Disseny d’un sistema de monitoratge en una empresa d’assegurances.

Miguel Sánchez Martín

Grau d’Enginyeria Informàtica

Àrea: GNU/Linux

Tutor: Joaquin Lopez Sánchez-Montañes

04/06/2023

A Giovanna, per la teva paciència, la teva fortalesa i coratge.

Als meus fills, Joanquel i Emma, perdoneu-me per tantes hores d'absències.

Als meus pares, Miguel i Antonia, per donar-me la vida, l'educació i els valors morals.

A la meva familia i els meus amics, per donar-me ànims per continuar.

A tots els professors/es i consultors/es amb qui m'he trobat en aquest camí tan llarg, pel seu suport i la seva feina.

Gràcies a tots,

Aquesta obra es troba subjecte a una llicència de
Reconeixement-No Comercial-Sense Obra Derivada
https://creativecommons.org/licenses/by-nc-nd/3.0/es/

FITXA DEL TREBALL FINAL

Títol del treball:	*Disseny d'un sistema de monitoratge en una empresa d'assegurances.*
Nom de l'autor:	*Miguel Sánchez Martín*
Nom del consultor/a:	Joaquin Lopez Sánchez-Montañés
Nom del PRA:	Montse Serra Vizern
Data d'entrega (mm/aaaa):	06/2023
Titulació:	Grau d'Enginyeria Informàtica
Àrea del Treball Final:	*GNU/Linux*
Idioma del treball:	*Català*
Paraules clau	Linux, Nagios, InfluxDB, NagVis, NagFlux, Grafana, Monitoratge

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball.*

A l'actualitat, per a qualsevol organització, és gairebé imprescindible disposar d'un sistema de monitoratge que permeti el control de la infraestructura i faciliti la seva gestió.

El present treball final de grau exposa una proposta de disseny d'un sistema de monitoratge per a una empresa d'assegurances amb l'objectiu de millorar l'eficiència i reduir tant el nombre d'incidències com el temps de resolució de les mateixes.

L'anàlisi comença amb l'estudi de la situació actual i les necessitats de l'organització. Mitjançant aquest anàlisi previ es detecten grans carències en els sistemes d'informació de l'organització en quant a monitoratge i es planteja una proposta adequada, fent una comparativa de diferents eines de monitoratge, i finalment construint la proposta amb sistemes operatius Linux i "software" "open source", complint els requeriments de la direcció de l'organització.

Durant la construcció de la proposta es tenen en compte elements com la integració de la solució amb d'altres departaments de l'organització, a més d'estudiar les configuracions inicials de cada component de la solució.

Fruit d'aquet treball s'ha pogut constatar que és possible i totalment viable, implementar un sistema de monitoratge amb una base econòmica continguda, tenint en compte els grans beneficis que comportaria per als sistemes d'informació la

implantació d'un sistema de monitoratge.

Abstract (in English, 250 words or less):

Nowadays, for any organization, it is almost essential to have a monitoring system that allows the control of the infrastructure and facilitates its management.

This final degree thesis presents a proposal for the design of a monitoring system for a insurance company with the aim of improving efficiency and reducing both the number of incidents and the time to resolve them.

The analysis begins with the study of the current situation and the needs of the organization. Through this prior analysis, major deficiencies are detected in the organization's information systems in terms of monitoring and an adapted proposal is considered, making a comparison of different monitoring tools, and finally building the proposal with Linux operating systems and "open source" "software", that fulfills the management requirements of the organization.

During the construction of the proposal, elements such as the integration of the solution with other departments of the organization are taken into account, in addition to studying the initial configurations of each component of the solution.

As a result of this work, it has been possible to ascertain that it is possible and fully viable to implement a monitoring system with a contained economic base, taking into account the great benefits that the implementation of a monitoring system would entail for information systems.

Índex

1. Resum

L'objectiu d'aquest treball és oferir una solució viable a la necessitat de l'empresa MEDIADORS I ASSEGURANCES, S.A. de monitorar els elements que conformen el seu Sistema d'Informació.

Primer de tot, he analitzat la situació actual, entrevistant els principals interessats i recollint la informació d'infraestructura que forma part del sistema d'informació.

Una vegada he analitzat tota aquesta informació, he buscat en el mercat possibles aplicacions vàlides per a monitorar tota l'estructura, de baix cost i amb les majors funcionalitats, escalable i flexible.

A continuació, he dissenyat una proposta escollint aquelles eines i aplicacions que puguin treballar conjuntament i planificant la seva implementació en un espai de temps factible.

L'estructura creada es basa en sistemes operatius Linux i en aplicacions de codi obert, com són Nagios, InfluxDB i Grafana, proporcionant eines de monitoratge i aplicacions de visualització, recollint les dades i processant-les per a tenir una solució de temps real millorant la gestió del sistema d'informació i proporcionant grans beneficis per a l'organització.

En el disseny de la proposta he tingut en compte punts clau, com són:

- Integració amb altres departaments.
- Polítiques d'aplicació.
- Primers passos, tant d'instal·lació com de configuració dels elements que formen el disseny.
- Pla de contigència.
- Gestió d'usuaris.
- Pla de manteniment.

També proposo una sèrie de proves a fer una vegada implementada la proposta, si aquesta arribés a fer-se realitat.

Ha sigut una experiència molt satisfactòria i més, sabent que aquesta es pot fer realitat, ja que s'ha basat en dades reals de l'organització on actualment treballo.

2. Índex de taules i figures

3. Índex de fitxers adjunts

- Diagrama de Gantt. Project GanttProject (PlaTreball_Monitoratge.gan)
- Llista d'elements i dispositius a monitorar(Infraestructura_2023.xlsx)
- Plantilla BBDD_SQLServer (Plantilla BBDD_SQLServer_v1.xlsx)
- Plantilla SO_WINDOWS (Plantilla SO_Windows_v1.xlsx)
- Plantilla SO_LINUX (Plantilla SO_Linux_v1.xlsx)
- Sol·licitud d'entrada de material al CPD (Sol·licitud CPD.xlsx)
- Sol·licitud d'instalació del Sistema Operatiu (Solicitud Instal·lació Equip.xlsx)
- Sol·licitud d'emmagatzematge (Solicitud Emmagatzematge.xlsx)
- Sol·licitud de recolzament (Solicitud Recolzament.xlsx)

4. Introducció

a) Justificació

El monitoratge és un procés essencial en qualsevol mena de projecte, sigui a nivell empresarial, tecnològic o social. Es tracta d'una eina que ens permet observar i analitzar de manera sistemàtica i contínua les activitats que es duen a terme en un entorn determinat, per tal de detectar problemes, errors o millores que es puguin implementar.

El monitoratge es converteix així, en una eina clau per a la presa de decisions i la millora contínua de qualsevol projecte. En la nostra empresa MEDIADORS i ASSEGURANCES, S.A. aquest monitoratge no es troba desenvolupat, de fet, no existeix cap eina de monitoratge o, si existeix, és una eina no centralitzada i no controlada pel departament de SI/TI.

En aquest treball, es presentarà una proposta d'implementació d'eines i processos necessaris per dur a terme l'observació i l'anàlisi dels servidors i processos principals, així com analitzar els resultats obtinguts i presentar les recomanacions per a millores futures.

b) Objectiu

El principal objectiu a assolir amb aquest treball és:

- ✓ Estudiar, dissenyar i fer una proposta per tal d'Implementar un Sistema de monitoratge que doni suport al sistema informàtic actual de MEDIADORS i ASSEGURANCES, S.A.

Com a objectius parcials que volem aconseguir amb aquest projecte tenim:

- ✓ Crear un mapa del monitoratge actual
- ✓ Recerca i implementació d'una eina o eines de monitoratge que permetin el control i gestió de monitoratge
- ✓ Disseny i implementació d'una política de monitoratge dels SI/TI
- ✓ Disseny de les plantilles necessàries per gestionar les peticions de monitoratge.
- ✓ Implementació de monitoratge dels servidors i els dispositius de la xarxa de l'organització
- ✓ Integració del sistema de monitoratge amb els sistemes de recolzament existents.
- ✓ Integració del sistema de monitoratge amb els sistemes de seguretat existents.
- ✓ Integració del sistema de monitoratge amb els sistemes d'emmagatzematge.
- ✓ Comprovació de monitoratge dels SI/TI i els dispositius de la xarxa de l'organització.
- ✓ Creació d'un pla de manteniment possible d'aquest sistema de monitoratge

c) Metodologia

Per tal d'aconseguir aquests objectius, m'he plantejat diferents aspectes a tenir en compte:

1) Infraestructura

A continuació es presenta un diagrama de la infraestructura a monitoritzar:

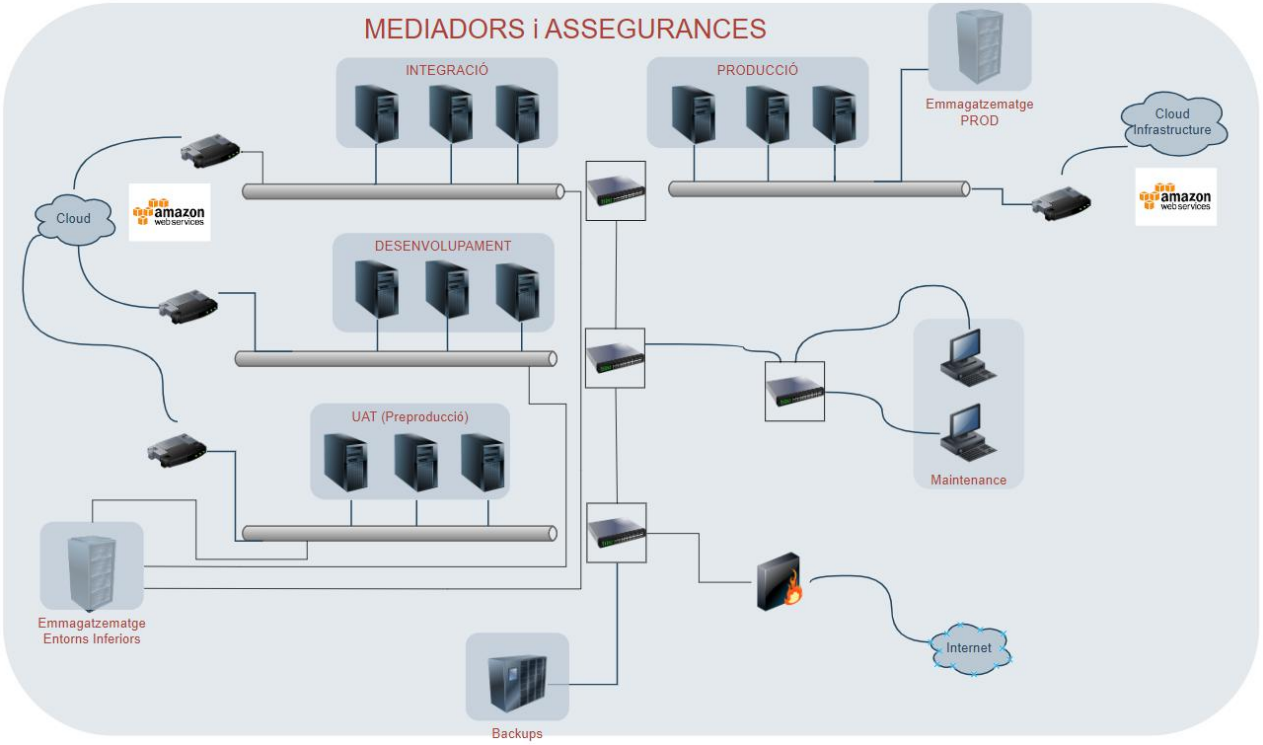


Figura 1. *Diagrama d'infraestructura actual.*

2) Elements a monitoritzar

Es troben, doncs, sota l'ambit d'aquest projecte els sistemes operatius següents:

- Linux
- Windows
- AIX
- Dispositius de xarxa Cisco i dispositius NetAPP d'emmagatzematge

I els entorns següents:

- Desenvolupament
- Integració
- Pre-producció
- Producció

S'han de controlar tots aquells aspectes que proporcionin control sobre el funcionament, rendiment i disponibilitat dels sistemes, alertant en cas necessari i presentant també els informes o panells de control que es sol·liciti per part de l'administració i/o la direcció.

3) Hardware

Disposem en el mercat de moltes possibilitats de hardware per tal d' instal·lar eines de monitoratge i també existeixen al mercat solucions on no es requereix un hardware propi, com poden ser els serveis MaaS (Monitoring as a Service) o SaaS ("software" as a Service) per exemple.
Un dels requisits de la Direcció és disposar del control total d'aquesta eina o eines que s'instal·lin, és per això que s'ha escollit disposar d'un hardware propi a les instal·lacions de l'empresa o en un proveïdor de CPD extern. Una de les tasques d'aquest projecte serà cercar i escollir el hardware necessari per a implementar el "software" necessari.

Figura 2. *Servidor Enrackable DellPowerEdge R550*

4) Sistemes operatius

Si bé és cert que existeixen diferents sistemes operatius, com Windows, AIX, OS/400, el més lògic en aquesta situació, i tenint en compte que es volen fer servir eines *“"open source"”*, que tradicionalment i en gran part es troben dissenyades per sistemes operatius Linux, he escollit aquest sistema operatiu. A l'organització es treballa amb CentOS 7 i 8 com a distribucions Linux, per tant, aquesta ha de ser la distribució a instal·lar.

5) Eines

Com he comentat anteriorment, és requisit de la Direcció que el cost de la implementació es mantingui en un pressupost baix. Les eines més importants i conegudes de monitoratge són de pagament, per exemple Dynatrace, AppDynamics o SolarWinds per citar algunes.
Així doncs, hem de cercar eines "*open source*" o d'un cost mínim com Nagios, Centreon o Zabbix, per exemple. Durant aquest projecte, hauré de realitzar una comparativa per tal d'escollir l'eina o eines més adequades per assolir els objectius. Vist que en una sola eina pot ser difícil trobar totes les funcionalitats que se'ns requereix, pot ser interessant presentar una solució conjunta amb diferents eines de monitoratge que es puguin complementar entre elles.

6) Informació dels sistemes a monitoritzar

Des del departament de SI/TI es requereix disposar de la següent informació com a mínim dels equips i servidors a monitorar:
CPU, Memòria RAM, I/O, Disc, Tràfic de xarxa, ports, processos i serveis principals.
És imprescindible disposar d'aquesta informació i guardar, com a mínim, una retenció de 6 mesos. També és necessari que aquesta informació estigui disponible per la seva consulta, a ser possible en gràfics i panells de control.

7) Notificacions

Quan un dispositiu no es trobi disponible o es produeixi un canvi d'estat en un dels dispositius o elements monitoritzats, és requisit del departament de SI/TI que s'enviï com a mínim correu a l'equip o llista de distribució que s'indiqui, per a cada element o dispositiu monitoritzat.

d) Planificació del treball

A continuació presento una planificació del treball a realitzar i la seva progressió:

	TFG			
	Setmana	**Activitat**	**Memòria**	**% Completat**
1	13/03 - 19/03	Definició del projecte objectius, ambit i justificació		100%
2	20/03 - 26/03	Definició de les tasques, planificació i creació del cronograma	Índex	100%
3	**27/03 - 02/04**	**Entrega PAC1: pla de Treball**		100%
4	03/04 - 09/04	Tasca1: Anàlisi i estudi de la situació actual		100%
5	10/04 - 16/04	Tasca2: Definició dels requisits i recerca		100%
6	**17/04 - 23/04**	Redacció Memòria **Entrega PAC2: Eines escollides i disseny**	**30%**	**100%**
7	24/04 - 30/04	Tasca 3: Implementació del sistema de monitoratge		100%
8	01/05 - 07/05	SubTasca 3.1: Instal·lació del hardware (Sistema operatiu i aplicacions de suport). SubTasca 3.2: Integració amb els sistemes d'emmagatzematge. SubTasca 3.3: Integració amb els sistemes de seguretat. SubTasca 3.4: Integració amb els sistemes de recolzament. SubTasca 3.3: Instal·lació de les aplicacions de monitoratge. SubTasca 3.4: Implementació de la política de monitoratge. SubTasca 3.5: Configuració de l'eina o eines de monitoratge.		100%

		SubTasca 3.6: Instal·lació i configuració dels agents, en el cas necessari. SubTasca 3.7: Configuració per els dispositius de xarxa.		
9	08/05 - 14/05	Tasca 4:Test		100%
10	**15/05 - 21/05**	Redacció Memòria **Entrega PAC3: resultats i anàlisis**	**70%**	**100%**
11	22/05 - 28/05	Tasca 5: Pla de manteniment		100%
12	29/05 - 04/06	Redacció i revisió final de memòria		100%
13	**05/06 - 11/06**	**Entrega PAC4: Lliurament Memòria**	**100%**	**100%**
14	12/06 - 18/06	Elaboració Presentació		100%
15	19/06 - 25/06			
16	26/06 - 02/07	Presentació Virtual		100%
17	03/07 - 09/07	Període de consulta del Tribunal		-
18	10/07 - 16/07			

***Taula 1**. Taula de planificació. Cronograma.*

Diagrama de Gantt

S'annexa una imatge del diagrama de Gantt realitzat amb GanttProject i la representació gràfica de cadascuna de les fases:

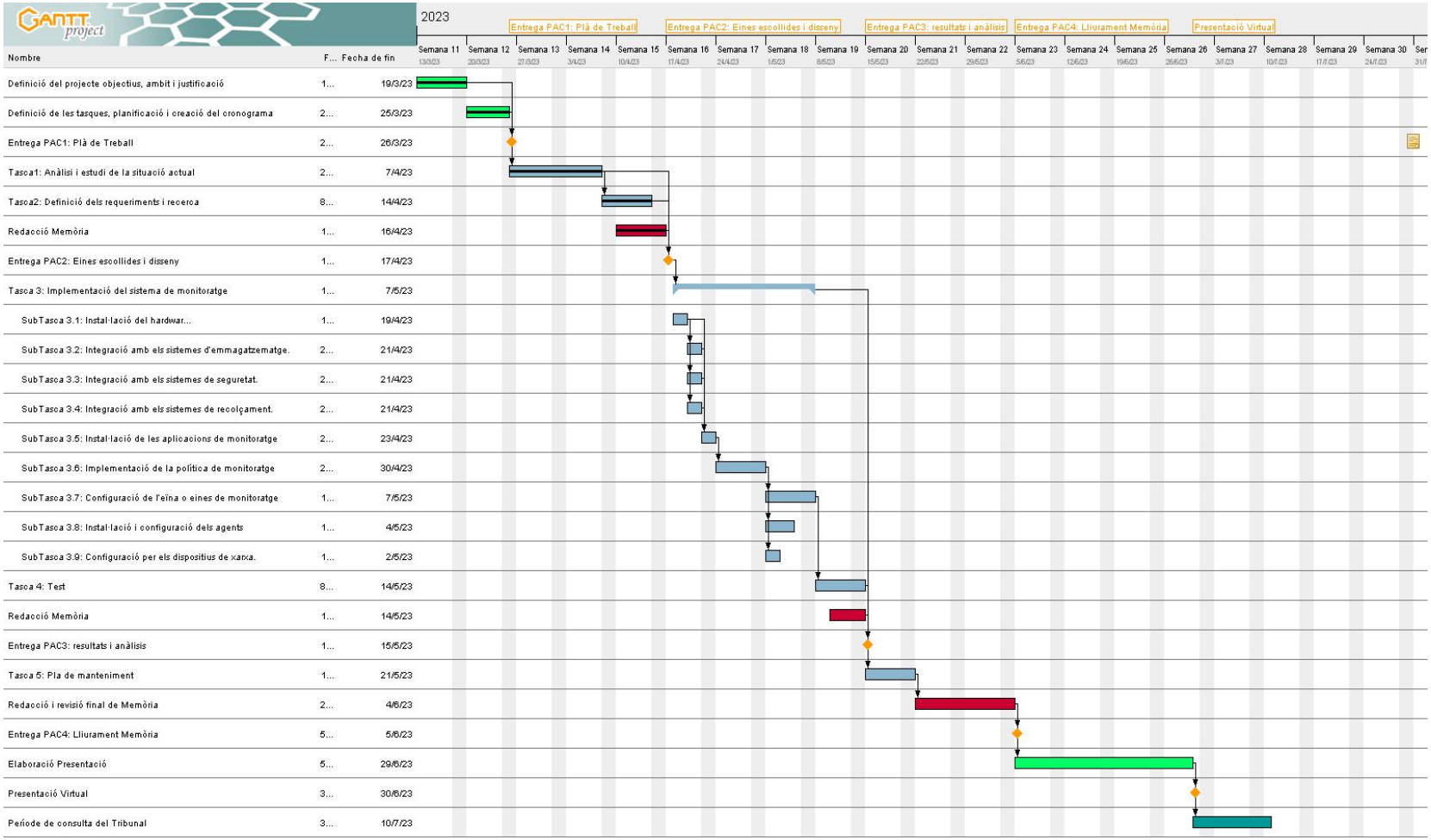


***Figura 3**. Diagrama de Gantt.*

Fase I. PAC 1 Pla de Treball.

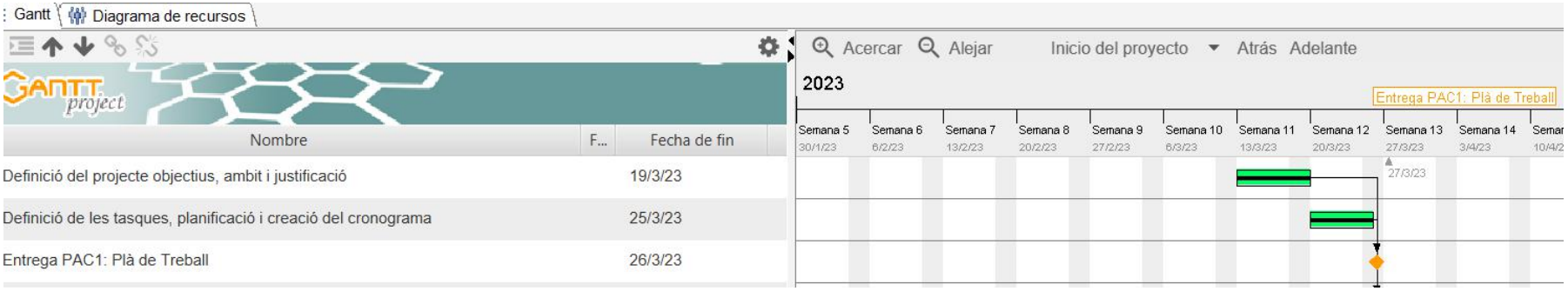


***Figura 4**. Diagrama de Gantt.Fase I*

Fase II. PAC2 Tasques 1 i 2.

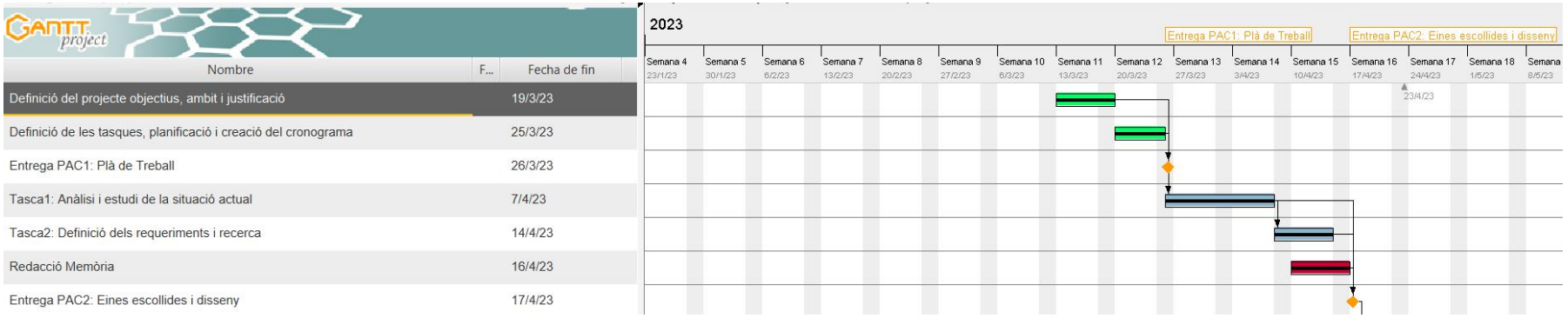
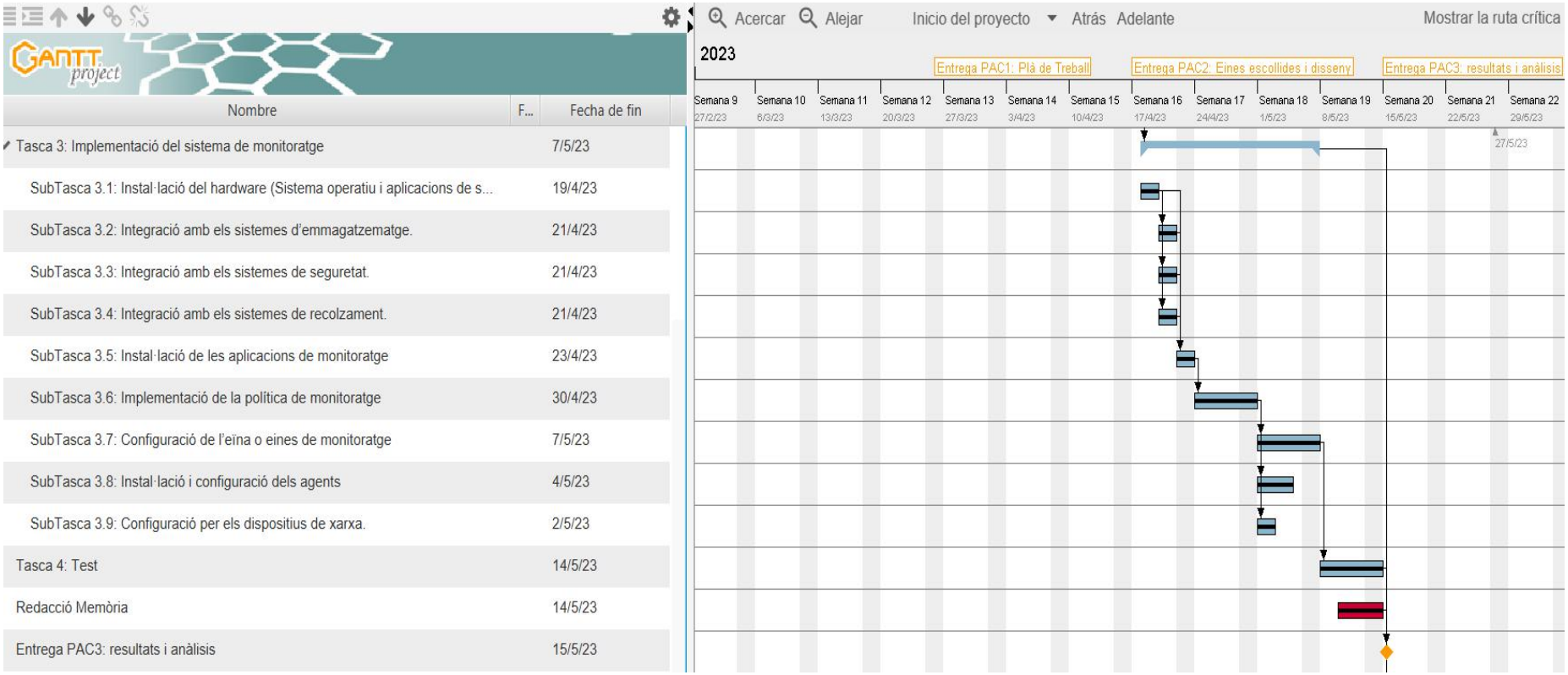


***Figura 5**. Diagrama de Gantt.Fase II*

Fase III. PAC3 Tasques 3 i 4.



Nombre	F...	Fecha de fin
Tasca 3: Implementació del sistema de monitoratge		7/5/23
SubTasca 3.1: Instal·lació del hardware (Sistema operatiu i aplicacions de s...		19/4/23
SubTasca 3.2: Integració amb els sistemes d'emmagatzematge.		21/4/23
SubTasca 3.3: Integració amb els sistemes de seguretat.		21/4/23
SubTasca 3.4: Integració amb els sistemes de recolzament.		21/4/23
SubTasca 3.5: Instal·lació de les aplicacions de monitoratge		23/4/23
SubTasca 3.6: Implementació de la política de monitoratge		30/4/23
SubTasca 3.7: Configuració de l'eïna o eines de monitoratge		7/5/23
SubTasca 3.8: Instal·lació i configuració dels agents		4/5/23
SubTasca 3.9: Configuració per els dispositius de xarxa.		2/5/23
Tasca 4: Test		14/5/23
Redacció Memòria		14/5/23
Entrega PAC3: resultats i anàlisis		15/5/23

***Figura 6**. Diagrama de Gantt. Fase III*

Fase 4. Tasca 5 i Conclusions.

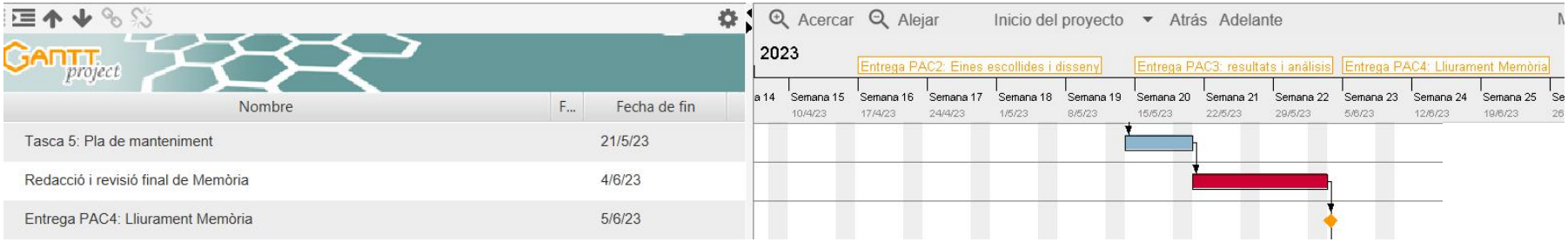


***Figura 7**. Diagrama de Gantt.Fase IV*

Elaboració de la presentació virtual.

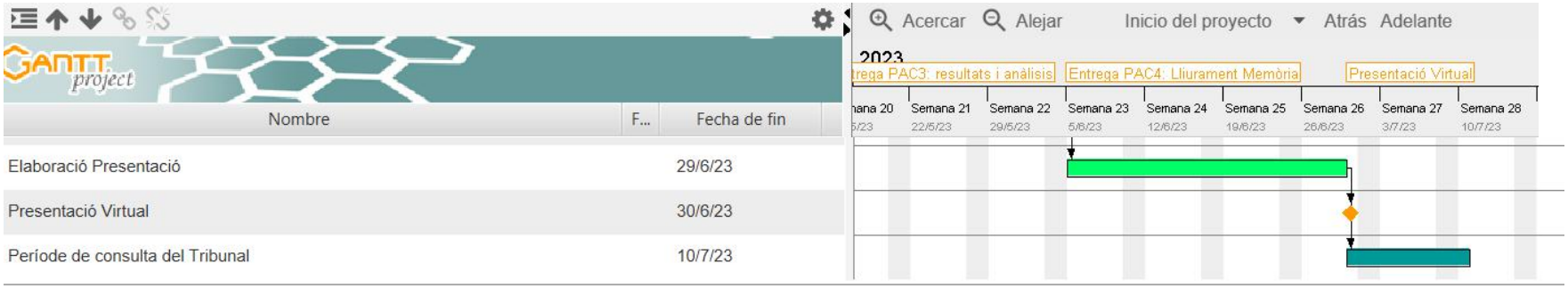


***Figura 8**. Diagrama de Gantt.Presentació Virtual i Consultes del Tribunal*

5. Breu descripció dels altres capítols

I. Estudi preliminar de la situació

Centro aquest apartat en l'anàlisi de la situació actual del monitoratge de l'organització i d'aquells requisits que he pogut recopilar dels principals interessats durant aquesta fase inicial.

II. Comparativa d'eines de monitoratge

Per tal de desenvolupar una proposta consistent he de cercar en el mercat les eines necessàries per assolir els objectius marcats. Faré en aquest apartat un resum de les propostes analitzades i presentaré la proposta final, indicant les motivacions i justificacions d'aquesta elecció.

III. Disseny i implementació del sistema de monitoratge

En aquest apartat dissenyaré la política de monitoratge necessària per implementar posteriorment el sistema de monitoratge, basant-nos en els requisits recollits en els apartats anteriors. També es planteja com s'integrarà aquest sistema de monitoratge en els sistemes actuals d'emmagatzematge, recolzament i seguretat.
Finalment, es formalitza la implementació i configuració dels productes escollits seguint la política definida.

IV. Proves i tests

Per tal de garantir els resultats i que el sistema de monitoratge funcionarà segons els requisits i objectius plantejats, dissenyaré un possible pla de proves i tests que es pugui executar en qualsevol moment. A més es descriu en aquest apartat el pla de recuperació, en cas de pèrdua del servei.

V. Pla de manteniment

En aquest apartat es descriurà el disseny del pla de manteniment una vegada s'hagi implementat el sistema de monitoratge, definint les instal·lacions, renovacions i/o recertificacions que s'hagi de dur a terme.

VI. Valoració pressupostaria

Finalment, es presenta en aquest apartat una valoració pressupostària que inclou les eines, instal·lacions i configuracions necessàries i una previsió de les despeses anuals corresponents al manteniment.

6. Estudi preliminar de la situació

a) Situació d'actual de monitoratge

He recollit dades dels servidors i dispositius que s'han de monitorar i del seu estat de monitoratge actual. Amb colors he definit l'estat actual que en cap cas és favorable.

No hi ha monitoratge

Monitoratge Bàsic (CPU, Memoria, Disc)

Monitoritatge de la propia aplicació

Monitoratge del proveïdor

En el cas que el monitoratge sigui del proveïdor, s'ha demanat, com a requisit, que s'incorpori a més, un monitoratge propi i també que la notificació arribi al proveïdor.

En altres casos, que s'ha definit el monitoratge existent com a bàsic, s'ha de comentar que no hi ha notificacions ni alertes, i que tan sols es recopila aquesta informació en el propi servidor, normalment servidors Linux, mitjançant l'eina nmon.

Per més informació, veure l'annex Infraestructura_2023.xlsx

ServerName	Description	DateFirstInvoice	Shared	SupportLevel	FunctionalClass	EnvPRD	EnvUAT
B0D0B002	DB FARM - DB2 Dev (Antiguo INFO - DEV - Integra DB)		TRUE		Application	FALSE	
B0D0BUV2	INFO - PRD - Erwin database (ESZ	3/1/2022	FALSE	Medium-24	Application	TRUE	
CEALA06091	INFO - UAT - WAS 9.0 Cluster	5/1/2017	FALSE	Low	Application	FALSE	
CEALA06092	INFO - UAT - WAS 9.0 Cluster	5/1/2017	FALSE	Low	Application	FALSE	
CEALA06174	INFO - PRD - WAS 9.0 Cluster	4/1/2017	FALSE	High	Application	TRUE	
CEALA06175	INFO - PRD - WAS 9.0 Cluster	4/1/2017	FALSE	High	Application	TRUE	
CEALA09201	ControlM - PRD - Control M Serv	7/1/2018	FALSE	Medium-24	Application	TRUE	
CEALA09202	ControlM - UAT - Control M Serv	7/1/2018	FALSE	Low	Application	FALSE	
CEALA09223	ELK LOGS - UAT - Ingestion + Elastic + Kibana Server		FALSE	Low	Application	FALSE	
CEALA09332	ELK LOGS - PRD - Ingestion Server		FALSE	Low	Application	TRUE	
CEALA09333	ELK LOGS - PRD - Elastic + Kibana		FALSE	Low	Application	TRUE	
CEALA09347	ELK LOGS - PRD - Elastic Server		FALSE	Low	Application	TRUE	
CEALA09358	ELK LOGS - PRD - Elastic Server		FALSE	Low	Application	TRUE	
CEALA09359	ELK LOGS - PRD - Elastic Server		FALSE	Low	Application	TRUE	
CEALA09361	ELK LOGS - PRD - Elastic Server		FALSE	Low	Application	TRUE	
CEALA09362	ELK LOGS - PRD - Elastic Server		FALSE	Low	Application	TRUE	
CEALA09705	ELK LOGS - PRD - Elastic Server		FALSE	Low	Application	TRUE	
CEALA09954	Plataform de Modelos - UAT - Online Server		FALSE	Medium-24	Application	FALSE	
CEALA09964	Plataform de Modelos - PRD - Online Server		FALSE	Medium-24	Application	TRUE	
CEALA09967	Plataform de Modelos - PRD - Online Server		FALSE	Medium-24	Application	TRUE	
CEALA09968	Plataform de Modelos - PRD - Batch Server		FALSE	Medium-24	Application	TRUE	
CEALA09972	Plataform de Modelos - UAT - Online Server		FALSE	Medium-24	Application	FALSE	
CEALA09980	Plataform de Modelos - UAT - Batch Server		FALSE	Medium-24	Application	FALSE	
CEALA12550	INFO - PRD - Aggregators Tomcat	9/1/2019	FALSE	High	Application	TRUE	
CEALA12551	INFO - PRD - Aggregators Tomcat	9/1/2019	FALSE	High	Application	TRUE	
CEALA13465	MDM - UAT - Application Server	5/1/2020	FALSE	Low	Application	FALSE	
CEALA13466	MDM - PRD - Application Server	5/1/2020	FALSE	Medium-24	Application	TRUE	
CEALA14487	DATA PIPELINE - PRD - Node 2 - N	11/1/2020	FALSE	Medium-24	Application	TRUE	
CEALA14494	DATA PIPELINE - PRD - Node 1 - N	11/1/2020	FALSE	Medium-24	Application	TRUE	

***Taula 2**. Taula de servidors i dispositius a monitoritzar*

b) Requisits

Recollir els requisits en un projecte és essencial perquè ajuda a assegurar que el projecte s'ajusti a les necessitats i les expectatives del client i dels interessats. En recopilar els requisits, s'identifiquen les metes, els objectius, les funcions i les

característiques del projecte, cosa que permet als equips de projecte i als interessats tenir una comprensió clara del que s'espera del projecte.

A més, recollir els requisits ajuda a evitar malentesos i assegura que tots els interessats estiguin alineats en termes del que s'està intentant aconseguir amb el projecte. També ajuda a definir els límits i abasts del projecte, cosa que és essencial per garantir que el projecte es lliuri dins del pressupost i del termini previstos.

A la taula següent s'ha inclòs un resum dels requisits que se m'han demanat durant les entrevistes mantingudes amb els diferents interessats:

Interessat	Descripció de requisits	Prioritat	ID
Direcció	El cost de la solució ha de ser mínim, ja que el pressupost és limitat.	Alta	RD1
	Qualsevol usuari ha de poder tenir accés si ho demana i és autoritzat.	Alta	RD2
	El projecte ha de seguir la normativa vigent respecte a seguretat, qualitat i legalitat.	Alta	RD3
	S'acceptarà no menys d'un 99% de disponibilitat del sistema sense comptar el temps de manteniment.	Alta	RD4
	S'establirà una finestra de manteniment per fer les còpies de seguretat i reinicis en cas necessari	Alta	RD5
	El sistema s'ha de dissenyar amb alta disponibilitat sempre que sigui possible, mantenint un cost baix	Alta	RD6
	En cas que es requereixi la instal·lació d'un agent en els servidors, aquests no poden consumir més d'un 1% dels recursos del sistema i en qualsevol cas no poden afectar el rendiment d'aquests.	Mitja	RD7
Departament de SI/TI	Davant d'una caiguda el sistema s'ha de recuperar en menys de 6 hores	Mitja	RS1
	El sistema ha de ser capaç d'enviar notificacions mínim per e-mail	Alta	RS2
	El sistema ha de ser capaç de generar informes d'estat, rendiment, capacitat, disponibilitat i errors d'almenys 6 mesos i d'enviar aquests informes per e-mail.	Alta	RS3
	El sistema ha de ser capaç de retenir les dades durant un mínim de 6 mesos.	Mitja	RS4
	El sistema ha de ser capaç de funcionar amb els recursos de les xarxes internes, sense necessitat d'accés a Internet, almenys en el que monitoratge de disponibilitat es refereix.	Alta	RS5
	El sistema ha de ser capaç de monitorar sistemes operatius, bases de dades, servidors web i dispositius de comunicacions, com a mínim.	Alta	RS6
	Les validacions dels servidors web poden incloure consultes des de ubicacions geogràfiques diferents.	Mitja	RS7
	El sistema ha de ser capaç de monitorar CPU, Memòria RAM, I/O, Disc, Tràfic de xarxa, ports, processos i serveis principals	Alta	RS8
	El sistema ha de ser capaç de configurar alertes segons uns llindars determinats que s'executin quan es traspassin aquests llindars.	Alta	RS9
	El sistema ha de ser capaç de funcionar correctament amb 100 usuaris concurrents, més de 100 servidors monitorats i prop de 5000	Mitja	RS10

	mètriques		
	S'ha de disposar d'un recolzament de les dades seguint la política de còpies de seguretat, diària, setmanal i mensual	Mitja	RS11
	Les peticions d'altes / baixes i modificacions del monitoratge es faran seguint el sistema de peticions de l'organització per tal de controlar i registrar l'activitat de l'equip assignat.	Mitja	RS12
	S'ha de documentar tant la instal·lació del sistema com la seva implementació i funcionalitat .	Alta	RS13
Usuaris	Ha de ser una aplicació de fàcil ús perquè qualsevol usuari la pugui consultar.	Mitja	RU1
	El sistema ha de permetre la creació de panells de control personalitzats	Mitja	RU2
	S'ha de realitzar sessions formatives i cursos per a fer servir l'eina	Mitja	RU3
IT Owners	El sistema ha de poder agrupar els usuaris per cada aplicació i pels diferents grups de treball que es dediquen a aquestes aplicacions.	Mitja	RI1
Proveïdors	El sistema ha de ser consultat des de fora de la xarxa de l'organització.	Baixa	RP1
Seguretat (GIS)	El sistema ha de ser capaç de validar els usuaris per usuari i contrasenya. Sense usuari no es podrà accedir al sistema	Alta	RG1
	El sistema disposarà d'un doble sistema d'autenticació (MFA), pot ser per OTP o un gestor d'autenticació com Google Authenticator.	Alta	RG2
	El sistema ha de tenir un registre de control dels usuaris, altes, baixes, modificacions, rols i perfils i de les peticions que s'hagin fet.	Alta	RG3

***Taula 3**. Taula de requisits de l'organització*

7. Comparativa d'eines de monitoratge

En el mercat trobem diferents i molt completes solucions de monitoratge "*open source*".

Faré a continuació una breu descripció de les eines analitzades i utilitzant una taula comparativa escollirem la millor de les opcions. S'acompanya annexada la comparativa realitzada (Comparativa Eines de Monitoratge.pptx)

Zabbix:

Zabbix és una eina de monitoratge de xarxa de codi obert i altament escalable que permet als usuaris monitorar i administrar de manera efectiva la seva infraestructura de TI. És altament personalitzable, compta amb una àmplia gamma de característiques i és utilitzat per una gran comunitat d'usuaris i desenvolupadors a tot el món.

PandoraFMS:

PandoraFMS és una eina de monitoratge de xarxa de codi obert molt potent i totalment configurable. Compta amb una àmplia varietat de "*plugins*" i monitors i una organització molt potent al darrere que ofereix suport i ampliacions constants.

Zenoss:

Zenoss és una plataforma de monitoratge i anàlisis relativament jove, va començar el 2006 i que es basa en el monitoratge sense agents, fent connexions SSH, WMI o SNMP. És una solució molt completa, però a la vegada és complexa d'instal·lar i configurar.

OP5:

ITRS OP5 Monitor és una solució de monitoratge de codi obert basat en Nagios. És capaç de mostrar el rendiment i disponibilitat d'elements TI. Té una interfície visual simple i de fàcil ús.

Centreon:

És una solució de monitoratge molt completa i d'arquitectura distribuida que permet una flexibilitat total, per exemple, es pot definir llindars diferents segons l'usuari que configuri l'alerta, generant així alertes personalitzades per usuari. Disposa d'una versió "open source" lliure amb certes limitacions, però totalment funcional.

Nagios:

Nagios és un dels *"software"* de monitoratge més antics. Es tracta d'una solució escalable i de supervisió d'infraestructures i xarxa. De fàcil integració ha anat millorant amb el temps. Abans es considerava només per perfils experimentats, però amb el temps ha evolucionat i ara és una opció molt a tenir en compte.

Prometheus:

Prometheus és una plataforma de monitoratge de sistemes i xarxes, versàtil i altament escalable. És un projecte "*open source*" mantingut al marge de qualsevol empresa pel que és totalment lliure i gratuït. És més orientat a monitoratge en "*cloud*" i Kubernetes, però també és vàlid per entorns "*on premise"*.

	Zabbix	PandoraFMS	Zenoss	OP5	Centreon	Nagios	Prometheus
Plataforma cloud	✔	✔	✔	✔	✔	✔	✔
Entorn local	✔	✔	✔	✔	✔	✔	✔
Alerting e-mail	✔	✔	✔	✔	✔	✔	✔
Anàlisi predictiu	✘	✔	✔	✔	✔	✔	✔
Reporting	✔	✔	✔	✔	✔	✔	✔
Retenció: 6 mesos	✔	✔	✔	✔	✔	✔	✔
Dashboards	✔	✔	✔	✔	✔	✔	✔
Integracions amb tercers	✔	✔	✔	✔	✔	✔	✔
Grups logics	✔	✔	✔	✔	✔	✔	✔
Agents	✔	✔	✘	✔	✔	✔	✔
BBDD	SQL	MySQL	RRDtool / MySQL	SQL	MariaDB/MySQL/RRDTool	RRDTool / MySQL	Time series (bbdd propia)
Seguretat	✔	Control Accès granular	✔	✔	✔	✔	✔
Preus	Free Pro 3€ Enterprise 5€ per node, per month	Des de 1800€ (18€ per agent)	Standard: 2995$ Professional:3995$	Free Pricing Model: Per User Standard:135/month	Free IT Edition Business Edition MSP Edition Preu per dispositiu	XI Standard: Des de 1.995$ XI Enterprise: Des de 3.495$ Core: Free	Free
Suport	Preu per servidor Zabbix	Suport NMS / Enterprise Suport 24/7	24/5 (Standard) 24/7 (Urgent)	Support e-mail and phone support with maintenance contract	Free:Support IT/Business:Community Premium Support MSP:MCO	Forum Support: Free e-mail Support (des de 1869$/year) Phone Support(des de 1995$/year)	Suport Free

***Taula 4**. Comparativa d'eines de monitoratge*

Després de revisar aquesta taula comparativa, veig que les opcions són molt similars, però cadascuna té unes característiques i funcionalitats que les fan a la vegada molt diferents.

Em decanto finalment per Nagios, en la seva versió Core**.** És un "software" que conec per la meva experiència, amb una alta flexibilitat, versatilitat i una comunitat de suport i desenvolupament francament enorme. Es pot començar instal·lant la versió Core i migrar a una versió amb suport una vegada implementada i consolidada la solució, com per exemple NagiosXI o Nagios Fusion.

He plantejat una solució que farà servir també altres eines de codi obert associades a eines de monitoratge, com poden ser:

- **NagVis:** Eina de representació gràfica de monitoratge basada en les dades proporcionades pel motor Nagios.
- **NagFlux**: Connector que transforma les dades de Nagios en fluxos de temps que pot interpretar Grafana - Histou.
- **Grafana:** Eina de representació de dades, mitjançant gràfiques i esquemes molt elaborats.
- **Histou:** Add-on de Grafana que interacciona amb les dades proporcionades per NagFlux per tal de crear plantilles específiques per a les dades de Nagios.
- **InfluxDB:** Plataforma de serialització de temps

Nagios aconsella la instal·lació física a partir de 1000 hosts o 5000 serveis. Com se m'ha demanat que sigui una solució escalable, farem la instal·lació física. Els requisits de Nagios XI són (la versió Core és molt menys exigent quant a recursos):

Monitored Nodes / Hosts	Monitored Services	Hard Drive Space	CPU Cores	RAM
50	250	40 GB	1 – 2	1 – 4 GB
100	500	80 GB	2 – 4	4 – 8 GB
> 500	> 2500	>120 GB	> 4	> 8 GB

Taula 5*. Taula de requisits de Nagios XI*

A més, com ja he comentat anteriorment la direcció de l'organització m'ha demanat que el monitoratge dels servidors sigui accessible en tot moment, encara que no estigui disponible l'accés a Internet. Això comporta que aquesta part del sistema ha de trobar-se a la xarxa de l'organització, encara que és possible que alguns elements estiguin fora.

Per tot això he d'escollir un maquinari adient. Els nostres proveïdors acceptats són HP, Fujitsu i Dell. He realitzat una petita comparativa entre 3 models d'aquests fabricants que es troben disponibles actualment. El maquinari escollit ha de ser econòmic però potent, i encara que innovador ha de ser un maquinari estable, ja provat.

	DELL	HP	Fujitsu
Imatge	 Smart Selection PowerEdge R550 Servidor Rack Plus **3.787,01 €** 3.129,76 € excluyendo el IVA Ver fechas de entrega · CPU: 1xSilver 4310 2.1GHz · Memoria:2x16GB RDIMM · Disco duro1x480GB SSD SATA RI	 P24841-B21 **Nombre del producto:** Hewlett Packard Enterprise ProLiant DL380 Gen10 servidor 72 TB 2,4 GHz 32 GB Bastidor (2U) Intel® Xeon® Silver 800 W DDR4-SDRAM **EAN:** 4548821156492 **Part Number:** P24841-B21	 Fujitsu PRIMERGY RX2520 M5 servidor 2,2 GHz 32 GB Bastidor (2U) Intel® Xeon® Silver 450 W DDR4-SDRAM
Model	PowerEdge R550	ProLiant DL380 G10	Primergy RX2520 M5
Preu	3787,01€	3.630€	3546,81€
Característiques principals	12x2,1Ghz - 32GB RAM - 480GB SSD	10x2,4Ghz - 32GB RAM - 450GB SSD	12x2,2Ghz - 32GB RAM - 480GB SSD

***Taula 6**. Taula comparativa de hardware*

Tots 3 tenen característiques molt similars i preus similars, però finalment escolliré el **Proliant DL380 G10,** ja que és un fabricant amb una reputació considerable i una qualitat / preu molt alta.

Com ja he comentat anteriorment, el sistema operatiu que instal·larem serà Linux. En l'organització s'instal·la CentOS 7 o 8 com a distribució Linux i es fa servir una imatge ja preconfigurada amb les configuracions i aplicacions corporatives.

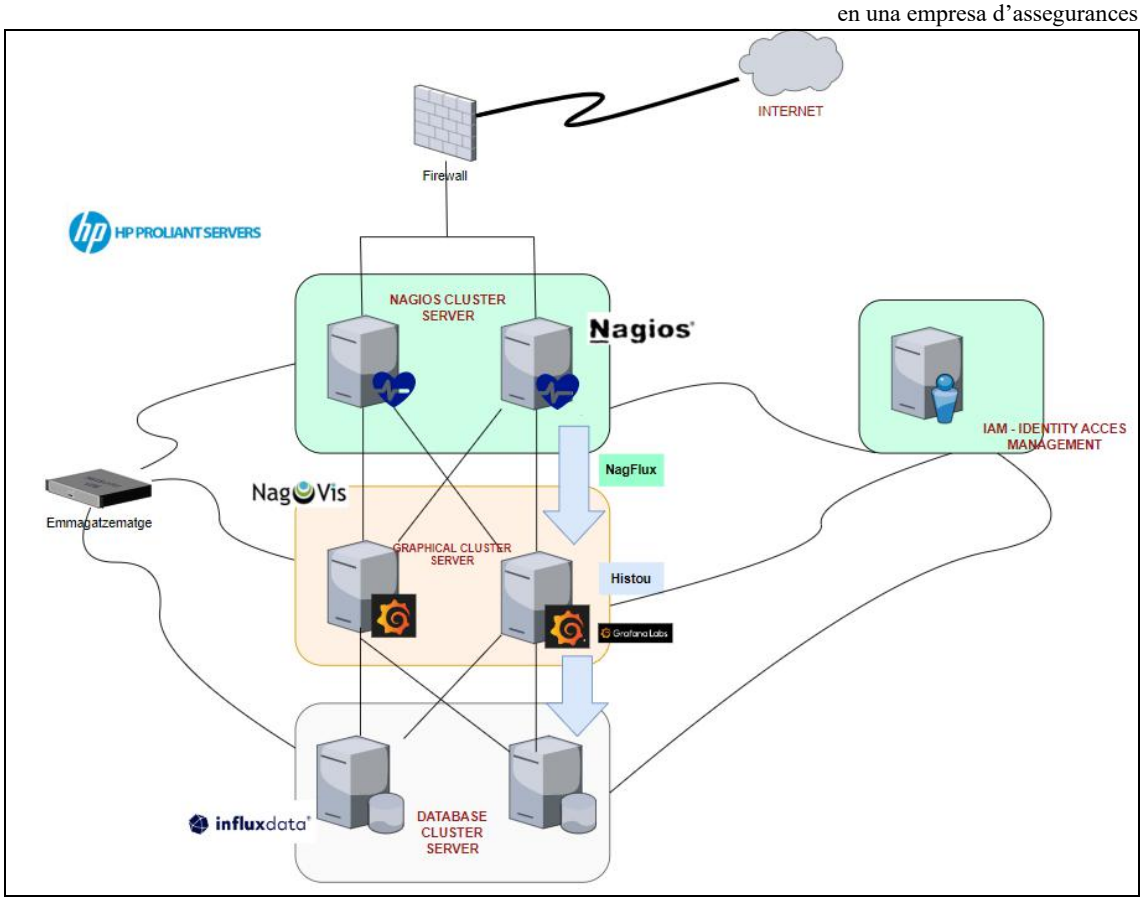


***Figura 9**. Diagrama Lògic de la proposta*

8. Disseny i Implementació del sistema de monitoratge

8.1. Política de Monitoratge

Començo el procés de disseny definint la política de monitoratge a aplicar. Aquesta política ens determinarà quins seran els elements a supervisar i com s'haurà d'actuar per a garantir el bon funcionament dels sistemes. El contingut d'aquesta política serà:

1. Objectius
2. Àmbit
3. Responsables
4. Definició dels elements a monitorar
5. Privacitat

S'adjunta en el document *Política de Monitoratge.doc* la definició d'aquesta política.

8.2. Instal·lació del hardware

Per a l'entrada del material al CPD s'ha de realitzar una petició i una ordre per enrackar els servidors a l'armari corresponent.

Adjunto una sol·licitud a mode d'exemple.

8.3. Instal·lació del Sistema Operatiu

A la nostra organització la instal·lació del sistema operatiu es realitza mitjançant una imatge pre-gravada. He de demanar al departament de TI la instal·lació d'un determinat sistema (Windows o Linux) i una vegada instal·lat, amb les utilitats com antivirus i còpies de seguretat, es fa entrega al sol·licitant. El nom i la IP també són assignades quan es fa la instal·lació.

Recentment, i veient que les versions 7 i 8 de CentOS han perdut el suport del fabricant o el perdran ben aviat, s'ha decidit per part de l'organització incloure imatges d'altres distribucions Linux; de les proporcionades per l'organització (Debian, Centos 7 /8, RHEL) hem escollit finalment Debian, ja que en el cas de RHEL tenim un cost addicional de les llicències i en el cas de CentOS aviat es veuran fora de suport. De la distribució Debian s'ha escollit per part de l'organització la versió **Debian 10.**

Afortunadament, aquest canvi no produeix una desviació en la meva planificació, ja que el temps d'entrega del servei és la mateixa.

S'inclou un fitxer d'exemple amb la sol·licitud de petició d'instal·lació del maquinari.

8.4. Instal·lació del programari

Segons quina imatge s'instal·li ja venen preinstal·lats alguns paquets de programari necessari, però molts altres s'han d'instal·lar. A continuació adjunto un breu resum del programari a instal·lar i es proporciona una guia de configuració i instal·lació de tot aquest programari.

- **Apache 2**: Servidor Web de codi obert, multiplataforma. És un dels servidors web més estès en el món.
- **PHP**: Conjunt de llibreries i fitxers perquè es puguin interpretar les ordres en llenguatge php des del servidor Apache.
- **SSH**: Aplicació que serveix per connectar al servidor mitjançant un protocol segur .
- **GCC**: Compilador integrat a Linux per tal de generar un executable binari a partir de codi C, C++, Objective o Fortran.
- **Wget**: Eina que serveis per descarregar contingut d'Internet de forma similar a com ho faria un navegador o explorador web.
- **Make:** Utilitat del sistema operatiu Linux que permet crear fluxos de configuració o instal·lació seguint les dependències prèviament establertes.
- **OpenSSL:** Llibreria compartida generada a partir de la implementació dels protocols TLS.
- **Dnsutils:** Conjunt d'utilitats per treballar amb servidors DNS.
- **SmbClient:** Utilitat client per a accedir a recursos de servidors de fitxers Samba. És similar a com funcionen els servidors FTP.
- **PaceMaker:** És una aplicació de gestió de recursos de clúster d'alta disponibilitat de codi obert. Es fa servir juntament amb CoroSync per a gestionar els nodes que pertanyen a un clúster de recursos.
- **CoroSync:** Sistema de comunicació de codi obert per a comunicar diferents nodes en un clúster

- **Rsync:** Eina per sincronitzar directoris i fitxers d'una manera segura i amb control de fallida.

- **Curl:** Eina per consultar i descarregar pàgines web, molt completa i amb infinitat d'opcions.

- **NTP:** Eina pel control i sincronització de l'hora actual.

S'acompanya una guia de programari on es veuen amb més detall aquests apartats.

8.5. Integració amb els sistemes d'emmagatzematge

Els servidors disposen del seu emmagatzematge local, proporcionat pels discos, però per guardar les bases de dades és necessari afegir un emmagatzematge addicional. A més és un sistema d'emmagatzematge més segur i amb més recolzament i menys punts de fallida, amb una alta disponibilitat.

He calculat que es necessiten uns 100 GigaBytes d'emmagatzematge per cada any de dades i per cada entorn. Com ens han demanat guardar un mínim de 6 mesos, amb un any estem arribant perfectament a l'objectiu marcat. Com he de disposar de 4 entorns, Producció, UAT, Integració i Desenvolupament, necessitaré 400GB inicialment.

Per demanar aquests 400 GigaBytes, he de realitzar una petició indicant la quantitat, les propietats i el tipus de disc que es vol. En aquest cas, com no és una gran quantitat, escolliré el tipus de disc amb el millor rendiment.

Es proporciona en els annexos un exemple de petició d'emmagatzematge.

8.6. Integració amb els sistemes de seguretat

En referència al departament de seguretat, que en la nostra organització s'anomena GIS, em demanen que l'aplicació tingui una seguretat per doble autenticació a més una validació per usuari / contrasenya. En la nostra organització per fer la doble autenticació es fa servir el proveïdor Google Authenticator, amb el que ja s'han realitzat diferents integracions. S'adjunta amb la configuració Apache de l'eina, aquesta configuració.

A més les dades han de trobar-se protegides i s'ha de mantenir el principi de confidencialitat, integritat i autenticitat. Gràcies al fet que les dades en tot cas es mantenen dins de la xarxa de l'organització, aquesta responsabilitat recau, en gran part, sobre les infraestructures internes de l'organització. He identificat, per la meva part, tant els rols necessaris, així com els usuaris que hauran de tenir els rols amb més privilegis.

Rol	Descripció
Administrator	Rol amb tots els privilegis i tots els grups
Editor	Rol amb tots els privilegis però sobre un grup de monitors o servidors definits prèviament
Operator	Aquest rol tan sols pot veure les alertes i anotacions dels monitors però no pot modificar res.
Contact Only	No tindrà accés a l'aplicació, però si podrà rebre correus o SMS

***Taula 7**. Taula de rols necessaris*

A més, he establert un flux per a la gestió d'usuaris (sol·licitud d'alta, baixa o modificació d'usuaris i els rols de l'aplicació, així com dels grups que es considerin necessaris).

La petició haurà d'arribar en tot cas mitjançant l'eina de *"ticketing"* de l'organització, amb les autoritzacions i documentació necessàries.

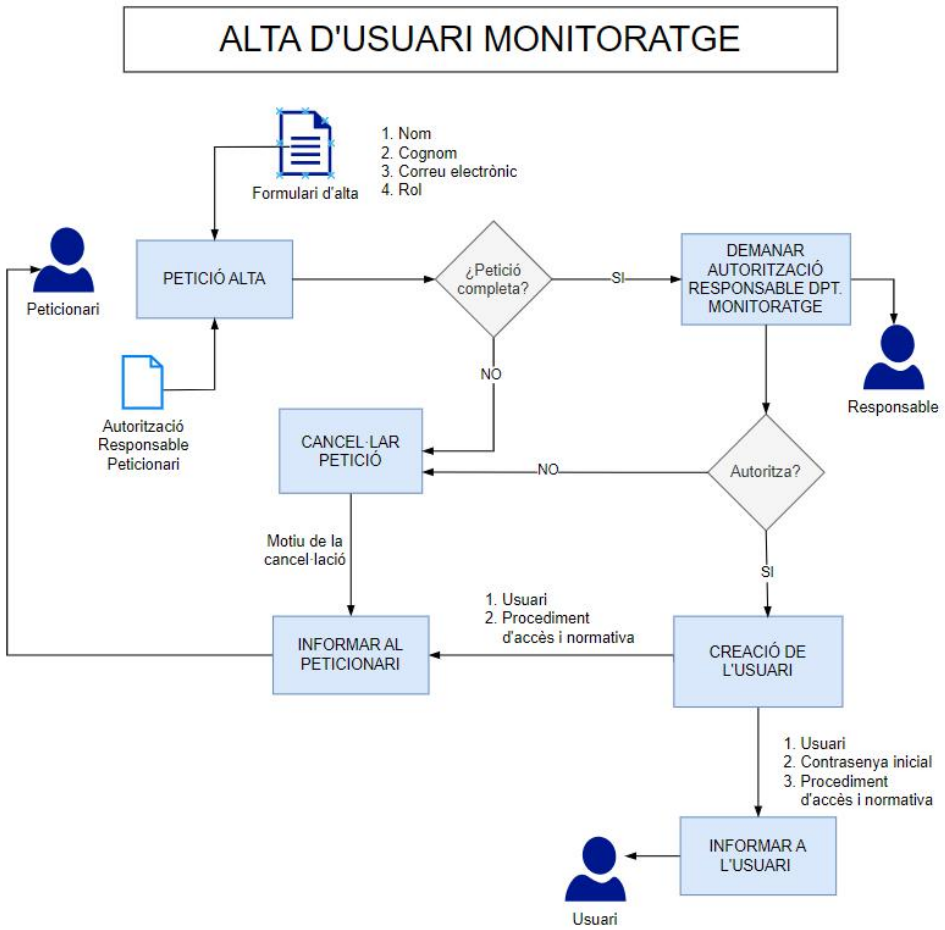


***Figura 10**. Flux d'alta d'usuari de monitoratge*

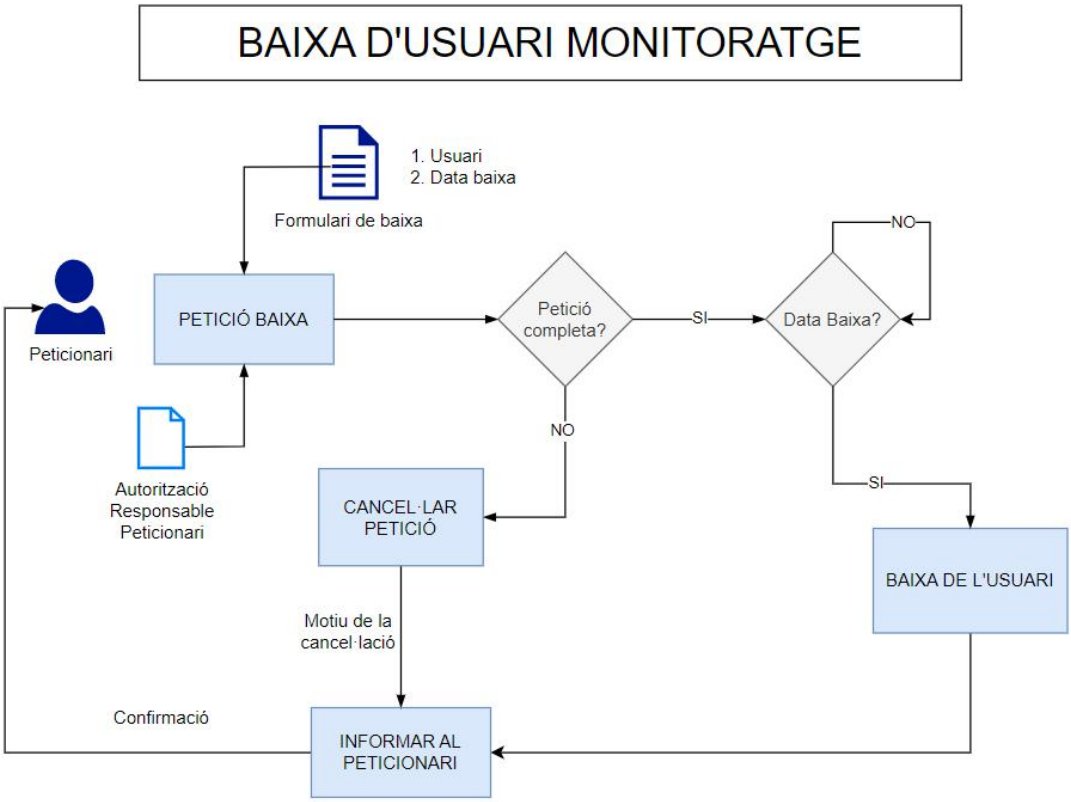


***Figura 11**. Flux de baixa d'usuari de monitoratge*

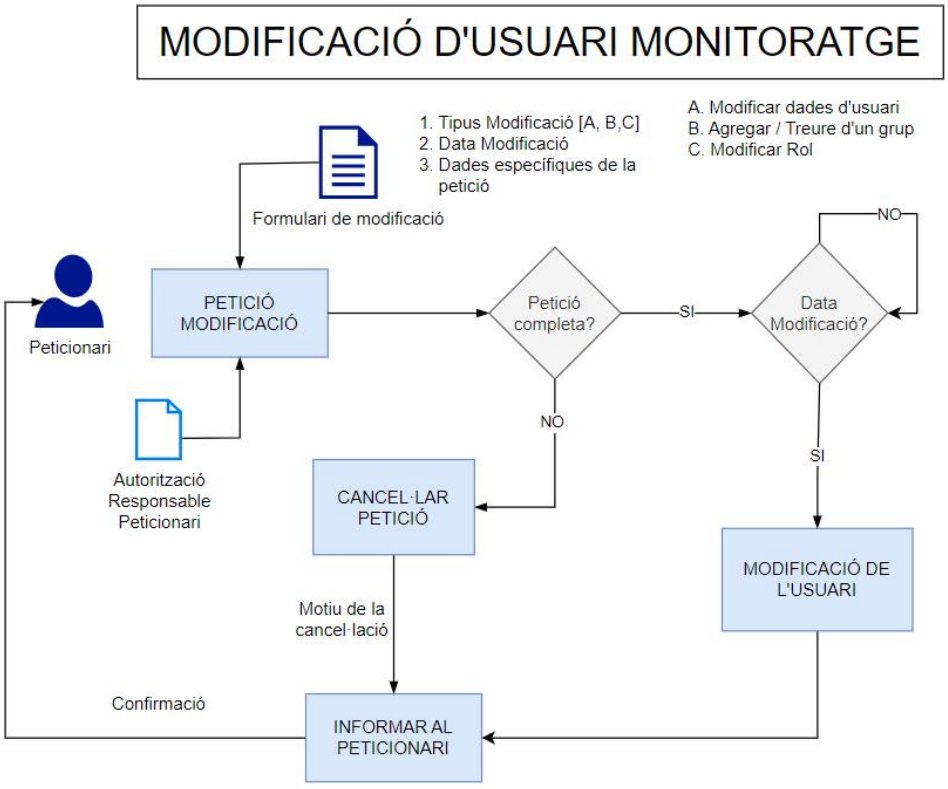


***Figura 12**. Flux de modificació d'usuari de monitoratge*

8.7. Integració amb els sistemes de recolzament

Òbviament, davant d'una contingència s'ha de disposar tant d'una còpia de seguretat d'on es puguin recuperar configuracions, dades o qualsevol fitxer que es requereixi, com davant d'un desastre total, disposar d'un pla de contingència.

Amb aquest objectiu, he creat un exemple de petició a l'equip de recolzament perquè assegurin les dades i també presento un model inicial del pla de contingència amb un anàlisis preliminar dels riscos més importants.

8.8. Instal·lació de les aplicacions de monitoratge

El nucli de les aplicacions de monitoratge es troba en l'aplicació Nagios Core i la solució que he dissenyat millora amb elements de *"time-series database"* com són InfluxDB i de representació gràfica com són Grafana i Nagvis.

Per a les aplicacions web, com el GUI de Nagios i Nagvis i el "*front-end*" de Grafana, es requerirà un balanceig.
- Nagios /Nagvis (4 balanceigs, un per cada entorn)
- Grafana (4 balanceigs, un per cada entorn)

Figura 13. *Imatge d'exemple Nagios Exfoliation Skin*

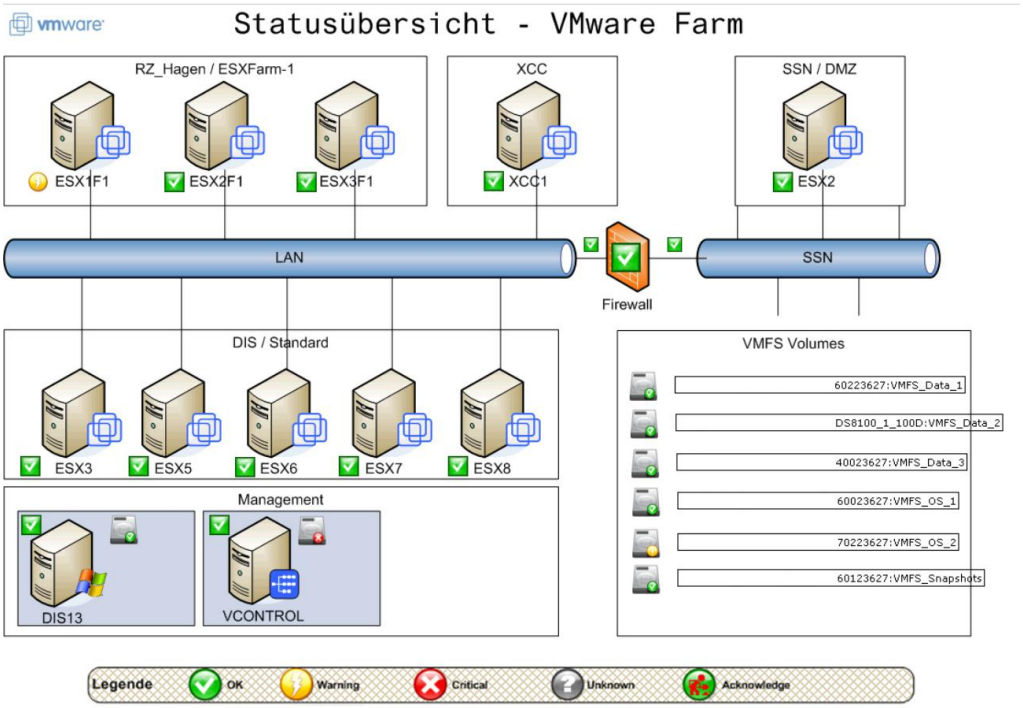


Figura 14. *Imatge d'exemple. NagVis - Map of VMWare Farm*

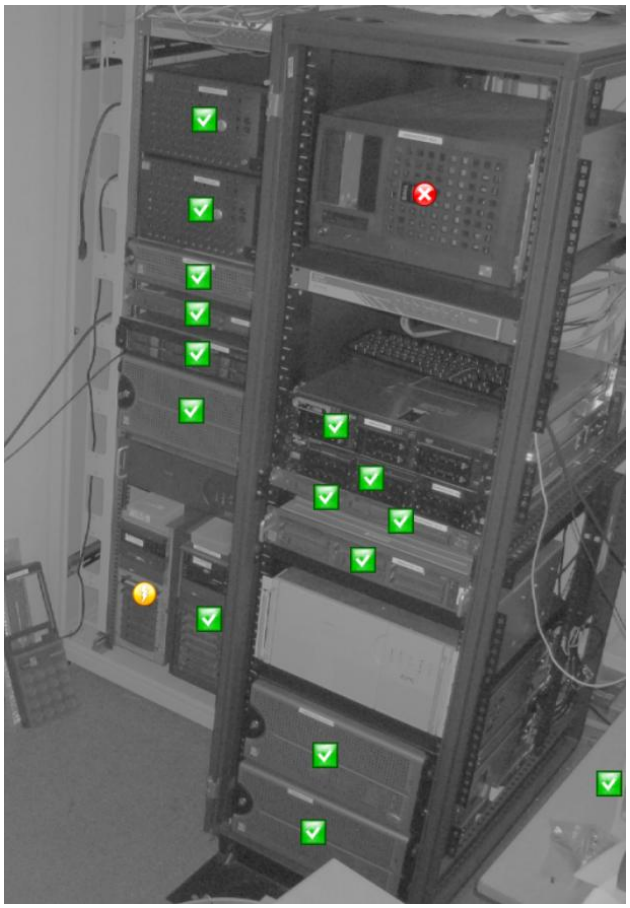


Figura 15. *Imatge d'exemple NagVis - Map of CPD rack*

A més, com es fa servir Nagios Core, hauré d'establir un script propi d'alta disponibilitat que quan no funcioni un dels dos nodes activi l'altre node, i també hauré de realitzar una sincronització dels fitxers de configuració, per entorn. Per a controlar el salt de recursos d'un node a l'altre, farem servir PaceMaker i Corosync. Per tal de no tenir un node sempre aturat, la configuració que escolliré serà Producció en un node, i en l'altre node la resta d'entorns, formant un clúster actiu/passiu, però creuat.

A InfluxDB, seguiré les instruccions i les recomanacions del fabricant, i afegiré 3 servidors de metadades com a valor òptim per a la majoria dels casos i dos servidors de dades. Els servidors de metadades conserven les configuracions dels altres nodes, permisos i consultes contínues. Els nodes de dades guarden les mètriques, els camps i claus reals.

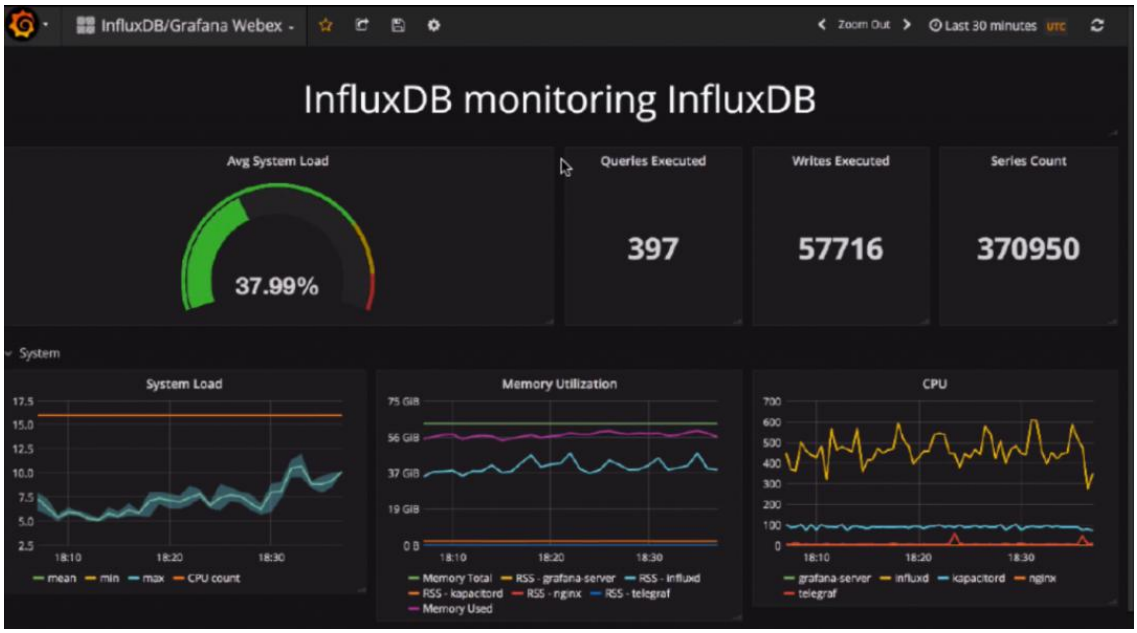


***Figura 16**. Imatge d'exemple. InfluxDB - Grafana Dashboard*

Com Nagflux es pot instal·lar com a servei i es tracta d'un connector, replicaré tants serveis com entorns i servidors hi ha disponibles, només modificant els paràmetres del servei.

En el cas de Grafana, a més de requerir un balanceig, per disposar de HA, he d'afegir a l'arquitectura una base de dades centralitzada. Per tal de no encarir el pressupost, aquesta base de dades l'hauré d'incloure en un servidor ja existent multiservei i si no és possible, en un dels tres servers que formen la infraestructura InfluxDB, aquell que tan sols té el rol de metadada. A més Grafana permet també la configuració de Google Authenticator per fer possible el MFA. Queda pendent de pròximes revisions si l'autenticació serà bàsica, pròpia de Grafana, o si faré servir el directori actiu de l'organització.

Figura 17. *Imatge d'exemple - Grafana dashboard*

Juntament amb la instal·lació de les aplicacions de suport he preparat una guia de la instal·lació del programari de monitoratge.

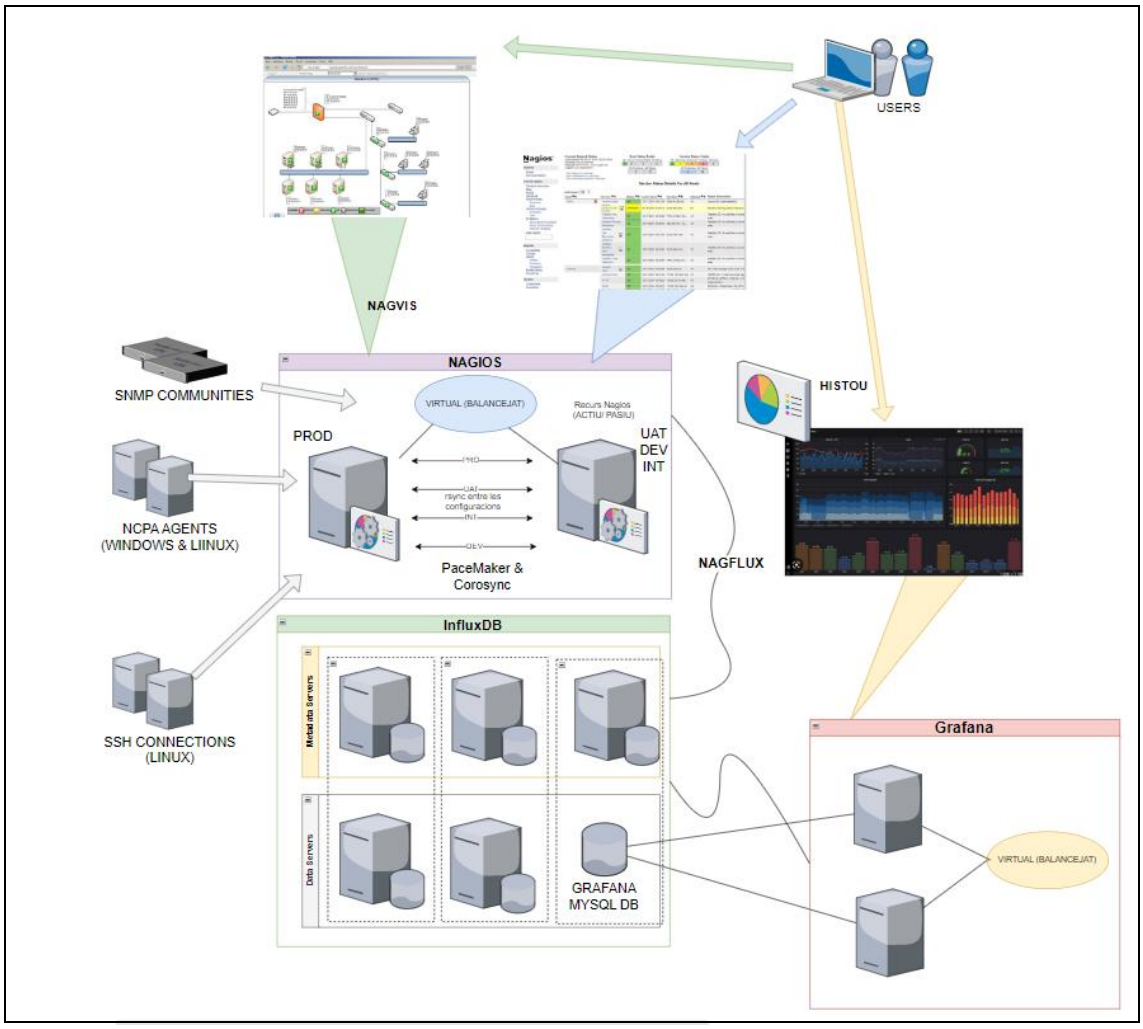


Figura 18. *Esquema lògic. Sol·lució final*

8.9. Implementació de la política de monitoratge

Les aplicacions escollides pel monitoratge són Nagios i Grafana, fent servir com base de dades InfluxDB, a més d'altres petites eines que serveixen de suport o per afegir funcionalitats de les quals no disposen aquestes eines.

A la definició de la política, en el document annex Política de Monitoratge.pdf, ja hem determinat quins seran els elements que es volen monitorar. A Nagios, aquests elements es tradueixen en tot un entramat de fitxers on cada servei, servidor i comanda és un objecte. Les definicions d'aquests objectes els veurem a l'apartat següent de configuració.

En referència a la periodicitat i freqüència del monitoratge, dependrà del servei, però tractant-se de sistemes d'informació, és molt probable que la freqüència sigui constant i continua (24x7). En el cas de Nagios, aquestes implementacions es configuren en un fitxer específic, amb uns objectes concrets que s'anomenen "*timeperiods*" i que es poden combinar per una major flexibilitat.

Com hem comentat en apartats anteriors, hi ha multitud de variables i mètriques a monitorar, que hem definit en fitxers plantilles, on s'agruparan a més els valors per defecte dels llindars d'aquestes variables i mètriques. Aquests es poden interpretar fàcilment. Els valors per defecte, sempre que sigui possible s'afegiran com a "template" de comanda a la configuració de Nagios, de manera que es puguin fer servir aquestes comandes per no javer de repetir constantment els paràmetres a cada objecte.

Existeixen a més a Nagios, plantilles de la configuració, tant de host, comandes, contactes, com altres objectes de la configuració. Quan es defineix una plantilla l'opció "*register"* ha de tenir valor 0. Indico a continuació alguns exemples:

- Definició de la plantilla d'un host:

```
define host{
        name                    linux-server    ; The name of this host template
        use                     generic-host    ; This template inherits other values from the generic-host template
        check_period            24x7            ; By default, Linux hosts are checked round the clock
        check_interval          5               ; Actively check the host every 5 minutes
        retry_interval          1               ; Schedule host check retries at 1 minute intervals
        max_check_attempts      10              ; Check each Linux host 10 times (max)
```

```
        check_command           check-host-alive    ; Default command to check
Linux hosts
        notification_period     workhours           ; Linux admins hate to be
woken up, so we only notify during the day

        notification_interval   120                 ; Resend notifications every 2
hours
        notification_options    d,u,r               ; Only send notifications for
specific host states
        contact_groups          admins              ; Notifications get sent to the
admins by default
        register                0                   ; DONT REGISTER THIS
DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }
```

- Ús de la definició de la plantilla de host:

```
define host {
   host_name       linux-server
   address         10.41.23.54
   use             generichosttemplate
}
```

- Definició de la plantilla d'un servei:

```
define service{
        name                    generic-service     ; The 'name' of this service
template
        active_checks_enabled   1                   ; Active service checks are
enabled
        passive_checks_enabled  1                   ; Passive service checks are
enabled/accepted
        parallelize_check       1                   ; Active service checks should
be parallelized (disabling this can lead to major performance problems)
        obsess_over_service     1                   ; We should obsess over this
service (if necessary)
        check_freshness         0                   ; Default is to NOT check
service 'freshness'
        notifications_enabled   1                   ; Service notifications are
enabled
        event_handler_enabled   1                   ; Service event handler is
enabled
        flap_detection_enabled  1                   ; Flap detection is enabled
        process_perf_data       1                   ; Process performance data
```

```
        retain_status_information       1               ; Retain status information
across program restarts
        retain_nonstatus_information    1               ; Retain non-status
information across program restarts
        is_volatile                     0               ; The service is not volatile
        check_period                    24x7            ; The service can be checked at
any time of the day
        max_check_attempts              3               ; Re-check the service up to 3
times in order to determine its final (hard) state
        normal_check_interval           10              ; Check the service every 10
minutes under normal conditions
        retry_check_interval            2               ; Re-check the service every
two minutes until a hard state can be determined
        contact_groups                  admins          ; Notifications get sent out to
everyone in the 'admins' group
        notification_options            w,u,c,r         ; Send notifications about
warning, unknown, critical, and recovery events
        notification_interval           60              ; Re-notify about service
problems every hour
        notification_period             24x7            ; Notifications can be sent out
at any time
        register                        0               ; DONT REGISTER THIS
DEFINITION - ITS NOT A REAL SERVICE, JUST A TEMPLATE!
        }
```

- Definició de la plantilla d'un contacte:

```
define contact{
        name                            generic-contact     ; The name of this contact
template
        service_notification_period     24x7                ; service notifications can be
sent anytime
        host_notification_period        24x7                ; host notifications can be sent
anytime
        service_notification_options    w,u,c,r,f,s         ; send notifications for all
service states, flapping events, and scheduled downtime events
        host_notification_options       d,u,r,f,s           ; send notifications for all host
states, flapping events, and scheduled downtime events
        service_notification_commands   notify-service-by-email     ; send service
notifications via email
        host_notification_commands      notify-host-by-email        ; send host
notifications via email
        register                        0               ; DONT REGISTER THIS
DEFINITION - ITS NOT A REAL CONTACT, JUST A TEMPLATE!
        }
```

La configuració de retenció de dades s'estableix a InfluxDB i en principi, serà de 6 mesos, si és possible per espai, 12 mesos. A més s'ha definit una retenció de les còpies de seguretat d'un any.

S'ha definit, a més, configuracions d'accés mitjançant Google Authenticator a més d'usuari i contrasenya, en espera de poder configurar l'accés amb validació LDAP, si el projecte s'accepta.

8.10. Configuració de les eines de monitoratge

En els sistemes Nagios els llindars es defineixen en cada servei com una variable que es pot incloure en la mateixa comanda. Així doncs, tenim un servei com el següent per controlar la càrrega de la CPU:

```
define service {
   use                     local-service
   host_name               localhost
   service_description     Current Load
   check_command           check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
}
```

Com podem observar, a més de passar la comanda que es farà servir per controlar el servei, es fan servir variables per passar els llindars (*5.0,4.0,3.0 i 10.0,6.0,4.0)*. Aquests llindars poden ser definits en el propi "*plug-in"* per defecte, de manera que si no es passa una variable per paràmetre, es pot fer servir el valor per defecte. Podem veure a continuació la definició d'una comanda d'exemple per controlar la càrrega de CPU:

```
define command {

   command_name    check_local_load
   command_line    $USER1$/check_load -w $ARG1$ -c $ARG2$
}
```

Com podem veure el "*plug-in"* es "*check_load",* que no te definits uns valors per defecte i és obligatori establir un llindar *"warning"* i un *"critical" amb els paràmetres -w i -c*. Si no es passen aquests paràmetres i en unes condiciones especifiques la definició pot ser incorrecte.

Així doncs, s'ha de pensar molt bé primerament, quins seran els valors per defecte per a cada tecnologia i per a cada mètrica que volem controlar. Aquests poden ser diferents, segons si estem parlant d'una subcategoria o altra. Per exemple, a sistemes operatius Windows, potser ens interessa tenir un percentatge de CPU i en un servidor Linux ens interessa tenir un altre o mesurar la càrrega de la CPU no per percentatge si no per càrrega del processador. A continuació els valors que establirem

per a cada servidor o element que volem monitorar, també poden ser diferents, segons si un servidor és de base de dades o és tracta d'un servidor web o d'aplicació.

Per acabar, i ja en una escala superior, hi ha possibilitat d'establir una lògica de mètriques, pel que fa al fet que si una mètrica es troba fora del llindar correcte, però una altra no, activar o no, una alerta. Fins i tot aquests elements poden ser agrupacions (*hostgroups o servicegroups*) de diferents servidors o de serveis diferents.

És a dir, potser per exemple que disposem d'un clúster SQL i tenim un dels nodes al 90% de CPU, però l'altra, de l'altre node, es troba en un 10%. Aquí no tenim una alerta crítica, sinó, que podem configurar una alerta o problema (warning), que sigui d'una criticitat inferior. En el cas que totes dues CPU's arribin a un llindar crític, llavors sí enviar l'alerta crítica.

A continuació es proposa algunes configuracions per defecte:

Categoria	Subcategoria	Descripció	Llindar Warning per defecte	Llindar Critical per defecte
Sistemes Windows	CPU	CPU used	80%	90%
Sistemes Linux	CPU	CPU Load	5.0,4.0,3.0	10.0,6.0,5.0
Sistemes Windows	Memòria	Current memory used	80%	90%
Sistemes Windows	Memòria	Page memory used	2 GB	3 GB
Sistemes Windows	Memòria	Cache memory used	6 GB	8 GB
Sistemes Linux	Memòria	Current memory used	80%	90%
Sistemes Linux	Memòria	Swap memory used	70%	80%
Sistemes Windows	Disc	Disk used percent	80%	90%
Sistemes Linux	Disc	Disk used percent	80%	90%
MSSQLServer	Database	Database size	8 GB	10 GB
MSSQLServer	Server	SQL Errors	20	40
MSSQLServer	Database	DBFreeSpace	20%	10%
MySQL	Server	Connections	40	50
MySQL	Server	Concurrent process	100	150
Apache	Server	Current Workers	600	800
Apache	Server	Requests per second	10	20

Taula 8. Taula de llindars per defecte

Aquests són alguns exemples. La llista de mètriques i tecnologies que es poden monitorar amb aquestes eines és considerablement molt més extensa i no es troba en l'àmbit d'aquest treball fer una llista extensa i completa de totes les mètriques i components que es poden monitorar.

8.11. Instal·lació i configuració dels agents

Sempre que sigui possible és millor el monitoratge sense agents o amb connexions segures i xifrades, però quan trobem sistemes tancats o dins d'un proxy, es fa necessari aquest tipus de monitoratge.

Nagios, per l'origen del seu "*core*", està pensat per tecnologies amb base Linux o sistemes operatius derivats, com poden ser AIX, UNIX, etc. Aquests es poden monitorar amb connexions segures SSH.

Per al monitoratge de sistemes tancats o d'altres fabricants, com Microsoft i Apple, es disposa d'agents que s'instal·len al servidor client i es configuren per a acceptar les connexions dels servidors Nagios.

Faig a continuació una descripció breu dels agents disponibles:

- NRPE (Nagios Remote Plugin Executor). Va ser el primer dels agents i ens permet monitorar remotament sistemes Linux i Apple iOS. L'agent s'instal·la al servidor remot i mitjançant peticions des del servidor, s'executen els scripts al sistema remot, retornant els resultats.

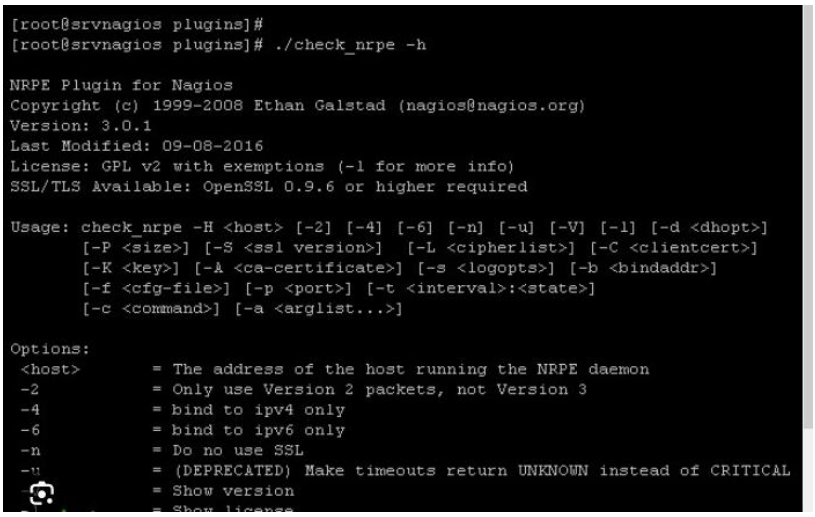


Figura 19. Check_nrpe help.

- NSCA (*Nagios Service Check Acceptor*). Es tracta d'un dimoni que permet, a més del monitoratge actiu que permet NRPE, un monitoratge passiu fent servir un procés en el mateix agent per cridar al servidor Nagios i entregar-li els resultats.

- NRDP/NRDS (Nagios Remote Data Processor/Sender) . Una evolució de NSCA que permet la comunicació amb protocols més flexibles com HTTP o XML.

- NSClient/NSClient++. Principalment utilitzat a sistemes Windows, és un dimoni que ens permet utilitzar agents NRPE, NSCA o NRDP d'una manera conjunta i fent servir la mateixa configuració, a més d'altres plataformes com poden ser Check_MK o Graphite. Com era un projecte de la comunitat, va quedar obsolet fa temps i ara ja no es fa servir.

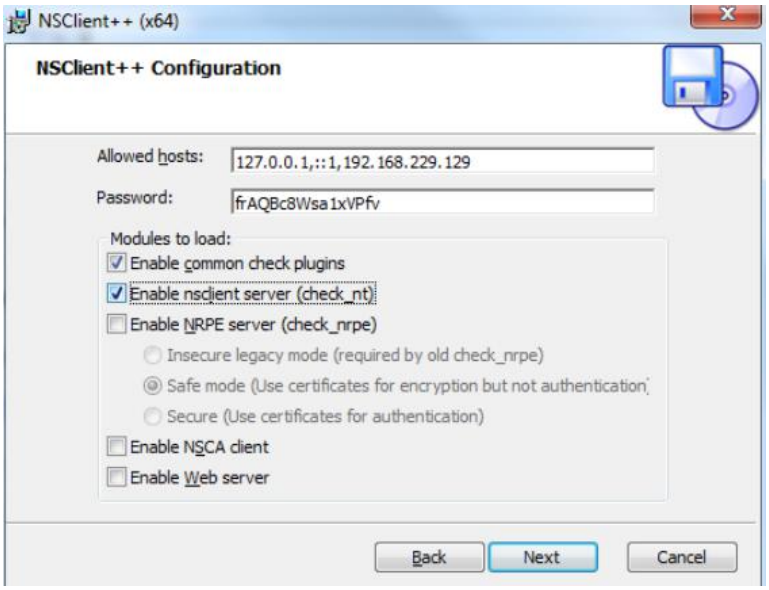


Figura 20. Instal·lació NsClient++

- NCPA (Nagios Cross-Platform Agent) . És l'actual plataforma d'agents de Nagios i permet gairebé totes les possibilitats dels altres agents. Es tracta d'una plataforma universal, per a molts sistemes, Linux, Windows i Apple i molt flexible. És la que faré servir a la meva proposta.

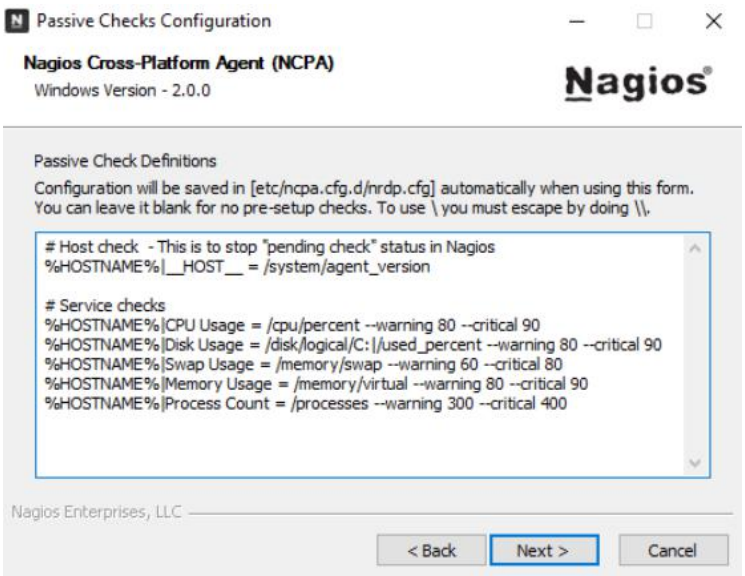


Figura 21. Instal·lació NCPA

A continuació presento una taula comparativa dels agents Nagios on es pot veure que NCPA té totes les característiques dels anteriors agents incorporant alguna més, com per exemple, la GUI per l'usuari.

Agent Comparison:

Features \ Edition	NCPA	NRDS Agent	NSClient ++	NRPE
Installs on Linux	✔	✔		✔
Installs on Windows	✔	✔	✔	
Installs on Mac OSX	✔	✔		✔
Graphical User Interface	✔			
Active Check Metrics	✔		✔	✔
Passive Check Capabilities	✔	✔	✔	
Flexible API Access	✔			
Seamless Integration with Nagios XI	✔		✔	✔
Integration with Nagios Core via NRDP	✔	✔	✔	
Official Nagios Enterprises Monitoring Agent	✔			
Pre-configured Monitoring Metrics	✔		✔	✔
Integration with NRDS Configuration Protocol		✔		

Taula 9. *Taula comparativa d'agents Nagios*

8.12. Configuració dels dispositius de xarxa

A més de les configuracions d'agents que hem vist a l'apartat anterior, hi ha certs sistemes, molt tancats, que no permeten gairebé cap mena de connexió i on només està permès la comunicació mitjançant protocols SNMP, principalment les versions SNMPv2 i v3 que són més estables i segures. Aquests dispositius solen ser dispositius de xarxa o "*appliances*" amb protocols i ports tancats, principalment amb sistemes operatius Linux, encara que també hi ha sistemes iOS o Android, que no permeten connexions SSH o d'altres protocols més configurables.

La configuració en aquests casos és realment simple. Una vegada configurat el protocol SNMP en el dispositiu (cada dispositiu pot ser molt diferent, segons el fabricant), s'ha de descarregar els MIBS del fabricant d'aquest dispositiu. Els MIBs del dispositiu ens indicaran els codis (OIDs)[Figura 22] que accepta aquest dispositiu i la informació que en podem treure per tal de monitorar-ho.

Amb un *"plug-in"* específic de Nagios, "check_snmp", farem servir l'OID de l'objecte que volem monitorar o el seu àlies, on, amb els paràmetres adequats podem extreure la informació del dispositiu. Per exemple, a continuació presento una comanda d'exemple:

#/usr/local/nagios/libexec/check_snmp -H 172.16.12.1 -o sysDescr.0 -P 3 -a MD5 -L authPriv -x AES -U nagios -A nagioskey -X nagioskey

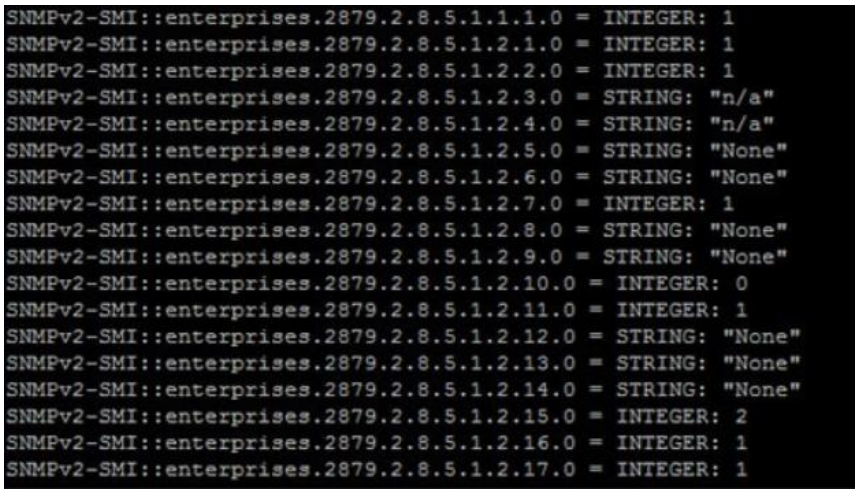


Figura 22. Exemple Estructura OID SNMP v2

Com veiem amb el "*plugin*" "check_snmp" a més de la IP del dispositiu, hem de passar alguns paràmetres més, que tindran a veure amb la versió del protocol SNMP que fem servir, com per exemple:

- Versió del protocol SNMP
- Protocol d'autenticació
- Protocol d'encriptació
- Usuari i contrasenya d'autenticació
- Clau d'encriptació
- L'àlies de l'OID o identificador del MIB

La resposta a aquesta comanda pot ser:

SNMP OK - "VyOS 1.2.0-rc8"

Això vol dir que la comunicació i configuració amb el dispositiu a monitorar és correcte. En aquest cas es retorna la descripció de l'objecte, però el monitoratge a través de SNMP ens pot donar a més informació de rendiment i disponibilitat dels elements que componen el dispositiu.

El resultat és similar al que veiem a la Figura 23.

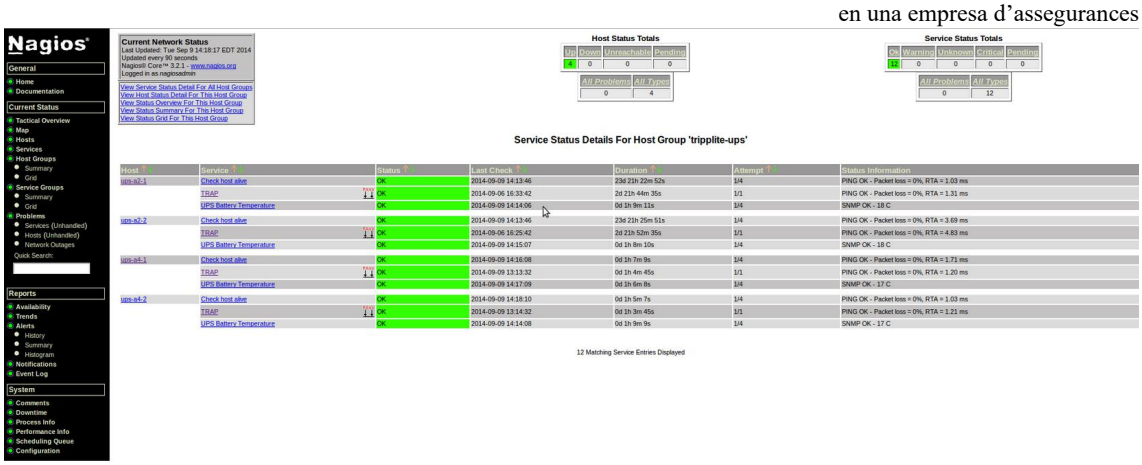


***Figura 23**. Imatge de monitoratge Nagios Dispositius SNMP*

9. Proves i tests

Una vegada tinguem la configuració de tots els elements de monitoratge, i fora de les proves que podem considerar dins del Pla de contingència, hem de realitzar una sèrie de proves per garantir que el sistema es troba ben configurat.

A continuació, presento una taula amb algunes de les proves imprescindibles que considero s'han de realitzar quan el sistema estigui completament configurat i l'objectiu de les mateixes:

Id prova	Descripció	Elements a provar	Resultat previst	En cas que no sigui OK, elements a revisar
1.1	Fallida d'un element monitorat, per exemple espai en disc o ús de memòria per sobre del llindar warning i critical	Nagios Nagvis Grafana	- Alerta "*Warning*" en el sistema Nagios, en el mapa Nagvis, en el "*dashboard*" Grafana i notificació a la llista de distribució establerta. - Alerta "*Critical*" en el sistema Nagios, en el mapa Nagvis, en el "*dashboard*" Grafana i notificació a la llista de distribució corresponent.	- Configuració de llindars del servei, la comanda i el "*plug-in*" de Nagios. - Configuració de Grafana - Configuració del mapa a Nagvis - Configuració de la llista de distribució i notificacions a Nagios
1.2	Aturar un servidor monitorat	Nagios Nagvis Grafana	- Alerta "*Critical*" en el sistema Nagios, en el mapa Nagvis, pèrdua de dades en el "*dashboard*" Grafana i notificació a la llista de distribució corresponent	- Configuració de llindars del servei, la comanda i el "*plug-in*"de Nagios. - Configuració de Grafana - Configuració del mapa a Nagvis - Configuració de la llista de distribució i notificacions a Nagios
1.3	Recuperació d'un element monitorat	Nagios Nagvis Grafana	- Recuperació de l'alerta a Nagios, Nagvis i Grafana. Notificació OK a la llista de distribució corresponent.	- Configuració de llindars del servei, la comanda i el "*plug-in*"de Nagios. - Configuració de Grafana - Configuració del mapa a Nagvis - Configuració de la llista de distribució i notificacions a Nagios
1.4	Recuperació d'un servidor monitorat	Nagios Nagvis Grafana	- Recuperació de l'alerta a Nagios, Nagvis i Grafana. Notificació OK a la llista de distribució corresponent.	- Configuració de llindars del servei, la comanda i el "*plug-in*"de Nagios. - Configuració de Grafana - Configuració del mapa a Nagvis

				- Configuració de la llista de distribució i notificacions a Nagios
1.5	Aturar un dispositiu monitorat amb agent SNMP	Nagios	- Alerta "*Critical*" a Nagios i notificació a la llista de distribució corresponent	- Configuració SNMP de Nagios i configuració SNMP al dispositiu monitoritzat
1.6	Aturar un servidor monitorat per NCPA	Nagios	- Alerta "*Critical*" a Nagios i notificació a la llista de distribució corresponent	- Configuració de NCPA de Nagios i configuració NCPA en el servidor agent.

Taula 10. Taula de proves

10. Pla de Manteniment

Un pla de manteniment és una eina de gestió que té com a objectiu principal conservar els actius i recursos de l'empresa protegint-los d'un mal funcionament i minimitzant els temps d'inactivitat.

La implementació d'un pla de manteniment comporta gran quantitat de beneficis per a l'organització, com la reducció d'inactivitats o interrupcions de servei produïdes per incidències augmentant l'eficiència i reduint les possibles despeses. En l'entorn empresarial actual, podem dir que un pla de manteniment és un element imprescindible, ja que garanteix la productivitat i el funcionament òptim de l'organització.

I no és tan sols un pla de reparacions o actualitzacions, sinó que hi ha diversos punts importants a tenir en compte, com poden ser els proveïdors, les estructures i la planificació d'activitats, així com procediments de seguiment i monitoratge d'aquestes activitats, intervencions realitzades i resultats obtinguts.

En aquest apartat descriuré els elements claus necessaris per a garantir que els recursos i actius que formen part del sistema de monitoratge proposat, es mantinguin en perfectes condicions:

- ✓ Objectius del pla: Establir en aquest punt els objectius principals i específics del pla de manteniment, com per exemple, garantir la disponibilitat del sistema de monitoratge, assolir els nivells de qualitat del servei, millorar l'eficiència operativa o reduir els temps d'inactivitat.

- ✓ Llista d'actius: Recollir tots els equips i dispositius susceptibles d'incloure's en el pla de manteniment amb l'objectiu de disposar d'un inventari de tots aquests elements i poder formalitzar una planificació organitzada.

- ✓ Processos i procediments: Establir, si no existeixen, processos i procediments per a realitzar cada tipus de manteniment amb les instruccions específiques, llistes d'actius que es veuen afectats i protocols de seguretat si escau. Definir els rols i responsabilitats del personal que hagi de participar en el pla de manteniment.

- ✓ Programació de manteniment: Una vegada tenim els actius identificats, haurem de crear la planificació, en temps i periodicitat, dates i horaris d'execució d'activitats així com el tipus de manteniment o activitat.

- ✓ Recursos requerits: Definir els recursos necessaris per a portar a terme la planificació establerta.

- ✓ Gestió de recanvis: En aquest cas, com es disposa d'elements físics, es necessita disposar de certes parts o recanvis del maquinari físic, i portar la gestió corresponent, és imprescindible en el pla de manteniment.

- ✓ Registre i documentació: El registre i documentació del pla de manteniment, de les activitats dutes a terme, dates, resultats de les intervencions i altres dades que puguin ser rellevants per mantenir el registre.

- ✓ Capacitació i formació: Junt amb la planificació de les activitats de manteniment, s'ha de planificar una formació o capacitació, en cas necessari, perquè el personal disposi de les habilitats necessàries per a executar les activitats amb eficàcia i eficiència.

- ✓ Gestió de proveïdors: És més que necessari, com en aquest cas, quan es disposa de diferents proveïdors, que es coordinin totes les activitats de manteniment, així com pactar nivells de servei, establir els requisits, assegurar la fiabilitat, monitorar i garantir els serveis contractats.

- ✓ Millora continua: En el pla de manteniment, com en qualsevol altre procés, també s'ha d'establir un procés de millora, amb elements clau (KPI) per avaluar l'efectivitat del pla de manteniment, i en cas que es pugui, identificar possibles millores i ajustar els processos i les estratègies, en conseqüència.

Com a exemple, faig una proposta de les activitats principals que podrien formar part del Pla de Manteniment:

Index	Activitat	Descripció	Periodicitat
1	Anàlisis prèvies	Realització d'un estudi previ de l'inventari actual i de les activitats a realitzar en cada element del sistema, revisar els llindars i nivells de servei dels proveïdors, així com informes interiors i dels proveïdors.	Anual. Recomanació: que es faci revisió semestral
2	Planificació	Definir el calendari, tenint en compte festius locals/nacionals i si ja es troba disponible, tenint en compte el calendari de negoci (campanyes i promocions nacionals i internacionals). S'establiran en aquest punt tasques BAU com els reinicis de servidors, la renovació de certificats, la renovació de llicències, els manteniments de bases de dades, les actualitzacions de "software", tant d'aplicacions pròpies com de sistemes operatius (Windows / Linux), , i també s'establiran al menys les reunions periòdiques amb els proveïdors. I encara que siguin orientatives, les dates de possibles auditories i proves de desastre (Disaster Recovery).	Anual, i revisió mensual. Recomanació: Proposar reunions mensuals o quinzenals amb els proveïdors. En cas d'auditories i proves de desastre (DR) és recomanable definir responsables exclusius d'aquests processos i preparar un grup de tècnics que portin a cap aquest tipus de proves, ja que la capacitació d'aquests ha de ser especial.
3	Seguiment i Monitoratge	Com s'ha recomanat a l'apartat anterior, és important realitzar seguiment de la planificació establerta, juntament amb el proveïdor o proveïdors, per tal d'analitzar els resultats de les diferents activitats. A més, per part de l'equip d'operacions, és recomanable que es facin reunions internes referents a la capacitat, rendiment o errors que es puguin identificar. En el cas d'un sistema de monitoratge, pot resultar curiós que es demani monitorar el sistema de monitoratge, però no està de més disposar d'una bateria de proves simples que es puguin dur a terme bé manualment o bé mitjançant un automatisme, que ens	El seguiment ha de ser continu, setmanal. Les reunions internes poden ser quinzenals o mensuals.

		alertin si el sistema de monitoratge té problemes.	
4	Gestió d'alertes	Les activitats de manteniment, com per exemple, actualitzacions de certificats o de "software", es poden automatitzar, i aquestes automatitzacions poden enviar notificacions.	El monitoratge és continu, per tant, les notificacions s'enviaran quan s'acompleixin les diferents activitats.
5	Gestió de canvis	La gestió de canvis ja es troba integrada a la nostra organització, però com la resta de canvis que afecten entorns productius, el sistema de monitoratge haurà de seguir les normes i procediments corresponents.	La gestió de canvis és contínua.
6	Manteniments específics	A les bases de dades, com per exemple a InfluxDB s'han de realitzar periòdicament neteja i revisió de les bases de dades. Igualment amb les bases de dades MySQL de Grafana.	Idealment, mensual.
7	Auditories	El departament de GIS ens ha d'indicar, seguint el pla de seguretat, quins controls i auditories s'han de seguir. Normalment, els accessos, i les dades que estiguin emparades per la LOPD han de seguir aquests controls.	Normalment, es realitza una auditoria anual, però no està de més fer-ne un seguiment semestral.
8	Documentació	És important portar registre del pla de manteniment, quant a resultats de les activitats, procediments a seguir, com es realitza el calendari, resultats d'auditories, etc.	Constant. Aquesta actualització de registre ha de ser revisat periòdicament.

Taula 11. Taula d'activitats del Plà de Manteniment

11. Valoració pressupòstaria

A continuació, presento una valoració aproximada del valor econòmic si es realitzés un projecte basat en aquesta proposta:

Concepte	Descripció	Quantitat	Valor Estimat
Nagios Cluster Servers	Servidor HP ProLiant DL380 G10 32 GB 450GB SSD	2	6.000 €
Grafana Cluster Servers	Servidor HP ProLiant DL380 G10 32 GB 450GB SSD	2	6.000 €
Database Cluster Servers	Servidors HP ProLiant DL380 G10 32 GB 450GB SSD	3	6.000 €
Emmagatzematge PROD	Gold type	100 GB	300 €
Emmagatzematge UAT	Gold type	100 GB	300 €
Emmagatzematge DEV	Gold type	100 GB	300 €
Emmagatzematge INT	Gold type	100 GB	300 €
Projecte de Disseny i implementació d'una solució de monitoratge	Disseny i implementació de la proposta (1 Analista)	240 hores	12.000€
	Disseny i implementació de la proposta (1 Tècnic)	120 hores	4.000€
	Instal·lació i configuració de les eines de monitoratge (1 Tècnic)	60 hores	2.000€
	Implementació dels monitors aplicant la política de monitoratge. (1 Tècnic)	30 hores	1.000€
	Proves i tests de la implementació. (1 Tècnic)	30 hores	1.000€
	Documentació i registre del projecte (1 Tècnic)	60 hores	2.000€
	Formació i capacitació (1 Tècnic)	30 hores	1.000€
	TOTAL		**42.200€**

Taula 12. Taula de valoració pressupostaria (Instal·lació. 1er any)

El valor final d'aquesta **proposta** és proper als **42.000 €** sumant el cost del "*hardware*", l'espai d'emmagatzematge, la instal·lació i configuració de les eines i el desplegament dels monitors inicials, així com documentar el projecte i preparar el personal que mantindrà el sistema.

No he considerat la possibilitat de crear un entorn de pre-producció, ja que els entorns, producció i UAT, haurien de ser el més similars possible i per tant, el pressupost arribaria a més de 60 mil euros. Això no significa que no es pugui tenir diferents instàncies de monitoratge, una per a cada entorn, amb bases de dades i configuracions separades.

Com hem vist en apartats anteriors, es poden realitzar configuracions per entorn de manera que aprofito al màxim els servidors. És contraproduent en el cas de desastre total, però és més econòmic i amb la virtualització és possible disposar de gairebé les mateixes funcionalitats, però en aquest cas, en entorns virtuals, com he comentat en el pla de contingència.

En aquesta valoració tampoc he tingut en compte llicències o contractes de suport. És cert, que en un entorn empresarial, fins i tot amb les eines "*open source*", se sol contractar un suport, però inicialment no ho contemplo per tal de contenir les despeses en el cost més baix possible.

A més del cost del propi projecte, també he estimat el cost del manteniment anual (running):

Concepte	Descripció	Quantitat	Valor Estimat
Emmagatzematge	Tots els entorns	400 GB	1.200€
Manteniment del sistema de monitoratge.	Cost d'un tècnic de monitoratge que s'encarregui de les peticions, incidències, creació d'alertes i monitors, creació d'informes, suport al diagnòstic d'incidències, etc.	1800 hores	25.000€
Manteniment de la infraestructura física	Revisió i manteniment de l'estructura física del CPD, serveis de mans remotes, gestió d'accessos, etc.	40 hores	1.200€
	TOTAL		**27.400€**

Taula 13. Taula de valoració pressupostaria (Running)

Amb tot això, veiem que el cost del manteniment anual serien uns **28.000 €** tenint en compte que disposem d'un tècnic pràcticament exclusiu per a la plataforma.

12. Conclusió

En conclusió, aquest treball ha ofert una proposta de monitoratge que s'adapta a la situació actual de l'organització MEDIADORS i ASSEGURANCES S.A. i que, compleix la majoria d'objectius establerts, si no tots, afavorint, en el cas que sigui implementada, la gestió dels sistemes d'informació i reduint el temps de resposta, i com a conseqüència, el temps d'interrupció dels serveis.

Durant la construcció d'aquesta proposta s'han identificat els següents punts clau:

En primer lloc, he analitzat la situació actual de la infraestructura i he avaluat les opinions dels diferents interessats. En aquest anàlisi previ he trobat una situació molt precària, sense gairebé cap mena de monitoratge per part de TI, i que en cas d'interrupció del servei, implicaria una llarga i, totalment ineficient, resolució.

En segon terme, una vegada detectada la necessitat, començo a desenvolupar una solució que permeti la gestió de la informació en temps real, el control dels sistemes i la presa de decisions informades.

La proposta es troba basada en tecnologia de codi obert, de cost contingut, però que cobreix gran part de les necessitats i requeriments esmentats pels interessats, a més d'aportar altres funcionalitats, que poden ser de gran interès per a la direcció, com són, els mapes de Nagvis o els panells de control a Grafana.

Aquesta proposta aporta entre d'altres, els següents beneficis:

- ✧ Millora la informació operativa, ja que proporciona dades i mètriques en temps real sobre els KPI's.
- ✧ Permet una presa de decisions informada i més àgil, cosa que permet optimitzar processos i explotar més eficaçment els recursos disponibles.
- ✧ Contribueix a reduir el temps dedicat a la resolució d'incidències i encarar amb més seguretat i estabilitat qualsevol risc que es pugui presentar en el futur.
- ✧ Permet la detecció de problemes que són invisibles encara perquè no han produït incidències i també permet veure patrons en el comportament, el que facilita les tasques de manteniment i prevenció.
- ✧ Millora la productivitat, ja que disposant d'informació actualitzada, es poden redistribuir els recursos per una optimització funcional i productiva.

Encara que aquesta proposta és molt beneficiosa, és just indicar que té carències i certes limitacions. Com que no s'ha pogut implementar completament, hi ha detalls de les configuracions que no s'han pogut abordar, i que es poden treballar amb més profunditat, com per exemple, la configuració en clúster, o les configuracions més complexes en Nagios, que són molt completes i que en aquest treball hem hagut de veure d'una manera gairebé superficial.

Disposant de certs recursos de maquinari es podria aprofundir molt més en aquesta investigació. El meu desig és que aquesta proposta es pogués convertir en un projecte real sufragat per l'organització. Realment, vist el monitoratge actual, és realment necessària una proposta de millora, sigui aquesta o una altra, però és altament recomanable per la carència detectada.

En resum, la proposta presentada en aquest treball, té prou potencial per a implementar-se i convertir-se en realitat, millorant considerablement el monitoratge de l'organització i aportant les millores ja comentades a un sistema crític per al negoci, com és el Sistema d'Informació.

13. Glossari

Alta disponibilitat (HA). És l'eliminació dels punts únics de fallida per a permetre que les aplicacions continuïn funcionant encara que s'hagi produït una caiguda d'algun component del sistema.

Anàlisi predictiva. És una forma d'anàlisi que fa servir les dades històriques i les mètriques recollides amb anterioritat, per tal de pronosticar l'activitat, els patrons i tendències que esdevindran i anticipar-se a situacions contràries.

Android. És un sistema operatiu relativament nou, basat en Linux estructurat per a dispositius mòbils, tauletes i altres dispositius intel·ligents.

Application Programming Interfaces (API). Conjunt d'aplicacions o eines que permeten la comunicació entre dues aplicacions que inicialment no es poden comunicar. També aquestes aplicacions poden ser mòduls de la mateixa aplicació i l'API permetre la comunicació entre aquests mòduls.

Autenticació Multi Factor (MFA). Es tracta d'un mètode de validació on es requereix dos o més factors de verificació. Aquests factors poden ser e-mail, empremtes digitals, altres accessos biomètrics,etc..

Back-End. Terme que s'utilitza per a definir la part lògica d'una pàgina o aplicació web. És la part no visible i que conté les funcions lògiques.

Base d'Informació Gestionada (Management Information Base o MIB). És la informació jeràrquica d'un dispositiu, de manera ordenada i estructurada i ens indica quines són les ordres i configuracions que es poden alterar en aquest dispositiu. L'estructura de totes les MIBs de tots els fabricants segueixen una estructura similar, que ve definida en la RFC2578.

Business As Usual (BAU). Són aquelles operacions ordinàries que no requereixen una autorització o que ja es troben preautoritzades perquè no impliquen cap risc o el risc ja es troba identificat.

Cloud. Conjunt de serveis que s'ofereixen a les empreses i particulars i que es subministren des d'una xarxa, principalment Internet. Se'n diu núvol perquè inicialment es representaven els accessos a Internet mitjançant aquesta representació.

Critical. Crític en anglès. En el context en el qual el fem servir, ens marca el llindar greu, en el que la situació pot ser insostenible, inclús ens pot indicar que no s'està oferint el servei o que el component que l'ofereix es troba en una situació molt greu.

Dashboard. Panell d'informació que ens mostra informació i mètriques de manera visual i que poden tenir un o diferents orígens.

Diagrama de Gantt. És un tipus de representació gràfica d'un projecte on es poden disposar de les gestions i recursos necessaris i administrar-los i representar el seu repartiment.

Disaster Recovery (DR). En català, Recuperació de Desastre. Es tracta d'una sèrie de proves en les quals se simula la pèrdua total o parcial del servei i es planifica la seva recuperació amb l'objectiu de trobar falles en el sistema, prendre temps de resposta i recuperació i entrenar tant al personal com als proveïdors.

Front-End. Part del desenvolupament web que veu l'usuari.

Identity Access Management (IAM). Control i visibilitat d'accessos de forma centralitzada.

Internet Service Provider (ISP). És un proveïdor de serveis que ens ofereix les connexions i la gestió d'aquestes a canvi d'una quantitat econòmica periòdica o mitjançant un contracte de servei.

iOS. Sistema operatiu dissenyat pel fabricant Apple.

Lightweight Directory Access Protocol (LDAP). Es tracta d'un protocol d'accés lleuger a directoris. Es fa servir principalment per facilitar i gestionar l'accés d'usuaris a fitxers i directoris.

Linux. Conjunt de sistemes operatius de la familia UNIX que es basen en el "*cuore*" Linux, de llicenciament obert, i que amplien i milloren moltes de les funcions dels sistemes anteriors.

Llei Orgànica de Protecció de Dades (LOPD). Llei que protegeix el dret fonamental de totes les persones a disposar i controlar l'ús de les seves dades personals.

Maquinari. Conjunt d'elements físics que estableixen el sistema informàtic.

Monitoring as a Service (MaaS). Se'n diu d'aquells models de servei que s'ofereixen al núvol aplicant les funcionalitats al monitoratge d'altres serveis i aplicacions del núvol.

Network Time Protocol (NTP): Protocol d'internet per a la sincronització de rellotges basat en una arquitectura client-servidor.

Object Identifier (OID). En les bases de dades MIB es fa servir aquest nom per determinar cadascun dels identificadors numèrics als objectes que fa referència.

One Time Password (OTP). Es tracta d'una forma d'autenticació més sòlida que aporta un major factor de seguretat, per tal de protegir les dades confidencials. El sistema consisteix en una contrasenya que és enviada via SMS, e-mail o mitjançant una aplicació a un dispositiu intermedi i que una vegada fet servir, caduca i no es pot reutilitzar.

Open source. Es diu d'aquell "software" pel qual el codi font original es troba disponible gratuïtament i es pot modificar i redistribuir amb una llicència també de codi obert.

Operating System (OS). Sistema operatiu.

PHP. Llenguatge de programació de codi obert, destinat a desenvolupar aplicacions web i pàgines web.

Plug-in. Complement d'una aplicació que contribueix o millora alguna de les funcions de l'eina principal i que s'implementa com una extensió i interacciona mitjançant una API.

Programari. Conjunt de les aplicacions i eines que formen part del sistema informàtic.

Rack. Armari o estructura que serveix per a emmagatzemar dispositius i servidors apilables, és a dir, que es poden apilar d'una manera ordenada. Serveix tant per dispositius de comunicacions com a altres servidors i dispositius amb diferents aplicacions.

Running. En català, corrent. En aquest context se'n diu quan una acció es produeix d'una manera regular.

Secure Shell(SSH). Protocol de xarxa que permet l'accés remot a una connexió xifrada.

Service Level Agreement (SLA). Acord de gestió d'un servei que permet indicar els límits i llindars que s'acceptaran com a mínim de qualitat del servei. Aquests es negocien amb el client i es documenten i avaluen per tal de concretar penalitzacions o gratificacions amb el proveïdor del servei o serveis.

Short Message Service (SMS). Servei que proporciona la possibilitat d'enviar missatges curts mitjançant la línia de comunicació mòbil. Actualment, es fa servir quan no hi ha arriben línies d'una amplada de banda major, com són les línies 4G o 5G.

Simple Network Management Protocol (SNMP). Protocol de capa aplicació que permet la comunicació entre dispositius amb aquest mateix protocol. Principalment, es fa servir en entorns de comunicacions com "*routers*", "*switches*" o "*modems*".

Software as a Service (SaaS). Es tracta d'un model de distribució de programari al núvol on el proveïdor ofereix les aplicacions prèviament pactades amb el client, i on el client no disposa del control de l'aplicació, sinó que tan sols en fa ús.

Transport Layer Security (TLS / SSL). És un protocol de seguretat, versió millorada del SSL (Secure Sockets Layer) i que serveix per autenticar, xifrar i desxifrar la informació.

User Acceptance Testing (UAT). És l'entorn on es realitzen les proves d'acceptació prèvia a la incorporació en l'entorn de Producció.

Warning. Avís en angles. En el context en el qual el fem servir, ens indica un primer llindar en el qual no s'ha arribat encara a una situació greu, però sí que s'ha de revisar l'abans possible.

Bibliografia

[1] **Thales Group**. (07.04.2023). Web Comercial. *One Time Password (OTP, TOTP) : definition, examples.*
https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp

[2] **BiometricVox**. (07.04.2023) Article. *Control de acceso biométrico: ¿qué es y en qué consiste?*
https://biometricvox.com/blog/biometria-de-voz/control-de-acceso-biometrico-que-es-y-en-que-consiste/

[3] **DellTechnologies.** (07.04.2023) Web Comercial. *Servidores de montaje en rack.*
https://www.dell.com/es-es/shop/servidores-dell-poweredge/sc/servers/poweredge-rack-servers?_gl=1*3ksy6e*_up*MQ..&gclid=CjwKCAjw0N6hBhAUEiwAXab-TQoswV4Ro5q2CFysAz2RDo32IE_CobRd5KsyJlWgzD6Z3s-HQUgFghoCNrwQAvD_BwE&gclsrc=aw.ds

[4] **Senectic.** (07.04.2023) Web Comercial. *Fujitsu PRIMERGY RX2520 M5*.
https://www.senetic.es/product/VFY:R2525SX080PL

[5] **DellTechnologies.** (07.04.2023) Web Comercial. *Servidor de montaje en rack PowerEdge R550.*
https://www.dell.com/es-es/shop/povw/poweredge-r550

[6] **PandoraFMS.** (07.04.2023) Article. *Las 16 mejores herramientas de monitoreo de redes*.
https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

[7] **Fujitsu.** (07.04.2023) Web Comercial. *Fujitsu Server Primergy RX25250 M5.*
https://www.fujitsu.com/es/products/computing/servers/primergy/rack/rx2520m5/

[8] **Senetic**.(07.04.2023) Web Comercial. *Hewlett Packard P24821-B21.*
https://www.senetic.es/product/P24841-B21?gclid=CjwKCAjw0N6hBhAUEiwAXab-TeCH9VwUxTKBeSVn4wWYM9PyVng44wjzrpDy2Yiy-IfEfUHuo1QhjRoCOA8QAvD_BwE

[9] **Zabbix.** (08.04.2023) Web Comercial. Zabbix 6.4. https://www.zabbix.com/

[10] **Wikipedia**.(08.04.2023) Article.*Pandora FMS.*
https://es.wikipedia.org/wiki/Pandora_FMS

[11] **Wikipedia**. (09.04.2023) Article. *Zabbix*. https://es.wikipedia.org/wiki/Zabbix

[12] **Pandora** FMS. (09.04.2023) Web Comercial. *PandoraFMS* https://pandorafms.com/es

[13] **Wikipedia**. (09.04.2023) Article. *Zenoss*. https://es.wikipedia.org/wiki/Zenoss

[14] **Zenoss Documents**. (09.04.2023). Document. *Zenoss Installation Guide*. https://www.zenoss.com/sites/default/files/documentation/Zenoss_Core_Installation_Guide_r5.0.x_d1051.15.343.pdf

[15] **Solutions Monitoring Service.** (09.04.2023). Web Comercial. *ITRS OP5 Monitor.* https://www.solucions-im.com/es/op5-monitor

[16] **ITRS Group**. (09.04.2023). Web Comercial. *Product Help.* https://docs.itrsgroup.com/docs/op5-monitor/9.4/index.htm

[17] **Centreon.** (09.04.2023) Web Comercial. Centreon .https://www.centreon.com/

[18] **Nagios**. (09.04.2023) Web Comercial. *Nagios Core*. https://www.nagios.org/projects/nagios-core/

[19] **Prometheus**. (09.04.2023) Web Comercial. *Prometheus. From Metrics to Insight*. https://prometheus.io/

[20] **North Networks**. (09.04.2023) Article. *La guía de comparación definitiva: Nagios XI vs Nagios Core.* https://www.north-networks.com/la-guia-de-comparacion-definitiva-nagios-xi-vs-nagios-core/

[21] **NagVis.** (09.04.2023) Web Comercial. *Nagvis Automap*. http://www.nagvis.org/

[22] **Grafana Labs.** (10.04.2023) Web Comercial. *Grafana, Your Monitoring Stack*. https://grafana.com/

[23] **InfluxDB.** (10.04.2023) Web Comercial. *InfluxDB, It's About Time.* https://www.influxdata.com/

[24] **GitHub**. (15.04.2023) Repositori codi. *GitHub, Griesbacher / nagflux.* https://github.com/Griesbacher/nagflux

[25] **GitHub**. (15.04.2023) Repositori codi. GitHub.*Griesbacher / histou.* https://github.com/Griesbacher/histou

[26] **Nagios Support Knowledgebase**. (20.04.2023). Web Suport. *Nagios Core - Performance Graphs Using InfluxDB + Nagflux + Grafana + Histou.* https://support.nagios.com/kb/article/nagios-core-performance-graphs-using-influxdb-nagflux-grafana-histou-802.html

[27] **Chacho Cool Net.** (21.04.2023). Article. *Cómo Instalar Apache en Debian 10 Buster.* https://chachocool.com/como-instalar-apache-en-debian-10-buster/

[28] **Nagios**. (01.05.2023). Web Suport. *Nagios Core Documentation.* https://library.nagios.com/library/products/nagios-core/documentation/

[29] **Nagios**. (01.05.2023) Web Suport. *Nagios Core 4 Documentation.* https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/index.html

[30] **GitHub**. (01.05.2023) Repositori codi. *Apache Two-Factor (2FA) Authentication with Google Authenticator* https://github.com/itemir/apache_2fa

[31] **GitHub**. (01.05.2023.) Repositori codi. *InfluxDB Cluster.* https://github.com/chengshiwen/influxdb-cluster

[32] **Nagios Core.** (01.05.2023) Web Suport. *Nagios Core Object Definitions.* https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/objectdefinitions.html

[33] **AJPD Soft.** (01.05.2023). Article. *Monitorizar servicio que no abre puertos en Nagios, instalar SNMP en Windows.* https://proyectoa.com/monitorizar-servicio-que-no-abre-puertos-en-nagios-instalar-snmp-en-windows/

[34] **UnixCop**. (01.05.2023). Article. *Grafana HA Cluster Setup.* https://unixcop.com/grafana-ha-cluster-setup/#:~:text=Grafana%20HA%20is%20a%20highly%20available%20and%20fault-tolerant,servers%20are%20there%20which%20fulfill%20the%20user%E2%80%99s%20request.

[35] **Nagios**. (12.05.2023) Web Suport. *Nagios - Agent Comparison.* https://assets.nagios.com/downloads/ncpa/docs/NCPA-Agent-Comparison.pdf

[36] **SysAdmins de Cuba**. Franco Diaz Hurtado. (12.05.2023) Article. *Monitoreo de red con Nagios - Parte II.* https://www.sysadminsdecuba.com/2019/09/monitoreo-de-la-red-con-nagios-parte-ii/

[37] **AxarNet**. (20.05.2023). Article. SSH: todo lo que necesitas saber. https://axarnet.es/blog/ssh

[38] **Hawar Koyi** . (21.05.2023) Web Comercial. *Tibber with Grafana Dashboard.* https://hawar.no/2022/09/tibber-with-grafana-dashboard/

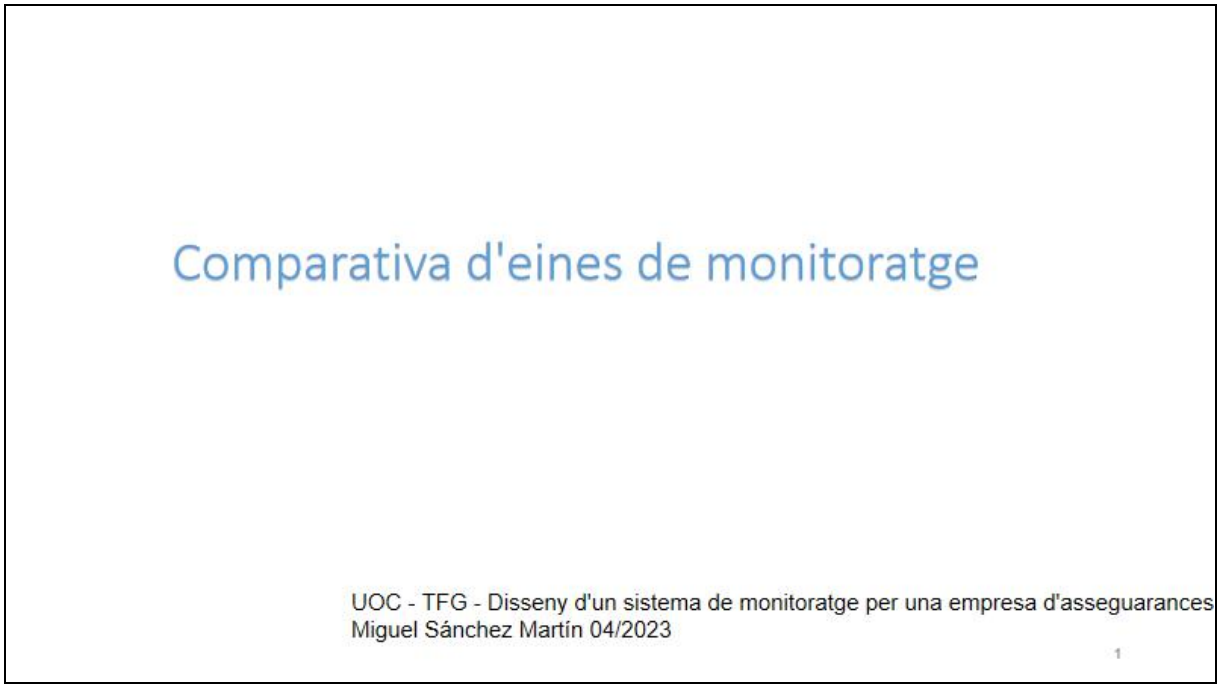
[39] **Formato Digital**. (21.05.2023). Article. *Plan de Mantenimiento Informático: Qué Es y Ejemplos.* https://formatodigital.net/it/plan-de-mantenimiento-informatico-que-es/

[40] **INZ S. Aragon S.COOP.** (21.05.2023) Article. *¿Qué es la LOPD?.* https://www.lopd-proteccion-datos.com/ley-proteccion-datos.php

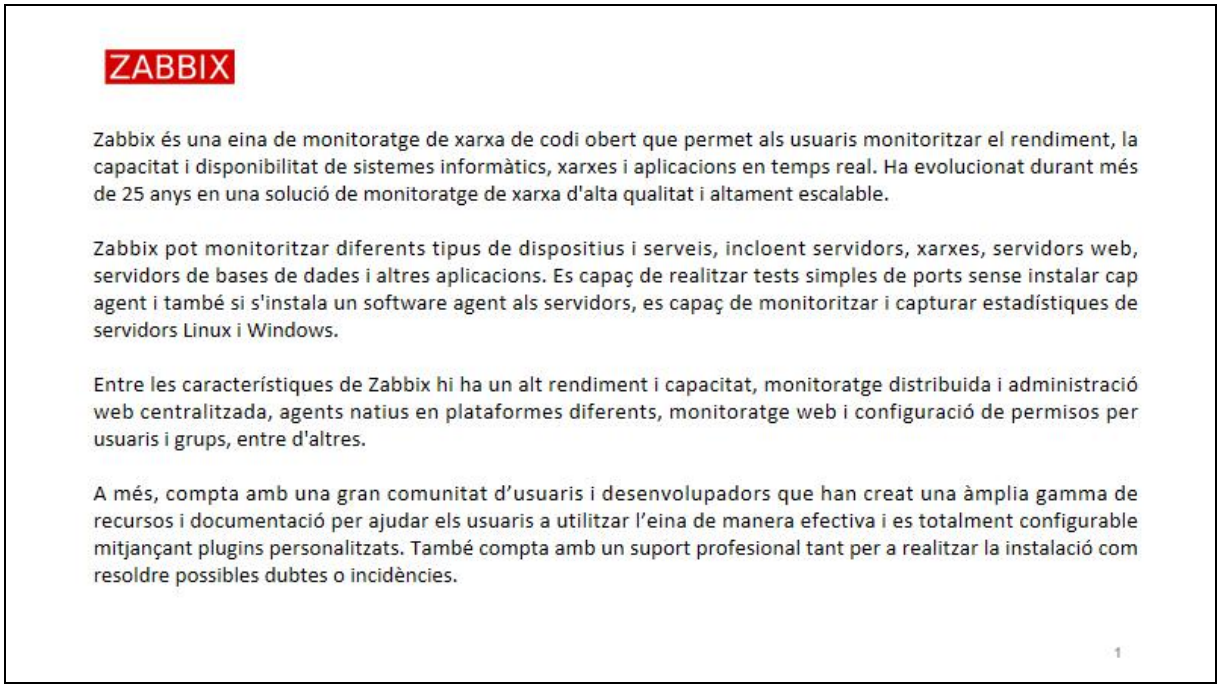
[41] **McConnell Brain Imaging Center** (21.05.2023) Article. *Server Setup*
http://www.bic.mni.mcgill.ca/PersonalMalouinjeanfrancois/NagiosBicSetup

ANNEXES

Annex I. Comparativa d'eines de monitoratge




❑ ZABBIX
ZABBIX
https://www.zabbix.com
❑ PANDORAFMS
PANDORAFMS
https://pandorafms.com/es
❑ ZENOSS
zenoss
Own IT.
https://www.zenoss.com/
❑ OP5 MONITOR
OP5
https://www.itrsgroup.com/products/network-monitoring-op5-monitor
❑ CENTREON
centreon
https://www.centreon.com/centreon-editions/centreon-open-source/
❑ NAGIOS
Nagios
https://www.nagios.org/
❑ PROMETHEUS
Prometheus
https://prometheus.io/
1


ZABBIX
Zabbix és una eina de monitoratge de xarxa de codi obert que permet als usuaris monitoritzar el rendiment, la capacitat i disponibilitat de sistemes informàtics, xarxes i aplicacions en temps real. Ha evolucionat durant més de 25 anys en una solució de monitoratge de xarxa d'alta qualitat i altament escalable.
Zabbix pot monitoritzar diferents tipus de dispositius i serveis, incloent servidors, xarxes, servidors web, servidors de bases de dades i altres aplicacions. Es capaç de realitzar tests simples de ports sense instalar cap agent i també si s'instala un software agent als servidors, es capaç de monitoritzar i capturar estadístiques de servidors Linux i Windows.
Entre les característiques de Zabbix hi ha un alt rendiment i capacitat, monitoratge distribuida i administració web centralitzada, agents natius en plataformes diferents, monitoratge web i configuració de permisos per usuaris i grups, entre d'altres.
A més, compta amb una gran comunitat d'usuaris i desenvolupadors que han creat una àmplia gamma de recursos i documentació per ajudar els usuaris a utilitzar l'eina de manera efectiva i es totalment configurable mitjançant plugins personalitzats. També compta amb un suport profesional tant per a realitzar la instalació com resoldre possibles dubtes o incidències.
1

1

PANDORAFMS

PandoraFMS és una eina de monitoratge de codi obert que serveix per monitoritzar tot tipus de dispositius i sistemes operatius, amb agents específics per a cada plataforma que recullen i envien la informació al servidor. A més pot monitoritzar sistemes de xarxa i altres monitors de forma remota, sense necessitat d'instal·lar agents.

El sistema es forma amb tres components Servidor, consola i agent, i a més hi ha mòduls remots i mòduls locals que són els que permeten el monitoratge de tecnologies de tercers o el monitoratge de sistemes locals respectivament.

Existeix una versió Open Source gratuita però limitada amb la qual es pot configurar gran part del monitoratge necessària, i existeix també una versió MaaS que ofereix la possibilitat de definir un servei gestionat a un preu per agent. Per a disposar de tot el potencial de la eina s'ha de contractar la versió Enterprise que a més te el suport i totes les funcionalitats de l'eina disponibles.

1

1

zenoss
Own IT.

Zenoss es una plataforma de supervisió TI de monitoratge i anàlisi que permet a les organitzacions monitoritzar tots els dispositius i servidors d'una xarxa mitjançant una arquitectura distribuida i un conjunt de tecnologies pensades per les organitzacions empresarials.

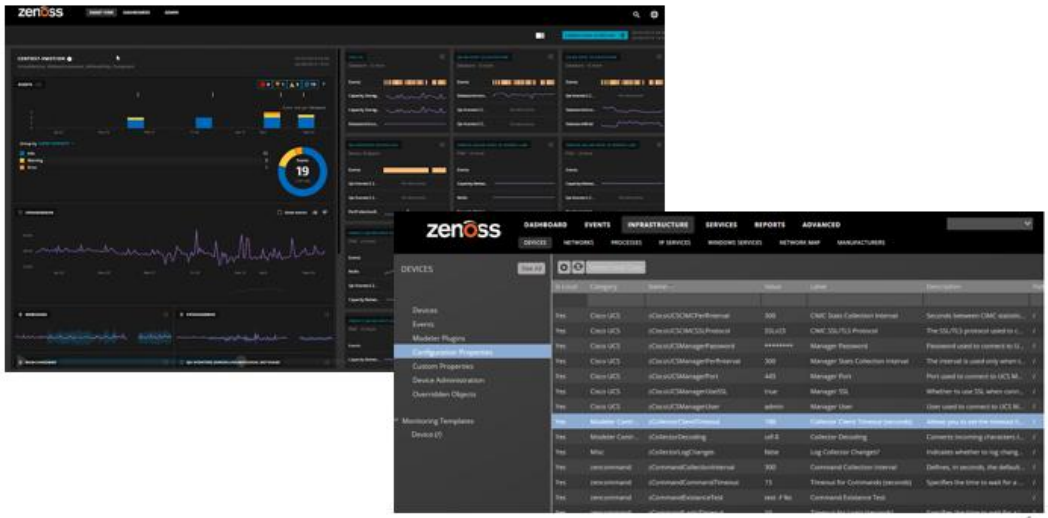
Es capaç de treballar en entorns de xarxes complexes hibrids (local/cloud). És un sistema molt ben dissenyat, encara que la instalació i desplegament es complex. Permet entre d'altres característiques, disposar d'una base de dades on es defineixen els actius previament, i mitjançant el qual es pot definir un monitoratge predictiu i sistemes de detecció previa.

El seu sistema gràfic es molt elaborat i permet el monitoratge remot sense agents mitjançant conexions SNMP, WMI i SSH. Per contra, requereix que es configurin els servidors per aquests accesos remots donant accès d'entrada, el que pot resultar no molt segur.

Te dues opcions de compra, Professional i Enterprise, limitada o sense limitacions segons el cas. No disposa d'una versió gratuita, però si una demo de 30 dies amb totes les funcionalitats disponibles.

1

zenoss Own IT.



1

OP5

OP5 és un sistema de monitoratge basat en Nagios. És una solució flexible i altament escalable que pot monitoritzar qualsevol entorn, tan híbrid com serveis de cloud.

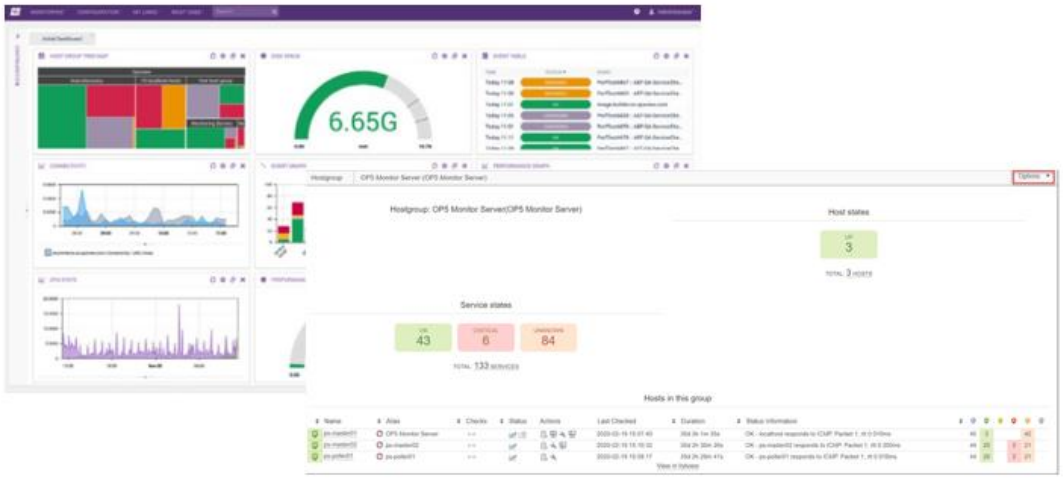
A diferencia de Nagios, OP5 disposa de les seves pròpies configuracions i plugins, recolçats per la seva propia comunitat de desenvolupadors, encara que pot aprofitar-se de les innovacions de la comunitat Nagios, així com fa servir algunes de les seves utilitats.

Com altres eines de monitoratge, es totalment configurable, però en aquest cas la configuració és basa en la simplicitat i busca que qualsevol usuari sense nocions expertes en la matèria hi pugui treballar.

Una propietat particular d'aquesta eina es el seu component d'autodiscover que escaneja la xarxa en busca d'elements a monitoritzar.

1

OP5



1

centreon

Centreon és una plataforma de monitoratge oberta, flexible i totalment escalable que permet diferents estructures de configuracions, com ara un grup de servidors remots i pollers o un servidor centralitzat, depenent de la càrrega que volguem monitoritzar.

A més de disposar d'una interficie visual de fàcil ús, és extremadament configurable i molt intuitiva. Permet la supervisió de xarxes hibrides, local i cloud, i monitoratge end2end.

Obviament la versió de pagament és molt més limitada que la resta, ja que no te moltes de les funcionalitats que s'han desenvolupat per Centreon, però es una versió totalment funcional i vàlida per un monitoratge complet.

Com aspecte destacable es pot comentar la gran versatilitat de l'eïna per a realitzar informes i panells de control.

1

centreon

1

Nagios®

Nagios és una de les eines més estables i consolidades del mercat, probablement el que més s'ha fet i s'està fent servir. Es tracta d'una solució versàtil, altament escalable i capaç del monitoratge de grans infraestructures amb un consum molt baix basada en la metodología de hosts i serveis.

La principal avantatge de Nagios és la flexibilitat que ofereix ja que es pot configurar i desenvolupar qualsevol eina o plugin que es necessiti.

La comunitat Nagios és molt ample i cada vegada hi ha més utilitats i aplicacions que integren o es poden arribar a integrar amb aquesta solució. Hi ha versions per organitzacions, amb suport i amb més funcionalitats, de pagament, però es possible disposar de l'aplicació totalment funcional de manera gratuita amb la versió anomenada Nagios Core.

Una característica interesant es la seva versatilitat per mostrar els informes i grafics, ja que es pot integrar amb Pnp4nagios, Graphana...

1

Nagios®

1

Prometheus

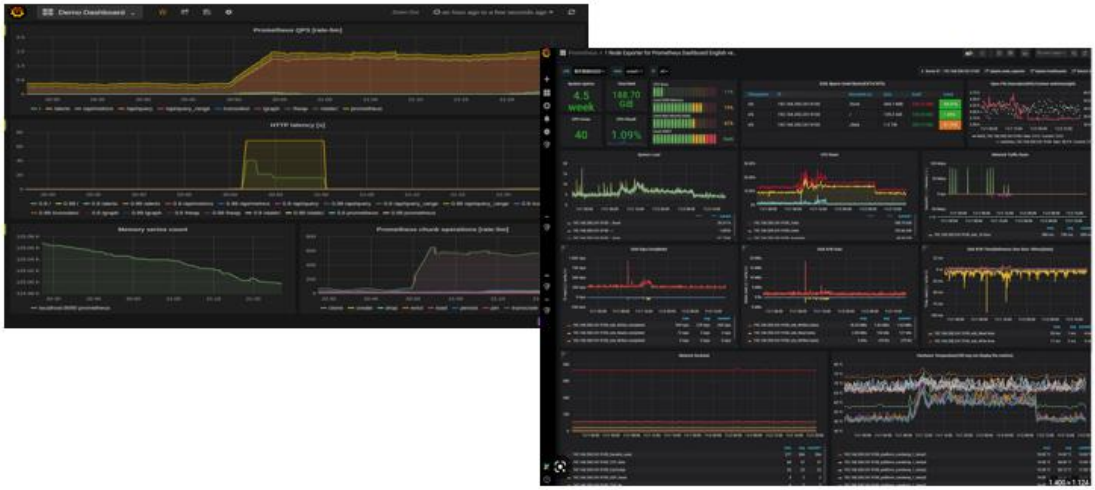
Prometheus és una plataforma de monitoratge relativament nova, porta uns 10 anys al mercat, pero ja s'ha fet un lloc important, gràcies a la seva flexibilitat i el seu alt rendiment.

Es tracta d'un model de dades multidimensional i de dades en series temporals. Fa servir PromQL, un llenguatge de consulta altament eficient que permet la consulta de les series temporals seguint un model d'extracció HTTP.

Els servidors i dispositius es poden descobrir o configurant-los de manera tradicional. A més una avantatge és poder disposar de diferents models de suport de gràfics (graphana, graphite...) característica que comparteix amb Nagios.

1

Prometheus

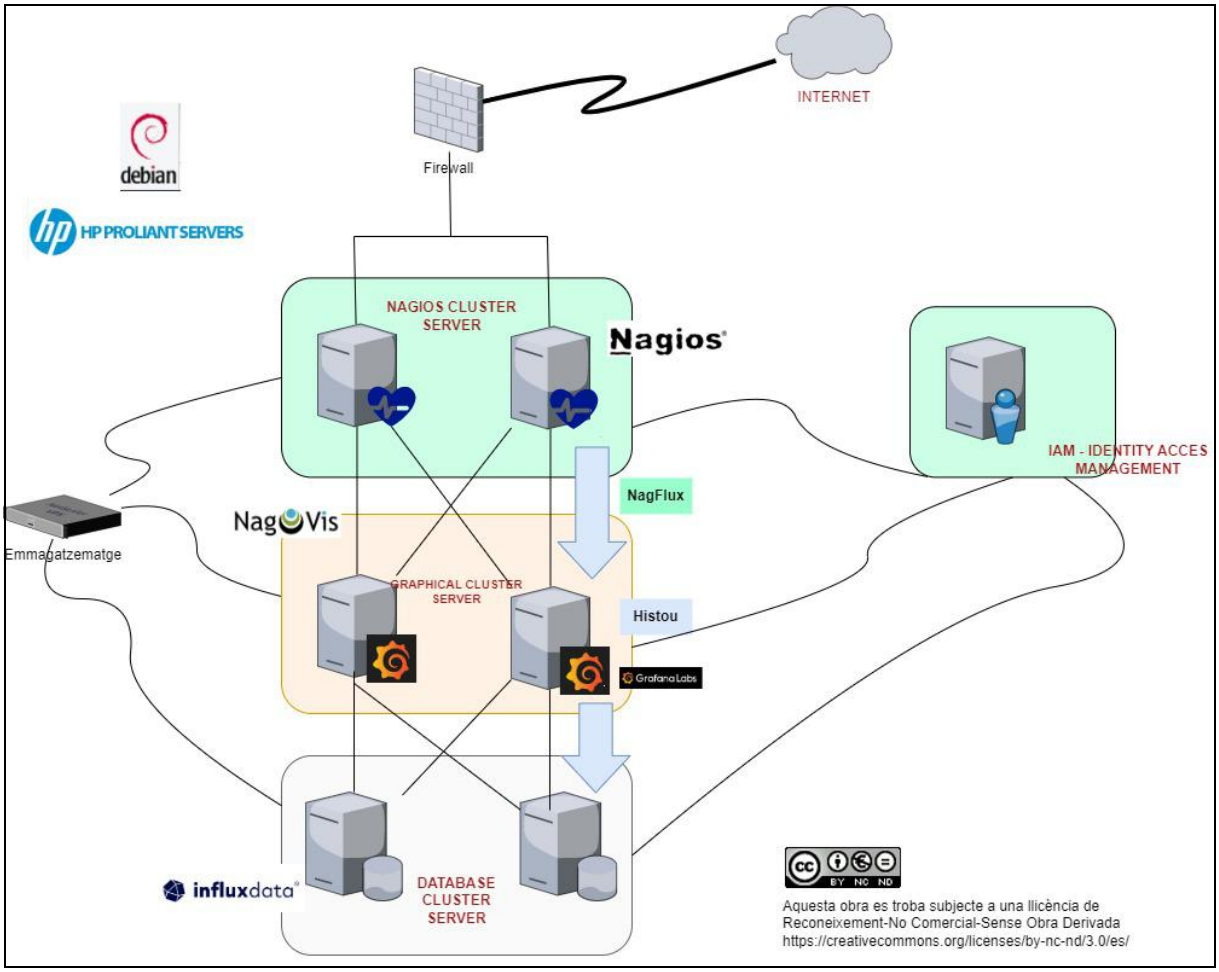


1

GRÀCIES!

1

Annex II. Esquema Lògic Solució Proposada



Annex III. Política de Monitoratge

Política de Monitoratge

Miguel Sánchez Martín

Grau d'Enginyeria Informàtica

Área: GNU/Linux

14/04/2023

Aquesta obra es troba subjecte a una llicència de
Reconeixement-No Comercial-Sense Obra Derivada
https://creativecommons.org/licenses/by-nc-nd/3.0/es/

Índex

1. Objectius

L'objectiu principal del monitoratge d'un sistema informàtic és supervisar, mantenir confiable i assegurar la operativitat del mateix. L'objectiu de definir aquesta política és assegurar que el sistema es manté fiable i proporciona els serveis adequadament.

2. Àmbit

Aquesta política de monitoratge aplica a tots els sistemes informàtics de l'organització Mediadors i Assegurances S.A. Entre ells els servidors i dispositius de comunicacions i emmagatzematge.

3. Responsabilitats

Els responsable primer del monitoratge serà l'equip de direcció, en concret el Gerent del departament SI/TI, encarregat de la gestió d'operacions i de mantenir alineats els objectius de negoci i els objectius de TI.

El responsable de mantenir la configuració i operació del monitoratge serà el departament de SI/TI, en concret l'equip d'Operacions. Aquests negociaran amb els gerents i caps de projecte els corresponents elements i llindars de monitorització, processos i paràmetres, seguint els definits en aquesta política.

Els responsables d'establir els llindars que operacions haurà de configurar són els IT Owner / App Owner de cada aplicació, i en el cas de projectes, el Project Manager, i en el seu defecte el Gerent de SI/TI.

Així també seràn aquests responsables els que hauran de determinar quin serà l'horari de servei i l'horari de monitoratge dels servidors de cada aplicació, així com les finestres de manteniment on no es monitoritzarà els sistemes o no s'enviaran notificacions. Si per exemple, fos necessària una finestra de manteniment per reiniciar els servidors o per realitzar les còpies de seguretat.

Tota aquesta informació haurà de restar al document de cada aplicació, que es troba al SharePoint de SI/TI i s'afegirà un apartat de Monitoratge per tal que constin aquests paràmetres i configuracions i serà responsabilitat dels IT Owner / App Owner / PM assegurar que aquesta informació hi consti.

Quan es presenti un nou projecte, els responsables del pas a Explotació / Producció, hauran d'afegir també un apartat de Monitoratge per controlar que durant el projecte s'hagi preparat el monitoratge de servidors i aplicacions durant la fase de Projecte.

4. Definició dels elements a monitoritzar

Es definirà per a cada tecnologia una plantilla on es determinaran els elements a monitoritzar i els llindars per defecte a configurar. S'haurà de disposar d'un document per a cada element i la seva configuració, que podrà fer-se servir també en les peticions, per a donar d'alta o baixa l'element del monitoratge actiu.

Es definiran equips o llistes de distribució per a que rebin tant les alertes dels elements monitoritzats, com les notificacions al respecte de la configuració o incidències que es puguin produir. Aquestes notificacions es rebran principalment via e-mail, i en cas que sigui possible, amb missatges SMS.

A més de les alertes, s'haurà de reflexar l'estat del sistema en un panell de control que sigui accessible des de l'organització, via web, i on es mostrarà entre d'altres, l'estat de CPU, RAM, Discos i I/O de tots els servidors i l'estat de disponibilitat de tots els dispositius.

L'aplicació o sistema de monitoratge haurà de mantenir un històric d'almenys 6 mesos, des del moment que es pren la informació. Aquesta informació s'haurà d'emmagatzemar en els propis sistemes de l'organització.

5. Privacitat

Els accessos a l'aplicació de monitoratge haurà d'estar restringida i controlada, i ningú sense autorització podrà veure ni molt menys modificar les dades i configuracions de l'eina.

Els sistemes hauran de protegir les dades i la informació d'accessos no autoritzats i salvant aquells casos que es requereixi facilitar aquesta informació a proveïdors o tercers, hauran de romandre amb accés privilegiat. Les peticions de facilitar aquestes dades a tercers s'haurà de fer sota l'autorització de la Direcció i fent servir canals de comunicació segurs.

Annex IV. Guia Instal·lació Programari

Guia d'instal·lació i configuració d'aplicacions de monitoratge

Miguel Sánchez Martín
Data: 28.04.2023

Versió: v1

Aquesta obra es troba subjecte a una llicència de
Reconeixement-No Comercial-Sense Obra Derivada
https://creativecommons.org/licenses/by-nc-nd/3.0/es/

Índex

1. Introducció.

En aquest document es preten reflexar el procés d'instal·lació i configuració, pas a pas, de les eines de monitoratge del nostre sistema. El monitoratge és una funció essencial per a garantir que els sistemes funcionin correctament i per a detectar possibles anomalies.

Aquest document es dirigeix a administradors i personal tècnic. L'eina principal que s'instal·larà es Nagios Core, una eina de monitoratge de servidors i dispositius. L'instal·lació es realitza sobre un sistema operatiu Debian 10.13.

Trobarem en aquest document els següents apartats:

- Instal·lació dels pre-requisits i aplicacions de suport
- Instal·lació de Nagios Core
- Instal·lació de Nagios Plugins
- Configuració de Nagios
- Configuració de clúster
- Instal·lació d'InfluxDB
- Instal·lació de Nagflux
- Instal·lació de Grafana
- Instal·lació de Nagvis
- Instal·lació d'Histou

2. Instal·lació dels pre-requisits i aplicacions de suport

Es comença la instal·lació preparant les utilitats de suport. Com a recomanació per a la instal·lació de Nagios Core s'indica que es realitzi sobre una instal·lació neta, sense altres productes. Així que tan sols s'instal·len les utilitats i el servidor web apache2:

Es comença instal·lant el software apache2:

#apt-get update

#apt-get install apache2

```
root@SERLA099334:/etc/apt# apt-get update
Hit:1 http://security.debian.org/debian-security buster/updates InRelease
Reading package lists... Done
root@SERLA099334:/etc/apt# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 659 kB of archives.
After this operation, 1,983 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /l
ib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.
service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for man-db (2.8.5-2) ...
Processing triggers for systemd (241-7~deb10u9) ...
root@SERLA099334:/etc/apt#
```

Instal·lem ara PHP:

#apt-get update

#apt-get install php

```
root@SERLA099334:/etc/apt# apt-get install php
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libc-dev-bin linux-libc-dev
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  binutils binutils-common binutils-i686-linux-gnu cpp cpp-10 gcc gcc-10
  gcc-10-base libapache2-mod-php7.4 libasan6 libatomic1 libbinutils libc-bin
  libc-dev-bin libc-l10n libc6 libcc1-0 libcrypt1 libctf-nobfd0 libctf0
  libffi7 libgcc-10-dev libgcc-s1 libgomp1 libisl23 libitm1 libnsl2 libnss-nis
  libnss-nisplus libquadmath0 libstdc++6 libtirpc-common libtirpc3 libubsan1
  locales manpages manpages-dev php-common php7.4 php7.4-cli php7.4-common
  php7.4-json php7.4-opcache php7.4-readline
Suggested packages:
  binutils-doc cpp-doc gcc-10-locales gcc-multilib autoconf automake libtool
  flex bison gdb gcc-doc gcc-10-multilib gcc-10-doc php-pear glibc-doc
Recommended packages:
  libc6-dev | libc-dev libc6-dev libc-devtools
The following packages will be REMOVED:
  build-essential g++ g++-8 libc6-dev libstdc++-8-dev
The following NEW packages will be installed:
  cpp-10 gcc-10 gcc-10-base libapache2-mod-php7.4 libasan6 libcrypt1
  libctf-nobfd0 libctf0 libffi7 libgcc-10-dev libgcc-s1 libisl23 libnsl2
  libnss-nis libnss-nisplus libtirpc-common libtirpc3 php php-common php7.4
  php7.4-cli php7.4-common php7.4-json php7.4-opcache php7.4-readline
The following packages will be upgraded:
```

```
Creating config file /etc/php/7.4/mods-available/json.ini with new version
Setting up php7.4-cli (7.4.33-1+deb11u3) ...
update-alternatives: using /usr/bin/php7.4 to provide /usr/bin/php (php) in auto mode
update-alternatives: using /usr/bin/phar7.4 to provide /usr/bin/phar (phar) in auto mod
e
update-alternatives: using /usr/bin/phar.phar7.4 to provide /usr/bin/phar.phar (phar.ph
ar) in auto mode

Creating config file /etc/php/7.4/cli/php.ini with new version
Setting up libnss-nisplus:i386 (1.3-4) ...
Setting up gcc (4:10.2.1-1) ...
Setting up libnss-nis:i386 (3.1-4) ...
Setting up libapache2-mod-php7.4 (7.4.33-1+deb11u3) ...

Creating config file /etc/php/7.4/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php7.4
Setting up php7.4 (7.4.33-1+deb11u3) ...
Setting up php (2:7.4+76) ...
Processing triggers for man-db (2.8.5-2) ...
Processing triggers for libc-bin (2.31-13+deb11u6) ...
Processing triggers for php7.4-cli (7.4.33-1+deb11u3) ...
Processing triggers for libapache2-mod-php7.4 (7.4.33-1+deb11u3) ...
```

Instal·lem la connexió remota SSH:

#apt-get install ssh

```
root@SERLA099334:/etc/apt# apt-get install ssh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libc-dev-bin linux-libc-dev
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libcbor0 libfido2-1 libselinux1 openssh-client openssh-server openssh-sftp-server
  runit-helper
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard ufw
The following NEW packages will be installed:
  libcbor0 libfido2-1 openssh-server openssh-sftp-server runit-helper ssh
The following packages will be upgraded:
  libselinux1 openssh-client
2 upgraded, 6 newly installed, 0 to remove and 1350 not upgraded.
Need to get 1,911 kB of archives.
After this operation, 3,415 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Finalment instal·lem la resta d'aplicacions i utilitats:

#apt-get install gcc wget make dnsutils smbclient pacemaker corosync curl libssl-dev rsync ntp

```
root@SERLA099334:/etc/apt# apt-get install gcc unzip wget make gcc dnsutils smbclient q
stat fping ufw pacemaker corosync curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Realitzarem aquestes comandes en els servidors corresponents.

3. Instal·lació de Nagios Core

Abans d'instalar Nagios, hem de crear els usuaris necessaris i afegir els grups corresponents. Com en aquesta instal·lació tindrem diferents entorns, hem de fer diferents identificacions per a cada instancia Nagios:

#useradd [usuari] -d [home]

#usermod -G www-data,[group] www-data
#passwd [usuari]

```
root@SERLA099334:~# useradd -d /usr/local/nagiosPro nagios_pro
root@SERLA099334:~# useradd -d /usr/local/nagiosUat nagios_uat
root@SERLA099334:~# useradd -d /usr/local/nagiosDev nagios_dev
root@SERLA099334:~# useradd -d /usr/local/nagiosInt nagios_int
```

```
root@SERLA099334:/etc/apt# usermod -G www-data,nagios_pro,nagios_uat,nagios_dev,nagios_
int www-data
```

```
root@SERLA099334:~# passwd nagios_pro
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
```

#groupadd nagcmd
#usermod -G nagcmd nagios_pro
#usermod -G nagcmd nagios_uat
#usermod -G nagcmd nagios_dev
#usermod -G nagcmd nagios_int

Instal·lem ara Nagios Core:

Descarreguem l'última versió de la pagina de descarrega:
https://www.nagios.org/downloads/nagios-core/

En aquest cas,l'última versió disponible es la 4.4.11:

Nagios Core

Latest Version 4 Releases

Version	Date	Notes	Type	Link
4.4.11	2023-04-14	Latest stable release	Source code	nagios-4.4.11.tar.gz
4.3.4	2017-08-24	Previous stable release	Source code	nagios-4.3.4.tar.gz

Una vegada descarregat, descomprimim el fitxer:

#tar xvzf nagios-4.4.11.tar.gz

```
root@SERLA099334:/Software# tar xvzf nagios-4.4.11.tar.gz
nagios-4.4.11/
nagios-4.4.11/.gitignore
nagios-4.4.11/.travis.yml
nagios-4.4.11/CONTRIBUTING.md
nagios-4.4.11/Changelog
nagios-4.4.11/INSTALLING
nagios-4.4.11/LEGAL
nagios-4.4.11/LICENSE
nagios-4.4.11/Makefile.in
nagios-4.4.11/README.md
nagios-4.4.11/THANKS
nagios-4.4.11/UPGRADING
```

Ja en el directori resultant, hem de configurar la instal·lació, com a exemple, fem servir l'entorn de Producció:

./configure --prefix=/usr/local/nagiosPro --with-cgiurl=/nagiosPro/cgi-bin --with-htmlurl=/nagiosPro/ --with-nagios-user=nagios_pro --with-nagios-group=nagios_pro --with-command-group=nagcmd

```
General Options:
-------------------------
        Nagios executable:  nagios
        Nagios user/group:  nagios_pro,nagios_pro
       Command user/group:  nagios_pro,nagcmd
            Event Broker:   yes
       Install ${prefix}:   /usr/local/nagiosPro
   Install ${includedir}:   /usr/local/nagiosPro/include/nagios
               Lock file:   /run/nagios.lock
  Check result directory:   /usr/local/nagiosPro/var/spool/checkresults
              Init directory:  /lib/systemd/system
 Apache conf.d directory:   /etc/apache2/sites-available
             Mail program:  /bin/mail
                  Host OS:  linux-gnu
          IOBroker Method:  epoll

Web Interface Options:
------------------------
                HTML URL:  http://localhost/nagios/
                 CGI URL:  http://localhost/nagiosPro/cgi-bin/
Traceroute (used by WAP):  /usr/sbin/traceroute
```

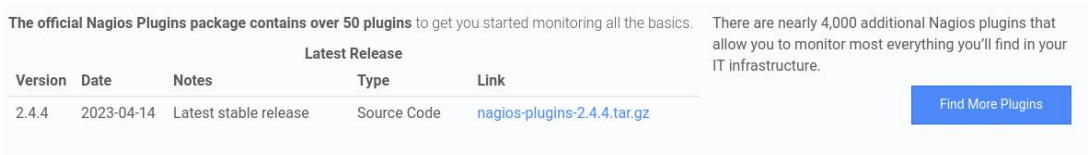
make all
make install
make install-init
make install-commandmode
make install-config
make install-daemoninit

Realitzarem les mateixes comandes per a la resta d'entorns i en tots els servidors corresponents.

4. Instal·lació de Nagios Plugins

Com hem vist anteriorment els plugins de Nagios també es poden descarregar de la mateixa pagina web de Nagios.

https://www.nagios.org/downloads/nagios-plugins



Una vegada descarregats, descomprimim el paquet

#tar xvzf nagios-plugins-2.4.4.tar.gz

```
root@SERLA099334:/Software# tar xvzf nagios-plugins-2.4.4.tar.gz
nagios-plugins-2.4.4/
nagios-plugins-2.4.4/build-aux/
nagios-plugins-2.4.4/build-aux/compile
nagios-plugins-2.4.4/build-aux/config.guess
nagios-plugins-2.4.4/build-aux/config.rpath
nagios-plugins-2.4.4/build-aux/config.sub
nagios-plugins-2.4.4/build-aux/install-sh
nagios-plugins-2.4.4/build-aux/ltmain.sh
nagios-plugins-2.4.4/build-aux/missing
nagios-plugins-2.4.4/build-aux/mkinstalldirs
nagios-plugins-2.4.4/build-aux/depcomp
nagios-plugins-2.4.4/build-aux/snippet/
nagios-plugins-2.4.4/build-aux/snippet/_Noreturn.h
```

Accedim al directori i executem les següents comandes:

#./configure --with-nagios-group=nagcmd
#make
#make install

```
eport bugs to the package provider.
oot@SERLA099334:/Software/nagios-plugins-2.4.4# ./configure --with-nagios-group=nagcmd
hecking for a BSD-compatible install... /usr/bin/install -c
hecking whether build environment is sane... yes
hecking for a thread-safe mkdir -p... /usr/bin/mkdir -p
hecking for gawk... gawk
hecking whether make sets $(MAKE)... yes
hecking whether make supports nested variables... yes
hecking whether to enable maintainer-specific portions of Makefiles... yes
hecking build system type... x86_64-pc-linux-gnu
hecking host system type... x86_64-pc-linux-gnu
hecking for gcc... gcc
hecking whether the C compiler works... yes
```

Ja tenim els plugins instal·lats. Aquestes comandes s'han de fer a cada servidor on vulguem instal·lar Nagios. Com els plugins són els mateixos para tots els entorns, farem tan sols una instal·lació per servidor.

Una modificació que haurem de realitzar en el fitxer de configuració de cada instancia Nagios, és modificar la ruta dels plugins després de la instal·lació ja que apuntarà a la pròpia instància i ens interessa que tots el plugins siguin comuns:

```
# Sets $USER1$ to be the path to the plugins
$USER1$=/usr/local/nagiosPro/libexec
```

S'ha de substituir per:
$USER1$=/usr/local/nagios/libexec

5. Autenticació de Nagios

La configuració del accès web a Nagios es realitza a traves del servidor web per a cada entorn i a més hem d'incloure la configuració de MFA.

Seguint les instruccions de https://github.com/itemir/apache_2fa

git clone https://github.com/itemir/apache_2fa

```
# cd apache_2fa
# apt-get install onetimepass
```

A continuació, hem de crear un directori per guardar els estats:

```
#mkdir /etc/apache2/state
```

La configuració per exemple, de l'entorn de Producció on tan sols hauríem de canviar amb les variables corresponents el nom del server Radius i la clau privada per a cada virtual host:

```
<VirtualHost *:8080>
    DocumentRoot /usr/local/nagiosPro/share
    ScriptAlias /nagios/cgi-bin /usr/local/nagiosPro/sbin
     AddRadiusAuth [servernameRadius]:1812 [sharedsecret] 5
    AddRadiusCookieValid 60

    RewriteEngine On

    RewriteCond %{REQUEST_URI} !^/auth/
    RewriteCond %{HTTP_COOKIE} !^.*2FA_Auth=([a-zA-Z0-9]+)
    RewriteRule ^(.*)$ /auth/auth?$1?%{QUERY_STRING} [L,R=302]

    RewriteCond %{REQUEST_URI} !^/auth/
    RewriteCond %{HTTP_COOKIE} ^.*2FA_Auth=([a-zA-Z0-9]+)
    RewriteCond /etc/apache2/state/%1 !-f
    RewriteRule ^(.*)$ /auth/auth?$1?%{QUERY_STRING} [L,R=302]

    ScriptAlias /auth/ /etc/apache2/state/

    <Directory /etc/apache2/state/>>
       AuthType Digest
       AuthName "yourdomain.com"
       AuthDigestDomain /
       AuthDigestProvider file
       /etc/apache2/state/apache_credentials
       Require valid-user
    </Directory>

    ScriptAlias /nagiosPro/cgi-bin /usr/local/nagiosPro/sbin

    <Directory /usr/local/nagiosPro/sbin>
       AuthType Digest
       AuthName "crs.com"
       AuthDigestDomain /
```

```
        AuthDigestProvider file
        AuthUserFile /etc/apache2/state/apache_credentials
        Require valid-user
    </Directory>

    Alias /nagiosPro /usr/local/nagiosPro/share
    <Directory "/usr/local/nagiosPro/share">
        Options None
        AuthName "Web-Based Radius Authentication"
        AuthBasicProvider "radius"
        AuthRadiusAuthoritative on
        AuthRadiusCookieValid 1
        AuthRadiusActive On
        Require valid-user
    </Directory>
</VirtualHost>
```

Hi haurà una configuració similar per la resta d'entorns, UAT, INT i DEV, canviant les corresponents configuracions. Els virtualHosts podrien ser:

*.:8080: Producció
*.:8081: Pre-Producció
*.:8082: Integració
*.:8083: Desenvolupament

Per crear els usuaris es pot fer servir la comanda:

```
# htdigest apache_credentials yourdomain.com <new_user>
```

També es pot lligar la validació dels usuaris a un directori LDAP o Active Directory mitjançant el mòdul mod_authnz_ldap i les següents instruccions:

```
AuthName "Acces ldap"
AuthBasicProvider ldap
AuthType Basic
AuthzLDAPAuthoritative on
AuthLDAPBindDN "CN=consultas,CN=Users,DC=cms,DC=com"
AuthLDAPBindPassword password
AuthLDAPURL
"ldap://dcserver.cms.com/CN=Users,DC=cms,DC=com?sAMAccountName?sub?(objectClass=
*)"
require ldap-group CN=Nagios_users,CN=Users,DC=cms,DC=com
AuthLDAPGroupAttributeIsDN on
```

Una vegada configurat, s'ha de reiniciar el servei apache i nagios amb les comandes:

#systemctl restart apache2
#systemctl restart nagiosPro (o els entorns que s'hagin configurat)

6. Configuració de Nagios

La configuració d'objectes de Nagios es complexa, però a la vegada és molt intuitiva. Els objectes a Nagios són cadascun dels hosts, contactes, comandes, es a dir, tot en Nagios és un objecte.

Hi ha una serie de fitxers en els que indiquem els objectes que el sistema farà servir. Aquests fitxers es relacionen en la configuració inicial del core del producte. Veiem a continuació com seria:

El fitxer principal de configuració es troba a "/usr/local/nagios/etc/nagios.cfg", en la nostra instal·lació "/usr/local/nagios[Entorn]/etc/nagios.cfg"

Aquí podem trobar la configuració d'exemple:

```
# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

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

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

# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagiosPro/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagiosPro/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagiosPro/etc/objects/printer.cfg
```

Nosaltres podem definir tants fitxers de configuració com vulguem. Cada estructura d'objecte té unes característiques i uns paràmetres que es poden modificar. Hi ha paràmetres comuns a tots i alguns específics per a cada tipus d'objecte. No entrarem en detall a cada especificació ja que no es l'objectiu d'aquest document i a més la documentació de Nagios es prou clara i extensa per a servir com a referència:

https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/objectdefinitions.html

A efectes pràctics podríem tenir tota la configuració en el mateix fitxer, però per tal de mantenir una lògica i un ordre, farem les següents separacions:

- commands.cfg : Definició de comandes i scripts que s'executen

- timeperiods.cfg: Definició de les diferents planificacions que podem tenir a Nagios.

- contacts.cfg: Definició dels contactes a qui pot arribar e-mail, sms o altres tipus de notificacions.

- templates.cfg: Definició de les plantilles necessàries. A Nagios podem disposar de plantilles per tal de no repetir comandes o estructures. És molt important aquest apartat per no fer feina de més.

- devices.cfg : Definició dels dispositius com impressores o apliances que no son estrictament de comunicacions.

- windows.cfg : Definició dels servidors windows. Aqui podem fer, segons la mida del maquinari, separació entre servidors virtuals i fisics, o també separacions geogràfiques. En el nostre cas no hi ha massa servidors.

- hostgroups.cfg: Definició dels grups de hosts que es poden definir, poden ser hosts de diferents sistemes que formin un servei o projecte, o bé agrupar per tecnologies, per exemple tots aquells hosts que donen servei de IIS Server, i mostrar les seves mètriques agrupades.

- linux.cfg : Igual que els servidors Windows, definició dels servidors amb sistema operatiu Linux / AIX.

- comms.cfg: Definició dels dispositius de comunicació, com routers, switches o firewalls.

- services_XXXX.cfg: Definició dels monitors o tests que es realitzaran a cada host. Els serveis es poden definir per un host, per molts o per hostgroups. En aquest cas tindrem una definició per tecnologia, per exemple, services_IIS, services_SAP, services_CPU, services_Disk, services_RAM, services_SQLServer. Aquesta agrupació ajuda a modificar i tenir controlats els diferents aspectes d'un host i modificar els mínims fitxers possibles.

- servicegroups.cfg: Igual que els hosts, els serveis es poden agrupar de manera que tinguem tots els serveis que controlen la CPU o el disc i mostrar les seves mètriques com grup.

7. Configuració de clúster

En molts dels components que s'implementen en aquesta estructura hi ha un component de clúster, configurant així una alta disponibilitat.

Per a configurar aquesta alta disponibilitat, farem servir les eines Pacemaker i Corosync.

```
#apt-get install pacemaker corosync
```

Creem la clau d'autenticació en el node1 i el copiarem al node2:

```
#corosync-keygen
node1#scp /etc/corosync/authkey node2:/etc/corosync/authkey
node2#chmod 400 /etc/corosync/authkey
```

En el fitxer /etc/corosync/corosync.conf afegirem la interficie que es farà servir per la comunicació:

```
bindnetaddr:    10.0.0.0
```

S'ha d'establir que el corosync cridi a pacemaker. Això es fa amb el fitxer de configuració /etc/corosync/service.d/pcmk

```
service{
    name :    pacemaker
    ver :     0
}
```

A més s'ha d'iniciar quan s'inicia el sistema. En el fitxer de configuració /etc/default/corosync

```
#start corosync at boot [yes/no]

START=yes
```

Aquestes configuracions s'hauran de realitzar a cada node. Una vegada realitzades, podem llençar la comanda a tot dos nodes :

```
#/etc/init.d/corosync start
```

Es recomanable configurar les següents propietats del crm (Cluster Resource Manager), la utilitat de gestió i configuració del cluster de Pacemaker:

Per a que els nodes no s'aturin entre ells:

```
#crm configure property stonith-enabled= false
```

I com, en principi disposem tan sols de dos nodes, podem ignorar les decisions preses a tots els nodes:

```
#crm configure property no-quorum-policy=ignore
```

Farem servir aquesta propietat per definir que el recurs sempre s'intenti aixecar en el mateix node:

#crm configure rsc_defaults resource-stickiness=1000

I a continuació configurem el recurs. En aquest cas afegim un recurs a la ip 10.0.0.11, que serà la que haurem de configurar en el recurs Nagios, per exemple. Aquesta seria la ip virtual a la que es configuraria, per exemple, el servidor apache.

#crm configure primitive FAILOVER-ADDR ocf:heartbeat:IPaddr2 params ip="10.0.0.11" nic="eth0" op monitor interval="10s" meta is-managed="true"

Si consultem el recurs una vegada configurat:

```
============
Last updated: Sun Mar  4 09:29:58 2012
Stack: openais
Current DC: node1 - partition WITHOUT quorum
Version: 1.0.9-74392a28b7f31d7ddc86689598bd23114f58978b
2 Nodes configured, 2 expected votes
1 Resources configured.
============

Online: [ node1 ]
OFFLINE: [ node2 ]

FAILOVER-ADDR   (ocf::heartbeat:IPaddr2):       Started node1
```

Per a cada recurs s'hauria de configurar una ip virtual. En el cas de Nagios, com la configuració és propia de cada servidor, s'haurà d'incorporar un script que faci la còpia de recursos del node1 al node2 i viceversa:

Configurem en el cron de l'usuari "nagios-[entorn]" de cada node les següents comandes cada minut:

```
* * * * * /home/nagios-[ENV]/bin/sync-nagios-[entorn].sh
```

Recordem que caldrà un script per a cada entorn.

El contingut de l'executable serà similar a aquest:

```
#! /bin/sh
rsync -av /usr/local/nagios-[entorn]/conf.d/ nagios@node2:/usr/local/nagios-
[entorn]/conf.d/
rsync -av /usr/local/nagios-[entorn]/nagios.cfg nagios@node2:/usr/local/nagios-
```

[entorn]/nagios.cfg
rsync -av /usr/local/nagios-[entorn]/resources.cfg nagios@node2:/usr/local/nagios-[entorn]/resources.cfg
rsync -av /usr/local/nagios-[entorn]/etc/objects/ nagios@node2:/usr/local/nagios-[entorn]/etc/objects/

8. Instal·lació de InfluxDB

Per instal·lar InfluxDB tan sols hem de realitzar la comanda:

#apt-get install influxdb

```
root@SERLA099334:~# apt-get install influxdb
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  influxdb
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 5.091 kB de archivos.
Se utilizarán 19,1 MB de espacio de disco adicional después de esta operación.
Des:1 http://security.debian.org/debian-security buster/updates/main amd64 infl
uxdb amd64 1.6.4-1+deb10u1 [5.091 kB]
Descargados 5.091 kB en 1s (6.908 kB/s)
Seleccionando el paquete influxdb previamente no seleccionado.
(Leyendo la base de datos ... 147993 ficheros o directorios instalados actualme
nte.)
Preparando para desempaquetar .../influxdb_1.6.4-1+deb10u1_amd64.deb ...
```

#systemctl start influxdb

Ara bé, per tal de disposar d'alta disponibilitat sense instal·lar versions comercials de Influxdb, seguirem les instruccions d'una alternativa Open Source. Segueix la mateixa filosofia que l'opció comercial, fent servir dos tipus de processos, metadades i dades:

https://github.com/chengshiwen/influxdb-cluster

Per instal·lació de metadata servers:
https://docs.influxdata.com/enterprise_influxdb/v1.8/install-and-deploy/production_installation/meta_node_installation/

Per instal·lació de data servers:
https://docs.influxdata.com/enterprise_influxdb/v1.8/install-and-deploy/production_installation/data_node_installation/

S'ha de tenir en compte que InfluxDB fa servir NTP per a fer els registres de temps, és important doncs que aquest servei estigui ben configurat en els servidors, tant, en el servidors d'InfluxDB com en la resta de servidors amb els que tingui connexió.

9. Instal·lació de Nagflux

Per integrar Nagios amb InfluxDB requerim d'un connector que faci la traducció de les dades. Aquest connector es Nagflux. Com tenim quatre entorns, necessitarem 4 dimonis de Nagflux per enviar les dades a InfluxDB.

Per instal·lar farem servir les comandes google i per tant, hem d'instal·lar els paquets i dependències necessaris:

```
#apt-get install -y golang golang-github-influxdb-usage-client-dev git
```

A continuació compilem i instal·lem Nagflux en llenguatge Google.

```
#cd /Software/goRepo
#go get -u github.com/griesbacher/nagflux
#go build github.com/griesbacher/nagflux
```

I a continuació crearem un servei Nagflux per a cada entorn.

```
#mkdir -p /usr/local/nagios[entorn]/var/spool/nagfluxperfdata
#mkdir -p /usr/local/nagios[entorn]/var/nagflux

cp /Software/goRepo/src/github.com/griesbacher/nagflux/nagflux.service
/lib/systemd/system/nagflux[entorn].service
```

Editem cada servei de la següent manera:

```
[Unit]
Description=A connector which transforms performancedata from
   Nagios/Icinga(2)/Naemon to InfluxDB/Elasticsearch
Documentation=https://github.com/Griesbacher/nagflux
After=network-online.target

[Service]
User=root
Group=root
ExecStart=/opt/nagflux/nagflux -configPath
   /usr/local/nagios[entorn]/nagflux/config.gcfg
Restart=on-failure

[Install]
WantedBy=multi-user.target
Alias=nagflux[entorn].service
```

```
#chmod +x /lib/systemd/system/nagflux[entorn].service
```

```
#systemctl daemon reload
#systemctl enable nagflux[entorn].service
```

D'aquesta manera tindrem 4 serveis Nagflux, un per cada entorn, i amb un fitxer de configuració diferent.

Aquesta configuració s'haurà de crear en el path:
/usr/local/nagios[entorn]/nagflux/config.gcfg

I haurà de tenir aquest format:

```
[main]
  NagiosSpoolfileFolder = "/usr/local/nagios[entorn]/var/spool/nagfluxperfdata"
  NagiosSpoolfileWorker = 1
  InfluxWorker = 2
  MaxInfluxWorker = 5
  DumpFile = "nagflux.dump"
  NagfluxSpoolfileFolder = "/usr/local/nagios[entorn]/var/nagflux"
  FieldSeparator = "&"
  BufferSize = 10000
  FileBufferSize = 65536
  # If the performancedata does not have a certain target set with NAGFLUX:TARGET.
  # The following field will define the target for this data.
  # "all" sends the data to all Targets(every Influxdb, Elasticsearch...)
  # a certain name will direct the data to this certain target
  DefaultTarget = "all"

[Log]
  # leave empty for stdout
  LogFile = ""
  # List of Severities https://godoc.org/github.com/kdar/factorlog#Severity
  MinSeverity = "INFO"

[Livestatus]
  # tcp or file
  Type = "tcp"
  # tcp: 127.0.0.1:6557 or file /var/run/live
  #Address = "127.0.0.1:6557"
  # The amount to minutes to wait for livestatus to come up, if set to 0 the detection is
disabled
  MinutesToWait = 2
  # Set the Version of Livestatus. Allowed are Nagios, Icinga2, Naemon.
  # If left empty Nagflux will try to detect it on it's own, which will not always work.
  Version = "Nagios"
```

```
[InfluxDBGlobal]
   CreateDatabaseIfNotExists = true
   NastyString = ""
   NastyStringToReplace = ""
   HostcheckAlias = "hostcheck"
   ClientTimeout  = 5

[InfluxDB "nagflux[Entorn]"]
   Enabled = true
   Version = 1.0
   Address = "http://[server]:[port]"
   Arguments = "precision=ms&u=root&p=root&db=nagfluxDB[entorn]"
   StopPullingDataIfDown = true

[InfluxDB "fast"]
   Enabled = false
   Version = 1.0
   Address = "http://127.0.0.1:8086"
   Arguments = "precision=ms&u=root&p=root&db=fast"
   StopPullingDataIfDown = false
```

Quan iniciem el servei, i si tot es troba ben configurat, es generarà una base de dades a InfluxDB, amb el nom corresponent, en cas de producció, nagfluxDBPro

Es pot consultar si s'ha creat la base de dades amb aquesta comanda:

#curl -G "http://[server]:[port]/query?pretty=true" --data-urlencode "q=show databases"


```
{
    "results": [
        {
            "statement_id": 0,
            "series": [
                {
                    "name": "databases",
                    "columns": [
                        "name"
                    ],
                    "values": [
                        [
                            "_internal"
                        ],
                        [
                            "nagfluxDBPro"
                        ]
                    ]
                }
            ]
        }
    ]
}
```

A la configuració principal de nagios, /usr/local/nagios[entorn]/etc/nagios.cfg, haurem de modificar les següents línies:

```
process_performance_data=1

host_perfdata_file=/usr/local/nagios[entorn]/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$\tHOSTNAM
E::$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECKCOMMAND::$HOST
CHECKCOMMAND$
host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file-nagflux

service_perfdata_file=/usr/local/nagios[entorn]/var/service-perfdata
service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOST
NAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPER
FDATA$\tSERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-perfdata-file-nagflux
```

Haurem de definir ara les comandes a Nagios en el fitxer /usr/local/nagios[entorn]/etc/objects/commands.cfg

```
define command {
    command_name    process-host-perfdata-file-nagflux
    command_line    /bin/mv /usr/local/nagios[entorn]/var/host-perfdata
/usr/local/nagios[entorn]/var/spool/nagfluxperfdata/$TIMET$.perfdata.host
    }

define command {
    command_name    process-service-perfdata-file-nagflux
    command_line    /bin/mv /usr/local/nagios[entorn]/var/service-perfdata
/usr/local/nagios[entorn]/var/spool/nagfluxperfdata/$TIMET$.perfdata.service
    }
```

Comprovem la configuració i reiniciem, si tot es correcte:

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
#systemctl restart nagios.service
```

10. Instal·lació de Grafana

Grafana ens permetrà visualitzar les dades recollides amb Nagios.

Per tal de disposar de HA a Grafana, necessitarem que els dos servidors que component el cluster tinguin accès a una base de dades centralitzada MySQL.

Per tal d'instalar el servidor mySQL seguirem les següents instruccions:

```
#apt-get update
#apt-get install mysql-server -y

#mysql_secure_installation
```

Una vegada validats al servidor de base de dades, crearem una base de dades per Grafana i un usuari amb privilegis.

```
mysql> CREATE DATABASE grafana;

> CREATE USER 'grafana_user'@'%' IDENTIFIED BY 'grafana_user_password';
> GRANT ALL ON grafana.* TO 'grafana_user'@'%';
> FLUSH PRIVILEGES;
```

Seguint les instruccions del fabricant, realitzarem la instal·lació de Grafana:

```
#mkdir -p /Software/Grafana/
#apt-get install -y adduser libfontconfig1
#wget https://dl.grafana.com/enterprise/release/grafana-enterprise_9.5.1_amd64.deb
#dpkg -i grafana-enterprise_9.5.1_amd64.deb
```

A continuació, modificarem el fitxer de configuració /etc/grafana/grafana.ini per incloure la base de dades mysql centralitzada:

```
#example, root_url=https://grafana.unixcop.com
enable_gzip = true

[database] url =
   mysql://grafana_user:grafana_user_password@[database_ip]:[port]/grafana

[remote_cache]
type = database
```

També per afegir l'autenticació amb Google Authenticator, haurem de configurar aquest apartat al fitxer grafana.ini:

```
################################### Google Auth ############################
[auth.google]
;name = Google
;icon = google
;enabled = false
;allow_sign_up = true
;auto_login = false
;client_id = some_client_id
;client_secret = some_client_secret
;scopes = https://www.googleapis.com/auth/userinfo.profile
https://www.googleapis.com/auth/userinfo.email
;auth_url = https://accounts.google.com/o/oauth2/auth
;token_url = https://accounts.google.com/o/oauth2/token
;api_url = https://www.googleapis.com/oauth2/v1/userinfo
;allowed_domains =
;hosted_domain =
;skip_org_role_sync = false
```

Una vegada configurat, aixequem el server:

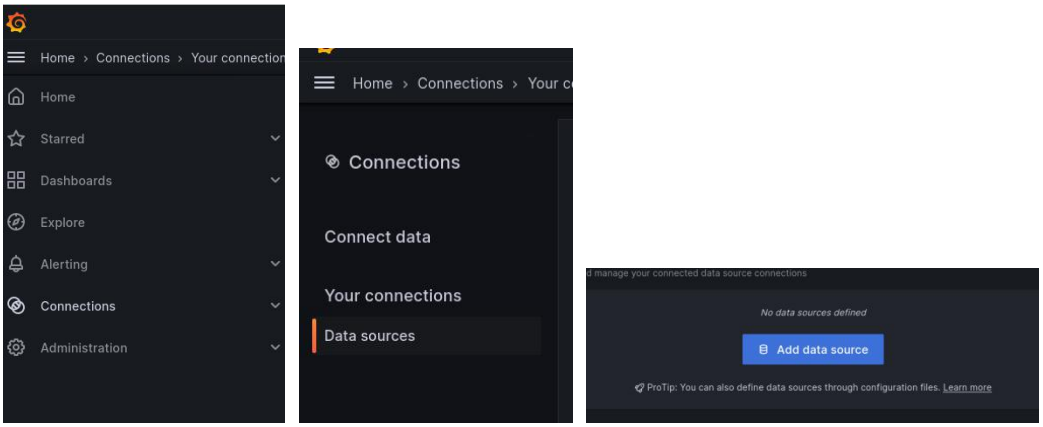
```
#systemctl start grafana-server
#systemctl enable grafana-server
```

Aquests pasos els haurem de repetir en els servers que formin part del cluster Grafana.

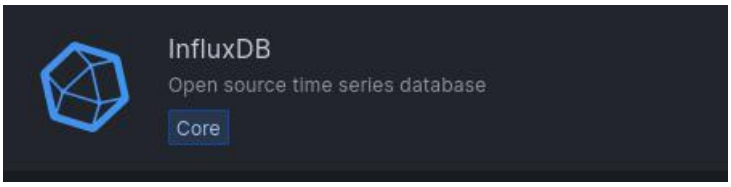
Una vegada instal·lat, farem servir la connexió per http per configurar els origens de dades. L'accès al servidor Grafana, s'haurà de realitzar mitjançant un balancejador.

A partir del menú inicial, seguiríem les següents instruccions:
https://grafana.com/docs/grafana/latest/datasources/influxdb/

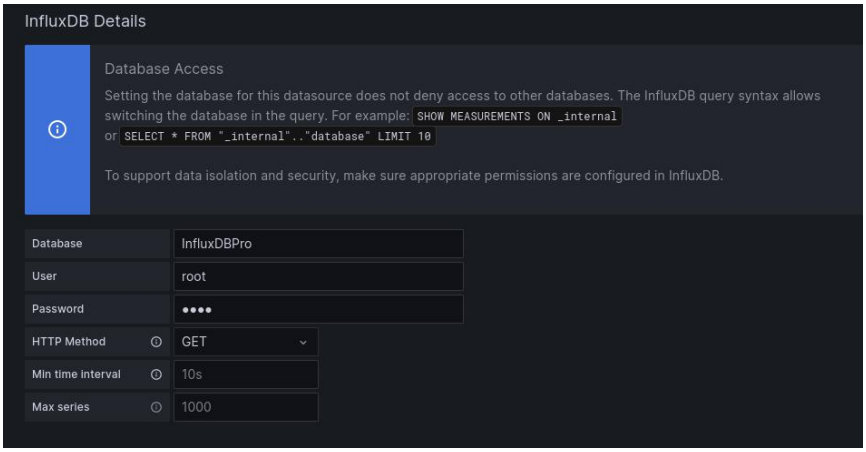
Resumint, escollirem Connections-->Data sources-->Add data source



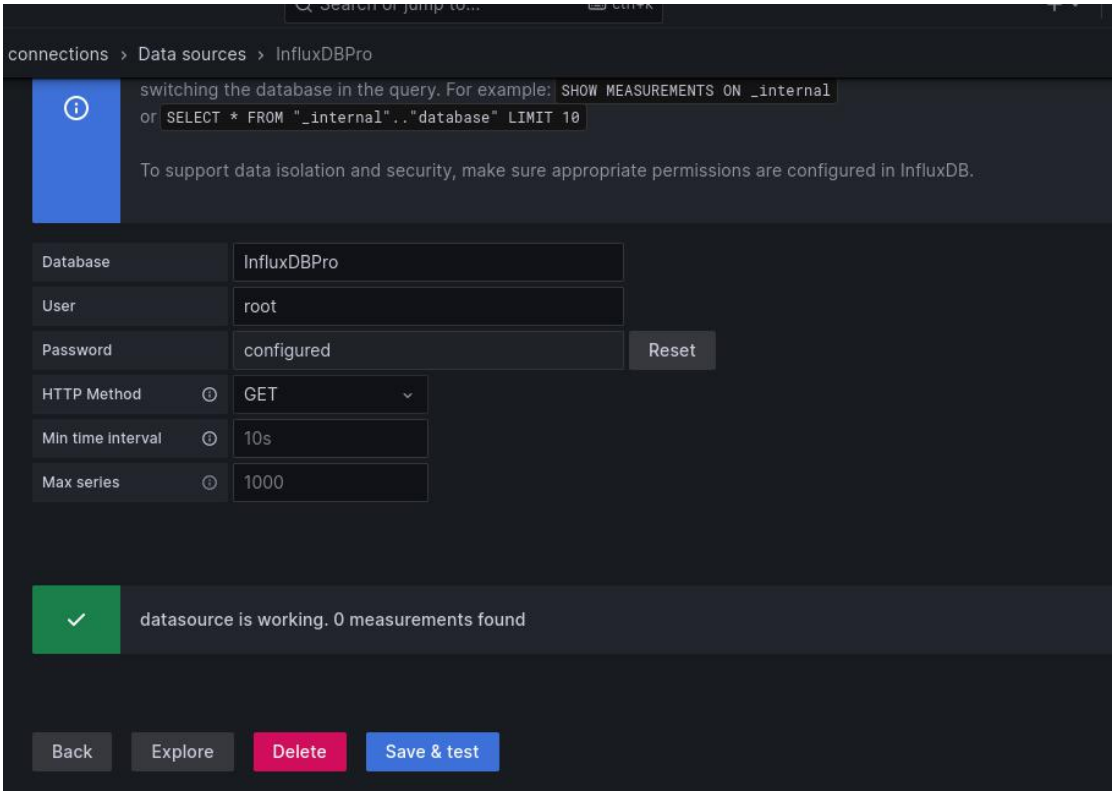
Escollirem InfluxDB



Haurem d'afegir les diferents bases de dades.



Si guardem i testejem, ens hauria d'apareixer un missatge com que està configurat correctament i que està treballant.



Afegirem les diferents bases de dades dels entorns seguint les mateixes instruccions.

11. Instal·lació de Nagvis

Nagvis és un producte lligat a Nagios. Per tal d'instal·lar el producte, descarraguem de la pagina del fabricant l'ultima versió disponible:

http://www.nagvis.org/downloads

En aquest cas, la versió 1.9.34.

Una vegada el tenim descarregat, el descomprimim

```
#tar xvzf nagvis-1.9.34.tar.gz
#cd nagvis-1.9.34
#chmod +x install.sh
```

#./install.sh

Aquesta instal·lació és un assistent on se'ns demanaran informacions referents a la nostra instal·lació de Nagios:

```
+------------------------------------------------------------------------------+
| Welcome to NagVis Installer 1.9.34                                           |
+------------------------------------------------------------------------------+
| This script is built to facilitate the NagVis installation and update       |
| procedure for you. The installer has been tested on the following systems:   |
| - Debian, since Etch (4.0)                                                   |
| - Ubuntu, since Hardy (8.04)                                                 |
| - SuSE Linux Enterprise Server 10 and 11                                     |
|                                                                              |
| Similar distributions to the ones mentioned above should work as well.       |
| That (hopefully) includes RedHat, Fedora, CentOS, OpenSuSE                   |
|                                                                              |
| If you experience any problems using these or other distributions, please    |
| report that to the NagVis team.                                              |
+------------------------------------------------------------------------------+
| Do you want to proceed? [y]:
```

```
+--- Checking paths -----------------------------------------------------------+
| Please enter the path to the nagios base directory [/usr/local/nagiosInt]:
```

```
|   nagios path /usr/local/nagiosInt                                    found |
| Please enter the path to NagVis base [/usr/local/nagiosInt/nagvis]:
```

```
|
+--- Checking prerequisites ------------------------------------------------
| PHP 7.3                                                                 found
|   PHP Module: gd                                                      MISSING
|   PHP Module: mbstring                                                MISSING
|   PHP Module: gettext compiled_in                                       found
|   PHP Module: session compiled_in                                       found
|   PHP Module: xml                                                     MISSING
|   PHP Module: pdo compiled_in                                           found
|   Apache mod_php                                                        found
dpkg-query: no packages found matching graphviz
| WARNING: The Graphviz package was not found.
|          This may not be a problem if you installed it from source
|   Graphviz Module dot                                                 MISSING
|   Graphviz Module neato                                               MISSING
|   Graphviz Module twopi                                               MISSING
|   Graphviz Module circo                                               MISSING
|   Graphviz Module fdp                                                 MISSING
dpkg-query: no packages found matching sqlite3
| WARNING: The SQLite package was not found.
|          This may not be a problem if you installed it from source
|
                                                                              |
---- Trying to detect Apache settings ----------------------------------------+
  Please enter the web path to NagVis [/nagvis]: /nagvisInt
  Please enter the name of the web-server user [www-data]:
  Please enter the name of the web-server group [www-data]:
```

```
+-------------------------------------------------------------------------------+
| Summary
+-------------------------------------------------------------------------------+
| NagVis home will be:           /usr/local/nagiosInt/nagvis
| Owner of NagVis files will be: www-data
| Group of NagVis files will be: www-data
| Path to Apache config dir is:  /etc/apache2/conf-available
| Apache config will be created: yes
|
| Installation mode:             install
|
```

```
+-------------------------------------------------------------------------------+
 Installation complete                                                         |
                                                                               |
 You can safely remove this source directory.                                  |
                                                                               |
 For later update/upgrade you may use this command to have a faster update:   |
 ./install.sh -n /usr/local/nagiosInt -p /usr/local/nagiosInt/nagvis -u www-dat
 -g www-data -w /etc/apache2/conf-available -a y
                                                                               |
 What to do next?                                                              |
 - Read the documentation                                                      |
 - Maybe you want to edit the main configuration file?                         |
   Its location is: /usr/local/nagiosInt/nagvis/etc/nagvis.ini.php             |
 - Configure NagVis via browser                                                |
   <http://localhost/nagvisInt/config.php>                                     |
 - Initial admin credentials:                                                  |
     Username: admin                                                           |
     Password: admin                                                           |
+-------------------------------------------------------------------------------+
```

Serà important afegir correctament les rutes on es vol instal·lar nagvis així com les configuracions apache que s'hauran de revisar, afegint la validació que hem vist en apartats anteriors però per aquests directoris:

Alias /nagvis[entorn] "/usr/local/nagios[entorn]/nagvis/share"

<Directory "/usr/local/nagios[entorn]/nagvis/share">

12. Instal·lació de Histou

Histou són un conjunt de templates que es poden afegir a Grafana de manera que ent pot ser més còmode a l'hora de crear panells de control per les dades recollides de Nagios:

En els servidors Grafana, executar les següents comandes:

cd /Software
wget -O histou.tar.gz https://github.com/Griesbacher/histou/archive/v0.4.3.tar.gz # mkdir -p /var/www/html/histou
cd /var/www/html/histou
tar xzf /tmp/histou.tar.gz --strip-components 1
cp histou.ini.example histou.ini

Modificar el fitxer histou.ini amb les següents entrades:

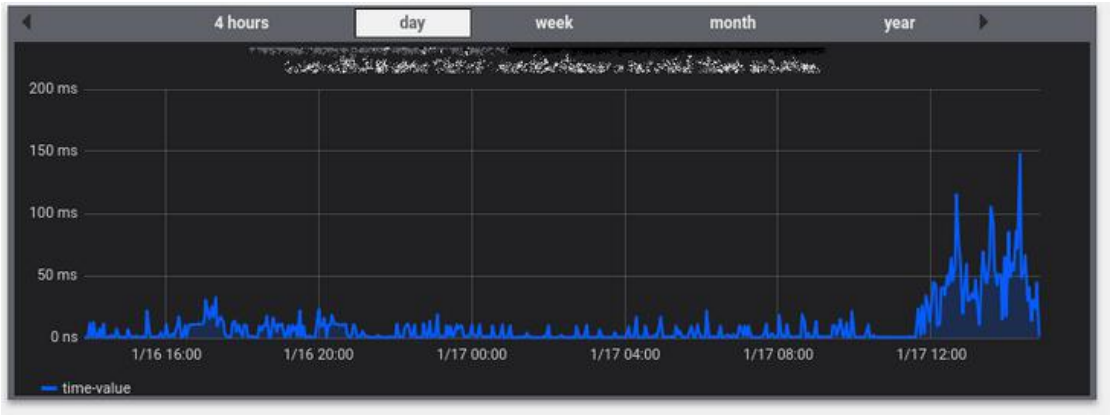
[influxdb] url = http://[InfluxDBServer]:[port]/query?db=nagflux hostcheckAlias = "hostcheck"

cp histou.js /usr/share/grafana/public/dashboards/

Modificar el fitxer /usr/share/grafana/public/dashboards/histou.js canviant tots els "localhost" per les dades del servidor de Grafana.

D'aquesta manera, quan fem peticions amb el histou.js a Grafana, podrem fer servir les queries afegint camps dels serveis Nagios similar a:

http://[ip]:[port]/dashboard/script/histou.js?host=$HOSTNAME$



Aquesta gràfica es pot adjuntar com a link a Nagios, de manera que es pugui consultar des de la pròpia consola.

Annex V. Pla de Contingència

PLA DE CONTINGÈNCIA

MONITORATGE

Aquesta obra es troba subjecte a una llicència de
Reconeixement-No Comercial-Sense Obra Derivada
https://creativecommons.org/licenses/by-nc-nd/3.0/es/

ÍNDEX

1.Introducció

Encara que hi ha sistemes de recolzament per a tots els sistemes, és imprescindible planificar la possible sol·lució a un desastre total, analitzant els riscos i minimitzant així, els possibles impactes que pugui patir l'organització.

2.Motivació

Garantir la continuïtat dels serveis de monitoratge i control de Mediadors i Assegurances, S.A de manera que en cas d'interrupció del servei, aquest es recuperi en el menor temps possible.

3.Objectiu

L'objectiu d'aquest pla és definir els punts inicials per a garantir la funcionalitat del servei i establir els processos i accions necessàries per a reduir o eliminar els impactes davant d'una pèrdua de servei parcial o total, i en el seu cas continuar prestant el servei encara que sigui d'una manera provisional i limitada.

Com a objectius secundaris es defineixen:
- Identificar, analitzar i avaluar els riscos existents que puguin afectar a les operacions i tecnologies del servei.
- Definir les accions i planificar l'execució de les mateixes, per tal de protegir el servei en els termes comentats dels possibles factors adversos tecnològics, humans i naturals.
- Capacitar el personal, tant propi com extern, per a actuar en cas de desastre o situació adversa.
- Definir les activitats que permetin avaluar les accions realitzades i els seus resultats, així com re-avaluar els riscos existents i els nous que puguin sorgir.

4. Àmbit

Aquest Pla de Contingència té com àmbit d'actuació tots aquells components i elements que participin total o parcialment en la composició del servei de monitoratge, com poden ser maquinari, comunicacions, bases de dades, aplicacions, serveis, processos i el personal que gestiona i administra aquest sistema.

5. Elements del sistema de monitoratge

A continuació es descriuen els elements principals del sistema de monitoratge. No s'inclouen en aquest llistat els elements transversals que donen suport a aquest sistema ni tampoc els elements no tecnològics com poden ser el processos o el personal d'administració del sistema:

Element	Descripció	Tipus	Prioritat
Nagios	Aplicació i motor de recolecció de dades	Web	1
Nagflux	Connector de Nagios i InfluxDB	Aplicació	1
Nagvis	Eina de visualització grafica. Fa servir imatges predefinides per mostrar graficament la disponibilitat i rendiment dels sistemes monitoritzats amb motors Nagios	Web	2
Grafana	Eina de visualització, especialment de series de dades.	Web	2
Histou	Plantilles de grafana orientades a les dades recollides per Nagios	Aplicació	2
InfluxDB	Base de dades de series de temps d'alt rendiment	Base de dades	1
MySQL Grafana	Base de dades interna de Grafana	Base de dades	2

6.Matriu de riscos

Podem identificar multitud de riscos que poden afectar el nostre sistema, des de possibles talls de corrent que afectin al CPD fins a desastres naturals que puguin afectar tot el negoci. Aquests riscos tenen una probabilitat i un impacte. Farem servir una matriu per tal de representar els riscos que requereixen un pla amb més immediatesa:

Id	Descripció	Probabilitat	Impacte
1.1	Fallida en un component de l'equip:CPU, memòria RAM, disc o accés a la xarxa de comunicacions.	Alta	Mig
1.2	Atacs de virus o hackers	Mitja	Alt
1.3	Falles en el programari utilitzat	Mitja	Alt
1.4	Connexions i comunicacions exteriors del CPD	Baixa	Alt
1.5	Talls o fluctuacions en la corrent elèctrica	Mitja	Alt
1.6	Desastres naturals: terremots, inundacions, incendis i/o tempestes	Baixa	Alt
1.7	Accidents laborals	Baixa	Mig
1.8	Riscos Socials (vagues)	Baixa	Mig
1.9	Pandemia i/o Epidemia	Mitja	Alt

7.Avaluació de riscos

Una vegada establerts els riscos, avaluem possibles mitigacions dels mateixos, aplicant accions específiques que es podrien prendre per cada cas:

Id	Avaluació	Acció
1.1	Aquests riscos es troben coberts gràcies a la alta disponibilitat en tots els components, a excepció de la base de dades MySQL de Grafana, que tan sols tenim cobert amb el recolzament de les còpies de seguretat. Disposem amb el proveïdor d'un contracte premium amb un temps de resposta de 4 hores.	· Modificar el disseny per a afegir una replica de la base de dades MySQL Grafana o aconseguir afegir aquesta base de dades en una infraestructura multiservei amb alta disponibilitat. · Planificar proves de recuperació de desastres periòdiques. · Preparar un pla de prevenció per aquesta situació
1.2	El sistema de seguretat de l'organització estableix una serie d'eines contra virus ja instal·lades als servidors, i també els	· Limitar el mínim possible i tenir control d'accés als diferents panells que es publiquin fora de la

	diferents sistemes de firewalls protegeixen d'un atac de hackers. En principi, el nostre sistema no tindrà accés des de fora de la xarxa de l'organització, a excepció de panells de control excepcionals per a proveïdors.	xarxa. · Preparar un pla de prevenció per aquesta situació
1.3	El programari d'aquest sistema es basa en arquitectures Linux amb actualitzacions de seguretat i funcionals, pràcticament continues, encara així hi ha eines que poden tenir un suport discontinu o limitat.	· A mig termini s'ha de contractar suport per a les eines que no tenen suport propi i negociar un suport amb els fabricants o proveïdors que disposin d'un contracte de suport. · Preparar un pla de prevenció per aquesta situació
1.4	En aquest cas el CPD disposa de comunicacions replicades d'alta disponibilitat. Es poc probable que es perdin totes dues línies de connexions a la vegada.	· Planificar proves de recuperació periòdiques amb el proveïdor del CPD o demanar les evidències de les proves que realitzi el proveïdor.. · Preparar un pla de prevenció per aquesta situació
1.5	També el CPD disposa d'un sistema de protecció davant aquests inconvenients, SAI i generador de gasoil. A més d'un contracte preferent amb les companyies de suministres, però encara així hem de preparar un pla en cas d'emergència.	· Planificar proves de recuperació periòdiques amb el proveïdor del CPD o demanar les evidències de les proves que realitzi el proveïdor. · Preparar un pla de prevenció per aquesta situació
1.6	Per la nostra situació, és molt poc probable patir terremots o inundacions, però si que es pot patir un incendi. El CPD es troba preparat per un incendi, però encara que pugui aturar-se a temps, hem de preparar un pla en cas d'emergència.	· Planificar proves de recuperació periòdiques amb el proveïdor del CPD o demanar les evidències de les proves que realitzi el proveïdor. · Preparar un pla de prevenció per aquesta situació
1.7	És poc probable i a més, encara que arribés a succeir, el sistema continuaria funcionant, encara que tindríem problemes per a gestionar-ho.	·Com acció mitigadora, es pot contractar un servei de gestió del sistema de monitoratge amb un proveïdor per possibles situacions futures d'aquest tipus. · Preparar un pla de prevenció per aquesta situació
1.8	És poc probable i a més, encara que arribés a succeir, el sistema continuaria funcionant, encara que tindríem problemes per a gestionar-ho.	·Com acció mitigadora, es pot contractar un servei de gestió del sistema de monitoratge amb un proveïdor per possibles situacions

		futures d'aquest tipus. · Preparar un pla de prevenció per aquesta situació
1.9	Encara que es poc probable, sí es cert que en els últims anys s'ha demostrat que es molt més possible del que es podia pensar.	· Establir un protocol de comunicació i actuació en cas de declaració de Pandemia. · Assegurar i establir els elements necessaris per tal de que tot el personal crític pugui teletreballar des del seu domicili. · Preparar un pla de prevenció per aquesta situació.

Annex VI. Esquema solució detallada