicació i també permet utilitzar components realitzats per tercers.
- **Extensions o *plugins***. Els *plugins* són seqüències d'ordres o scripts que s'executen per comprovar l'estat d'una màquina o servei.
- **Interfície web**. El web resideix en el mateix servidor Nagios i utilitza el programari web Apache2 per a la publicació. Està programada en HTML i CSS i utilitza scripts CGI. A través de la interfície web es pot observar el resultat de la monitorització dels equips i dels serveis, permetent l'administrador de la infraestructura tenir un control visual i gràfic del seu comportament.
- **Bases de dades**. La informació de configuració i la informació de l'històric es guarden en arxius de text permetent la seva anàlisi posterior. Entorns MySQL o PostgreSQ.

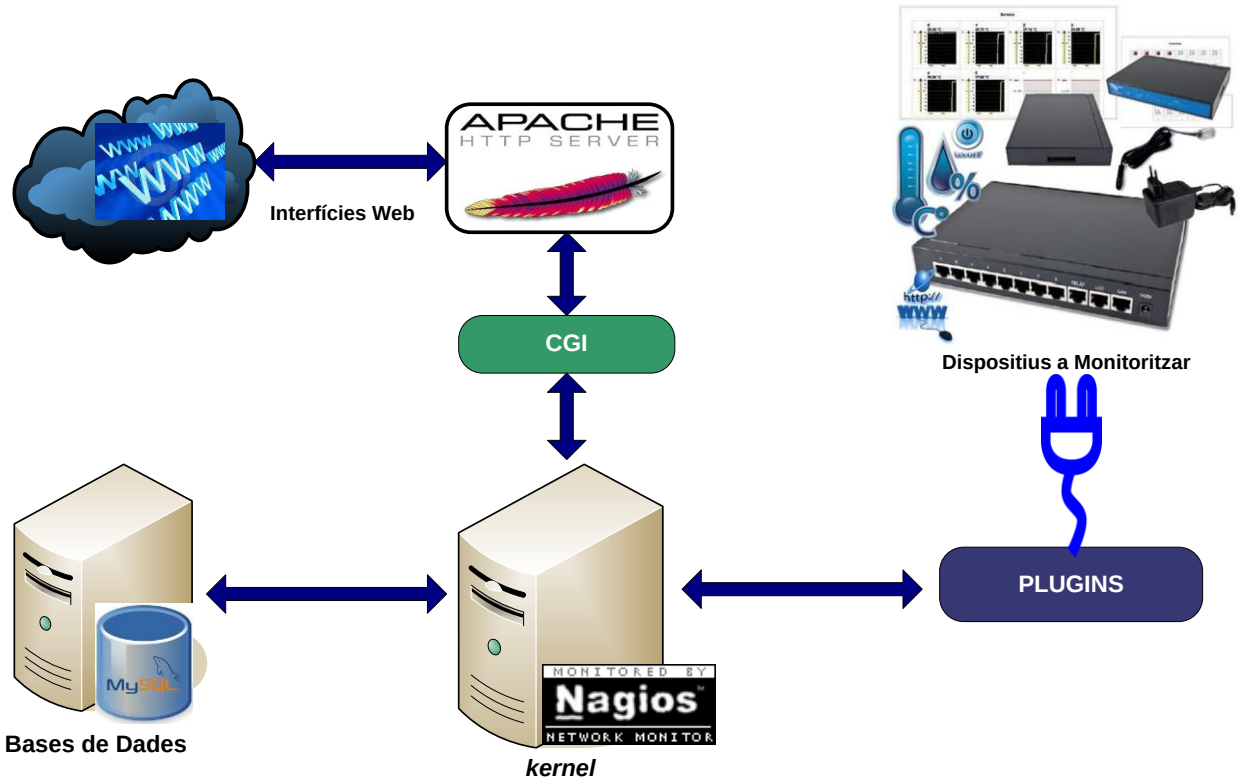


Figura 4: Arquitectura de Nagios

2.2.2 Funcionament

Nagios és un programari molt potent i flexible, però per què funcioni correctament pot resultar una mica complex. Per poder realitzar la instal·lació i una correcta configuració del programa, és recomanable conèixer el seu funcionament intern. Definirem alguns conceptes.

2.2.2.1 Plugins:

Nagios no inclou cap mecanisme intern per comprovar l'estat dels equips o serveis. Es basa en programes externs anomenats plugins i utilitza el resultat de l'execució de cada plugin per determinar l'estat d'un equip o servei i prendre les mesures necessàries, per exemple notificar a l'administrador de la xarxa de la situació.

Hi ha una distribució oficial de plugins per Nagios per controlar els recursos bàsics, però també es poden dissenyar i escriure plugins segons les necessitats de gestió de cada xarxa. Poden ser escrits en llenguatges de programació Bash, C + +, Perl, Ruby, Python, PHP, C #, etc.

Cal esmentar que Nagios no entén els detalls del què s'està monitoritzant, només registra els canvis en l'estat dels recursos. Els plugins són els que saben realment què és el que s'està monitoritzant i prenen les accions necessàries (com activar els processos per solucionar un esdeveniment o enviar notificacions). El text que generen abans que acabi la seva execució és el resultat de l'acció principal de cada plugin i és l'estat de l'operació. Aquest estat es mostra a la interfície web de Nagios i també es guarda en un arxiu de registres o Log.

2.2.2.2 Estat d'equips i serveis :

Nagios verifica primer el estat dels serveis d'un equip. Si un servei mostra un estat erroni, Nagios verifica l'estat de l'equip mitjançant la comanda ping.

Si l'equip respon al ping, Nagios interpreta que és el servei el que no funciona correctament i procedeix a realitzar les notificacions corresponents i / oa prendre les mesures pertinents.

Si l'equip no respon al ping, Nagios interpreta que hi ha un problema amb l'equip, cancel · les notificacions sobre l'estat dels seus serveis (ja que si un equip no respon, no es poden monitoritzar els seus serveis) i notifica l'estat de l'equip al administrador de la xarxa.

2.2.2.3 Tipus d'estats:

L'estat real dels serveis i dels equips monitoritzats es determina per dos components:

- ***Estat del servei o de l'equip***. Nagios utilitza quatre estats per saber el valor real retornat per els *plugins* a la consulta que realitzen als equips o serveis. Aquest són: OK, WARNING, CRITICAL i UNKNOWN

- ***Tipus d'estat virtual en què es troba el servei o l'equip***. Els estats són crucials per a la lògica de monitoratge i també s'utilitzen per determinar quan s'executen els controladors d'esdeveniments i quan s'envien les notificacions. Hi ha dos tipus d'estats en Nagios: SOFT i HARD.

2.2.2.4 Interrupcions a la xarxa:

Nagios té la capacitat de determinar si els equips que s'estan monitoritzant tènen l'estat inactiu (DOWN) o bé l'estat inabastable (UNREACHABLE). Hi ha una gran diferència entre aquests dos estats i conèixels permet localitzar amb precisió els problemes de la xarxa.

2.2.2.5 Notificacions:

Nagios envia les notificacions a tots els membres del grup de contactes especificats en la variable "contact_group" que es troba en la definició de cada equip i servei. Si un contacte es troba en més d'un grup, només se li envia la notificació un cop, per evitar duplicacions.

Per evitar l'enviament de moltes notificacions innecessàries s'utilitzen filtres:

- ***Filtre de programa***. És el primer filtre que s'ha de passar i consisteix a comprovar que el servei de notificació està actiu verificant el valor de la directiva "enable_notifications" de l'arxiu de configuració principal. Es pot desactivar individualment per a qualsevol equip o servei.
- ***Filtres d'equip i servei.*** Són un conjunt de 5 filtres
- ***Filtres de contacte***: cada contacte té els seus propis filtres pels quals les notificacions han de passar abans que el contacte les rebi.

Nagios és capaç d'enviar notificacions per diferents vies (correu electrònic, SMS, etc.). Per defecte, les notificacions s'envien per correu electrònic però pot modificar el mètode instal · lant els connectors necessaris i configurant els comandaments de notificació als arxius de configuració.

2.2.3 Configuració

Amb la instal·lació de Nagios, s'instal·len uns arxius de configuració d'exemple al directori "/usr/local/ nagios/etc/". Aquests arxius de configuració es poden utilitzar directament eliminant la paraula "sample" amb algunes modificacions per adaptar Nagios a les necessitats particulars de la xarxa, els equips i els serveis que es vol monitoritzar en cada cas.

Hi ha quatre tipus de fitxers de configuració:

- ✓ ***Arxiu de configuració principal*** (Main Config File)
- ✓ ***Arxiu de recursos*** (Resource File)
- ✓ ***Arxiu de definició d'objectes*** (Object Definition File)
- ✓ ***Arxiu de configuració de CGI*** (CGI Config File)

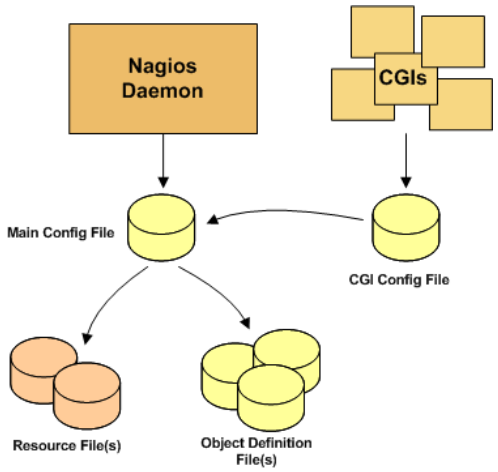


Figura 5: Estructura arxius configuració de Nagios

Font de la figura 5 : http://nagios.sourceforge.net/docs/3_0/config.html

2.2.4 Preparació de l'entorn

Tal com ja havíem avançat, Nagios és una plataforma pensada en entorns de sistemes operatius Linux u altres variants de Linux, com per exemple Ubuntu.

Per tant un dels requisits és fer l'instal.lació en un sistema operatiu de codi obert per seguir amb la línea dels open source. Farem una breu descripció d'aquest sistema operatiu i dels arxius necessaris per preparar l'entorn.

2.2.4.1 Ubuntu

Ubuntu és un sistema operatiu mantingut per ***Canonical*** i la comunitat de desenvolupadors. Utilitza un nucli Linux, i el seu origen està basat en Debian. Ubuntu està orientat a nous usuaris sense experiència i d'altres ja més iniciats, però molt centrat en la facilitat d'ús i en la millora de l'experiència d'usuari.

Ubuntu està format d'un programari normalment distribuït sota una llicència lliure o de codi obert. Hi ha estadístiques que parlent d'un percentatge de mercat d'Ubuntu dins de "distribucions linux" d'un 49% aproximadament, i amb una tendència a pujar com servidor web.

El seu patrocinador Canonical, és una companyia britànica propietat de l'empresari sud-africà Mark Shuttleworth que ofereix el sistema de manera gratuïta i que es finança per mitjà de serveis vinculats al sistema operatiu, venent suport tècnic.

A més de mantenir-lo lliure i gratuït, l'empresa és capaç d'aprofitar els desenvolupadors de la comunitat per millorar els components del seu sistema operatiu. Extraoficialment la comunitat de desenvolupadors proporciona suport per derivacions d'Ubuntu amb altres entorns: Kubuntu, Xubuntu, Edubuntu, Ubuntu Studio, Mythbuntu i Lubuntu.

Cada sis mesos es publica una nova versió d'Ubuntu la qual rep suport per part de Canonical, durant divuit mesos, mitjançant actualitzacions de seguretat, i actualitzacions menors de programes. Les versions LTS (Long Term Support), que s'alliberen cada dos anys, reben suport durant cinc anys en els sistemes d'escriptori i de servidor.

En particular i per provar l'entorn de NAGIOS, hem instal.lat **UBUNTU versió 12.04** en un entorn de màquina virtual ***ORACLE VIRTUALBOX***.

Figura 6: Pantalles dels entorns màquina VirtualBox i Sistema Operatiu Ubuntu

2.2.4.2 Descàrrega de Nagios

Per la instal·lació podem descarregar els arxius de la pàgina oficial de Nagios.

Els paquets de les darreres versions descarregats són:

- nagios-3.4.1.tar.gz

- nagios-plugins-1.4.16.tar.gz

2.2.5 Instal.lació bàsica de Nagios.

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

Totes les instal·lacions les farem per línea de comandes (terminal d'Ubuntu).

2.2.5.1 Pas 1 : Prerequisits

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

- ✓ **Servidor Web**: Apache o qualsevol altre que suporti CGI, per a utilitzar la interfície web.

  Instal.lem Apache 2:

  ```
  sudo apt-get install apache2
  ```

- ✓ **PHP:** és un interprèt basat en Perl per els scripts, ja que els plugins estan escrits en aquest llenguatge. Alguns plugins també necessiten Perl Net::Snmp per a poder comunicar-se amb dispositius mitjançant el protocol SNMP.

  Instal.lem PHP:

  ```
  sudo apt-get install libapache2-mod-php5
  ```

- ✓ **GCC:** Són compiladors per GNU i altres llibreries bàsiques.

  Instal.lem GCC:

  ```
  sudo apt-get install build-essential
  ```

- ✓ **Llibreries GD** de gràfics per la interfície web:

  Finalment instal.lem GD, per versions superiors a la 7.10:

  ```
  sudo apt-get install libgd2-xpm-dev
  ```

També hi ha disponibles molts altres paquets de programari per l'entorn Nagios.

2.2.5.2 Pas 2 : Crear informació de compte d'usuari

Una vegada completada la fase de prerequisits, començarem a instal.lar l'eina Nagios en l'entorn del sistema operatiu Ubuntu 12.04

En primer lloc per poder seguir tots els passos per la instal.lació en caldrà entrar com "***root***":

```
sudo –s
```

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

En el nostre cas farem:

Crear un nou compte d'usuari "***nagios*** " i contrasenya (amb l'opció "/bin/bash" indicarem l'interpret de comandes a utilizar) :

```
/usr/sbin/useradd -m -s /bin/bash nagios
```

Donar una contrasenya (s'ha d'introduir dues vegades):

```
passwd nagios
```

Crear un grup ***nagcmd*** per a permetre que comandes externes siguin introduïdes mitjançant la interfaç web.

```
/usr/sbin/groupadd nagcmd
```

Introduïr l'usuari ***nagios*** i l'usuari apache ***www-data*** en el grup ***nagcmd*** de forma que el servidor web estigui funcionant normalment www-data

```
/usr/sbin/usermod -a -G nagcmd nagios
```

```
/usr/sbin/usermod -a -G nagcmd www-data
```

2.2.5.3 Pas 3 : Descàrrega de Nagios i dels Plugins

En l'anterior apartat ja he esmentat les versions descarregades, però en l'entorn Ubuntu i des del seu terminal, es recomanable crear una carpeta per guardar aquests fitxers comprimits.

```
mkdir /downloads
```

La instrucció des de terminal per poder descarregar directament Nagios és:

```
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.4.1.tar.gz
```

i dels Plugins és:

```
wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-
1.4.16.tar.gz
```

2.2.5.4 Pas 4 : Compilar i instal·lar Nagios

Una vegada els paquets descarregats de la plana oficial de Nagios i preparat l'entorn podem començar amb la compilació i instal.lació dels mateixos.

Primer descomprimirem el paquet de Nagios

```
tar xzf nagios-3.4.1.tar.gz
```

Entrem a la carpeta que hem descomprimit:

```
cd nagios-3.4.1
```

Executarem l'script de configuració del Nagios amb el nom del grup que hem donat d'alta anteriorment.

```
./configure --with-command-group=nagcmd
```

Compilarem el codi font de Nagios:

```
make all
```

Instal·larem els arxius binaris, l'script d'inici, els fitxers de configuració i el directori de comandes externes respectivament:

```
make install
```

```
make install-init
```

```
make install-config
```

```
make install-commandmode
```

2.2.5.5 Pas 5 : Personalitzar la configuració

Amb Nagios instal.lat en Ubuntu, de moment encara no tenim l'entorn preparat i és recomanble primer fer algunes modificacions personalitzades.

Anirem al directori "usr/local/nagios/etc" on tenim els fitxers de configuració de Nagios on podrem modificar per personalitzar la configuració.

En aquest cas modificarem l'adreça **de e-mail que utilitzarem per les notificacions de Nagios,** de manera que per fer això obrirem el fitxer " contacts.cfg " amb un editor de textes:

```
gedit /usr/local/nagios/etc/objects/contacts.cfg
```

Modificarem l'adreça indicada en la línia 35 per la nostra on volem rebre les notificacions

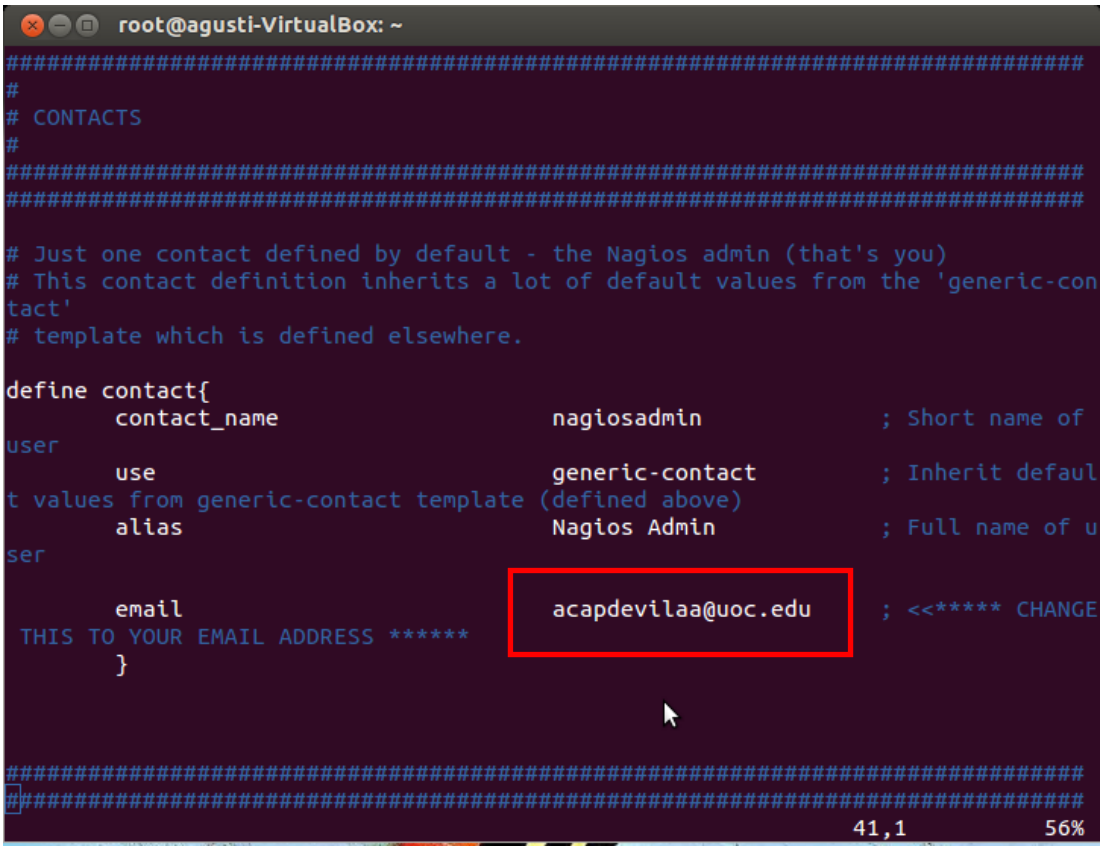


Figura 7: Captura de configuració personalitzada de l'arxiu contacts.cfg

2.2.5.6 Pas 6: Configurar la interfície web

Configurem Nagios per a poder accedir-hi mitjançant la interfície web.

Instal·larem l'arxiu de configuració de Nagios en el directori conf.d d'Apache:

```
make install-webconf
```

Crearem un usuari (***nagiosadmin***) que pugui accedir a la interfície web de Nagios:

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Reiniciem apache per tal que els canvis tinguin efecte

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

2.2.5.7 Pas 7 : Compilar i instal·lar Nagios Plugins

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

Extreurem els plugins del arxiu Nagios comprimit:

```
tar xzf nagios-plugins-1.4.16.tar.gz
```

a la carpeta que acabem de descomprimir:

```
cd nagios-plugins-1.4.16/
```

Compilarem els plugins (amb "*with openssl*" habilitem el suport per a SSL i amb "*enableperl-modules*" i habilitarem els mòduls de perl)

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

Fem la instal.lació dels Plugins:

```
Make
```

```
make install
```

2.2.5.8 Pas 8 : Iniciar Nagios

Finalment farem la configuración de Nagios per tal que s'inicií automàticament quan arrenqui el sistema, amb un script que ja haurem creat amb tota l'anterior instal.lació:

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

Revisarem els arxius de configuració i instal·lació de Nagios si són correctes:

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

Si no tenim errors iniciarem Nagios:

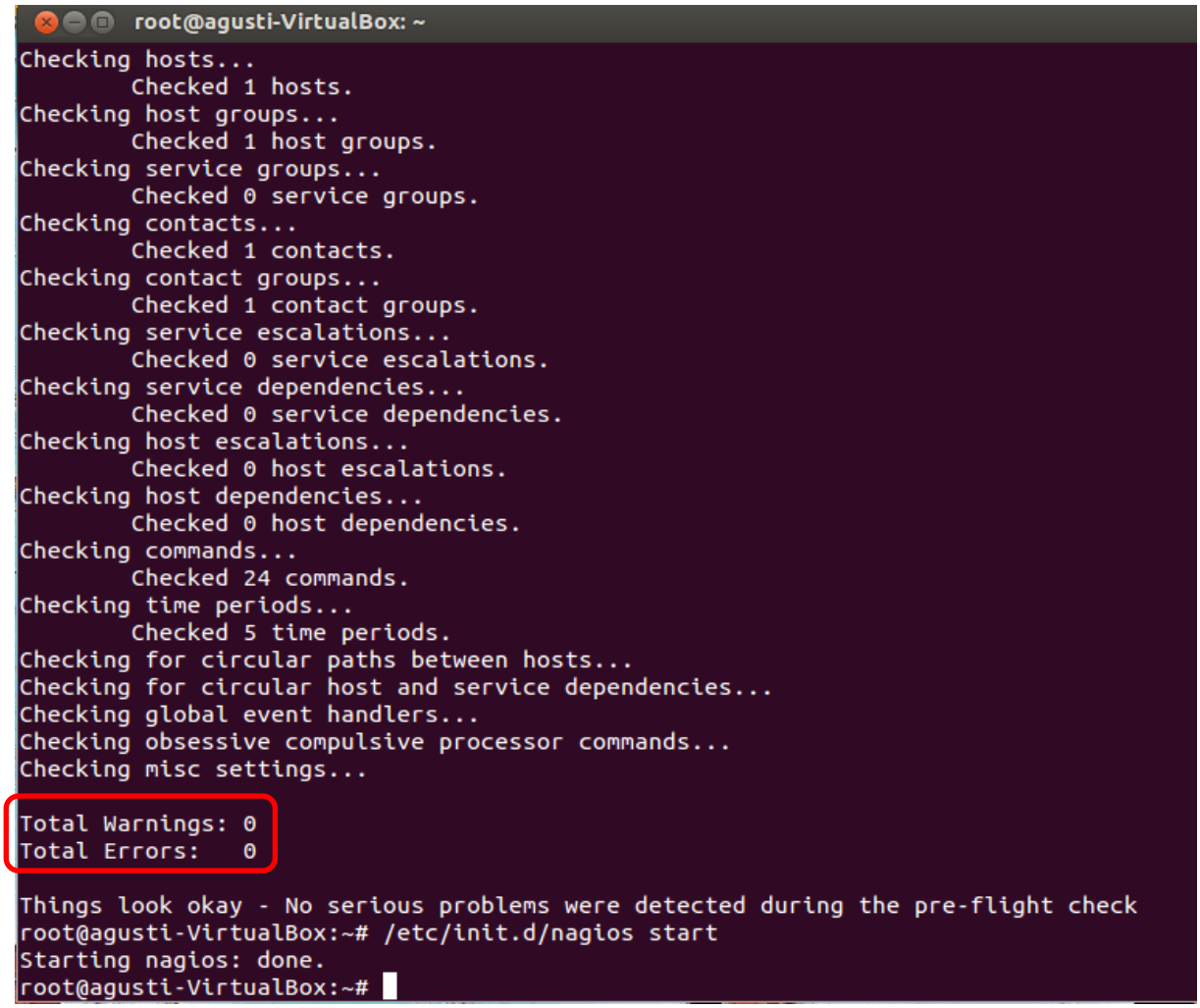


Figura 8: Captura del fitxer de verificació d'errors

Observem en la captura de la figura 8 que no hi ha errors i iniciem Nagios

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

2.2.5.9 Pas 9 : Entrar en la interfície Web

En principi si tota la instal.lació s'ha fet correctament, ja podriem entrar a Nagios des de l'explorador Web mitjançant l'adreça: ***http://localhost/nagios.***

Ens demanarà el nom d'usuari (***nagiosadmin***) i la contrasenya (***nagiosadmin***).

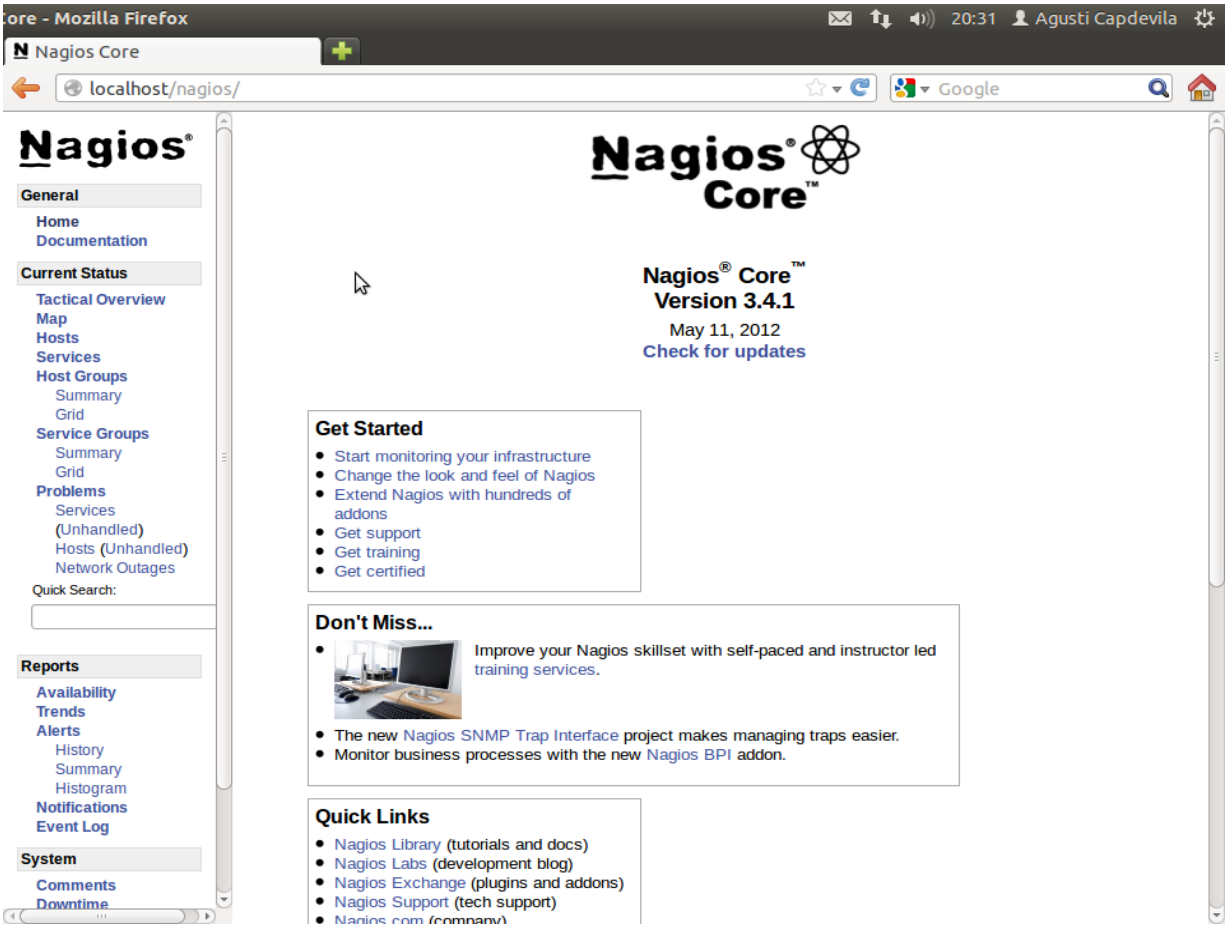


Figura 9: Captura de la interface Web de Nagios

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

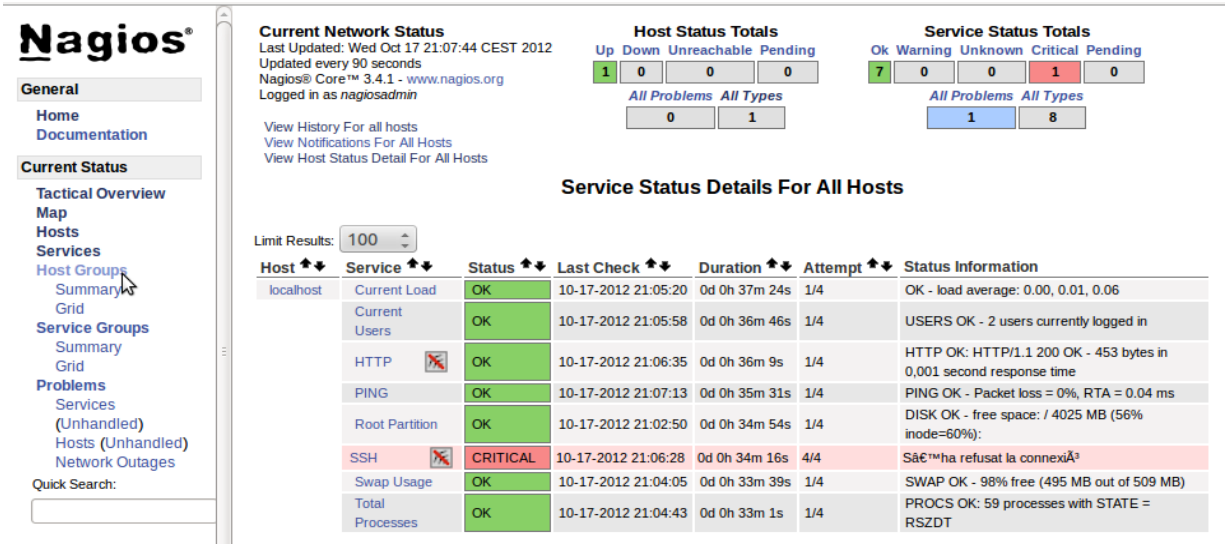


Figura 10: Captura dels serveis en curs de Nagios amb warning SSH

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

Procedim a instal·lar aquest nou paquet SSH :

```
sudo apt-get install ssh
```

Després d'esperar uns minuts, en la figura 11 observem que ja està restablert :

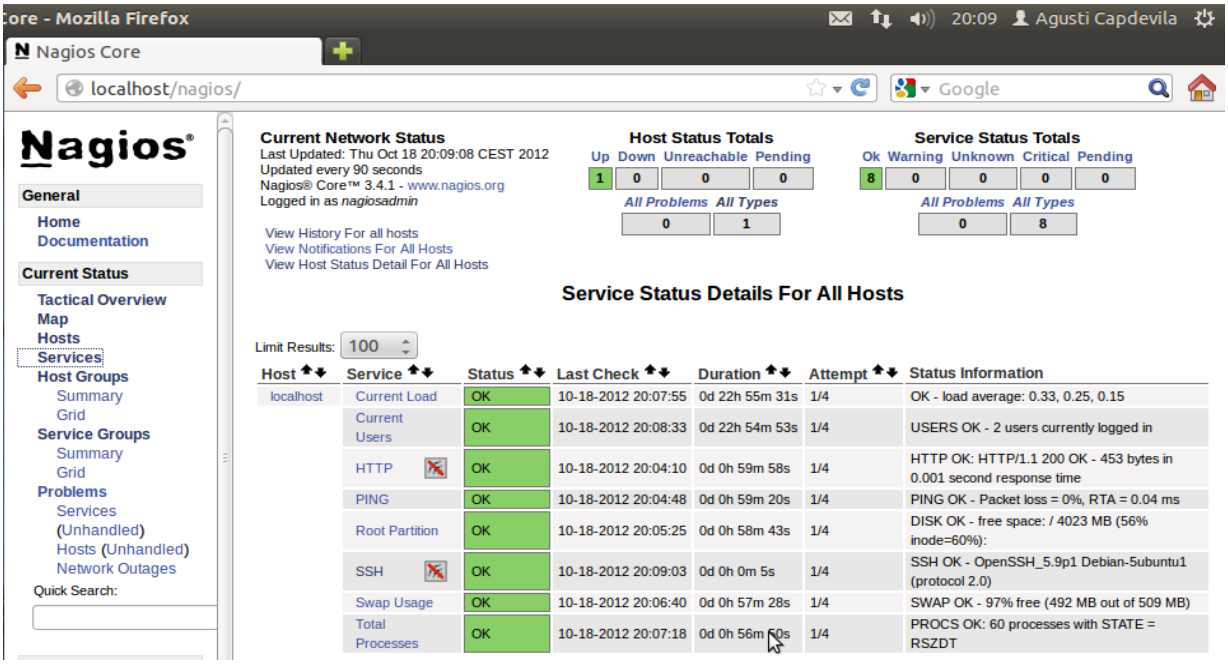


Figura 11: Captura dels serveis en curs de Nagios sense warnings

2.2.5.10 Pas 10 : Altres Modificacions

En el pas 4, després de la instalació de Nagios en Ubuntu, hem modificat l'adreça de e-mail a la que aren arriben les **notificacions de Nagios**. De totes maneres, per rebre aquestes notificacions és necessari **instal.lar algún servidor de correo**.

Per tant podem **instal.lar postfix** com servidor de correu:

```
apt-get install postfix
```

Configurem l'opció de "**Internet con <smarthost>**", amb aquesta opció indiquem que utilitzarem un servidor de correu extern per enviar els correus.

El nom del sistema de correus introduim "**nagios.local**"

També en caldrà **instal.lar mailutils** per enviar emails per línea de comandes:

```
apt-get install mailutils
```

Tornem a **reiniciar Nagios**:

```
udo /etc/init.d/nagios restart
```

2.2.6 Monitorització de serveis i equips

Un centre de processament de dades hi poden haver una gran quantitat d'equips , com sondes de control de temperatura i humitat, equips d'alimentació SAI, servidors de tot tipus, equips de comunicacions i el propi servidor Nagios.

Com a títol pràctic d'aquest TFC apart de la instal.lació de NAGIOS que funciona perfectament, veurem com podem monitoritzar alguns serveis i equips, per exemple el pròpi servei UBUNTU i entre els equips, el meu router.

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

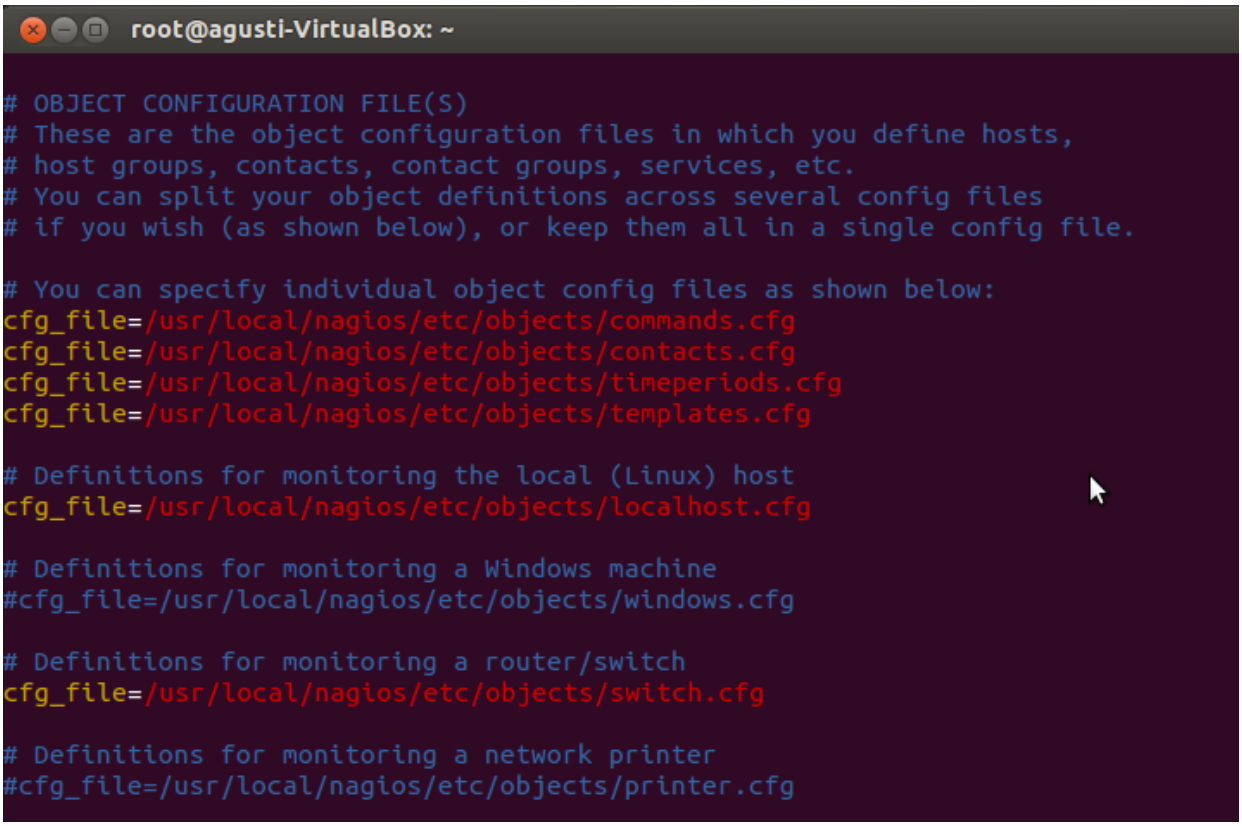


Figura 12: Captura del fitxer de configuració nagios.cfg

Per poder monitoritzar els serveis que volem, cal descomentar # dels equips o serveis que volem configurar.

Podem veure que tenim actius els següents objectes :

- ***localhost.cfg*** : per monitoritzar el host local (Linux)
- ***switch.cfg***: per monitoritzar el router o switch.

2.2.6.1 Monitoritzar equips amb Linux

Nagios permet monitoritzar alguns dels serveis i atributs de màquines Linux/Unix:

- Ús de la memòria
- Càrrega de la CPU
- Ús del disc dur
- Usuaris assignats
- Processos que s'estant executant, etc.

Per a configurar el host, el hostgroup i els serveis que volem monitoritzar s'ha d'adaptar el següent fitxer: ***/usr/local/nagios/etc/objects/localhost.cfg***

En la figura 13 es mostra un exemple de configuració del host :

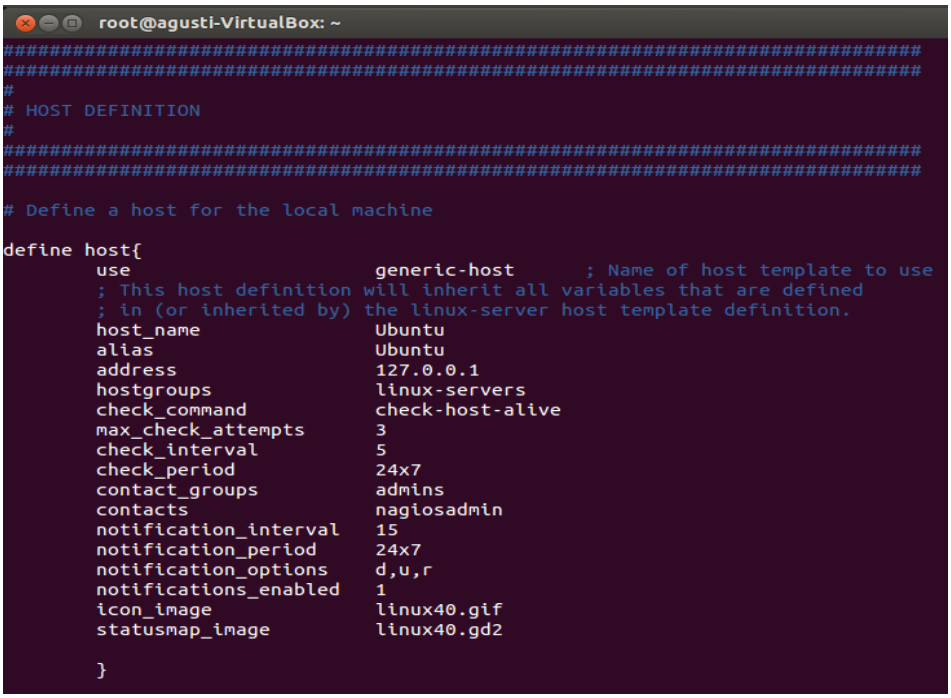


Figura 13: Definició host Ubuntu

En la figura 14 es mostra la dels serveis que ja estàn per defecte :

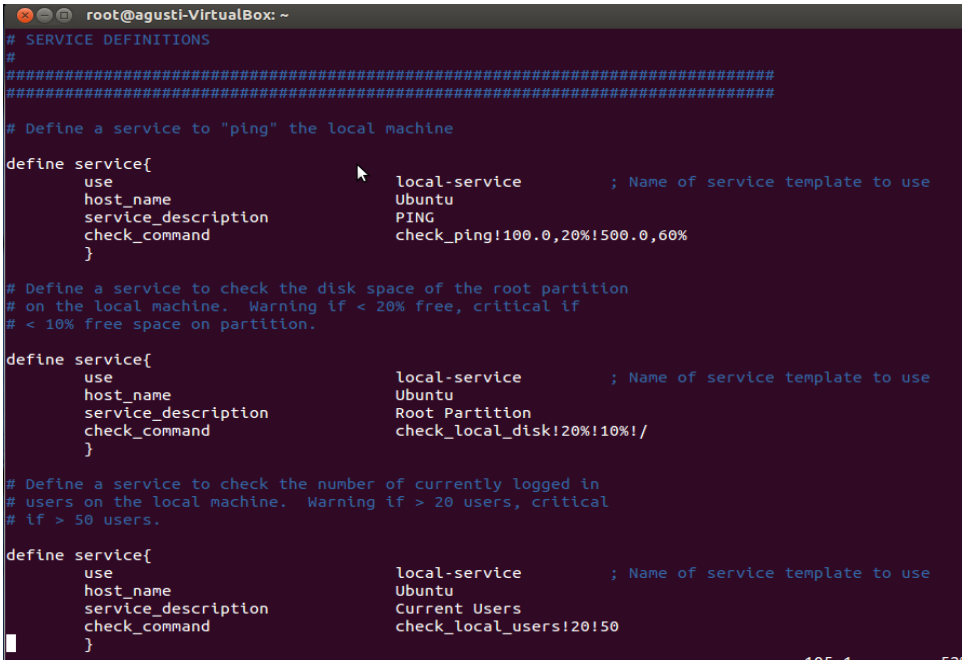


Figura 14: Definició serveis Ubuntu

2.2.6.2 Monitoritzar routers i switches

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

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

Per a configurar el host, el hostgroup i els serveis que volem monitoritzar en el routers s'ha adaptat el següent fitxer: ***/usr/local/nagios/etc/objects/switch.cfg***

En la figura 15 es mostra un exemple de configuració del host d'un router :

```
root@agusti-VirtualBox: ~
##############################################################################
##############################################################################
#
# HOST DEFINITIONS
#
##############################################################################
##############################################################################

# Define the switch that we'll be monitoring

define host{
        use             generic-switch  ; Inherit default values from a template
        host_name       RouterADSL      ; The name we're giving to this switch
        alias           RouterADSL      ; A longer name associated with the swit
ch
        address         192.168.1.1     ; IP address of the switch
        hostgroups      routers         ; Host groups this switch is associated
with
        icon_image      router.gif
        statusmap_image router.gd2
        check_command   check_ping!3!200.0,20%!600.0,60%
        max_check_attempts 3
        check_interval      5
        check_period        24x7
        contact_groups      admins
        contacts            nagiosadmin
        notification_interval  15
        notification_period    24x7
```

Figura 15: Definició host RouterADSL

En la figura 16 es mostra la dels serveis que ja estàn per defecte d'un switch o router:

```
root@agusti-VirtualBox: ~
##############################################################################
#
# SERVICE DEFINITIONS
#
##############################################################################
##############################################################################

# Create a service to PING to switch

define service{
        use                     generic-service ; Inherit values from a template
        host_name               RouterADSL      ; The name of the host the servi
ce is associated with
        service_description     PING            ; The service description
        check_command           check_ping!200.0,20%!600.0,60%  ; The command us
ed to monitor the service
        normal_check_interval   5               ; Check the service every 5 minu
tes under normal conditions
        retry_check_interval    1               ; Re-check the service every min
ute until its final/hard state is determined
        }


# Monitor uptime via SNMP

define service{
        use                     generic-service ; Inherit values from a template
        host_name               RouterADSL
        service_description     Uptime
        check_command           check_snmp!-C public -o sysUpTime.0
        }
```

Figura 16: Definició serveis RouterADSL

Si observem la figura 15 de la configuració del host, hem optat per la utilització del check command amb PING, però en els serveis també veiem que està disponible el SNMP, amb el que hauríem pogut utilitzar-lo per rebre totes les dades procedents dels equips que monitoren els sensors.

De totes maneres, no és l'objecte d'aquest TFC extendrens en la total configuració de Nagios, ja que ens caldria un altra treball sobre aquesta materia.

2.2.6.3 Exemple de monitorització

En el següent mapa de Nagios podem veure els diferents equips que hem intentat monitoritzar

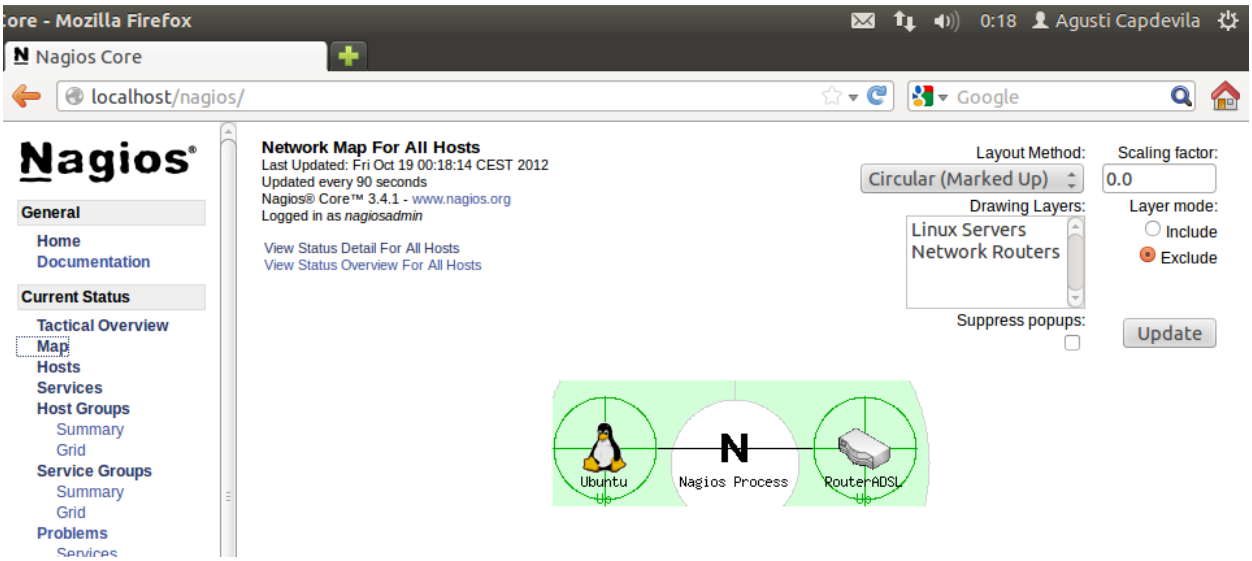


Figura 17: Exemple de monitorització amb Nagios

2.2.7 Altres eines associades a Nagios.

En aquest apartat comentarem que a més de les pròpies característiques de Nagios, de vegades és interessant poder recopilar les dades que anirem reben dels equips que monitoritzen els sensors i poder extreuren gràfiques, de manera que sigui més fàcil o intuïtiu per el administrador de sistemes obtenir una ràpida visió de l'estat dels serveis, equips i de les variables ambientals.

Esmentarem a continuació una breu descripció d'eines que faciliten aquests gràfics.

2.2.7.1 RRDTool

RRDtool2 és l'acrònim de "Round Robin Database tool". Es tracta d'una eina per generar gràfiques i obtenir dades estadístiques directament d'una base de dades.

El mètode Round Robin permet explorar una llista ordenadament i de forma circular (tornant al primer element després d'analitzar l'últim).

2.2.7.2 N2RRD

N2RRD3 és un acrònim de "Nagios to Round Robin Database". Es tracta d'una eina que emmagatzema dades generades pels plugins de Nagios en bases de dades Round Robin.

N2RRD inclou l'eina de visualització rrd2graph, encara que els arxius que genera es poden visualitzar utilitzant qualsevol altra eina de visualització com per exemple CACTI.

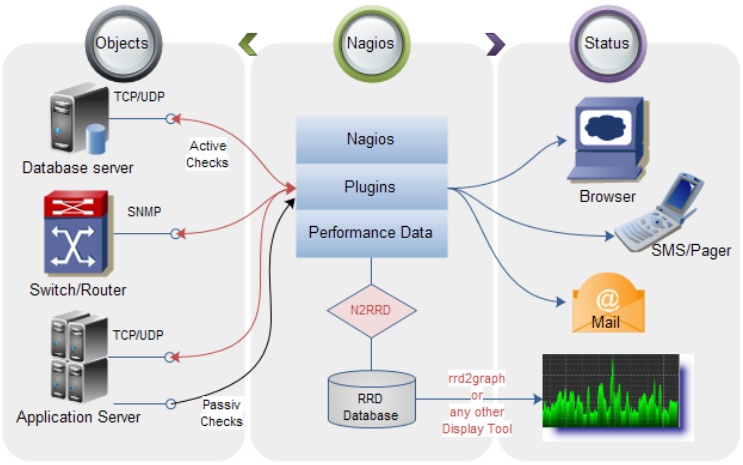


Figura 18: Arquitectura N2RRD

2.2.7.3 CENTREON

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

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

- Eina de configuració avançada
- Gràfics en temps real
- Informes detallats
- Interfície multiusuari

2.2.7.4 Generació de gràfiques

Mitjançant l'eina RRDTool i el plugin Nagios2RRD, Nagios guarda les dades en bases de dades circulars, monitoritzant les 24 hores del dia tots els dies de la setmana, de manera que es genera una gran quantitat de dades.

Amb l'eina RRDTool les bases de dades són circulars i de mida definida, de manera que les dades es sobreescriuen seguint un procés circular.

Font de la figura 18 : http://n2rrd-wiki.diglinks.com/display/n2rrd/Addon

2.3 Sensors Ambientals

En el marc tecnològic d'aquesta memòria ja varem descriure el que eren els sensors i algunes de les seves característiques. En aquest apartat ens centrarem però en els principals sensors que mesuren les variables ambientals d'un CPD, com la temperatura, humitat, inundació i fum. Esmenterem també d'altres dos sensors importants com la detecció de fallada d'energia i detecció d'apertura.

2.3.1 Sensors de Temperatura

La mesura de la temperatura és un dels aspectes més importants dels centres de dades i que cada vegada més ha anat en augment. Les velocitats dels processadors, els factors de forma de servidors petits, una concentració elevada de racks afecten de manera important en la temperatura d'un CPD, de manera que és necessari la seva monitorització per millorar el rendiment i la eficiència del aire condicionat de la sala. Els marges de temperatura i la seva ubicació són també importants.

La darrera recomenació d'ASHRAE TC 9.9[1] per la temperatura en un CPD, és que hauria de cobrir un rang entre el 18ºC i 27ºC.

2.3.1.1 Conceptes i definició de Temperatura

La temperatura és un paràmetre termodinàmic del estat d'un sistema que caracteritza el calor. En el Sistema Internacional d'Unitats, la unitat de temperatura és el Kelvin (K) i la escala de referencia és la Kelvin o escala absoluta, que s'assòcia el valor del cero absolut, i es gradua amb una mida de grau igual al grau Celsius. En àmbits fora del científic , també està molt generalitzat l´ús de l'escala Celsius o centígrada (ºC)), a excepció dels Estats Units, que utilitzen la escala Fahrenheit (ºF).

2.3.1.2 Tipus de Sensors de Temperatura

Com a dispositius per mesurar la temperatura en tenim principalment de tres tipus :

- ***Dispositius Elèctrics*** : Termoparells, RTDs, Termistors,Diodes, etc.
- ***Dispositus Mecànics*** : Sistemes de dilatació (capil·lars), termòmetres de vidre, bimetal.lics, etc.
- ***Dispositius de Radiació tèrmica***: Piròmetres de radiació, termòmetres infrarrojos, òptics, etc.

Dels dispositus indicats (tot i que ni han de molts més tipus) els que sense dubte són més utilitzats en la industria són els sensors de **tipus elèctric**. A continuació definirem alguns tipus dels principals sensors elèctrics:

- ***Termoparells*** : Els termoparells basan el seu funcionament en la unió de dos fils de metalls diferents en un extrem, i que al aplicar temperatura en aquesta unió es produeix un voltatge molt petit, del ordre de milivolts que augmenta en funció de la temperatura. Aquesta propietat termoelèctrica la va descobrír T.J. Seebeck a l'any 1821 i es conegut també com efecte "Seebeck".

  Aquest dispositus són fràgils i acostumen anar encapsulats en vaines per a protegirlos de les condicions extremes dels processos industrials que han de controlar. Com avantatge principal, els termoparells poden cobrir un ampli rang de temperatures entre -200ºC a 2800ºC. L'inconvenient però és la seva baixa precisió i que precisen circuits de d'acondicionament o compensació de la senyal per no ser lineals.

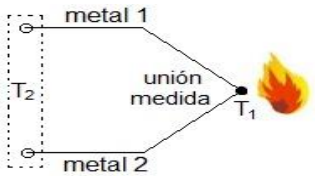


Figura 19: Esquema d'un termoparell

[1] *ASHRAE TC9.9 Mission Critical Facilities (infraestructures de misió crítica), "Thermal Guidelines for Data Processing Environments" 2011.*

- ***Termorresistencies o RTD*** : Les RTD són metalls que amb l'augment de temperatura augmenta també la seva resistència. La seva principal característica és que són elements molt lineals, precisos i estables. Poden cobrir un ampli rang de temperatures entre -250ºC fins a 1100ºC en el cas del Platí, on els detectors amb aquest material són els de més qualitat, estables i amb una gran exactitud fins a una temperatura de 500ºC.

  Les RTD amb tot però, tenen un cost elevat precisament per aquests materials. Són dispositius pasius o bé que necessiten d'una alimentació de tensió. Són poc resistents també i necessiten ser encapsulats o protegits.

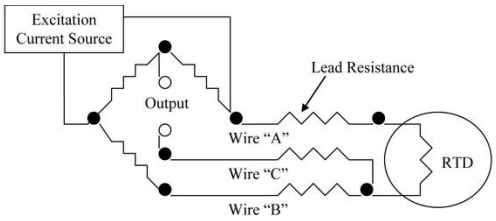


Figura 20: Circuit excitació d'una RTD

- ***Termistors***: Els termistors són semiconductors electrònics sensibles a la temperatura. Ni han de dos tipus, els NTC (*Negative Temperature Coefficient*) i els PTC (*Positive Temperature Coefficient*). Ambdos tipus tenen una resposta no lineal i decreixent amb l'augment de temperatura en el cas dels NTC i creixent per els PTC. Són molt sensibles, precisos i amb un temps de resposta molt ràpid. Ténen uns marges de temperatura que van dels -200ºC als 450ºC.

  Són dispositius pasius i molt més econòmics que les RTD. Normalment els termistors serveixen per mesurar la temperatura tant de gasos, com de líquids i sòlids. També pel seu reduït tamany normalment van inserits en allotjaments especialment dissenyats i adaptats a les necessitats de l'entorn que han de mesurar. Normalment els termistors més utilitzats són de llarg els NTC.

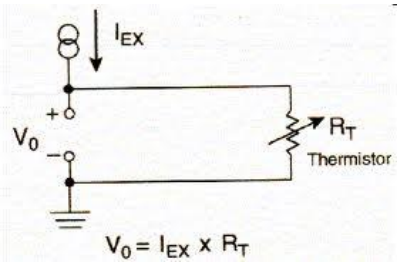


Figura 21: Circuit excitació d'un termistor

2.3.1.3 Millors pràctiques per l'ubicació de sensors de temperatura

Un factor clau de les temperatures dels centres de dades és saber on prendre mesures. En definitiva un mal lloc on prendre aquestes mesures, podria ser igual a no fer rés, per tant més que centrar-se en mesurar la temperatura de la sala, segons especialistes en aire acondicionat indiquen que la temperatura a tenir en compte és l'aire que entra al rack de servidors, perquè aquest aire és el que s'utilitza per eliminar la calor generada per el servidors. Així doncs, com a millors practiques en relació la situació dels sensors de temperatura, es recomanen els següents criteris:

- ***Temperatura mínima de cobertura*** : Posar 1 sensor de temperatura a la meitat de l'altura de la part frontal del rack i 1 sensor a la meitat de l'altura de la part posterior del rack

- ***Temperatura típica de cobertura*** : Posar 2 sensors de temperatura a la part frontal de cada rack ,a uns 40 cm de la part inferior i uns 40 cm de la part superior i 1 sensor a la meitat de l'altura de la part posterior del rack

- ***Temperatura màxima de cobertura***: Posar 3 sensors de temperatura a la part frontal de cada rack a uns 40 cm de la part inferior, a la meitat i uns 40 cm de la part superior i 1 sensor a la meitat de l'altura de la part posterior del rack

2.3.2 Sensors d'Humitat

La mesura d'humitat és un altra dels paràmetres importants en un centre de dades. No només la temperatura afecta el rendiment dels sistemes, sinó també la humitat poden provocar un ràpid deteriorament dels sistemes. La vigilància de la humitat en un centre de dades és tan important com el control de la temperatura. Una humitat massa baixa pot donar lloc a electricitat electrostàtica, causant danys immediats permant equip i una humitat molt alta podria crear condensacions i corrosió en els components, que sovint és un procés lent i irreversible.

Actualment segons ASHRAE TC 9.9[2], la humitat recomanada en un CPD hauria de ser menor del 60% RH, juntament amb una temperatura de punt de rosada inferior a 5.5ºC i superior a 15ºC.

2.3.2.1 Conceptes i definició d'humitat.

La humitat és un fenomen natural que es presenta a nivell molecular, i es troba bàsicament relacionada amb la quantitat de molècules d'aigua presents en una determinada substància, la qual pot estar en estat sòlid o de gas. Normalment es denomina humitat ambiental a la quantitat de vapor d'aigua present en l'aire.

Es pot expressar en forma absoluta mitjançant la humitat absoluta, o de forma relativa mitjançant la humitat relativa o grau d'humitat. La humitat relativa és la relació percentual entre la quantitat de vapor d'aigua que hi ha en l'aire i la que necessitaria contenir per saturar l'aire a idèntica temperatura. Quan més gran és la temperatura, més capacitat tindrà l'aire per absorbir el vapor d'aigua. La humitat relativa s'expresa en percentatge, de manera que quant aquesta arriba al 100% significa que l'aire està saturat d'aigua.

La majoria de sensors d'humitat es basan en la humitat relativa.

2.3.2.2 Tipus de Sensors d'humitat.

Bàsicament hi han tres tecnologies per mesurar la humitat relativa: sensors d'humitat capacitius, sensors d'humitat resistius i sensors per conductivitat.

A continuació es citen les principals característiques de cada tipus:

- ***Sensors d'humitat capacitius*:** Són potser els més difosos en la indústria i en meteorologia**,** ja que són de fàcil producció, baix costs i alta fidelitat. Els sensors d'humitat capacitius estan formats per un substrat en el qual una fina capa de polímer o òxid de metall es diposita entre dos elèctrodes conductors. La superfície sensible és coberta amb un elèctrode porós metàl·lic per protegir-lo de la contaminació que hi ha en l'ambient que es troba. El substrat pot ser de vidre, ceràmic o de silici.

  El canvi de la constant dielèctrica del sensor d'humitat capacitiu és directament proporcional a la humitat relativa de l'ambient en què es troba. Els principals avantatges dels sensors d'humitat capacitius són la seva aproximació gairebé lineal en un marge d'humitats, el seu ampli espectre de mesura i la seva estabilitat a llarg termini.

Figura 22: Principi del Sensor Humitat capacitiu.

[2] *ASHRAE TC9.9 Mission Critical Facilities (infraestructures de misió crítica), "Thermal Guidelines for Data Processing Environments" 2011.*

- ***Sensors d'humitat resistius:*** Mesuren el canvi en la impedància elèctrica d'un mitjà higroscòpic com pot ser un polímer conductor, una sal o un substrat tractat. Els sensors resistius tenen una resposta no lineal davant canvis d'humitat relativa i per tant han de ser tractats per circuits per ser linealitzats. Tenen major exactitud a altes humitats relatives però menor exactitud a baixes respecte als sensors d'humitat capacitius. Són elements de baix cost i grandària i tenen una bona estabilitat a llarg termini.

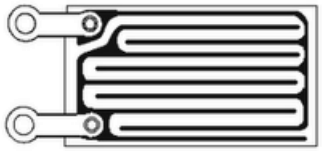


Figura 23: Sensor Humitat resistiu

- ***Sensors d'humitat per conductivitat:*** Aquests sensors basen el seu funcionament en mesurar la humitat absoluta quantificant la diferència entre la conductivitat en un material sec i un material que conté vapor d'aigua de l'aire. Aquests sensors tenen una major resolució que els capacitius i resistius a temperatures per sobre dels 90 º C.

2.3.2.3 Millors pràctiques per l'ubicació de sensors d'humitat

La humitat no varia tant ràpidament com la temperatura en un centre de dades i els sensors d'humitat normalment es col·loquen en els passadissos freds o en espaiats bastant grans.

Com millors pràctiques es recomana prendre en compte:

- ***Humitat mínima de cobertura***: Posar 1 sensor d'humitat a la mitad de cada filera de racks (a la part frontal d'un rack)
- ***Humitat típica de cobertura*** : Posa 1 sensor d'humitat cada 5 racks (a la part frontal d'un rack)
- ***Humitat màxima de cobertura*** : Posa 1 sensor d'humitat cada 3 racks (a la part frontal d'un rack)

És força habitual que alguns fabricants combinin sensors de temperatura i humitat en un mateix dispositiu, de manera que facilita molt el cablejat dins d'un mateix bastidor.

Font de la figura 19 : http://scileaden.com/
Font de la figura 20 : http://www.jms-se.com/rtd.php
Font de la figura 21 :http://www.unet.edu.ve/~ielectro/Sensores%20de%20Temperatura.htm
Font de la figura 22 :http://www.monografias.com/trabajos10/humed/humed.shtml
Font de la figura 23 :http://granadoangel.blogspot.com.es/

2.3.3 Sensors per detecció d'aigua

Els danys per aigua és probablement una de les amenaces ambientals més desconegudes en un centre de dades. L'aigua en una sala de servidors poden provenir de múltiples fonts com ara per els defectes dels sistemes d'aire condicionat, les fuites de canonades que passen a través de la sala d'ordinadors o bé les fuites en les sales del costat o sobre les sales d'ordinadors.

Les inundacions d'aigua sovint no són visibles ja que la major part d'equips informàtics o de comunicacions que estan instal.lats en els racks, es troben en un pis elevat per facilitar el cablejat. Els sensors per inundació són els més adequats per evitar aquests riscos i prevenir-los.

2.3.3.1 Tipus de sensors per detecció d'aigua o d'inundació (flooding)

Els sensors per a detecció de liquids basen el seu principi en la propietat conductora de l'aigua, de manera que el detector està format per un parell de contactes separats tal que al entrar en contacte amb l'aigua tancaria el circuit i donaria un avís alarma.

Bàsicament en tenim de dos tipus :

- ***Detecció puntual de líquids*** (***flood sensor spot***) : aquest són emprats per detectar punts concrets on sigui susceptible la presencia de filtracions de líquids.

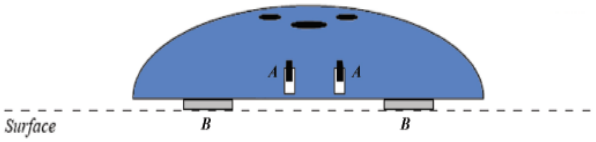


Figura 24: Detall Detector de líquids tipus puntual

- ***Detecció de líquids per cable*** (***flood sensor w/cable***) : aquest tipus és el més recomenat per fer una detecció de líquids distribuïda. En el fals sòl de les sales d'ordinadors el sistema de detecció per cable proporciona una cobertura total trobant la fuita abans que es converteixi en un problema.

  El cable detector està format per tres fils, que al detectar el líquid en tot el seu recorregut permet detectar filtracions en el seu origen. Aquest cable esta dissenyat per ser extremadament resistent a la corrosió i abrasió, i no permet que la humitat quedi atrapada en la seva constitució, ja que s'aseca ràpid.

  Com a millors pràctiques el cable s'instal·la al perímetre de la sala, prop de desaigües, canonades d'aigua i equips CRAC o aire condicionat. Tot i que no hi ha pautes concretes en la industria.

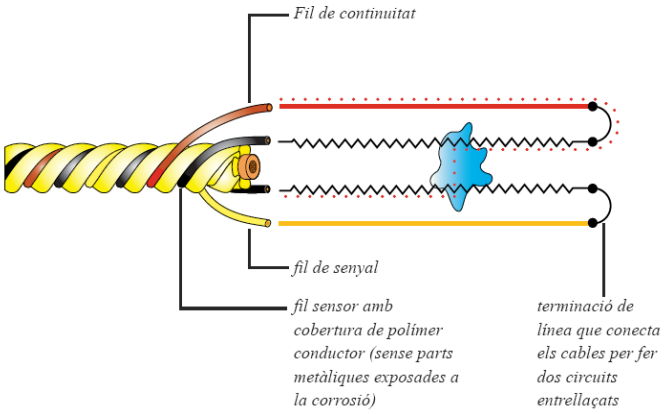


Figura 25: Detall Cable Detector de líquids

Font de la figura 24 : http://avtech.com/Products/
Font de la figura 25 : http://www.tracelec.com/pdf/pdf211(ES).pdf

2.3.4 Sensors per detecció de fum

No menys important que la detecció d'agua, és la detecció de foc o fum en un centre de dades en el que a monitorització ambiental respecte. Apart dels equips contra incendis que normalment disposent els CPD d'acord a les normes TIA-942 , un dels requisits per establir una estratègia de protecció contra el foc ha de respondre a tres factors : detecció, alarma i extinció. El sistemes de detecció proactius de fum són els principals protagonistes. Per generar una prealarma aquest sistemes de detecció s'han de distribuir per tot el CPD i principalment als punts calents o més susceptibles de poder iniciar un incendi. Aquestes alarmes poden avançar un avís perquè els especialistes verifiquin quin és el problema. Posteriorment els sistemes VESDA, com exemple d' una de les marques més conegudes en sistemes d'extinció poden evitar el pitjor.

2.3.4.1 Conceptes dels detectors de fum

Els detectors de fum son dispositus que s'activen amb las partícules visibles o invisibles de la combustió. Atés aquest principi, els detectors de fum són sistemes de seguretat que detecten la presència de fum en l'aire fruit de la combustió i activen una senyal alertant d'un potencial origen d'incendi.

2.3.4.2 Tipus de sensors per detecció de fum

En funció del mètode emprat per a la detecció, aquests detector de fum es classifiquen en sis grups: detectors fotoelèctrics, iònics, de pont de resistència, per anàlisi de mostra, combinats i de combustió tipus Taguchi amb semiconductor.

A continuació esmentarem només els fotoelèctrics i els iònics per ser els més emprats:

- ***Detectors Fotoelèctrics*** : També són coneguts com detectors òptics. Ni han de dos tipus:
  - **Detectors de raig infraroig**, formats per un dispositu emissor i un altra de receptor. Quan l'espai entre ells enfosqueix a causa del fum, només una fracció de la llum emesa arriba al receptor provocant que el senyal elèctric produït per aquest sigui més feble i s'activi l'alarma.
  - **Detectors de tipus puntual,** formats per un emissor i un receptor que es troben allotjats en el mateix recinte, però no es veuen en formar els seus eixos un angle major de 90 º i estar separats per una pantalla, de manera que el raig emès no arriba al receptor.

    Quan entra fum a la cambra el feix de llum emès es refracta en les partícules de fum i pot aconseguir al receptor, activant l'alarma.

    És el tipus més utilitzat ja que té una resposta molt ràpida del fum i són de fàcil muntatge. Té l'inonvenient que si el fum és negre no el detecta.

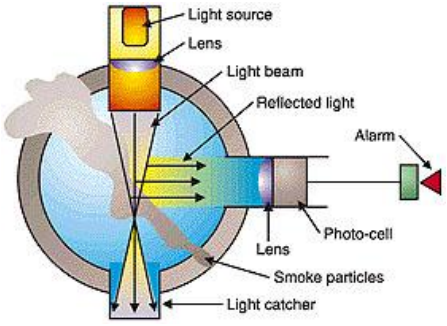


Figura 26: Principi del detector de fum fotoelèctric

Font de la figura 26 : http://www.engineersgarage.com/articles/smoke-detectors?page=3

- ***Detectors iónics*** : Aquest tipus de detector és més barat que l'òptic i pot detectar partícules que són massa petites per influir en la llum. La càmara d'ionització d'aquestes alarmes, conté una ínfima quantitat (menys d'1 microgram) de americi-241 que emet radiació alfa. Aquest isòtop radioactiu emet partícules alfa (nuclis d'heli d'alta energia) durant segles. A causa de la gran capacitat d'ionitzar l'aire de les partícules alfa, només un full de paper o uns 7 cm d'aire són suficients per absorbir-les.

  La radiació passa a través d'una càmera oberta a l'aire en la qual es troben dos elèctrodes, permetent una petita i constant corrent elèctric. Si entra fum en aquesta cambra es redueix la ionització de l'aire i el corrent disminueix o fins i tot s'interromp, amb el que s'activa l'alarma. Quan el fum entra a la cambra de ionització, les partícules alfa queden pràcticament immobilitzades pels productes de la combustió, disminuint notablement el corrent elèctric. Ni han també basats en partícules beta.

2.3.5 Altres sensors

Fins ara s'han detallat els sensors per monitoritzar els principals paràmetres ambientals d'un CPD. A continuació definirem altres sensors que també tenen rellevant importància per un Centre de Dades, encara que sense dubte podríem citar d'altres que ens ocuparia un nou treball.

2.3.5.1 Sensors de fallada d'energia

En general, els Centres de Dades en el seu interior tenen una qualitat d'energia superior a la que es té en edificis destinats a oficines, però cal fer ús d'alguns dispositius dels que es pugui assegurar que l'energia estigui correctament administrada i flueixi als diferents equips dins de la sala de forma neta.

És comú que en un Centre de Dades es tinguin equips de protecció d'energia com reguladors, supressors de pics o UPS, sistemes d'aire condicionat que proveeixin un clima controlat i també racks o armaris d'ubicació física per als elements de xarxa com switches, encaminadors, servidors, tallafocs, IDS, etc. Tots ells, es poden energitzar de forma neta i administrada a través d'un PDU (Unitat de Distribució d'Energia).

Tot i que normalment els PDU tenen dispositius que controlen fallades d'energia, també hi han sensors de fallada d'energia més simples amb funcionalitats de monitoratge remot que permeten conèixer el consum elèctric o identificar alguna interrupció d'energia. Aquesta característica és important i s'ha de prendre en compte, ja que d'aquesta manera es poden establir alertes o notificacions que arribin a l'administrador per donar millor temps de resposta en l'atenció d'aquests incidents i garantitzar l'eficiència energètica del CPD o qualsevol pèrdua sobtada de dades.

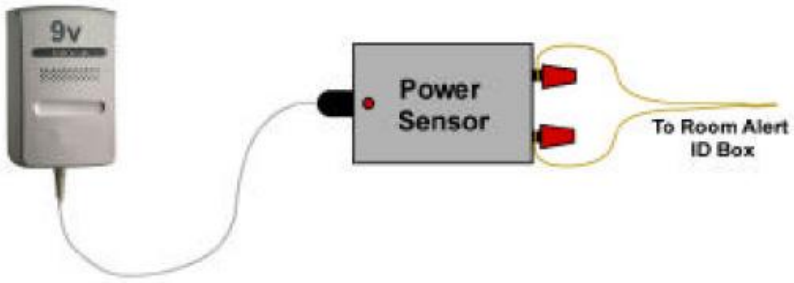


Figura 27: Detector de fallada d'energia

Font de la figura 27 : http://avtech.com/Products/

2.3.5.2 *Sensors d'apertura*

Tot i que aquest sensors responen a causes de seguretat física més que de tipus ambiental, és important de vegades tenir monitoritzat si es té accés a un armari o rack, o una entrada no autoritzada o forçada amb fins malintencionats, provocant danys als equips, o bé per evitar pèrdues d'aire dins de la sala climatitzada.

Només esmentarem que aquest sensors d'apertura proporcionen en temps real el reconeixement de si una porta està oberta. L'ús estàndard és muntar el sensor connectat al marc d'una porta d'un rack o bastidor i de l'accés al CPD. A continuació, cal muntar l'actuador oposat corresponent del sensor a la pròpia porta. Quan la porta s'obre, els dos components es separen i s'obté una senyal binaria que ens dona l'avís corresponent.

2.3.6 Recollida i monitorització dades

Una vegada escollits i instal.lats els sensors, el pas següent seria la recollida i anàlisis de les seves dades. En general, els sensors en si mateixos no es poden conectar de forma individual a la xarxa IP, sinó que necessiten de dispositius electrònics que interpretin les dades d'aquest sensors i enviïn alertes al sistema central.

Aquest dispositius recol.lectors s'anoment també **monitors de dades** i normalment estan instal.lats de manera distribuïda en area físiques limitades i diferents dins del CPD per reduir la complexitat del cablejat dels sensors, a més d'eliminar el risc d'un únic punt de fallada que es podria produir en utilitzar un únic dispositu recol.lector central. Amb aquesta arquitectura, tots els monitors poden anar connectats a una xarxa IP i conectarse a un sistema de monitorització central.

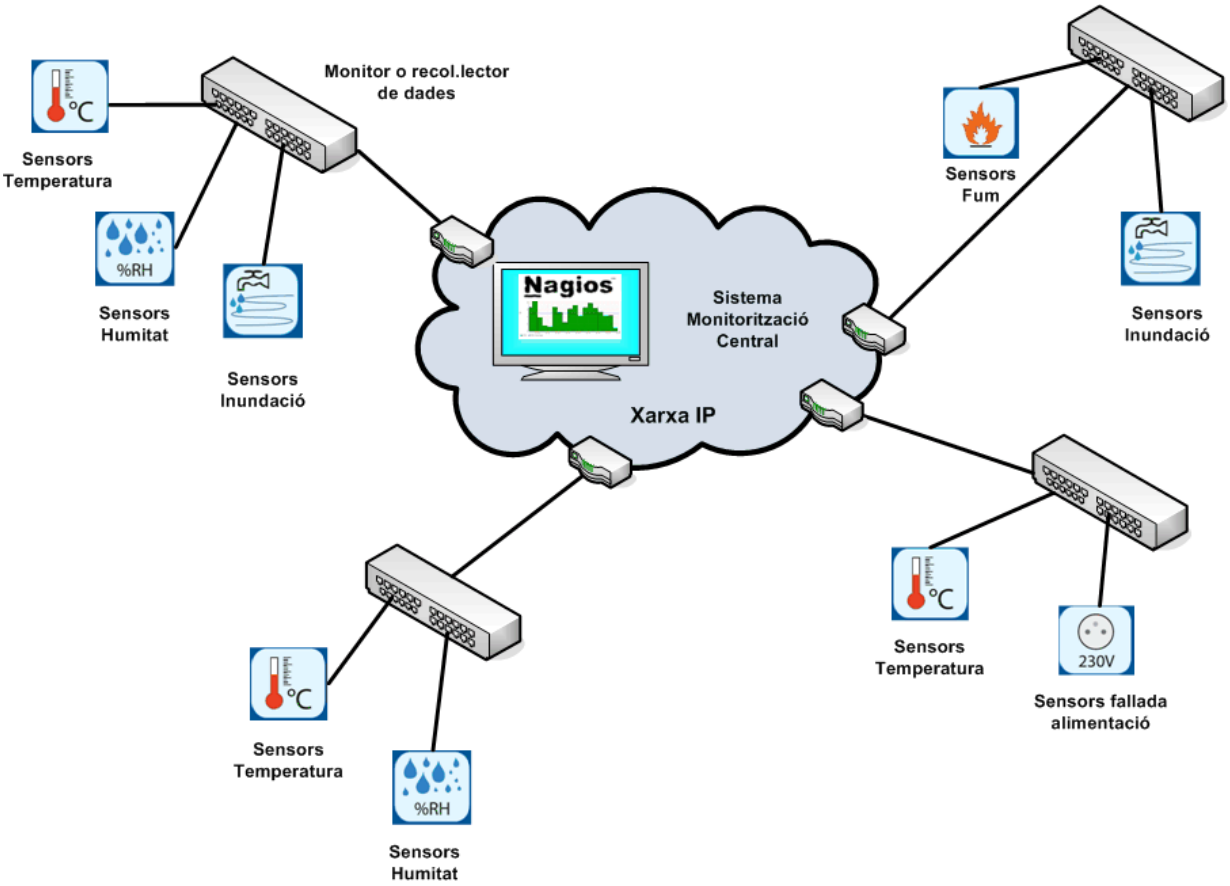


Figura 28: Arquitectura Monitorització Distribuida

2.3.7 Solució de monitorització ambiental

A partir de la base teòrica vista fins el moment, és definirà a continuació una proposta de solució bàsica per un Centre de Dades de dimensions petites (10 mts x 20 mts) i detallarem el tipus de sensor a utilitzar. Per les reduïdes dimensions del CPD proposat, s'ha optat per sensors amb tecnologia de cablejat convencional, en lloc de tecnologia inal.lambrica. De totes maneres seria compatible amb el mateix sistema instal.lar sensors inal.làmbrics.

Per a aquesta solució s'ha considerat, dels molts possibles distribuïdors comercials consultats sobre monitorització ambiental que hi ha al mercat, un dels fabricants principals en aquesta anomenat AVTECH. Aquest distribuïdor amb seu a Warren- Rhode Island (EUA), és el que m'ha semblat tenir equipament per a monitorització ambiental més complert i a preus força assequibles.

2.3.7.1 Tipus sensors escollits i especificacions.

Sensor de Temperatura

Variable ambiental monitoritzada	Temperatura
Tipus/Tecnologia del sensor	Termistor , tractament senyal analogic a digital pel monitor
Rang Sensor Temperatura	-55º a 125º C
Precissió Sensor Temperatura	+/- 0.125 %
Alimentació sensor	VoltFree (través d'unitat de monitorització)
Conexió Sensor i Cable Tipus	RJ-11 Cable
Longitud Cable Sensor estandard	7,5 mts
Nombre de sensors s/millors pràctiques	3 unitats per rack
Ubicació	Rack

Figura 29: Especificacions i detall del sensor Temperatura AVTECH

Sensor de Temperatura i Humitat

Variable ambiental monitoritzada	Temperatura i humitat
Tipus/Tecnologia del sensor	Termistor, RH Capacitiu , tractament senyal analogic a digital pel monitor
Rang Sensor Humitat / Temperatura	0% a 100% RH / -40º a 85ºC
Precissió Sensor Humitat / Temperatura	+/-3.5 % / +/-0.125 %
Alimentació sensor	VoltFree (través d'unitat de monitorització)
Conexió Sensor i Cable Tipus	RJ-11 Cable
Longitud Cable Sensor estandard	7,5 mts
Nombre de sensors s/millors pràctiques	1 unitat per cada filera de racks
Ubicació	Rack

Figura 30: Especificacions i detall del sensor Temperatura i Humitat AVTECH

Sensor d'inundació (flooding sensor)

Variable ambiental monitoritzada	Aigua
Tipus/Tecnologia del sensor	Cable detecció , senyal tipus binari
Alimentació sensor	5VDC 1A Adapter
Longitud Cable detecció	7.5 mts
Cable Detecció d'extensió	2,5 mts via AVTECH Flood Cable Extender
Conexió Sensor i Cable Tipus	RJ-11, 2 Wire Sensor Cable
Longitud Cable Sensor estandard	7,5 mts
Nombre de sensors s/millors pràctiques	No hi ha instruccions en la industria
Ubicació	Sala , a prop d'equipaments CRAC

Figura 31: Especificacions i detall del sensor d' inundació AVTECH

Sensor de Fum (smoke sensor scape light)

Variable ambiental monitoritzada	Fum
Tipus/Tecnologia del sensor	Fotoelèctric , senyal tipus binari
Alimentació sensor	9V Alkaline Battery. Avís sonor de bacteria esgotada.
Conexió Sensor i Cable Tipus	RJ-11, 2 Wire Sensor Cable
Longitud Cable Sensor estandard	7,5 mts
Nombre de sensors s/millors pràctiques	1 unitat per rack , tot i que no hi ha pautes en la industria
Ubicació	Rack

Figura 32: Especificacions i detall del sensor de fum AVTECH

Sensor de fallada d'energia (power sensor)

Variable ambiental monitoritzada	Power
Tipus/Tecnologia del sensor	Detecció, Senyal tipus binari
Alimentació sensor	5VDC 1A Adapter
Conexió Sensor i Cable Tipus	RJ-11, 2 Wire Sensor Cable
Longitud Cable Sensor estandard	7,5 mts
Nombre de sensors s/millors pràctiques	1 unitat per PDU
Ubicació	PDU

Figura 33: Especificacions i detall del Power Sensor AVTECH

Sensor de apertura (room entry sensor)

Variable ambiental monitoritzada	Apertuta Portes
Tipus/Tecnologia del sensor	Detecció, Senyal tipus binari
Alimentació sensor	5VDC 1A Adapter
Conexió Sensor i Cable Tipus	RJ-11, 2 Wire Sensor Cable
Longitud Cable Sensor estandard	7,5 mts
Nombre de sensors s/millors pràctiques	1 unitat per RACK I accés sala
Ubicació	Rack i Sala

Figura 34: Especificacions i detall del Room Entry Sensor AVTECH

2.3.7.2 Tipus Monitor de dades escollits i especificacions

Principalment centrarem la nostra solució en els dos dispositius recol.lectors següents:

Monitor Room Alert 24E

Adaptat a montatge en Rack (1U 19")
1 Sensor temperatura i humitat incorporats
6 canals externs per connexió sensors digitals
16 canals externs per connexió sensors tipus switch
1 port expansió connexió RJ-45
Longitud Cable Sensors externs fins a 30 mts
Interface Ethernet
Ethernet Port & Tipus RJ45, 10/100Mbps Base TX
Valors i alertes en temps real
Mètodes Alertes : Email, SNMP Trap, SMS, Web
Supported Protocols SNMP v1
Unitats de Temperatura en ºC i ºF
Alimentació 110/240 VAC, 50/60 Hz
Font alimentació 5VDC 1A inclosa

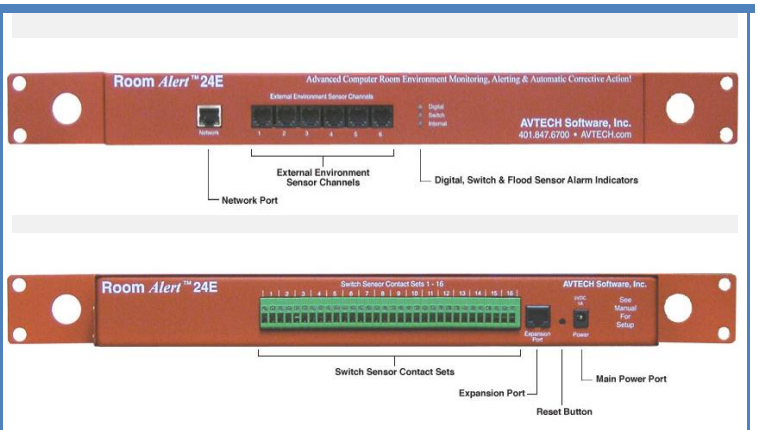


Figura 35: Especificacions i detall del Monitor Room Alert 24E AVTECH

Monitor TempPageR 3ER

Adaptat a montatge en Rack (1U 19")
1 Sensor temperatura incorporat
2 canals externs per connexió de sensors digitals
1 port expansió connexió RJ-45
Longitud Cable Sensors externs fins a 30 mts
Interface Ethernet
Ethernet Port & Tipus RJ45, 10/100Mbps Base TX
Valors i alertes en temps real
Mètodes Alertes : Email, SNMP Trap, SMS, Web
Supported Protocols SNMP v1
Unitats de Temperatura en ºC i ºF
Alimentació 110/240 VAC, 50/60 Hz
Font alimentació 5VDC 1A inclosa

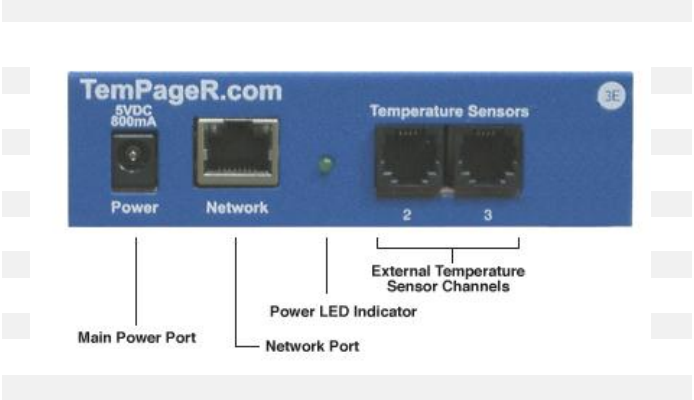


Figura 36: Especificacions i detall del TempPageR 3ER AVTECH

2.3.7.3 Distribució de Sensors i Monitors Ambientals

En aquest apartat definirem el criteris per el nombre i ubicació dels sensors que conformarà la solució de monitorització del nostre CPD virtual de petites dimensions (10 x 20 mts).

- ***Sensors Temperatura***: en relació als sensors de temperatura s'ha fixat una temperatura de cobertura típica amb 2 sensors a la part frontal de cada rack ,a uns 40 cm de la part inferior i uns 40 cm de la part superior i 1 sensor a la meitat de l'altura de la part posterior del rack
- ***Sensors Humitat***: al ser un CPD petit , s'ha establert una cobertura d'humitat mínima i corresponent a un sensor d'humitat a la mitat de cada filera de racks i situat a la part del rack en contacte amb el passadís fred.
- ***Sensors detecció líquids***: No hi ha en principi una pauta definida en la industria, però normalment s'acostuma a instal.lar per l'entorn de cada sistema CRAC i per sota del fals terra, en punts susceptibles d'existència de filtracions d'aigua. En la solució s'ha previst un sensor de detecció de líquids per cable de detecció d'uns 10 mts entorn a l'equip CRAC.
- ***Sensors de fum*** : En CPD's petits on normalment el pressupost d'un equip contra incendis dedicat que compleixi amb la normativa TIA 942 i codis de construcció de Centres de Processament de Dades pot ser no adequat a la inversió, llavors una possible solució és la col.locació d'un sensor de fum per rack que pot proporcionar un cert grau d'avís proactiu. Tampoc hi ha pautes que defineixin el nombre de sensors de fum a instal.lar.
- ***Sensors de fallada d'energia*** : Suposem també que la PDU no té un sistema propi d'avís de fallades d'energia, pel que hem optat per instal.lar un sensor de fallada d'energia al punt de connexió de distribució d'energia de la PDU per cada filera de racks.
- ***Sensors d'apertura de portes:*** tot i que ja vam comentar que responen més a securetat física que a una amenaça ambiental, hem optat per instal.lar un sensor d'apertura de portes per cada rack i un altra sensor a la porta d'accés. En tot cas, aquest darrer seria el més relacionat amb una monitorització ambiental, ja que podria advertir d'una pèrdua de l'eficiència del aire acondicionat de la sala en el cas d'haver la porta oberta per un descuit del personal.
- ***Dispositius recol.lectors de dades***: Donat al nombre de sensors establert s'ha considerat dos monitors RoomAlert 24E per tractar les senyals dels sensors de fum, detecció portes, power sensor, detecció líquids, 3 sensors temperatura i 1 d'humitat per cada filera de racks, i ubicat en el rack situat a la meitat de cada filera. La resta de temperatures serà tractada pel dispositiu TempPageR3ER per cada rack. Ampliarem el seu detall en els annexes A i B.

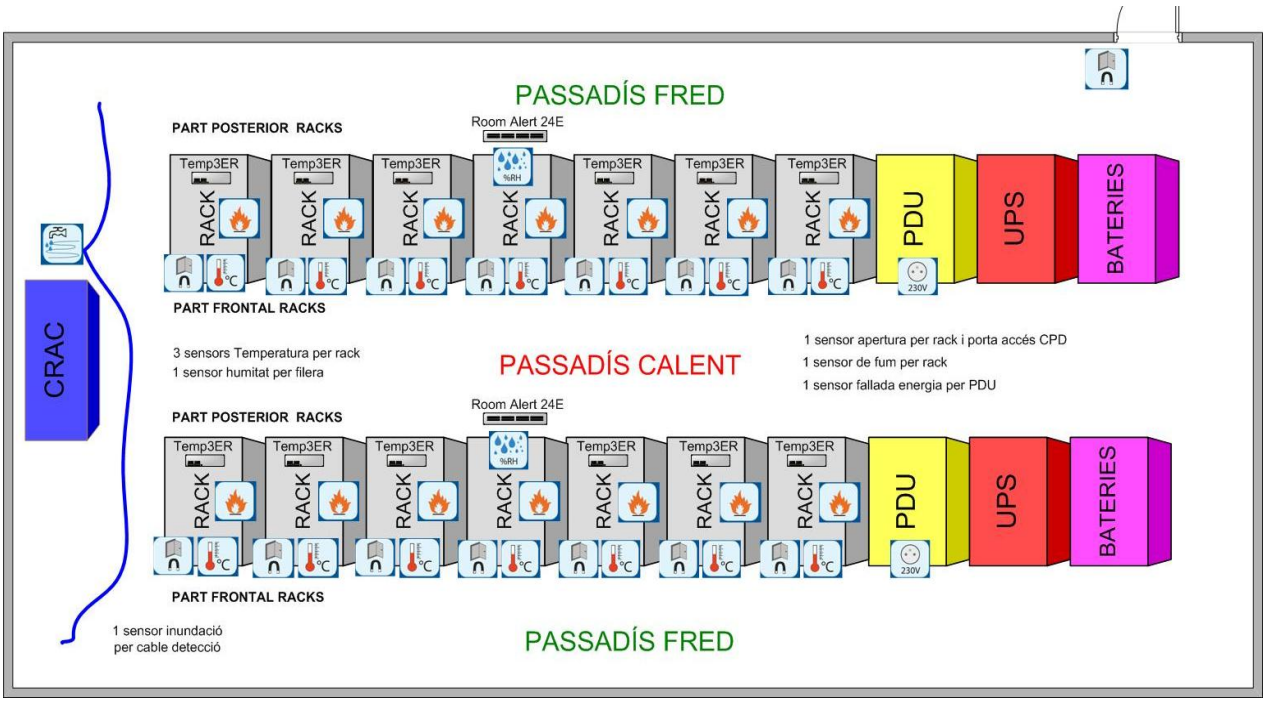


Figura 37: Esquema distribució sensors i monitors ambientals en un CPD

2.4 Valoracions econòmiques

En aquest darrer apartat, farem la valoració de tot l'equipament necessari i bàsic per la monitorització ambiental del nostre CPD proposat.

Les dades corresponents a la construcció i dotació del CPD, com equips CRAC, infraestructura sanitaria, eléctrica, PDU, UPS, bateries, equipament informàtic, equips de comunicacions, bastidors, etc., queden al marge d'aquest TFC.

Com observació particular, s'ha de tenir en compte que els preus indicats són en USD $ (Dòlars Americans) tal com els dona directament el fabricant AVTECH en la seva página web i que pòden estar subjectes a variacions de preu. S'ha considerat posar aquest valors en USD per no introduïr errors de fluctuació de moneda en els valors donats a la taula següent. El valor final será donat també en €.

Pressupost Monitorització Ambiental CPD				
Descripció Dispositiu	**Pack**	**Quantitat**	**Preu Unitari (USD $)**	**Preu Total (USD $)**
Sensor Temperatura	1u / cable 7,5mts / RJ11	14 u	35 $	490 $
Sensor Humitat/Temperatura	Integrat en RoomAlert 24E	0 u	85 $	0 $
Flood Sensor w/7,5m cable detector	1u / cable 7,5mts / RJ11	1 u	375 $	375 $
Smoke Sensor w/scape light	1u / cable 7,5mts / RJ11/9Vbattery	14 u	75 $	1050 $
Power Sensor	Integrat en RoomAlert 24E	0 u	65 $	0 $
Room Entry Sensor	1u / cable 7,5mts / RJ11	13 u	25 $	325 $
Cable extensió	1u / cable 7,5mts / RJ11	30 u	6 $	180 $
Monitor RoomAlert 24E	***Veure annexe A***	2 u	595 $	1190 $
Monitor TemPageR 3ER	***Veure annexe B***	12 u	245 $	2940 $
AVTECH Plugin Pack	Software Package	1 u	475 $	475 $
AVTECH Shipping	Transport Internacional UPS	1 u	381 $	381 $
Nagios Core v 3.4.1	Software Package	1 u	gratuit	0 $
Nagios Plugins v 1.4.16	Software Package	1 u	gratuit	0 $
Nagios Support Plants	Annual support	1 u	2495 $	2495 $
Cost adicional intal.lació estimat	Cablejat, commissioning i posada en servei, incloent: • Ma d'obra instal.lació dispositius en racks i fals terra (estimat 1tècnic sistemes x 1setmana) • Eines i Material instal.lació complementari.	1 u	3000 $	3000 $
			Cost Total en USD $	**12.901 $**
			Cost Total en €	**9.860 €**

Figura 38: Taula valoració econòmica Sistema Monitorització

En la valoració anterior s'han tingut en compte els serveis professionals de suport de la plataforma de Nagios per un periode contractat anual. En relació als serveis professionals de l'empresa AVTECH, no han estat considerats per tenir una amplia cobertura de suport online a través de la seva web i els manuals d'instal.lació són força intuïtius, però el cost addicional per aquets suport anual és d'uns 355$.

També és important considerar que, en el cas d'instal.lar sensors inal.làmbrics, hi hauria un estalvi d'instal.lació de cablejat que repercutiria en el cost final, però que curiosament a nivell de dispositius, el cost normalment és superior que el d'una solució cablejada, doncs es requereixen antenes i adaptadors per els sensors inal.làmbrics.

AVTECH ofereix gratuïtament i conjuntament amb el seus productes de monitorització el programari DEVICE MANAGER, amb una fàcil implementació i amb possibilitat de oferir una gestió de les variables, generar alertes i crear gràfics, pero no deixa de ser un programari comercial i dedicat, on per complir amb les regles d'escabilitat, compatibilitat i flexibilitat que havíem esmentat al principi d'aquesta memòria, no és recomanable fer ús del mateix, ja que si volguesim canviar de producte, ens trobariem limitats amb un únic proveïdor.

Per aquest fet, es creu convenient que NAGIOS segueix sent la millor plataforma, a més de que disposa de moltes més prestacions que DEVICE MANAGER. Amb tot però, si tenim que els sensors d'AVTECH suporten SNMP i són compatibles amb NAGIOS.

NAGIOS ja havíem indicat també que és un programari de codi obert i de distribució gratuïta, però s'ha considerat el suport anual que ofereix. No és un preu econòmic, però possiblement es recomanable en una nova implementació d'un sistema de monitorització tenir aquest suport i evitar pèrdues de temps que serien més costoses.

En resum, podem observar que el cost total de la inversió per la implementació d'un sistema de monitorització ambiental d'un CPD de mida petita no és gens abusiu, per tant la solució de monitorització seria viable per qualsevol petita empresa u organització que vulgui protegir proactivament les seva infraestructura informática i asegurar la disponibilitat de les seves dades a un cost força competitiu.

Obviament la valoració indicada és orientativa i s'han considerat en base als preus actuals del proveïdor AVTECH, però possiblement aquest cost comparat entre d'altres fabricants, podria ser sensiblement més gran en funció de les prestacions. Amb tot però, s'estima que el cost d'una instal.lació bàsica no seria molt significativa.

Segurament el control de les variables ambientals podràn repercutir en la eficiencia energética del seu CPD i en la seva amortització. Igualment davant d'un posible desastre en l'equipament informàtic i la conseqüent pèrdua de dades, el cost seria probablement molt superior.

3 Conclusions

Al inici d'aquest treball vam posar de manifest la importància de monitoritzar les variables ambientals en un CPD i dels seus impactes.

L'objectiu era arribar a una solució en monitorització ambiental d'un CPD i analitzar la seva viabilitat. Per això, s'han contactat empreses relacionades amb el sector per consultar la seva experiència, recomanacions i pautes sobre els sensors ambientals, per valorar en base a els seus productes de referència una possible solució.

Podem concloure que les tecnologies disponibles per monitoritzar les variables ambientals poden cobrir un ampli ventall de possibilitats i destaquen per la seva flexibilitat, facilitat d'implementació i adaptació a qualsevol necessitat.

Així doncs, amb una inversió no molt gran de temps inicial, és possible oferir múltiples solucions a petites i grans empreses a un cost raonable i força competitiu.

Per la gestió i monitorització de les variables ambientals, s'ha apostat per una plataforma de codi lliure com NAGIOS i demostrat la seva simplicitat d'implementació.

És cert que, en principi, cal invertir temps per familiaritzar-se en el seu entorn i probablement sigui un factor negatiu per els responsables de sistemes d'algunes empreses en el moment d'escollirla com a solució, però sens dubte, que el suport d'una comunitat existent en relació a NAGIOS, és una bona referència per la seva el.lecció donades les grans funcionalitats que ofereix aquesta eina.

En resum, penso que els sistemes de monitorització tenen un gran potencial i pot ajudar a moltes empreses i organitzacions a controlar proactivament molts aspectes ambientals i d'eficiència energètica del seu CPD, de forma relativament fàcil, pràctica i econòmica.

A títol personal, el desenvolupament d'aquest treball ha estat del tot profitós i m'ha permés posar en pràctica els coneixements apresos al llarg de la carrera, i demostrar que amb aquests estudis, és possible obrir líneas d'investigació o desenvolupar solucions, de les que sense una experiència prèvia facilitin l'obtenció de conclusions sobre la viabilitat d'algunes infraestructures informàtiques. Aquest fet és el que més m'ha enriquit i del que espero m'ajudi a tenir noves perspectives professionals.

Glosari

ASHRAE: acrònim de l'anglès ***American Society of Heating, Refrigerating and Air Conditioning Engineers***. És una societat dedicada en les tecnològies de la construcció amb més de 50.000 membres a tot el món. La societat i els seus membres es centren en els sistemes de construcció, eficiència energètica, qualitat de l'aire interior, la refrigeració i la sostenibilitat de la indústria.

CGI: acrònim de l'anglès ***Common Gateway Interface***. És un mecanisme de comunicació entre un servidor web i una aplicació externa. CGI especifica un estàndar per transferir dades entre client i programa.

CPD: Centre de Processament de Dades. Edifici on està ubicada tota la infraestructura informática que dona servei a una organització o empresa.

CPU: acrònim de l'anglés de ***Central Processing Unit***. És el component principal de l'ordinador i altres dispositius programables, que interpreta les instruccions contingudes en els programes i processa les dades.

CSV: acrònim de l'anglès ***Comma-Separated Values*** . Són un tipus de document en format obert senzill per representar dades en forma de taula, en què les columnes se separen per comes i les files per salts de línia.

CRAC: acrònim de l'anglès ***Control Room Air Conditioned***. Són sistemes definits per controlar i climatitzar l'aire dels CPD i sales de servidors dins d'uns paràmetres que permeten garantir l'eficiencia de la infraestructura informàtica.

FTP: acrònim de l'anglès ***File Transfer Protocol***. És un protocol de xarxa per a la transferència d'arxius entre sistemes connectats a una xarxa TCP, basat en l'arquitectura client-servidor.

GNU: Acrònim recursiu que significa GNU No és Unix. És un sistema operatiu similar a Unix basat en programari lliure. GNU utilitza normalment un nucli anomenat Linux.

GPL: General Public License o GNU General Public License és una llicància creada per la Free software Foundation en 1989 i orientada principalment per protegir la lliure distribució, modificació i ús de programari. És un segell d'identitat per indicar que un programari és open source i protegirlo contra altres propòsits.

HTML: acrònim de l'anglès ***HyperText Markup Language.*** Fa referència al llenguatge de marcat predominant per a l'elaboració de pàgines web que s'utilitza per descriure i traduir l'estructura i la informació en forma de text, així com per complementar el text amb objectes tals com imatges.

HTTP: acrònim de l'anglès ***Hypertex Transfer Protocol***. És el protocol emprat en cada transacció de la World Wide Web (WWW).

ICMP: acrònim de l'anglès ***Internet Control Message Protocol***. És un sub protocol de control i notificació d'errors del Protocol d'Internet (IP). Com a tal, s'usa per enviar missatges d'error, indicant per exemple que un servei determinat no està disponible o que un router o host no pot ser localitzat.

IEEE: acrònim de l'anglès ***Institute of Electrical and Electronics Engineers***. És una associació tècnic professional dedicada a la estandardització. El seu treball és promoure la creativitat, el desenvolupament i la integració, a més de compartir i aplicar els avanços en les tecnologies de la informació, electrònica i ciències en general per a benefici de la humanitat i dels mateixos professionals. Alguns dels seus estàndards més destacat és el IEEE 802.11.

IPMI: acrònim de l'anglès ***Intelligent Platform management Interface***. És una interfície d'equips estandarditzats utilitzats per els administradors de sistemes per administrar un sistema informàtic i controlar el seu funcionament.

ITIL: acrònim de l'anglès ***Information Technology Infraestructure Library***. És un conjunt de conceptes i pràctiques per a la gestió de serveis de tecnologies de la informació, el desenvolupament de tecnologies de la informació i les operacions relacionades amb aquesta en general.

NNTP: acrònim de l'anglès ***Network News Transport Protocol***. És un protocol inicialment creat per a la lectura i publicació d'articles de notícies en Usenet. La seva traducció literal a l'espanyol és "protocol per a la transferència de notícies en xarxa".

PDU : acrònim de l'anglès ***Power Distribuiton Unit***. És un dispositiu equipat amb sortides múltiples dissenyades per distribuir l'energia elèctrica, especialment als bastidors dels ordinadors i equips de xarxa ubicats dins dels centres de dades.

PING: acrònim de l'anglès ***Packet Internet Groper***. Significa Cercador o rastrejador de paquets en xarxes. Ping és una utilitat diagnòstica en xarxes de computadors i que comprova l'estat de la connexió del host local amb un o diversos equips remots d'una xarxa TCP/IP per mitjà de l'enviament de paquets ICMP de sol·licitud i de resposta.

POP3: acrònim de l'anglès ***Post Office Protocol***. És un protocol d'Oficina de Correu en clients locals de correu per obtenir els missatges de correu electrònic emmagatzemats en un servidor remot. És un protocol de nivell d'aplicació en el Model OSI.

SNMP: acrònim de l'anglès ***Simple Network Management Protocol***. Protocol de la capa d'aplicació que facilita l'intercanvi d'informació entre dispositus d'una xarxa.

SMTP: acrònim de l'anglès ***Simple Mail Transfer Protocol***. És un protocol de la capa d'aplicació i enfocat a l'intercanvi de missatges de correu electrònic entre computadores o altres dispositius (PDA, telèfons mòbils, etc.).

SMS: acrònim de l'anglès ***Short Message Service***. És un servei disponible en els telèfons mòbils que permet l'enviament de missatges curts (també coneguts com a missatges de text, o més col·loquialment, textos) entre telèfons mòbils, telèfons fixos i altres dispositius de mà.

SQL: acrònim de l'anglès ***Structured Query Language***. És un llenguatge declaratiu d'accés a bases de dades relacionals que permet especificar diversos tipus d'operacions en elles.

SSH: acrònim de l'anglès ***Secure Shell***. És el nom d'un protocol i del programa que l'implementa, i serveix per accedir a màquines remotes a través d'una xarxa.

SSL: acrònim de l'anglès ***Secure Sockets Layer***. Són protocols criptogràfics que proporcionen comunicacions segures en una xarxa, normalment en Internet.

TIA: Telecomunications Industry Association. TIA-942 és un estándar que defineix els nivells de disponibilitat que ha de tenir un centre de processament de dades.

TIER: Nivell de disponibilitat davant de fallades en els sistemes d'un CPD. Aquest són 4 nivells definits en el estándar TIA-942.

TCP: acrònim de l'anglès ***Transmission Control Protocol***. Un dels protocols principals en Internet destinats a la comunicació i orientats a connexió i de la fiabilitat del nivell de la capa de transport.

UDP: acrònim de l'anglès ***User Datagram Protocol***. Protocol de la capa de transport basat en l'intercanvi de datagrames i no fiable.

UPS: acrònim de l'anglès ***Uninterruptible Power Supply .*** Són dispositius que gràcies a les seves bateries o altres elements d'emmagatzematge d'energia, poden proporcionar energia elèctrica per un temps limitat a tots els dispositus que tingui connectats, i en el cas d'una fallada del sistema elèctric principal. També s'utilitzen per estabilitar les fluctuacions de corrent que proporciona la xarxa elèctrica principal.

URLs: acrònim de l'anglès ***Uniform Resource Locator***. És una seqüència de caràcters, d'acord amb un format modèlic i estàndard, que s'usa per anomenar recursos a Internet per a la seva localització o identificació, com ara documents textuals, imatges, vídeos, presentacions digitals, etc.

WMI: acrònim de l'anglès ***Windows management Instrumentation***. És la implementació de WBEM (Web-Based Enterprise Management) de Microsoft, que és una iniciativa que pretén establir normes estàndard per accedir i compartir la informació d'administració a través de la xarxa d'una empresa.

XMPP: acrònim de l'anglès ***Extensible Messaging and Presence Protocol***. És un protocol obert i extensible basat en XML, originalment ideat per missatgeria instantània.

XML: acrònim de l'anglès ***eXtensible Markup Language***. És un llenguatge de marques desenvolupat pel World Wide Web Consortium (W3C). Deriva del llenguatge SGML i permet definir la gramàtica de llenguatges específics per estructurar documents grans.

Bibliografía i Refèrencies

[1] Conceptes sobre sistemes de monitorització:

http://es.wikipedia.org/wiki/Sistemas_de_monitorizaci%C3%B3n_y_control

www.rediris.es/difusion/publicaciones/boletin/90/ponencia4.B.pdf

http://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes

http://www.hw-group.com/software/pd_snmp_en.html#IBM_Tivoli

http://doc.ubuntu-es.org/Monitorizaci%C3%B3n/Comparativa

[2] Informació sobre Pandora FMS

http://pandorafms.org/

http://es.wikipedia.org/wiki/Pandora_FMS

http://openideas.info/wiki/index.php?title=Pandora_3.0:Documentation

http://pandorafms.com/clientes/Case%20studies/downloads/Successful_Story_Telefonica_ES.pdf

http://www.youtube.com/watch?v=Bv89wTaFqHM

[3] Informació sobre Zabbix

http://es.wikipedia.org/wiki/Zabbix

http://www.zabbix.com/

[4] Informació sobre Zennos

http://www.zenoss.com/

http://es.wikipedia.org/wiki/Zenoss

http://www.slideshare.net/ces1227/zenoss-manual-presentation

[5] Informació sobre Nagios

Wojciech Kocjan (2008) *Learning Nagios 3.0 , Birmingham-UK: Packt Publishing*

http://www.nagios.org/

http://es.wikipedia.org/wiki/Nagios

http://www.cnl-consulting.com/blog/item/71-introducción-a-la-monitorización-de-sistemas.html

[6] Informació sobre openNMS

http://www.opennms.org/

http://en.wikipedia.org/wiki/FCAPS

http://www.opennms.org/wiki/Comparison_with_other_network_management_systems

http://www.rootdev.com/tech/opennms-vs-nagios

[7] Informació sobre IBM Tivoli

http://www-01.ibm.com/software/es/tivoli/

http://www.ibm.com/developerworks/ssa/downloads/tiv/tivolimonitoring/faq-ec2-tivolimonitoring.html

http://www-142.ibm.com/software/products/es/es/tivomoni/

http://www-01.ibm.com/software/ar/demos/tivoli.shtml

http://ibm-tivoli-storage-manager.software.informer.com/wiki/

[8] Informació sobre protocol SNMP

http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

http://www.unainet.net/documents/SNMP.pdf

http://www.snmplink.org/

[9] Informació sobre eines gràfiques RRD , N2RRD , CENTREON

http://es.wikipedia.org/wiki/RRDtool

http://en.wikipedia.org/wiki/N2rrd

http://www.centreon.com/

[10] Informació sobre sensors i variables ambientals

http://es.wikipedia.org/wiki/Sensor

http://www.teksar.com.mx/sistema-monitoreo/variables-de-medicion.html

http://www.teksar.com.mx/novedades/generales/97-amenazas-presentes-en-los-data-centers.html

http://es.wikipedia.org/wiki/Termopar

http://es.wikipedia.org/wiki/RTD

http://es.wikipedia.org/wiki/Termistor

http://es.wikipedia.org/wiki/Sensor_de_humedad

http://es.wikipedia.org/wiki/Detector_de_humo

http://es.wikipedia.org/wiki/Temperatura

http://es.wikipedia.org/wiki/Humedad

http://es.wikipedia.org/wiki/Sensor_capacitivo

[11] Documents referencia sobre millors pràctiques i pautes ubicació de sensors ambientals

http://info.rfcode.com/Portals/186315/docs/best_practices_for_wire-free_environmental_monitoring.pdf

http://www.apcmedia.com/salestools/JMON-5ZLP8M_R3_ES.pdf

http://tc99.ashraetcs.org/documents.html

[12] Empreses, organismes i proveïdors de dispositius per monitorització ambiental consultats

http://www.tracelec.com/pdf/pdf211(ES).pdf

http://www.insht.es/InshtWeb/Contenidos/Documentacion/FichasTecnicas/NTP/Ficheros/201a300/ntp_215.pdf

http://www.abast.es/monitorizacion_cpds.shtml

http://www.areadata.com.ar/Monitoreo_Ambiental.html

http://www.hw-group.com/products_en.html#h

http://www.apc.com/prod_docs/results.cfm?DocType=White%20Paper&Query_Type=10

http://www.rimatrix5.es/

http://www.serverscheck.es/sensors/

http://avtech.com/Products/

Annexos

Annex A - Detall equipament monitor Room Alert 24E

Room Alert 24E és la solució de maquinari avançat del fabricant AVTECH per el control mediambiental de qualsevol Centre de Dades, a més de crear alertes i altres funcions proactives. S'ha dissenyat específicament per monitoritzar variables com la temperatura, humitat, potència i d'altres més en diferents punts d'un CPD, i també es pot utilitzar per administrar i fer el seguiment del consum d'energia, el que permet possibilitats de reduir els costos d'energia.

Room Alert 24E ofereix també una interfície fàcil d'usar amb navegador web per configuració i la visualització en temps real dels canvis de temperatura, de la humitat, l'energia i l'estat d'un altre sensor d'ambient des de qualsevol lloc, ja que inclou una llicència de programari ***Device Manager***, que és una solució avançada per la gestió, generació de gràfics, i creació d' alertes .

Device Manager s'executa com un servei de Windows i detecta automàticament els sensors, facilitant als usuaris estar informats immediatament de quan es passen els llindars ambientals. AVTECH ofereix també pluggins a un preu baix per a tota la funcionalitat disponible. No és objecte d'aplicació en la solució d'aquest TFC, en tractar-se, com ja s'havia esmentat, d'un programari comercial dedicat.

El sistema de monitorització ***Room Alert 24E*** inclou el seguent equipament:

(1) Monitor RoomAlert 24E
(1) Kit instal·lació monitor en bastidor o rack (1U 19 ")
(1) Sensor de Temperatura digital integrat.
(1) Sensor d'humitat digital integrat.
(1) Sensor extern de temperatura digital (pot ser instal.lat fins a 30 m. del monitor)
(1) Sensor extern de control d'accés (pot ser instal.lat fins fins a 275 m del monitor)
(1) Sensor extern de control potència i fallada d'energia amb 7,5 m de cable i adaptador de corrent
(6) Canals externs, per a la connexió de sensors digitals.
(16) Canals externs per a la connexió de sensors tipus interruptor.
(1) Botó de restabliment
(1) Connexió Ethernet (RJ-45)
(1) Ampliació port (RJ-45)
(1) 3 m Cable Ethernet
(1) Adaptador d'alimentació 5 V (110/240V)
LED d'estat del sensor.
Interface WEB.
Interface SNMP Trap i consulta habilitades. Device Manager Software i Recursos.
12 mesos de servei de manteniment, suport i actualització (MSU).
30 dias de arantia de satisfacció.

Annex B - Detall equipament monitor TempPageR 3E

TempPageR 3ER és també una solució de maquinari avançat del fabricant AVTECH per el control mediambiental de qualsevol Centre de Dades, però enfocat a la mesura i control exclusiu de la temperatura. ***TempPageR 3ER*** disposa de les mateixes prestacions,serveis i funcionalitats que els seus equivalents Room Alert, però amb el següent equipament :

(1) Monitor TemPageR 3E
(1) Kit instal·lació monitor en bastidor o rack (1U 19 ")
(1) Sensor de temperatura digital
(1) Sensor extern de temperatura digital (pot ser instal.lat fins a 30 m. del monitor)
(2) Canals externs per a la connexió de sensors temperatura digitals
(1) Botó de restabliment
(1) Connexió Ethernet (RJ-45)
(1) 3 m Cable Ethernet.
(1) Adaptador d'alimentació 5 V (110/240V)
LED d'estat del sensor
Interface WEB.
Interface SNMP Trap i consulta habilitades. Device Manager Software i Recursos.
12 mesos de servei de manteniment, suport i actualització (MSU).
30 dias de Garantia de Satisfacció.

Annex C – Scripts d'exemple configuració sensors en Nagios

- Definició host del dispositu RoomAlert:

```
# check_snmp_RoomAlert' command definition

define command  {

    command_name  check_snmp_RoomAlert
    command_line $USER1$/check_snmp -P 1 -H $HOSTADDRESS$ -o $ARG1$ -c $ARG2$
    -u $ARG3$
}
```

- Definició del serveis dispositu de temperatura:

```
define service{
     use                   generic-service ; Name of service template to use
     host_name             RoomAlert
     service_description   DataCenter Temperature
     check_command         check_snmp_RoomAlert!1.3.6.1.4.1.20916.1.3.1.2.2.0!
                             15:23!"Degrees Celsius"
        }
```

- Definició del serveis dispositu d'humitat:

```
define service{
     use                   generic-service ; Name of service template to use
     host_name             RoomAlert
     service_description   DataCenter Humidity
     check_command
     check_snmp_RoomAlert!1.3.6.1.4.1.20916.1.3.1.2.3.0!
                           30:45!"%Relative Humidity"
```