Implantación Sistema Monitorización

Adm. de xarxes i de sist. operatius en entorns de p.ll.

Junio 2011

Autor:

Ignacio Iglesias Fernández

Consultores:

Helena Rifà Pous

Miguel Martín Mateo

Licencia:

GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright

notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides

prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

Resumen:

Nagios es un sistema de código abierto de monitorización de redes, hardware, servicios, sistemas... realmente flexible que permite definir distintos tipos de alertas en función de la disponibilidad de los objetos monitorizados.

Proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador.

Entre sus características destacaremos:

1. Monitorización de todo tipo de servicios de red, SMTP, POP3, HTTP, NTTP, ICMP, SNMP.
2. Monitorización de los recursos de equipos (estado del procesador, ocupación de los discos, logs del sistema) en todo tipo de sistemas operativos, como Microsoft Windows a través de los plugins NRPE_NT o NSClient++.
3. Monitorización remota, a través de túneles SSL cifrados o SSH.
4. Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#...).
5. Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
6. Notificaciones a los contactos definidos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, buscapersonas, IM, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
7. Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
8. Rotación automática del archivo de registro.
9. Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros...

Contenidos:

Memoria:

Introducción

Alcance

En el presente documento se pretende describir el funcionamiento de la instalación del Sistema de monitorización que se está implantando para el cliente en su sede principal así como sus delegaciones.

Esta descripción será un punto de partida para la definición del funcionamiento del sistema. En él se describe el flujo de información y se establecen las bases para el desarrollo del análisis funcional que será el documento definitivo que determine el funcionamiento del sistema.

Objetivo del documento

El objetivo de este documento es identificar y analizar los requerimientos funcionales del software a implementar para gestionar el sistema de monitorización así como los aspectos técnicos de la instalación requerida por el cliente.

Del mismo modo, se detallan los sistemas de control así como los componentes hardware de los mismos que estén relacionados directamente con el sistema de monitorización.

Comentario sobre este documento

En este documento se recogen las funcionalidades aplicables a los distintos componentes y servicios gestionados por la aplicación de monitorización. Es por ello que para fases posteriores del desarrollo del proyecto este documento de Análisis Funcional quedará invalidado debiéndose redactar uno nuevo.

Ámbito de aplicación

El presente documento es la primera propuesta para la implantación del sistema de monitorización y la Interfase con los sistemas informáticos del cliente con objeto de dar funcionalidad al sistema, integrando el proceso y el intercambio de información con los referidos sistemas.

El desarrollo que aquí se analiza ha de adaptarse al modelo del cliente, con el objeto de gestionar las alertas de los diferentes sistemas y servicios proporcionados.

El control de los distintos elementos se realizará por parte de Nagios. Por encima de este sistema se encontrará el Interfase que enlazará con el sistema de Gestión del cliente.

El sistema de gestión de las distintos elementos que se monitoricen en los clientes será gestionado por el SGI.

El Sistema estará basado en productos estandarizados que Nagios ha desarrollado además de las particularizaciones que sean necesarias para dar la funcionalidad que el cliente haya requerido.

La gestión de las alertas y la gestión de incidencias a través de los diferentes sistemas, se realizará utilizando las Bases de Datos (MySQL) que residirá en el sistema informático del SM.

El SM será una arquitectura cliente-servidor, que se desarrollará bajo plataforma GNU/Linux. Se aprovecharán las facilidades que una base de datos como MySQL proporciona en cuanto a integridad de información, protección transaccional, etc.

El SM básicamente realizará las siguientes funciones:

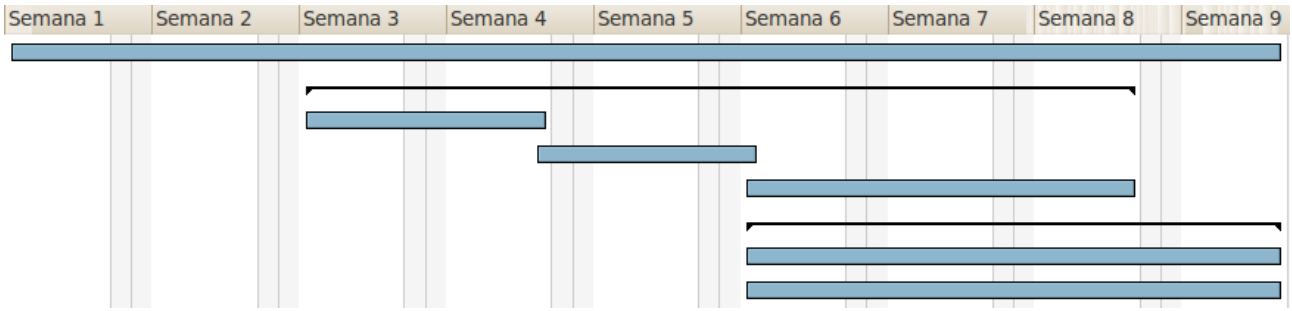
1. Monitorización de todo tipo de servicios de red, SMTP, POP3, HTTP, NTTP, ICMP, SNMP.
2. Monitorización de los recursos de equipos (estado del procesador, ocupación de los discos, logs del sistema) en todo tipo de sistemas operativos, como Microsoft Windows a través de los plugins NRPE_NT o NSClient++.
3. Monitorización remota, a través de túneles SSL cifrados o SSH.
4. Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#...).
5. Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
6. Notificaciones a los contactos definidos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, buscapersonas, IM, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
7. Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas pro activas.
8. Rotación automática del archivo de registro.
9. Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros...

Requisitos

- Servidor Web (En este caso se usará Apache)
- Base de datos (Para este desarrollo se utilizará MySQL)
- Php (Para la interfase web)
- Gcc (Compilador de C)
- Libgd (es una librería gráfica necesaria para mostrar el statusmap)
- Perl
- Servidor de correo (Para enviar las alertas por correo)
- Diversos módulos (Comunicaciones con todo tipo de máquinas)

Planificación:

Los trabajos se dividirán en tres grandes bloques que se superpondrán en el



tiempo. La duración planificada para la puesta en marcha del sistema principal será de nueve semanas y se dividirá en las siguientes tareas principales:

WBS	Nombre	Trabajo
1	Planificación y desarrollo	45d
2	**Instalacion oficinas**	**32d**
2.1	Montaje e instalacion servidores	10d
2.2	Instalación sistema nagios	7d
2.3	Ajustes sistema nagios	15d
3	**Implantación en equipos**	**40d**
3.1	Implantación interna	20d
3.2	Implantación en clientes	20d

- **Planificación y desarrollo:** Comenzará dos semanas antes que el resto de las tareas y se extenderá durante todo el tiempo que duren los trabajos. El cometido principal será servir de apoyo y cuidar que se cumplan los tiempos estipulados de planificación así como acometer tareas de desarrollo que se pudiesen derivar del resto de tareas.

- **Instalación en oficinas:** En esta fase se instalarán los dispositivos en los que se apoyará todo el sistema. Se instalarán en el CPD de la oficina central y sucursales el equipamiento, tanto servidores como electrónica de red, designados para este cometido, se instalarán los sistemas operativos GNU/Linux basados en la distribución debian e instalarán las dependencias necesarias para el correcto funcionamiento de nagios, servicio de páginas web apache, servicio de base de datos, mysql, servicio de correo postfix y demás servicios necesarios para un correcto desempeño del sistema.

- **Implantación en equipos:** Ua vez se han concluido los trabajos relativos a la instalación de los servidores que proporcionarán la base del sistema, se completará con la implantación de los checks sobre los servicios que se quieran monitorizar en los clientes.
En esta fase el trabajo se dividirá en dos tareas principales y que se diferenciarán en cuanto al ámbito de implantación y que se llevarán a cabo

simultáneamente. Por un lado se implantará internamente en los sistemas de la empresa y por otro lado externamente en los clientes.
A la vez se dará formación a los técnicos de telemantenimiento para que se familiaricen con el sistema y sepan actuar en los casos en que las alarmas muestren cualquier tipo de incidencia.

Definición técnica de la instalación

La instalación se compone de una oficina principal con distintas sucursales (actualmente 2) y diferentes obras de clientes que serán gestionadas por un único sistema de gestión centralizado en las dependencias principales.

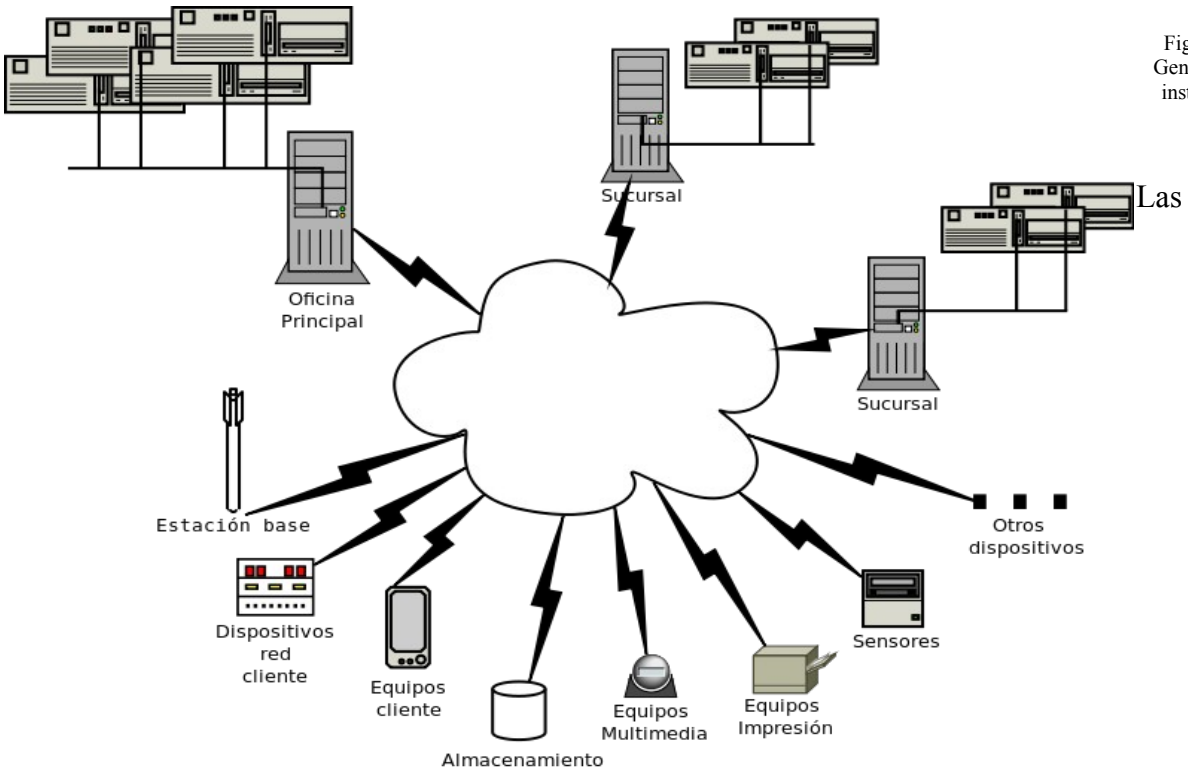


Fig1. Vista General de la instalación.

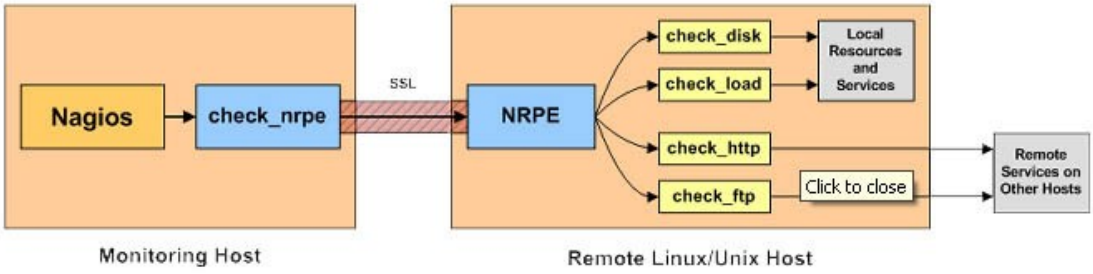
Las notificaciones parten de los diferentes elementos monitorizados y se envían ya bien a los servidores en las obras (siempre que la envergadura de las mismas requiera el empleo de un equipo), las sucursales, si la proximidad geográfica u otros motivos lo requieran y finalmente todas se reciben de manera centralizada en las oficinas principales.

La ventaja de la distribución es clara: suponiendo, como es el caso, que tenemos 2 delegaciones, si se cortan las comunicaciones, cada Nagios seguirá monitorizando el entorno local donde está ubicado, los datos a traspasar a la base de datos esperarán en cola hasta que las comunicaciones se restablezcan. Eso permite ser más realistas en caso de corte, ya que en realidad algunos servicios probablemente siguen funcionando en el entorno local y nos puede interesar que no computen como perdida de servicio.

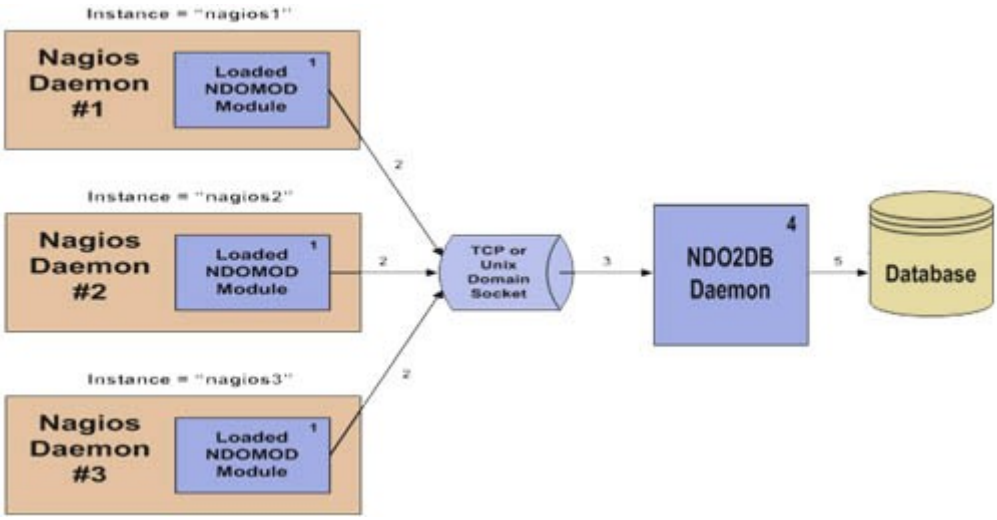
Características del Sistema de monitorización

Un servidor lanza peticiones vía sus checks en **/nagios/libexec**. A su vez una serie de tests se ejecutan en las máquinas remotas mediante el NRPE: un demonio que se instala en las máquinas y que escucha en el puerto 5666 las peticiones que le manda la máquina que monitoriza. La máquina 'cliente' tiene definidos los comandos en **/nagios-plugins/nrpe.cfg** y devuelve los resultados. Las comunicaciones se transmiten mediante un canal cifrado SSL.

En este esquema una máquina tiene la carga del motor de Nagios, los archivos de texto con los datos y la carga del frontend.



En el siguiente esquema, una **arquitectura distribuida**, se permite tener una consola central independiente de las individuales y así centralizar la monitorización, a la par que permite la inclusión de otros Add-ons para Nagios que obtienen los datos del MySQL.



Complementos

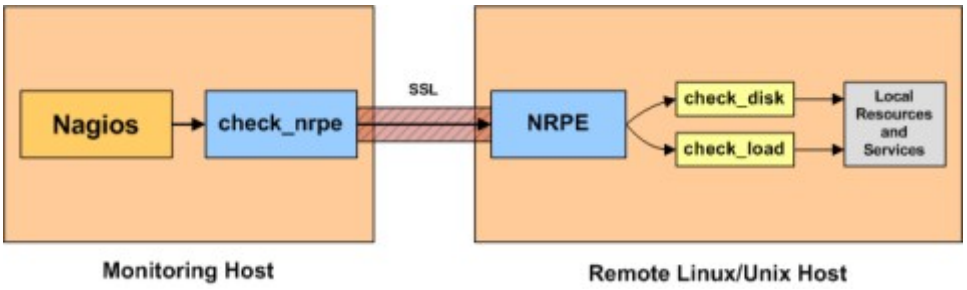
Hay una gran cantidad de complementos para Nagios. Estos complementos se usan para extender la funcionalidad o para integrar el núcleo del sistema con otras aplicaciones.

Podemos encontrar complementos para las siguientes funciones:

- Gestión de archivos de configuración a través de entorno web.
- Monitorización de maquinas remotas (Windows, *NIX, etc)
- Envío de checks pasivos desde máquinas remotas..
- Extensión y simplificación de notificaciones y reportes.
- Envío de eventos de respuesta
- Y un largo etcétera...

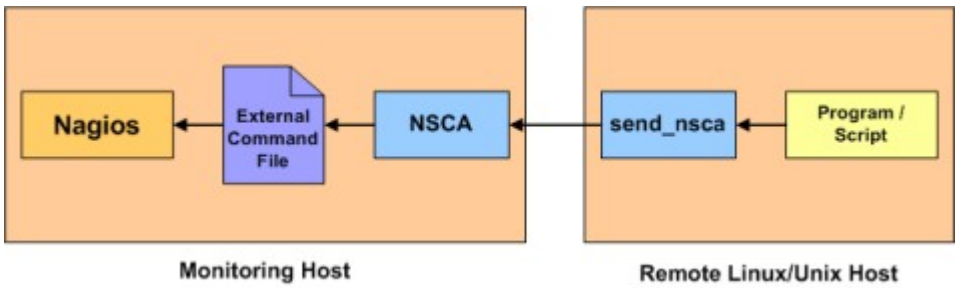
NRPE

NRPE es un complemento que nos permite ejecutar plugins en maquinas *NIX. Es útil si se necesita monitorizar recursos como lo son el uso de los discos, carga de la CPU, uso de memoria, etc.



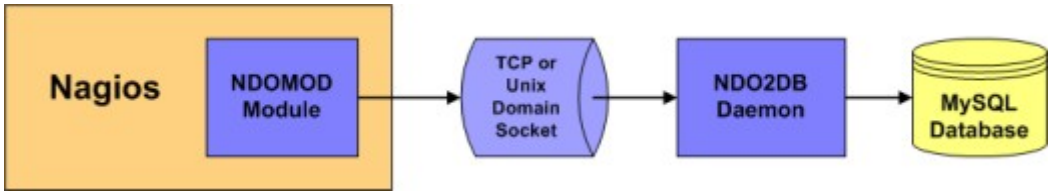
NSCA

Con el complemento NSCA podemos enviar checks pasivos desde maquinas remotas al demonio de Nagios. Este método se muestra especialmente eficaz en sistemas distribuidos y redundantes.



NDOUtils

Con este complemento podemos almacenar toda la información de estado en una base de datos MySQL. Múltiples instancias pueden, a su vez, almacenar la información en una misma base de datos para una labor centralizada de informes.



Controladores de eventos

El envío de eventos es un sistema de comandos opcional (scripts o ejecutables) que se desencadenan cuando ocurre un cambio en el estado de un servicio o máquina.

Un uso obvio para los controladores de eventos es la capacidad del sistema Nagios para arreglar los problemas de forma pro-activa antes de que se envíen notificaciones. Algunos otros usos para los controladores de eventos son:

- Reinicio de servicios caídos.
- Envío de notificaciones a un sistema de gestión de incidencias.
- Registro de eventos informativos en una base de datos.
- Reinicio de servidores en caso de problemas.
- Etc...

Los controladores de eventos son desencadenados si un servicio o maquina se encuentra en las siguientes situaciones:

- El estado cambia a SOFT.
- El estado cambia a HARD.
- El elemento se recupera de un estado SOFT o HARD.

Son considerados estados SOFT en las siguientes circunstancias:

- Cuando una maquina o servicio se encuentran en un estado no OK o no UP durante un determinado número de comprobaciones inferior al número dado.
- Cuando se recupera de un estado de error SOFT. Esto se considera una recuperación SOFT.

Son considerados estados HARD en las siguientes circunstancias:

- Cuando una maquina o servicio se encuentran en un estado no OK o no UP durante un determinado número de comprobaciones superior al número dado.
- Cuando una maquina o servicio transita de un estado de error a otro (WARNING a ERROR)
- Cuando un servicio se encuentra en un estado no OK y la correspondiente maquina que lo aloja está en estado DOWN o UNREACHABLE.
- Cuando se recupera de un estado de error HARD. Esto se considera una recuperación HARD.

He aquí un ejemplo de cómo se determinan los tipos de estado, cuando se producen cambios de estado, y cuando los controladores de eventos y notificaciones se envían. La siguiente tabla muestra los controles consecutivos de un servicio a través del tiempo. El servicio tiene un valor de 3 como número máximo de intentos.

Tiempo	Check	Estado	Tipo	Estado	Notas
0	1	OK	HARD	No	Estado inicial
1	1	CRITICAL	SOFT	Yes	Primera detección de un estado no-OK. Los controladores de eventos se lanzan.
2	2	WARNING	SOFT	Yes	Servicio continúa en un estado no-OK. Los controladores de eventos se lanzan.
3	3	CRITICAL	HARD	Yes	Número máximo de intentos de se ha alcanzado, por lo que el servicio entra en un estado HARD. Los controladores de eventos se lanzan. Se envía notificación.
4	1	WARNING	HARD	Yes	Cambio a estado HARD o WARNING. Los controladores de eventos se lanzan. Se envía notificación.
5	1	WARNING	HARD	No	Se estabiliza en estado HARD. Dependiendo en que estado de notificación se encuentra, se envía otra notificación.
6	1	OK	HARD	Yes	El servicio se recupera de un estado HARD. Los controladores de eventos se lanzan. Se envía notificación.
7	1	OK	HARD	No	El servicio se encuentra OK.
8	1	UNKNOWN	SOFT	Yes	El servicio cambia a un estado SOFT no OK. Los controladores de eventos se lanzan.
9	2	OK	SOFT	Yes	El estado cambia a una recuperación SOFT. Los controladores de eventos se lanzan. No hay notificación ya que no se considera un problema real.
10	1	OK	HARD	No	El servicio se estabiliza en estado OK.

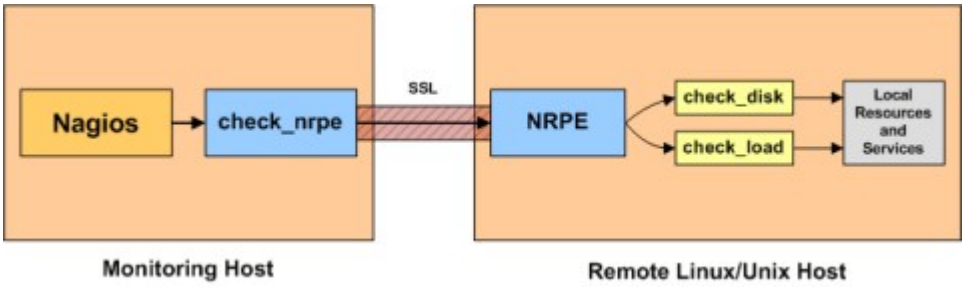
Elementos a monitorizar

*Monitorización de maquinas *NIX*

Se pueden monitorizar servicios y características de maquinas tales como:

- Carga de la CPU.
- Uso de la memoria.
- Uso de los discos.
- Usuarios en el sistema.
- Procesos en ejecución.
- Etc...

Los servicios que provee cualquier servidor de la familia *nix (HTTP, FTP, SSH, SMTP, etc.) son fácilmente configurables para su supervisión.



Hay diversos modos para monitorizar servicios o máquinas *NIX:

- Mediante claves públicas SSH, mediante las cuales ejecutar plugins en servidores remotos. Este método puede ser fuente de altas cargas en el uso de los recursos en casos en los que se supervisen cientos o miles de parámetros. La sobrecarga viene producida por la creación/destrucción de conexiones SSH.

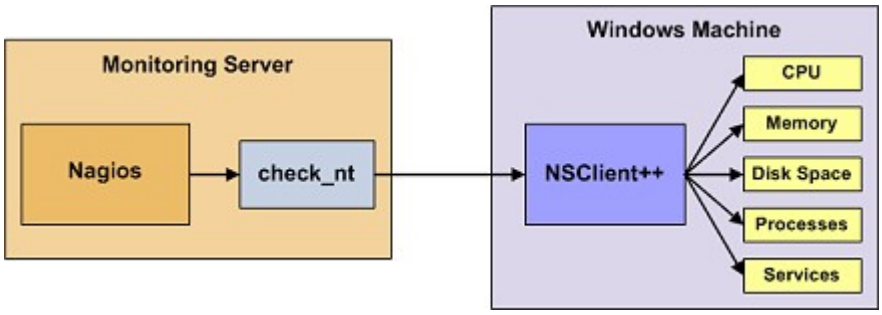
- Otro método común de control a distancia de anfitriones *nix es usar el complemento NRPE. NRPE le permite ejecutar complementos a distancia en anfitriones *nix. Esto es útil si se necesita controlar los recursos locales y los atributos como el uso de disco, carga de la CPU, uso de memoria, etc en un host remoto.

Monitorización de maquinas Windows

Se pueden monitorizar servicios y características de maquinas tales como:

- Carga de la CPU.
- Uso de la memoria.
- Uso de los discos.
- Usuarios en el sistema.
- Procesos en ejecución.
- Etc...

Los servicios que provee cualquier servidor Windows (HTTP, FTP, IMAP, SMTP, etc.) son fácilmente configurables para su supervisión.

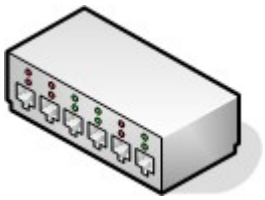


Para la supervisión de servidores Windows se debe instalar un agente en la maquina a monitorizar. Dicho agente actúa como un proxy entre los plugins de Nagios que se encargan de hacer el seguimiento y los servicios o características del servidor a monitorizar. Sin el referido agente no se podrá monitorizar, de manera activa, los servicios o parámetros de los servidores Windows.

El agente más popular en estos casos es el NSClient++ del lado de Windows junto con el complemento check_nt del lado de Nagios.

Existen alternativas a dicho agente como lo puede ser NC_Net que ofrecen características que se debieran estudiar para evaluar su conveniencia en el caso de que se precisasen dichas opciones.

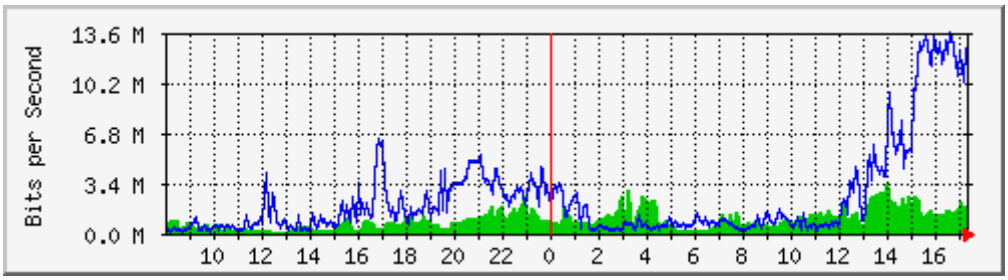
Monitorización de Electrónica de Red



La electrónica de red “no administrable” no tiene IP y por lo tanto es invisible en la red por lo que no es monitorizable, pero aquellos dispositivos que, como router o switches, que tengan asignada una IP pueden ser monitorizables:

- Paquetes perdidos.
- Tiempos promedio.
- Ancho de banda.
- Trafico de red.

Con el uso del complemento mrtgtraf se pueden generar gráficas de los parámetros de uso de estos dispositivos para su uso estadístico.



De este modo se pueden observar diversos parámetros que nos pueden ayudar en la prevención de problemas derivados del uso de la red.

Cada día es más importante para nuestras labores cotidianas, el uso de las comunicaciones, mantenernos informados de la demanda de los diversos protocolos de red nos ayudarán a ofrecer un servicio acorde a las necesidades demandas.

Es importante señalar que la base de la monitorización es la red, las comunicaciones viajan a través de ella, por lo que es primordial hacer un buen uso y mantenimiento de la misma para que el resto de sistemas funcionen correctamente.

Monitorización de sistemas SNMP

Actualmente una gran mayoría de dispositivos, como lo pueden ser los anteriormente tratados, poseen características mediante las cuales gestionar mensajes SNMP.

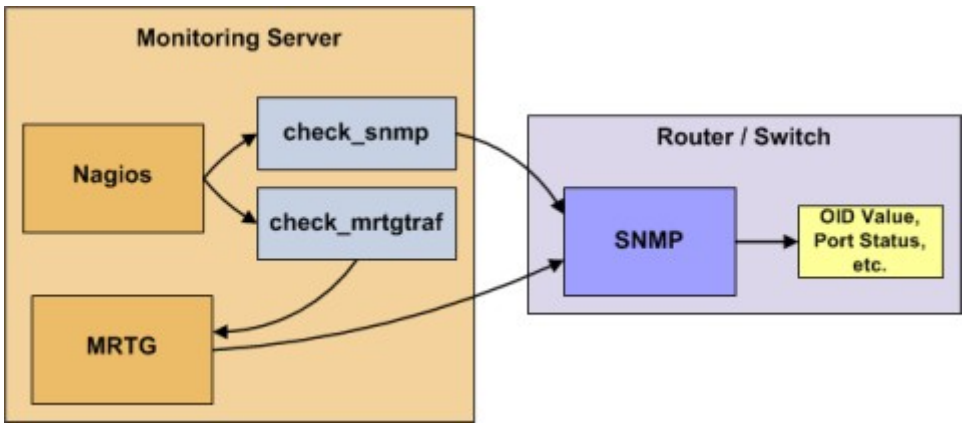
Las versiones existentes son SNMPv1, SNMPv2, SNMPv3.

SNMPv2 posee operaciones adicionales a la versión 1.
SNMPv3 implementa cambios en aspecto de seguridad.

Este protocolo es de la capa de aplicación de la familia TCP/IP (transporte, sesión, presentación y aplicación), pero de tipo datagrama (es decir la capa sesión no aplica) cada intercambio es una transacción independiente entre el gestor y el agente. SNMP facilita el intercambio de información de administración entre dispositivos de red.

SNMP nos permite:

- Supervisar desempeño de red.
- Buscar.
- Resolver problemas.
- Planear crecimiento



Una red administrada a través de SNMP tiene tres componentes claves:

- Dispositivos administrados
- Agentes
- Sistemas administradores de red (NMSs)

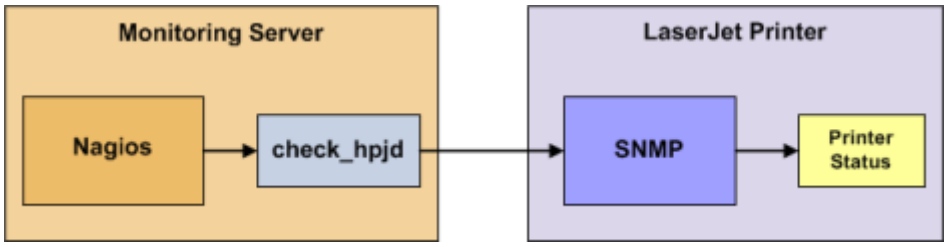
Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: lectura, escritura, notificación y operaciones transversales.

Monitorización de Impresoras de red

El plugin provisto por Nagios se basa en el protocolo JetDirect de HP por lo que cualquier impresora, que tenga un dispositivo o tarjeta tanto interna como externa, basada en dichas características puede ser fácilmente monitorizable por este método.

El plugin es capaz de detectar los siguientes estados de impresora:

- Atasco de papel.
- Papel agotado.
- Impresora fuera de linea.
- Intervención requerida.
- Toner bajo.
- Memoria insuficiente.
- Compartimento abierto.
- Etc...



Monitorizar el estado de las impresoras de red es muy sencillo mediante este método. Las impresoras compatibles con JetDirect tienen habilitado el servicio SNMP el cual, como ya se ha especificado, facilita a Nagios la labor de interrogar al dispositivo acerca de los parámetros a monitorizar.

Aquellas impresoras que no posean esta facilidad proporcionada por la característica reseñada, podrán ser igualmente monitorizadas sin ningún tipo de problemas por parte de SNMP, siempre y cuando posean dicho servicio.

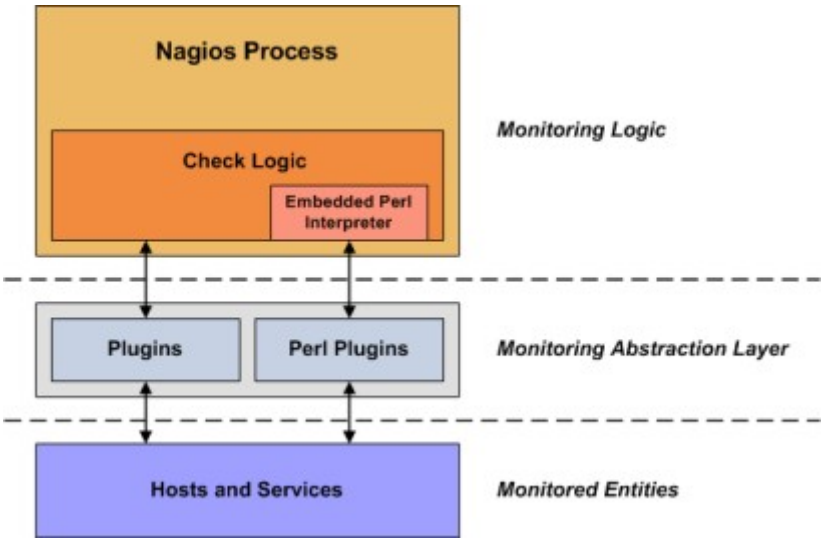
Monitorización de servicios Públicos

La extensa variedad de plugins incluidos en Nagios facilitan nuestra labor ya que una gran mayoría de los mismos ya están disponibles para su uso a la hora de monitorizar todo tipo de servicios.

Por servicios públicos entendemos cualquiera que pueda ser accesible a través de la red, ya bien sea una red local o internet. Ejemplos de estos servicios incluyen HTTP, POP3, IMAP, FTP... hay infinidad de protocolos que se usan en un día normal en la actividad diaria. Estos servicios y aplicaciones, así como sus protocolos de bajo nivel, pueden ser monitorizados sin ningún tipo de permisos de acceso adicional.

Si bien Nagios provee una gran cantidad de plugins incluidos, también existe una extensa comunidad que desarrolla y pone a disposición pública otra serie de plugins especializados en todo tipo de tareas. En la web NagiosExchange.org se alojan un extenso número de plugins escritos por usuarios que sin duda cubrirán la mayor parte de nuestras monitorizaciones.

Los plugins son ejecutables o bien scripts (perl scripts, shell scripts, etc...) que pueden ser ejecutados desde una línea de comandos para verificar el estado de un parámetro determinado de una máquina o bien un servicio.



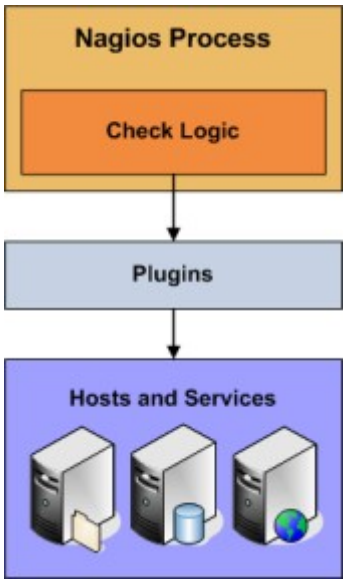
Como se puede observar en el gráfico, actúan como una capa de abstracción entre la lógica de control de demonio de Nagios y los servicios o máquinas reales que están siendo monitorizados.

Checks activos

Nagios es capaz de monitorizar maquinas y servicios de dos formas: activa y pasivamente. Los checks pasivos se describirán a continuación, ocupemonos ahora en los activos. Los checks activos son el método más común a la hora de monitorizar maquinas y servicios. Las características principales de estos checks son:

- Los checks activos son iniciados por el demonio de Nagios.
- Los checks activos son lanzados regularmente.

Los checks activos son iniciados por la lógica de verificación del demonio de Nagios. Cuando la programación de un plugin se ejecuta, este reclama la información al host o servicio determinado. Nagios procesará los resultados de la comprobación de la máquina o servicio y tomar las medidas apropiadas en caso necesario (por ejemplo, enviar notificaciones, ejecutar controladores de eventos, etc.)



Los checks activos son ejecutados:

- A intervalos regulares definidos tanto en la configuración de maquina como de servicio.
- Bajo demanda cuando sea requerido.

Checks pasivos

En la mayor parte de los casos, Nagios es usado para monitorizar maquinas y servicios en una programación regular usando checks activos, es decir, desencadenados desde el propio demonio de Nagios. Nagios también soporta un modo de monitorizar maquinas y servicios pasivamente. Este modo de monitorización pasiva actúa de la siguiente manera.

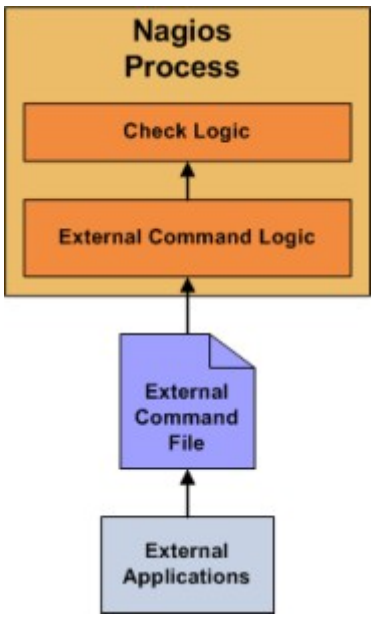
- Los controles pasivos se desencadenan por parte de aplicaciones o servicios externos.
- Los resultados de la verificación pasiva se envían para su procesamiento al demonio de Nagios.

La principal diferencia entre los checks activos y pasivos es la fuente que desencadena la acción. En el caso de los activos es Nagios mientras que los pasivos son desencadenados por aplicaciones externas.

Los checks pasivos son útiles en las siguientes situaciones:

- Servicios de naturaleza asíncrona que no se pueden controlar de manera eficaz de manera convencional.
- Dispositivos situados tras cortafuegos que no pueden ser controlados activamente desde el servidor de vigilancia.

Los checks pasivos actúan del siguiente modo:



1. Una aplicación externa comprueba el estado de un host o servicio.
2. La aplicación externa escribe los resultados de la verificación en el archivo de comandos externos.
3. La próxima vez que Nagios lea el archivo de comandos externos, pondrá los resultados de todos los controles pasivos en una cola para su posterior procesamiento. La misma cola que se utiliza para almacenar los resultados de los controles activos también se utiliza para almacenar los resultados de los controles pasivos.
4. Nagios periódicamente ejecutará una verificación de eventos externos, escaneando la cola en busca de resultados. Cada resultado encontrado en la cola se procesa de la misma manera, con independencia de si el check estaba en activo o pasivo. Nagios puede enviar notificaciones, alertas de registro, etc dependiendo de la información.

Operativa del sistema

Objetos

Objetos son los elementos involucrados en la lógica de monitorización y notificación. Los tipos de objetos incluyen:

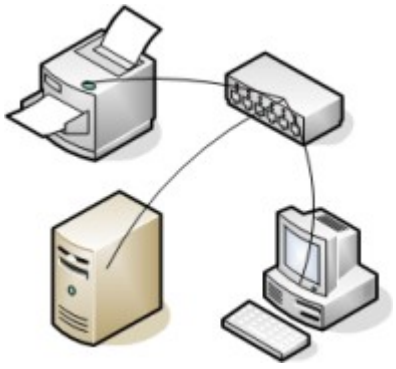
- Servicios.
- Grupos de servicios.
- Maquinas.
- Grupos de máquinas.
- Contactos.
- Grupos de contactos.
- Comandos.
- Periodos de tiempo.
- Escalado de notificaciones.
- Notificaciones y ejecuciones dependientes.

Los objetos pueden ser definidos en uno o más ficheros de configuración especificadas en el archivo de configuración general.

Hosts

Constituidos por cualquier objeto de la lógica de monitorización. Atributos importantes que determinan que sea un hosts son los siguientes:

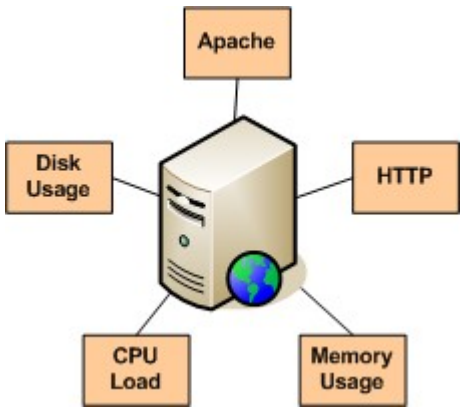
- Los Hosts son dispositivos en la red tales como servidores, estaciones de trabajo, routers, switches, impresoras...
- Los Hosts tienen una dirección bien sea IP o MAC.
- Los Hosts tienen servicios asociados.
- Los Host tienen relaciones de padre/hijo con otros hosts, las cuales representan conexiones de red entre los mismos.



Los grupos de Hosts están integrados por uno o más Hosts. Los grupos de Hosts son útiles para las vistas de estado en el interfaz web y simplifica su configuración.

Servicios

Son objetos centrales en la lógica de monitorización. Los servicios están asociados con los Hosts y pueden ser:



- Atributos de los hosts (Carga de la CPU, Uso del disco, Tiempo de actividad, etc...)
- Servicios provistos por los Hosts (HTTP, POP3, FTP, etc...)
- Otros aspectos asociados con los Hosts (DNS, copias de seguridad)

Los grupos de servicios están integrados por uno o más servicios. Los grupos de servicios son útiles para las vistas de estado en el interfaz web y simplifica su configuración.

Contactos

Como contactos entendemos las personas involucradas en el proceso de notificación:

- Los contactos pueden tener uno o más métodos de notificación (teléfonos móviles, email, mensajería instantánea, etc...)
- Los contactos reciben las notificaciones de los hosts y servicios de los que son responsables.

Los grupos de contactos están integrados por uno o más contactos. Los grupos de contactos son útiles para las vistas de estado en el interfaz web y simplifica su configuración.

Periodos de tiempo

Los periodos de tiempo se usan para controlar:

- Cuando los hosts y servicios han de ser monitorizados.
- Cuando los contactos deben recibir las notificaciones.

Comandos

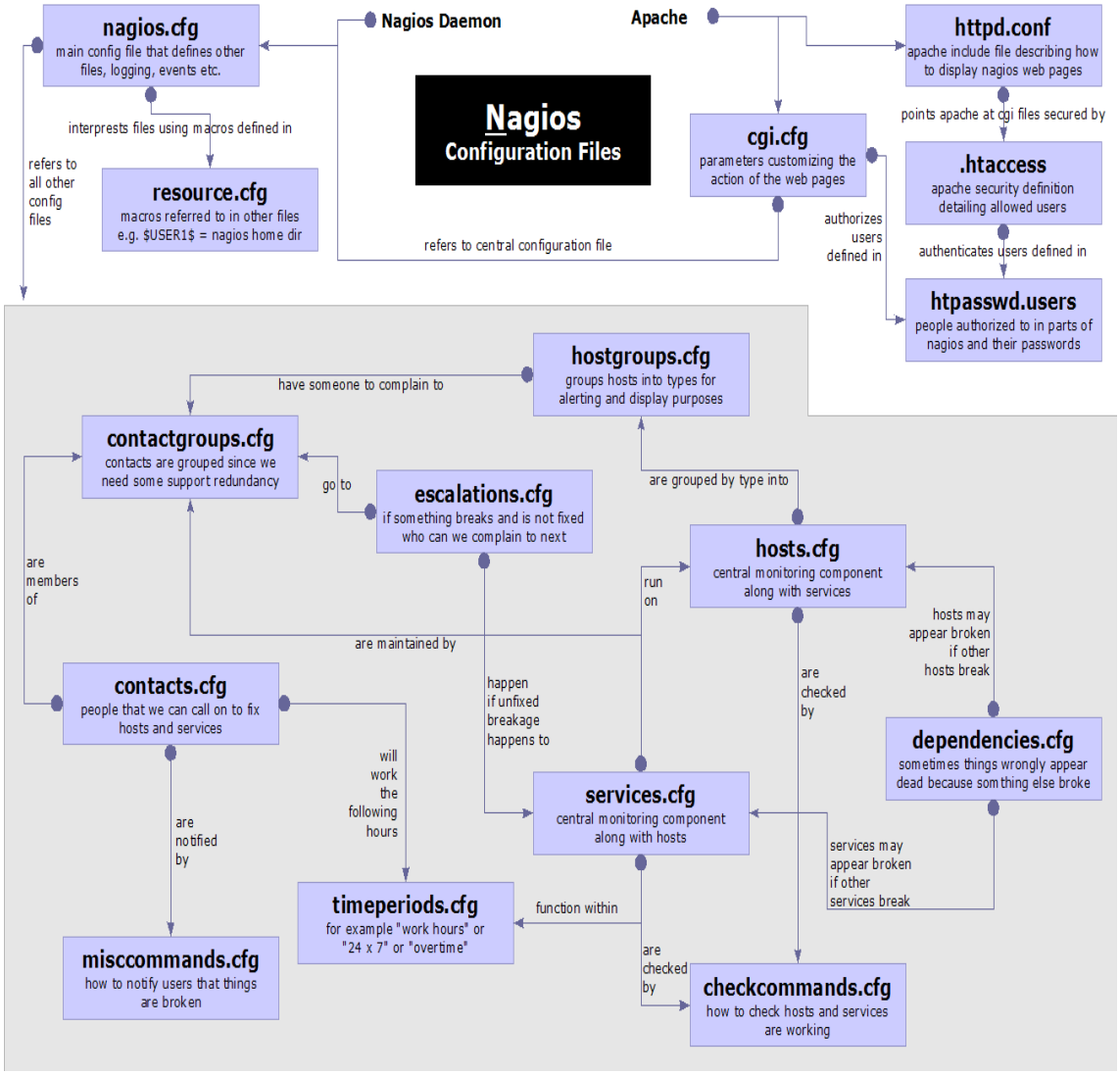
Se usan para indicar a Nagios que programas, scripts, etc... se ejecutan para llevar a cabo:

- Checks de Hosts y servicios.
- Notificaciones.
- Controladores de eventos.
- Etc...

Lógica del sistema

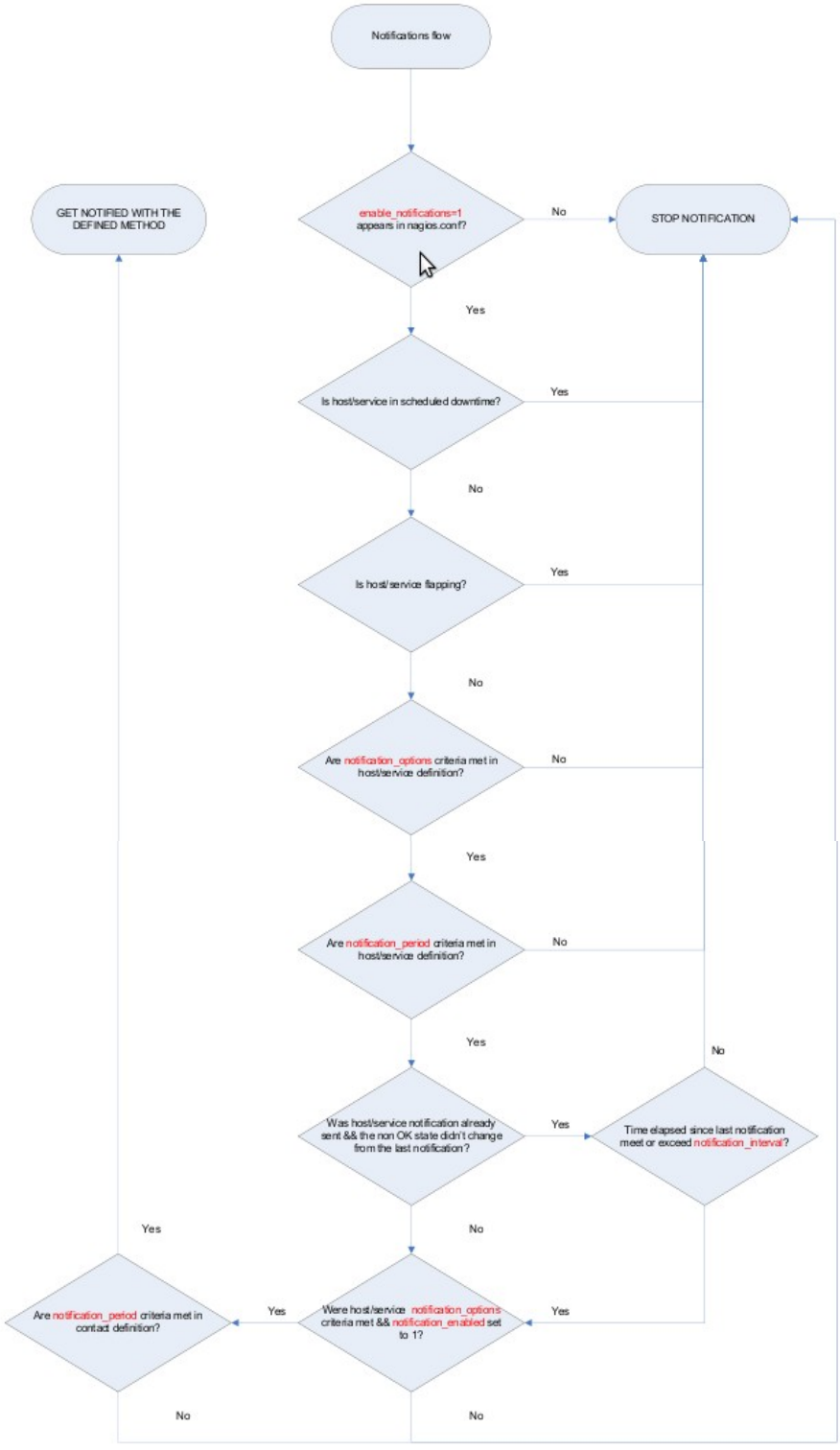
De configuración

A continuación se muestra un esquema de los principales servicios así como los ficheros de configuración imprescindibles para la puesta en funcionamiento y ajuste del sistema de monitorización.



Como se puede observar los nombres de los ficheros son auto-descriptivos y coinciden con la serie de objetos, descritos anteriormente, susceptibles de monitorización.

De notificaciones



Objetivos:

El sistema propuesto pretende facilitar, mediante la automatización, tareas encaminadas a la disponibilidad de los servicios en los diferente ambientes de la empresa.

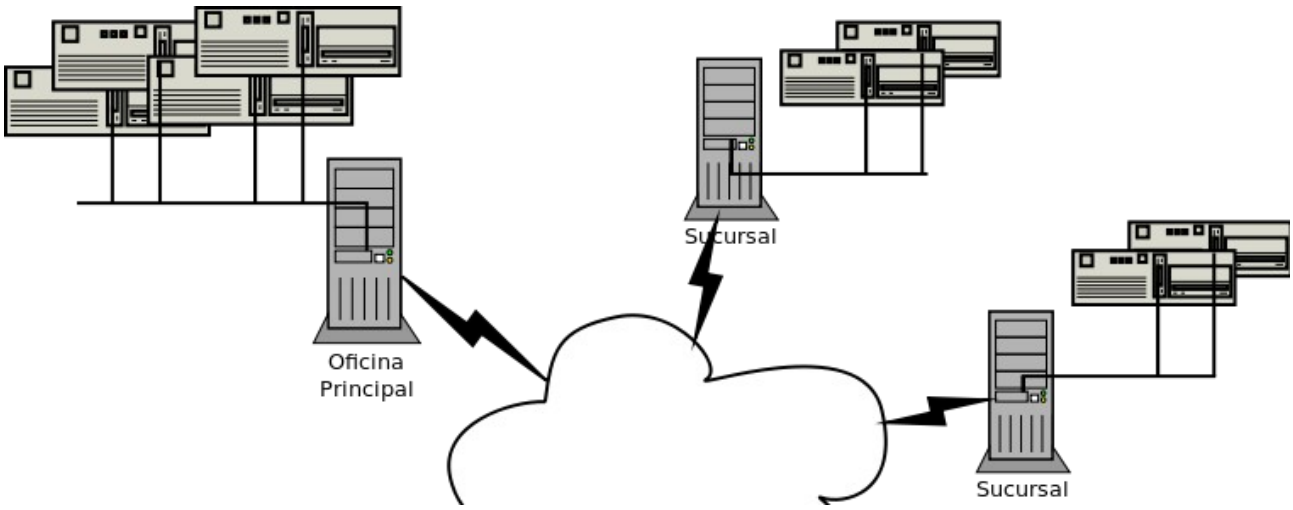
Sus principales características son:

- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#...).
- Notificaciones a los contactos definidos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, buscapersonas, IM, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas pro activas.
- Rotación automática del archivo de registro.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros

Muchos de dichos sistemas tienen una prioridad crítica para el correcto funcionamiento del modelo de negocio de la empresa y se necesita estar informado en todo momento de su estado para poder prevenir y actuar con la mayor celeridad ante las posibles caídas que puedan acontecer. Por otro lado se monitorizarán otros sistemas que aunque no tan críticos forman parte de la dinámica del negocio y deben ser mantenidos para un óptimo funcionamiento.

Se dividirán los ambientes según su tipología y grado de criticidad así como por los diferentes departamentos que deben ser notificados en caso de cualquier tipo de problema. De este modo podemos agrupar dichos entornos como se detalla a continuación.

- Oficina principal y sucursales:



En este entorno nos encontramos con dos tipos de servicios con diferente criterio de monitorización a nivel de criticidad.

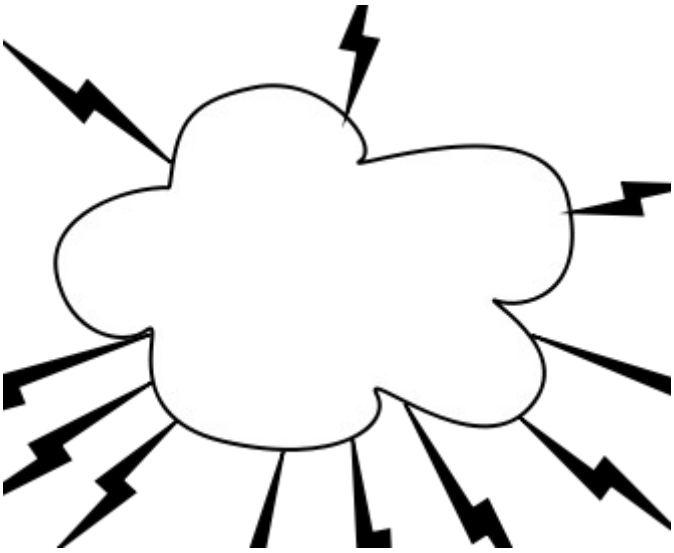
1. Por un lado tenemos los servidores y dispositivos de red que dan servicios a toda la organización y que se consideran criticas debido a las tareas que desempeñan. La parada en alguno de estos elementos puede dejar sin servicio a toda la organización y por ende sin capacidad de respuesta ante los clientes. La inteligencia del negocio así como la capacidad para que este se lleve a cabo dependen de estos sistemas.

    - Monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP.).
    - Monitorización de Bases de datos.
    - Monitorización de sistemas de ficheros.
    - Monitorización de tareas de respaldo (copias de seguridad).
    - Monitorización de tareas programadas y servicios.

2. Por otro lado tenemos los equipos cliente que clasificaremos con una prioridad baja ya que aunque el trabajo depende de los mismos no se prevee, salvo por causas de fuerza mayor, que estos impidan el correcto funcionamiento de la empresa.

    - Monitorización de los recursos de equipos (estado del procesador, ocupación de los discos, logs del sistema) en todo tipo de sistemas operativos, como Microsoft Windows a través de los plugins NRPE_NT o NSClient++.

- Redes:



Las comunicaciones con el exterior, así como las internas, también están catalogadas como altamente críticas ya que la mayor parte del trabajo y de los sistemas que se deben supervisar se encuentran fuera de los centros de trabajo. Mantener en todo momento las comunicaciones es primordial para mantener la supervisión y los servicios que constituyen el modelo de negocio de la empresa.

- Monitorización de los recursos de todo tipo de dispositivos de red implicados en las comunicaciones.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.

Valoramos de un modo muy especial los datos que se transfieren por parte de nuestros clientes y aseguramos la confidencialidad de los mismos en los casos en los que se requiera.

- Monitorización remota, a través de túneles SSL cifrados o SSH.

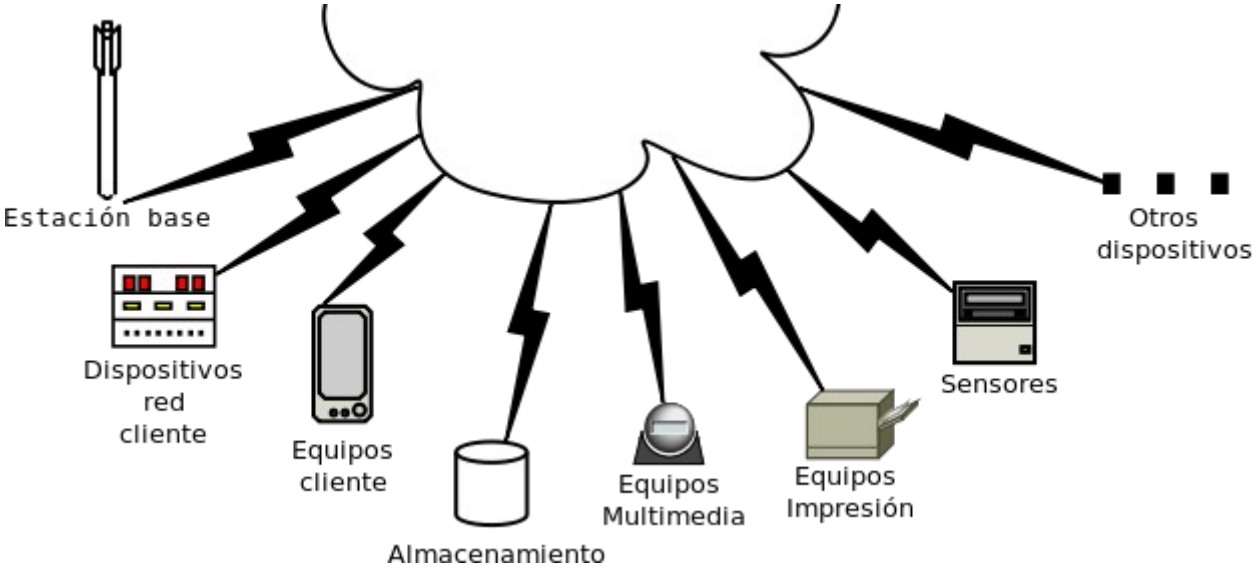
- Obras:

En ellas se encuentran los sistemas principales a monitorizar ya que son estos los que a su vez proporcionan los servicios a clientes. De ellos depende que los clientes perciban la calidad del servicio proporcionado por lo que el nivel de prioridad es altamente crítico.

Se pueden configurar de manera autónoma con su propios sistemas de monitorización “in situ” o bien dependientes de la central o las sucursales. Este tipo de decisión viene dada por el numero de dispositivos implicados.

- Sistemas provistos de servicio SNMP para consultar el estado de los sistemas.

- Diversas localizaciones.



En este apartado se recogen todo tipo de dispositivos autónomos que funcionan aislados de los principales centros de trabajo de los clientes pero que pueden constituir un engranaje más en el funcionamiento de otros sistemas. El nivel de criticidad varía según el dispositivo y su desempeño.

- Todo tipo de dispositivos con posibilidades de comunicación, desde electrónica de red hasta sensores de la más variada naturaleza, con soporte SNMP.

Recursos:

- Materiales.

En el caso en concreto que nos ocupa y dado que la empresa posee sucursales en varias ciudades del territorio nacional, así como asociaciones con empresas en el extranjero, se propone la instalación de al menos un servidor en la central que controlará tanto dispositivos de cliente como los sistemas internos.

Por otro lado en las sucursales se plantea el uso de un servidor por cada una de ellas que a su vez controle los equipos internos y los servicios proporcionados a clientes. Estos servidores que llamaremos satélites se comunicarán con el central para enviar puntualmente las actualizaciones del estado para ser guardadas para su posterior procesamiento y tratamiento estadístico.

En cualquier caso los avisos que se deriven de situaciones que deban ser atendidas con urgencia se enviarán directamente a los responsables a través de medios como puedan ser el correo electrónico o los SMS.

Los servidores destinados, exceptuando el principal, no necesitan tener unas prestaciones espectaculares, por lo que, en la medida que se disponga de ellos, se pueden reutilizar servidores que se hayan sustituido por haberse quedado obsoletos o hayan sido renovados.

- Humanos.

Para la puesta en marcha del proyecto se desplegarán tres equipos multidisciplinares, encargados de los diferentes aspectos necesarios para realizar las diferentes tareas encaminadas a la consecución de los objetivos propuestos.

- El primer equipo, desde nuestras oficinas, se encargará de las tareas de planificación y desarrollo para dar soporte a nuestros técnicos durante el despliegue.
- El segundo equipo se encargará de la puesta en marcha en las oficinas del cliente, tanto de los sistemas principales, como del despliegue de los primeros checks durante los cuales también se instruirá a personal del cliente para la posterior realización del despliegue en el resto de sistemas.

Bibliografía:

1. JOSEPHSEN, David. Building a Monitoring Infrastructure with Nagios. 1A edición. Prentice Hall, p. xix e xx, 2007.

2. Debian página principal del proyecto.
   http://www.debian.org/

3. Nagios página principal del proyecto.
   http://nagios.org/

4. Nagios Version 3.x Documentación. Disponible en:
   http://nagios.sourceforge.net/docs/nagios-3.pdf.

5. Nagios Exchange.
   http://exchange.nagios.org/

6. NSCA (with Nagios).
   http://nagios.sourceforge.net/download/contrib/documentation/misc/NSCA_Setu p.pdf.

7. NSCA_Win32Client.
   http://nagiosexchange.altinity.org/nagiosexchange/NSCA_Win32Client/.

8. NRPE Documentación.
   http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf

9. NDOUTILS Documentación.
   http://nagios.sourceforge.net/docs/ndoutils/NDOUtils.pdf