ANALISIS, DISEÑO E IMPLEMENTACION DE UNA SUITE DE MONITOREO A LA RED DE DATOS DE LA EMPRESA JL Y RB S.A.S- ELECTROMILLONARIA

HENRY GAVIRIA CERON
JULIÁN CAMILO PORTILLA LAGOS

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERIA
DEPARTAMENTO DE INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO
2018

ANALISIS, DISEÑO E IMPLEMENTACION DE UNA SUITE DE MONITOREO A LA RED DE DATOS DE LA EMPRESA JL Y RB S.A.S- ELECTROMILLONARIA|

HENRY GAVIRIA CERON
JULIÁN CAMILO PORTILLA LAGOS

Trabajo de Grado presentado como requisito para optar el título de Ingenieros de Sistemas

Asesor del Trabajo
Ing. EDGAR ROBERTO DULCE VILLAREAL, Esp.

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERIA
DEPARTAMENTO DE INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO
2018

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son Responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010, emanado del Honorable Consejo Académico.

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

San Juan de Pasto 19 de abril de 2018

RESUMEN

En este trabajo se hace un análisis, diseño e implementación de una suite de monitoreo a la red de datos de la empresa JL Y RB S.A.S- ELECTROMILLONARIA, con el fin de facilitar la gestión de la red de datos en tiempo real, sirviendo de apoyo en la toma de decisiones y ayudando a la disminución de costos en tiempo, procesos y dinero.

La suite de monitoreo está compuesta por cuatro herramientas. La herramienta Nagios que es el núcleo de la suite de monitoreo, este es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila sin importar el sistema operativo los equipos (hardware), servicios (software) y servicios de red (SMTP, POP3, HTTP, SNMP, ETC), alertando cuando su comportamiento no sea el deseado, la herramienta check_mk que es un maravilloso paquete de software que envuelve a Nagios complementándolo y potenciándolo. check_mk es la interface web de Nagios core, la herramienta PNP4Nagios es un módulo para Nagios que analiza los datos de rendimiento de los servicios que son monitoreados en cada componente de red y los muestra en forma gráfica y la herramienta Nagvis que es un complemento de visualización para Nagios este complemento se utiliza para visualizar la infraestructura de red mediante georeferenciación por stream maps.

En este trabajo se realizó una monitorización de los recursos de sistema hardware y software de los componentes de red, se monitoreó los servicios de red: HTTP, FTP, SSH, PROXY, DNS, OPENFIRE. En total se monitoreó 92 componentes de red y 1254 servicios. Además, se analizaron los resultados del monitoreo mediante reportes obtenidos con Nagios.

ABSTRACT

This project is an analysis, design and implementation of a monitoring suite to JL AND RB SAS- ELECTROMILLONARIA company data network, in order to facilitate the management of real-time information, serving as support in the taking of decisions and helps to reduce costs in time, processes and money.

The monitoring suite is composed of four tools. The Nagios tool that is the core of the monitoring suite, this is a widely used, open source, network monitoring system that monitors the equipment without regard to the operating system (hardware), services (software) and network services (SMTP, POP3, HTTP, SNMP, ETC), warning when its behavior is not the expected, the check_mk tool is a wonderful software package that wraps Nagios complementing and enhancing it.

check_mk is the web interface of Nagios core, the tool PNP4Nagios is a module for Nagios that analyzes the performance data of the services that are monitored in each network component and shows them in graphical form and the Nagvis tool is a visualization complement for Nagios, this add-on is used to visualize the network infrastructure through georeferencing by stream maps.

In this project a monitoring of the hardware and software system resources of the network components was performed, the network services that were monitored are: HTTP, FTP, SSH, PROXY, DNS, and OPENFIRE. In total, 92 network components and 1254 services. In addition, the monitoring results are analyzed through reports that are obtained through Nagios.

CONTENIDO

Pag.

INTRODUCCIÓN 25
1. MARCO TEÓRICO 30
1.1 REDES DE COMPUTADORES 30
1.2 SERVICIOS EN RED 30
1.2.1 Tipos de servicios. 31
1.3 TOPOLOGÍAS DE RED 36
1.3.1 Topología en árbol. 36
1.4 TIPOS DE REDES DE COMUNICACIÓN 37
1.4.1 Redes de área personal. 37
1.4.2 Redes de área local. 38
1.5 DISPOSITIVOS DE RED DE DATOS 38
1.5.1 Enrutadores. 38
1.5.2 Tarjetas de red: 40
1.5.3 Tranceiver: 41
1.5.4 Switch. 41
1.6 TRANSMISIÓN DE DATOS 42
1.7 MODELO DE REFERENCIA OSI 43
1.7.1 Capas de modelo osi capa de aplicación. 44
1.8 TCP/IP 48
1.9 PROTOCOLO IP 50
1.9.1 Clases de redes. 51
1.9.2 Máscara de subred. 52
1.9.3 Direcciones sin clase 53
1.10 GESTIÓN DE REDES 53
1.11 SNMP 55

1.11.1 SNMP como protocolo. 55
1.11.2 Arquitectura SNMP. 55
1.12 NAGIOS 57
1.12.1 Estructura de Nagios. 58
1.12.2 Requerimientos del sistema. 59
1.12.3 Licencia. 59
1.12.4 Características de Nagios. 60
1.13 CHECK_MK 61
1.13.1 Componentes del proyecto check_mk. 62
1.14 PNP4 NAGIOS 63
1.14.1 Requerimientos software: 64
1.14.2 Versiones: 64
1.15 NAGVIS 64
1.15.1 Funcionamiento general de Nagvis. 65
1.15.2 Licencia. 66
1.15.3 Requisitos del sistema. 66
1.15.4 Requisitos especiales por backends. 67
1.16 ARQUITECTURA DE UNA SOLUCIÓN DE MONITORIZACIÓN BASADA EN CHECK_MK 67
1.17 OTRAS HERRAMIENTAS DE MONITOREO 69
1.17.1 Pandora fms. 70
1.17.2 Mumin. 70
1.17.3 Zabbix. 71
1.17.4 Cacti. 71
2. OBJETIVOS 73
2.1 OBJETIVO GENERAL 73
2.2 OBJETIVOS ESPECÍFICOS 73
3. JUSTIFICACIÓN 75
4. ANTECEDENTES 77

4.1 ANTECEDENTES INTERNACIONALES 77
4.2 ANTECEDENTES NACIONALES 78
4.3 ANTECEDENTES REGIONALES 79
5. METODOLOGÍA 81
6. RESULTADOS ESPERADOS 84
7. RECURSOS 84
7.1 RECURSOS HUMANOS 85
7.2 RECURSOS TECNOLÓGICOS 86
7.3 RECURSOS MATERIALES 87
7.4 RECURSOS VARIOS 88
7.5 RECURSOS FINANCIEROS 88
7.6 RECURSOS OPERATIVOS 89
8. CRONOGRAMA 90
8.1 TABLA DE ACTIVIDADES 90
9. DESARROLLO DEL PROYECTO 99
9.1 INFORMACIÓN GENERAL DE LA EMPRESA ELECTROMILLONARIA 99
9.1.1 Misión. 99
9.1.2 Visión. 99
9.1.3 Breve historia. 99
9.1.4 Área de influencia. 100
9.1.5 Organigramas sectoriales. 111
9.2 INFORMACIÓN RECOLECTADA DE LA RED DE DATOS 123
9.3 ANÁLISIS DE LA RED DE DATOS 124
9.3.1 Análisis de los componantes de red. 124
9.3.2 Análisis de la red de datos. 139
9.4 DISEÑO LÓGICO Y FÍSICO DE LA RED DE DATOS 141
9.4.1 Diseño lógico sede principal: 142
9.4.2 Diseño lógico agencia calle 19: 143

9.4.3 Diseño lógico agencia calle 17: 143
9.4.4 Diseño lógico agencia keeway calle 17: 144
9.4.5 Diseño lógico agencia carrera 20: 145
9.4.6 Diseño lógico agencia carrerea 25: 146
9.4.7 Diseño lógico agencia keeway américas: 148
9.4.8 Diseño lógico bodega principal: 149
9.4.9 Diseño lógico agencia las lunas: 149
9.4.10 Diseño lógico sede Cali: 151
9.4.11 Diseño lógico sede Yumbo: 152
9.4.12 Diseño lógico sede Popayán: 152
9.4.13 Diseño lógico sede Tumaco: 154
9.4.14 Diseño lógico sede Mocoa: 155
9.4.15 Diagrama físico: 156
9.5 INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS DE RED EN ENTORNO VIRTUAL 157
9.6 IMPLEMENTACIÓN DE LA SUITE DE MONITOREO EN ENTORNO VIRTUAL 158
9.7 CONFIGURACIÓN DE NOTIFICACIONES EN NAGIOS Y CHECK_MK 158
9.8 MIGRACIÓN DE LA SUITE DE MONITOREO DE RED A SERVIDOR DE LA EMPRESA 159
9.8.1 Requerimientos hardware y software del servidor: 159
9.8.2 Instalación de la suite de monitoreo. 159
9.8.3 Configuración y puesta en marcha de suite de monitoreo. 160
9.8.4 Pruebas de funcionamiento de la suite de monitoreo. 178
9.8.5 Reportes de monitoreo con Nagios. 179
9.8.6 Actualización de la suite de monitoreo. 210
9.9 INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR ESPEJO 221
9.9.1 Instalación y configuración de la herramienta rsync con ssh. 221

9.10 MANUAL DE FUNCIONAMIENTO DE CHECK_MK 227
9.11 CAPACITACIÓN AL PERSONAL DEL ÁREA DE SISTEMAS..... 228
10. CONCLUSIONES 230
11. RECOMENDACIONES 232
REFERENCIAS BIBLIOGRAFICAS..... 233

LISTA DE TABLAS

Pág.

Tabla 1. Clasificación de los procesadores con base en la escala. 37
Tabla 2. Direcciones IP especiales reservadas. 52
Tabla 3. Tabla comparativa de herramientas de monitoreo de red. 69
Tabla 4. Tabla de análisis de secuencia de actividades. 82
Tabla 5. Recursos humanos 85
Tabla 6. Recursos tecnológicos 86
Tabla 7. Recursos materiales 87
Tabla 8. Recursos varios 88
Tabla 9. Recursos financieros 88
Tabla 10. Recursos operativos 89
Tabla 11. Actividades planeadas para el desarrollo del trabajo. 90

LISTA DE FIGURAS

Pág.

Figura 1. Topología en árbol. 36
Figura 2. Enrutador, dispositivo de red. 39
Figura 3. Tarjeta de red, dispositivo de red. 40
Figura 4. Tranceiver, dispositivo de red. 41
Figura 5. Switch, dispositivo de red. 41
Figura 6. Comportamiento de paquetes de datos en modelo OSI en emisor y receptor. 44
Figura 7. Pila de protocolos TCP/IP. 49
Figura 8. Representación en byte de red clase C. 51
Figura 9. Arquitectura en bloques de SNMP v3. 56
Figura 10. Estructura general de Nagios. 58
Figura 11. Arquitectura integrada Nagios, nagvis, check_mk, pnp4. 68
Figura 12. Diagrama de secuencia de actividades. 83
Figura 13. Mapa regiona de Nariño, ubicación de tiendas. 101
Figura 14. Mapa regional Valle del Cauca, ubicación de tiendas. 105
Figura 15. Mapa regional de Putumayo, ubicación de tiendas. 107
Figura 16. Mapa regional Cauca, ubicación de tiendas. 109
Figura 17. Organigrama sede administrativa. 113
Figura 18. Organigrama regional Nariño. 116
Figura 19. Organigrama INTERELEC. 117
Figura 20. Organigrama KEEWAY central. 118
Figura 21. Organigrama regional Valle. 121
Figura 22. Organigrama regional Cauca. 122
Figura 23. Organigrama regional Putumayo. 123
Figura 24. Gabinete de servidores, azkaban, voldemort, slytherin, gryffindor. 125
Figura 25. Switches sede principal. 125
Figura 26. Dispositivo de aire acondicionado cuarto de servidores. 126
Figura 27. Switches segundo piso. 126
Figura 28. Router principal y switches segundo piso. 127
Figura 29. Switches cuarto piso. 127
Figura 30. Switches de 24 puertos. 128
Figura 31. UPS servidores principales. 128
Figura 32. Gabinete switches calle 19. 129

Figura 33. Servidor respaldo calle 19. 129
Figura 34. Switch tres antenas tp-link, agencia principal tercer piso. 130
Figura 35. Antena con radioenlaces Ubiquiti. 130
Figura 36. Cuatro radioenlaces ubiquiti. 131
Figura 37. Router tp-link 8 puertos, agencia carrera 25. 131
Figura 38. Router ARRIS 4 puertos, agencia carrera 20. 132
Figura 39. Router OFFCOM 4 puertos, agencia las americas. 132
Figura 40. Switch tp-link 4 puertos, área de cartera sede principal. 133
Figura 41. Impresora EPSON L380, sede keeway las americas. 133
Figura 42. Impresora HP hp1460, sede calle 19. 134
Figura 43. Impresora KYICERA FS-1325MFP, sede principal. 134
Figura 44. Punto de red de datos, sede principal. 135
Figura 45. Punto de red da datos y de voz, agencia principal. 135
Figura 46. Terminal tonta HP agencia carrera 20. 136
Figura 47. Computador área interelec sede principal. 136
Figura 48. Computador área interelec sede principal. 137
Figura 49. Portátil área ventas sede principal. 137
Figura 50. Computador área cartera sede principal. 138
Figura 51. Computador área jurídico sede principal. 138
Figura 52. Cable de datos y de voz área interelec sede principal. 139
Figura 53. Diseño lógico de sede principal Pasto. 142
Figura 54. Diagrama lógico agencia calle 19 Pasto. 143
Figura 55. Diagrama lógico agencia calle 17 Pasto. 144
Figura 56. Diagrama lógico agencia calle 19 Pasto. 145
Figura 57. Diagrama lógico agencia carrera 20 Pasto. 146
Figura 58. Diagrama lógico agencia carrera 25 Pasto. 147
Figura 59. Diagrama lógico agencia keeway las americas Pasto. 148
Figura 60. Diagrama lógico bodega principal Pasto. 149
Figura 61. Diagrama lógico agencia las lunas Pasto. 150
Figura 62. Diagrama lógico sede Cali. 151
Figura 63. Diagrama lógico sede Yumbo. 152
Figura 64. Diagrama lógico sede Popayán. 153
Figura 65. Diagrama lógico sede Tumaco. 154
Figura 66. Diagrama lógico sede Mocoa. 155
Figura 67. Diagrama físico red de datos. 156
Figura 68. Archivos del directorio objects de Nagios. 160
Figura 69. Definición de archivo servicios.cfg en archivo nagios.cfg. 160

LISTA DE FIGURAS DEFINICIÓN DE HOST

Pág.

Figura DH 1. Plataforma de administración WATO, creación de host. 161
Figura DH 2. Plataforma de administración WATO, creación de host. 162
Figura DH 3. Plataforma de administración WATO, creación de host. 162
Figura DH 4. Plataforma de administración WATO, creación de host. 163
Figura DH 5. Plataforma de administración WATO, creación de host. 163
Figura DH 6. Plataforma de administración WATO, creación de host. 164
Figura DH 7. Plataforma de administración WATO, creación de host. 164
Figura DH 8. Plataforma de administración WATO, creación de host. 165
Figura DH 9. Plataforma de administración WATO, creación de host 165

LISTA DE FIGURAS DEFINICIÓN DE IMPRESORAS

Pág.

Figura DI 1. Plataforma de administración WATO, creación de impresora. 166
Figura DI 2. Plataforma de administración WATO, creación de impresora. 167
Figura DI 3. Plataforma de administración WATO, creación de impresora. 168
Figura DI 4. Plataforma de administración WATO, creación de impresora. 168
Figura DI 5. Plataforma de administración WATO, creación de impresora. 169
Figura DI 6. Plataforma de administración WATO, creación de impresora. 169
Figura DI 7. Plataforma de administración WATO, creación de impresora. 170
Figura DI 8. Plataforma de administración WATO, creación de impresora. 170
Figura DI 9. Plataforma de administración WATO, creación de impresora. 171

LISTA DE FIGURAS DEFINICIÓN DE RADIO ENLACES

Pág.

Figura DRE 1. Plataforma de administración WATO, creación de radio enlace. . 172
Figura DRE 2. Plataforma de administración WATO, creación de radio enlace. . 172
Figura DRE 3. Plataforma de administración WATO, creación de radio enlace. . 173
Figura DRE 4. Plataforma de administración WATO, creación de radio enlace. . 173
Figura DRE 5. Plataforma de administración WATO, creación de radio enlace. . 174
Figura DRE 6. Plataforma de administración WATO, creación de radio enlace. . 174
Figura DRE 7. Plataforma de administración WATO, creación de radio enlace. . 175
Figura DRE 8. Plataforma de administración WATO, creación de radio enlace. . 175
Figura DRE 9. Plataforma de administración WATO, creación de radio enlace. . 176

LISTA DE FIGURAS CREACION DE REPORTES

Pág.

Figura CR 1. Creación de reportes de disponibilidad en Nagios. 180
Figura CR 2. Creación de reportes de disponibilidad en Nagios. 181
Figura CR 3. Creación de reportes de disponibilidad en Nagios. 181
Figura CR 4. Creación de reportes de disponibilidad en Nagios. 182
Figura CR 5. Creación de reportes de disponibilidad en Nagios. 183
Figura CR 6. Creación de reportes de disponibilidad en Nagios. 184
Figura CR 7. Creación de reportes de disponibilidad en Nagios. 184
Figura CR 8. Creación de reportes de disponibilidad en Nagios. 185
Figura CR 9. Creación de reportes de disponibilidad en Nagios. 186
Figura CR 10. Creación de reportes de disponibilidad en Nagios. 187
Figura CR 11. Creación de reportes de disponibilidad en Nagios. 188
Figura CR 12. Creación de reportes de disponibilidad en Nagios. 188
Figura CR 13. Creación de reportes de disponibilidad en Nagios. 189
Figura CR 14. Creación de reportes de disponibilidad en Nagios. 190
Figura CR 15. Creación de reportes de disponibilidad en Nagios. 191
Figura CR 16. Grafica de historial de estado de servidor voldemort. 192
Figura CR 17. Gráfica de historial de estado de servidor azkaban.....192
Figura CR 18. Resultados de historial de alertas de todos los host y servicios...193
Figura CR 19. Resumen de las utimas 25 alertas generadas por Nagios. 194
Figura CR 20. Gráfico de frecuencia de alertas de host y servicios del servidor voldemort. 195
Figura CR 21. Gráfico de frecuencia de alertas de host y servicios del servidor azkaban. 196
Figura CR 22. Reporte de notificaciones de host y servicios a contactos. 197
Figura CR 23. Reporte de servicios de eventos Nagios. 197
Figura CR 24. Gráfica, tiempo de equipos en estado UP, mes de enero 2018. ..199
Figura CR 25. Gráfica, tiempo de equipos en estado UP, mes de enero 2018. ..200
Figura CR 26. Estado OK de servicios en servidor azkaban en el mes de enero de 2018. R 202
Figura CR 27. Estado CRITICAL de servicios en servidor azkaban en el mes de enero de 2018. 203
Figura CR 28. Estado OK de servicios en servidor voldemort en el mes de enero de 2018. 205

Figura CR 29. Estado WARNING de servicios en servidor voldemort en el mes de enero de 2018. 206
Figura CR 30. Estado UNKNOWN de servicios en servidor voldemort en el mes de enero de 2018. 207
Figura CR 31. Estado CRITICAL de servicios en servidor voldemort en el mes de enero de 2018. 208
Figura CR 32. Estado CRITICAL de servicios en servidor voldemort en el mes de enero de 2018. 209

LISTA DE FIGURAS ACTUALIZACION CHECK_MK

Pág.

Figura ACH 1. Definición de rutas de instalación. 211
Figura ACH 2. Definición de rutas de instalación. 212
Figura ACH 3. Definición de rutas de instalación. 212
Figura ACH 4. Definición de rutas de instalación. 213
Figura ACH 5. Definición de rutas de instalación 214
Figura ACH 6. Definición de rutas de instalación. 215
Figura ACH 7. Definición de rutas de instalación. 216
Figura ACH 8. Definición de rutas de instalación. 217
Figura ACH 9. Definición de rutas de instalación 218
Figura ACH 10. Definición de rutas de instalación. 219

LISTA DE FIGURAS CAPACITACION PERSONAL DE SISTEMAS ELECTROMILLONARIA

Pág.

Figura CP 1. Imagen capacitación a personal del área de sistemas. 228
Figura CP 2. Imagen capacitación a personal del área de sistemas 229
Figura CP 3. Imagen capacitación a personal del área de sistemas. 229
Figura CP 4. Imagen capacitación a personal del área de sistemas. 230

LISTA DE ANEXOS

Pág.

Anexo A. Información de equipos. 239
Anexo B. Analisis de la red de datos. 273
Anexo C. Resultado acotado de análisis con herramienta Wireshark. 297
Anexo D. Instalación y configuración servidor DNS bind9..... 303
Anexo E. Instalación y configuración de servidor web Apache. 316
Anexo F. Instalación y configuración de servidor proxy SQUID. 329
Anexo G. Instalación y configuración de servidor ftp..... 339
Anexo H. Instalación y configuración de servidor ssh. 346
Anexo I. Instalación y configuración de servidor chat OPEN FIRE..... 370
Anexo J. Instalación y configuración de servidor de correo postfix. 400
Anexo K. Implementación de la suite de monitoreo en entorno virtual. 419
Anexo L. Dedifinición de servicios públicos y privados en Nagios..... 535
Anexo N. Funcionamiento de suite de monitoreo..... 572
Anexo O. Resultados de reporte Nagios Availability Host Groups. 606
Anexo P. Resultados de reporte Nagios Availability Individual Host. 610
Anexo Q. Resultados de reporte en archivo .cvs avail individual all hots. 612
Anexo R. Resultados de reporte en archivo .cvs avail all service servidores Azkaban y Voldemort..... 620
Anexo S. Manual Check_MK. 627
Anexo T. Acta de capacitación personal área de sistemas. 665
Anexo U. Carta de satisfacción por realización del trabajo. 667

GLOSARIO

Análisis de red: proceso donde se examina el estado de la red existente, incluyendo los problemas que podría tener, evalúa flujos de tráfico, así como también el mapeo de usuarios, aplicaciones y dispositivos, de esta manera se recopila información para las etapas de arquitectura y diseño.

Diseño físico: diagrama que muestra la disposición física real de los componentes que forman la red, incluidos cables y hardware. Ofrece una vista panorámica de la red en su espacio físico, como un plano de planta.

Diseño lógico: diagrama que describe la forma en que la información fluye a través de una red, muestra subredes (incluidas direcciones, máscaras e ID de VLAN), dispositivos de red, como enrutadores y cortafuegos, y protocolos de enrutamiento.

Georeferenciación: posicionamiento espacial de un cuerpo en una localización geográfica de acuerdo a un sistema de coordenadas y a datos específicos.

Gestión de red: proceso que consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.

Monitoreo de red: uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico u otras alarmas.

Plugin: aplicación que, en un programa informático, añade una funcionalidad adicional o una nueva característica al software.

Protocolo de red: sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física.

Puertos de Internet: valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host, o puesto de trabajo.

Red de datos: infraestructura o rede de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.

Servicios de red: aplicaciones especiales que permiten a las computadoras en red compartir recursos.

Servidor: aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Servidor espejo: servidor que contiene una réplica exacta de otro.

Suite: conjunto de programas (software) que permiten realizar distintas tareas comunes referentes a lo laboral.

Virtualización: creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

INTRODUCCIÓN

En la actualidad, gracias a la aparición de la red internet y su fácil disposición, las empresas han optado por aprovechar sus beneficios, implementando herramientas y servicios con el fin de suplir la demanda que existe en el mercado. Varias empresas han logrado expandir sus servicios a través de sucursales en distintos sectores y ciudades, incluso han logrado internacionalizarse gracias a la implementación de redes de datos, por tal motivo tienen un mayor nivel de competitividad logrando agilizar sus procesos.

De acuerdo con lo anterior, se resalta la importancia que tienen las redes de datos en las empresas debido a los servicios que brindan cuando es necesario la comunicación entre sucursales que tienen un propósito en común. Las redes tienen como objetivo la transmisión de datos, además de compartir servicios entre los equipos que estén dentro de la red. Dichas redes se componen de diferentes dispositivos y servicios, por ejemplo, routers, switches, impresoras, servidores, terminales brutas, servicios de internet, entre otros. Por tal motivo es indispensable que exista una gestión de la red que de soporte y responda a un problema oportunamente, para que el sistema no se afecte y las empresas estén disponibles para ofrecer sus servicios en cualquier momento.

Existen muchas plataformas que se encargan de la gestión de redes de datos, entre las más utilizadas se encuentran: Nagios, Zabbix, Cacti, Pandora y Munin. Algunas plataformas son más utilizadas que otras, dependiendo de la facilidad de uso, de los servicios que prestan y de las necesidades particulares de cada empresa, por tal razón se plantea la propuesta del trabajo titulado: análisis, diseño e implementación de una plataforma de monitoreo de la red de datos de la empresa JL Y RB S.A.S- ELECTROMILLONARIA DE LA CIUDAD DE PASTO, la cual es la sede principal de operación y administración de la empresa mencionada. La plataforma que se utilizará es Nagios puesto que se acomoda a las necesidades actuales de la empresa y es una de las más completas al momento de realizar la gestión de una red de datos.

A continuación, se da a conocer el contenido del trabajo realizado. Se presenta el alcance, descripción del problema, marco teórico, objetivos, justificación, antecedentes, metodología, resultados esperados, y posteriormente su ejecución.

TEMA

Título

ANALISIS, DISEÑO E IMPLEMENTACION DE UNA SUITE DE MONITOREO A LA RED DE DATOS DE LA EMPRESA JL Y RB S.A.S – ELECTROMILLONARIA.

Modalidad

El trabajo se desarrolló mediante la modalidad de aplicación complementado con parte de investigación, para poder alcanzar los objetivos propuestos y mejorar la calidad del trabajo, esta modalidad está estipulada por la facultad de Ingeniería de la Universidad de Nariño.

Linea de linvestigación

El trabajo de grado, se encuentra bajo la línea gestión, seguridad y control, enmarcada dentro del tema Telemática específicamente en el proceso de gestión de redes de datos.

Alcance y delimitaciones

Se realizó el análisis de la red de datos junto con el diseño lógico y físico, y se implementará una suite de monitoreo.

La suite de monitoreo de red de datos compuesta por las herramientas Nagios, Check_MK, Nagvis y PNP4Nagios es una suite, la cual se encarga de monitorear equipos (Hardware), servicios (Software) y servicios de red, según se especifiquen en la configuración. Esta gestión se lleva a cabo en tiempo real lo que permite que haya un control continuo de la red, dando como beneficio la prevención de fallos, mejorando la administración y facilitando el trabajo al administrador del sistema. La suite de monitoreo cuenta con una interface web amigable la cual muestra el estado de la red de datos presentada de forma clara, precisa y dinámica, la cual contribuye a la toma de decisiones, llevando a la empresa a mejoras en cuanto a inversión disminuyendo gastos y mejorando la disponibilidad de los servicios que esta presta.

La suite de monitoreo se instaló en un servidor de la sede principal de la empresa JL Y RB S.A.S- ELECTROMILLONARIA, ubicada en la Ciudad de Pasto; con dicha suite se monitoreó todos los componentes de la red de datos de la sede principal (todos los equipos de las áreas que componen la sede principal de la empresa, servidores de terminales, impresoras multifuncionales, radio enlaces), además de los servidores que tienen instalados los servicios: WEB, PROXY, SSH, DNS, OPENFIRE, FTP. Además, en las agencias de la Ciudad de Pasto que funcionan

con servidor de terminales se monitoreó dichos servidores y en aquellas agencias que funcionan con radio enlaces se monitorearon todos los equipos de dicha sede, incluyendo su radio enlace. En total se monitoreará 9 agencias en la Ciudad de Pasto.

Debido a que la empresa JL Y RB S.A.S- ELECTROMILLONARIA cuenta con sedes en los departamentos del Suroccidente Colombiano se monitoreó un equipo principal de las sedes: Tumaco, Mocoa, Popayán, Yumbo y Cali, dejando abierta la posibilidad de adaptar el monitoreo a las demás sedes de los departamentos, incluyendo los equipos que el administrador de la red de datos desee conveniente según la necesidad de la empresa, ya que al estar en funcionamiento la suite de monitoreo facilita adaptar nuevos equipos que estén dentro de la red sin importar su ubicación.

La implementación de la suite de monitoreo cuenta con un servicio de seguridad compuesto por el uso del protocolo (SSL) y un método de restricción de acceso por IP, esta seguridad se configura en Apache. Esto se hace debido a la importancia de la empresa donde se realizo el trabajo. Además, se realizó una réplica espejo de la configuración de la suite de monitoreo en un equipo (computador), diferente dentro de la empresa para que el servicio siempre se encuentre disponible en caso de fallar el servidor principal, complementando la réplica se dará a conocer la forma de obtener backups de configuración con la herramienta de administración de Nagios llamada Check_MK.

Una de las particularidades de Nagios es que permite emitir notificaciones cuando algo no anda bien dentro de la red, esto lo hace a través de correos electrónicos, ventaja que es utilizada en el trabajo para que el jefe de sistemas de la empresa reciba dichas notificaciones, teniendo así una herramienta de apoyo que facilite su trabajo. Además, se realizaron reportes del monitoreo con las opciones que permite Nagios.

Cabe resaltar que toda configuración que se realizó dentro de la suite de monitoreo se hizo conforme con necesidades de la empresa teniendo en cuenta las limitaciones que esta tiene, siempre buscando optimizar procesos y no afectar su buen funcionamiento.

DESCRIPCIÓN DEL PROBLEMA

Planteamiento del problema

La empresa JL Y RB S.A.S- ELECTROMILLONARIA presta sus servicios en los departamentos de: Nariño, Putumayo, Cauca y Valle del Cauca. En el departamento de Nariño en San Juan de Pasto, Ipiales, Tumaco, Túquerres, la Unión y Sandoná.

En la ciudad de San Juan de Pasto se encuentra su sede principal con dirección Calle 19 # 26- 58 Centro, además de 9 agencias.
La empresa JL Y RB S.A.S- ELECTROMILLONARIA enlaza sus agencias a través de la red de datos administrada desde la sede principal, utilizando el servicio VPN y un medio de transmisión de radio enlace.

Debido a la arquitectura de conexión de la red de datos de la empresa se encontraron múltiples problemas que afectan el óptimo funcionamiento de los procesos internos dentro de la empresa, tales como:

- La empresa no dispone de una bitácora de almacenamiento de los antecedentes de problemas presentados en la red de datos, debido a lo anterior se hace muy difícil realizar planes de contingencia preventivos que permitan una toma de decisiones adecuada al momento de dar solución a un problema futuro.
- Dentro de la empresa no se cuenta con una plataforma de monitorio de la red de datos, por tal motivo no hay un seguimiento en tiempo real de los fallos que se presentan continuamente, ocasionando conflictos como cuellos de botella en el flujo de datos.
- La empresa no cuenta con los diagramas lógico y físico de la red de datos, lo cual hace que la gestión y administración de la red sea complicada y no se pueda dar solución oportuna a problemas presentados inesperadamente al momento de estar prestando el servicio de transferencia de datos.
- En la empresa no es posible visualizar de forma gráfica toda la red de datos lo cual complica la localización de fallos que es de gran importancia para detectar las causas de dicho fallo y dar soluciones oportunas.
- La empresa depende en gran medida de la disponibilidad de la red de datos, por tal motivo cuando hay problemas en cuanto a conexión en alguna (s) sucursal (es) el problema no se soluciona sino hasta cuando el administrador de la red es informado de la situación, lo cual hace que los procesos de la empresa se retrasen.
- Debido al crecimiento de la empresa en cuanto a su infraestructura tecnológica es necesaria la adquisición continua de elementos que suplan las nuevas necesidades, la empresa carece de un sistema de registro de hardware que permita llevar un monitoreo continuo del estado actual de dichos elementos, lo cual conlleva a sobrecostos y gastos innecesarios al momento de hacer escalable la nueva infraestructura.

Con base en lo anterior se planteó el análisis, diseño e implementación de una suite de monitoreo a la red de datos que permitió dar solución a los problemas anteriormente mencionados.

Formulación del problema

¿La implementación de una suite de monitoreo de redes de datos en tiempo real logrará mejorar y facilitar la gestión de la red de datos de la empresa JL Y RB S.A.S-ELECTROMILLONARIA?

1. MARCO TEÓRICO

1.1 REDES DE COMPUTADORES

Una red es un conjunto de dispositivos, computadores u otros equipos informáticos, (a menudo denominados nodos) conectados por enlaces de un medio físico, con la finalidad de compartir información y recursos. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red.

Según el blog educativo a través de la compartición de información y recursos en una red, los usuarios de los sistemas informáticos de una organización podrán hacer un mejor uso de los mismos, mejorando de este modo el rendimiento global de la organización.

Dentro de una organización una red de computadores trae consigo una serie de ventajas como:

- Mayor facilidad en la comunicación entre usuarios.
- Reducción en el presupuesto para software.
- Reducción en el presupuesto para hardware
- Posibilidad de organizar grupos de trabajo.
- Mejoras en la administración de los equipos y programas.
- Mejoras en la integridad de los datos.
- Mayor seguridad para acceder a la información.

Para tener acceso a todas estas ventajas, dentro de la red de computadoras es necesario que existan los denominados servicios en red.

1.2 SERVICIOS EN RED

Se podría denominar a un servicio en red, como la creación de una red de trabajo en un computador, dentro de una red de computadores para satisfacer las necesidades de los usuarios.

Para tener mayor claridad sobre los servicios de red, a continuación, se describirá los tipos:

- Administración y configuración: este tipo de servicios facilitan tanto la configuración como la administración de los equipos dentro de la red de datos.
- Acceso: este tipo de servicio se encarga de permitir la conexión de usuarios a la red, desde lugares remotos.

- Ficheros: se encarga de ofrecer a la red capacidad de almacenamiento, descarga, eliminación, de ficheros en una red de computadores.
- Impresión: este servicio de red permite compartir impresoras en una red de computadores.
- Información: son los encargados del almacenamiento de las bases de datos, en los cuales los usuarios de la red pueden realizar consultas dentro de las bases de datos o de otro tipo de información, como por ejemplo documentos de hipertexto.
- Comunicación: este tipo de servicio se encarga de permitir la comunicación entre los usuarios a través de diferentes herramientas de comunicación (mensajería, video llamada, vozip.) entre otros.

1.2.1 Tipos de servicios. Servicio de nombres de dominio (dns): según Mifsud Talón & Lerma Blasco[1], este servicio gestiona y mantiene de forma distribuida las direcciones de Internet y los nombres de sistema. Se trata de un servicio de búsqueda de direcciones IP y de nombres de ordenadores para una red TCP/IP. El servicio DNS escucha por los puertos 53, tanto UDP como TCP.

En una red TCP/IP, las máquinas se identifican mediante su dirección de red o numero IP. Sin embargo, para las personas resulta mucho más sencillo recordar un nombre que se asocia a una máquina concreta. También es más fiable, ya que la dirección IP puede cambiar, pero no así el nombre. El procedimiento requiere un mecanismo que traduzca los nombres de las maquinas a direcciones IP. El DNS permite que esta tarea se lleve a cabo. Existen varias aplicaciones (paquetes), utilizados para poner en marcha el servicio DNS, la más conocida y utilizada en Internet es BIND.

Servicio de acceso y control remoto: de acuerdo a lo encontrado en Mifsud Talón & Lerma Blasco[2], los servicios de acceso y control remotos permiten, mediante la utilización de determinadas aplicaciones software, establecer conexiones con equipos a distancia y administrarlos de manera centralizada sin necesidad de acceder a ellos. Utiliza por defecto el puerto 22 TCP.

En el caso de que se disponga de equipos que no tienen teclado o pantalla, o bien de servidores apilados en un rack o que no estén físicamente presentes, es muy importante contar con mecanismos que permitan administrarlos remotamente de forma cómoda, rápida y segura.

Sin embargo, hay que tener mucho cuidado al momento de implementar este servicio ya que, si no se lleva a cabo condiciones de seguridad bien definidas,

[1] Mifsud Talón, E., & Lerma Blasco, R. (01 de Abril de 2013). Servicios en red. Mexico D.F, Mexico.

[2] Ibid.

cualquier brecha de seguridad que presenten dichas herramientas hacen vulnerable el acceso a terceros no deseados pudiendo tener acceso a información confidencial. SSH (Secure Shell) es una herramienta que permite establecer conexiones seguras entre equipos conectados mediante una red insegura como puede ser, por ejemplo, Internet. Ha sido desarrollado para establecer conexiones remotas y transmitir de manera segura cualquier tipo de datos como archivos y contraseñas, así como la ejecución de órdenes de administración en un sistema remoto, sesiones de login, sesiones gráficas, entre otras.

Sin embargo, su aportación más importante es el soporte seguro que da a cualquier protocolo que funcione sobre TCP y que se basa en la utilización de mecanismos de criptografía, de forma que toda transmisión de información este cifrada y el mecanismo de autenticación del usuario sea transparente.

Servicio http: tomando como referencia a Mifsud Talón & Lerma Blasco[3], las siglas HTTP corresponden al Protocolo de Transferencia de Hipertexto (HiperText Transfer Protocol), creado en 1990 en el CERN (Laboratorio Europeo de Física de las Partículas) como un medio para compartir datos científicos a escala internacional de una manera rápida u con coste moderado. Es el método más común de intercambio de información en la World Wide Web, por el cual se transfieren las páginas web o HTML a un ordenador. El hipertexto no es más que el contenido de las páginas web o HTML a un ordenador.

Existe una versión segura de HTTP llamada HTTPS, la primera escucha por el puerto 80 TCP, la segunda escucha por el puerto 443 TCP, esta última permite el uso de cualquier método de cifrado siempre que lo compartan el servidor y el cliente. Basta con agregar uno componentes a los equipos para que ejecuten el algoritmo correspondiente de encriptación.

HTTP es un protocolo cliente-servidor cuyo funcionamiento está basado en el envió de mensaje. Su mecanismo es el siguiente:

- El usuario especifica en el cliente web (o navegador) la dirección de la página web que quiere consultar según un formato http://direccion[:puerto][path.
- El cliente web descodifica la información de la URL diferenciando el protocolo de acceso, la IP o nombre de dominio del servidor, el puerto, entre otro.
- El cliente web establece una conexión (socket) con el servidor web y solicita la página (mensaje request).
- El servidor envía dicha página (si no existe, envía un código de error) u el cliente web interpreta el código HTML recibido (mensaje response del servidor).
- Se cierra la conexión.

[3] Ibid.

Servicio ftp: según Mifsud Talón & Lerma Blasco[4], el servicio FTP o protocolo de transferencia de archivos proporciona un mecanismo estándar de transferencia de archivos entre sistemas a través de redes TCP/IP.

Para utilizar FTP, se necesita disponer de una cuenta en la máquina que va a recibir o enviar los archivos, aunque numerosos servidores FTP en Internet permiten el uso de sus sistemas utilizando una cuenta anónima (anonymus).

De igual manera que HTTP, FTP es un servicio basado en la arquitectura cliente-servidor. Su funcionamiento se describe a continuación:

Un servidor FTP conectado a la red (ya sea local o en Internet) proporciona el servicio a través de dos puertos bien conocidos:

- El puerto 20, para la trasferencia de datos.
- El puerto 21, para la transferencia de ordenes (control).

El cliente se conecta al servidor haciendo uso de un puerto local (origen) mayor que 1024 y tomando como puerto destino el puerto 21 del servidor. Una vez se ha establecido la conexión ya se puede hacer uso de las órdenes especificas FTP de manejo de archivos y directorios remotos.

Servivio de correo electrónico: para Mifsud Talón & Lerma Blasco[5], el funcionamiento del correo electrónico (e-mail) es muy similar al postal, pero trasladado y adaptado al mundo virtual. Los mensajes digitales pueden considerarse una transposición de las cartas escritas a papel. La diferencia radica en que correo electrónico se hace a través de las conexiones que establecen los usuarios en la red, sin necesidad de que estén conectados simultáneamente, en ambos casos, el mensaje llega al destinatario si la dirección es correcta.

Los elementos básicos del servicio de correo electrónico, son los siguientes:

- Buzón de usuario: espacio donde se almacenan los mensajes en el servidor que estará asociado a una cuenta de correo que hará de identificador.
- Cuentas de correo: elemento identificador de una cuenta de correo que tiene un buzón asociado. Por ejemplo, **cuenta_corre@electro.com**.
- Cuentas de correo redirigidas: cuentas, de correo sin buzón, a las que se asocia una cuenta correo de otro dominio, donde se envía cada mensaje que recibe. Por ejemplo, **cuenta_correo@electro.co**, puede estar redirigida al anterior.

---

[4] Ibid.

[5] Ibid.

- Alias: su función es similar a la de la cuenta de correo redirigida cuando se trabaja en el mismo dominio, tanto para esta como para la cuenta normal. Por ejemplo, **alias@electro.como** reenvía a **cuenta_correo@electro.com**.

Los protocolos de correo electrónico más utilizados son el SMTP que utiliza el puerto 25 TCP, POP utiliza los puertos 110 y 995 TCP, e IMAP utiliza los puertos 143 y 993 TCP, aunque existen otros, como el X.400, basado en el modelo OSI.

Servicio proxy: un servicio proxy está dado por un sistema informático que se encuentra entre el cliente que solicita un documento web y el servidor de destino (otro sistema informático) que sirve el documento. Soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet, además, protocolos ICP, HTCP, CARP y caché digests que tienen como objetivo permitir a un proxy preguntar a otros cachés si tienen almacenado un recurso determinado. En su forma más simple, un servidor proxy facilita la comunicación entre el cliente y el servidor de destino sin modificar solicitudes o respuestas.

En formularios avanzados, un servidor proxy puede filtrar peticiones basadas en varias reglas y puede permitir la comunicación sólo cuando las solicitudes se pueden validar con las reglas disponibles. Las reglas generalmente se basan en una dirección IP de un cliente o servidor de destino, protocolo, tipo de contenido de documentos web, tipo de contenido web, entre otros.

Los clientes no pueden hacer solicitudes directas a los servidores web. Facilita la comunicación entre clientes y servidores web.

A veces, un servidor proxy puede modificar peticiones o respuestas, o incluso puede almacenar las respuestas del servidor de destino localmente para cumplir la misma solicitud del mismo u otros clientes en una etapa posterior. El almacenamiento en caché es utilizado por los servidores proxy para ahorrar ancho de banda, potenciar los servidores web y mejorar la experiencia de navegación del usuario final.

Los servidores proxy se implementan principalmente para realizar lo siguiente:

- Reducir el uso de ancho de banda.
- Mejorar la experiencia de navegación del usuario al reducir el tiempo de carga de la página, lo que, a su vez, se logra almacenando en caché los documentos web.
- Aplicar políticas de acceso a la red.
- Supervisión del tráfico de usuarios o informes de uso de Internet para usuarios o grupos individuales.
- Mejorar la privacidad del usuario al no exponer la máquina de un usuario directamente a Internet.

- Distribuir la carga entre diferentes servidores web para reducir la carga en un solo servidor.
- Habilitar un servidor web de bajo rendimiento.
- Filtrar solicitudes o respuestas utilizando un sistema integrado de detección de virus / malware.
- Carga de equilibrio del tráfico de red a través de múltiples conexiones a Internet.
- Retransmitir tráfico alrededor de una red de área local.

Servicio de mensajeria instantánea: tomando como referencia a Primo Guijarro[6], el servicio de mensajería instantánea permite la comunicación entre dos o más personas basada en texto. Para esto requiere el uso de un cliente de mensajería instantánea que realiza el servicio y se diferencia del correo electrónico en que las conversaciones se realizan en tiempo real. La mayoría de los servicios ofrecen el "aviso de presencia", indicando cuando el cliente de una persona en la lista de contactos se conecta o en qué estado se encuentra, si está disponible para tener una conversación. En los primeros programas de mensajería instantánea, cada letra era enviada según se escribía y así, las correcciones de las erratas también se veían en tiempo real. Esto daba a las conversaciones más la sensación de una conversación telefónica que un intercambio de texto. En los programas actuales, habitualmente, se envía cada frase de texto al terminarse de escribir. Además, en algunos, también se permite dejar mensajes, aunque la otra parte no esté conectada al estilo de un contestador automático. Otra función que tienen muchos servicios es el envío de ficheros. La mayoría usan redes propietarias de los diferentes softwares que ofrecen este servicio. Adicionalmente, hay programas de mensajería instantánea que utilizan el protocolo abierto XMPP, con un conjunto descentralizado de servidores. Los clientes de mensajería instantánea más utilizados son ICQ, Yahoo! Messenger, Windows Live Messenger, Pidgin, AIM (AOL Instant Messenger) y Google Talk (que usa el protocolo abierto XMPP). Estos servicios han heredado algunas ideas del viejo, aunque aún popular, sistema de conversación IRC. Cada uno de estos mensajeros permite enviar y recibir mensajes de otros usuarios usando los mismos software clientes, sin embargo, últimamente han aparecido algunos clientes de mensajerías que ofrecen la posibilidad de conectarse a varias redes al mismo tiempo (aunque necesitan registrar usuario distinto en cada una de ellas). También existen programas que ofrecen la posibilidad de conectarte a varias cuentas de usuario a la vez como aMSN.

Para llevar a cabo el servicio de mensajería instantánea existen varios protocolos que se utilizan, entre los más utilizados están, Skype y SIP, IRC (Internet Relay Chat), OSCAR (Open System for Communication in Realtime) y XMPP.

---

[6] Primo Guijarro, Á. (2012 de Febrero de 23). Servcios de mensajería instantanea. Ciudad Real, España.

1.3 TOPOLOGÍAS DE RED

Según en términos de una red de comunicaciones topología se refiere a la forma como se interconectan entre sí los puntos finales, o estaciones, conectados a una red.

1.3.1 Topología en árbol. Esta topología es una generalización de la topología en bus. El medio de transmisión es un cable ramificado sin bucles cerrados que comienza en un punto conocido como raíz o cabecera. Uno o más cables comienzan en el punto raíz y cada uno de ellos puede presentar ramificaciones. Las ramas pueden disponer de ramas adicionales, dando lugar a esquemas más complejos. La transmisión en este tipo de tipología se da desde una estación que se propaga a través del medio y puede alcanzar al resto de estaciones. Este tipo de disposición presenta dos problemas. En primer lugar, dado que la transmisión desde una estación se puede recibir en las demás estaciones, es necesario algún método para indicar a quién va dirigida la transmisión. En segundo lugar, se precisa un mecanismo para regular la transmisión, ya que, si dos estaciones intentan transmitir simultáneamente, sus señales se superpondrán y serán erróneas, como también se puede dar el caso en que una estación quiere transmitir durante un largo lapso de tiempo. Para dar solución a estos dos problemas las estaciones transmiten datos en bloques pequeños llamados tramas[7].



Figura 1. Topología en árbol.
Fuente. (FITEC Institucion de educacion superior, 2017)

[7] Stallings, W. (2008). Comunicaciones y Redes de Computadores. Madrid (España): Pearson Educacion, S.A.

1.4 TIPOS DE REDES DE COMUNICACIÓN

Se tiene un criterio alterativo para clasificar las redes, el cual es por su escala. La distancia es una medida importante como medida de clasificación, debido a que las distancias tecnológicas se utilizan a diferentes escalas.

Tal como lo hace Tanenbaum & Wetherall, en la tabla 1, se clasifica los tipos de redes según su distancia y la ubicación de los procesadores.

Tabla 1. Clasificación de los procesadores con base en la escala.

DISTANCIA ENTRE PROCESADORES	PROCESADORES UBICADOS EN EL (LA) MISMO (A)	TIPO DE RED
1 m	Metro cuadrado	Red de área personal
10 m	Cuarto	Red de área local
100 m	Edificio	Red de área local
1 km	Campus	Red de área local
10 Km	Ciudad	Red de área metropolitana
100 km	País	Red de área amplia
1000 km	Continente	Red de área amplia
10000 km	Planeta	Interred

Fuente. (Tanenbaum & Wetherall, 2012)

1.4.1 Redes de área personal. Generalmente, llamadas PAN (¨Personal Area Network) permiten a los dispositivos comunicarse dentro del rango de una persona. Un ejemplo común es una red inalámbrica que conecta a una computadora con sus periféricos. Casi todas las computadoras tienen conectado un monitor, un teclado, un ratón y una impresora. Sin embargo, sin la tecnología inalámbrica es necesaria la conexión mediante cables. Para la comunidad de los usuarios, algunas empresas se pusieron de acuerdo para diseñar una red inalámbrica de corto alcance conocida como Bluetooth, con esta tecnología se evitó la utilización de cables para la conexión de componentes dentro de la PAN. En forma simple, las redes Bluetooth utilizan el paradigma maestro-esclavo, es decir la unidad del sistema por lo general (la PC) es el maestro el cual trata al ratón, el teclado, etc., como sus esclavos. El maestro dice a los esclavos que direcciones usar, cuándo pueden transmitir información, durante cuánto tiempo pueden transmitir, qué frecuencia usar, etc.

La tecnología Bluetooth es utilizada en otras aplicaciones tales como la de los audífonos conectados inalámbricamente al celular, el reproductor musical digital al automóvil con solo tenerlo dentro de rango de cobertura. Una clase completamente distinta de la red Pan se forma cuando un dispositivo médico integrado, como un marcapasos, bomba de insulina o audífonos para discapacitados se comunica con un control remoto operado por el usuario[8].

1.4.2 Redes de área local. Generalmente llamadas LAN (Local Area Network), son redes de propiedad privada que operan dentro de un solo edificio, como una casa, oficina o fábrica. Las redes LAN se utilizan ampliamente para conectar computadoras personales electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información. Cuando las empresas utilizan redes LAN se les conoce como redes empresariales.

Las redes LAN pueden ser tanto inalámbricas como alámbricas, en los primeros, cada computadora utiliza un módem y una antena que utiliza para comunicarse con otras computadoras. En la mayoría de casos, cada computadora se comunica con un dispositivo generalmente puesto se coloca en el techo. A este dispositivo se lo denomina AP (Access Point, Punto de Acceso), enrutador inalámbrico o estación base; transmite paquetes entre computadoras inalámbricas y también entre éstas e internet. Hay un estándar para las redes LAN inalámbricas llamado IEEE 802.11, mejor conocida como WiFi[9].

1.5 DISPOSITIVOS DE RED DE DATOS

Son todos aquellos elementos que se conectan de forma directa a un segmento de red, teniendo en cuenta el documento “Dispositivos activos de red”, realizado por SENA, a continuación, se describirán algunos de los más importantes:

1.5.1 Enrutadores. Dispositivos para conectar redes en la capa tres del modelo OSI y asegurando el enrutamiento de los paquetes entre las redes limitando el tráfico de brodcasting proporcionando: control, seguridad y redundancia; éste dispositivo también se puede utilizar como un firewall. (Ver figura 2).

[8] Tanenbaum, A., & Wetherall, D. (2012). Redes de computadoras. Naucalpan de Juárez, Estado de México: Pearson.

[9] Ibid.



Figura 2. Enrutador, dispositivo de red.
Fuente. (SENA (Servicio Nacional de Aprendizaje), 2017)

Tipos:

- En función del Área

  Locales: Interconectan dos redes por conexión de los medios físicos de ambos router.

  Extensa: Conectan redes distantes.

- De la manera como se actualizan las tablas de encaminamiento(Routing):

  Estáticos: ésta se hace manualmente.

  Dinámicos: Es realizada por el router de forma automática.

- Según los protocolos:
  Routing Information Protocol (RIP): Comunican diferentes sistemas que pertenecen a la misma red lógica. Poseen tablas dinámicas e intercambian información según su necesidad, permitiendo un total de 14 saltos como máximo.
  Exterior Gateway Protocol (EGP): Permite conectar dos sistemas. Buscando entre los routers el camino desde el origen hasta el destino.

  Open Shortest Path First Routing (OSPF): Minimiza el tráfico de enrutamiento, permitiendo autenticar mensajes salientes; poseen una copia de la topología de la red y todas son idénticas, distribuyendo la información al router adyacente, debido a que cada uno de ellos construye su propio árbol de enrutamiento.

- Multiprotocolo: utiliza tramas de forma simultánea para diferentes protocolos de Red, enrutándolas a su destino de forma más rápida y con el menor costo.

Son catalogados como router de segunda generación, ahorrando gastos innecesarios como el tener un router por cada protocolo.

- Brouter (bridging router): Routers multiprotocolo con las características de un bridge. Su funcionamiento es como los router con protocolos enrutables, source routing y spanning tree bridging y protocolos no enrutables.

- Trouter: Combinación entre un router y servidor de terminales, utilizado para hacer pequeños grupos de trabajo y con conexión a RALs, WANs, modems, impresoras, y otros computadores, pero pueden ocasionar una degradación en el tiempo de respuesta.

1.5.2 Tarjetas de red:

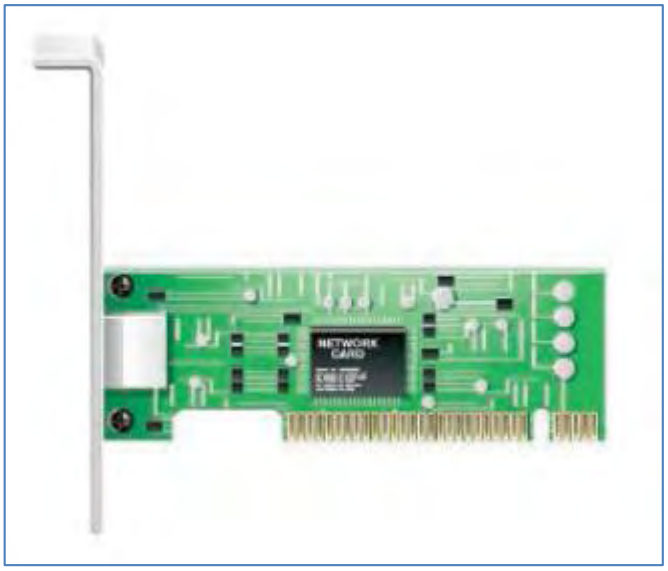


Figura 3. Tarjeta de red, dispositivo de red.
Fuente: (SENA (Servicio Nacional de Aprendizaje), 2017)

Denominadas adaptadores de red o tarjetas de interfaz de red o NIC, es un periférico que permite la comunicación entre una computadora, el cable de red y la red, permitiendo también compartir recursos con otros computadores de una red. (Ver figura 4).

1.5.3 Tranceiver:

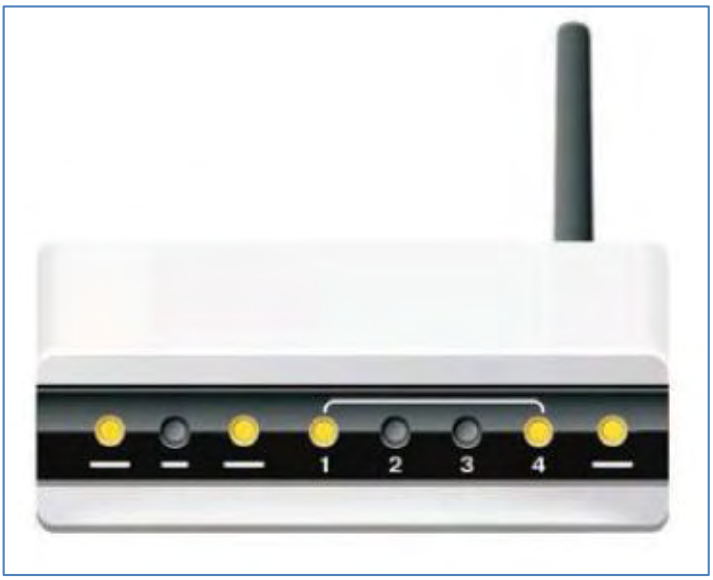


Figura 4. Tranceiver, dispositivo de red.
Fuente: (SENA (Servicio Nacional de Aprendizaje), 2017)

Conocido como Transceptor, denominado bajo la forma de Transductor, siendo que se encarga de transmitir una Potencia de un punto a otro. Este dispositivo puede ser de tipo Electromagnéticos, Acústico o Mecánicos, que transmiten una señal hacia otro dispositivo, pero con una transformación de medios.

1.5.4 Switch

Dispositivo de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. (Ver figura 5).



Figura 5. Switch, dispositivo de red.
Fuente: (SENA (Servicio Nacional de Aprendizaje), 2017)

Tipos:

- Capa 2: tienen la capacidad de asimilar y apilar direcciones de red de los dispositivos conectados a cada uno de los puntos de los puertos.

- Capa 3: son dispositivos que integran routing y switching, para altas velocidades, determinando el camino con información de la capa de red (capa 3), haciendo validación de integridad del cableado por un checksum (control de redundancia), posibilitan la comunicación entre las diversas VLAN's, sin la necesidad de utilizar un router externo; es más escalable que un router, los switches sobreponen la función de ruteo encima del switching.

- Capa4: llamados también Layer 3+. Incorporan las funcionalidades de un Switch de capa 3, implementa políticas, filtros a partir de informaciones de capa 4 obre puertos: TCP/UDP, SNMP, FTP, etc.

1.6 TRANSMISIÓN DE DATOS

Según Macías Ríos, Rentería Anguiano, & Rangel Licea[10], la transmisión de datos es el intercambio de datos entre dos dispositivos a través de alguna forma de medio de transmisión[11], complementa lo anterior diciendo, que para que la transmisión datos sea posible, los dispositivos de comunicación deben ser parte de un sistema de comunicación formado por hardware (equipo físico) y software (programas). Además, añade que la efectividad del sistema de comunicación de datos depende de cuatro características fundamentales, las cuales son:

- Entrega. El sistema debe entregar los datos en el destino correcto. Los datos deben ser recibidos por el dispositivo o usuario adecuado y solamente por ese dispositivo o usuario.

- Exactitud. El sistema debe entregar los datos con exactitud. Los datos que se alteran en la transmisión son incorrectos y no se pueden utilizar.

---

[10] Macías Ríos, E., Rentería Anguiano, E., & Rangel Licea, V. (10 de 2009). Paginas personales en la web. Recuperado el 02 de 02 de 2017, de http://profesores.fi-b.unam.mx/victor/CCNA/Productos/Notas%20de%20Curso/Manual%20de%20la%20Asignatura%20de%20Redes%20de%20Datos%20I%20y%20II%20%20(avance%2050%25).pdf

[11] Forouzan, B. A. (2007). Transmisión de datos y redes de comunicaciones. Madrid: McGraw-hill/Interamericana de España S.A.U.

- Puntualidad. El sistema debe entregar los datos con puntualidad. Los datos entregados tarde son inútiles. En el caso del video, el audio y la voz, la entrega puntual significa entregar los datos a medida que se producen, en el mismo orden en que se producen y sin un retraso significativo, este tipo de entregas se llama transmisión.

- Jitter (retardo variable). Se refiere a la variación en el tiempo de llegada de los paquetes. Es el retraso inesperado en la entrega de paquetes.

1.7 MODELO DE REFERENCIA OSI

Creada en 1947, la Organización Internacional de Estandarización (ISO, International Standards Organization) Un estándar ISO que cubre todos los aspectos de las redes de comunicación es el modelo de Interconexión de sistemas abiertos (OSI, Open System Interconnection). Un sistema abierto es un modelo que permite que dos sistemas diferentes se puedan comunicar independientemente de la arquitectura subyacente. El modelo OSI no es un protocolo; es un modelo para comprender y diseñar una arquitectura de red flexible, robusta e interoperable.

El modelo de interconexión de sistemas abiertos es una arquitectura por niveles para el diseño de sistemas de red que permite la comunicación entre todos los tipos de computadoras. Está compuesto por siete niveles separados, pero relacionados, cada uno de los cuales define un segmento del proceso necesario para mover información a través de una red[12].
El modelo de referencia OSI divide el proceso global de comunicación en funciones que son desempeñadas por varias capas. En cada capa, un proceso en una computadora desarrolla una conversación con un proceso paritario en la otra máquina.

En la figura 6, se muestra las diferentes capas existentes en el modelo OSI en un entorno emisor-receptor, además del comportamiento de la pila de datos en cada capa tanto en la computadora emisora como en la receptora.

- En 1, se observa el encabezado de la capa de aplicación.

- En 2, se observa el encabezado de la capa de presentación.

- En 3, se observa el paquete de datos que la computadora emisora enviará al receptor mediante un entorno físico de red.

---

[12] Ibid.

- Una vez transmitido por la computadora emisora el paquete de datos por el entorno físico de red, es recibido por la computadora receptora, se puede observar en 4, que a medida que el paquete sube por la capa OSI de la computadora receptora, el encabezado de la capa inmediatamente anterior es suprimido. (Ver figura 6).

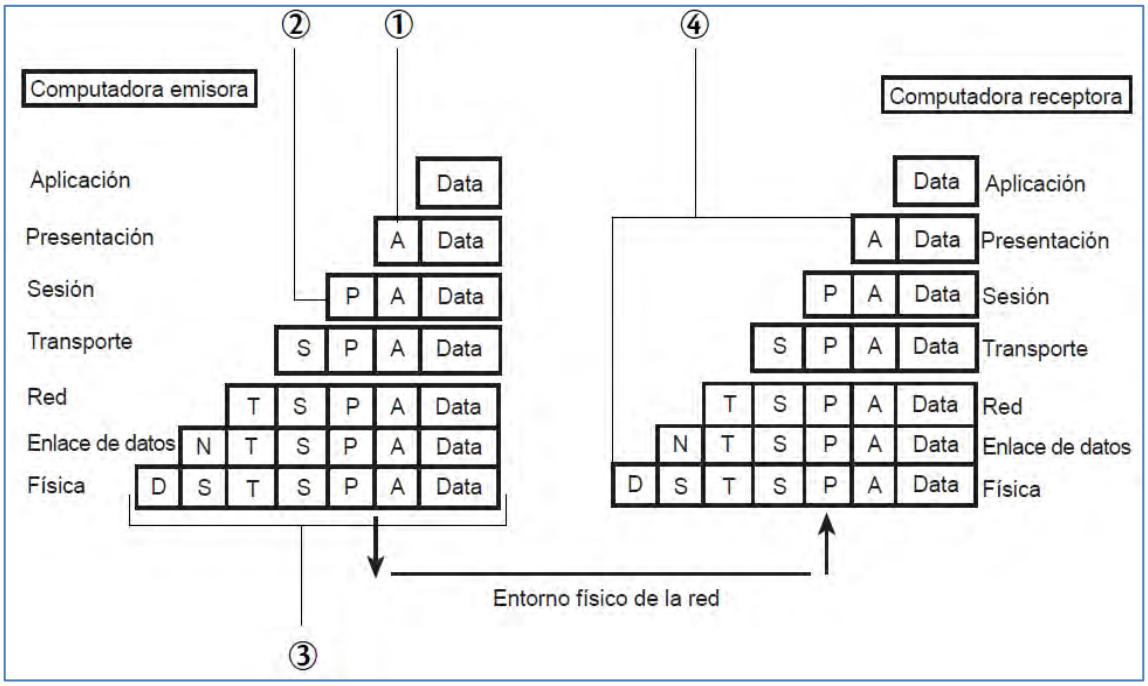


Figura 6. Comportamiento de paquetes de datos en modelo OSI en emisor y receptor.

A continuación, se describe en detalle cada una de las capas del modelo OSI.

1.7.1 Capas de modelo osi capa de aplicación. La capa de aplicación proporciona la interfaz de usuario, normalmente un programa/proceso de aplicación, a una variedad de servicios de información distribuida que abarca toda la red. Entre ellos se cuentan transferencia y gestión de archivos, así como servicios generales de intercambio de documentos y mensajes. Existen varios protocolos estándar para estos y otros tipos de servicios.

Además de la transferencia de archivos de información, la capa de aplicación proporciona servicios como:

- Identificación del o los interlocutores buscados, por nombre o por dirección.
- Determinación de la disponibilidad actual de un interlocutor buscado.
- Establecimiento de la autorización para comunicarse.

- Acuerdo sobre mecanismos de confidencialidad (Cifrado).

- Verificación de la autenticidad de un interlocutor buscado.

- Selección de la disciplina de diálogo, incluidos los procedimientos de inicio y liberación.

- Acuerdo sobre quién se encargará de la recuperación de errores.

- Identificación de restricciones de la sintaxis de los datos (conjunto de caracteres, estructuras de datos, etc.).

Capa de presentación. La capa de presentación se ocupa de la representación (sintaxis) de los datos durante la transferencia entre dos procesos de aplicación en comunicación. La capa de presentación negocia y selecciona la o las sintaxis de transferencia apropiadas que se usarán durante una transacción, de modo que se mantenga la sintaxis (estructura) de los mensajes intercambiados entre dos entidades de aplicación. Si esta forma de representación es distinta de la forma abstracta interna, el protocolo de presentación efectuará la conversión necesaria.

Otra función de la capa de presentación es la encargada de la seguridad de los datos. En algunas aplicaciones, antes de ser enviados, los datos se cifran con una clave que (es de esperarse) sólo conozca la capa de presentación del destinatario al que van dirigidos. Ésta descifra los datos recibidos con la clave correspondiente antes de pasarlos al destinatario.

Capa de sesión. Con la capa de sesión, dos entidades de protocolo de la capa de aplicación pueden organizar y sincronizar su dialogo y gestionar el intercambio de sus datos. Así pues, la capa de sesión se encarga de establecer (y liberar) un canal de comunicación (dialogo) entre dos entidades de protocolo de la capa de aplicación (entidades de protocolo de la capa de presentación, en la práctica) mientras dure la transacción de red completa. Además, la capa de sesión proporciona varios servicios opcionales, entre ellos los siguientes:

- Gestión de interacciones. El intercambio de datos asociado a un diálogo puede ser dúplex (bidireccional simultáneo) o semidúplex (semidireccional alterado). En el segundo caso el protocolo de la capa de sesión proporciona recursos para controlar el intercambio de datos (unidades de diálogo) en forma sincronizada.

- Sincronización. Si la transacción de red es prolongada, el usuario (por medio de los servicios provistos por la capa de sesión) puede optar por establecer periódicamente puntos de sincronización asociados a la transferencia. Si ocurre un fallo durante una transacción, el diálogo podrá reiniciarse en un punto de sincronización (previo) convenido.

- Informe de excepciones. La capa de sesión puede notificar a la capa de aplicación la ocurrencia de excepciones no recuperables durante una transacción.

Capa de transporte. La capa de transporte actúa como interfaz entre capas superiores, orientadas a las aplicaciones, y las capas de protocolos subyacentes, dependientes de la red. La capa de sesión se vale de la capa de transporte como un recurso de transferencia de mensajes que es independiente del tipo de red subyacente. Al proporcionar a la capa de sesión un conjunto definido de recursos para transferencia de mensajes, la capa de transporte oculta a la capa de sesión los detalles del funcionamiento de la red subyacente.

La capa de transporte ofrece varias clases de servicio para compensar la calidad de servicio (QOQ: quality of service) variable de las capas de red de los diferentes tipos de red. Hay cinto clases de servicio que van desde la clase 0, que proporciona sólo las funciones básicas necesarias para establecer conexiones y transferir datos, hasta la clase 4, que ofrece procedimientos completos de control de errores y control de flujo[13].

Capa de red. La capa de red se ocupa de la obtención de paquetes procedentes de la fuente y encaminarlos durante todo el camino hasta alcanzar su destino, en el camino puede surgir la necesidad de hacer varios saltos en nodos intermedios a lo largo del recorrido. La capa de red es la capa que se ocupa de la transmisión extremo a extremo de la información mediante el diálogo entre las entidades homólogas de la capa de red de cada nodo intermedio que interviene en la comunicación. De esta manera la capa de transporte mantendrá ya directamente un dialogo extremo a extremo con la entidad homologada del otro extremo de la comunicación (y no con nodos intermedios). Los nodos intermedios se denominan también IMP (Procesadores de Intercambio de Mensajes), Routers o Encaminadores, aunque hay que puntualizar que en el caso de las dos últimas denominaciones, se supone que tienen capacidad para el encaminamiento de paquetes[14].

Capa de enlace. La tarea principal de esta capa es transformar un medio de transmisión puro en línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión. Logra esta tarea haciendo que el emisor fragmente

---

[13] Halsall, F. (1998). Comunicación de datos, redes de computadores y sistemas abiertos. Naucalpan de Juárez: Pearson educación.

[14] Universidad de Oviedo. (03 de 02 de 2017). Universidad de Oviedo área de ingeniería de sistemas y automática. Recuperado el 03 de 02 de 2017, de http://www.isa.uniovi.es/docencia/redes/Apuntes/tema5.pdf

los datos de entrada en tramas de datos (típicamente, de algunos cientos o miles de bytes) y transmitiendo las tramas de manera secuencial.

Otra cuestión que surge en la capa de enlace de datos (y en la mayoría de capas superiores) es cómo hacer que un transmisor rápido no sature de datos a un receptor lento. Por lo general, se necesita un mecanismo de regulación de tráfico que indique al transmisor cuánto espacio de búfer tiene el receptor en ese momento. Con frecuencia, esta regulación de flujo y el manejo de errores están integrados.

Las redes de difusión tienen un aspecto adicional en la capa de enlace de datos controlan el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos, la subcapa de control de acceso al medio, se encarga de este problema, en esta subcapa se define el direccionamiento físico, que permite a los hosts identificar las tramas destinadas a ellos. Este direccionamiento es único, identifica el hardware de red que se está usando y el fabricante, y no se puede cambiar[15].
Capa física. El nivel físico coordina las funciones necesarias para transmitir el flujo de datos sobre un medio físico. Trata con las especificaciones eléctricas y mecánicas de la interfaz y del medio de transmisión. También, define los procedimientos y funciones que los dispositivos y las interfaces tienen que llevar a cabo para que sea posible la transmisión. El nivel físico se relaciona con lo siguiente:

- Características físicas de las interfaces o el medio. El nivel físico define las características de la interfaz entre los dispositivos y el medio de transmisión. También define el tipo de medio de transmisión.

- Representación de los bits. Los datos del nivel físico están compuestos por un flujo de bits (secuencias de ceros y unos) sin ninguna interpretación. Para que puedan ser trasmitidos, es necesario codificar los bits en señales eléctricas u ópticas.

- Tasa de datos. El nivel físico también define la tasa de transmisión, es decir, el número de bits enviados cada segundo, en otras palabras, el nivel físico define la duración de un bit, es decir cuánto tiempo dura.

- Sincronización de bits. El emisor y el receptor deben estar sincronizados a nivel de bit. En otras palabras, los relojes de emisor y el receptor deben estar sincronizados.

- Configuración de la línea. El nivel físico está relacionado con la conexión de dispositivos al medio. En una configuración punto a punto se conectan dos

[15] S. Tanenbaum, A. (02 de 02 de 2017). Google academico. Recuperado el 02 de 02 de 2017, de https://books.google.es/books?hl=es&lr=&id=WWD-4oF9hjEC&oi=fnd&pg=0capa&f=false

dispositivos a través de un enlace dedicado. En una configuración multipunto, un enlace es compartido por varios dispositivos.

- Topología física. La topología física define cómo están conectados los dispositivos para formar una red. Los dispositivos deben estar conectados usando una topología en malla (cada dispositivo conectado a otro dispositivo), una topología en estrella (dispositivos conectados a través de un dispositivo central), una topología en anillo (un dispositivo conectado al siguiente, formando un anillo) o una topología de bus (cada dispositivo está conectado a un enlace común).

- Modo de trasmisión. El nivel físico también define la dirección de la transmisión entre dos dispositivos: simplex, semiduplex, o full-duplex. En el modo simplex solamente un dispositivo puede enviar; el otro solo puede recibir. El modo simplex es una comunicación en un solo sentido. En el modo semiduplex, dos dispositivos pueden enviar o recibir, pero no al mismo tiempo. En el modo full-duplex (o simplemente duplex), dos dispositivos pueden enviar o recibir al mismo tiempo[16].

1.8 TCP/IP

La familia de protocolos TCP/IP, se desarrolló antes que el modelo OSI, por tanto, los niveles de protocolo TCP/IP no coinciden exactamente con los del modelo OSI. El protocolo TCP/IP original fue definido con cuatro niveles: host a red, Internet, transporte y aplicación. Sin embargo, cuando se compara TCP/IP con OSI, se pude decir que el nivel host a red es equivalente a la combinación de los niveles físicos y de enlace de datos. El nivel de internet es equivalente al nivel de red y el nivel de aplicación hace aproximadamente el trabajo de los niveles de sesión, presentación y aplicación con el nivel de transporte en TCP/IP encargándose de parte de las responsabilidades del nivel de sesión.

TCP/IP es un protocolo jerárquico compuesto de módulos interactivos, cada uno de los cuales ofrece una funcionalidad específica, sin embargo, los módulos no son interdependientes. Mientras que el modelo OSI especifica que funciones pertenecen a cada uno de sus niveles, los niveles de familia de protocolos TCP/IP contienen protocolos relativamente independientes que pueden ser mezcla de o coincidir dependiendo de las necesidades del sistema. El término jerárquico significa que cada protocolo de nivel superior es soportado por uno o más protocolos de nivel inferior[17].

---

[16] Forouzan, B. A. (2007). Transmisión de datos y redes de comunicaciones. Madrid: McGraw-hill/Interamericana de España S.A.U.
[17] Ibid.

De manera más sencilla ORACLE[18], da una descripción de esta familia de protocolos diciendo: "'TCP/IP' es el acrónimo que se utiliza comúnmente para el conjunto de protocolos de red que componen el conjunto de protocolos de Internet. Se utiliza el término 'Internet' para describir tanto el conjunto de protocolos como la red de área global. 'TCP/IP' hace referencia específicamente al conjunto de protocolos de Internet. "Internet" hace referencia a la red de área extensa y los elementos que rigen Internet".

A grosso modo Halsall[19], explica cómo se establece una conexión en el protocolo TCP/IP, diciendo que todos los servidores tienen asociado un nombre que se traduce en una dirección de red correspondiente. El procedimiento de traducción lo efectúa un proceso llamado servidor de nombres de dominio. La dirección de red resultante de un proceso servidor consta de dos partes: la dirección IP a nivel de red del sistema anfitrión en el que está ejecutando el proceso y un número de puerto local. El IP de cada pasarela de interred utiliza la dirección IP para enrutar los datagramas por la interred hasta el sistema anfitrión de destino solicitado. El número de puerto sirve para que el TCP del sistema anfitrión, identifique el proceso específico en ese sistema anfitrión al cual debe enviarse el mensaje recibido. (Ver figura 7).

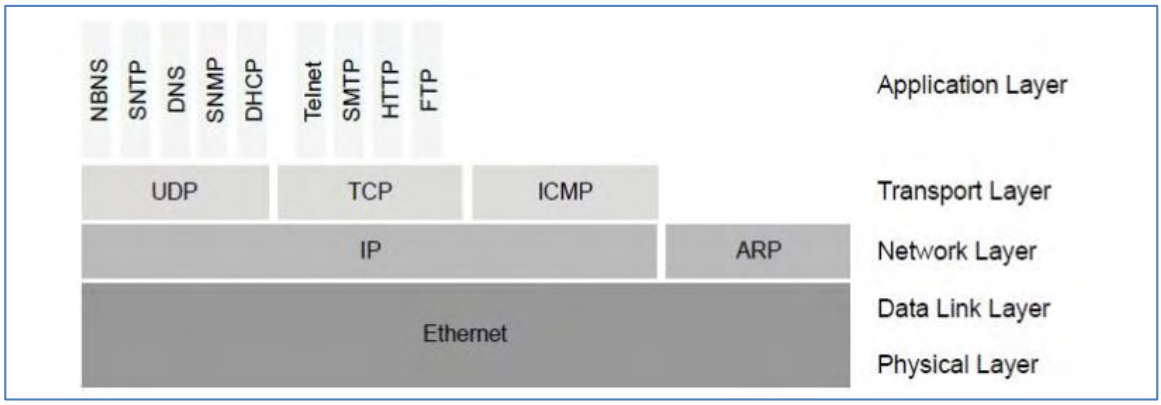


Figura 7. Pila de protocolos TCP/IP.
Fuente. (Tekmikro, 2017)

[18] ORACLE. (01 de 01 de 2017). ORACLE help center. Recuperado el 02 de 02 de 2017, de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html

[19] Halsall, F. (1998). Comunicación de datos, redes de computadores y sistemas abiertos. Naucalpan de Juárez: Pearson educación.

1.9 PROTOCOLO IP

Tal como dice en el libro “Protocolos de Internet diseño e implementación en sistemas UNIX” de López & Novo[20], el protocolo IP (Internet Protocol) fue diseñado para interconectar sistemas basados en redes de intercambio de paquetes.

Este protocolo de Internet permite el intercambio de bloques de datos, los cuales se denominan datagramas, entre hosts conectados en una red, éstos tienen una dirección única denominada dirección IP.
IP implementa dos funciones básicas, las cuales son:

1. Encaminamiento. Para esta función hace uso de uno de los campos que aparecen en la cabecera de los datagramas, estos identifican la dirección IP de cada host de destino. Esta dirección se utiliza para transmitir los datagramas hacia el host correspondiente.

2. Fragmentación. Esta función se encuentra directamente influenciada con la capa directamente inferior de la capa IP, se trata de la capa de enlace. Los datagramas generados por IP deben amoldarse al tamaño máximo que es capaz de tratar la red, esta delimitación está dada por el nivel de enlace. Si el tamaño máximo de una trama (nombre que se la da a la unidad de datos a nivel físico) es más pequeño que el datagrama generado por IP, entonces la capa IP es obligada a fragmentar los datagramas, de manera que puedan ser enviados por la red.

El protocolo IP trata cada datagrama como una unidad independiente del resto de los datagramas. Para poder llevar a cabo su servicio, IP utiliza cuatro campos especiales, los cuales se denominan:

1. Tipo de servicio. Indica la calidad del servicio deseado.

2. Tiempo de vida. Establece el tiempo máximo que un datagrama puede tardar en alcanzar su destino. Este tiempo se va decrementando a medida que el datagrama atraviesa los diferentes nodos de la red. Cuando el valor de este campo llega a cero, el datagrama se descarta.

3. Opciones. Proporcionan funcionalidad de control en algunas situaciones incluyen entre otros, mecanismos de seguridad, encaminamiento especial entre otros.
4. Checksum. Proporciona la verificación de la información se ha recibido de manera correcta; sin embargo, esta comprobación se hace únicamente a nivel

[20] López, Á., & Novo, A. (2000). Protocolos de Internet diseño e implementacion en sistemas UNIX. Mexico D.F.: Alfaomega grupo editor , S.A. de C.V.

de la cabecera, por lo que no existe garantía de que la información transportada por el datagrama sea correcta. Se el checksum falla el datagrama se descarta.

1.9.1 Clases de redes. Una dirección IP (IP v4), está constituida por cuatro números enteros, cada uno de ellos de un byte y separados por un punto. Las direcciones IP se componen de dos partes, la primera identifica a la red, la segunda a un host concreto dentro de la red. Dependiendo del número de bytes que destine a cada una de las dos partes, se puede encontrar con cuatro tipos de redes[21].

- Redes de clase C

Destinan tres bytes para identificar la red y un byte para identificar a los hosts. (Ver figura 8).

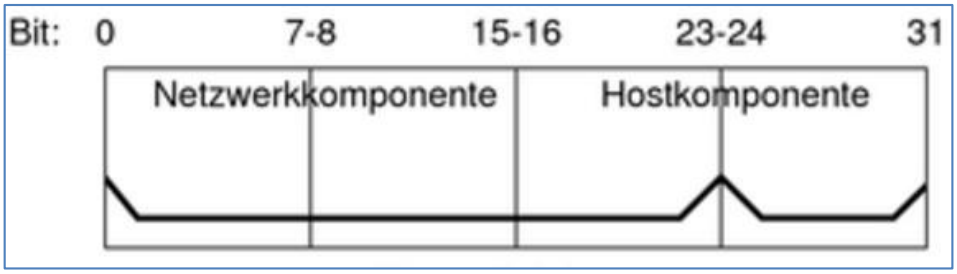


Figura 8. Representación en byte de red clase C.
Fuente. https://docs.oracle.com/cd/E24842_01/html/820-2981/ipref-4.html

Los tres bits más significativos de los bytes que identifican la red valen uno, uno y cero respectivamente. Esto permite rangos que van desde 192.1.1.1 hasta 223.254.254, y mediante el byte destinado a los hosts se puede identificar a 254 host.

Cabe destacar que existen una serie de direcciones especiales, en diferentes clases de redes, en la siguiente tabla se las describirá. (Ver tabla 2).

DIRECCIÓN	DESCRIPCIÓN
0.0.0.0	Se utiliza como origen de una solicitud de configuración de arranque.
127.0.0.0	Reservada
127.0.0.1	Interna (loopback). Cliente y servidor están en la misma máquina.
127.0.02 – 127.255.255.255	Reservadas

[21] Ibid.

128.0.0.0	Reservada
191.255.0.0	Reservada
192.0.0.0	Reservada
10.0.0.0 – 10.255.255.255	Clase A reservada para Internet
172.16.0.0 – 172.31.255.255	Clase B reservada para Internet
192.168.0.0 – 192.168.255.255	Clase C reservada para Internet
255.255.255.0	Reservada
254.0.0.0 - 255.255.255.254	Reservada
255.255.255.255	Broadcast a todos los nodos de la red local

Tabla 2. Direcciones IP especiales reservadas.
Fuente. (López & Novo, 2000)

1.9.2 Máscara de subred. La parte que corresponde a la red de una dirección de clase A, B o C, tiene un tamaño fijo, sin embargo, las diferentes empresas u organizaciones pueden tener la necesidad de variar este tamaño y decidir cuantos bits van a destinar para identificar las redes y cuantos para identificar los hosts. Por este motivo los routers deben ser capaces de saber a priori cuantos bits se han destinado para identificar una red, y así poder encaminar los paquetes en un sentido o en otro. Para llevar a cabo dicho propósito se utiliza el concepto de máscara de subred. La máscara de subred es una secuencia de 32 bits, dentro de los cuales aquellos que tengan el valor 1 identifican la red y los que tienen el valor cero identifican los hosts[22]. Para entenderlo mejor se da el siguiente ejemplo:

11111111.00000000.00000000.00000000

La anterior es una dirección de red de clase A, ya que su primer byte (que es el encargado de identificar la red, tiene todos sus bits en 1), mediante esta máscara se observa que se ha destinado un byte para identificar la red y tres para identificar los hosts.

La anterior dirección expresada en forma decimal seria:

255.0.0.0

[22] Ibid.

1.9.3 Direcciones sin clase .cidr. El método de manejo de direcciones de red del tipo A, B y C es bastante ineficiente, ya que, si por ejemplo se tuviera 1000 equipos en una red, con una dirección de clase C no tendría suficiente, ya que este tipo de direcciones solo permite tener 254 host dentro de una red; sin embargo, con la dirección de clase B estaría desperdiciando miles de direcciones, ya que este tipo permite direccionar más de 65000 hosts. Lo ideal sería que cada uno pudiese elegir cuantos bits necesita realmente pare direccionar cada uno de los equipos de una red o subredes. Esto se consigue mediante la implementación de redes utilizando la técnica CIDR (Classless Internet Domain Rounting).

En este tipo de implementación, una dirección del tipo 10.0.0.0 no supone que se trata de una clase A. El tipo viene dado por la máscara de subred, de esta forma, si la máscara de subred es 255.255.0.0, se tratará de una red de clase B[23].

1.9.4 Subneting. Haciendo uso de la técnica anterior es posible obtener mayor número de hosts dentro de una red. Sin embargo, en numerosas ocasiones las empresas se ven obligadas a crear pequeñas redes dentro de una red; este tipo de tipo de estrategia se denomina subneting[24].
Se puede decir entonces que subneting es el ejercicio o la práctica de formar subredes, teniendo en cuenta las mascara de subred predeterminada para formar grupos más grandes o más pequeños de Host. Es posible combinar direcciones de clases A, B, C con cualquier mascara.

1.10 GESTIÓN DE REDES

Son varios los significados que se le da a la gestión de red[25], la define como el proceso o control de la información compleja que circula por la red para maximizar su eficiencia y productividad, añade diciendo, que proveen un conjunto de herramientas que permite una monitorización de las redes antes de la ausencia de fallas y ofrece diagnósticos remotos así como cambios y eventos que el administrador considere necesario, concluye haciendo referencia que las áreas fundamentales en las que actúa son la gestión de fallos, gestión de la configuración, gestión de la seguridad, gestión de la ejecución y gestión de la contabilidad.

---

[23] Ibid.

[24] Ibid.

[25] Acuña Garcia, E., & Caicedo Urresta, V. M. (02 de 02 de 2017). Repositorio digital Universidad Técnica de Ambato. Recuperado el 02 de 02 de 2017, de http://repositorio.uta.edu.ec/bitstream/123456789/326/3/Tesis_t167si.pdf

Por su parte Forouzan[26], define la gestión de red como la monitorización, pruebas, configuraciones y resolución de problemas de los componentes de una red con el objetivo de cumplir los requisitos definidos por una organización. Estos requisitos incluyen la operación eficiente de la red que ofrece la calidad de servicio predefinida para el usuario. Para llevar a cabo esta tarea, un sistema de gestión de red utiliza componentes hardware, software y personas.

Teniendo en cuenta a Leon Garcia & Widjaja[27], quien dice que la gestión de redes implica escuchar y vigilar una red para que funcione como se pretendía. También proporciona un medio para configurar el sistema mientras todavía se satisfagan o excedan las especificaciones de diseño. Además, que la función realizada por un sistema de redes se puede dividir en las siguientes cinco áreas:

- Gestión de fallos. Se refiere a la detección, aislamiento y resolución de problemas de la red. Puesto que un fallo puede causar el mal funcionamiento de parte de la red o incluso de la totalidad de la red, la gestión de fallos proporciona un medio de seguir que la red sea fiable. Así, la detección de un fallo en un enlace de la transmisión o en un componente de la red, la reconfiguración de la red durante el fallo para mantener el nivel de servicio y la restauración de la red cuando el fallo se arregle.

- Gestión de configuración. Se refiere al proceso de configurar una red inicialmente y luego ajustarla como respuesta a los requerimientos de cambio de la red. Esta función es quizás el área más importante de la gestión de redes, ya que una configuración incorrecta puede causar que la red funcione por debajo de lo normal o incluso nada.

- Gestión contable. Implica hacer el seguimiento del uso de los recursos de la red. Por ejemplo, se puede monitorizar la carga de usuarios para determinar cómo situar mejor los recursos. Alternativamente, se puede examinar el tipo o el nivel de tráfico que fluye a través de un puerto concreto. La gestión contable también incluye actividades como administración de contraseñas de acceso y facturación.

- Gestión de rendimiento. Implica el control del uso de la red, del tiempo de respuesta extremo a extremo, y de otras medidas del rendimiento en varios puntos de la red.
- Gestión de seguridad. Se refiere al proceso de hacer segura la red. Este proceso, por supuesto, implica la gestión de los servicios de seguridad que se

[26] FOROUZAN, Op. Cit.

[27] Leon Garcia, A., & Widjaja, I. (2002). Redes de comunicación. Madrid: McGraw-Hill/Interamericana de España, S.A.U.

refieren al control de acceso, autenticación, confidencialidad, integridad, y no rechazo.

1.11 SNMP

1.11.1 SNMP como protocolo. En sus siglas en ingles SNMP (Simple Network Management Protocol) que traduce Protocolo sencillo de gestión de redes, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento. Se puede conocer datos internos de dispositivos a monitorear, por ejemplo uso de CPU, Memoria, Disco, Uptime entre otros[28]. En si SNMP es utilizado para referirse a un conjunto de pasos en donde se enmarca al protocolo en sí mismo, la definición de la base de datos (MIB) y a conceptos que los asocian.

1.11.2 Arquitectura SNMP. En la figura 9, se observa el diagrama general de bloques de una entidad SNMPv3. Cada entidad incluye sólo un motor SNMP que implementa funciones para enviar y recibir mensajes SNMP, poder autenticar y encriptar mensajes y controlar el acceso. Estas funciones están a cargo de ciertos modulo qué exponen estas funciones como servicios para que las puedan invocar o utilizar otras aplicaciones, de esta manera conformando lo que se conoce como entidad SNMP.

Según se observa en la figura 9, tanto las aplicaciones como el motor, están definidas en módulos. Lo que permite tener una ventaja: el rol de cada entidad está determinado por los módulos que implementa, permitiendo que se mucho más sencillo modificar los módulos[29].

---

[28] Cayuqueo, S. D. (14 de 07 de 2016). Cayu - Wiki de Sergio Cayuqueo. Recuperado el 02 de 02 de 2017, de http://cayu.com.ar/files/manuales-nagios.pdf

[29] Botero Arana, N. (01 de Junio de 2005). Pontificia Universidad Javeriana Bogotá. Obtenido de Pontificia Universidad Javeriana Bogotá: http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf

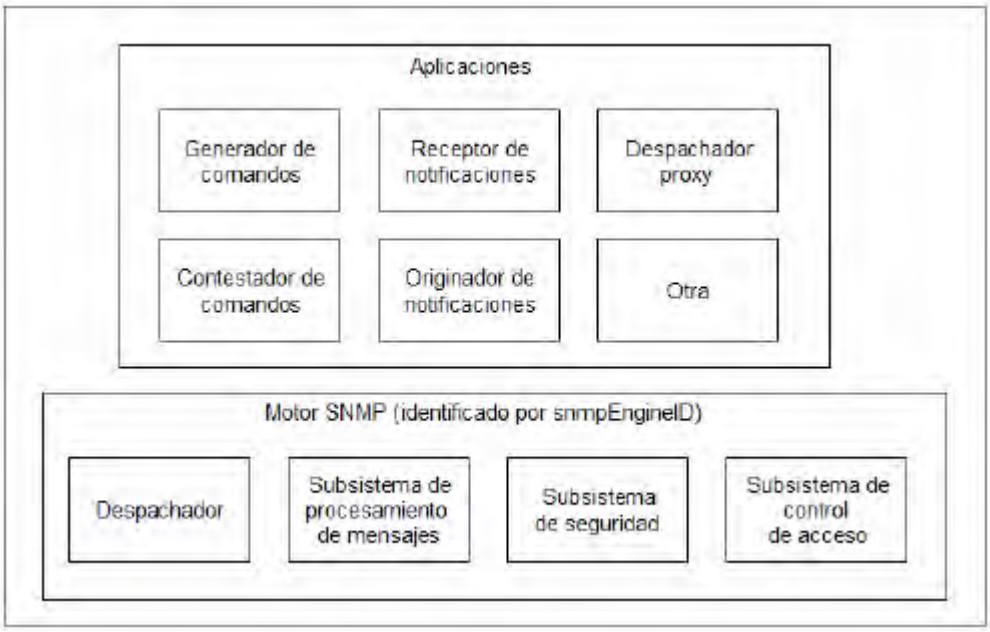


Figura 9. Arquitectura en bloques de SNMP v3.
Fuente. (Botero Arana, 2005)

Como lo describe Botero Arana, en su trabajo de tésis de ingeniería de sistemas, los componentes de una unidad SNMP son:

- Despachador. Permite el soporte de distintas versiones de mensajes SNMP, es el encargado de aceptar y enviar la PDU (Unidad de Datos de Protocolo), de pasarlas al subsistema de procesamiento de mensajes y enviar los mensajes por medio de la red.

- Subsistema de procesamiento de mensajes. Es el responsable del envío de mensajes y la extracción de datos de mensajes recibidos.

- Subsistema de seguridad. Es el encargado de proveer los servicios de autenticación y cifrado.

- Subsistema de control. Esta proveer servicios de autorización a recursos y además define que aplicación posee derechos como también el tipo de acceso que esta tiene.

- Generador de comandos: Inicializa las PDU de los mensajes y procesa la respuesta.

- Contestador de comandos: recibe las PDU destinadas a la entidad cuyo campo de contexEngineID es igual a la identificación del motor SNMP, ayuda al control de acceso, genera una respuesta adecuada.

- Originador de notificaciones. Se encarga de monitorear continuamente el sistema por evento o condiciones particulares y de ser necesario, genera una operación trap.

- Receptor de notificaciones. Mediante mensajes de notificación (o Traps) escucha, realizado esto genera un mensaje de respuesta.

- Despachador proxy. Direcciona los mensajes SNMP.

1.12 NAGIOS

El sitio oficial Nagios org[30], da una resumida idea de lo que es Nagios, refiriéndose a él como un sistema un sistema Open Source y una aplicación de monitoreo de red, que se encarga de monitorear los anfitriones y los servicios que se especifiquen, alertando cuando las cosas van mal y se requieren mejoras.
Por otro lado, en el trabajo "Evaluación de Nagios para Linux" realizado por Domínguez Dorado & Zarandieta Morán[31], aclara más el concepto de Nagios diciendo, que es un sistema de monitorización de equipos y de servicios de red, creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red que administran y conocer los problemas que ocurren en la infraestructura, antes de que los usuarios de la misma los perciban. Es un sistema complejo y completo en cuanto a sus características, que además hace uso en algunos casos de diversos sistemas como, por ejemplo, sistemas gestores de bases de datos, servidores web, etcétera. Es relativamente complejo de instalar y configurar. Concluye diciendo, Nagios es un software usado en todo el mundo, que debe correr en sistemas Linux (en la mayoría de los UNIX funciona sin problemas) y que permite extender su funcionalidad con la utilización/creación de extensiones. (Ver figura 10).

[30] Nagios org. (01 de 01 de 2017). Nagios. Obtenido de Nagios: https://www.nagios.org/documentation/

[31] Domínguez Dorado, M., & Zarandieta Morán, J. A. (01 de 05 de 2003). Manuel Domínguez Dorado ingeniería informática y dirección de proyectos. Obtenido de Manuel Domínguez Dorado ingeniería informática y dirección de proyectos: http://www.manolodominguez.com/wp-content/uploads/2016/10/20161007-M_Dominguez_Dorado-EvaluacionNagios1.pdf

1.12.1 Estructura de Nagios. Nagios sigue a grosso modo la siguiente estructura[32].

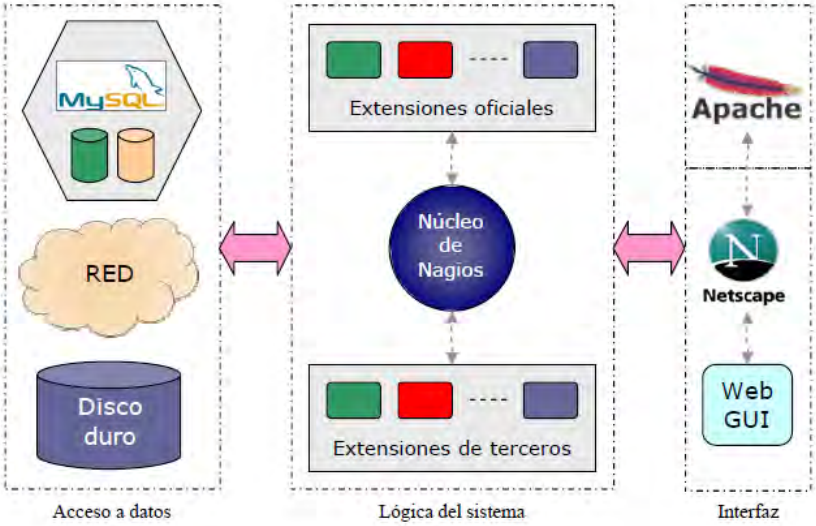


Figura 10. Estructura general de Nagios.
Fuente. (Domínguez Dorado & Zarandieta Morán, 2003)

Un núcleo de la aplicación que forma la lógica de control de negocio de la aplicación contiene el software necesario para realizar la monitorización de los servicios y máquinas de la red para la que está preparado. Hace uso de diversos componentes que vienen con la aplicación, y puede hacer uso de otros componentes realizados por terceras personas.

Aunque permite la captura de paquetes SNMP Trap para notificar sucesos, no es un sistema de monitorización y gestión basado en SNMP, sino que realiza su labor basándose en una gran cantidad de pequeños módulos software que realizan chequeos de parte de la red.

Muestra los resultados de la monitorización y del uso de los diversos componentes en una interfaz web a través de un conjunto de CGI's y de un conjunto de páginas HTML que vienen incorporadas de serie. Y que permiten al administrador una completa visión de qué ocurre, dónde y en algunos casos, por qué.

Por último, si se compila para ello, Nagios guardará los históricos en una base de datos para que, al detener y reanudar el servicio de monitorización, todos los datos sigan como iban, sin cambios.

[32] Ibid.

1.12.2 Requerimientos del sistema. Según Nagios org[33], el único requisito de funcionamiento de Nagios Core es una máquina que ejecuta Linux (o variante de UNIX) que tiene acceso a la red y un compilador de C instalado (si se instala desde el código fuente).

No se está en la obligación de utilizar el CGI que se incluye con Nagios Core. Sin embargo, si se decide usarlo, es necesario tener instalado el siguiente software:

- Un servidor web (preferiblemente Apache)
  .
- Una librería gd de Thomas Boutell versión 1.6.3 o superior (requerido por la statusmap y tendencias CGI).

Sin embargo, teniendo en cuenta la experiencia de Primantech[34], quien describe algunos requerimientos para el sistema tanto hardware como software.

Requerimientos hardware: Los requisitos hardware son muy variables, depende en gran medida del número de servicios y servidores a controlar. Para tener una idea, con una infraestructura de unos 200 equipos, seria necesario un Dual-Core con 250GB de HDD y 4-8GB de RAM

Requerimientos software:

- Sistema Operativo CentOS 5.x ó 6 (recomendado x32 para compatibilidades con plugins)
- Apache
- PHP
- GCC Compiler
- GD Development libraries

1.12.3 Licencia. Nagios Core está licenciado bajo los términos de la Licencia Pública General GNU Versión 2 publicada por la Free Software Foundation. Esto le da permiso legal para copiar, distribuir y/o modificar Nagios bajo ciertas condiciones.

Nagios Core se proporciona gratuitamente, sin garantía de ningún tipo, incluida la garantía de diseño, comercialización e idoneidad para un propósito específico.

---

[33] Nagios org, Op. Cit.

[34] Primantech. (08 de 05 de 2012). PrimanTech Blog dedicado a la divulgación y ayuda sobre el mundo de las TIC. Obtenido de PrimanTech Blog dedicado a la divulgación y ayuda sobre el mundo de las TIC: http://primantech.blogspot.com.co/2012/05/nagios-instalacion-en-centos.html

1.12.4 Características de Nagios. Las muchas características y capacidades que ofrece Nagios hacen que sea fácil de implementar en casi cualquier entorno.

Monitoreo integral:

- Capacidades para monitorear aplicaciones, servicios, sistemas operativos, protocolos de red, métricas del sistema y componentes de infraestructura con una sola herramienta.
- Las poderosas API de secuencias de comandos permiten un fácil monitoreo de aplicaciones, servicios y sistemas internos y personalizados

Visibilidad y conciencia:

- Vista centralizada de toda la infraestructura de TI supervisada.
- Información de estado detallada disponible a través de la interfaz web.
- Rápida detección de cortes de infraestructura.
- Las alertas se pueden entregar al personal técnico por correo electrónico o SMS.
- Las capacidades de escalamiento garantizan que las notificaciones de alerta lleguen a las personas adecuadas.

Remediación del problema:

- Los reconocimientos de alerta proporcionan comunicación sobre problemas conocidos y respuesta al problema.
- Los controladores de eventos permiten el reinicio automático de aplicaciones y servicios fallidos.

Planificación proactiva:

- Los complementos de planificación de la capacidad y de las tendencias garantizan que usted esté al tanto de la infraestructura envejecida.
- El tiempo de inactividad programado permite la supresión de alertas durante las actualizaciones de la infraestructura.

Informes:

- Los informes de disponibilidad aseguran que los SLAs se están cumpliendo.
- Los informes históricos proporcionan un registro de alertas, notificaciones, interrupciones y respuesta de alerta.
- Los complementos de terceros amplían las capacidades de informes.

Capacidades para múltiples inquilinos:

- El acceso multiusuario a la interfaz web permite a los interesados ver el estado de la infraestructura.
- Las vistas específicas del usuario garantizan que los clientes solo vean sus componentes de infraestructura.

Arquitectura extensible:

- La integración con aplicaciones internas y de terceros es fácil con múltiples API.
- Cientos de complementos desarrollados por la comunidad amplían la funcionalidad básica de Nagios.

Plataforma estable, fiable y respetada:

- Más de 10 años de desarrollo activo.
- Escalas para monitorear miles de nodos.
- Las capacidades de conmutación por error garantizan una supervisión continua de los componentes críticos de la infraestructura de TI.
- Múltiples premios, cobertura mediática y reconocimiento demuestran el valor de Nagios.

Comunidad extensa:

- Más de 1 millón de usuarios en todo el mundo.
- Las listas de correo de la comunidad activa proporcionan soporte gratuito.
- Cientos de complementos desarrollados por la comunidad amplían la funcionalidad básica de Nagios.
- Código personalizable.
- Software de código abierto.
- Acceso completo al código fuente.

1.13 CHECK_MK

En su página web Mathias Kettner[35], se refiere a Check MK como una solución completa de monitoreo de TI en la tradición de Nagios check_mk está disponible en una Free Edition, es 100% disponible bajo licencias de código abierto, y un Enterprise Edition, incluyendo características y de apoyo profesional adicional.

[35] Kettner, M. (26 de 09 de 2017). MK Mathias Kettner. Obtenido de MK Mathias Kettner: http://mathias-kettner.de/check_mk.html

El check_mk Raw Edición es un sistema de control integral de TI - disponible bajo la GNU GPL versión 2 y varias otras licencias de código abierto. Es libre de usar, modificar y compartir siempre y cuando cumpla con los términos de estas licencias.

El Check_MK Enterprise Edition se basa en la edición Raw, pero contiene muchas características empresariales adicionales y proporciona soporte profesional del fabricante.

1.13.1 Componentes del proyecto check_mk. En el sitio oficial web Kettner[36], describe cada uno de los componentes de Check_MK. A continuación, se realiza un resumen de cada uno de ellos.

Configuration & check engine: lo nuevo del Check_MK es su elegante método de configuración de Nagios. En lugar de los archivos de configuración normales de Nagios, se produce la detección automática del servicio y la generación de la configuración. Pero Check_MK también funciona de manera muy eficiente durante la ejecución de los chequeos. Los resultados del chequeo se envían a Nagios como cheques pasivos. Esto ahorra recursos sustanciales en el servidor y el cliente.

Livestatus: es un módulo intermediario de Nagios que proporciona acceso directo al estado de los hosts y servicios a través de un socket UNIX. Esto permite que complementos como NagVis accedan de forma rápida y eficiente a los datos de estado y hace que la base de datos NDO sea obsoleta. El acceso es a través de su propio protocolo simple y es posible desde todos los lenguajes de programación sin una biblioteca especial, incluso desde el shell.

Multisite: el Web GUI Multisite reemplaza a la GUI clásica de Nagios y también se puede usar sin Check_MK's Configuration & Check Engine. Con un look moderno y rápida carga de la página que ofrece vistas personalizables, incluyendo el monitoreo distribuido por varias instancias de monitoreo a través de estado en tiempo real, integración de NagVis y pnp4nagios, el acceso a la información de estado a través de la web y mucho más. Multisite utiliza Livestatus para acceder a los datos de estado.

[36] Ibid.

Wato: el Check_MK WATO (Web Administration Tool) hace que un sistema basado en Check_MK sea completamente manejable a través del navegador. Esto no se limita a administrar hosts y servicios y las típicas reglas Check_MK, sino que también incluye la administración de usuarios, roles, grupos, periodos de tiempo, revisiones Nagios clásicas y mucho más. A través de un concepto de rollo moderno, las autorizaciones se pueden asignar para que las tareas se pueden delegar a los colegas con seguridad.

Notify: el nuevo sistema de notificación de Check_MK hace que la configuración de notificaciones sea fácil y flexible. Varios usuarios pueden ser configurados y configurados de forma diferente por usuario. Por ejemplo, los mensajes de correo electrónico se pueden activar todo el día, SMS sólo para problemas importantes durante los tiempos de espera - sin tener que crear varios usuarios artificiales. Los usuarios pueden configurar sus propias notificaciones.

Event console: la consola de eventos Check_MK integra el procesamiento de mensajes de registro y capturas SNMP en la supervisión. Un daemon separado - el mkeventd - se configura a través de un conjunto flexible de reglas y decide cuál de los mensajes entrantes se clasifican como. Puede contar, correlacionar, esperar mensajes, reescribir mensajes y mucho más. La consola de eventos tiene incluso un daemon syslog incorporado que escucha directamente los mensajes del puerto 514.

1.14 PNP4 NAGIOS

En el sitio oficial web Monitoring Plugins Development Team[37], describe a PNP como un complemento para Nagios, de licencia libre GPL v2, completamente gratuito que analiza los datos de rendimiento obtenidos por los plugins y los almacena automáticamente en bases de datos RDD (Round Robin Databases).

Además, habla de que en el desarrollo de PNP se valoró que tuviera una fácil instalación y un mínimo mantenimiento mientras está en producción. Un administrador debería dedicar su tiempo a otras tareas en lugar de dedicarse a configurar herramientas gráficas.

Por otro lado, dice, que para conseguir esto los desarrolladores de PNP4 NAGIOS se han centrado en usar estándares. PNP sólo procesa datos de rendimiento de acuerdo a Developer Guidelines para plugins de nagios. Con este requerimiento gracias al trabajo de Nagios Plugin Developers se facilita adherir líneas de trabajo en PN4 NAGIOS.

---

[37] Monitoring Plugins Development Team. (15 de 03 de 2012). PNP4 NAGIOS. Obtenido de PNP4 NAGIOS: http://docs.pnp4nagios.org/es/pnp-0.6/start

1.14.1 Requerimientos software:

- Perl >= 5.x sin módulos adicionales.
- RRDtool >= 1.x, mejor 1.2 pero no obligatorio.
- Atención: instalar RRDtool sin un gestor de paquetes puede causar errores con las fuentes dejavu. Si ve gráficos sin texto, esta podría ser la causa.
- PHP >= 5.1.6 para el frontal web basado en Kohana.
- Nagios >= 2.x.
- Kohana necesita que el módulo de Apache "mod_rewrite" esté habilitado. Para más detalles, revise la documentación específica de su distribución sobre su servidor web.

1.14.2 Versiones:

El desarrollo de PNP está organizado usando Sourceforge.Net. PNP está registrado bajo "PNP4nagios".

La versión estable actual 0.4.x se puede encontrar en el área de descarga: Sourceforge Download.

Si se quiere estar al día, se puede usar la última versión de desarrollo de la rama 0.4.x que se genera automáticamente sobre una base diaria desde el repositorio SVN.

A partir de la versión PNP 0.6.x el repositorio de código fuente ha cambiado de SVN a GIT.

La versión actual de desarrollo puede verse en cualquier momento en http://pnp4nagios.git.sourceforge.net/. Haciendo click en PNP Devel version descargará un archivo que contiene la última versión.

1.15 NAGVIS

En su página web oficial Black Duck Software[38], se refiere a NagVis como un complemento de visualización para el conocido sistema de gestión de red Nagios. NagVis se puede utilizar para visualizar datos Nagios, por ejemplo, para mostrar procesos de TI como un sistema de correo o una infraestructura de red. Utilizando los datos suministrados por un backend, actualizará los objetos colocados en los mapas en ciertos intervalos para reflejar el estado actual. Estos mapas permiten organizar los objetos para mostrarlos en diferentes diseños:

[38] Black Duck Software, Inc. . (01 de 01 de 2013). Nagvis. Obtenido de Nagvis: http://nagvis.org/

- Físico (por ejemplo, todos los anfitriones en un rack / habitación / departamento).
- Lógico (por ejemplo, todos los servidores de aplicaciones).
- Geográfica (por ejemplo, todos los anfitriones de un país).
- Procesos empresariales (por ejemplo, todos los hosts / servicios involucrados en un proceso)

1.15.1 Funcionamiento general de Nagvis. Las diferentes vistas en NagVis se llaman "mapas". El tipo clásico y más común de mapas de NagVis son los mapas estáticos. Esto significa que se crea una configuración de mapa usando el editor de configuración basado en web o usando un editor de texto para crear la configuración del mapa.

En NagVis 1.7xa se ha realizado una nueva extensión a la configuración del mapa. Todavía se basa en el enfoque de configuración de mapas estáticos, pero ahora es posible ampliar esas partes de configuración estáticas mediante mecanismos dinámicos y programables.
La nueva característica ha sido llamada "fuentes de mapa". Cada mapa puede hacer uso de una o varias fuentes de mapa. Cada una de estas fuentes puede borrar, reemplazar o alterar toda la configuración del mapa.

Una fuente de mapa está construida con varias funciones de PHP que toman un conjunto estandarizado de parámetros para hacer su trabajo. Las funciones son completamente gratuitas en lo que están haciendo. Una fuente puede leer archivos CSV con objetos y coordenadas, puede conectarse a bases de datos para buscar información o leer datos de servicios externos. Depende del desarrollador.

Los backends soportados, son:

- Mklivestatus (predeterminado desde NagVis 1.5).
- NDOUtils / IDOUtils (requiere MySQL).
- Merlin (requiere MySQL)

Se puede colocar todos los objetos de Nagios (host, servicios, grupos de hosts, grupos de servicios) en los mapas llamados. Cada mapa se puede configurar a través de su propio archivo de configuración. Además, se puede editar los archivos de configuración directamente usando su editor de texto favorito o los mecanismos de configuración web. Como también, se puede agregar algunos objetos NagVis especiales a los mapas. Estos objetos son formas, cuadros de texto y objetos de referencia para otros mapas.

Cada uno de los objetos de los mapas se puede configurar para satisfacer necesidades de diferentes tipos de redes de datos. Por ejemplo, hay enlaces al frontend de Nagios en cada objeto que representa un objeto Nagios. Se puede personalizar fácilmente estos enlaces.

Hay un menú flotante que está activado de forma predeterminada. El menú flotante muestra información detallada para cada objeto. Los menús orientables se pueden modificar fácilmente cambiando las plantillas para ellos. También puede desactivar el menú de desplazamiento.

De forma predeterminada, el estado de los objetos se muestra mediante iconos en el mapa. Se puede cambiar estos iconos añadiendo conjuntos de iconos de la página principal de NagVis o crear los suyos. El estado de los objetos también se puede mostrar como líneas o como gadgets.

Aparte de los mapas normales hay un automap. Los objetos son lugares que comienzan automáticamente desde la host raíz especificado. Dependiendo del valor del directice "filter_by_state" mostrará todos los objetos o sólo los que están en un estado no OK (incluyendo el camino desde el objeto raíz).
Para poder utilizar el automap se tiene que definir las directivas de los padres en sus objetos del anfitrión de Nagios.

1.15.2 Licencia. NagVis es un software libre; puede redistribuirlo y / o modificarlo bajo los términos de la versión 2 de la Licencia Pública General GNU publicada por la Free Software Foundation.

NagVis es distribuido con la esperanza de que sea útil, pero SIN NINGUNA GARANTÍA; sin la garantía implícita de COMERCIABILIDAD o ADECUACIÓN PARA UN PROPÓSITO PARTICULAR.

1.15.3 Requisitos del sistema. Se necesita un Nagios instalado, configurado y en funcionamiento para que NagVis funcione.

MKLivestatus (instalado, agregado a Nagios).
Desde NagVis 1.5 se ha cambiado el backend por defecto a MKLivestatus ya que es mucho más rápido, más ligero y estable que el NDO. Por último, pero no menos importante es fácil de manejar e instalar. No se necesita ninguna base de datos para ejecutar MKLivestatus.
MKLivestatus es un módulo de Broker de eventos para Nagios que sirve un socket unix en el que se pueden conectar aditamentos de terceros como NagVis para recopilar información de estado en vivo de una manera muy rápida.

Se puede obtener MKLivestatus desde la página oficial de MKLivestatus.
Servidor web con soporte PHP.

NagVis es una aplicación basada en web realizada en Javascript y PHP. Necesita un servidor web con soporte de PHP para ejecutar NagVis. Recomendamos el uso de Apache Webserver con mod_php.

El requisito de versión mínima de PHP es 5.0.0.

Además del paquete php base, son necesarios los siguientes módulos en la instalación de PHP. Los nombres de los módulos pueden variar entre distribuciones:

- php5-gd
- php5-gettext
- php5-mbstring
- sesión php5
- php5-json (Builtin desde PHP 5.2).
- php5-pdo y pdo-sqlite (Nuevo en 1.5, para el módulo de Autenticación / Autorización por defecto).
- Nota: Tal vez algunas de estas funciones ya están compiladas en su PHP. php –m mostrará los módulos incorporados.

1.15.4 Requisitos especiales por backends. Los backends se conectan a fuentes de datos externas y a menudo necesitan algunos módulos especiales. Aquí hay una lista de los módulos necesarios para los diferentes backends. Sólo se necesita cumplir con los requisitos de los backends que utiliza.

- Mklivestatus
- php-net-socket (Debian) / php5-sockets (SLES)
- nydy
- php5-mysql
- Merlinmy
- php5-mysql
- Graphviz para el automap

El Automap se basa en Graphviz. Se necesita cuando se quiera usar la función automap. Se recomienda el uso de la versión de Graphviz> = 2.14 (Las versiones anteriores (con números de versión más bajos) tienen algunos problemas con la representación truecolor).

Graphviz está disponible en algunas distribuciones. Cuando no se puede utilizar un paquete de distribución precompilado, se puede obtener Graphviz desde la página oficial de Graphviz para compilarlo por su cuenta.

También se necesitará más paquetes como gd, libpng, freetype, pero si se obtiene graphviz compilado y / o instalado debe funcionar.

1.16 ARQUITECTURA DE UNA SOLUCIÓN DE MONITORIZACIÓN BASADA EN CHECK_MK

En la siguiente imagen, la arquitectura de bloques muestra la interacción del núcleo de monitoreo Nagios con el resto de complementos, Check_MK, PNP4 y Nagvis. (Ver figura 11).

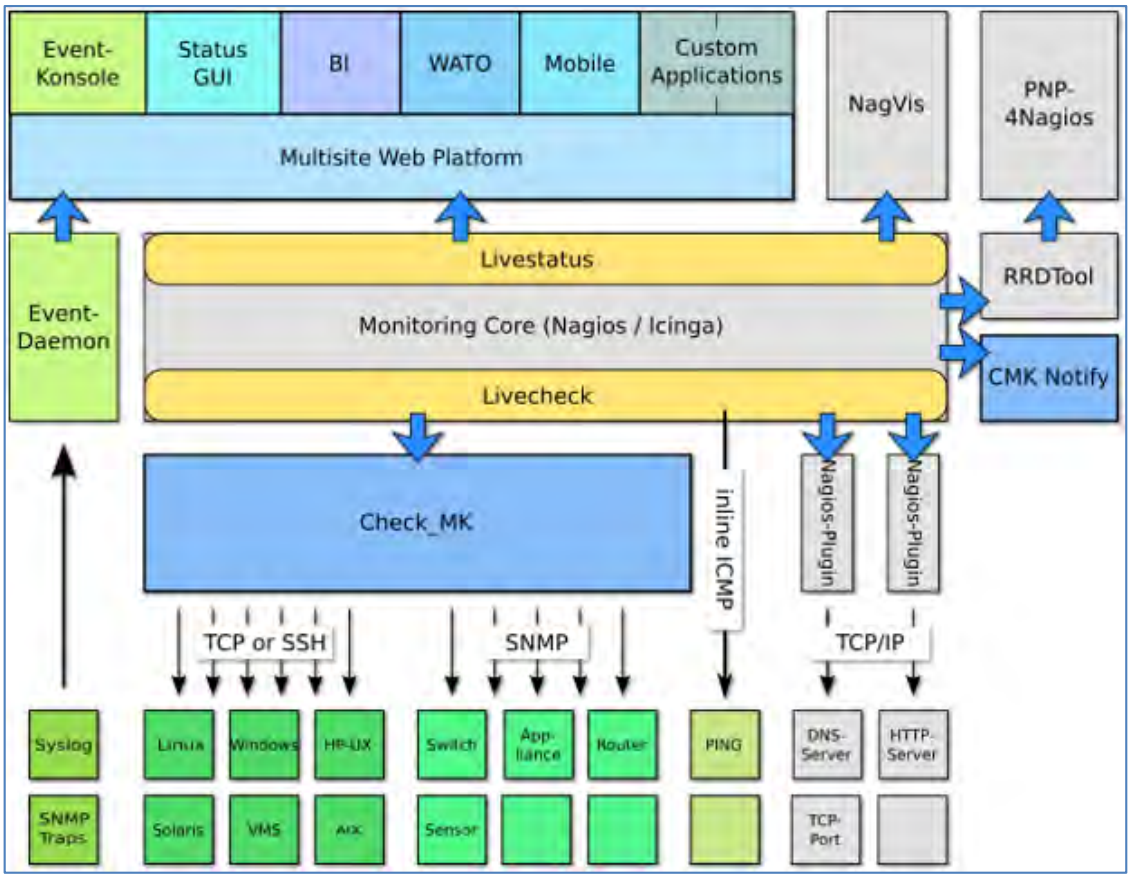


Figura 11. Arquitectura integrada Nagios, nagvis, check_mk, pnp4.
Fuente. (Kettner, 2017).

1.17 OTRAS HERRAMIENTAS DE MONITOREO

En la siguiente tabla 3, se muestra las herramientas de monitoreo con las características más relevantes que una herramienta de estas debería tener.

Nombre	Gráficas	Informes	Grupos lógicos	Estadísticas	Autodescubrimiento	Agentes	SNMP	Complementos (*plugins*)	Alertas	Aplicación web	Monitorización
i-enable	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pandora FMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Entuity	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Nimsoft	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Netscope	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zyrion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PacketTrap	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
dopplerVUE	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
CA eHealth	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
Nagios	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LoriotPro	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ganglia	✓	Desconocido	✓	Desconocido	✓	✓	✓	✓	✓	Sólo visualización	✓
op5 Monitor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zabbix	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Munin	✓	✓	✓	✓	✓	✓	✓	✓		Sólo visualización	Desconocido
Cacti	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Desconocido
Zenoss	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Argus	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	
Hobbit Monitor	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
OpenNMS	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓
FireScope BSM: BE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SolarWinds Orion	✓	Desconocido	Desconocido	✓	✗	✓	tabla comparacion.jpg		✓	✓	✓
GroundWork Community	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗
GroundWork Enterprise	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
NeDi	✓	Desconocido	✗	✓	✗	✗	✓	✗ Desconocido	✓	✓	Desconocido
Wormly	✓	Desconocido	✗	✓	✗	✓	✗	✗	✓	✓	✓
Hyperic	✓	Desconocido	✓	Desconocido	✓	✓	✓	✓	✓	✓	✓
Osmius	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Tabla 3. Tabla comparativa de herramientas de monitoreo de red.
Fuente. (Duque Padilla, 2011)

A continuación, se describirán cuatro de las herramientas de monitoreo de red más utilizadas.

1.17.1 Pandora fms. Según lo encontrado en el sitio oficial Pandora org[39], pandora FMS es un software de monitorización para gestionar infraestructuras IT. Esto incluye equipos de red, servidores Windows y Unix, infraestructura virtualizada y todo tipo de aplicaciones. Pandora FMS tiene multitud de funcionalidades, las cuales lo convierten en un software de nueva generación que cubre todos los aspectos de monitorización que requiere su compañía.

Pandora FMS puede medir el ancho de banda de su red, consultando su router/switch mediante SNMP o también procesando las estadísticas de Netflow enviadas por su router. Routers modem, switches, modems, API's y otros equipos de red usan un lenguaje común: SNMP. Con Pandora FMS se puede configurar cualquier dispositivo con un par de clicks, y empezar a monitorizar el ancho de banda, el estado de la interfaz, promedio de carga, espacio de almacenamiento y uso de la memoria entre otras muchas cosas.

1.17.2 Mumin. Según el sitio oficial (Munin org., 2017), Munin la herramienta de monitoreo examina todas las computadoras y recuerda lo que vio. Presenta toda la información en gráficos a través de una interfaz web. Su énfasis está en las capacidades plug and play. Después de completar una instalación, un gran número de complementos de monitorización se reproducirá sin más esfuerzo.

Con Munin se puede monitorear fácilmente el rendimiento de computadoras, redes, SANs, aplicaciones, mediciones meteorológicas y lo que le venga a la mente. Hace que sea fácil determinar "lo que es diferente hoy en día" cuando surge un problema de rendimiento. Hace que sea fácil ver cómo se está haciendo en función de la capacidad en cualquier recurso.

Munin utiliza el excelente RRDTool (escrito por Tobi Oetiker) y el framework está escrito en Perl, mientras que los complementos pueden ser escritos en cualquier idioma. Munin tiene una arquitectura maestra / nodo en la que el maestro se conecta a todos los nodos a intervalos regulares y les pide datos. A continuación, almacena los datos en los archivos RRD, y (si es necesario) actualiza los gráficos. Uno de los principales objetivos ha sido la facilidad de crear nuevos complementos (gráficos).

[39] Pandora org. (01 de 01 de 2017). Pandora fms community. Obtenido de Pandora fms community: https://pandorafms.org/es/producto/introduccion-a-pandora-fms/

1.17.3 Zabbix. En el sitio oficial Zabbix LLC[40], la herramienta de monitoreo de rede Zabbix es el último software de nivel empresarial diseñado para monitorear la disponibilidad y el rendimiento de los componentes de la infraestructura de TI. Zabbix es de código abierto y viene sin costo alguno.

Con Zabbix es posible reunir tipos virtualmente ilimitadas de datos de la red. Alto rendimiento monitoreo en tiempo real significa que decenas de miles de servidores, máquinas virtuales y dispositivos de red pueden ser monitoreados simultáneamente. Junto con el almacenamiento de los datos, características de visualización son disponibles (descripciones, mapas, gráficos, pantallas, etc.), así como varios métodos flexibles de análisis de los datos con el fin de alertar.

Zabbix ofrece un gran rendimiento para la recolección de datos y se puede escalar a entornos muy grandes. Ofrece opciones de monitorización distribuidos que están disponibles con el uso de proxies Zabbix. Zabbix viene con una interfaz basada en la web, autenticación de usuarios segura y un esquema de permisos de usuario flexible. Sondeo y la captura se admite, con agentes de alto rendimiento, reuniendo datos de prácticamente cualquier sistema operativo populares; métodos de control sin agentes están disponibles también.

El monitoreo web, así como la vigilancia de las máquinas virtuales de VMware es posible con Zabbix. Zabbix puede descubrir automáticamente los servidores y dispositivos de red, así como realizar el descubrimiento de bajo nivel con los métodos de asignación automática de controles de rendimiento y disponibilidad de entidades detectadas.

1.17.4 Cacti. En la página oficial Cacti Group[41], Cacti es una solución completa de gráficos de red diseñada para aprovechar el poder de RRDtool que almacena toda la información necesaria para crear gráficos y rellenar con los datos en una base de datos MySQL. La interfaz está completamente impulsada en PHP. Cacti proporciona un fast poller, plantillas gráficas avanzadas, múltiples métodos de adquisición de datos y gestión de usuarios. Además, de ser capaz de mantener gráficos, fuentes de datos y archivos de Round Robin en una base de datos. También hay soporte SNMP para la creación de gráficos de tráfico con MRTG. Todo esto está envuelto en una interfaz intuitiva y fácil de usar, interfaz que tenga sentido para LAN e instalaciones de redes complejas con miles de dispositivos.

Una vez que una o más fuentes de datos se definen, un gráfico de RRDTool se puede crear con los datos. Cacti le permite crear casi cualquier gráfico de RRDTool

---

[40] Zabbix LLC. (01 de 01 de 2017). Zabbix. Obtenido de Zabbix: http://www.zabbix.com/

[41] Cacti Group, Inc. (01 de 01 de 2017). Cacti the complite rrdtool based graphing solution. Obtenido de Cacti the complite rrdtool based graphing solution: http://cacti.net/

imaginables utilizando todos los tipos estándar de gráficos rrdtool y funciones de consolidación. Un área de selección de color y la función automática de relleno de texto también ayuda en la creación de gráficos para hacer el proceso más fácil.

No sólo se puede crear gráficos basados en rrdtool cacti, hay muchas formas de mostrarlos. Junto con una "vista de la lista" estándar y un "modo de vista previa", que se asemeja a la interfaz de RRDTool 14all, hay una "vista de árbol", que le permite poner gráficos en un árbol jerárquico para los propósitos de la organización.

Debido a las muchas funciones de cacti, una herramienta de gestión basada en el usuario, este está construido en que puede añadir usuarios y darles derechos a ciertas áreas de cacti. Esto permitiría que algunos usuarios pueden cambiar los parámetros del gráfico, mientras que otros sólo pueden visualizar las gráficas. Cada usuario también mantiene su propia configuración cuando se trata de gráficos de visualización.

Por último, cacti es capaz de escalar a un gran número de fuentes de datos y gráficos mediante el uso de plantillas. Esto permite la creación de una única plantilla, gráfico o fuente de datos que define cualquier fuente o gráfico de los datos asociados con él. Plantillas de acogida permiten definir las capacidades de un huésped, de modo que los cactus pueden sondear para obtener información sobre la adición de un nuevo huésped.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Analizar, diseñar e implementar una suite de monitoreo de redes de datos de código abierto en la empresa JL Y RB S.A.S- ELECTROMILLONARIA que facilite la administración de la red en tiempo real.

2.2 OBJETIVOS ESPECÍFICOS

- Caracterizar la información necesaria para el despliegue de la instalación de la suite de monitoreo de red de datos, compuesta por la herramienta de monitoreo Nagios y las herramientas de administración, Check_mk, Nagvis y Pnp4nagios.

- Analizar la situación actual de la red de datos.

- Diseñar los diagramas físico y lógico de la red de datos de la empresa.

- Instalar los servicios de red web, proxy, SSH, DNS, Open Fire y FTP en entorno virtual.

- Implementar y configurar la suite de monitoreo en entorno virtual para monitorear servicios, equipos y componentes de red en diferentes plataformas dentro de la red de datos.

- Instalar la suite de monitoreo configurando un servicio de seguridad para dicha suite.

- Migrar los archivos de configuración al servidor en la sede principal de la empresa JL Y RB S.A.S- ELECTROMILLONARIA en la ciudad de Pasto.

- Colocar en marcha la suite de monitoreo y realizar pruebas de funcionamiento.

- Obtener reportes del moniteo con Nagios.

- Instalar y configurar un servidor espejo dentro de la empresa como respaldo de la configuración del servidor donde funciona la suite de monitoreo de la red de datos.

- Presentar un entregable al jefe de sistemas de la empresa JL Y RB S.A.S-ELECTROMILLONARIA que contendrá todo lo relacionado con la implementación y uso de la suite de monitoreo de la red de datos.

- Realizar una capacitación al personal que estará encargado de la suite de monitoreo de la red de datos después de su implementación y configuración.

3. JUSTIFICACIÓN

Actualmente las empresas han sistematizado todos sus procesos debido al avance de la tecnología, la cual brinda una optimización de tiempo y disminución de costos mejorando la competitividad de las empresas en el mercado, además contribuye en tomas de decisiones para mejorar siempre el servicio que se ofrece en cada una de estas sin importar su labor, lo que hace depender de los servicios que brinda el área de redes y servicios telemáticos, tanto la red de datos como los servicios tienden a estar vulnerables a fallos continuamente que afectan en una forma parcial o total al sistema, por tal motivo toda empresa requiere de un administrador que se encargue de gestionar tales servicios que están dentro de la red de datos para que se asegure una prestación de servicios con calidad, ya que toda empresa que dependa económicamente de la venta de sus servicios debe tener clientes satisfechos.

En la actualidad existen diversas plataformas que ayudan al administrador a gestionar la red de datos en tiempo real, siendo muy utilizadas en el ámbito empresarial y mucho más cuando estas tienen puntos de conexión en diferentes lugares, es por ello que la empresa JL Y RB S.A.S- ELECTROMILLONARIA busca la implementación de una plataforma.

Con el objetivo de implementar en esta empresa una suite de gestión de red de datos, se llevó a cabo el trabajo análisis, diseño e implementación de una suite de monitoreo a la red de datos de la empresa JL Y RB S.A.S- ELECTROMILLONARIA, en la etapa de análisis se estudió la información recolectada de la situación actual para detectar los problemas en la red de datos y definir las necesidades de la empresa para plantear los objetivos, llegando a las respectivas soluciones. Las dos siguientes etapas dependen de los resultados del análisis, la etapa de diseño permite establecer oficialmente un diagrama lógico y físico actualizado de la red de datos, dichos diagramas contribuyen a obtener un inventario actualizado de los componentes de la red de la empresa, esto ayuda a renovar el hardware y el software de acuerdo a las necesidades. Además, dichos diagramas sirven como recurso para ubicar tanto los componentes como el diseño de la red de datos para la toma de decisiones en caso de modificar o actualizar la red.

Conociendo las necesidades de la empresa, se estableció la implementación de una suite de monitoreo, compuesta por: Nagios como nucleo de la suite y herramientas de administración como: Check_MK, Nagvis y Pnp4nagios. Nagios es una plataforma de gestión de redes que monitoriza activamente la disponibilidad de nodos y servicios en tiempo real, permitiendo anticiparse a las fallas antes de que los usuarios de la misma los perciban. Nagios tiene una licencia libre GPL v2 (General Public License versión 2), por tal motivo, no implica costos de mantenimiento ni de licencia de instalación y uso. De igual forma, la herramienta de

administracion Check_mk cuenta con una interface web amigable y de fácil uso que visualiza detalladamente el estado activo o inactivo de actividades y procesos dentro de la red de datos. Además, permite llevar un historial de eventos que contribuyen a tomas de decisiones, y una de las principales características de esta herramienta es permitir la configuración para enviar notificaciones mediante email, facilitando el trabajo al administrador del sistema, lo que le ayuda a estar al tanto de otras actividades para beneficio de la empresa. La herramienta Nagvis hace posible la visualización del diagrama lógico de la red por medio de la interface gráfica, facilitando la localización inmediata de fallos. Esta suite de monitoreo es administrable desde la web lo que permite solucionar fallos remotamente para garantizar la disponibilidad de los servicios de la empresa.

La fácil adaptabilidad de nuevos dispositivos a la configuración de la suite para ser monitoreados, permite que la empresa tenga una proyección a futuro, no solo para monitorear las agencias de la Ciudad de Pasto sino también para tener una gestión completa a nivel Nacional.

La implementación de la suite de monitoreo de red de datos propuesta en este trabajo, es la mejor opción para la empresa JL Y RB S.A.S- ELECTROMILLONARIA de acuerdo a los resultados del análisis de la red de datos, este trabajo contribuyó a dar solución a problemas que actualmente afectan el normal desarrollo de los procesos internos de la empresa, y debido a que más de 350 empleados dependen del buen funcionamiento del sistema se considera que el impacto de este trabajo es considerablemente alto. Con su implementación se mejorará su competitividad a nivel regional, aumentando ingresos y disminuyendo costos innecesarios por no contar con una plataforma de gestión de la red de datos.

4. ANTECEDENTES

En la búsqueda de antecedentes que beneficien al proceso de contextualización del trabajo se encontraron proyectos realizados en diferentes entidades, en su mayoría orientados a la implementación y configuración de la herramienta Nagios para la gestión de la red de datos.

4.1 ANTECEDENTES INTERNACIONALES

En el ámbito internacional se encontró el proyecto IMPLEMENTACIÓN DE UN SERVIDOR NAGIOS PARA EL CONTROL Y MONITOREO DE LA RED DEL GDF realizado por Martínez Ramírez[42], el cual implementa un sistema de monitoreo de red dentro de la Secretaria de Finanzas de la ciudad de México, con el fin de detectar de forma inmediata problemas que se presentan dentro de la red de datos antes de que los usuarios se percaten de ello.

De acuerdo con el contenido de este trabajo se encontraron similitudes en cuanto a la implementación, instalación y configuraciones necesarias, así como las acciones que se toman para notificar de la existencia de algún problema, además de la entrega de un documento final, el cual incluye la instalación y configuración de la herramienta de monitoreo de red Nagios.

En cuanto a las diferencias se encontró, que no realizan una recolección de información previa del estado actual de la red de datos, además no poseen un diseño lógico y físico de la infraestructura de la red, como también no se encontró que realizaran una simulación en un entorno virtual antes de la puesta en marcha en el servidor real, por último, en este trabajo no se encontró que se realizara una capacitación al personal encargado del área en donde se implementó la herramienta.

En conclusión, este trabajo posee más diferencias que similitudes con el que se desea realizar, pero contribuye con valiosa información de gran ayuda al momento de implementar nuestro trabajo.

Otro antecedente encontrado en el ámbito internacional tiene como nombre ANALISIS, DISEÑO E IMPLEMENTACION DE UNA HERRAMIENTA DE

---

[42] Martínez Ramírez, S. (01 de 01 de 2016). Repositorio digital de la Facultad de Ingeniería - UNAM. Recuperado el 24 de 02 de 2017, de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/10527/Tesina.pdf?sequence=1

MONITOREO Y CONTROL DE DATACENTER BASADO EN HERRAMIENTAS OPEN SOURCE. APLICADO AL BANCO DE GUAYAQUIL, realizado por Alvarez Cevallos[43], el cual se basa en la implementación de la herramienta open source Nagios y Cacti, por un lado Nagios se encarga del monitoreo del hardware y software de la red datos, facilitando al administrador la detección oportuna de fallos mediante sistemas de alarmas. Por otro lado, Cacti se encarga de mantener un historial del consumo de interfaces de red, lo cual facilita mediante graficas detectar anomalías en la red y elementos hardware tales como CPU y RAM.

De acuerdo con lo observado en este trabajo se encontraron similitudes en cuanto al estudio previo realizado para identificar el problema y así poder plantear los objetivos, además se encontró que las herramientas utilizadas en este trabajo funcionan bajo la arquitectura SNMP el cual facilita el intercambio de información de administración entre dispositivos de red.

En cuanto a diferencias encontradas en este trabajo se identificó que se plantea modificar el código fuente de las herramientas Nagios y Cacti adaptándolas a las necesidades de la empresa, además la metodología empleada está relacionada con la construcción de software y no con la gestión de redes de datos.

En conclusión, los aportes brindados al trabajo que se realizará están ligados a la configuración y uso de la herramienta Nagios ya que se encontró un tutorial detallado.

4.2 ANTECEDENTES NACIONALES

Dentro del ámbito Nacional se encontró el trabajo titulado SISTEMA DE MONITOREO MEDIANTE NAGIOS EN LA EMPRESA AST GRUPO DE LA CIUDAD DE PEREIRA, realizado por Duque Padilla[44], el cual se basa en la implementación de Nagios como servicio de monitoreo de la red de datos de AST en la ciudad de Pereira, esto con el fin de prevenir y detectar errores principales dentro de la red de dicha empresa.

Las similitudes en cuanto a nuestro trabajo están en el objetivo, el cual busca prevenir y detectar errores dentro de la red. Además, se realiza una obtención de información y se procede a la instalación y configuración de Nagios, también utiliza

---

[43] Alvarez Cevallos, A. (01 de 04 de 2015). Repositorio digital Universidad Politécnica Salesiana Ecuador. Recuperado el 25 de 02 de 2017, de http://dspace.ups.edu.ec/bitstream/123456789/10298/1/UPS-GT001194.pdf

[44] Duque Padilla, A. S. (101 de 01 de 2011). Biblioteca virtual Universidad Católica de Pereira CDCH. Obtenido de Biblioteca virtual Universidad Católica de Pereira CDCH: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/3007/CDPEIST61.pdf?sequence=1

la configuración de sistema de alarmas y visualización del estado de la arquitectura de la red.

En cuanto a las diferencias, se logró evidenciar que solo se realizó un monitoreo de la red en la ubicación principal de la empresa en la ciudad de Pereira, nuestro trabajo realizara monitoreo en nueve puntos diferentes de la empresa en la ciudad de Pasto, con diferentes medios de transmisión , no realiza diseño de la red lógico y físico de la red de datos, ni realiza pruebas de instalación y configuración antes de la ejecución de Nagios en el entorno real, como también no lleva a cabo capacitación al personal implicado en la gestión de la red de datos de dicha empresa.

Este trabajo aporta información de la comparación gráfica de las características de diversas herramientas de monitoreo. Además, de manuales de instalación y configuración que se tendrán en cuenta en el desarrollo de este trabajo.

Otro de los antecedentes encontrados es el trabajo titulado ACTUALIZACIÓN DE NAGIOS HERRAMIENTA DE MONITOREO DE LA EMPRESA UNE – TELEFÓNICA DE PEREIRA EN EL 2013, realizado por Zuleta Londoño[45], este trabajo tiene como objetivo actualizar la herramienta de monitoreo Nagios como sugerencia para mejorar la gestión de la red de datos y aumentar funcionalidades de monitoreo a la empresa Une-Telefónica Pereira.

Dentro de las similitudes se puede decir que se tiene en común, la búsqueda de mejorar y facilitar la gestión de la red de datos de las empresas mediante la herramienta Nagios y la adaptación de la herramienta a las necesidades de cada empresa.

Las diferencias son notorias debido a que este trabajo solo se dedica a la actualización de la herramienta, eso quiere decir que no realiza ninguna de las actividades que se plantean realizar en nuestro trabajo.

En conclusión, el trabajo contribuye en cuanto a conocer la herramienta de una forma gráfica, detallando diversas funcionalidades de Nagios. Nos muestra la importancia de su funcionamiento en la empresa ya que esta necesitaba de la actualización de la herramienta para un mejor desempeño. Además, de dar a conocer conceptos relacionados con el proceso de gestión de redes de datos.

4.3 ANTECEDENTES REGIONALES

[45] Zuleta Londoño, M. Á. (01 de 01 de 2013). Biblioteca virtual Universidad Católica de Pereira CDCH. Obtenido de Biblioteca virtual Universidad Católica de Pereira CDCH: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/2000/DDPAIST36.pdf?sequence=1

En el ámbito regional se encontró el trabajo con nombre ANUBIS, SUITE DE APLICACIONES DESTINADAS A LA ADMINISTRACION DE SERVICIOS DE REDES DE ÁREA LOCAL TIPO IP BAJO PLATAFORMA GNU/LINUX, realizado por, Arellano Ruiz & Cuasquer Viveros[46], este trabajo fue realizado y ejecutado en la Universidad de Nariño, con el fin de controlar y administrar los servicios prestados a los usuarios de la red OASI dentro de la institución Universitaria, mediante la creación de un sistema modular. Los servicios que fueron tenidos en cuenta para ser administrados fueron: servicio de correo electrónico, servidor proxy, filtro web, ancho de banda, corta fuegos (firewall), usuarios conectados en la red. Esto con el objetivo de que los usuarios finales se beneficien de forma transparente de la mejora de uso de dichos servicios.

Las similitudes frente al trabajo realizado, son en cuanto a la implementación de software libre para administrar servicios dentro de la red, con el fin de mejorar la prestación de los servicios a los usuarios finales. Realizan un análisis de la situación actual de la red y posteriormente un modelo estructurado del funcionamiento del sistema de la red.

La diferencia notoria encontrada es que no se utiliza la herramienta de gestión de red basada en el protocolo SNMP (Nagios), el trabajo se basa en crear un nuevo sistema que solo monitoree servicios y no componentes hardware dentro de la red. Además, se fundamenta en una metodología de desarrollo de software como es el modelo RUP que contiene diagramas UML como, por ejemplo: diseño de bases de datos, casos de uso, entre otras. Debido a que el objetivo del trabajo es la codificación de un sistema para mejorar la administración de la red.

El aporte de este trabajo, radica en la información que nos brinda del funcionamiento de servicios dentro de la red, ya que nuestro trabajo tiene como uno de los objetivos administrar tales servicios, como también una información amplia del protocolo IP, sus componentes y funcionamiento.

[46] Arellano Ruiz, J. F., & Cuasquer Viveros, D. A. (01 de 01 de 2007). Biblioteca virtual Alverto Quijano Guerrero. Obtenido de Biblioteca virtual Alverto Quijano Guerrero: http://biblioteca.udenar.edu.co:8085/bibliotecavirtual/viewer.aspx?&var=70963

5. METODOLOGÍA

A continuación, se describe la metodología utilizada para el desarrollo de este trabajo. Para esta se tuvo en cuenta las necesidades de la empresa, el alcance y delimitaciones anteriormente expuestas.

1. Administración de la configuración.
1.1 Planeación de la implementación y diseño de los diagramas de la red.
1.1.1 Obtención de información de las necesidades de la red de datos y requerimientos para el buen funcionamiento de la herramienta de gestión de red.
1.1.2 Análisis de la información recopilada y diagramas físico y lógico de la empresa.
1.2 Instalación y administración de la herramienta de gestión de datos.
1.2.1 Actualización de software y hardware de la red de datos si es necesario para la instalación de la herramienta de gestión de red.
1.2.2 Respaldo de configuraciones actuales de los equipos que están dentro de la red si es necesario volver a un estado anterior.
1.2.3 Instalación, configuración y administración de la herramienta de gestión de red.

2. Administración del rendimiento.
2.1 Monitoreo.
2.1.1 Monitoreo de los estados activos e inactivos de los dispositivos que componen la red de datos (impresoras, switch, routers, servidores, host).
2.1.2 Monitoreo de los recursos hardware (carga de procesador, uso de discos, uso de memoria RAM, número de usuarios conectados).
2.1.3 Monitoreo de servicios (HTTP, SMTP, SNMP, ICMP, POP3, FTP, SSH, PING.)
2.1.4 Monitoreo del tráfico de la red.
2.2 Análisis.
2.2.1 Análisis del administrador de la red de datos de la empresa de los reportes obtenidos (utilización elevada, trafico inusual, elementos principales de la red, calidad de servicio, control de tráfico) a través de la herramienta de gestión de red para la toma de decisiones.

3. Administración de fallas.
3.1 Monitoreo de alarmas.
3.1.1 Configuración de la herramienta de gestión de red para enviar alarmas por medio de MNS y/o correo electrónico de anomalías que se presenten dentro de la red de datos de la empresa gracias a que la herramienta se basa en el protocolo SNMP.

3.2 Localización de fallas.
3.2.1 Configuración de la herramienta de gestión de red para visualizar de forma gráfica el diagrama lógico de la red de datos debido a que la herramienta cuanta con una interface web de usuario.
3.2.2 Realización de pruebas de diagnóstico para verificar el buen funcionamiento de la implementación de la herramienta de gestión de red.
3.3 Corrección de fallas.
3.3.1 Corrección de fallas por parte del administrador de la red de datos de la empresa según el diagnóstico reportado con la herramienta de gestión de red.
3.3.2 Administración de reportes.
3.3.3 Administración de reportes por parte del administrador de la red de datos de la empresa.

4. Documentación y capacitación de personal.
4.1 Elaboración de la documentación y entrega del informe final.
4.2 Capacitación al personal del área de sistemas de la empresa.

Tabla 4. Tabla de análisis de secuencia de actividades.

ACTIVIDADES ANTERIORES	ACTIIVIDADES PLANEADAS			ACTIVIDADES POSTERIORES
	ORDEN	DETALLE	DURACION SEMANAS	
--	A	Obtener la información necesaria para llevar a cabo la implementación de la plataforma de monitoreo (Nagios).	4	B
A	B	Analizar la información de la situación actual de la red de datos de la empresa JL Y RB S.A.S-ELECTROMILLONARIA	2	C
B	C	Diseñar el diagrama lógico y físico de la red de datos de la empresa JL Y RB S.A.S-ELECTROMILLONARIA	2	F
--	D	Consultar los requerimientos necesarios para el buen funcionamiento de Nagios.	3	E
D	E	Instalación de la plataforma de monitoreo Nagios en un entorno virtual.	3	F
C,E	F	Configuración de la plataforma de monitoreo Nagios en entorno virtual para monitorear servicios y equipos en diferentes plataformas dentro de la red de datos.	7	G

ACTIVIDADES ANTERIORES	ACTIIVIDADES PLANEADAS			ACTIVIDADES POSTERIORES
	ORDEN	DETALLE	DURACION SEMANAS	
F	G	Realización de pruebas en entorno virtual	3	H
G	H	Migración de la suite de monitoreo al servidor de la empresa JL Y RB S.A.S- ELECTROMILLONARIA	6	I
H	I	Instalacion y configuración de servidor espejo. Realización de pruebas y obtención de reportes.	2	k
--	J	Preparación del informe final y entrega al jefe de sistemas de la empresa JL Y RB S.A.S- ELECTROMILLONARIA	32	K
J	K	Capacitación del personal del área sistemas de la empresa JL Y RB S.A.S- ELECTROMILLONARIA	2	--

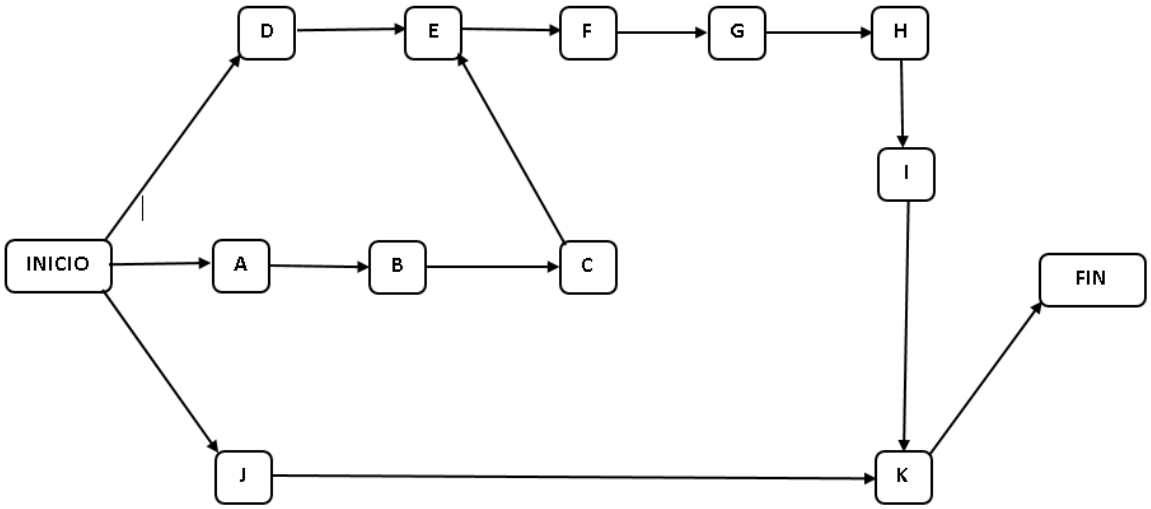


Figura 12. Diagrama de secuencia de actividades.

6. RESULTADOS ESPERADOS

- Apropiación y aplicación en entorno real de conocimientos relacionados con redes de datos, modelo OSI, protocolos, SNMP, plataformas de monitoreo, servicios de internet, servicio de seguridad, gestión de redes de datos, replica de datos.

- Conocimiento de la implementación, configuración y funcionamiento de las herramientas Nagios, Check_MK, Nagvis, PNP4Nagios.

- Analisis de la situación actual de la red de datos.

- Diseño actualizado del diagrama lógico y físico de la red de datos de la empresa JL Y RB S.A.S- ELECTROMILLONARIA.

- Funcionamiento de la suite de monitoreo en la sede principal de la empresa JL Y RB S.A.S- ELECTROMILLONARIA monitoreando todos los elementos que componen la red de datos de la sede principal en la Ciudad de Pasto.

- Monitoreo de todos los equipos de las 9 agencias en la Ciudad de pasto con su respectivo radio enlaces.

- Monitoreo del equipo principal en las sedes de las ciudades de Tumaco, Mocoa, Popayán, Yumbo y Cali.

- Reportes del monitoreo con Nagios.

- Funcionamiento del servidor espejo en la sede principal de la empresa.

- Mejorar y Facilitar la gestión de la red de datos dentro de la empresa.

- Informe final del trabajo.

- Actas de capacitación al personal de la empresa.

7. RECURSOS

7.1 RECURSOS HUMANOS

Tabla 5. Recursos humanos

RECURSO HUMANO	FORMACIÓN ACADÉMICA	CANTIDAD	FUNCIÓN DENTRO DEL TRABAJO	DEDICACIÓN HORAS/SEMANA	HONORARIOS MENSUALES EN PESOS
Asesor del trabajo	Ingeniero de sistemas	1	Es el encargado de la asesoría continua del trabajo	5	1.000.000
Desarrollador del trabajo	Estudiantes de ingeniería de sistemas	2	Son los encargados de la realización del trabajo dentro de la empresa	32	1.500.000
Personal del área de sistemas de la empresa	Ingeniero de sistemas	2	Brindar información de la empresa para llevar a cabo este trabajo	6	1.200.000
TOTAL					3.700.000

7.2 RECURSOS TECNOLÓGICOS

Tabla 6. Recursos tecnológicos

RECURSO (HW o SW)	JUSTIFICACIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
Computador i7 quinta generación 8GB DD 1TB	Necesario para realizar el trabajo escrito como también realizar las pruebas de la herramienta de monitoreo de red en un entorno virtual	2	1.500.000	3.000.000
Smart phone	Necesario para realizar registros (grabaciones, fotos, videos) que ayuden a la recolección de información	2	500.000	1.000.000
Disco duro portable 1 TB	Necesario para almacenar información del trabajo	1	120.000	120.000
Software Nagios	Software de monitoreo de red que se va a implementar en la empresa	1	0	0
Oracle VM VirtualBox	Necesario para montar el Sistema Operativo (Linux) en un entorno virtualizado	1	0	0
ISO (Linux Debian)	Sistema operativo donde será montada la herramienta de monitoreo en entorno virtualizado	1	0	0
TOTAL				4.120.000

7.3 RECURSOS MATERIALES

Tabla 7. Recursos materiales

MATERIALES	CANTIDAD	VALOR UNITARIO	SUBTOTAL
Resma de papel	1	150.000	150.000
CDs	5	2.000	10.000
Fotocopias	500	100	50.000
Carpetas	5	800	4000
Libros	4	0	0
Porta minas	4	1.500	6.000
borrador	2	500	1.000
lapicero	4	1.500	6.000
TOTAL			227.000

7.4 RECURSOS VARIOS

Tabla 8. Recursos varios

DESCRIPCION	VALOR MES
Servicio de Internet	30.000
Servicio de energía eléctrica	10.000
Transporte de estudiantes	96.000
Alimentación de estudiantes	300.000
SUBTOTAL	436.000

7.5 RECURSOS FINANCIEROS

Tabla 9. Recursos financieros

RUBROS	SUBTOTAL
Recursos Humanos	3.700.000
Recursos Tecnológicos	4.120.000
Recursos Materiales	227.000
Recursos varios	436.000
TOTAL	8.483.000

7.6 RECURSOS OPERATIVOS

Tabla 10. Recursos operativos

SOFTWARE A IMPLEMENTAR	DEPENDECIA DONDE SE UTILIZARÁ	PERSONAL NECESARIO PARA SU MANUPULACIÓN	CAPACITACIÓN	
			SI	NO
Herramienta de monitoreo de red Nagios	Departamento de Ingeniería de Sistemas de la empresa JL Y RB S.A.S-Electromillonaria de la ciudad de Pasto	3	x	

8. CRONOGRAMA

8.1 TABLA DE ACTIVIDADES

Tabla 11. Actividades planeadas para el desarrollo del trabajo.

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
1	Obtener la información necesaria para llevar a cabo la implementación de la suite de monitoreo compuesta por la herramienta de monitoreo Nagios y las herramientas de administración, Check_mk, Nagvis y Pnp4nagios.	Presentación de la empresa JL Y RB S.A.S-ELECTROMILLONARIA	1	4
		Identificación del diseño actual de la red de datos de la empresa.		
		Identificación de los equipos, servidores y componentes de red que van a ser monitoreados		
		Especificación de las características de equipos, servidores y componentes de red a ser monitoreados.		
		Obtención de las IP de los equipos, servidores y componentes de red que van a ser monitoreados.		
		Identificar los servicios de red que van a ser monitoreados.		

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
2	Analizar la situación actual de la red de datos de la empresa JL Y RB S.A.S-ELECTROMILLONARIA.	Utilización de herramientas para el análisis de la red de datos.	1	4
		Organización de la información obtenida.		
		Depuración de información obtenida.		
		Descripcion del estado, de los componentes físico de la red de datos.		
3	Diseñar el diagrama lógico y físico de la red de datos de la empresa JL Y RB S.A.S-ELECTROMILLONARIA	Realización del bosquejo del diagrama físico y lógico de la red de datos de la empresa.	2	6
		Utilización de la herramienta Visio para realizar el diagrama lógico y físico de la red de datos.		
		Verificación de los diagramas realizados con la fuente que suministro la información.		
4	Consultar los requerimientos de instalación y configuración de las herramientas que componen la suite de monitoreo.	Documentación del funcionamiento de la herramienta de monitoreo Nagios y las herramientas de administración.	4	3
		Establecer los requerimientos hardware y software para una correcta		

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
		instalación y configuración.		
5	Instalación de la suite de monitoreo en un entorno virtual.	Obtención de herramientas software para instalación en entorno virtual (VirtualBox, ISO Debian 8, Nagios, Check_mk, Nagvis, Pnp4nagios)	4	11
		Instalación y configuración de VirtualBox e ISO Debian 8.		
		Instalación de requerimientos software para el funcionamiento de la instalación de la suite de monitoreo.		
		Instalación de Nagios, Check_mk, Nagvis, Pnp4nagios.		
6	Configuración de las herramientas que componen la suite de monitoreo en entorno virtual para monitorear componentes de red de datos, servidores y equipos en diferentes plataformas de funcionamiento.	Instalación de los servicios de red: DNS, FTP, WEB, PROXY, OPENFIRE, SSH.	7	7
		Modificación del archivo de configuración de apache para implementar un servicio de seguridad de ingreso mediante protocolo SSL y restricción por IP.		
		Descarga e instalación de agentes cliente para monitoreo de equipos Windows y Linux. Activacion de protocolo SNMP en Router.		

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
6			7	7
		Ingreso de equipos, servidor de servicios y componentes de red con la herramienta de administración Check_mk para ser monitoreados.		
		Descarga e instalación de plugins específicos para monitoreo de servicios de red en Nagios		
		Configuración de archivos de Nagios para monitoreo de servicios de red.		

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
6		Configuración de plugins básicos para monitoreo de equipos y componentes de red, y de plugins específicos para el monitoreo de servicios.	7	7
		Configuración de Nagios, Check_mk, Nagvis y Pnp4nagios para un completo monitoreo de la red de datos de la empresa.		
		Instalación y configuración del servidor de correo Postfix para el envío de notificaciones por email.		
		Organización de la presentación del monitoreo con la herramienta de administración check_mk creando carpetas, subcarpetas de ubicación de		

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
6		equipos y definición de Hostgroups. Con la herramienta Nagvis se hace una presentación de los equipos mediante georreferenciación.	7	7
7	Realización de pruebas en entorno virtual	Diseñar una red virtual para llevar a cabo las pruebas Simulación de fallos en la red virtual para verificar la correcta configuración de la suite de monitoreo.	8	2
8	Migración de la suite de monitoreo a un servidor de la sede principal de la empresa Electromillonaria.	Verificación de características requeridas tanto en hardware como software del servidor de la empresa.		

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
8		Adaptación de lo realizado en la actividad 5 y 6 en el servidor de la empresa. Puesta en marcha de la suite de Monitoreo.	9	10
9	Realización de pruebas y evaluación de resultados	Realizar fallos intencionales en la configuración de los plugins de monitoreo con el fin de probar el buen funcionamiento de las herramientas. Verificación de los resultados de las pruebas, si existe error se realizaran las respectivas correcciones.	10	4
10	Instalación y configuración de servidor espejo dentro de la empresa como respaldo de la configuración del servidor donde funciona la suite de monitoreo de la red de datos	Documentación sobre instalación, configuración y funcionamiento de servidores espejo. Establecer tipo de servidor espejo a utilizar con los requerimientos de la empresa.	11	5

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
10		Instalación de la suite de monitoreo en servidor espejo de la empresa.		
		Instalacion y coniguracion de la herramienta Rsync con ssh para servicio espejo.		
		Realizacion de script.sh para ser ejecutado con el administrador de tareas de Linux Crontab para realizar respaldo de configuración de servidor principal a servidor espejo.		
11	Preparación de informe final y entrega al jefe de sistemas de la empresa JL Y RB S.A.S-ELECTROMILLONARIA	Reuniones del equipo de trabajo durante todo el proceso de realización del trabajo.	1	48
		Apropiación de normas, contenidos e información para la presentación del informe final.		
12	Capacitación del personal del área sistemas de la empresa Electromillonaria	Preparación de material didáctico	12	2
		Realización de la exposición de capacitación para la		

N°	ACTIVIDAD	TAREA	MES DE INICIO	DURACIÓN (SEMANAS)
		configuración y uso de las herramientas.		

9. DESARROLLO DEL TRABAJO

9.1 INFORMACIÖN GENERAL DE LA EMPRESA ELECTROMILLONARIA

La misión, visión y la breve reseña histórica fueron tomadas de (JL Y RB S.A.S – ELECTROMILLONARIA, 2017)

9.1.1 Misión. Caracterizarnos por el profesionalismo e innovación en el servicio y la atención a nuestros clientes, contando con la calidad del talento humano competente para satisfacer las expectativas de nuestros clientes. Comprometidos con el crecimiento y la rentabilidad de la empresa contribuimos así con el desarrollo social de la comunidad.

9.1.2 Visión. Convertirnos en una de las mejores opciones de compra para los hogares colombianos, aumentado participación en los mercados regionales y nacionales, con electrodomésticos y motocicletas de tecnología actualizada y diseño atractivo, fundamentados en:

- Calidad en el Servicio al cliente.
- Variedad de marcas de electrodomésticos.
- Facilidad de compra.
- Valor agregado y compromiso para nuestros clientes.
- Calidad en el talento humano competente.
- Confianza y satisfacción para nuestros clientes.
- Ser una empresa responsable y comprometida con la sociedad.

9.1.3 Breve historia. Todo comienza cuando el fundador de este grupo, el Sr. Jesús Alberto López Casanova, decide abandonar su humilde hogar a la edad de 17 años y comenzar a buscar un futuro mejor.

Comenzó a trabajar en pueblos pequeños del suroccidente colombiano, pasando a ser un muy buen vendedor y luego estableciendo una de las primeras loterías de productos en el país ¨LA MILLONARIA DEL PUTUMAYO¨. Después de esta lotería decide fundar Electromillonaria y el resto de las empresas que pertenecen a este grupo.

El grupo empresarial JLC, nacido hace más de 30 años en el mercado colombiano de Electrodomésticos, Muebles y Hogar. Con presencia en el territorio colombiano desde el centro del país hacia el sur de este abarcando el Triángulo del Café, Valle del Cauca, Cauca, Nariño, Huila, Caquetá y Putumayo. Con una clara visión de ser los líderes del mercado en diferentes áreas referidas a productos tecnológicos tanto

en el canal Retail como Wholesale, para esto contamos con la propia flota de transporte de casi 50 vehículos, más de 51 tiendas, generando más de 800 empleos directos y 400 indirectos, tiene 2 almacenes centrales uno en Pasto y uno en Yumbo con un área de 12,000 metros cuadrados y también la estructura comercial y administrativa requerida para lograr sus objetivos.

9.1.4 Área de influencia. La empresa cuenta a nivel nacional con:

- 26 tiendas
- 24 pequeñas tiendas
- 7 puntos Keeway
- 1 tienda especializada Benelli en Bogota

En las figuras 13, 14 15 y 16, se muestra los mapas regionales por área de influecia de las tiendas de los departamentos de Nariño, Valle del Cauca, Putumayo y Cauca, respectivamente.

Área de influencia en Nariño:

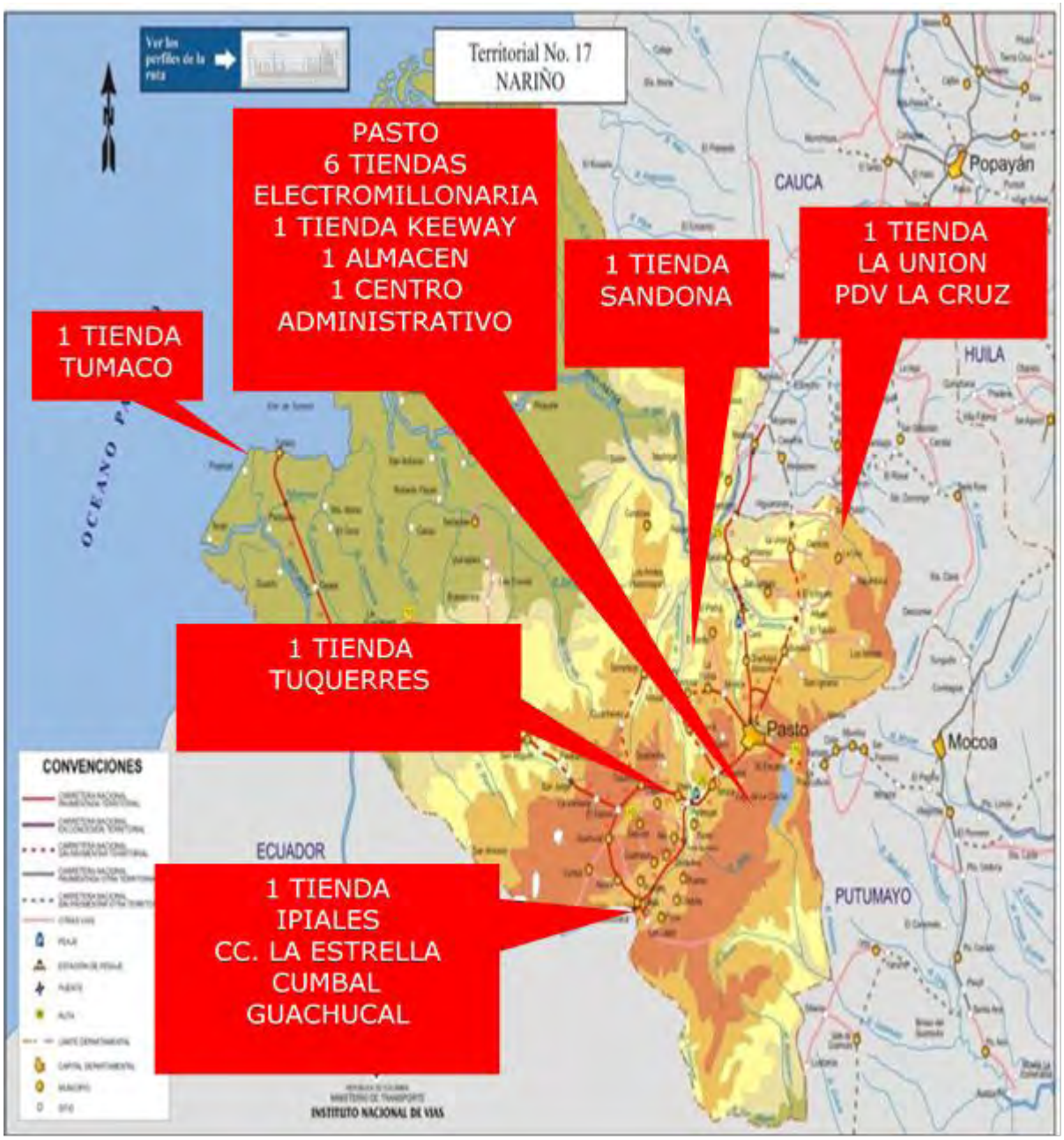


Figura 13. Mapa regiona de Nariño, ubicación de tiendas.

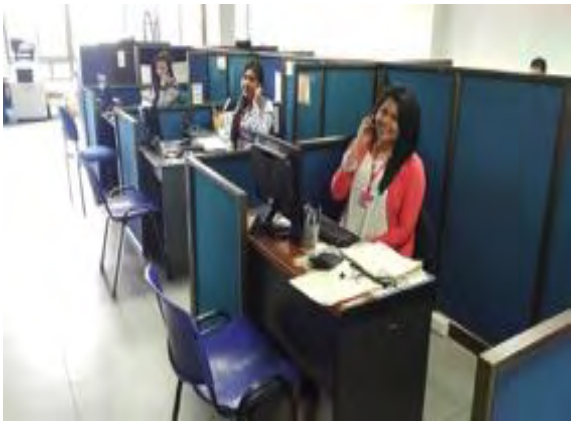
A continuación, se muestra imágenes de las oficinas y personal del edificio administrativo de la empresa Electromillonaria.

Imágenes de oficinas y personal edificio sede administrativa, Electromillonaria.

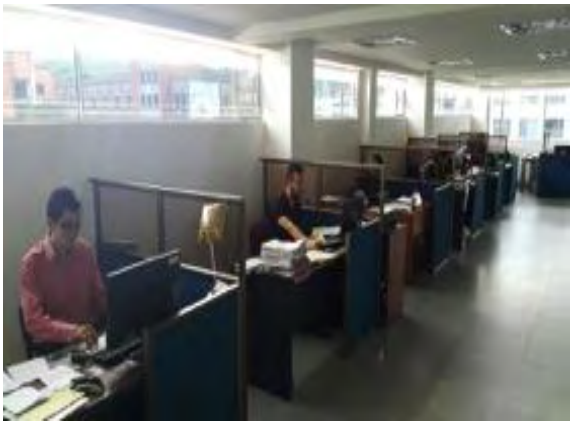
















A continuación, se muestra imágenes de las tiendas ubicadas en el departamento de Nariño.





















Área de influencia en Valle del Cauca:

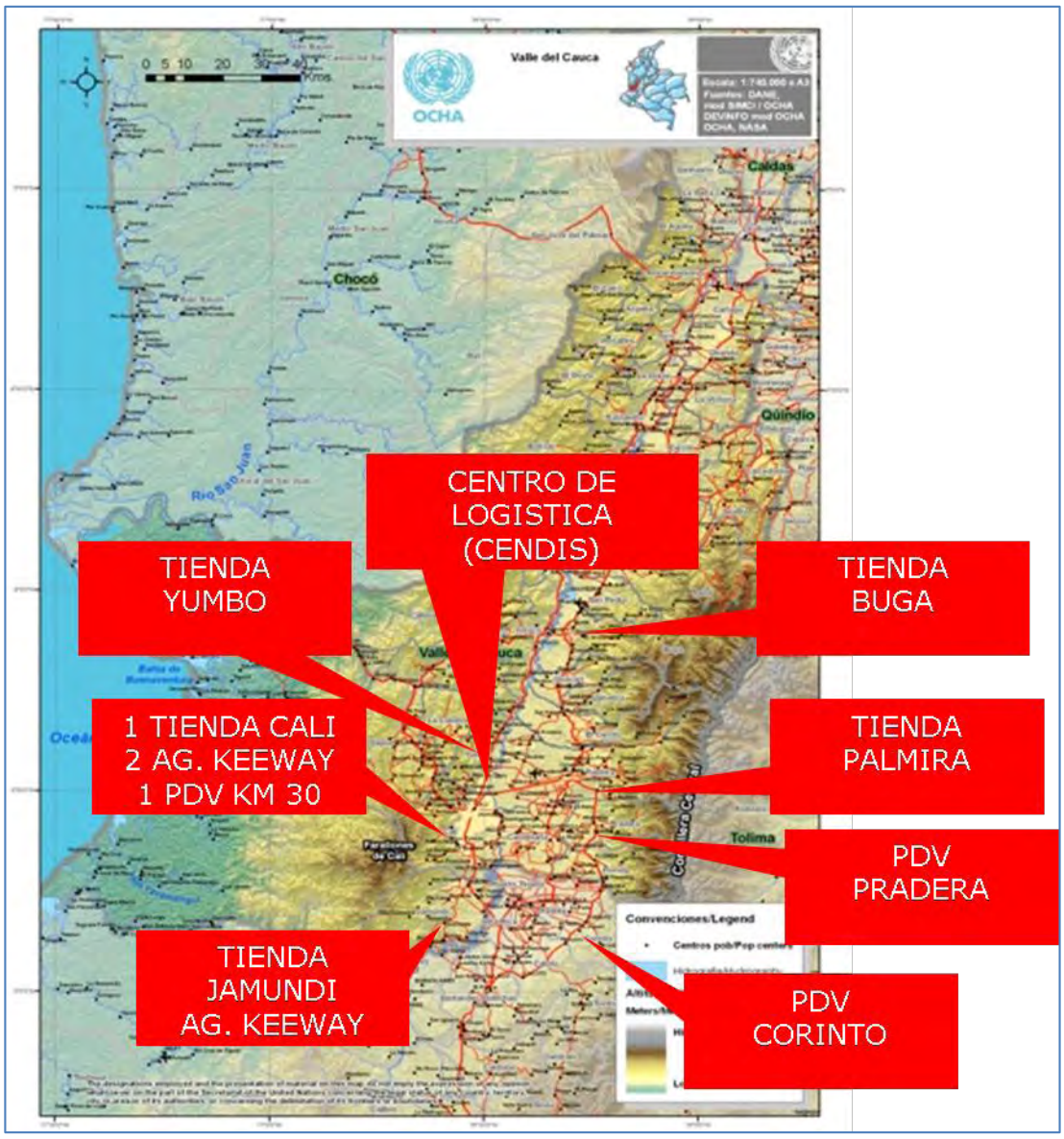


Figura 14. Mapa regional Valle del Cauca, ubicación de tiendas.

A continuación, se muestra imágenes de las tiendas ubicadas en el departamento del Valle del Cauca


KEEWAY
electromillonaria


KEEWAY
MOTOR
electromillonaria


electromillonaria
KEEWAY


electromillonaria
Petecas


electromillonaria
KEEWAY
MOTOR


electromillonaria

Área de influencia en el Putumayo:



Figura 15. Mapa regional de Putumayo, ubicación de tiendas.

A continuación, se muestra imágenes de las tiendas ubicadas en el departamento de Putumayo.


LG
.electromillonaria


.electromillonaria
Sabemos llegar...


.electromillonaria
KEEWAY
MOTOS


.electromillonaria
ICASA
SONY


.electromillonaria
Haceb
Haceb


.electromillonaria
KEEWAY
MOTOS

Área de influencia en el Cauca:

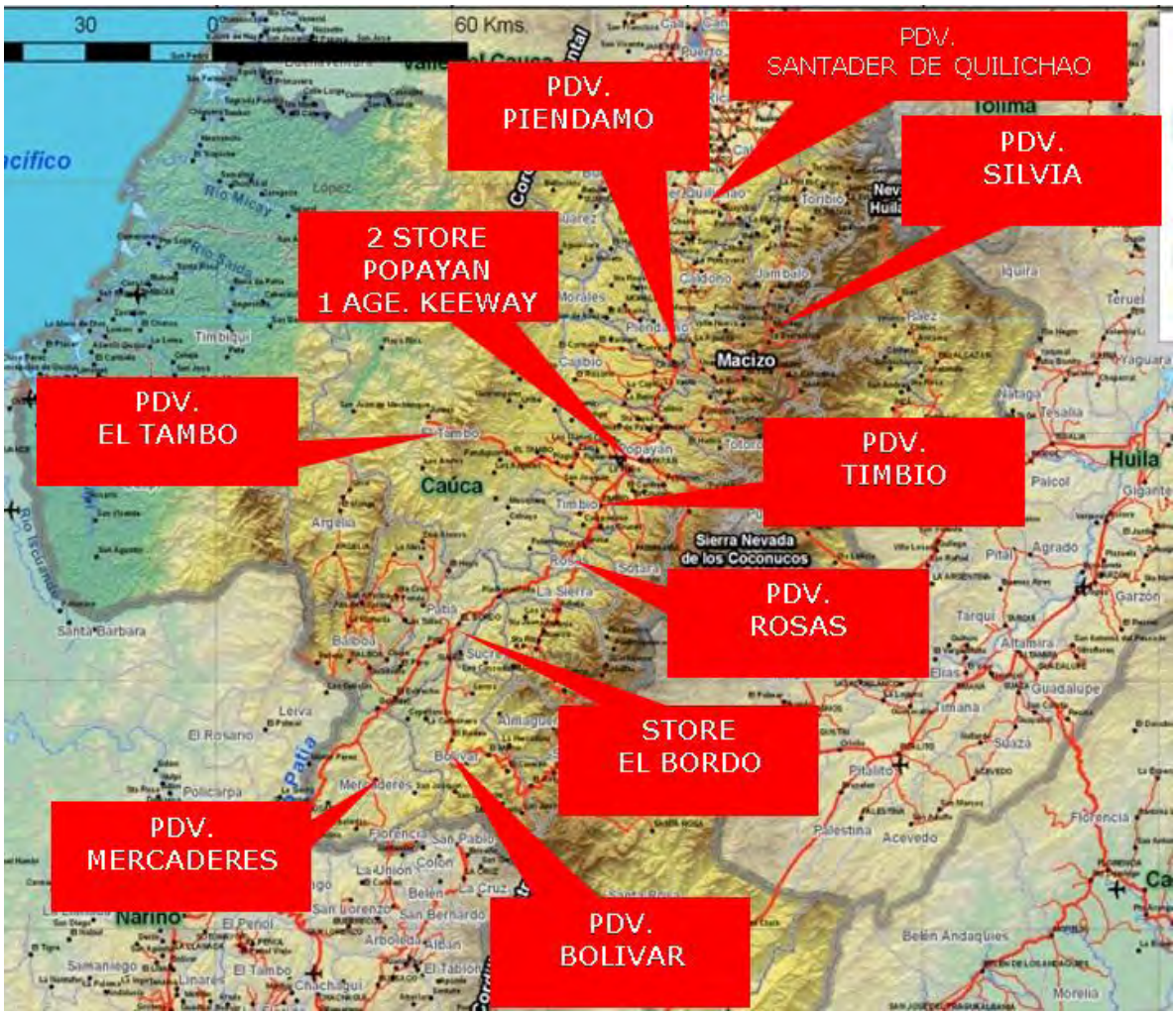


Figura 16. Mapa regional Cauca, ubicación de tiendas.

A continuación, se muestra imágenes de las tiendas ubicadas en el departamento de Cauca.


electromillonaria
Sabemos llegar
Calle 5 # 12 - 65 Tel. 821 1967
KEEWAY
KEEWAY


electromillonaria
Sabemos llegar
6-61

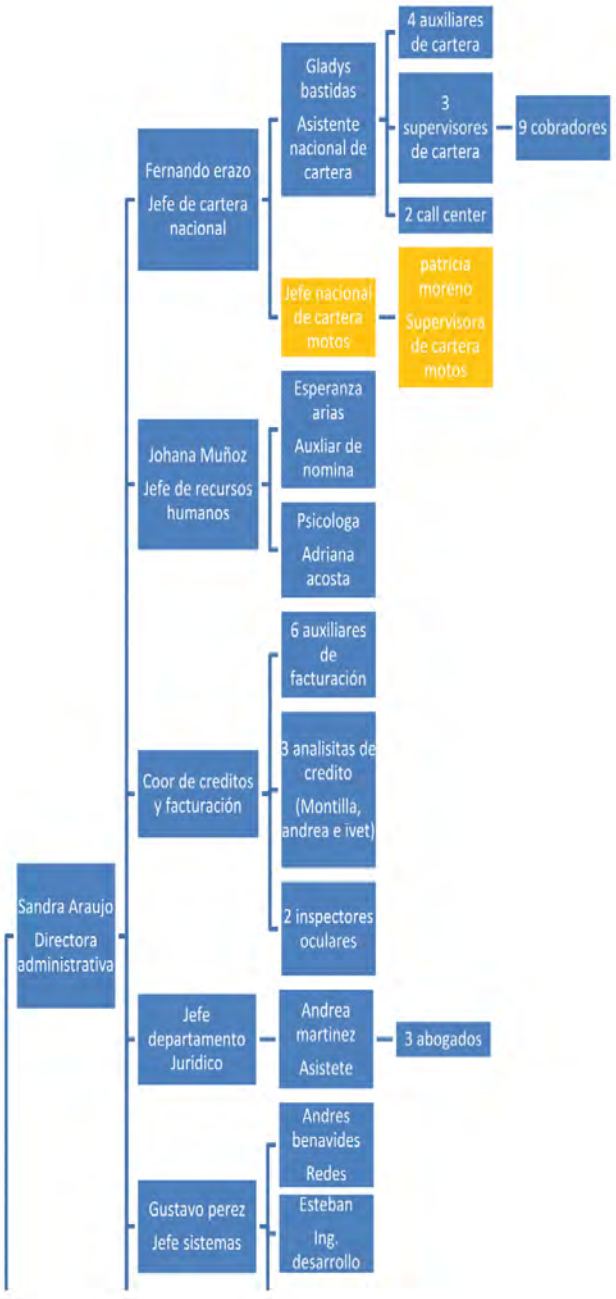


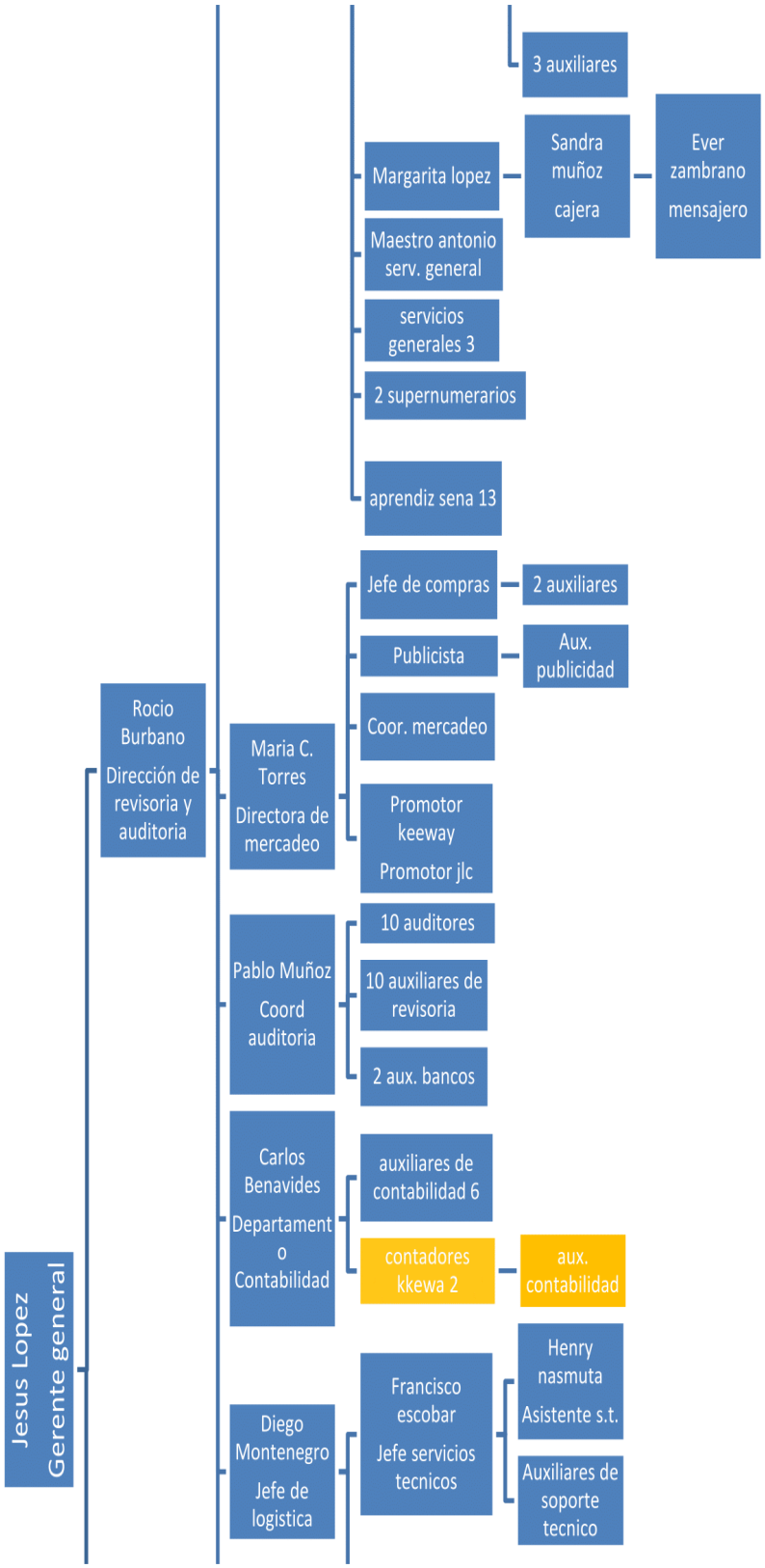

LG


AGROCENTRO



9.1.5 Organigramas sectoriales. La empresa JL Y RB S.A.S-ELECTROMILLONARIA tiene cobertura a nivel nacional, por tal motivo el departamento de recursos humanos al momento de realizar la representación de la estructura de la empresa, tomo la decisión de hacer un organigrama por cada región o sector. A continuación, se muestra los organigramas.
Organigrama sede administrativa:




Jesus Lopez
Gerente general
Rocio Burbano
Dirección de revisoria y auditoria
Maria C. Torres
Directora de mercadeo
Jefe de compras
2 auxiliares
Publicista
Aux. publicidad
Coor. mercadeo
Promotor keeway
Promotor jlc
Pablo Muñoz
Coord auditoria
10 auditores
10 auxiliares de revisoria
2 aux. bancos
Carlos Benavides
Departamento Contabilidad
auxiliares de contabilidad 6
contadores kkewa 2
aux. contabilidad
Diego Montenegro
Jefe de logistica
Francisco escobar
Jefe servicios tecnicos
Henry nasmuta
Asistente s.t.
Auxiliares de soporte tecnico
Margarita lopez
Sandra muñoz
cajera
Ever zambrano
mensajero
Maestro antonio serv. general
servicios generales 3
2 supernumerarios
aprendiz sena 13
3 auxiliares

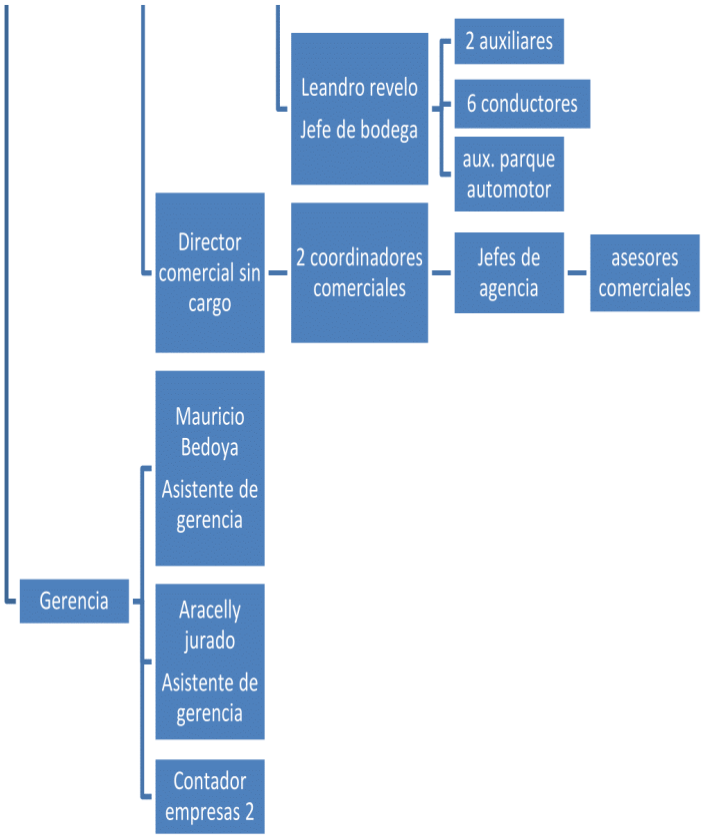
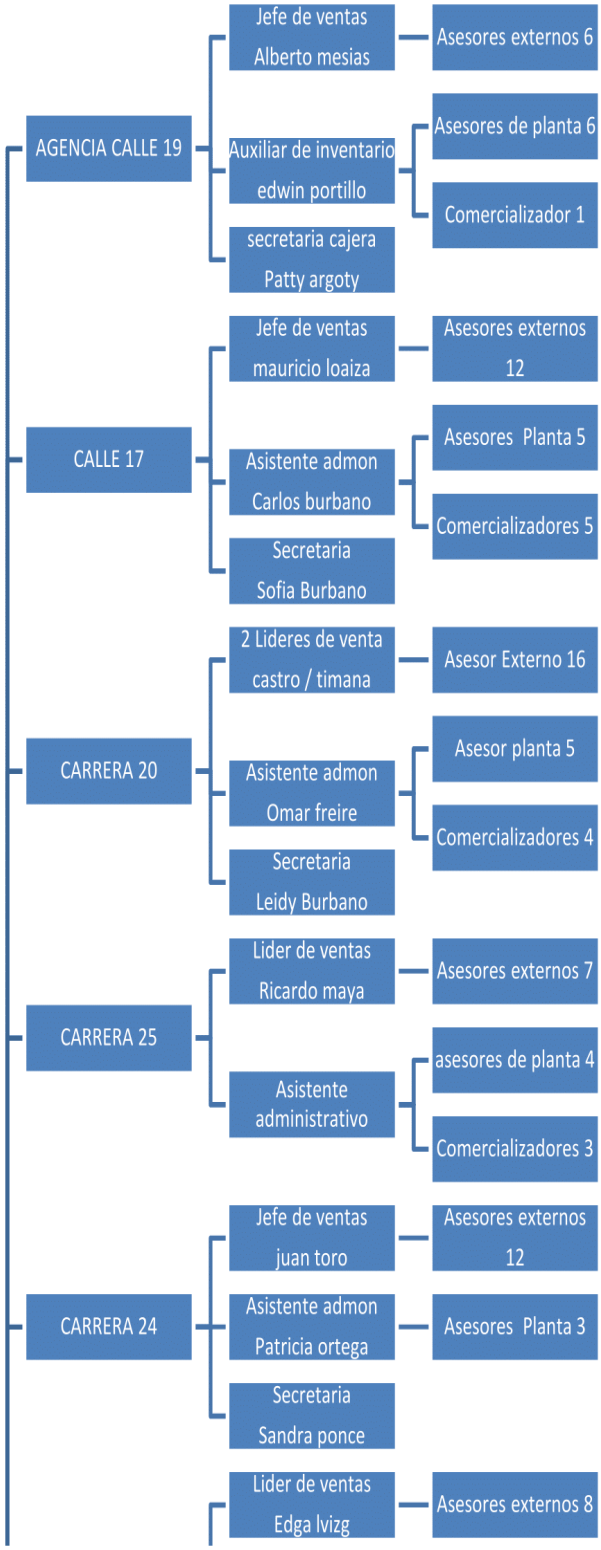
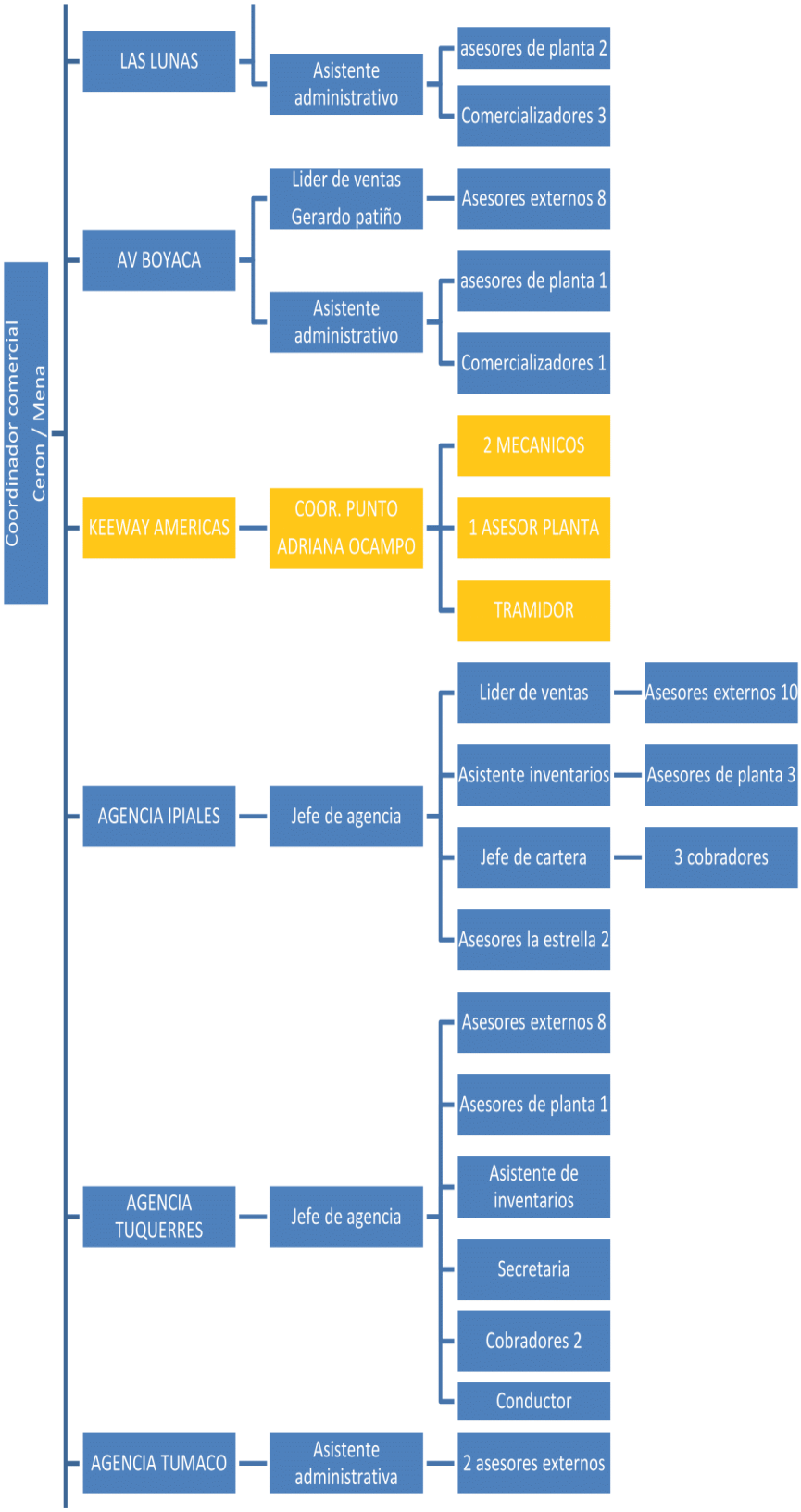


Figura 17. Organigrama sede administrativa.

Organigrama regional Nariño:




Coordinador comercial
Ceron / Mena
LAS LUNAS
Asistente administrativo
asesores de planta 2
Comercializadores 3
AV BOYACA
Lider de ventas
Gerardo patiño
Asesores externos 8
Asistente administrativo
asesores de planta 1
Comercializadores 1
KEEWAY AMERICAS
COOR. PUNTO
ADRIANA OCAMPO
2 MECANICOS
1 ASESOR PLANTA
TRAMIDOR
AGENCIA IPIALES
Jefe de agencia
Lider de ventas
Asesores externos 10
Asistente inventarios
Asesores de planta 3
Jefe de cartera
3 cobradores
Asesores la estrella 2
AGENCIA TUQUERRES
Jefe de agencia
Asesores externos 8
Asesores de planta 1
Asistente de inventarios
Secretaria
Cobradores 2
Conductor
AGENCIA TUMACO
Asistente administrativa
2 asesores externos

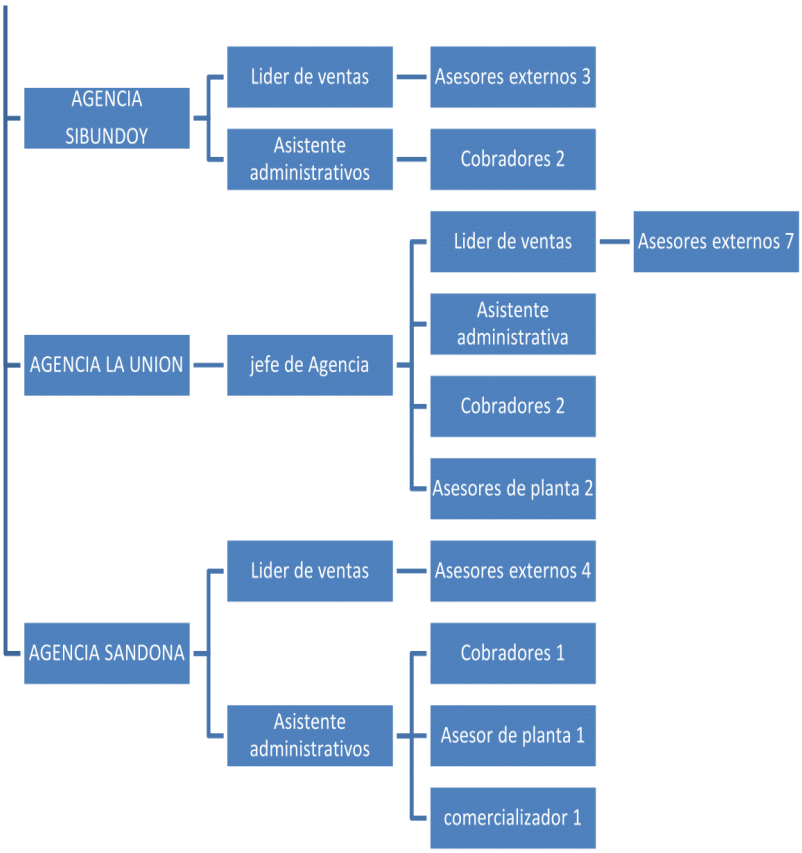


Figura 18. Organigrama regional Nariño.

Organigrama Interelec:

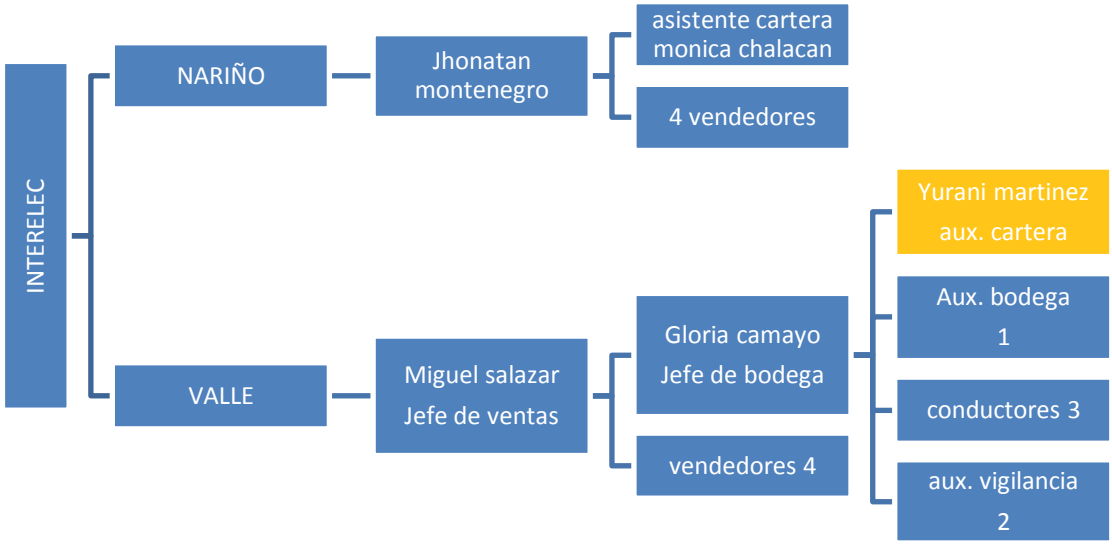


Figura 19. Organigrama INTERELEC.

Organigrama keeway central:

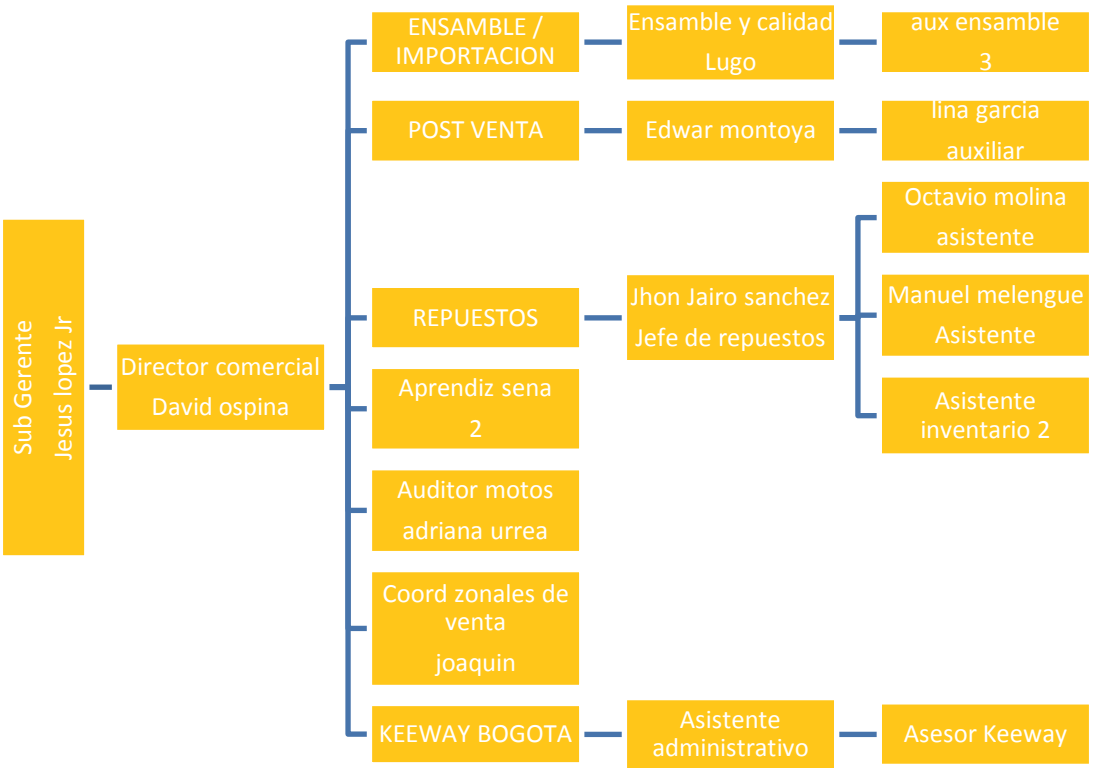
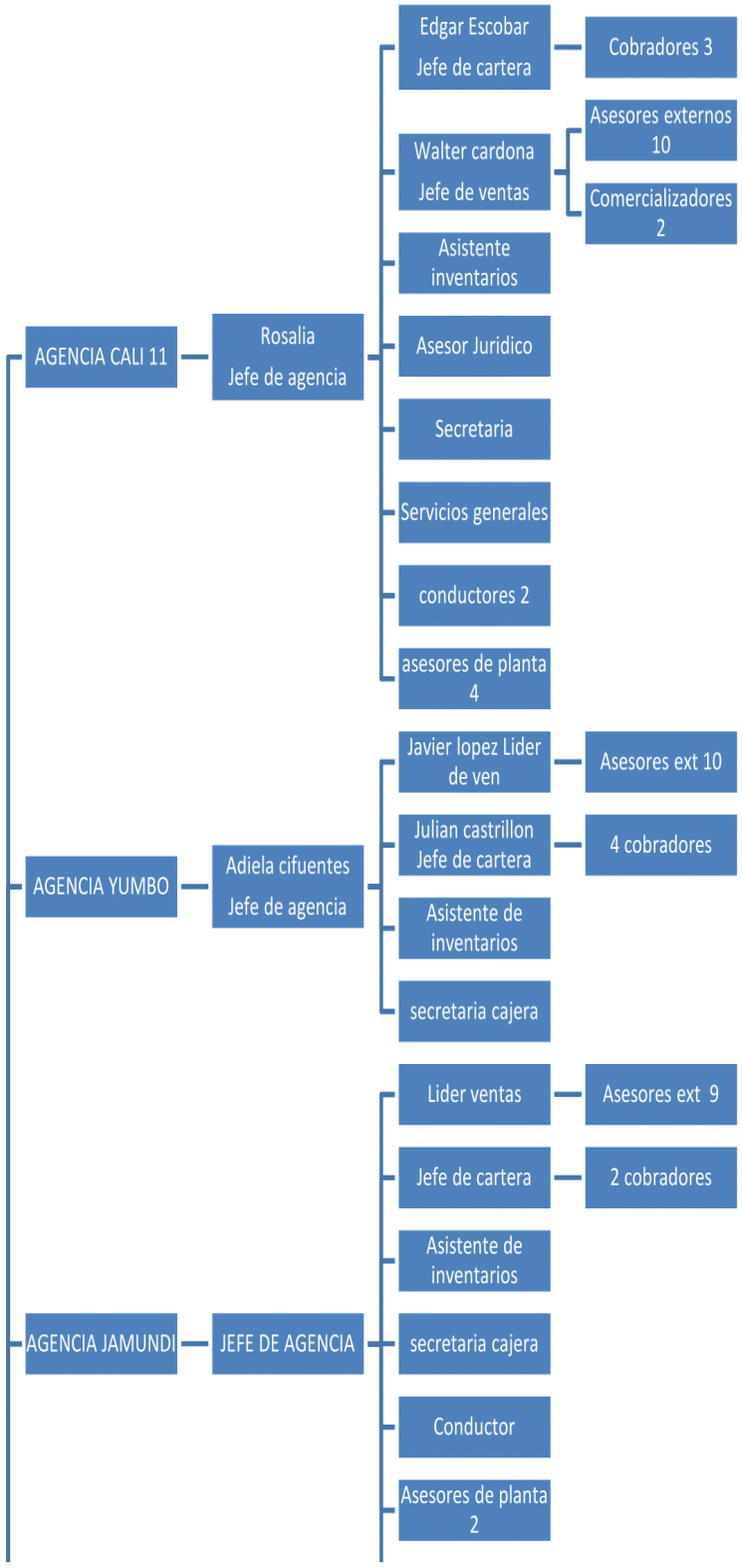
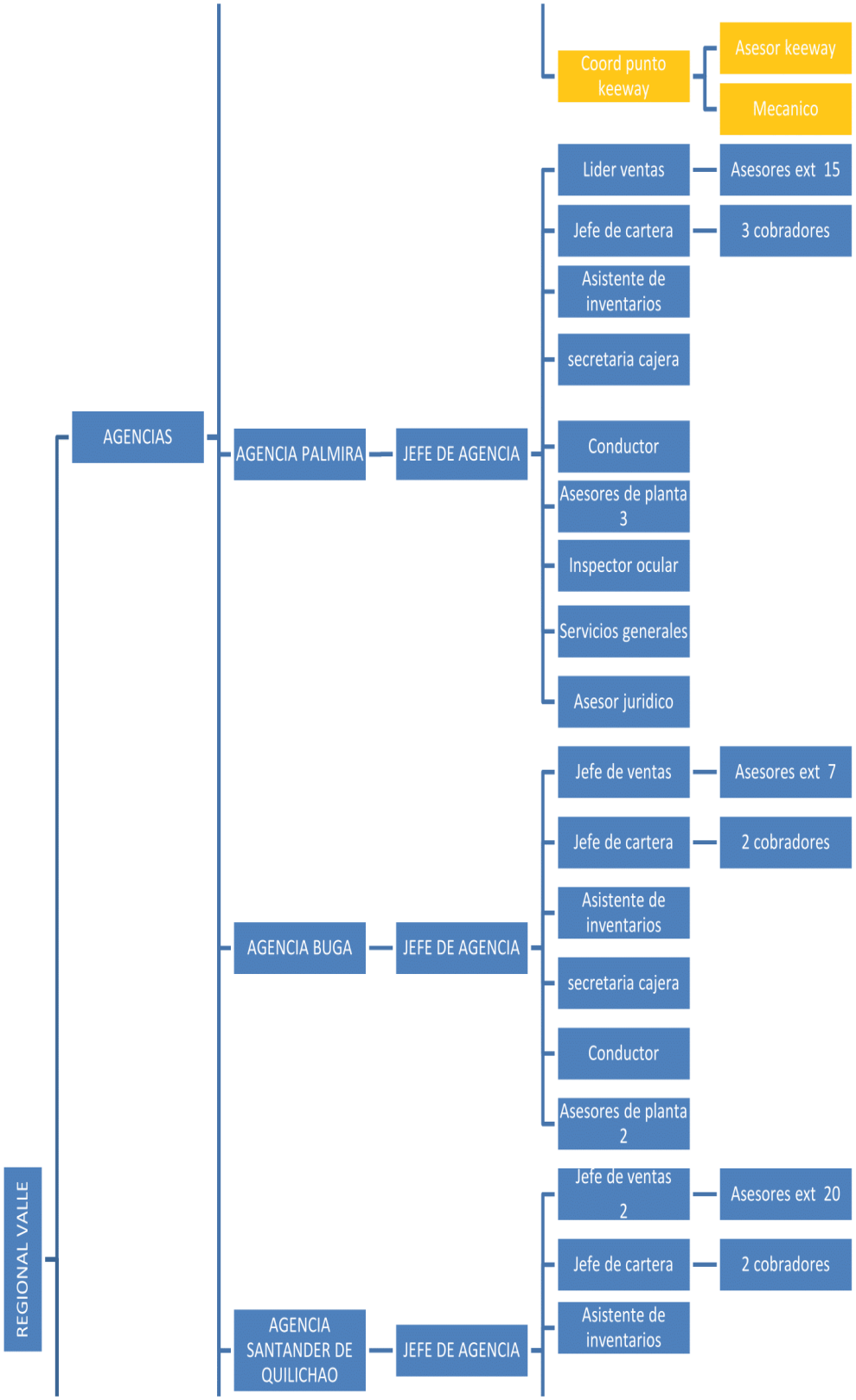


Figura 20. Organigrama KEEWAY central.

Organigrama regional Valle:




REGIONAL VALLE
AGENCIAS
AGENCIA PALMIRA
JEFE DE AGENCIA
Coord punto keeway
Asesor keeway
Mecanico
Lider ventas
Asesores ext 15
Jefe de cartera
3 cobradores
Asistente de inventarios
secretaria cajera
Conductor
Asesores de planta 3
Inspector ocular
Servicios generales
Asesor juridico
AGENCIA BUGA
JEFE DE AGENCIA
Jefe de ventas
Asesores ext 7
Jefe de cartera
2 cobradores
Asistente de inventarios
secretaria cajera
Conductor
Asesores de planta 2
AGENCIA SANTANDER DE QUILICHAO
JEFE DE AGENCIA
Jefe de ventas 2
Asesores ext 20
Jefe de cartera
2 cobradores
Asistente de inventarios

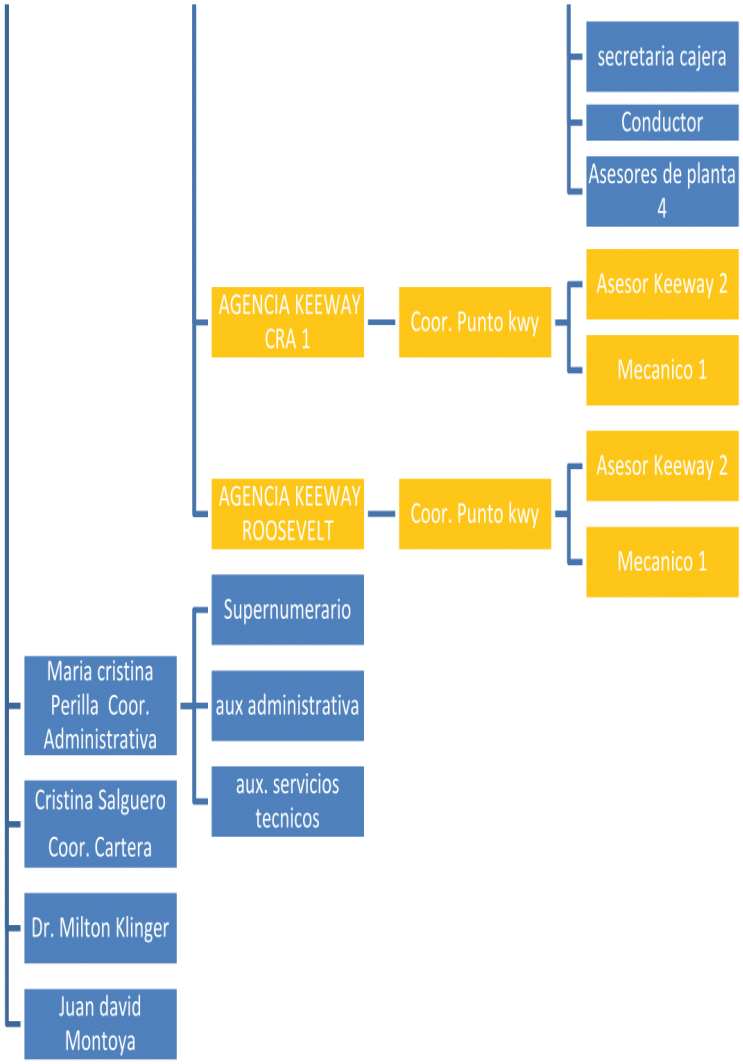


Figura 21. Organigrama regional Valle.

Organigrama regional Cauca:

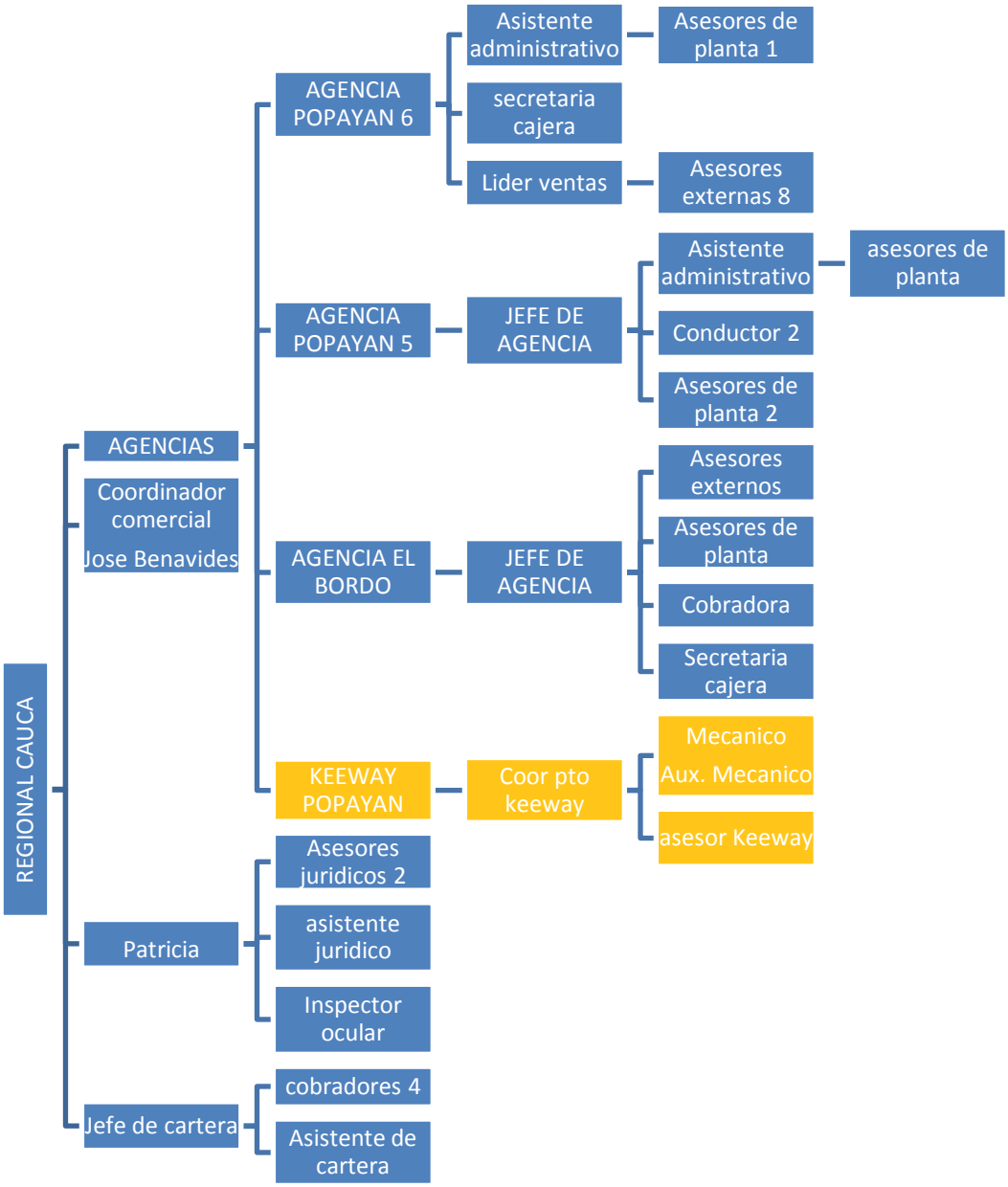


Figura 22. Organigrama regional Cauca.

Organigrama regional Putumayo:

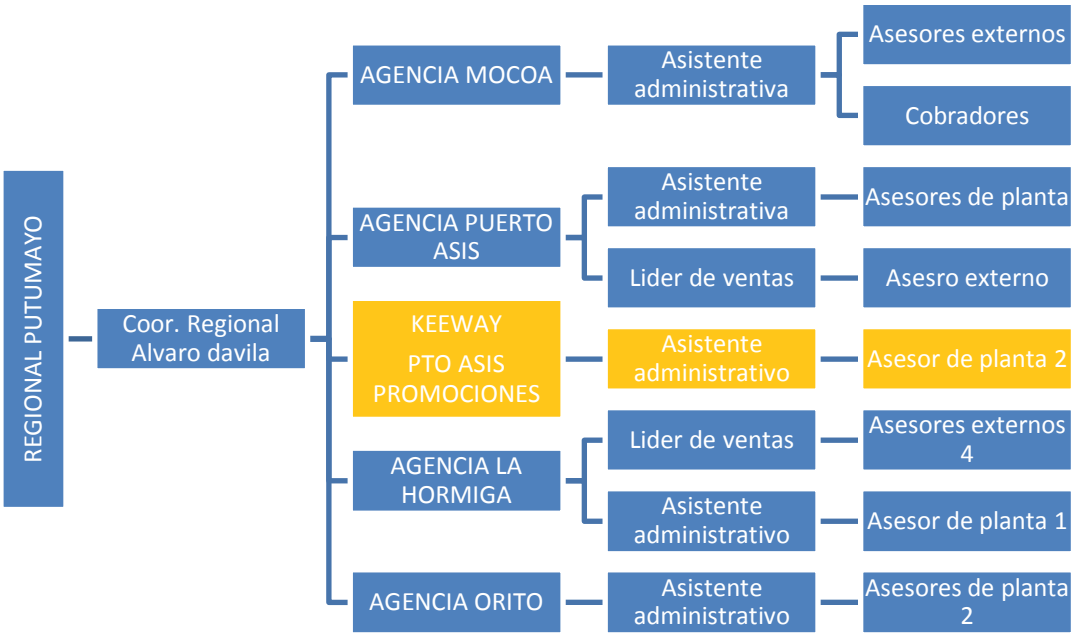


Figura 23. Organigrama regional Putumayo.

9.2 INFORMACIÓN RECOLECTADA DE LA RED DE DATOS

De acuerdo con la información obtenida de la empresa, se identificó que se emplea una topología de red en árbol, mostrada tanto en el diseño lógico y físico de la empresa.

Dentro de la información de datos de la empresa se encuentra la descripción de los equipos y componentes de red.

La información de los equipos de cómputo recolectada en la sede principal se hizo por áreas, entre las que se encuentran:

- Area de administración 4 equipos.
- Área facturación 3 equipos.
- Área jurídica 5 equipos.
- Área cartera 11 equipos.
- Área sistemas 6 equipos.
- Área comercial 4 equipos.
- Área gerencia 7 equipos.
- Área contabilidad 6 equipos.
- Área revisoría 14 equipos.
- Área interelec 2 equipos.

- Área fondelec 1 equipos.
- Área publicidad 1 equipos.

Dentro de las agencias de Pasto, se tiene:

- Keeway americas 2 equipos.
- Electromillonaria carrera 20, 2 equipos
- Keeway calle 17, 1 equipo.
- Electromillonaria calle 17, 1 equipo.
- Electromillonaria carrera 25, 1 equipo.
- Electromillonaria carrera 24, 2 equipo.
- Electromillonaria calle 19, 4 equipo.
- Bodega principal 5 equipos.
- Electromillonaria las lunas, 1 equipo.

En cuanto a dispositivos de red, como radioenlaces, servidores, impresoras y router, se tiene:

- 7 radioenlaces.
- 1 router.
- 11 servidores.
- 4 impresoras multifuncionales.

Para detallar la información recolectada mirar

Anexo A. Información de equipos.

9.3 ANÁLISIS DE LA RED DE DATOS

El analisis de la red de datos es un proceso que se debe realizar periodicamente en las empresas, para saber el estado de los componentes de red. Con el analisis se puede dar solución a posibles causas de problemas, evitando el deterioro de los componentes; logrando optimizar el funcionamiento de la empresa.

9.3.1 Análisis de los componantes de red. Los servidores se encuentran en el tercer piso, ubicados en gabinetes y en áreas restringuidas, cuentan con aire acondicionado para mantener los servidores a buena temperatura y con UPS para dar disponiblidad del servicio en caso de problemas electricos. (Ver figura 24).



Figura 24. Gabinete de servidores, azkaban, voldemort, slytherin, gryffindor.

Switches de las áreas del tercer piso y que dan conexión a los componentes de red de los otros pisos. (Ver figura 25)



Figura 25. Switches sede principal.

Dispositivo utilizado para la refrigeracion de los cuartos donde se encuentran los servidores de red. (Ver figura 26).



Figura 26. Dispositivo de aire acondicionado cuarto de servidores.

Switches de las áreas del segundo Piso:



Figura 27. Switches segundo piso.

Se puede observar el router del provedor de Internet que da conexión a la sede principal de la empresa electromillonaria. Además, no hay una organización adecuada de los cables de red, dificultando la identificación de fallos. (Ver figura 28).

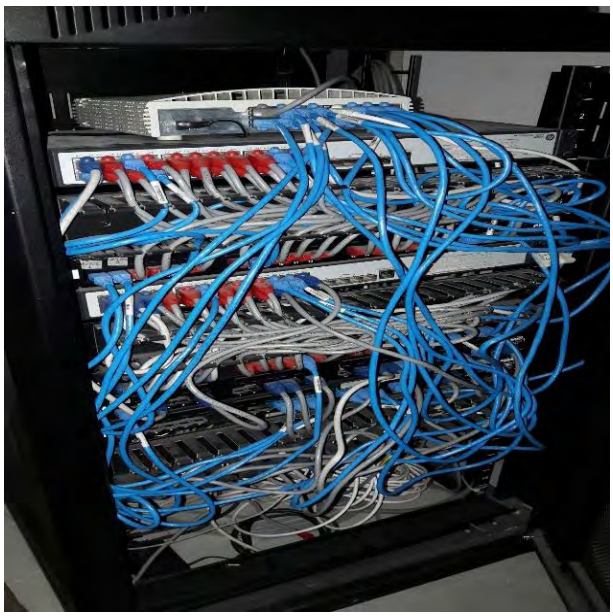


Figura 28. Router principal y switches segundo piso.

Switches de las áreas del cuarto Piso, los switches estan vulnerables al polvo lo que conlleva a posibles problemas por su deterioro. (Ver fig. 29).



Figura 29. Switches cuarto piso.

Los swiches utilizados en la empresa son de veinti cuatro (24) puertos con tarjetas de red Gigabit. (Ver figura 30).

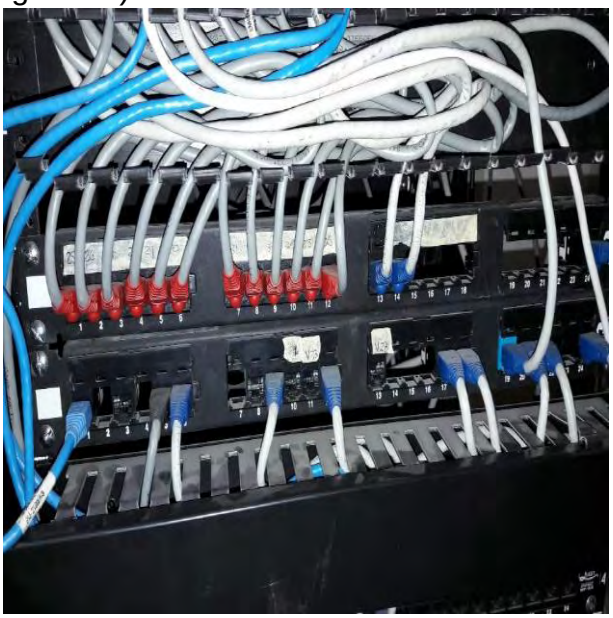


Figura 30. Switches de 24 puertos.

Sistema con UPS para dar disponibilidad de los servidores en caso de fallas electricas. (Ver figura 31).



Figura 31. UPS servidores principales.

Routers y Switches de la agencia calle 19. Con su respectivo gabinete y adecuada conexión electrica. (Ver figura 32).



Figura 32. Gabinete switches calle 19.

Servidor de respaldo ubicado en agencia calle 19, con seguridad de acceso. (Ver figura 33).



Figura 33. Servidor respaldo calle 19.

A continuación, se muestra los diferentes dispositivos que conectan las agencias de Pasto con la sede principal. (Ver figura 34).



Figura 34. Switch tres antenas tp-link, agencia principal tercer piso.

En la sede principal se encuentra la antena con los radios enlaces de la marca Ubiquiti, que conectan cuatro agencias de Pasto con la sede Principal. (Ver figura 35).

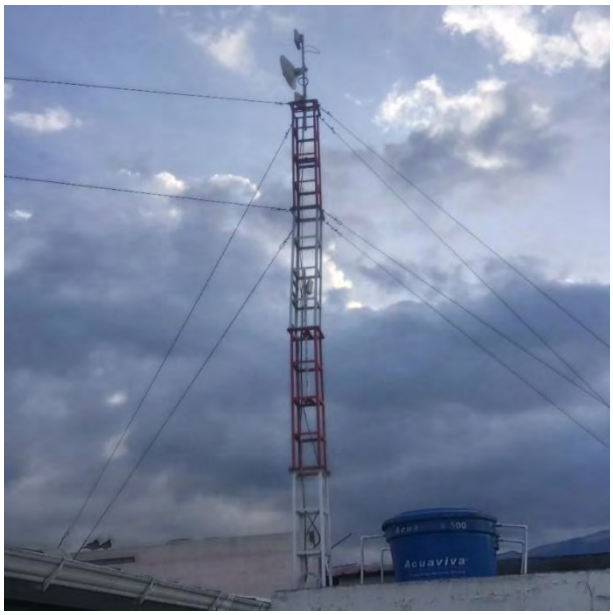


Figura 35. Antena con radioenlaces Ubiquiti.

Se observan los diferentes tipos de dispositivos Ubiquiti utilizados, dependiendo de la distancia a la que se encuentran las agencias. (Ver figura 36).

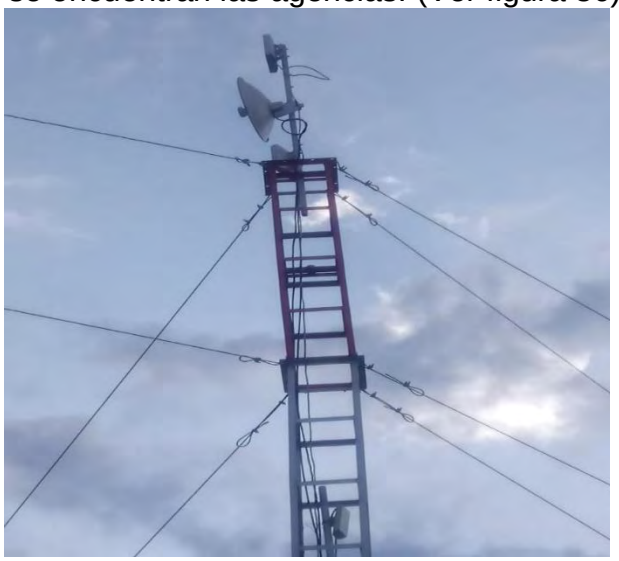


Figura 36. Cuatro radioenlaces ubiquiti.

Routers proveedores de internet de las agencias de Pasto. (Ver figura 37-40).



Figura 37. Router tp-link 8 puertos, agencia carrera 25.



Figura 38. Router ARRIS 4 puertos, agencia carrera 20.



Figura 39. Router OFFCOM 4 puertos, agencia las americas.



Figura 40. Switch tp-link 4 puertos, área de cartera sede principal.

Algunas áreas en la sede principal utilizan switches para conectar sus dispositivos, ahora se muestra un ejemplo de cómo no ubicar un switch.

A continuacion, se muestra las impresoras utilizadas en la empresa. Impresora utilizada en las agencias de la ciudad de Pasto. (Ver figura 41).

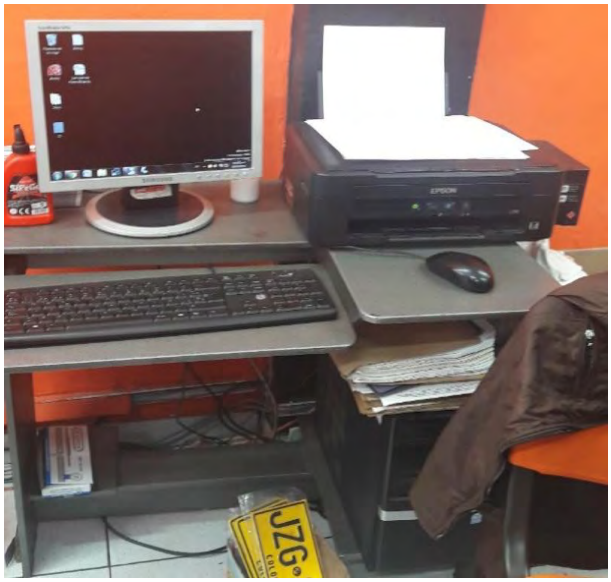


Figura 41. Impresora EPSON L380, sede keeway las americas.

Impresora utilizada en las agencias de la ciudad de Pasto:

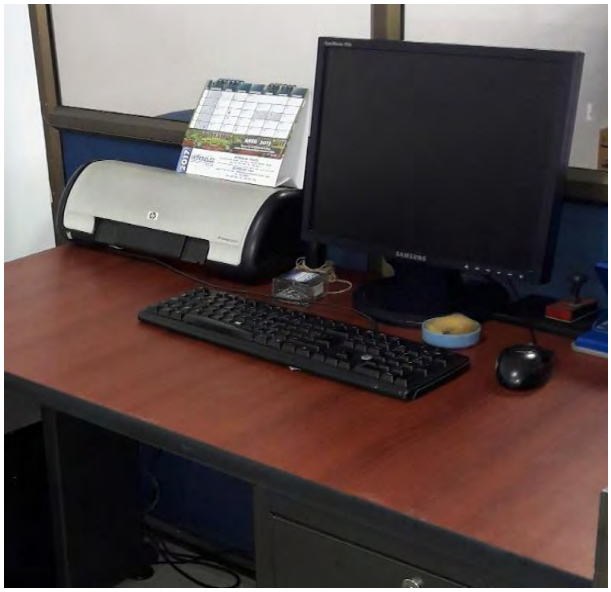


Figura 42. Impresora HP hp1460, sede calle 19.

La siguiente imágen muestra una impresora multifuncional kyocera. De este tipo son manejadas cuatro impresoras en la sede principal, dos en el segundo piso, una en el tercero y otra en el cuarto. Conectadas a regulador de corriente. (Ver figura 43).



Figura 43. Impresora KYICERA FS-1325MFP, sede principal.

Los puntos de red son distribuidos a través de tapas plásticas conectadas en las paredes. El cable utilizado para la conexión en la empresa es cable de par trenzado categoría sies (6). Algunos cables y cajas plásticas están en mal estado afectando la calidad de conexión. (Ver figura 44-45).



Figura 44. Punto de red de datos, sede principal.



Figura 45. Punto de red da datos y de voz, agencia principal.

En la mayoría de las agencias de Pasto, los hosts se conectan con terminales tontas al equipo principal que funciona como servidor. Este sistema es viable para ahorrar costos, pero no es recomendable para asegurar disponibilidad. (Ver figura 46).



Figura 46. Terminal tonta HP agencia carrera 20.

En las visitas iniciales a la empresa la mayoria de los computadores eran viejos y deteriorados. (Ver figura 47).



Figura 47. Computador área interelec sede principal.

En la actualidad se estan cambiando por computadores nuevos. (Ver figura 48).

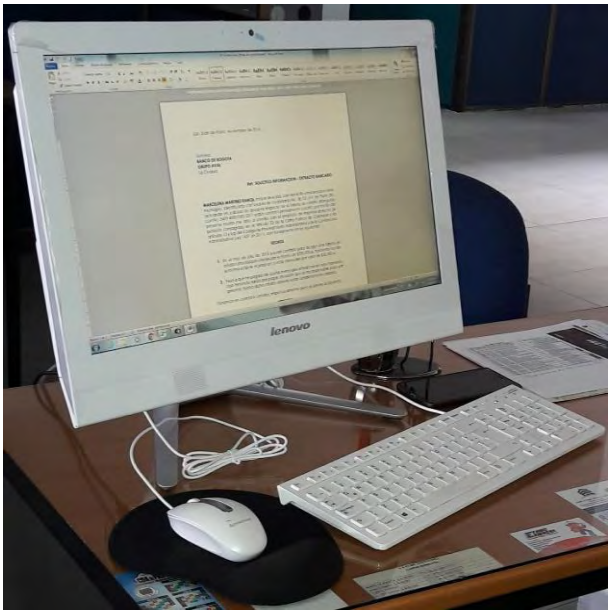


Figura 48. Computador área interelec sede principal.

En algunas áreas de la sede principal utilizan computadoras portátiles. (Ver figura 49).

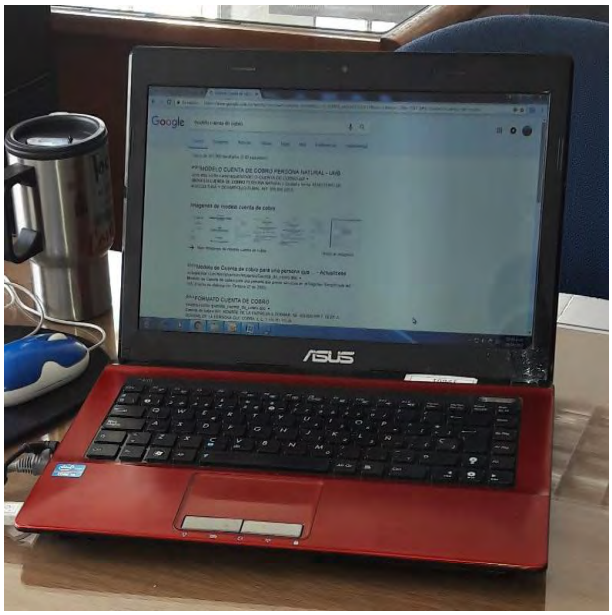


Figura 49. Portátil área ventas sede principal.

Una buena práctica utilizada en la empresa es la conexión de los componentes de red a reguladores de corriente para la protección eléctrica de los equipos. (Ver figura 50).

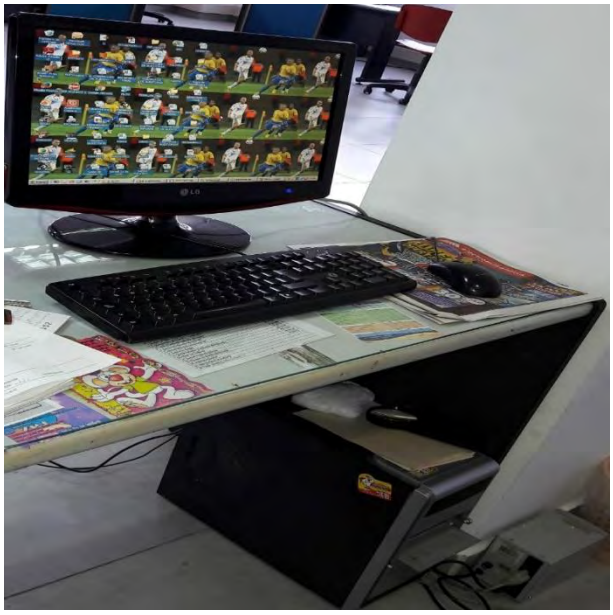


Figura 50. Computador área cartera sede principal.

En la empresa es muy regular el uso del sistema operativo Windows 7 por su facilidad de uso para la mayoría del personal. (Ver figura 51).

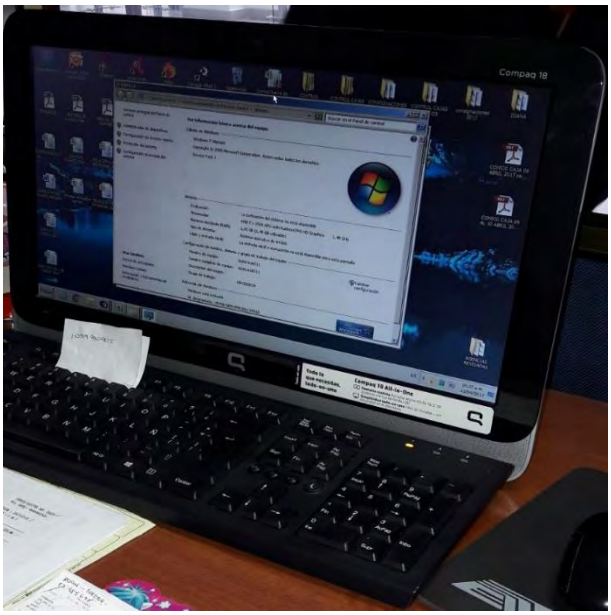


Figura 51. Computador área jurídico sede principal.
Algunos cables no están distribuidos con canaletas, siendo vulnerables a daños.



Figura 52. Cable de datos y de voz área interelec sede principal.

9.3.2 Análisis de la red de datos. En el analisis realizado a la red de datos de la empresa electromillonaria en la ciudad de Pasto, se describen los componentes de red detallando su estado. Ademas, se analizó la red de datos con la ayuda de las herramientas: Free IP Tools, Iperf, Acrylic Wi-fi professional, Speedtest y Wireshark.

Para detallar el analisis de la red de datos y observar los resultados obtenidos mirar

Anexo B. Analisis de la red de datos.

Para detallar los resultados del tráfico de red con la herramienta wireshark mirar el Anexo C. Resultado acotado de análisis con herramienta Wireshark. Por el tamaño del archivo original, se muestra solamente una parte de los resultados.

Según la información suministrada por la página web (ESnet / Lawrence Berkeley National Laboratory., 2016), iPerf3 es una herramienta para mediciones activas del ancho de banda máximo alcanzable en redes IP, es compatible con protocolos TCP, UDP, SCTP con IPv4 e IPv6. Para cada prueba, informa el ancho de banda, la perdida y otros parámetros. Es una herramienta multiplataforma.

La página web de la herramienta Acrylic Wi-Fi Professional (Tarlogic Security, 2017) la define como un software de análisis WIFI para identificar puntos de acceso y canales wifi, y para analizar y resolver incidencias en redes inalámbricas 802.11a/b/g/n/ac en tiempo real.

La herramienta web SpeedTest ayuda a medir el rendimiento en internet a través de pruebas y métricas de rendimiento. Según su página web (Ookla, 2017) Speedtest es la forma definitiva de medir su rendimiento en Internet. Con miles de millones de usos activos hasta la fecha, además aclara diciendo que es el líder mundial dominante en pruebas y métricas de rendimiento de Internet. La misión de Speedtest es ayudar a construir una Internet mejor y más rápida.

Según lo anterior, concluye deciendo que la tecnología probada detrás de Speedtest está especialmente diseñada para realizar pruebas de rendimiento de Internet precisas e imparciales, lo que permite a las personas de todo el mundo calibrar y solucionar los problemas de la velocidad de sus conexiones a Internet.

Otra herramienta utilizada fue wireshark según su página web (Combs, 11), la describe como el analizador de protocolo de red más importante y ampliamente utilizado en el mundo. Le permite ver lo que está sucediendo en su red a un nivel microscópico y es el estándar de facto en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. El desarrollo de Wireshark prospera gracias a las contribuciones voluntarias de expertos en redes en todo el mundo y es la continuación de un proyecto iniciado por Gerald Combs en 1998.

Además, se utilizo la herramienta IPtools, en su página web (Sørensen, 2013), la describe como un conjunto de herramientas completo para los controles de red. Actualmente incluye doce funciones de red principales diferentes que se utilizan comúnmente en la actualidad.

Por último, dice que todas las herramientas se pueden ejecutar haciendo clic en el botón de inicio, las herramientas incluidas: Un escáner de puertos, ping, traceroute,

NSLookup, verificación de correo electrónico y aplicaciones utilizadas para explorar recursos de red compartidos.

En general, Free IP Tools ofrece un poderoso conjunto de comandos en una interfaz gráfica de usuario; perfecto para usuarios principiantes o aquellos que no se sienten cómodos usando una línea de comando.

9.4 DISEÑO LÓGICO Y FÍSICO DE LA RED DE DATOS

Para el diseño lógico de la red de datos se tuvo en cuenta nueve agencias en la ciudad de Pasto, incluyendo la sede principal y cinco sedes fuera de Pasto distribuidas en Cali, Yumbo, Popayan, Tumaco y Mocoa.

Tres agencias de Pasto se conectan por medio de radio enlace y cuatro por VPN. Las sedes de los diferentes municipios también se encuentran conectadas por VPN. En general, se observó una topología en árbol, la cual se ramifica desde el router ubicado en la sede principal de la empresa hacia las demás sucursales y sedes en las diferentes ciudades.

Para el diseño físico de red de datos se tuvo en cuenta las agencias de la ciudad de Pasto, incluyendo la sede principal.

9.4.1 Diseño lógico sede principal:

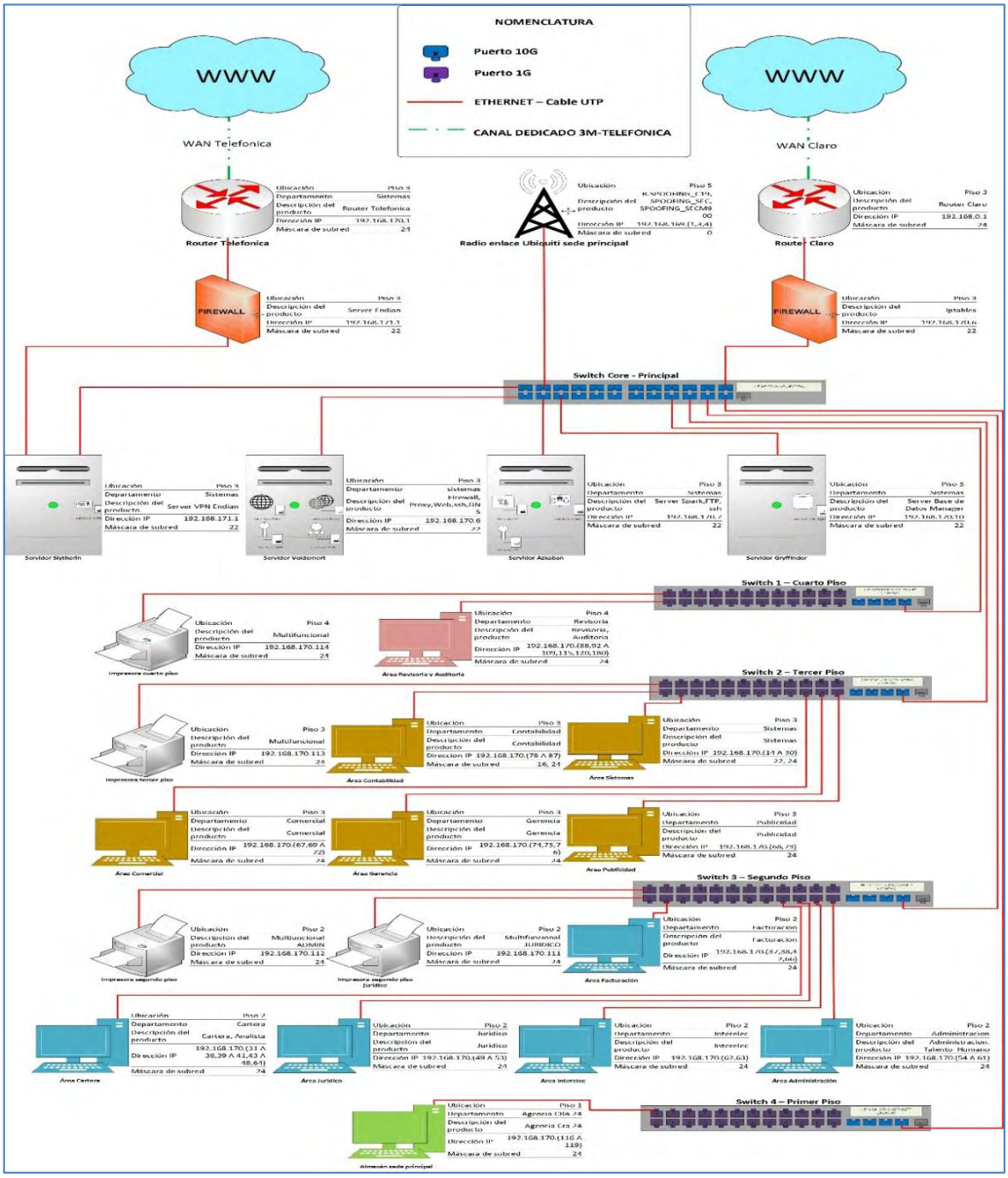


Figura 53. Diseño lógico de sede principal Pasto.

9.4.2 Diseño lógico agencia calle 19:

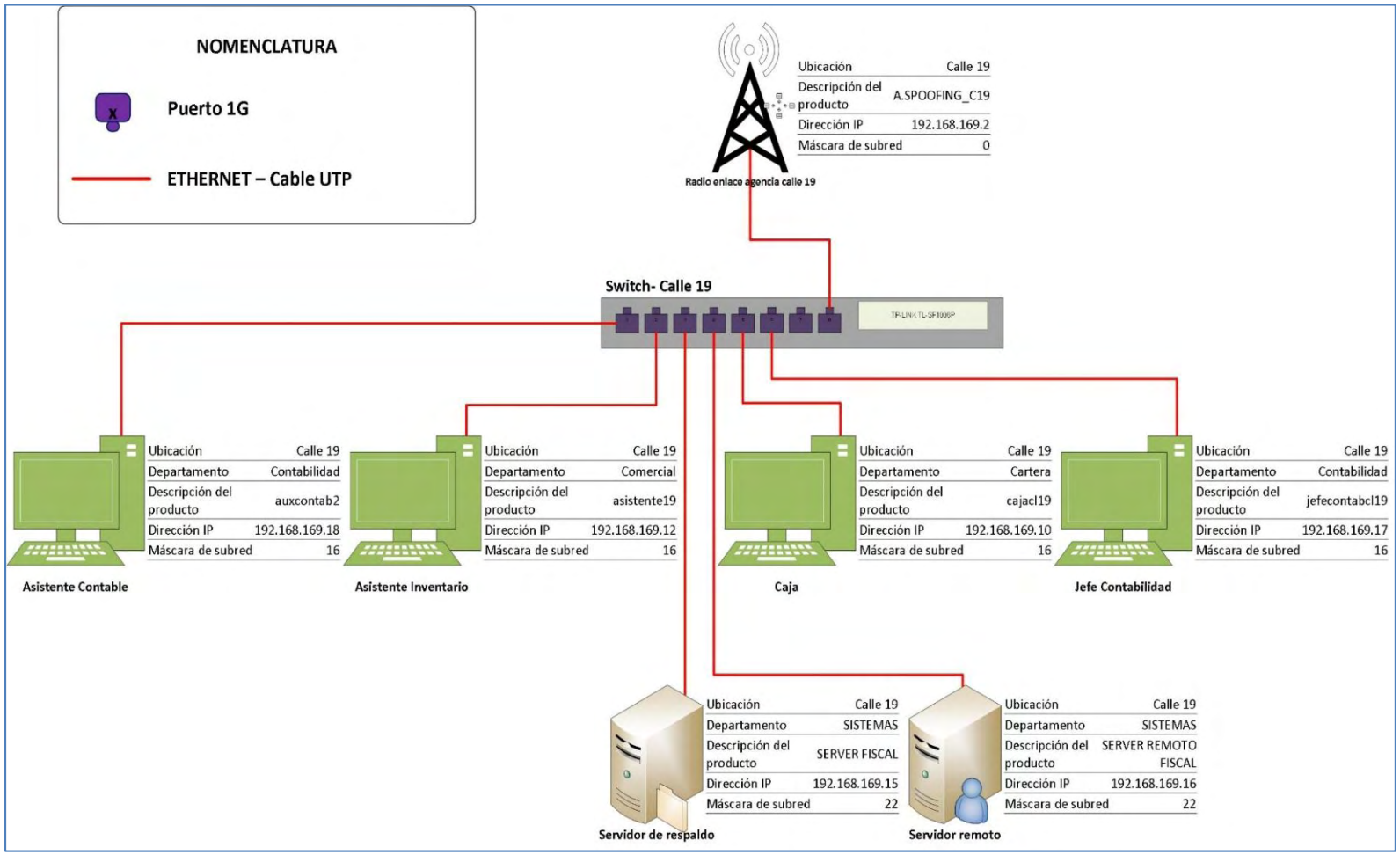


Figura 54. Diagrama lógico agencia calle 19 Pasto.

9.4.3 Diseño lógico agencia calle 17:

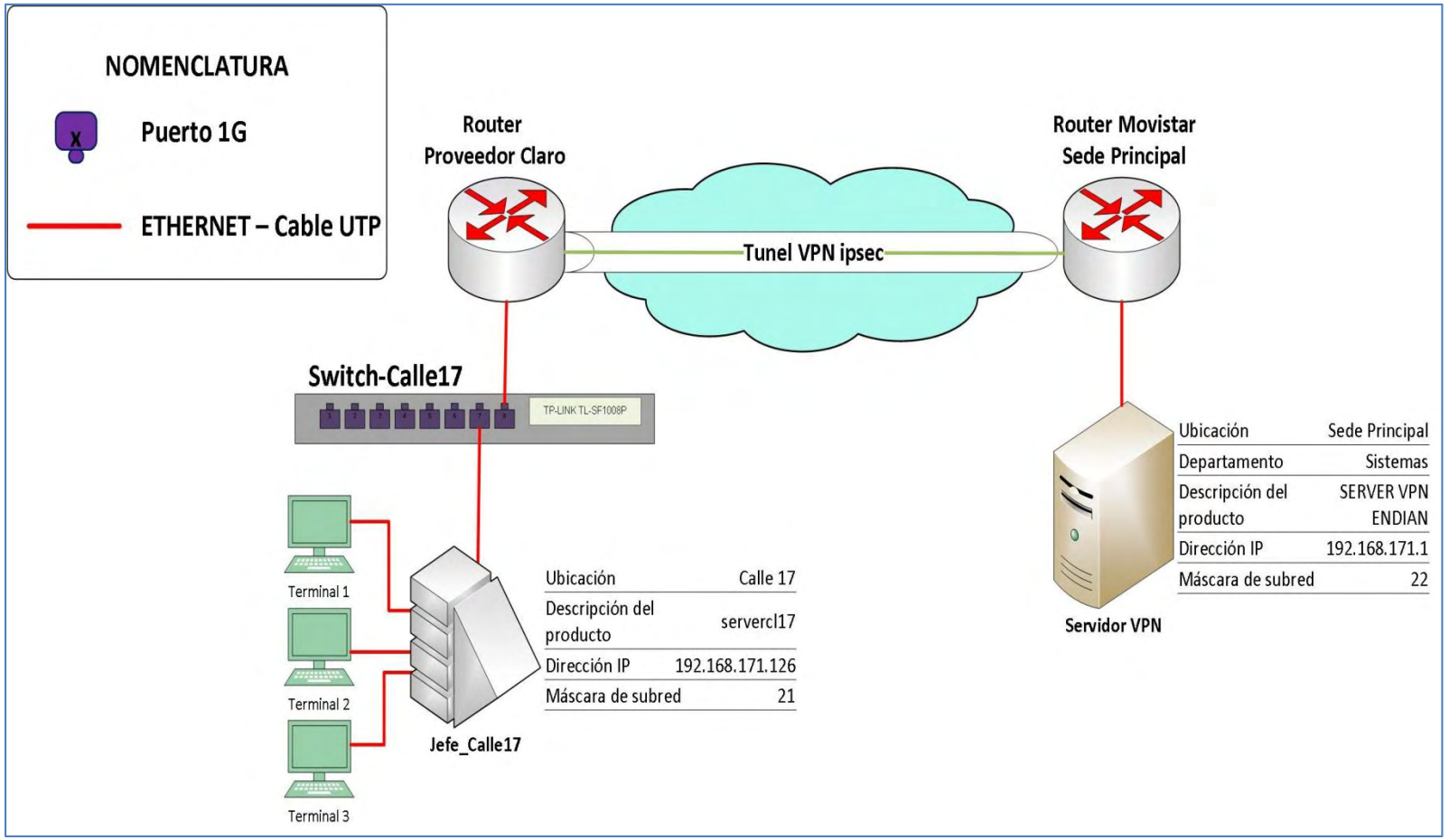


Figura 55. Diagrama lógico agencia calle 17 Pasto.

9.4.4 Diseño lógico agencia keeway calle 17:

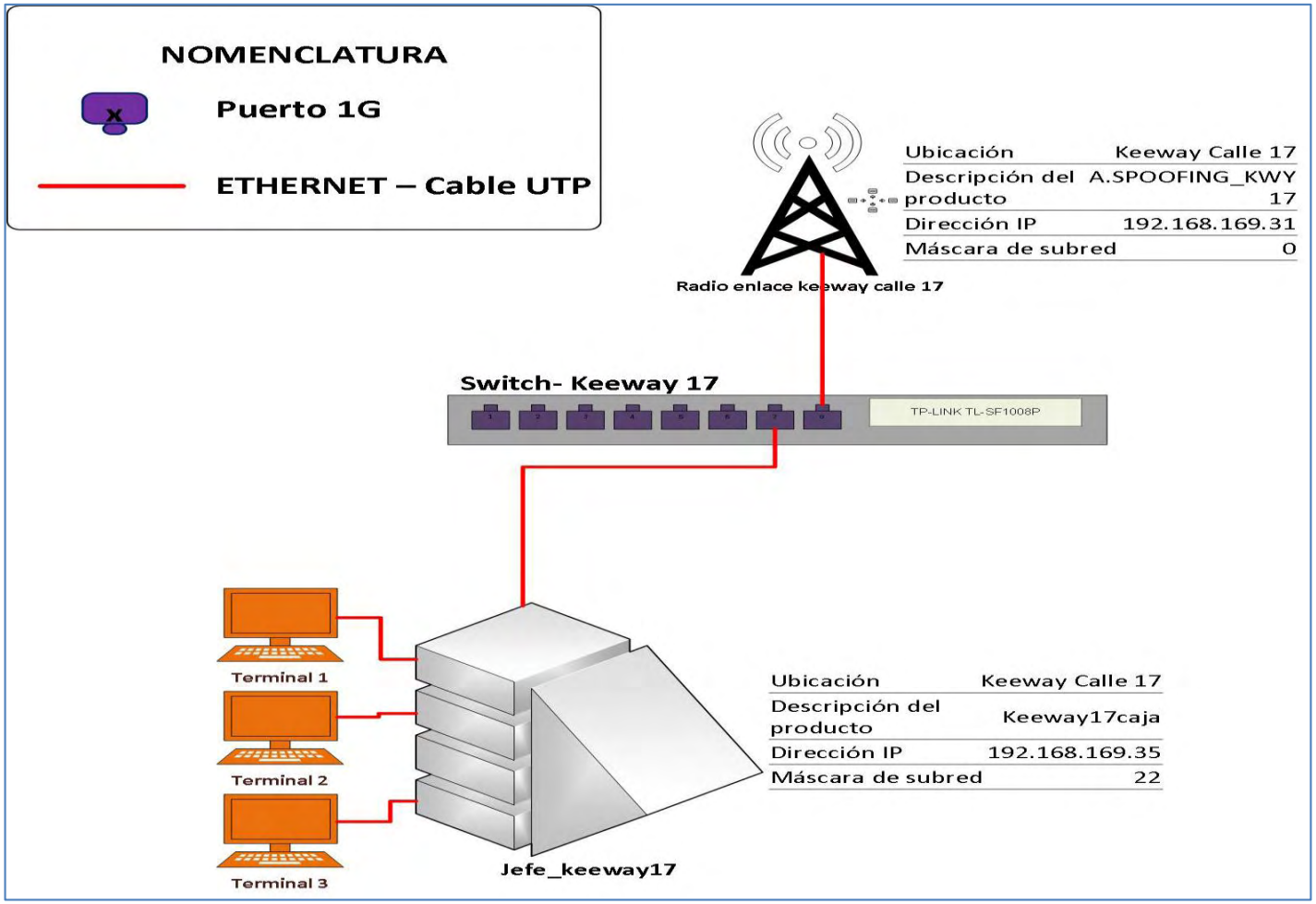


Figura 56. Diagrama lógico agencia calle 19 Pasto.

9.4.5 Diseño lógico agencia carrera 20:

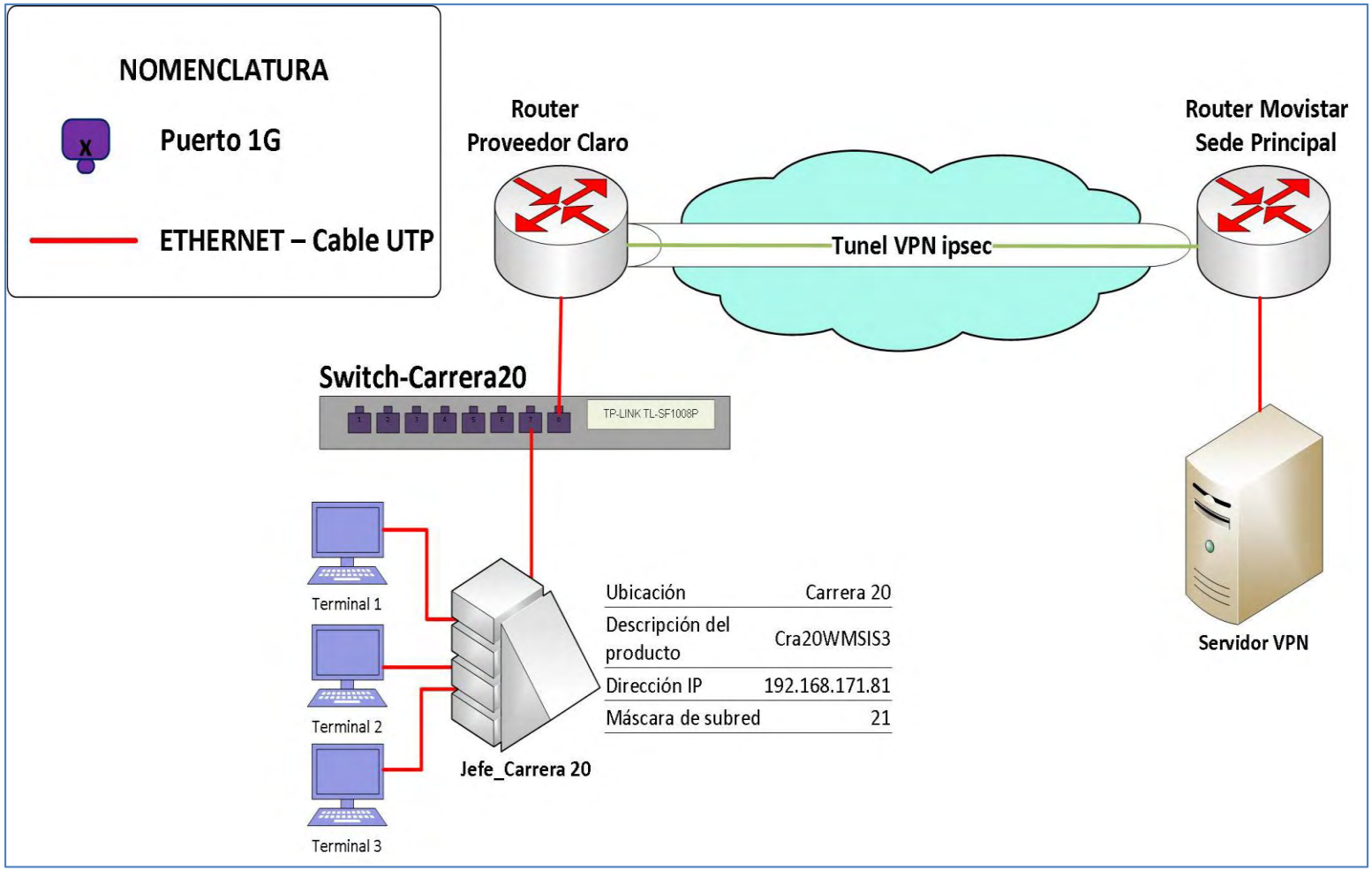


Figura 57. Diagrama lógico agencia carrera 20 Pasto.

9.4.6 Diseño lógico agencia carrerea 25:

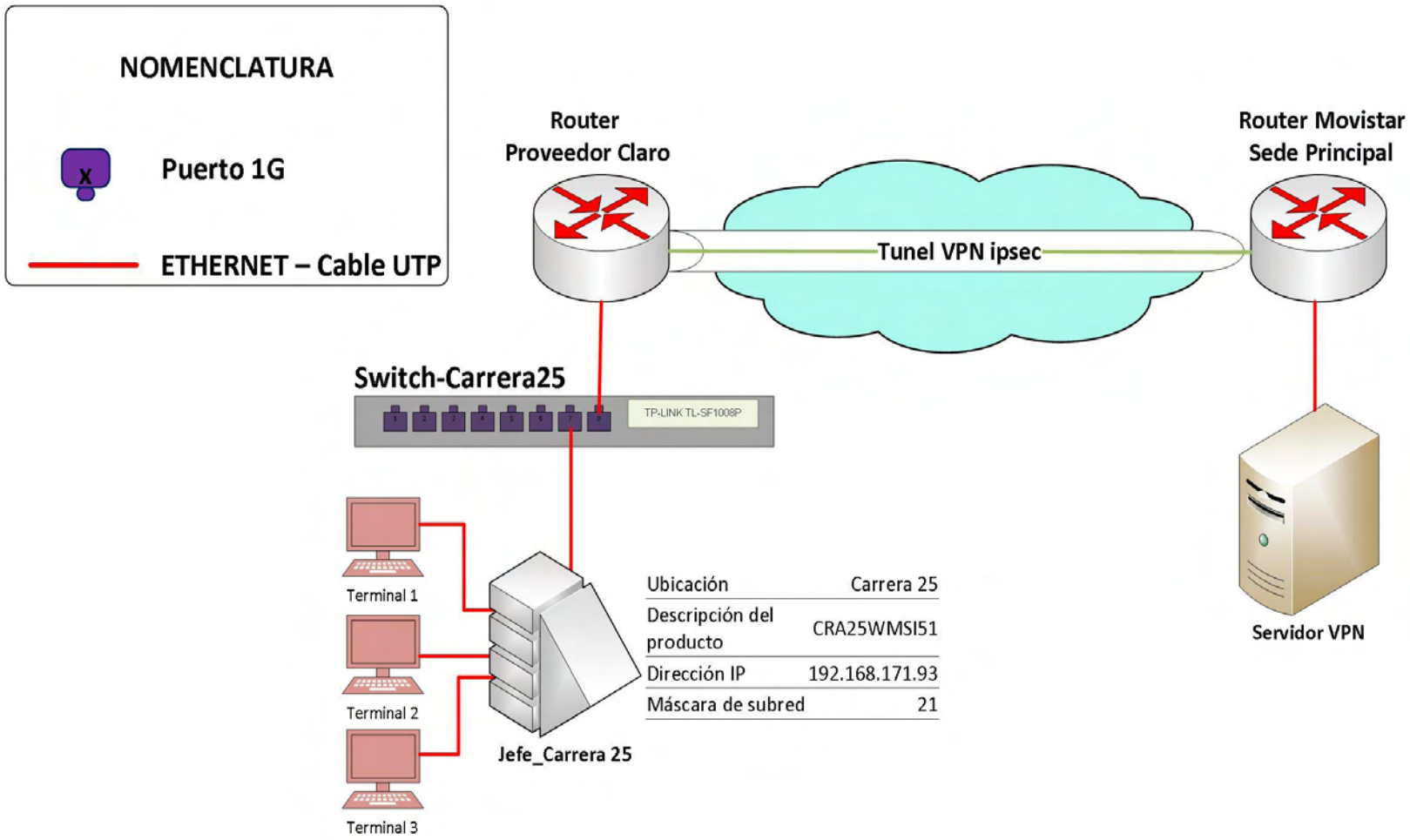


Figura 58. Diagrama lógico agencia carrera 25 Pasto.

9.4.7 Diseño lógico agencia keeway américas:

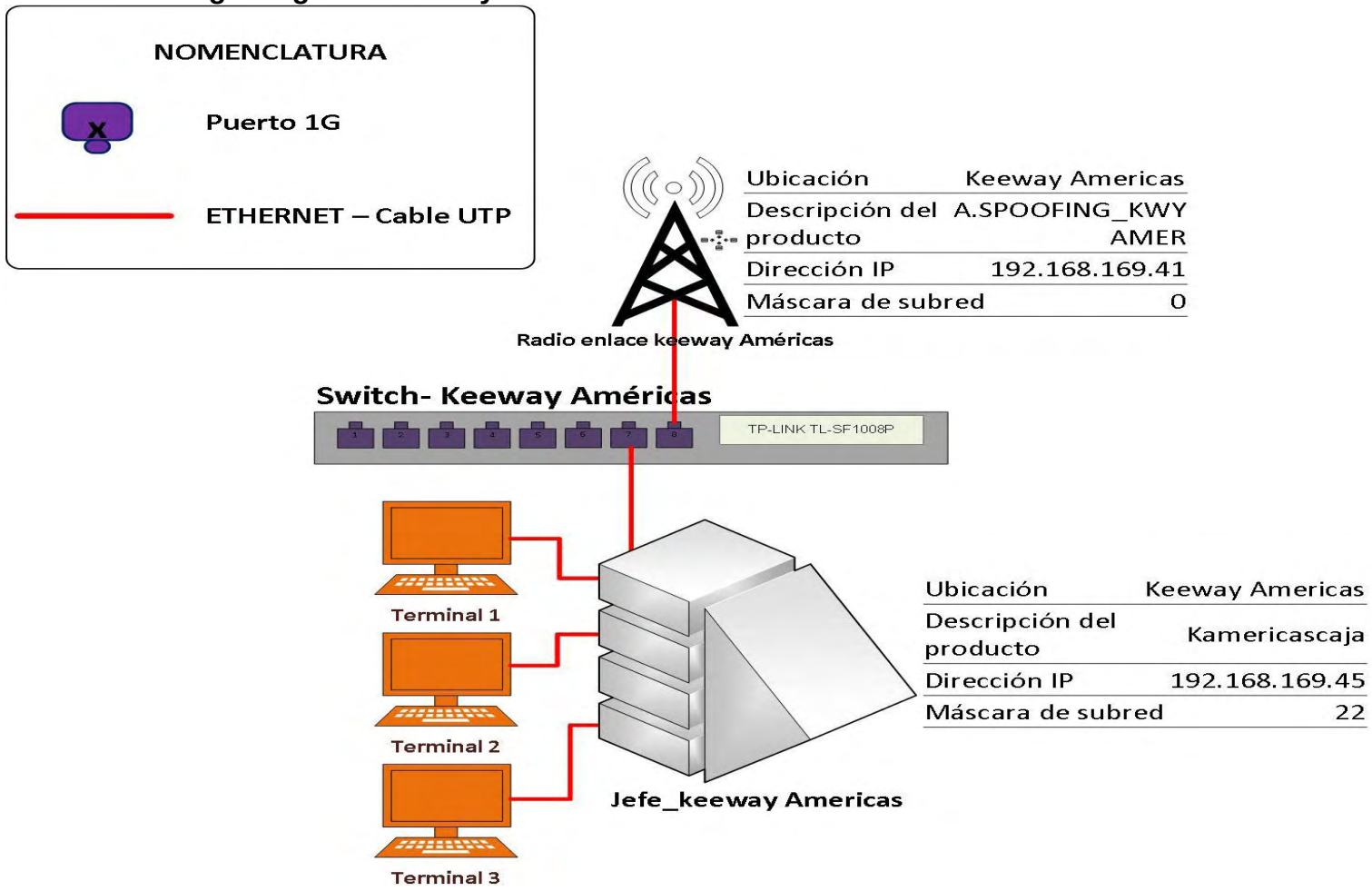


Figura 59. Diagrama lógico agencia keeway las americas Pasto.

9.4.8 Diseño lógico bodega principal:

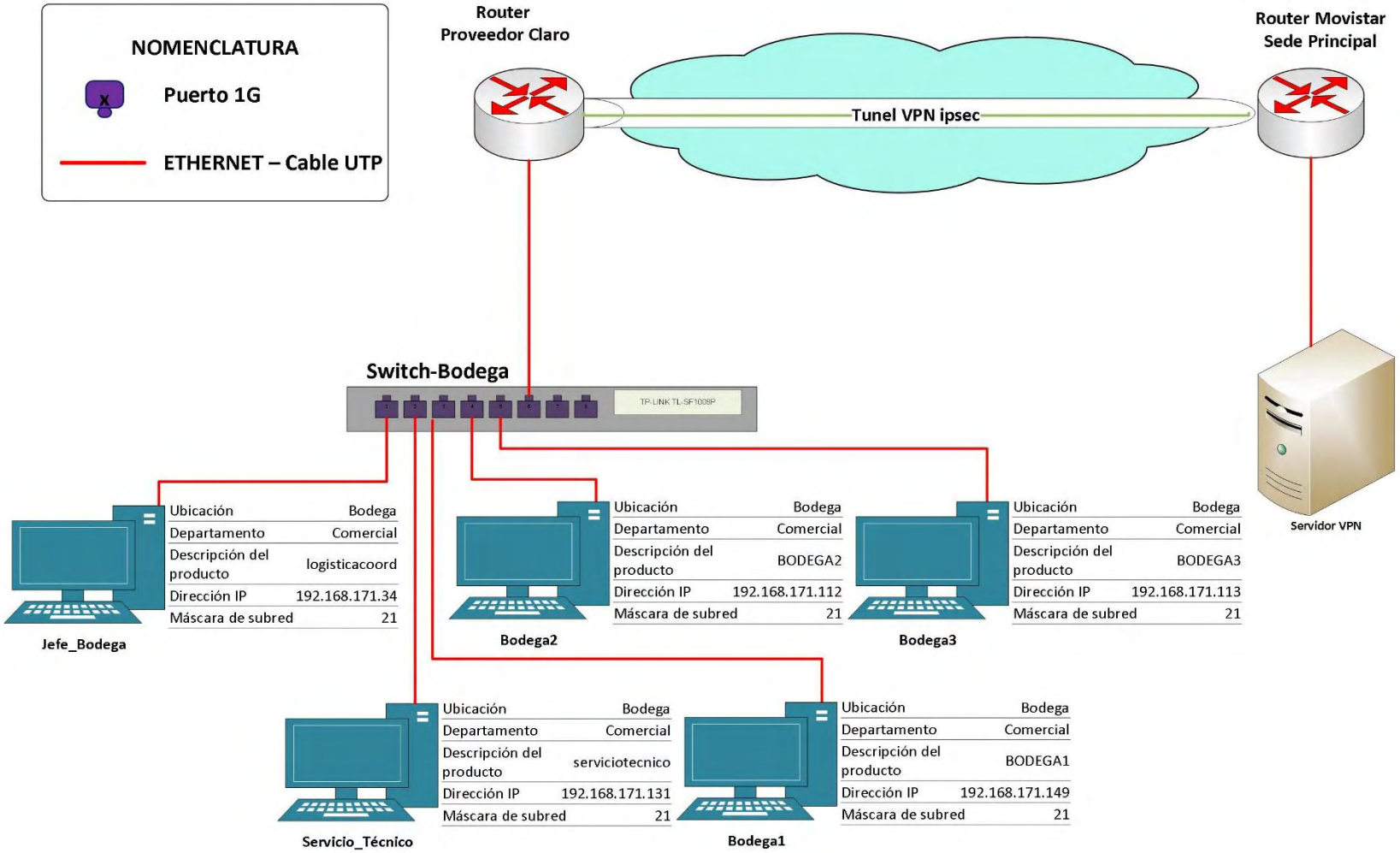


Figura 60. Diagrama lógico bodega principal Pasto.

9.4.9 Diseño lógico agencia las lunas:

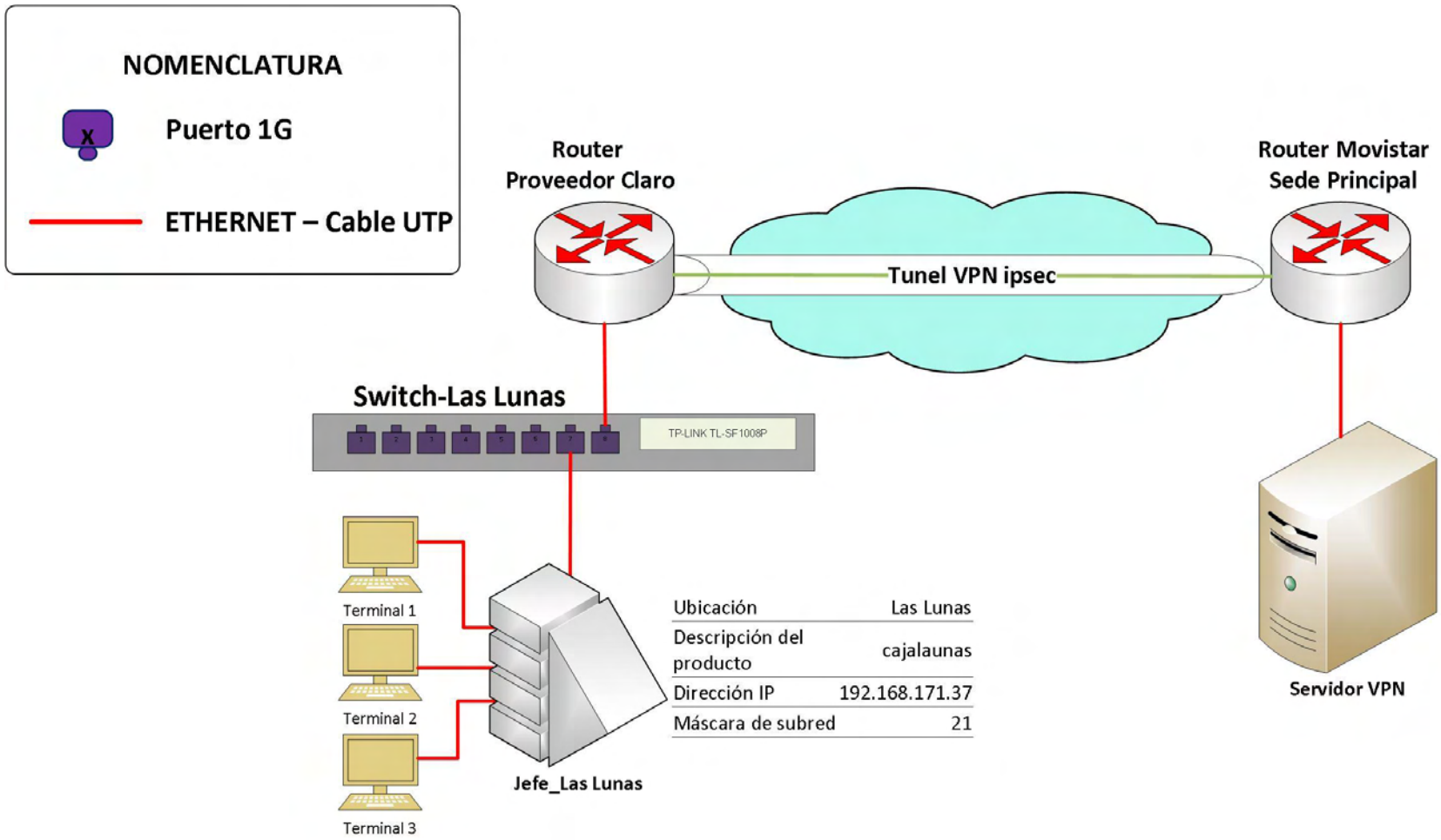


Figura 61. Diagrama lógico agencia las lunas Pasto.

9.4.10 Diseño lógico sede Cali:

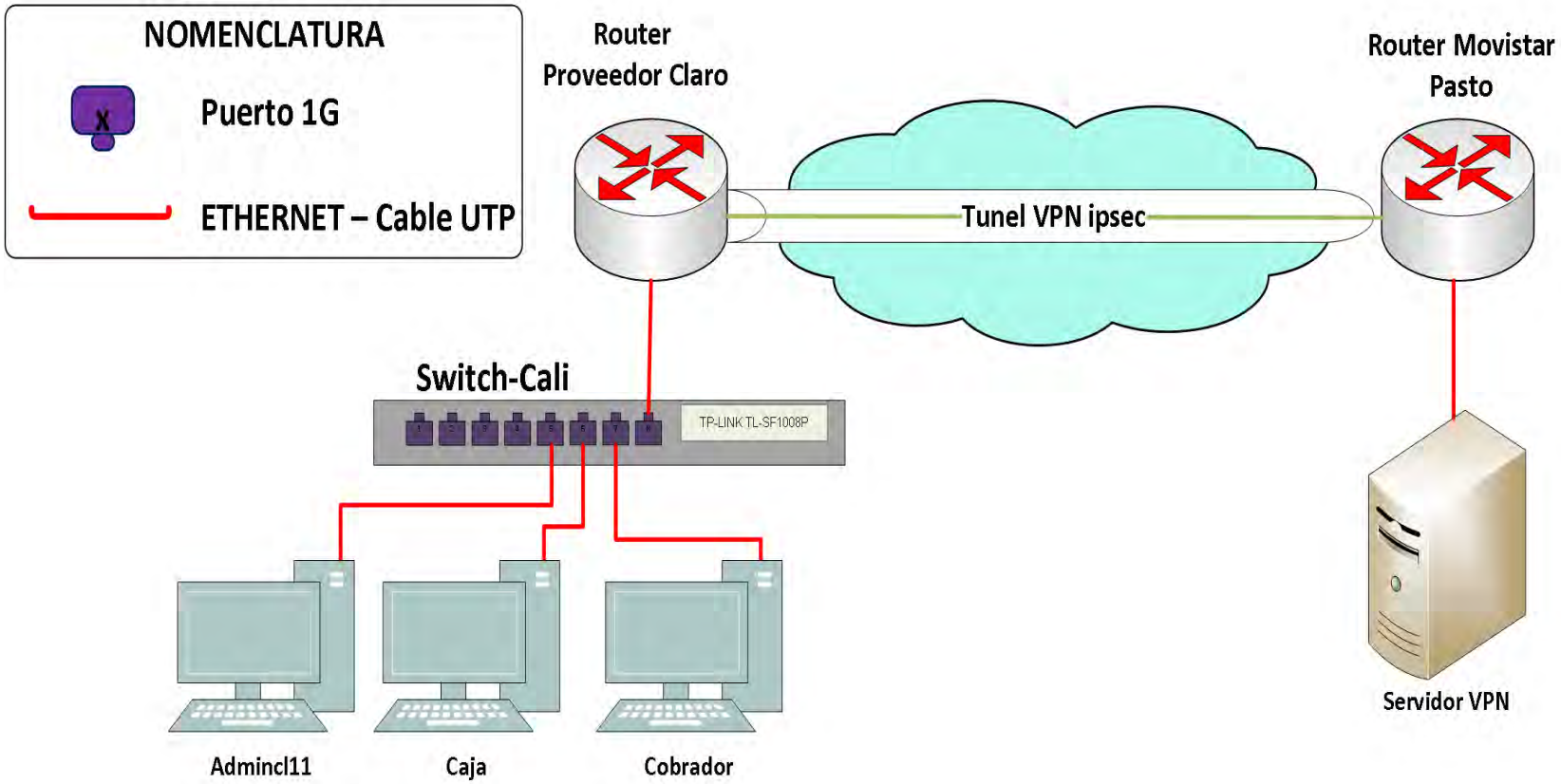


Figura 62. Diagrama lógico sede Cali.

9.4.11 Diseño lógico sede Yumbo:

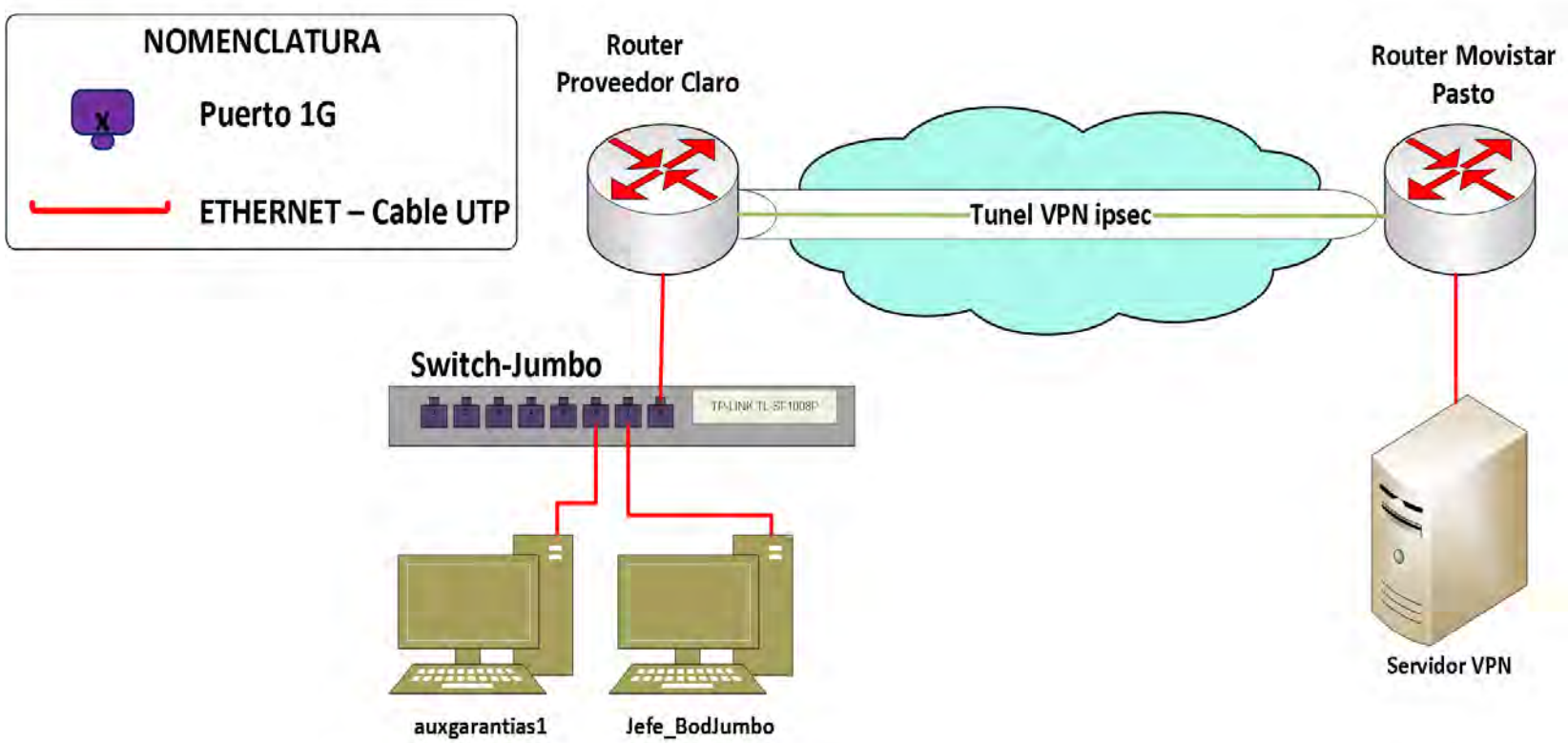


Figura 63. Diagrama lógico sede Yumbo.

9.4.12 Diseño lógico sede Popayán:

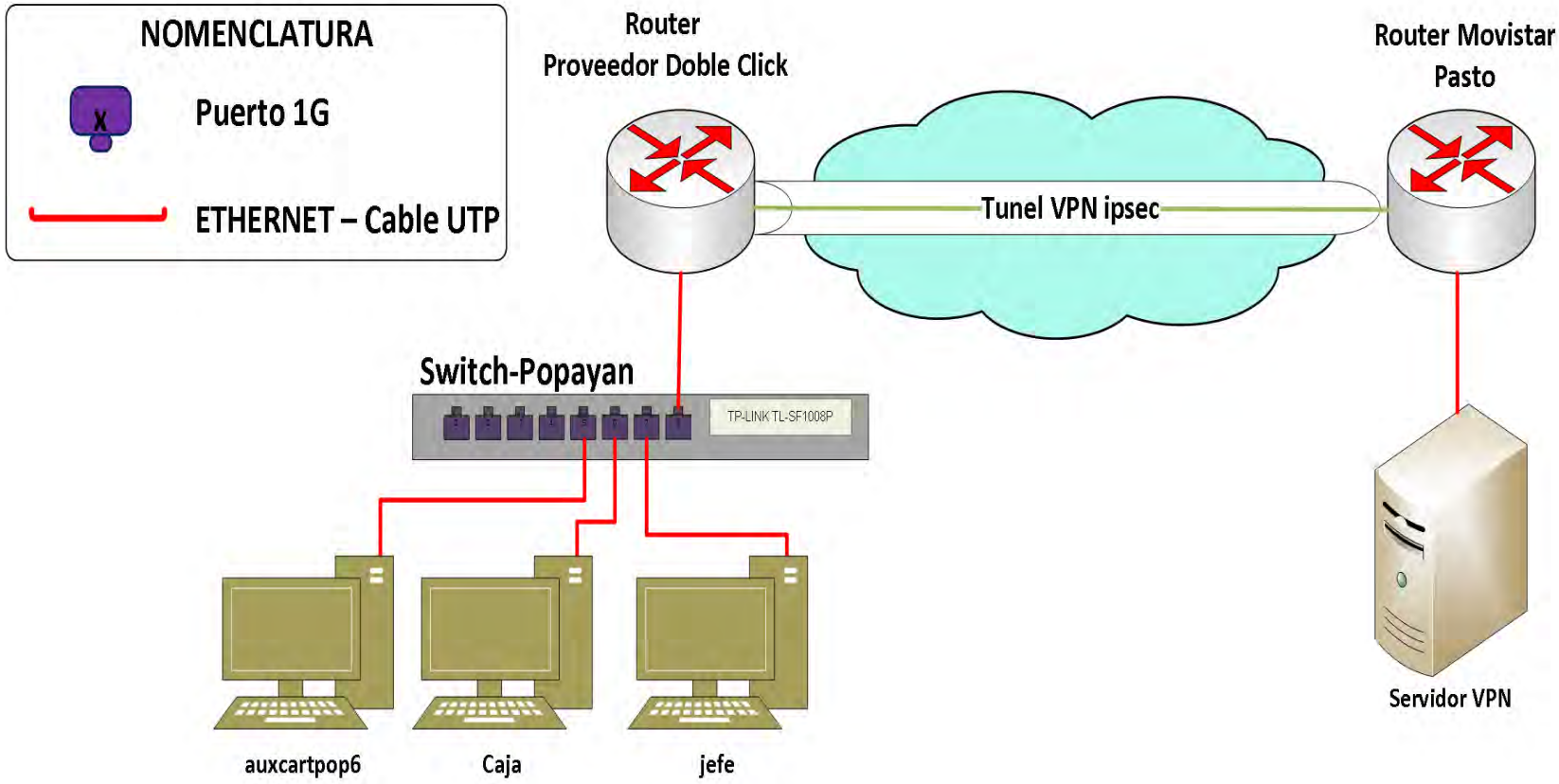


Figura 64. Diagrama lógico sede Popayán.

9.4.13 Diseño lógico sede Tumaco:

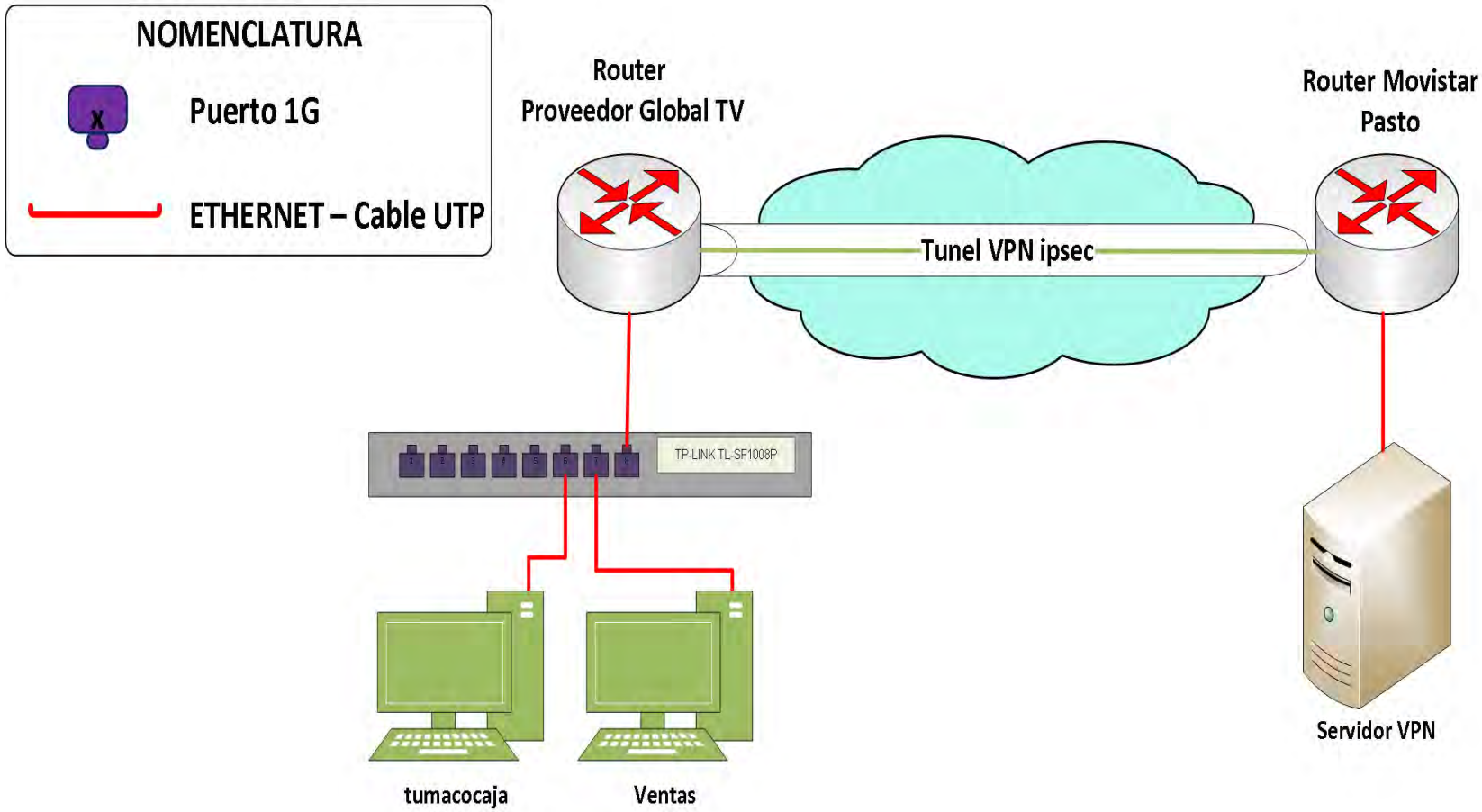


Figura 65. Diagrama lógico sede Tumaco.

9.4.14 Diseño lógico sede Mocoa:

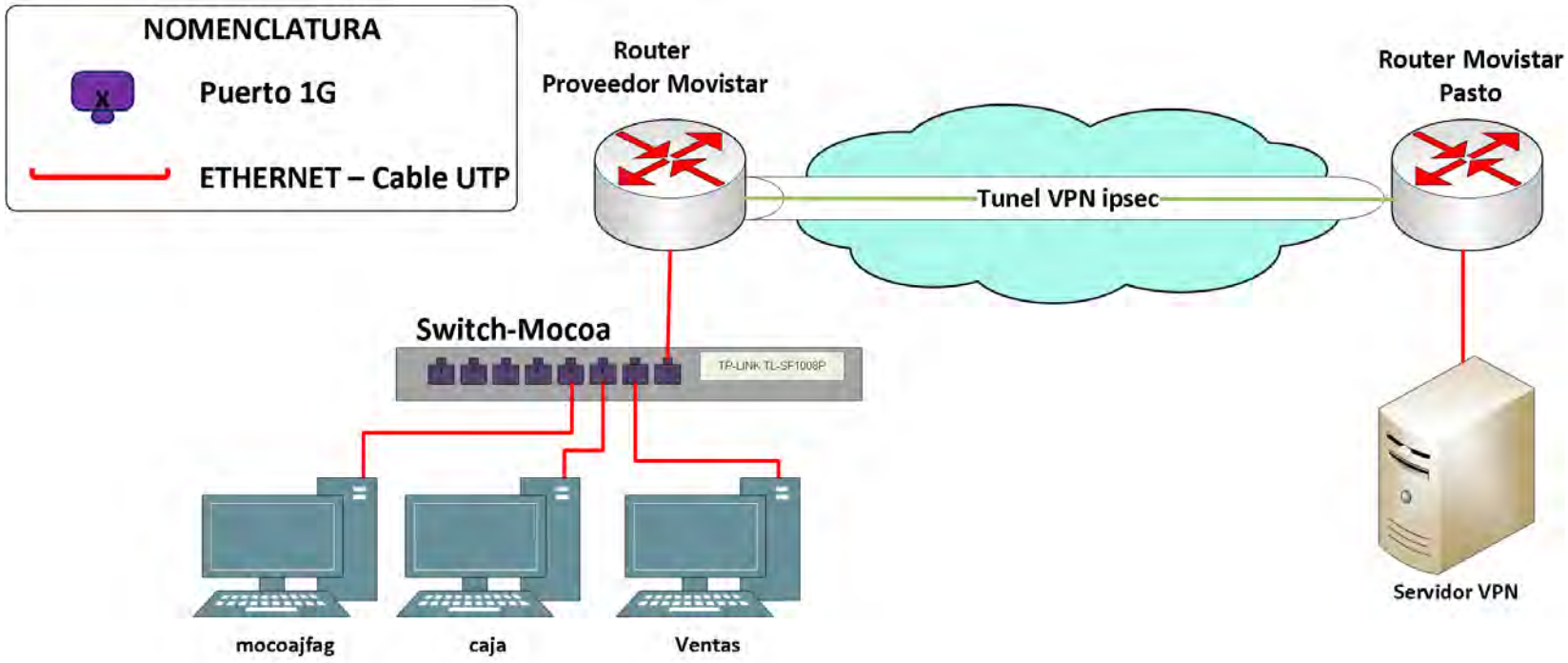


Figura 66. Diagrama lógico sede Mocoa.

9.4.15 Diagrama físico:

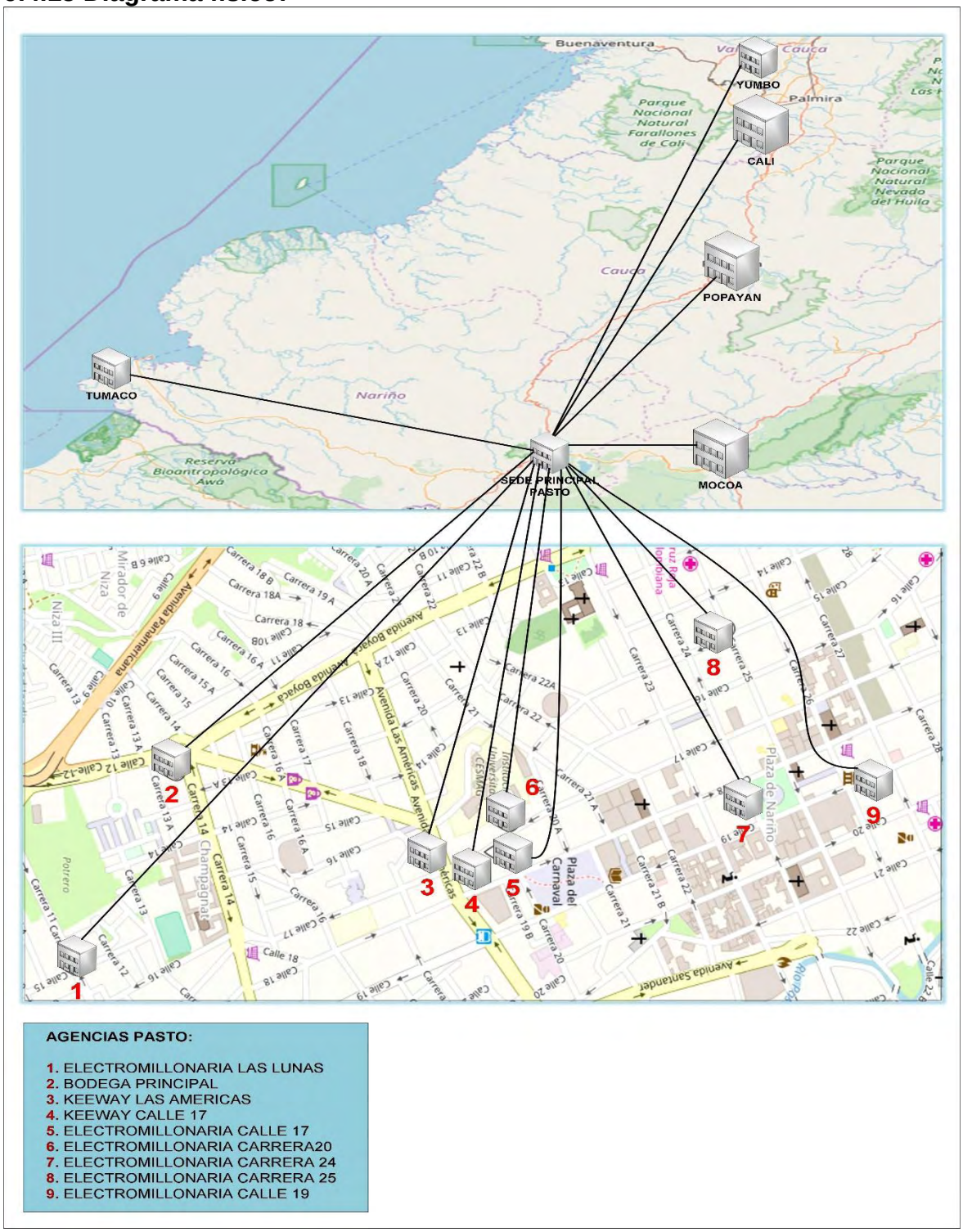


Figura 67. Diagrama físico red de datos.

9.5 INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS DE RED EN ENTORNO VIRTUAL

Para tener mayor claridad de los servicios de red que se van a monitorear fue necesario instalarlos y configurarlos en un entorno virtual, ya que es necesario realizar pruebas de instalación y configuración antes de configurar la suite de monitoreo en el servidor principal, porque la empresa ELECTROMILLONARIA está en continuo funcionamiento por su amplia cobertura. Por tal motivo no se puede interrumpir el funcionamiento de sus procesos.

Los siguientes servicios de red son los que se van a monitorear y fueron instalados y configurados en entorno virtual, dicho proceso se mostrara en los anexos descritos en cada servicio.

- SERVICIO DNS BIND9

  Ver

Anexo D. Instalación y configuración servidor DNS bind9.

- SERVICIO WEB APACHE2

  Ver

Anexo E. Instalación y configuración de servidor web Apache.

- SERVICIO PROXY SQUID

  Ver

Anexo F. Instalación y configuración de servidor proxy SQUID.

- SERVICIO FTP SFTP

  Ver

Anexo G. Instalación y configuración de servidor ftp.

- SERVICO ACCESO REMOTO SSH

  Ver

Anexo H. Instalación y configuración de servidor ssh.

- SERVICIO MENSAJERIA INSTANTANEA OPENFIRE

Anexo I. Instalación y configuración de servidor chat OPEN FIRE.

9.6 IMPLEMENTACIÓN DE LA SUITE DE MONITOREO EN ENTORNO VIRTUAL

La implementación de la suite de monitoreo se realizó en un entorno virtual, esto facilitó la instalación y configuracion de cada uno de los paquetes que integran la suite: Nagios, Check_MK, PNP4Nagios y Nagvis. Para la instalación y configuración de los paquetes fue necesario tener instalada una maquina virtual Ubuntu de 64bits, con una distribución Debian8 Jessie, solamente con los paquetes iniciales de instalación. Una vez instalado el SO en donde se iba a correr la suite de monitoreo, se realizó la intalación del software necesario para montar la suite tanto en los servidores como en las maquinas remotas. Terminada la instalación y configuración de cada uno de los paquetes de la suite, se hace una una vinculación de los paquetes instalados quedando integrados para que funcionen como uno solo. Dicha vinculación fue posible mediante investigación desarrollada por los integrantes de este trabajo.

Finalmente, se tuvo en cuenta prácticas de seguridad sugeridas por Nagios para la implementación de la suite dentro de la empresa, prácticas como autenticación implicita, implementacion de ssl en apache y controles de acceso mediante restricciones de IP.

Para detallar todo el proceso de implementación de la suite de monitoreo en entorno virtual ver

Anexo K. Implementación de la suite de monitoreo en entorno virtual.

9.7 CONFIGURACIÓN DE NOTIFICACIONES EN NAGIOS Y CHECK_MK

El sistema de envió de notificaciones disponible en Nagios y check_mk, es una herramienta fundamental al momento de monitorear la red de datos, ya que a través de ésta el administrador puede mantenerse informado del estado no deseados de los componentes de la red sin estar presente en el servidor de monitoreo, permitiéndole realizar otras actividades sin descuidar el estado de la red de datos.

Para poder implementar este servicio es necesario instalar el servidor de correo Postfix y realizar configuraciones en las herramientas Nagios (envio de notificaciones de servicios de red) y check_mk (envio de notificaciones componentes de red), dicha instalación y configuración se detallan en el

Anexo J. Instalación y configuración de servidor de correo postfix.

9.8 MIGRACIÓN DE LA SUITE DE MONITOREO DE RED A SERVIDOR DE LA EMPRESA

9.8.1 Requerimientos hardware y software del servidor. Requerimientos hardware: la implementación de la suite de monitoreo se realizó sobre:

- Nombre del dispositivo: DebianServer
- Memoria: 3,8GiB
- Procesador: Intel core i3-4005U CPU@1.70GHz x 4
- Gráficos: Intel Haswell Mobile
- Sistema Base: Debian GNU/Linux 8 (jessie) 64-bit
- Disco: 198,3 GB
- GNOME: versión 3.14.1

Requerimientos software: en cuanto a requerimientos software se opto por intalar el paquete LAMP, se denomina LAMP al conjunto de herramientas para describir un conjunto de soluciones en una infraestructura de red de datos.

Las herramientas utilizadas son:

- **L**inux, sistema operativo.
- **A**pache, servidor web.
- **M**ariaDB, gestor de base de datos.
- **P**hp, lenguaje de programación.

Para detalles en cuanto a la instalación y configuracion del paquete LAMP ver

Anexo K. Implementación de la suite de monitoreo en entorno virtual. En el punto 1.2. Como guía referente para la instalación se tomo lo encontrado en (geekland , 2018).

9.8.2 Instalación de la suite de monitoreo. Para la migración de la suite de monitoreo al servidor de la empresa es necesario hacer la instalación total de la suite de monitoreo, es decir instalar desde cero los paquetes de Nagios, Check_MK, Nagvis y PNP4Nagios. Para esto se debe mirar el

Anexo K. Implementación de la suite de monitoreo en entorno virtual. Punto 2. Esto se hace debido a que el servidor tiene en funcionamiento otros servicios de red, impidiendo hacer una réplica total de la máquina virtual al servidor.

El único archivo que se migra, es: “servicios.cfg”, donde se encuentra la configuración del monitoreo de servicios de red que se realizó a través de Nagios.

El archivo se encuentra en la siguiente ruta:

```
cd /usr/local/nagios/etc/objects
```

Debe quedar de la siguiente manera:



Figura 68. Archivos del directorio objects de Nagios.

Y en la siguiente ruta:

```
cd /usr/local/nagios/etc/
```

Se edita el archivo:

```
nano nagios.cfg
```

En el archivo “nagios.cfg” Se debe adicionar la línea:
“cfg_file=/usr/local/nagios/etc/objects/servicios.cfg”.

Debe quedar de la siguiente manera:



Figura 69. Definición de archivo servicios.cfg en archivo nagios.cfg.

9.8.3 Configuración y puesta en marcha de suite de monitoreo. Para la configuración y puesta en marcha de la suite se deben seguir los pasos planteados en el

Anexo K. Implementación de la suite de monitoreo en entorno virtual. En los puntos 3.1 y 3.2.

Definición de máquina Windows y Linux con check_MK:

NOTA: Los pasos para definir un nuevo host, ya sea Windows o Linux son los mismos.

Todas las configuraciones de monitoreo en la plataforma de administración check_mk se realizan en el panel WATO configuration.

Se selecciona la opción Hosts

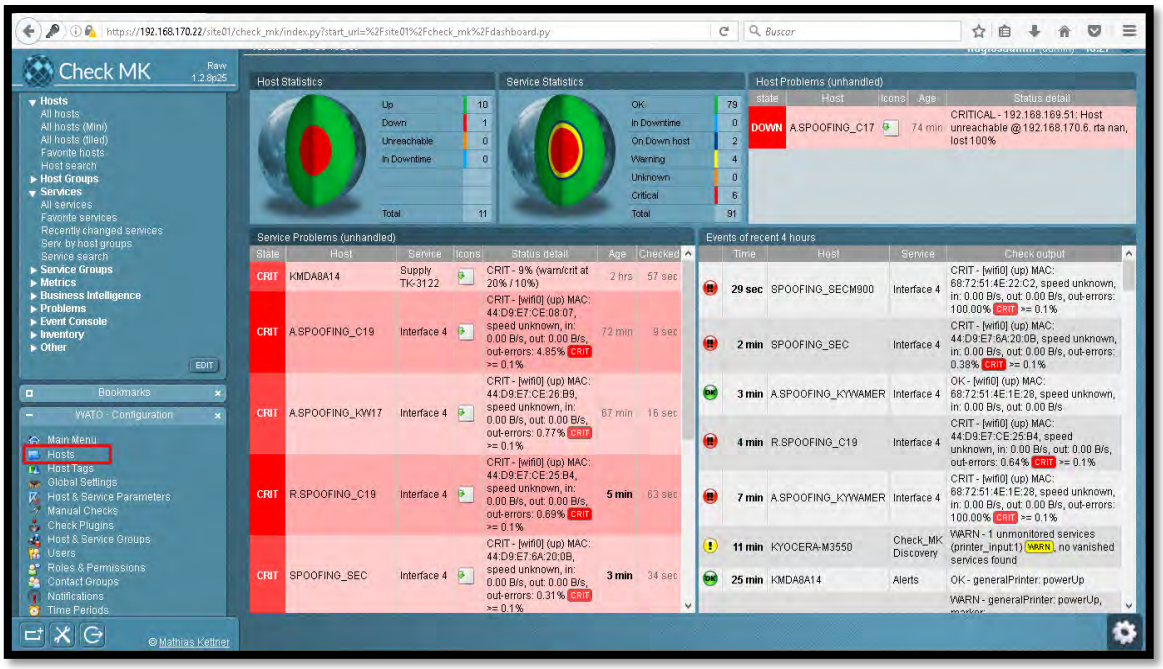


Figura DH 1. Plataforma de administración WATO, creación de host.

En seguida, se selecciona la opción New host, el nuevo host se creará en la ubicación que se desee, en este caso se creó en el folder que contiene los hosts del área de administración.

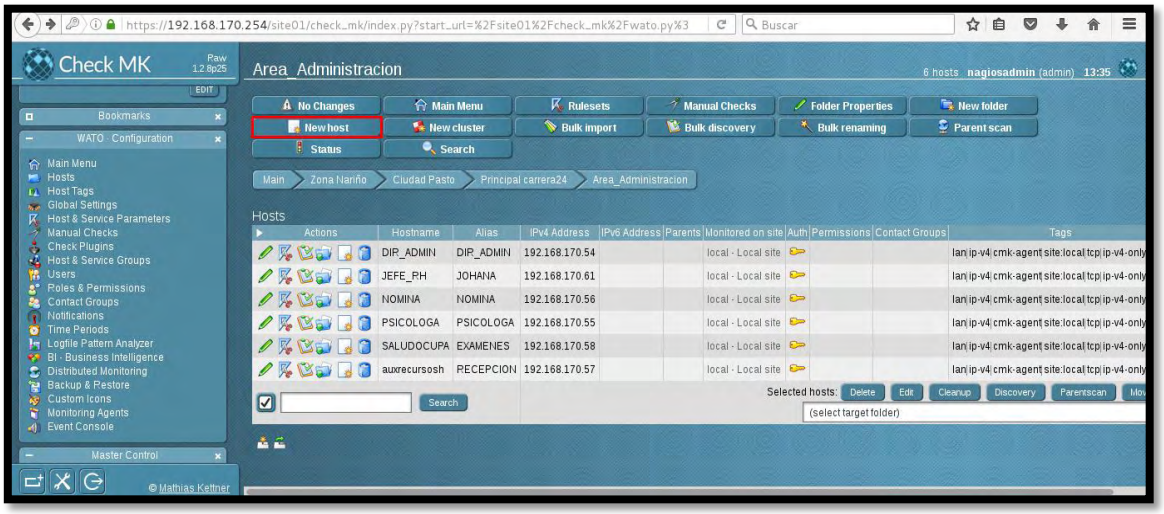


Figura DH 2. Plataforma de administración WATO, creación de host.

Luego, se completa la información requerida del host a crear, algo a tener en cuenta es el tipo de agente a utilizar, este varía dependiendo del dispositivo a monitorear. Para el caso de las maquinas Windows y Linux se utiliza el agente Check_MK Agent (server).

Después, se guarda la información y se realiza un test para verificar la comunicación de la máquina cliente con el servidor mediante el agente.

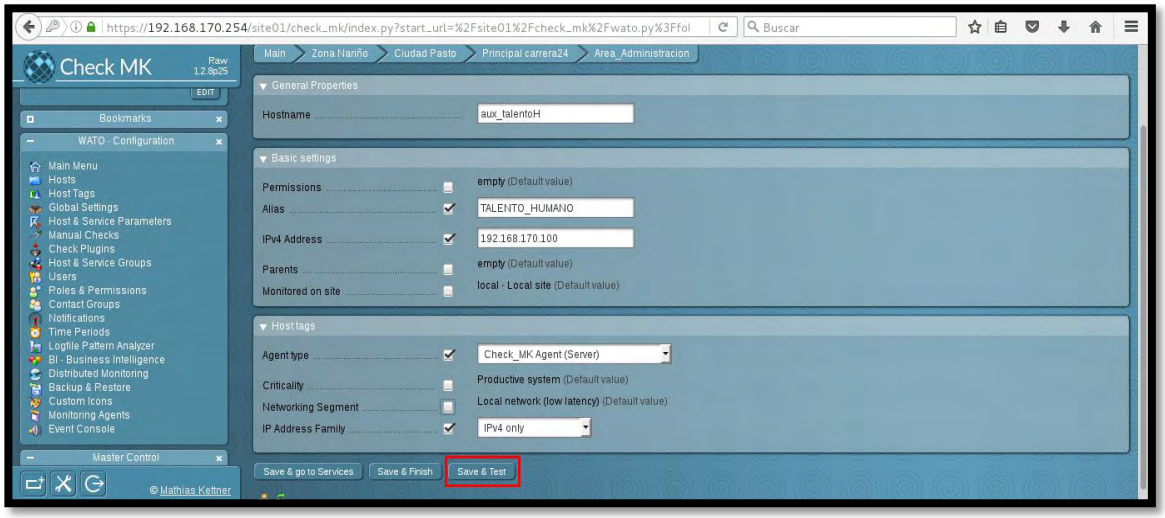


Figura DH 3. Plataforma de administración WATO, creación de host.

Luego, se verifica la comunicación, se puede observar que tiene ping y el agente responde perfectamente.

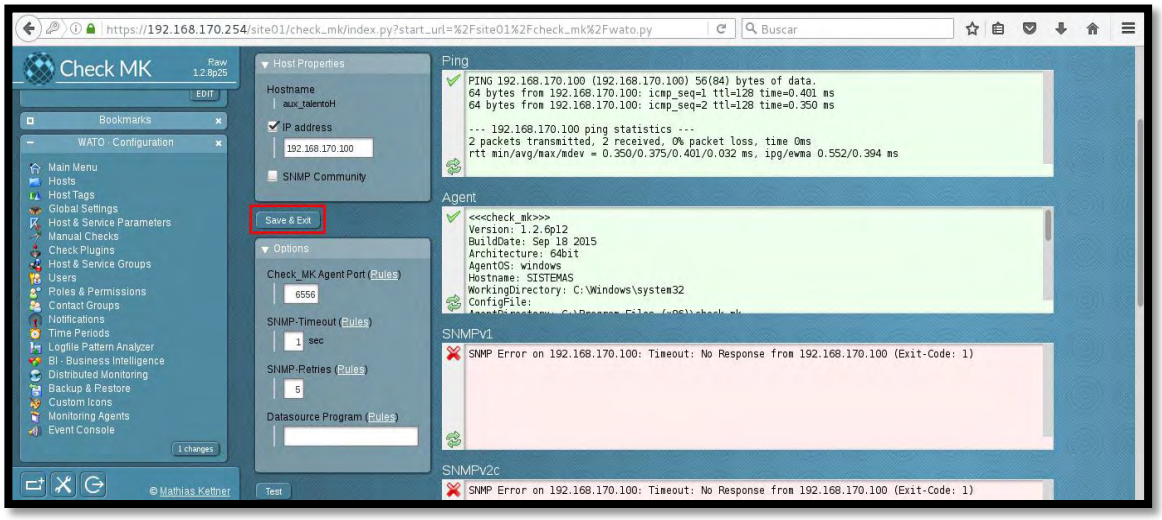


Figura DH 4. Plataforma de administración WATO, creación de host.

Una vez definido el nuevo host se da en la opción “services” para mirar el estado de los servicios que seran monitoredos en esta máquina.

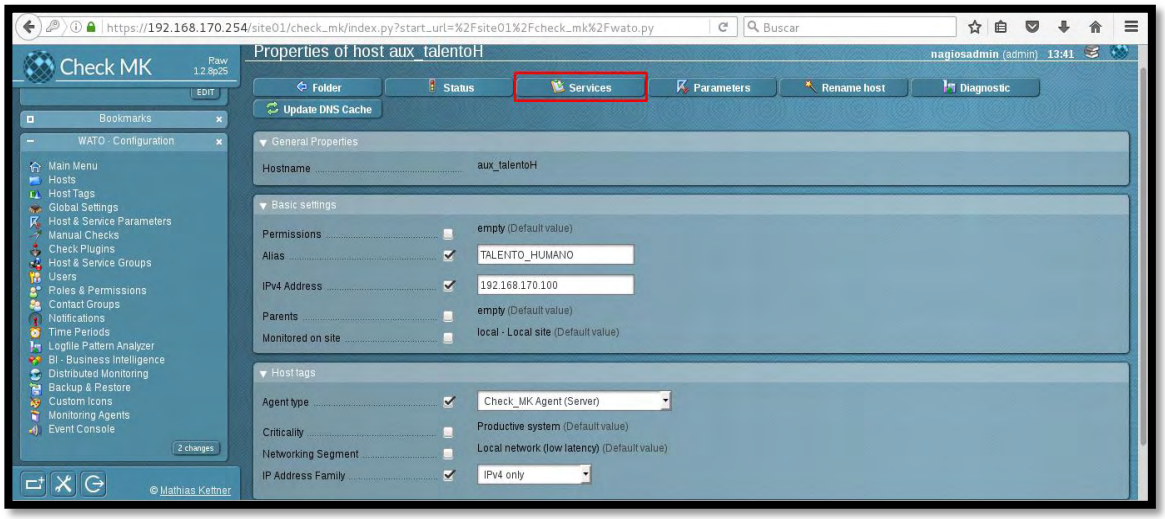


Figura DH 5. Plataforma de administración WATO, creación de host.

Se observa el estado de los servicios, luego se guarda de forma manual la configuración.

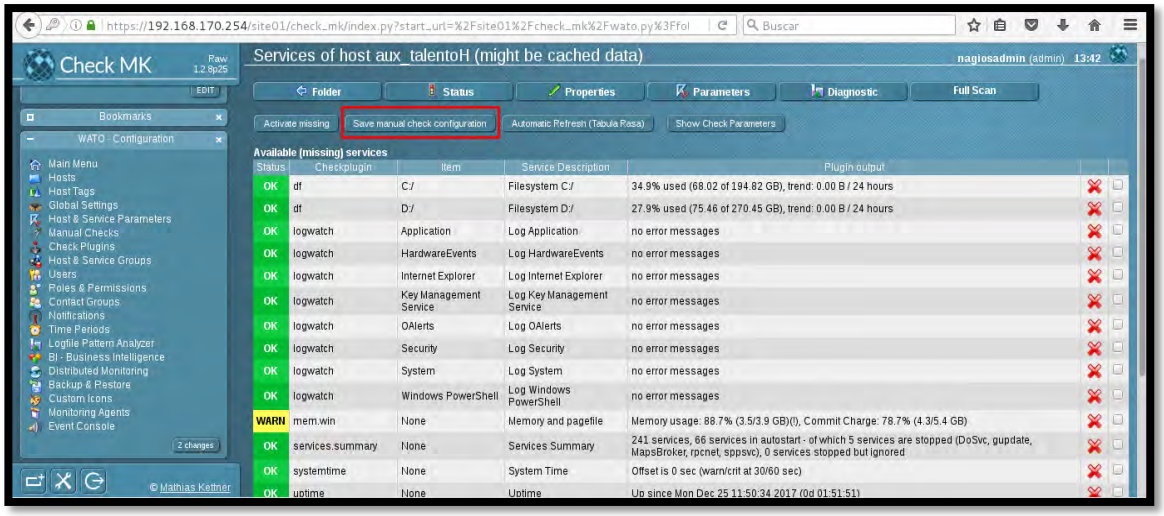


Figura DH 6. Plataforma de administración WATO, creación de host.

Luego, se guardan los cambios realizados. Se observa que el nuevo host ya se encuentra definido.

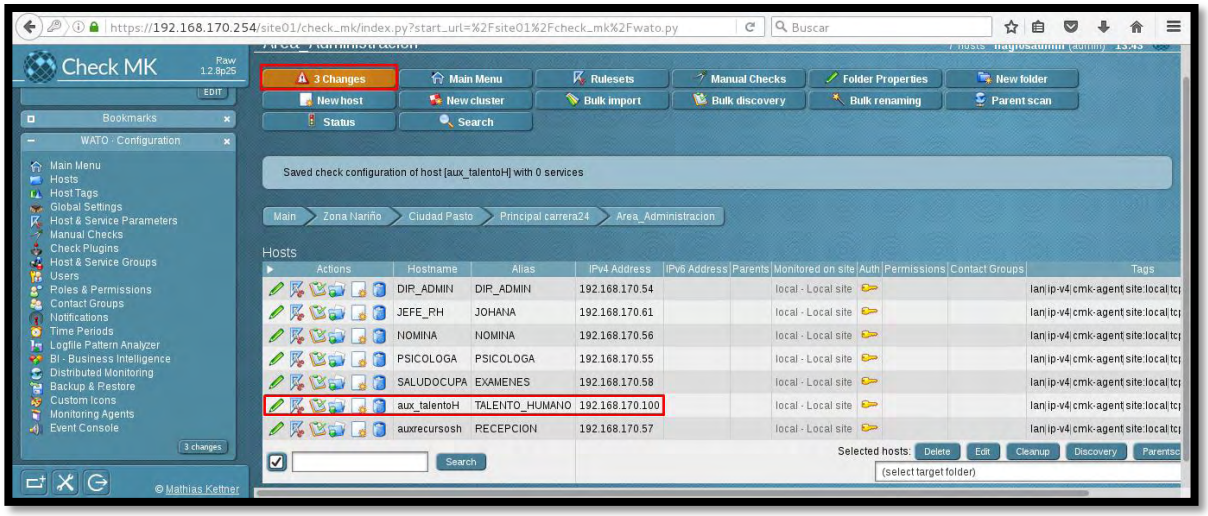


Figura DH 7. Plataforma de administración WATO, creación de host.

En seguida, se activan los cambios.

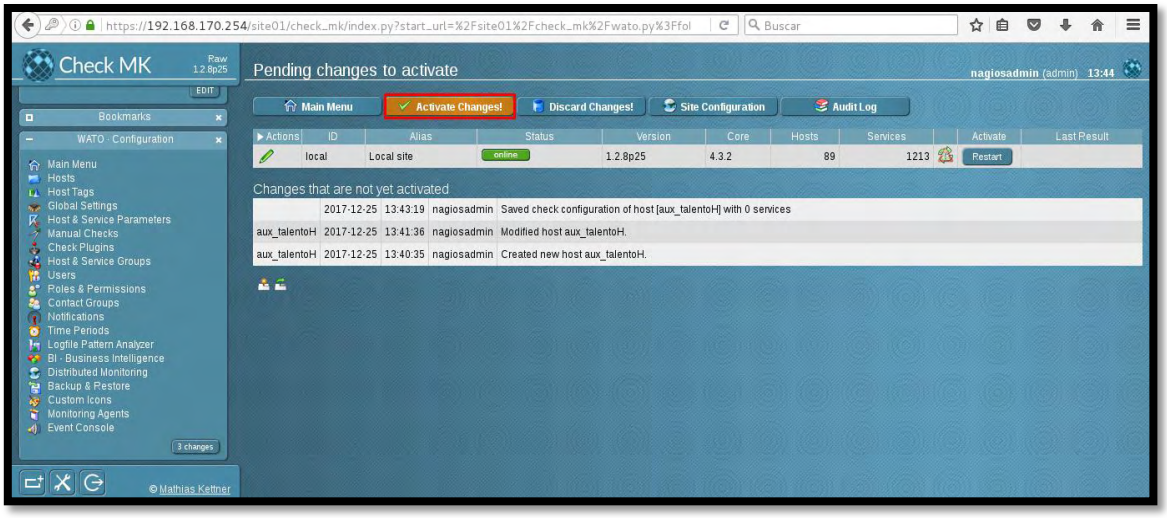


Figura DH 8. Plataforma de administración WATO, creación de host.

Despúes, se verifica que la nueva configuración se realizó satisfactoriamente. Luego se puede detallar la información del monitoreo del host creado en el panel de check_mk.

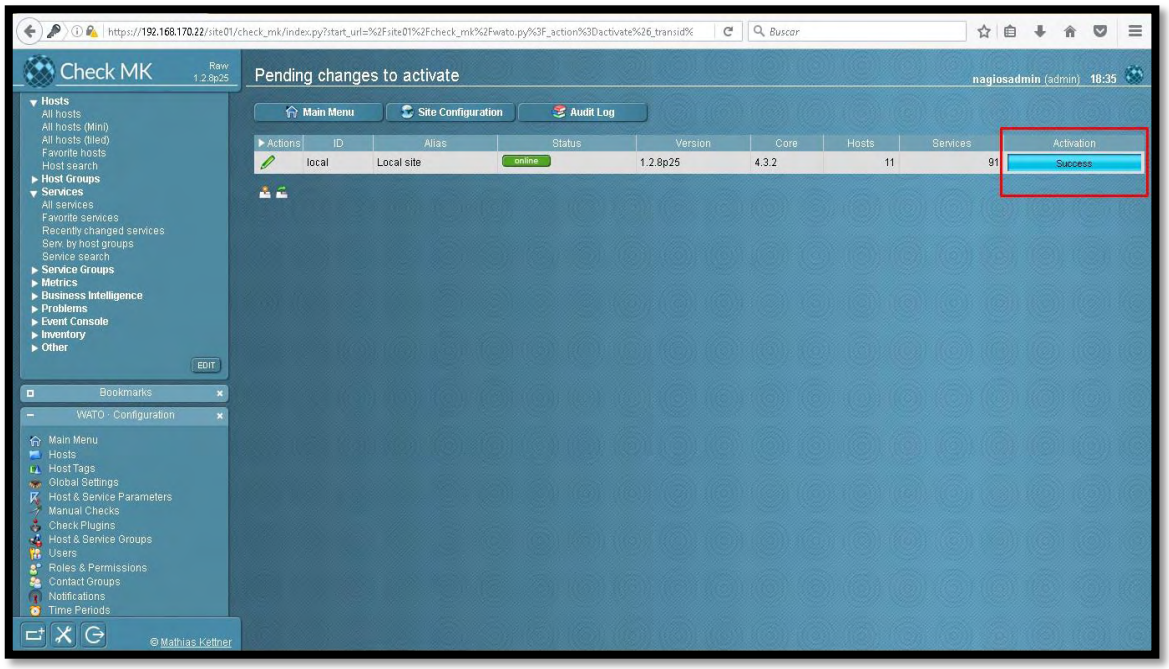


Figura DH 9. Plataforma de administración WATO, creación de host

Definición de impresoras: todas las configuraciones de monitoreo en la plataforma de administración check_mk se realizan en el panel WATO configuration.

En primer lugar, se selecciona la opción Hosts:



Figura DI 1. Plataforma de administración WATO, creación de impresora.

Luego, se selecciona la opción New host, el nuevo host se creará en la ubicación que se desee.

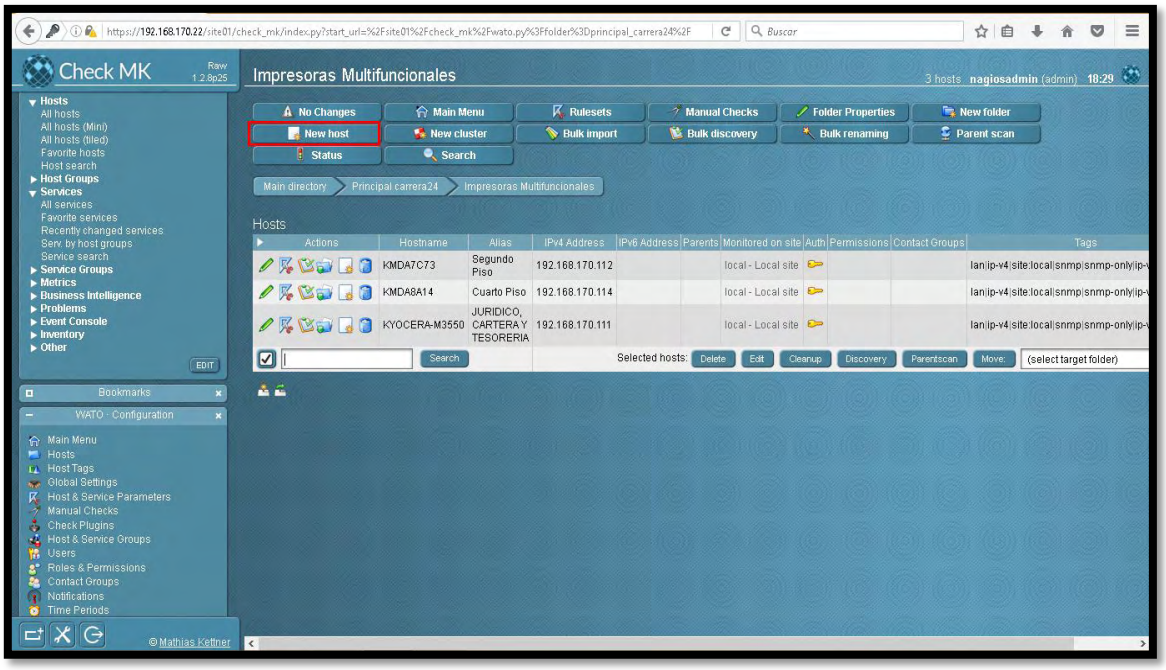


Figura DI 2. Plataforma de administración WATO, creación de impresora.

En seguida, se completa la información requerida del host a crear, algo a tener en cuenta es el tipo de agente a utilizar. Para el caso de las impresoras se utiliza el agente SNMP (Networking device, Appliance).

Posteriormente, se guarda la información y se realiza un test para verificar la comunicación de la máquina cliente con el servidor mediante el agente.

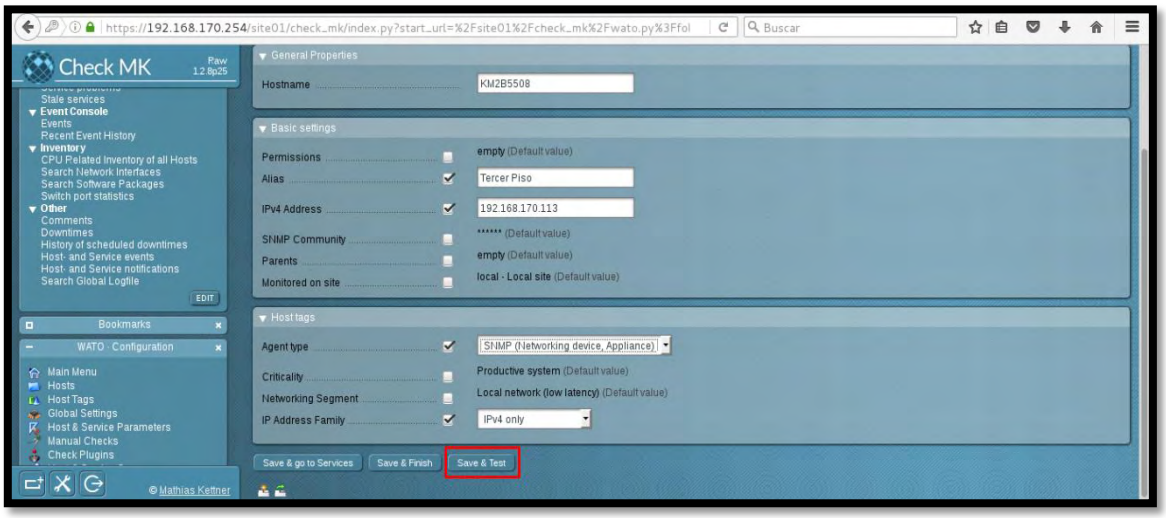


Figura DI 3. Plataforma de administración WATO, creación de impresora.

Luego, se verifica la comunicación, se puede observar que tiene ping y el agente responde perfectamente.

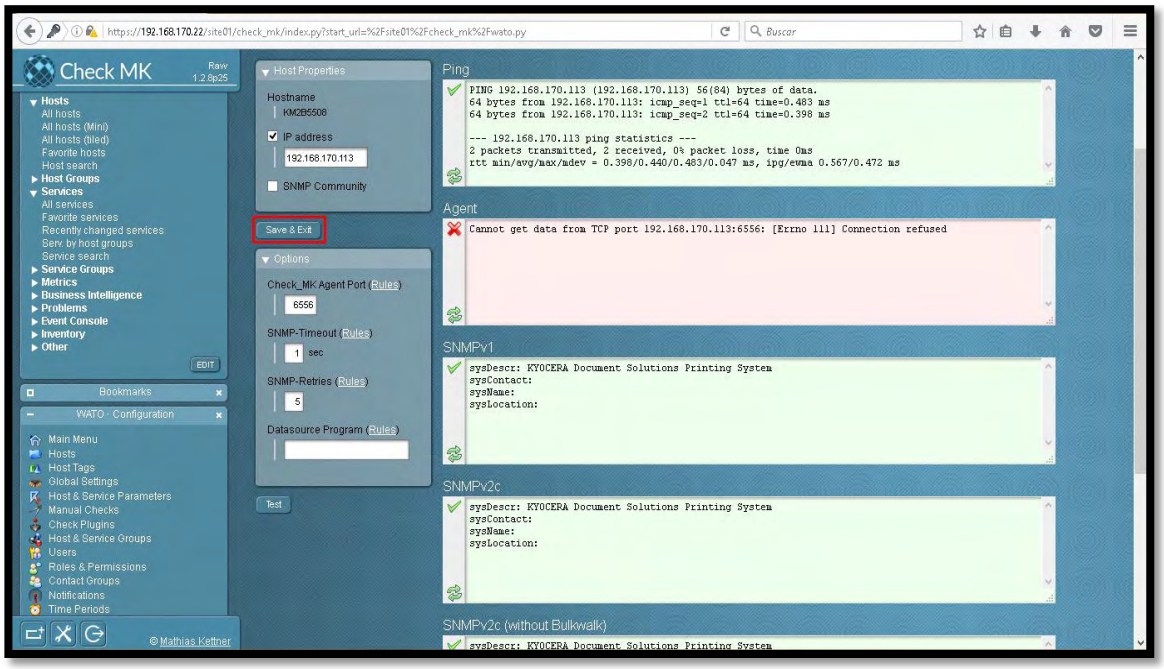


Figura DI 4. Plataforma de administración WATO, creación de impresora.

Una vez definido el nuevo host, se da en la opción “save & go to services” para mirar el estado de los servicios que seran monitoredos en esta máquina.

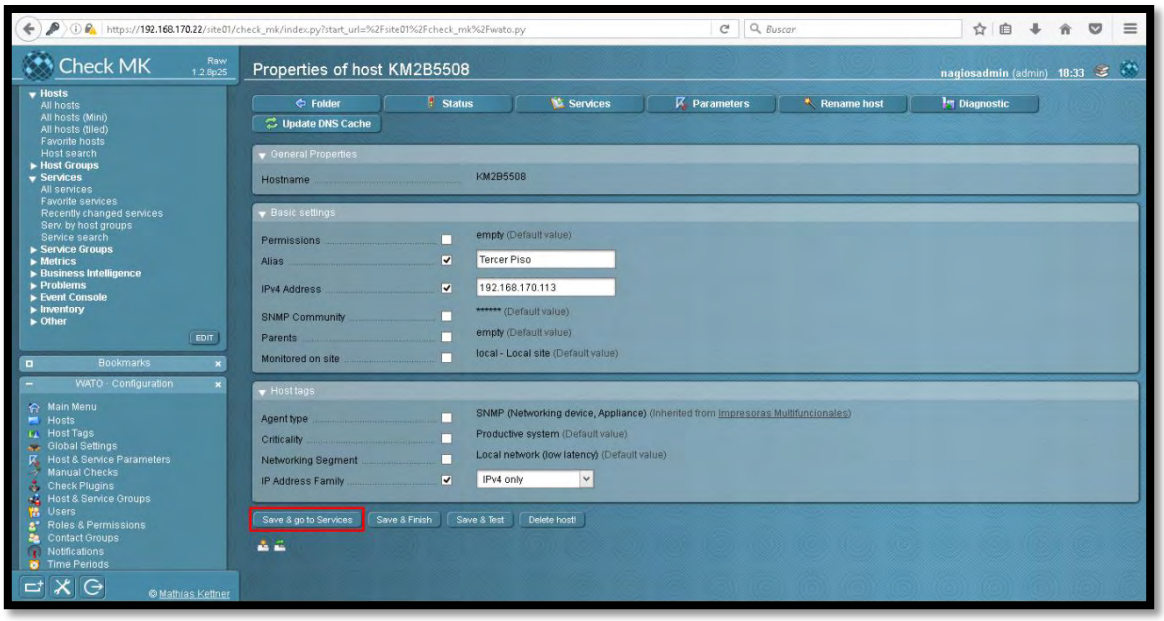


Figura DI 5. Plataforma de administración WATO, creación de impresora.

En seguida, se observa el estado de los servicios, luego se guarda de forma manual la configuración.

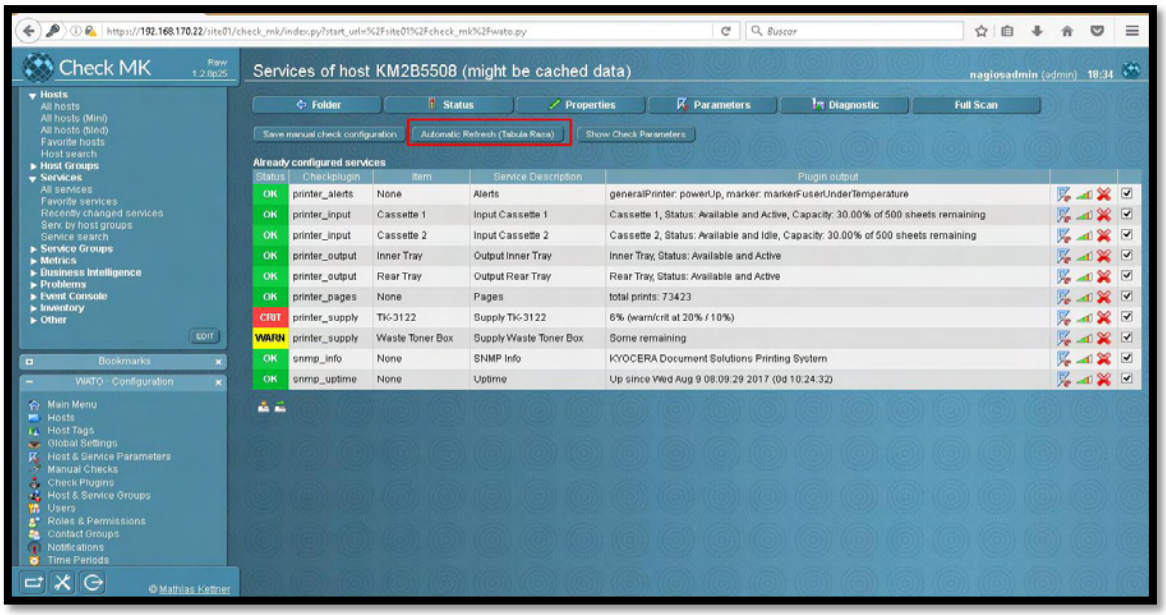


Figura DI 6. Plataforma de administración WATO, creación de impresora.

Se guardan los cambios realizados. Se observa que el nuevo host ya se encuentra definido.

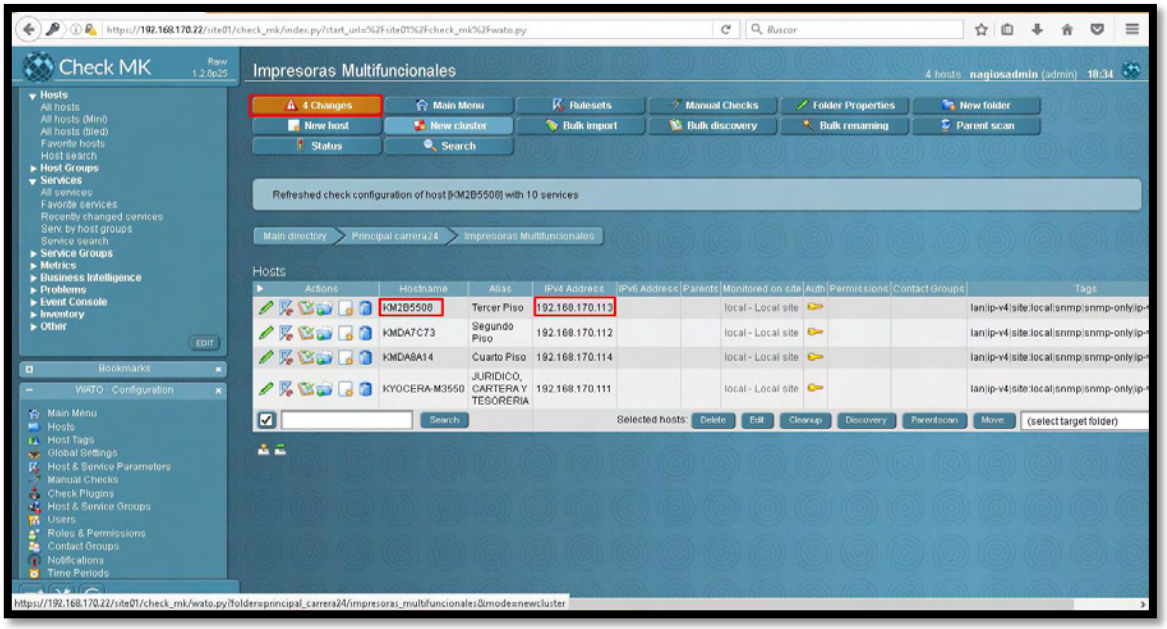


Figura DI 7. Plataforma de administración WATO, creación de impresora.

Posteriormente, se activan los cambios.

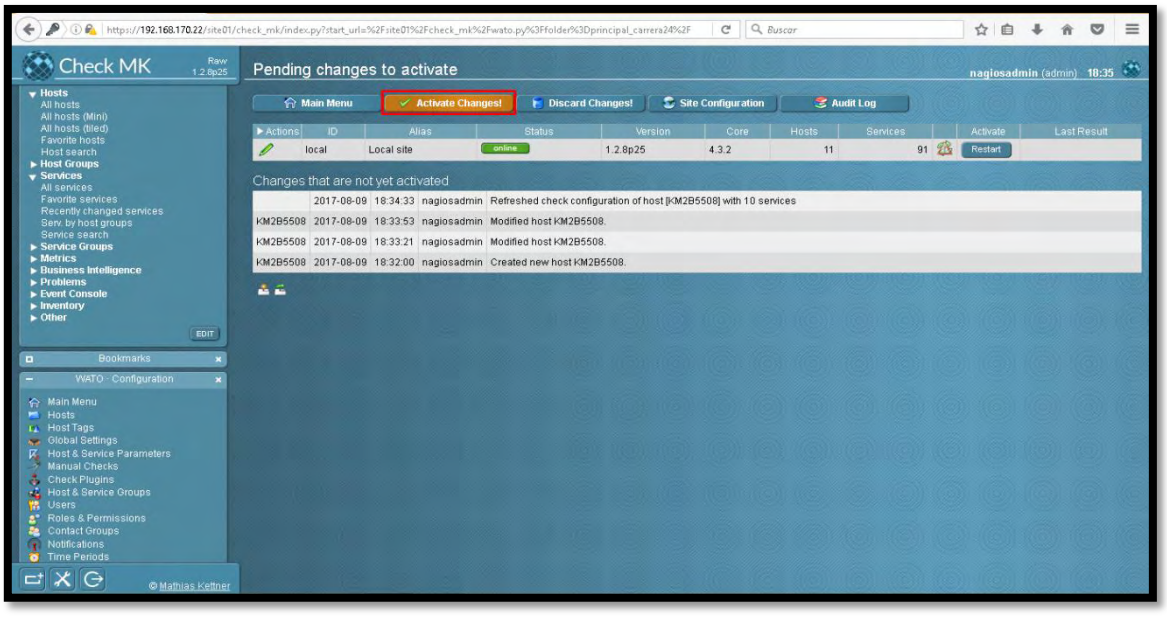


Figura DI 8. Plataforma de administración WATO, creación de impresora.

Por último, se verifica que la nueva configuración se realizó satisfactoriamente. Luego se puede detallar la información del monitoreo de la impreora creada en el panel de check_mk

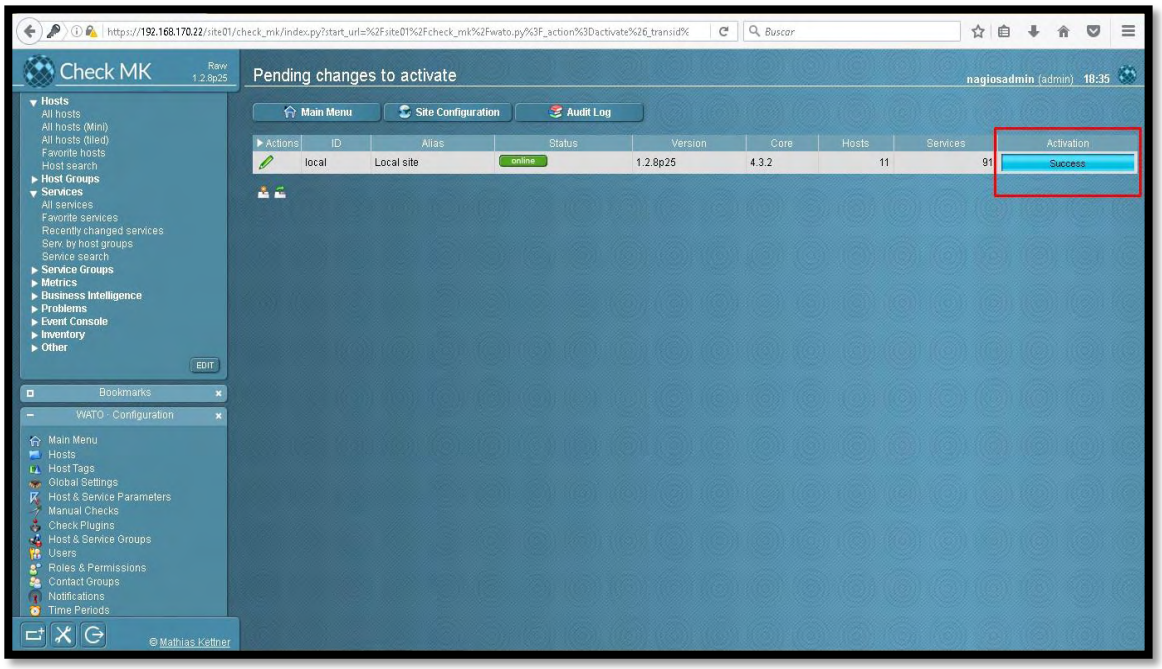


Figura DI 9. Plataforma de administración WATO, creación de impresora.

Definición de radioenlaces: todas las configuraciones de monitoreo en la plataforma de administración check_mk se realizan en el panel WATO configuration.

En primer lugar, se selecciona la opción Hosts:

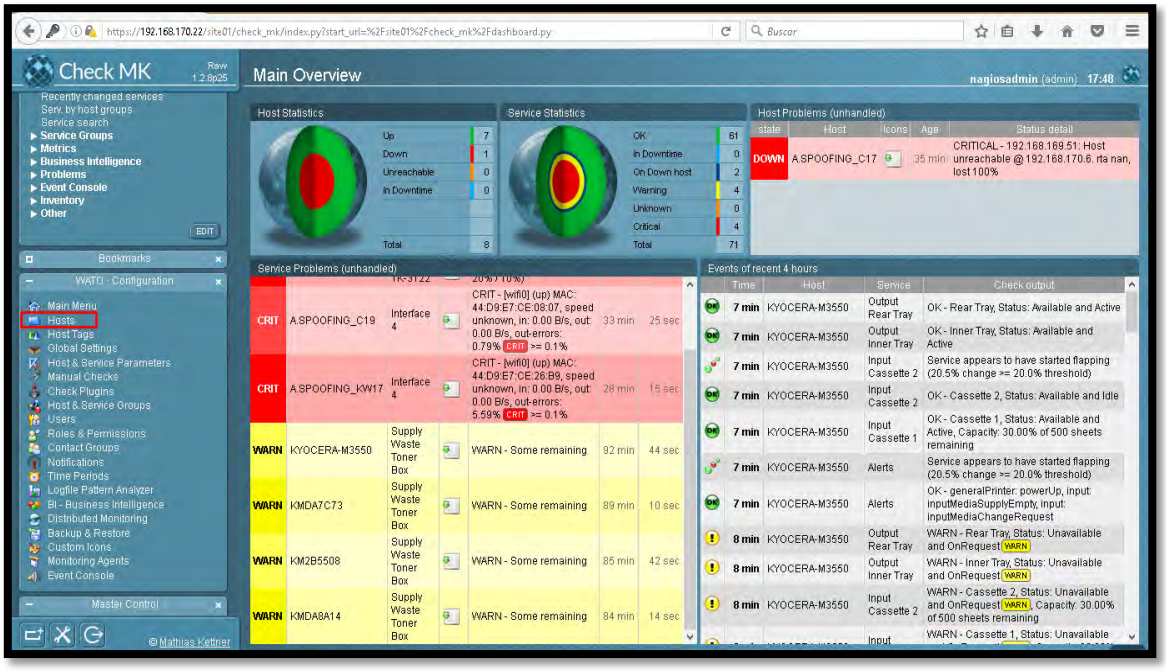


Figura DRE 1. Plataforma de administración WATO, creación de radio enlace.

Luego, se selecciona la opción New host, el nuevo host se creará en la ubicación que se desee.

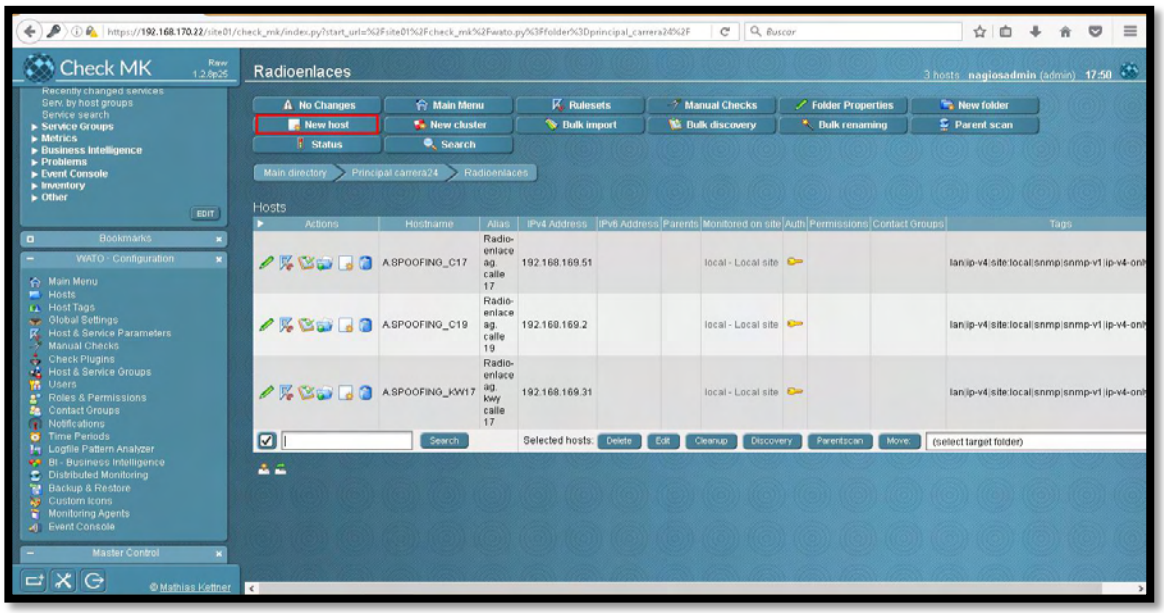


Figura DRE 2. Plataforma de administración WATO, creación de radio enlace.

En seguida, se completa la información requerida del host a crear, algo a tener en cuenta es el tipo de agente a utilizar. Para el caso de Los routers, switches

administrables y radioenlaces se utiliza el agente Legacy SNMP device (Using V1), dependiendo de la versión de SNMP que soporte el dispositivo a monitorear.

Se guarda la información y se realiza un test para verificar la comunicación de la maquina cliente con el servidor mediante el agente.

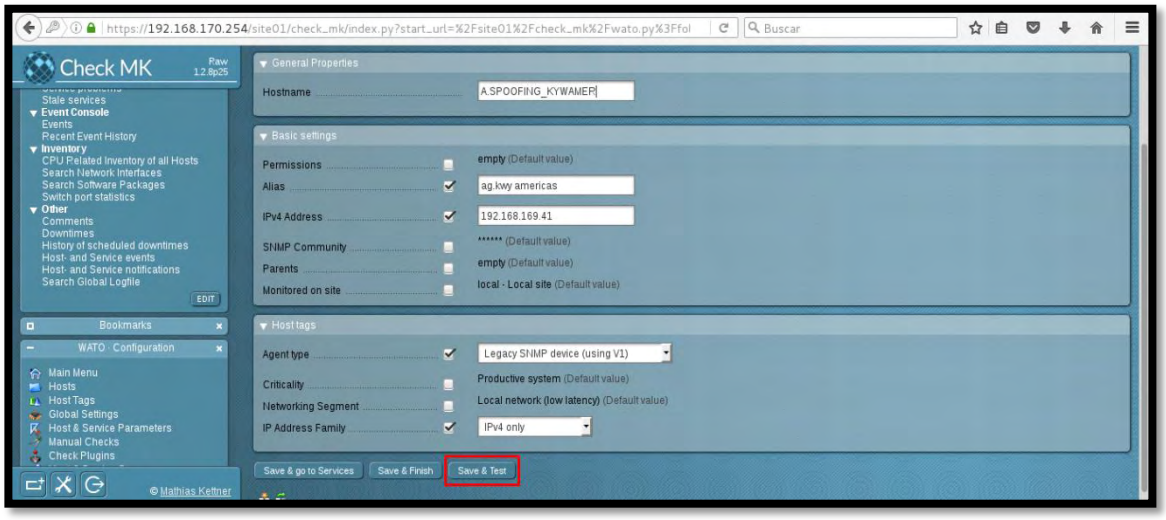


Figura DRE 3. Plataforma de administración WATO, creación de radio enlace.

Posteriormente, se verifica la comunicación, se puede observar que tiene ping y el agente responde perfectamente.

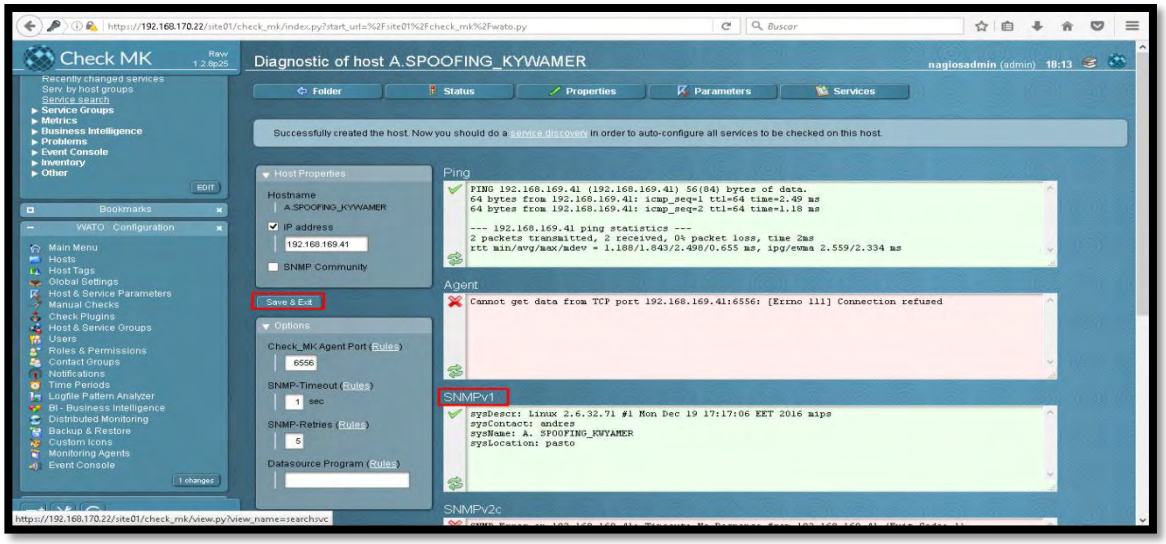


Figura DRE 4. Plataforma de administración WATO, creación de radio enlace.
Una vez definido el nuevo host se da en la opción “save & go to services” para ver el estado de los servicios que seran monitoredos en esta maquina.

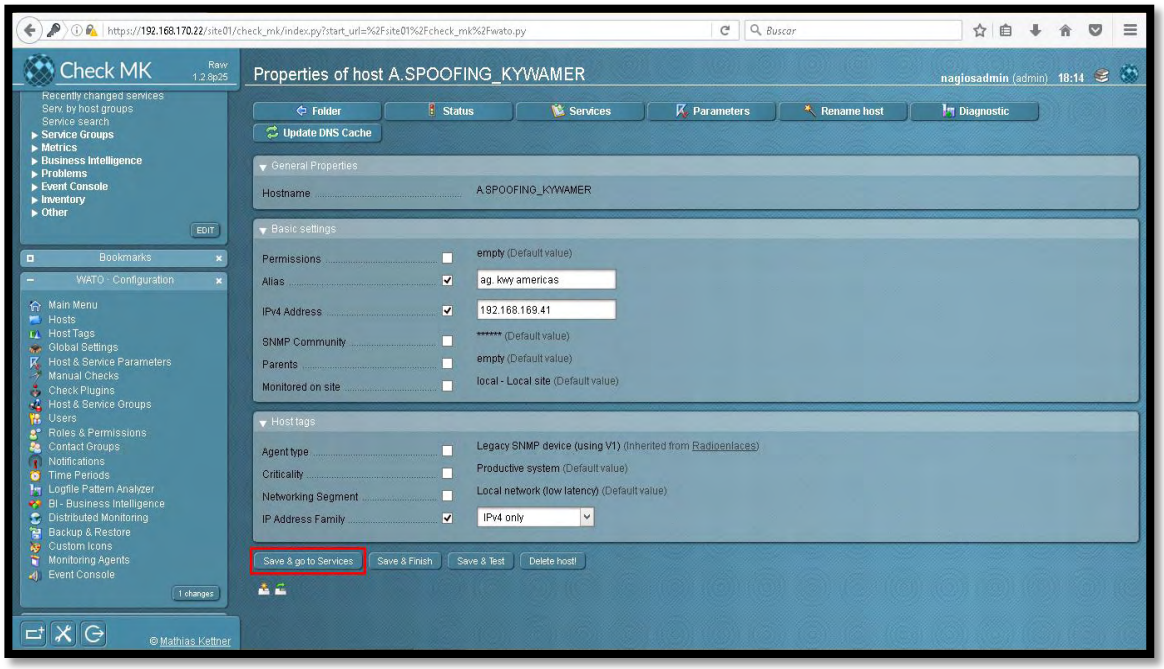


Figura DRE 5. Plataforma de administración WATO, creación de radio enlace.

Se observa el estado de los servicios, luego se guarda de forma manual la configuración.

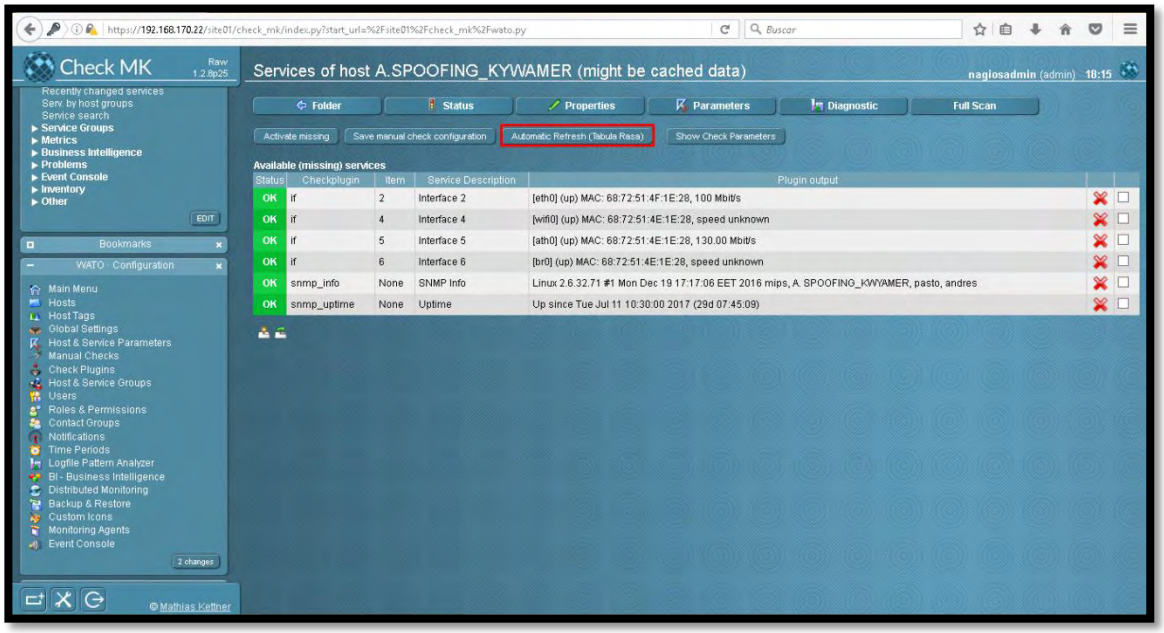


Figura DRE 6. Plataforma de administración WATO, creación de radio enlace.

Luego, se guardan los cambios realizados. Se observa que el nuevo host ya se encuentra definido.

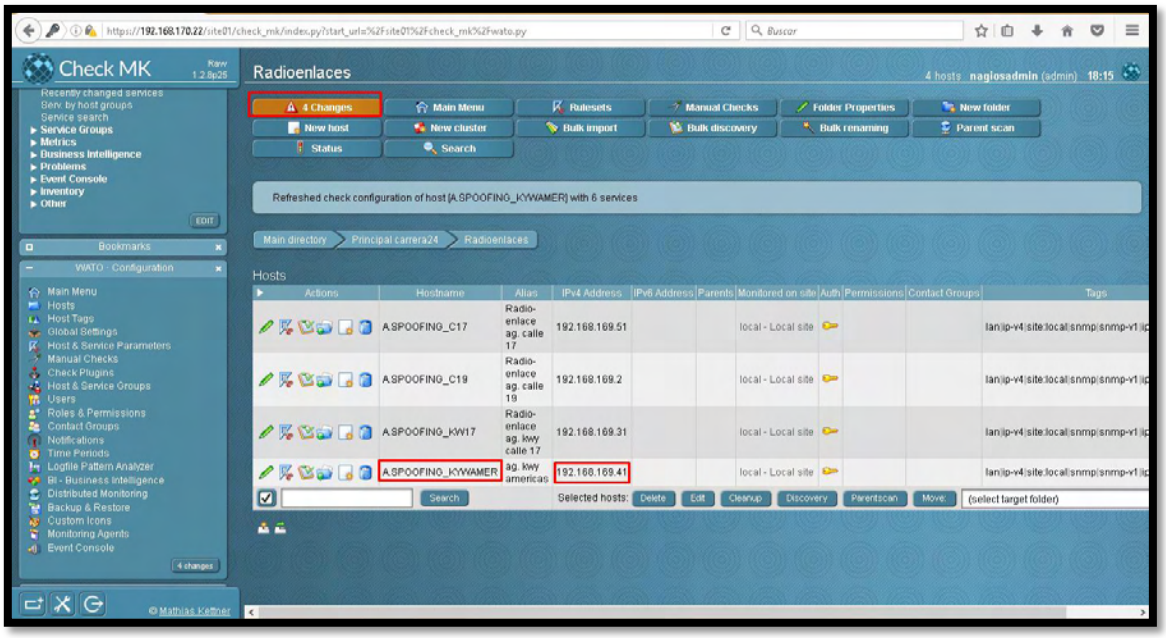


Figura DRE 7. Plataforma de administración WATO, creación de radio enlace.

En seguida, se activan los cambios.

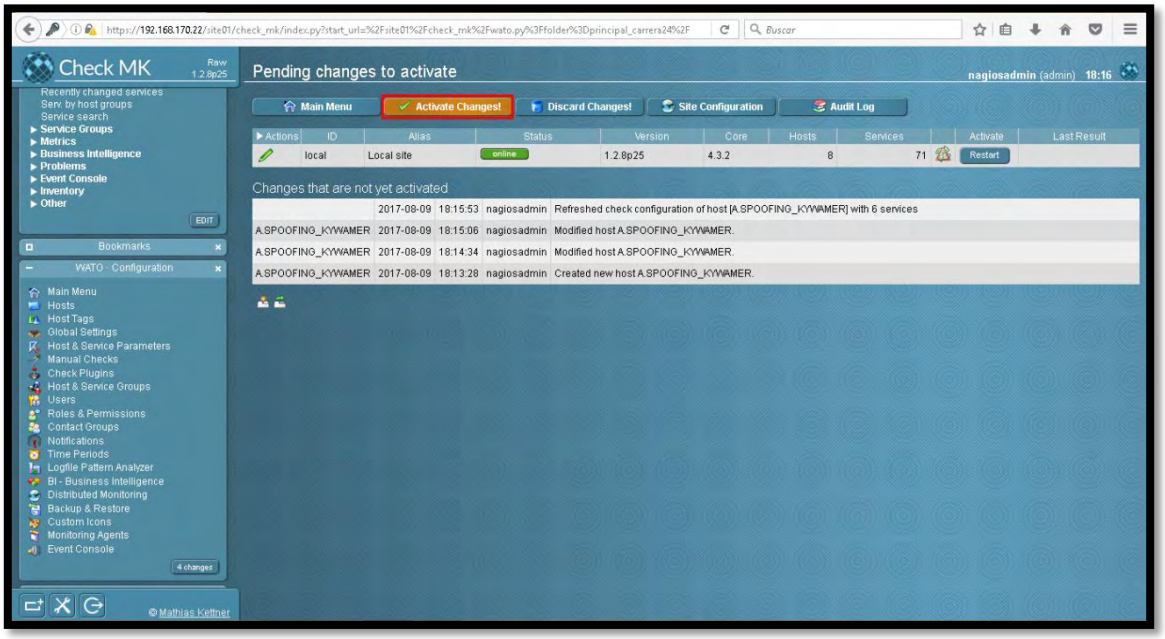


Figura DRE 8. Plataforma de administración WATO, creación de radio enlace.

Por último, se verifica que la nueva configuración se realizó satisfactoriamente. Luego se puede detallar la información del monitoreo del radio enlace creado en el panel de check_mk.

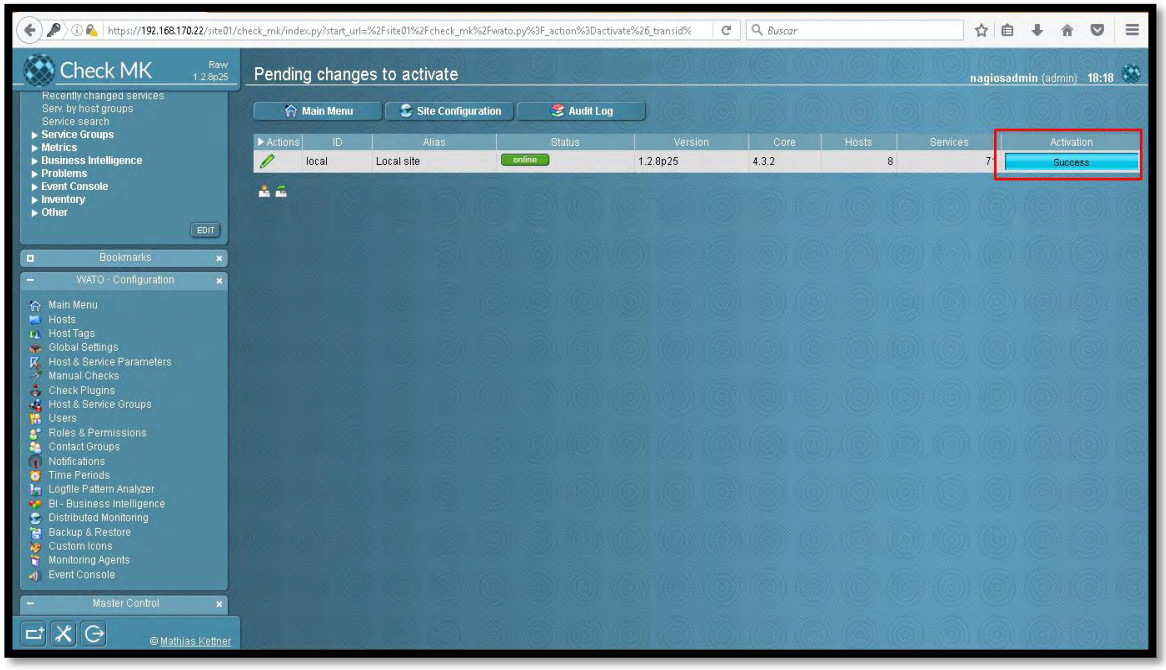


Figura DRE 9. Plataforma de administración WATO, creación de radio enlace.

Monitoreo de servicios de red: los servicios de red de la empresa fueron monitoreados a través de Nagios, debido a que es un sistema que cuenta con diversidad de plugins para monitorear servicios, los cuales vienen por defecto en su instalación. Además, se pueden instalar plugins tomados de Internet o se pueden programar plugins específicos para nuevos sistemas o servicios. Se recomienda monitorear servicios de red con Nagios.

Nagios describe dos clases de servicios, públicos y privados, el primero lo describe como aquellos que se pueden acceder a través de la red, puede ser de la red local o de Internet. Como ejemplo de servicios públicos incluyen, HTTP, SSH, FTP, DNS, entre otros muchos.

Los servicios privados, a diferencia de los públicos, no pueden ser monitoreados por Nagios sin un agente intermediario. Algunos ejemplos de servicios privados asociados a hosts están la carga de la CPU, uso de memoria, uso de disco, velocidad de tarjeta de red, entre otros. Estos servicios no están disponibles a clientes externos, por tal motivo si se pretende llevar un monitoreo de estos, es necesario que haya un intermediario (agente de supervisión), que esté pendiente del estado de dichos servicios.

Dentro de la empresa, los servicios privados de equipos de cómputo, computadores portátiles y de escritorio, se monitorean a través de un agente llamado check_mk y routers e impresoras de red se hacen a través un agente snmp.

Por el contrario, los servicios públicos se monitorean a través de Nagios sin ningún requisito de acceso especial, se realizan mediante plugins (complementos) de Nagios.

Para ahondar en cuanto a la configuración y definición de servicios públicos y privados únicamente detro de Nagios mirar el

Anexo L. Dedifinición de servicios públicos y privados en Nagios.

Georeferenciación y mapeo con Nagvis: al momento de instalar Nagvis este contiene varios mapas de demostración en la instalación inicial. Tambien se encuentra un mosaico de los principales mapas, el cual Nagvis lo denomina Rotation pools, en donde se encuentran los principales mapas, tanto físicos como geográficos de la red de demostración en la instalación inicial. Tanto los mapas de demostración como los Rotation pools se pueden eliminar a conveniencia.

Nagvis hace uso de diferentes vistas llamadas “mapas” entre los que se encuentran están:

- Nagvis Automaps: esta función permite reemplazar el mapa incorporado en Nagios, el problema principal de este mapa es que no es escalable, es decir, que en grandes instalaciones en Nagios, la función automap no es utilizable.

- Nagvis Worldmaps: NagVis Worldmap se introdujo en NagVis 1.9. Ha sido desarrollado para hacer posible la creación de mapas geográficos modernos e interactivos. Puede poner cualquier tipo de objeto NagVis en un mapa del mundo que luego se representa utilizando Open Street Map.

  La diferencia de estos mapas con los clásicos es que los mapas del mundo únicos no tienen un conjunto dedicado de objetos de mapa. De hecho, un mapa del mundo es principalmente la definición de una ventana gráfica (área visible, zoom) en el mundo. Cada objeto que se coloca en un mapa del mundo se guarda globalmente en todos los mapas del mundo. Esto significa que si agrega un objeto a un mapa del mundo en un zoom alto (nivel de detalle), el objeto también se agrega a los mapas del mundo que muestran toda la tierra. Los desarrolladores de Nagvis lo hicieron así, suponiendo que cada objeto geográficamente ubicado tiene una posición única en todos los mapas.

- Nagvis Geomaps: Se introdujo en NagVis 1.7. Ha sido desarrollado para obtener mapas generales bien renderizados y escalados sin mucho trabajo.

  El geomap representa varios hosts en un mapa habilitado de Open Street Map que se utiliza como imagen de fondo.

  Para el geomap actual, todo lo que necesita es un archivo CSV que le indique a NagVis los hosts que debe representar y las coordenadas geográficas donde deben ubicarse los hosts.

  A diferencia de NagVis Worldmaps, que se han introducido con NagVis 1.9, los geomaps están diseñados para ser mapas estáticos sin interacción del

usuario. No puede acercar / alejar y desplazarse como se puede en los mapas del mundo.

- Nagvis Dynamic Maps: este tipo de mapas se introdujeron en NagVis 1.8. Fue creado para facilitar la creación de mapas esquemáticos que contienen tipos de objetos iguales.

  Por ejemplo, al tener un solo mapa que contenga varios objetos host, quizás todos los hosts cuyo nombre comience con un prefijo definido por ejemplo *electro_*. Sin los mapas dinámicos, siempre deberá agregar un objeto host al mapa si se agrega un nuevo host al monitoreo y también es eliminado si se eliminan algunos de esos hosts.

  Al usar los mapas dinámicos, se puede calcular sus definiciones de reglas una vez y cada vez que cambia la configuración de monitoreo, el mapa se verifica si es necesario agregar, eliminar o reubicar algún host.

En el presente trabajo se hizo uso únicamente de las funciones Nagvis Worldmaps y Nagvis Dynamic Maps.

Para profundizar en cuanto a georeferenciacion y mapeo mirar dirigirse a la docuementación oficial de Nagvis.

9.8.4 Pruebas de funcionamiento de la suite de monitoreo. Se hace una prueba de funcionamiento de la suite de monitoreo dentro de la empresa, haciendo una demostración con las opciones más importantes al momento de visualizar resultados, las opciones en cada herramienta son las siguientes:

Con Nagios se visualiza el estado de todos los hosts, mapa de los host y grupos de host. Con Check_mk se visualiza el estado de los servicios por cada host, grupos de host, y monitoreo de los servidores azkaban y voldemort donde se monitorean los servicios de red. Con Nagvis se visualiza el geomapa regional, los geomapas de Pasto, Popayán, Tumaco, Yumbo, Cali y Mocoa, y se muestra el estado del host colocando el puntero en los iconos que representan los componentes de red en los diagramas lógicos anexados en Nagvis. Con Pnp4Nagios es observa un resumen gráfico de monitoreo. Además, se muestra como se reciben las notificaciones por email.

Se puede visualizar la prueba de funcionamiento en el

Anexo M. Funcionamiento de suite de monitoreo.

9.8.5 Reportes de monitoreo con Nagios. Nagios puede generar reportes a partir de eventos que se generan de los estados de los equipos monitoreados.

En la interface gráfica de Nagios existe un apartado Reports “Reportes” en la que se pueden generar diferentes tipos de reportes según la necesidad del administrador de la red.

Existen cinco apartados dentro del menú de reportes, los cuales son:

1. Availability

2. Trends

3. Alerts

- Alert History
- Alert Summary
- Alert Histogram

4. Notifications

5. Event Log

Se especificará con mayor detalle la creación de reportes del apartado uno (1) Availabity, ya que facilita el análisis de los resultados entregados. Los demás apartados serán conceptualizados.

Nota: los reportes generados a continuación fueron durante el mes de enero de 2018, tiempo en el cual Nagios tuvo un trabajo ininterrumpido.

Availability: el reporte de Availability (disponibilidad), proporciona el tiempo de actividad histórico para hosts y servicios. Esto es útil para determinar los requisitos y el cumplimiento de que los servidores y aplicaciones estén en línea y funcionen correctamente en un porcentaje de tiempo.

Para la generación de estos reportes se debe dirigir a la página principal de Nagios, una vez en ella se debe dirigir al menú lateral izquierdo y en *Reports* damos clic sobre *Availability.*

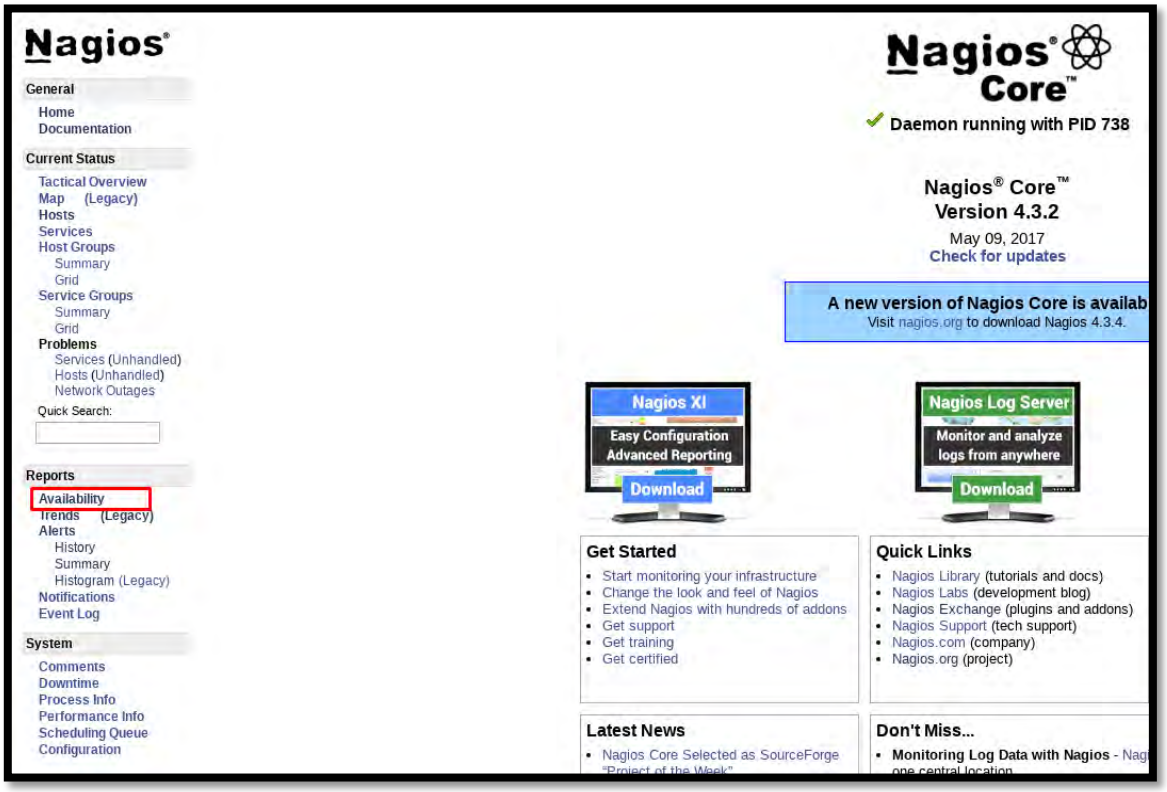


Figura CR 1. Creación de reportes de disponibilidad en Nagios.

- Reportes por hostgroups

Este tipo de reportes son generedos a partir de los grupos de equipos que fueron creados en check_MK.

Se selecciona la opcion **Hostgroup(s).**



Figura CR 2. Creación de reportes de disponibilidad en Nagios.

Enseguida se selecciona la opción **ALL HOSTGROUPS.**



Figura CR 3. Creación de reportes de disponibilidad en Nagios.

Luego, se escoge los parámetros que se ajustaran al reporte, y se lo genera.

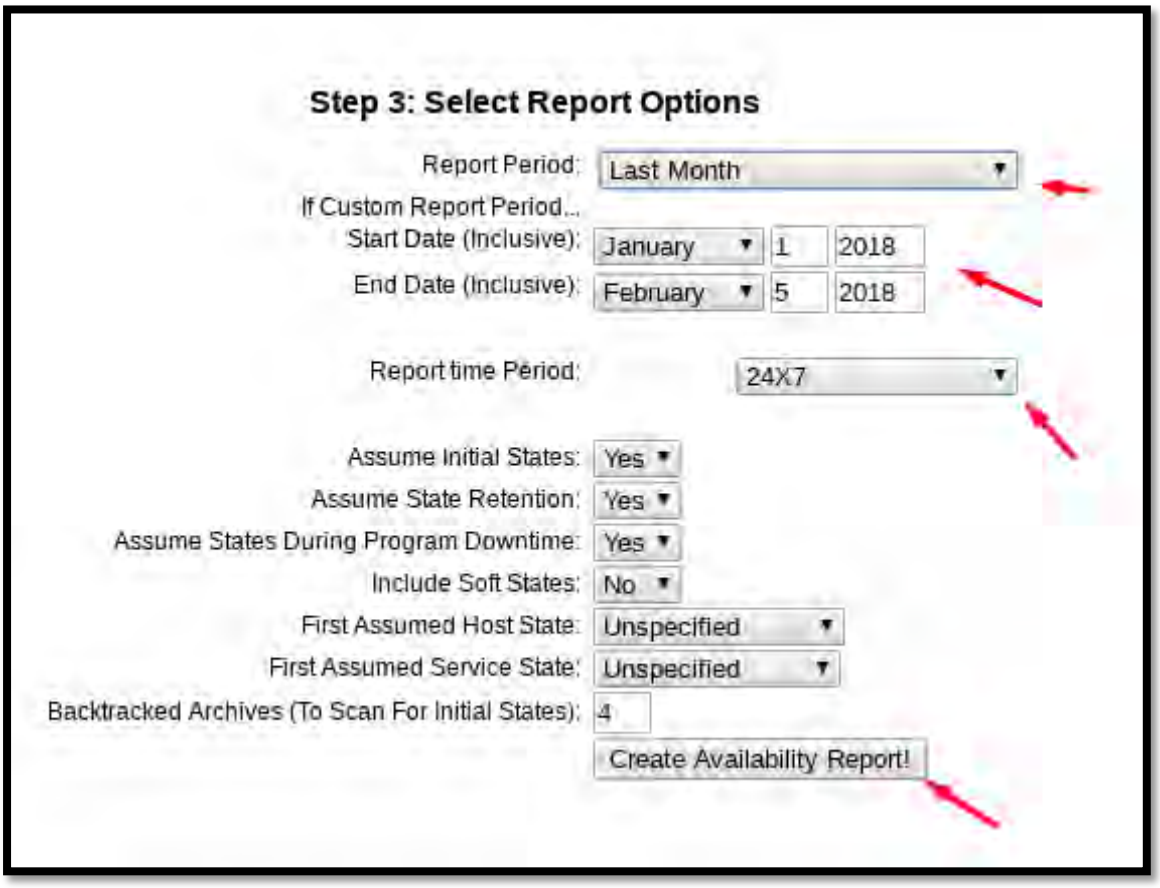
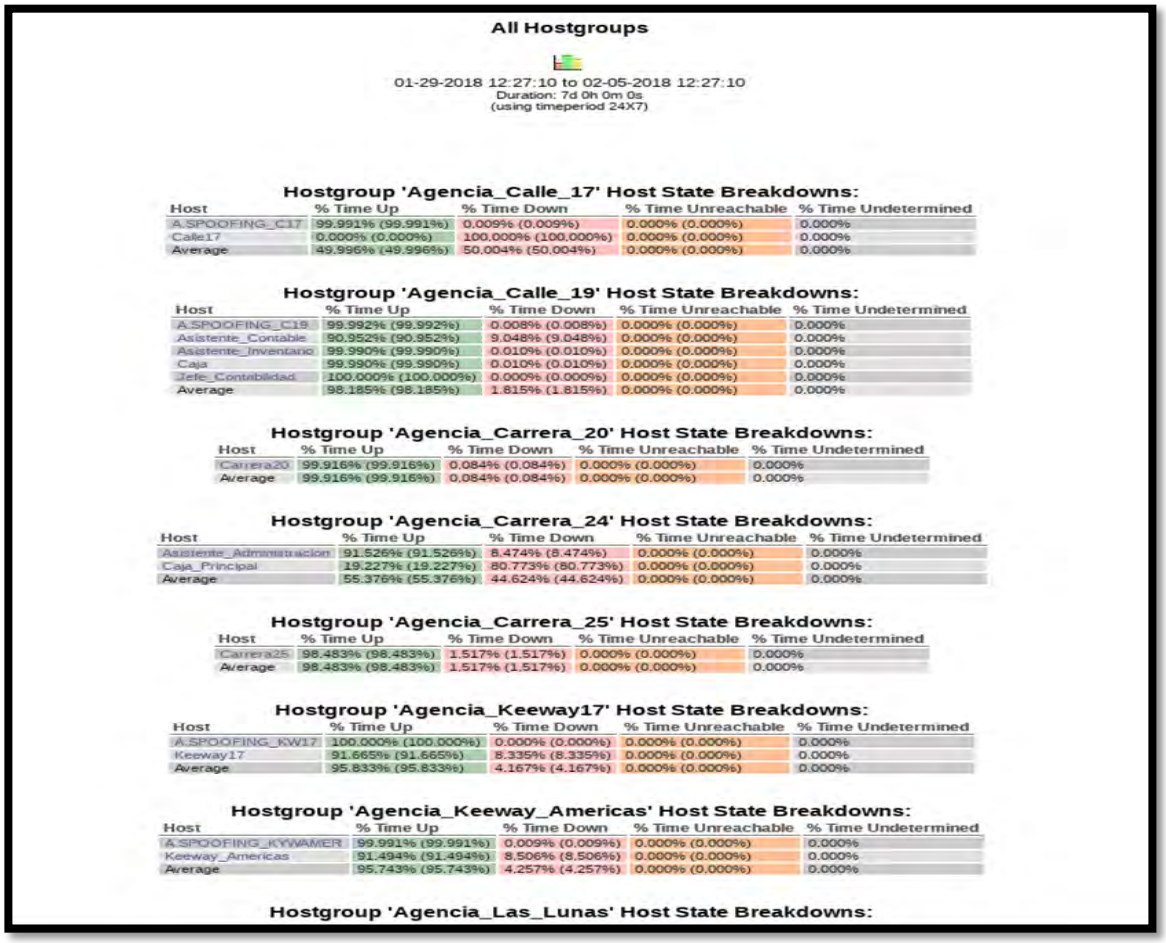


Figura CR 4. Creación de reportes de disponibilidad en Nagios.

Por último, el reporte de disponibilidad es visible en una página web, en donde muestra en forma discriminada por grupos de equipos, el porcentaje de tiempo durante un mes del funcionamiento.

El reporte completo se puede observar en el Anexo N. Resultados de reporte Nagios Availability Host Groups.



All Hostgroups

01-29-2018 12:27:10 to 02-05-2018 12:27:10
Duration: 7d 0h 0m 0s
(using timeperiod 24X7)

Hostgroup 'Agencia_Calle_17' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_C17	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
Calle17	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Average	49.996% (49.996%)	50.004% (50.004%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Calle_19' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_C19	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
Asistente_Contable	90.952% (90.952%)	9.048% (9.048%)	0.000% (0.000%)	0.000%
Asistente_Inventario	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Caja	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Jefe_Contabilidad	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	98.185% (98.185%)	1.815% (1.815%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Carrera_20' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Carrera20	99.916% (99.916%)	0.084% (0.084%)	0.000% (0.000%)	0.000%
Average	99.916% (99.916%)	0.084% (0.084%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Carrera_24' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Asistente_Administracion	91.526% (91.526%)	8.474% (8.474%)	0.000% (0.000%)	0.000%
Caja_Principal	19.227% (19.227%)	80.773% (80.773%)	0.000% (0.000%)	0.000%
Average	55.376% (55.376%)	44.624% (44.624%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Carrera_25' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Carrera25	98.483% (98.483%)	1.517% (1.517%)	0.000% (0.000%)	0.000%
Average	98.483% (98.483%)	1.517% (1.517%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Keeway17' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_KW17	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Keeway17	91.665% (91.665%)	8.335% (8.335%)	0.000% (0.000%)	0.000%
Average	95.833% (95.833%)	4.167% (4.167%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Keeway_Americas' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_KYWAMER	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
Keeway_Americas	91.494% (91.494%)	8.506% (8.506%)	0.000% (0.000%)	0.000%
Average	95.743% (95.743%)	4.257% (4.257%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Las_Lunas' Host State Breakdowns:

Figura CR 5. Creación de reportes de disponibilidad en Nagios.

- Reportes por host

Esto tipo de reportes son generedos a partir de cada uno de los equipos individuales creados en check_MK.

Se selecciona la opcion **Host(s)**.



Figura CR 6. Creación de reportes de disponibilidad en Nagios.

Enseguida, se selecciona la opción **ALL HOST**.



Figura CR 7. Creación de reportes de disponibilidad en Nagios.

Luego, se escoge los parámetros que se ajustaran al reporte, y se lo genera.

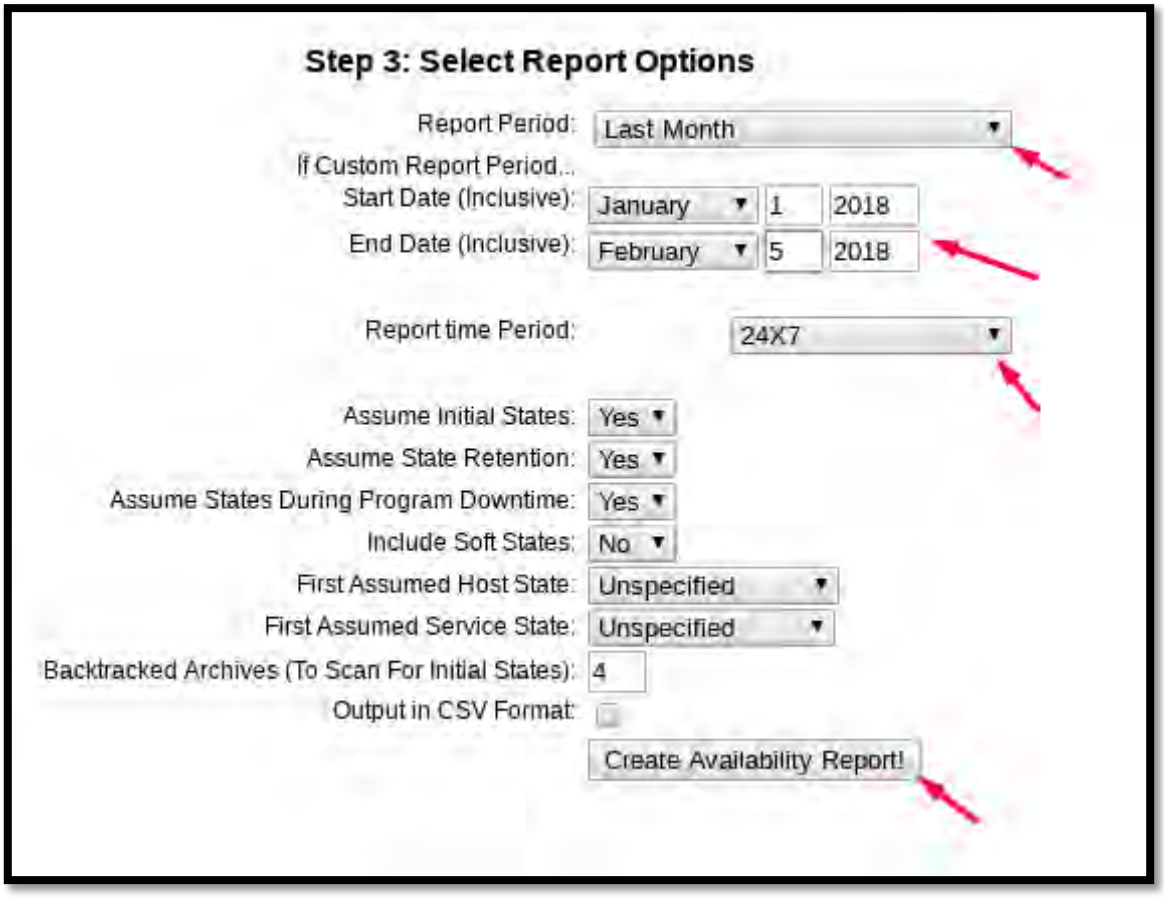
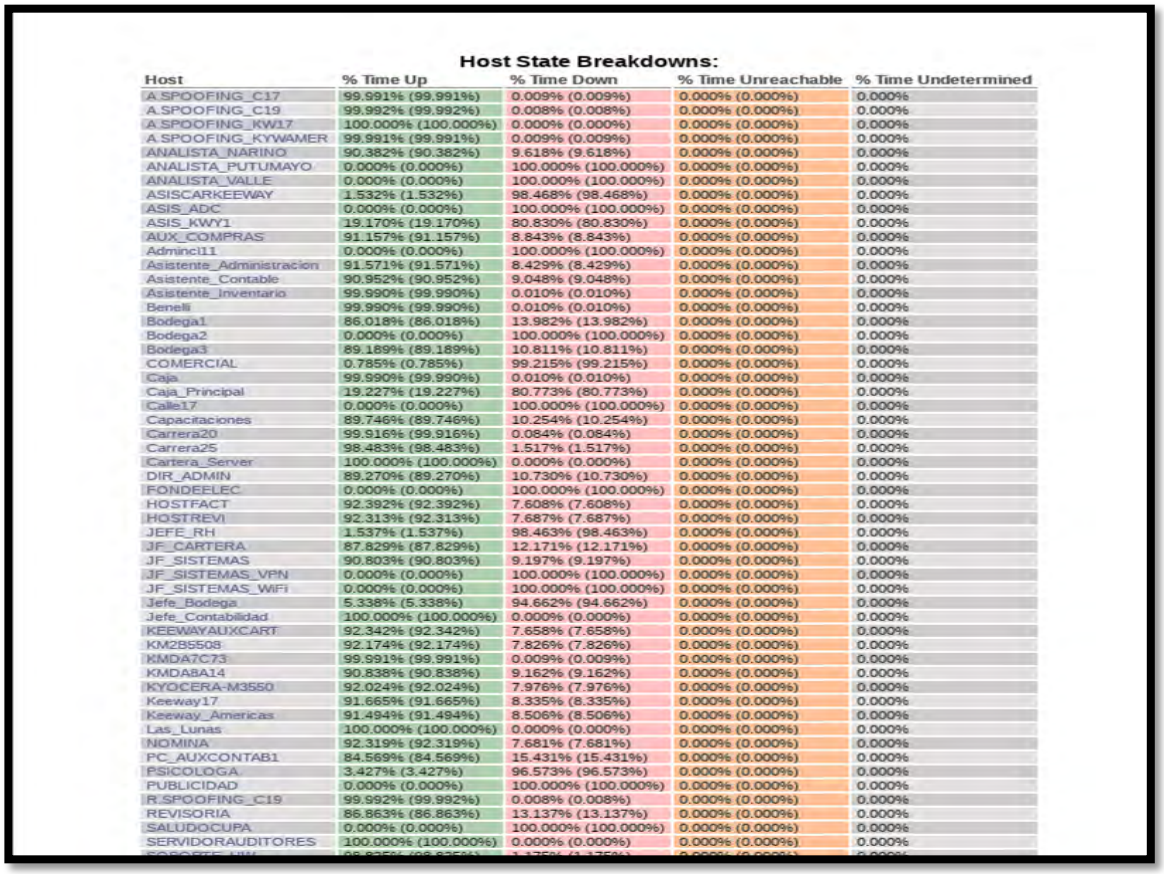


Figura CR 8. Creación de reportes de disponibilidad en Nagios.

El reporte de disponibilidad es visible en una página web, en donde muestra en forma discriminada por cada equipo, el porcentaje de tiempo durante un mes del funcionamiento.

El reporte completo se puede observar en el Anexo O. Resultados de reporte Nagios Availability Individual Host.



Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_C17	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
A.SPOOFING_C19	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
A.SPOOFING_KW17	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
A.SPOOFING_KYWAMER	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
ANALISTA_NARINO	90.382% (90.382%)	9.618% (9.618%)	0.000% (0.000%)	0.000%
ANALISTA_PUTUMAYO	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
ANALISTA_VALLE	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
ASISCARKEEWAY	1.532% (1.532%)	98.468% (98.468%)	0.000% (0.000%)	0.000%
ASIS_ADC	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
ASIS_KWY1	19.170% (19.170%)	80.830% (80.830%)	0.000% (0.000%)	0.000%
AUX_COMPRAS	91.157% (91.157%)	8.843% (8.843%)	0.000% (0.000%)	0.000%
Admincl11	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Asistente_Administracion	91.571% (91.571%)	8.429% (8.429%)	0.000% (0.000%)	0.000%
Asistente_Contable	90.952% (90.952%)	9.048% (9.048%)	0.000% (0.000%)	0.000%
Asistente_Inventario	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Benelli	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Bodega1	86.018% (86.018%)	13.982% (13.982%)	0.000% (0.000%)	0.000%
Bodega2	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Bodega3	89.189% (89.189%)	10.811% (10.811%)	0.000% (0.000%)	0.000%
COMERCIAL	0.785% (0.785%)	99.215% (99.215%)	0.000% (0.000%)	0.000%
Caja	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Caja_Principal	19.227% (19.227%)	80.773% (80.773%)	0.000% (0.000%)	0.000%
Calle17	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Capacitaciones	89.746% (89.746%)	10.254% (10.254%)	0.000% (0.000%)	0.000%
Carrera20	99.916% (99.916%)	0.084% (0.084%)	0.000% (0.000%)	0.000%
Carrera25	98.483% (98.483%)	1.517% (1.517%)	0.000% (0.000%)	0.000%
Cartera_Server	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
DIR_ADMIN	89.270% (89.270%)	10.730% (10.730%)	0.000% (0.000%)	0.000%
FONDEELEC	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
HOSTFACT	92.392% (92.392%)	7.608% (7.608%)	0.000% (0.000%)	0.000%
HOSTREVI	92.313% (92.313%)	7.687% (7.687%)	0.000% (0.000%)	0.000%
JEFE_RH	1.537% (1.537%)	98.463% (98.463%)	0.000% (0.000%)	0.000%
JF_CARTERA	87.829% (87.829%)	12.171% (12.171%)	0.000% (0.000%)	0.000%
JF_SISTEMAS	90.803% (90.803%)	9.197% (9.197%)	0.000% (0.000%)	0.000%
JF_SISTEMAS_VPN	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
JF_SISTEMAS_WIFI	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Jefe_Bodega	5.338% (5.338%)	94.662% (94.662%)	0.000% (0.000%)	0.000%
Jefe_Contabilidad	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
KEEWAYAUXCART	92.342% (92.342%)	7.658% (7.658%)	0.000% (0.000%)	0.000%
KM285508	92.174% (92.174%)	7.826% (7.826%)	0.000% (0.000%)	0.000%
KMDA7C73	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
KMDABA14	90.838% (90.838%)	9.162% (9.162%)	0.000% (0.000%)	0.000%
KYOCERA-M3550	92.024% (92.024%)	7.976% (7.976%)	0.000% (0.000%)	0.000%
Keeway17	91.665% (91.665%)	8.335% (8.335%)	0.000% (0.000%)	0.000%
Keeway_Americas	91.494% (91.494%)	8.506% (8.506%)	0.000% (0.000%)	0.000%
Las_Lunas	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
NOMINA	92.319% (92.319%)	7.681% (7.681%)	0.000% (0.000%)	0.000%
PC_AUXCONTAB1	84.569% (84.569%)	15.431% (15.431%)	0.000% (0.000%)	0.000%
PSICOLOGA	3.427% (3.427%)	96.573% (96.573%)	0.000% (0.000%)	0.000%
PUBLICIDAD	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
R.SPOOFING_C19	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
REVISORIA	86.863% (86.863%)	13.137% (13.137%)	0.000% (0.000%)	0.000%
SALUDOCUPA	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
SERVIDORAUDITORES	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Figura CR 9. Creación de reportes de disponibilidad en Nagios.

Otra manera de generar el reporte es mediante un archivo en formato CSV, en el cual se muestra de forma mas detallada los estados de disponibilidad de cada uno de los equipos.

El archivo generado puede ser visto como Anexo P. Resultados de reporte en archivo .cvs avail individual all hots.

Se detallará un poco más sobre estos archivos mas adelante.

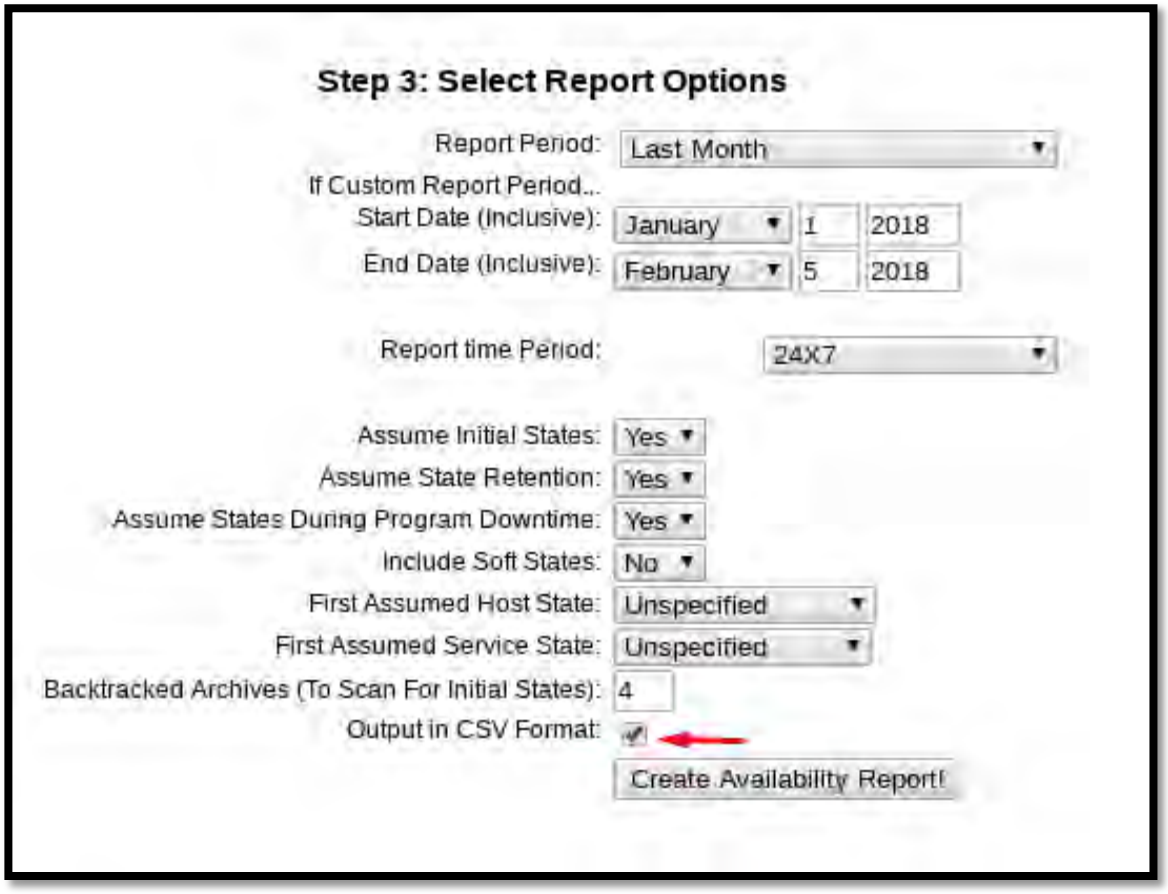


Figura CR 10. Creación de reportes de disponibilidad en Nagios.

- Reportes por servicios

Este tipo de reportes son generedos a partir de cada uno de los servicios definidos y configurados tanto en Nagios como en check_MK.

Se selecciona la opcion *Services(s).*



Figura CR 11. Creación de reportes de disponibilidad en Nagios.

Enseguida, se selecciona la opción *ALL SERVICES.*

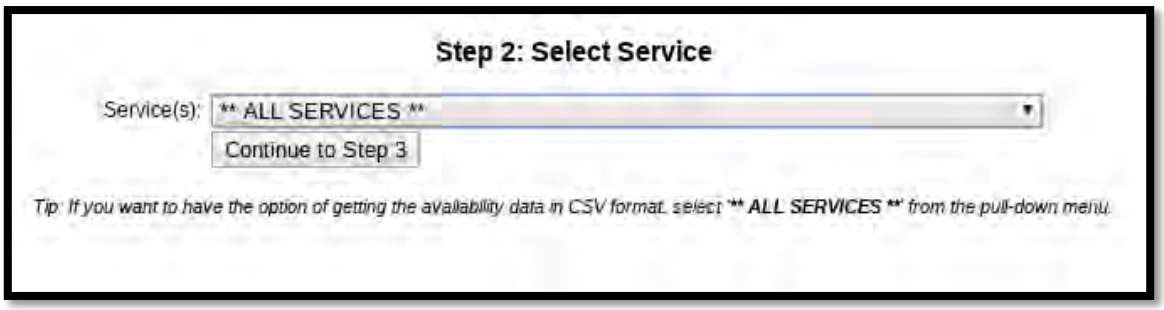


Figura CR 12. Creación de reportes de disponibilidad en Nagios.

Luego, se escoge los parámetros que se ajustaran al reporte, y se lo genera.

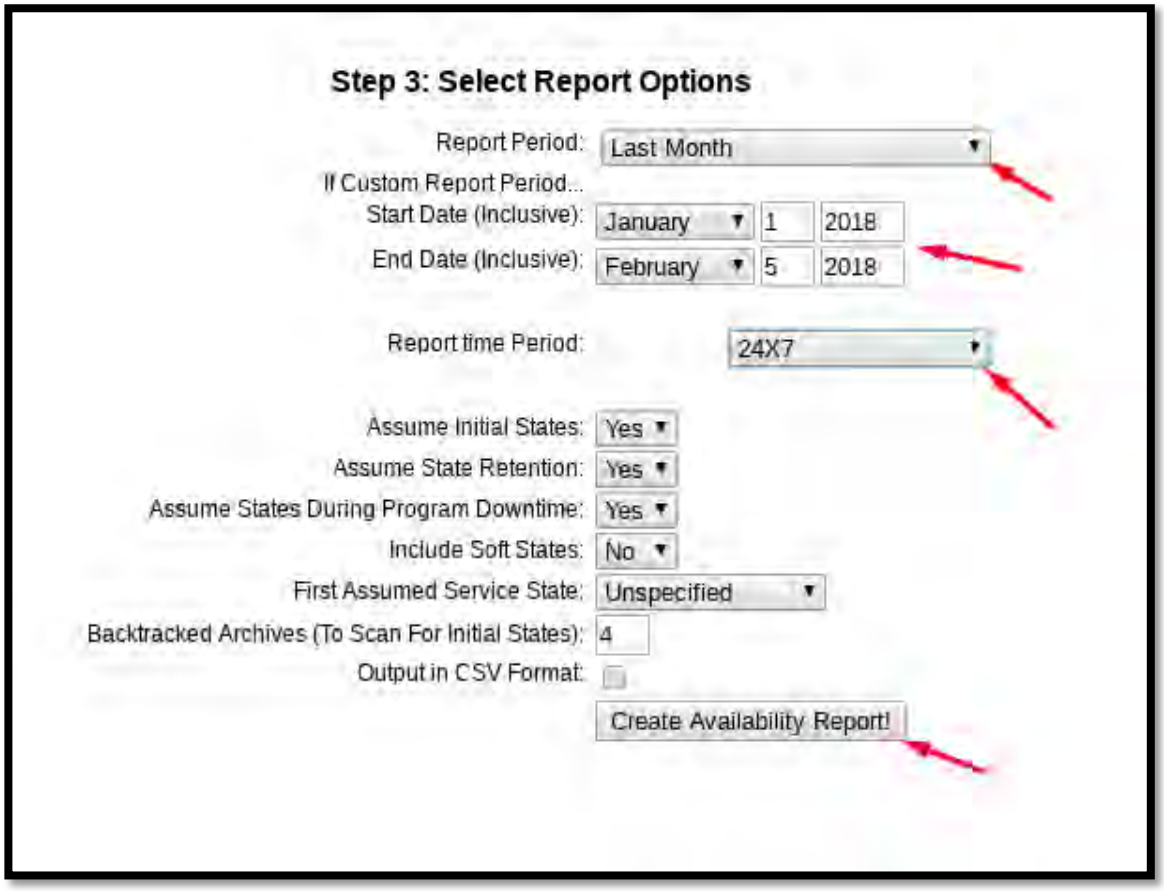
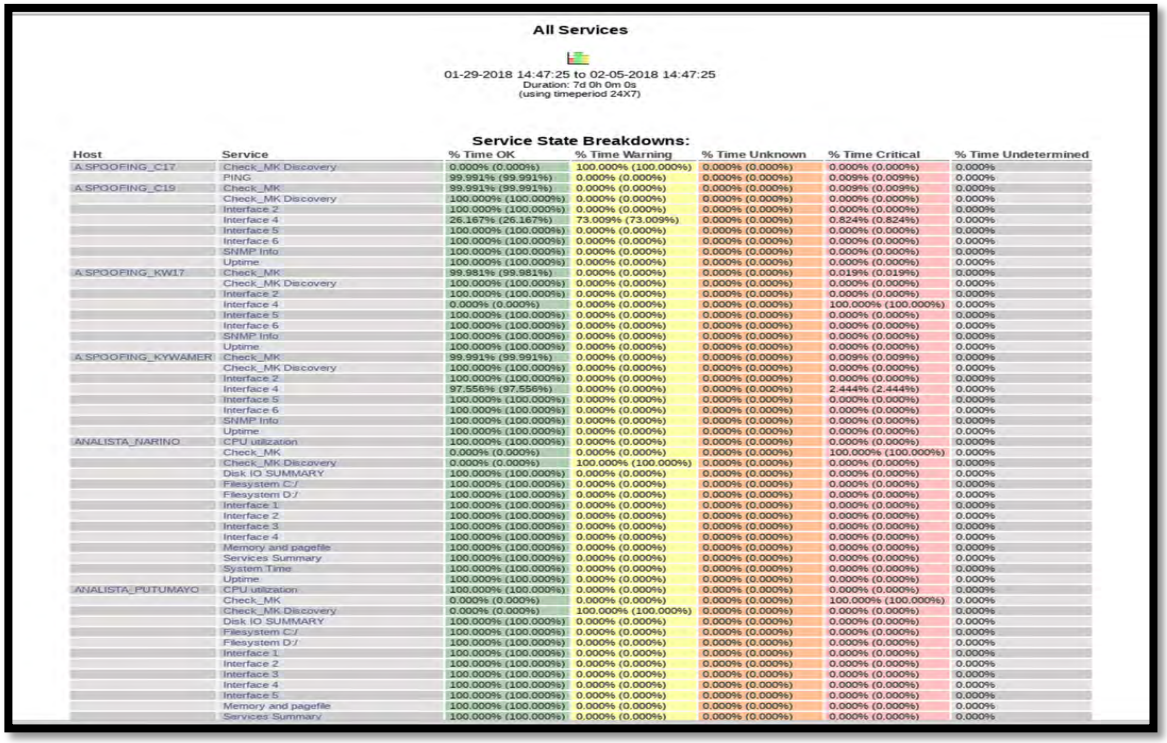


Figura CR 13. Creación de reportes de disponibilidad en Nagios.

El reporte de disponibilidad es visible en una página web, en donde muestra en forma discriminada por cada servicio, el porcentaje de tiempo durante un mes del funcionamiento.



All Services

01-29-2018 14:47:25 to 02-05-2018 14:47:25
Duration: 7d 0h 0m 0s
(using timeperiod 24X7)

Service State Breakdowns:

Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
A.SPOOFING_C17	Check_MK Discovery	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	PING	99.991% (99.991%)	0.000% (0.000%)	0.000% (0.000%)	0.009% (0.009%)	0.000%
A.SPOOFING_C19	Check_MK	99.991% (99.991%)	0.000% (0.000%)	0.000% (0.000%)	0.009% (0.009%)	0.000%
	Check_MK Discovery	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 4	26.167% (26.167%)	73.009% (73.009%)	0.000% (0.000%)	0.824% (0.824%)	0.000%
	Interface 5	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 6	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	SNMP Info	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Uptime	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
A.SPOOFING_KW17	Check_MK	99.981% (99.981%)	0.000% (0.000%)	0.000% (0.000%)	0.019% (0.019%)	0.000%
	Check_MK Discovery	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 4	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
	Interface 5	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 6	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	SNMP Info	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Uptime	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
A.SPOOFING_KYWAMER	Check_MK	99.991% (99.991%)	0.000% (0.000%)	0.000% (0.000%)	0.009% (0.009%)	0.000%
	Check_MK Discovery	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 4	97.556% (97.556%)	0.000% (0.000%)	0.000% (0.000%)	2.444% (2.444%)	0.000%
	Interface 5	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 6	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	SNMP Info	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Uptime	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
ANALISTA_NARIÑO	CPU utilization	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Check_MK	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
	Check_MK Discovery	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Disk IO SUMMARY	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Filesystem C:/	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Filesystem D:/	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 3	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 4	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Memory and pagefile	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Services Summary	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	System Time	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Uptime	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
ANALISTA_PUTUMAYO	CPU utilization	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Check_MK	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
	Check_MK Discovery	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Disk IO SUMMARY	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Filesystem C:/	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Filesystem D:/	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 2	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 3	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 4	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Interface 5	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Memory and pagefile	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Services Summary	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Figura CR 14. Creación de reportes de disponibilidad en Nagios.

Otra manera de generar el reporte es mediante un archivo en formato CSV, en el cual se muestra de forma mas detallada los estados de disponibilidad de los servicios en cada uno de los equipos.

Por cuestiones de tamaño, para poder mostrar los resultados, se tuvo en cuenta los servicios de los servidores Azkaban y Voldemort, en el Anexo Q. Resultados de reporte en archivo .cvs avail all service servidores Azkaban y Voldemort. Se pueden ver los resultados.

Se detallará un poco más sobre estos archivos mas adelante.

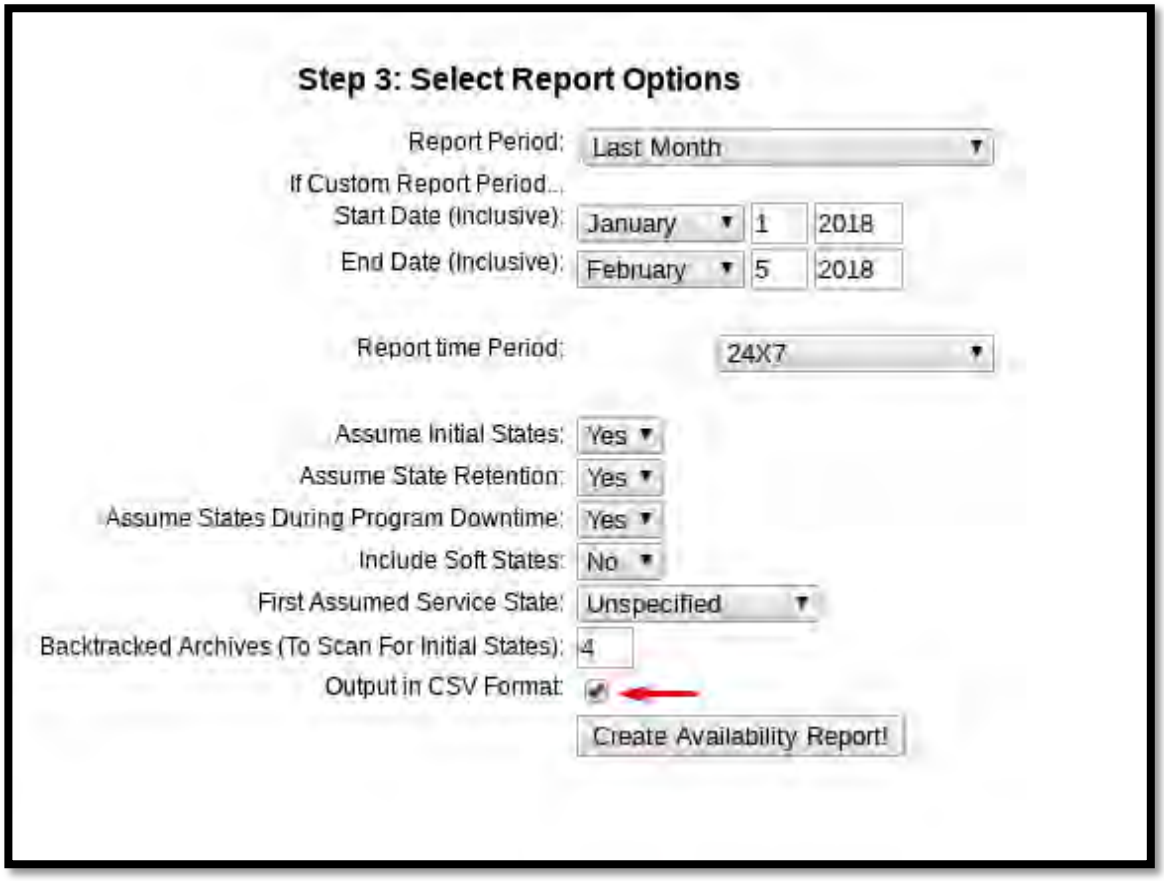


Figura CR 15. Creación de reportes de disponibilidad en Nagios.

Trends: el reporte de Trends (tendencias) proporciona un desglose gráfico y cronológico del estado de un servidor o servicio en particular.

Este tipo de reportes es individual, es decir que los resultados que muestra es de un host o servicio en particular.

A continuación, se muestra los resultados obtenidos de los servidores azkaban y voldemort durante un mes.

Los resultados del servidor voldemort tal como muestra la Figura CR 16*, el* servidor ha trabajado de forma contínua durante todo el mes, ya que casi la mayor parte del tiempo un 99.976% su estado a sido Up (Arriba) y una minima un 0.024% Down (Abajo).

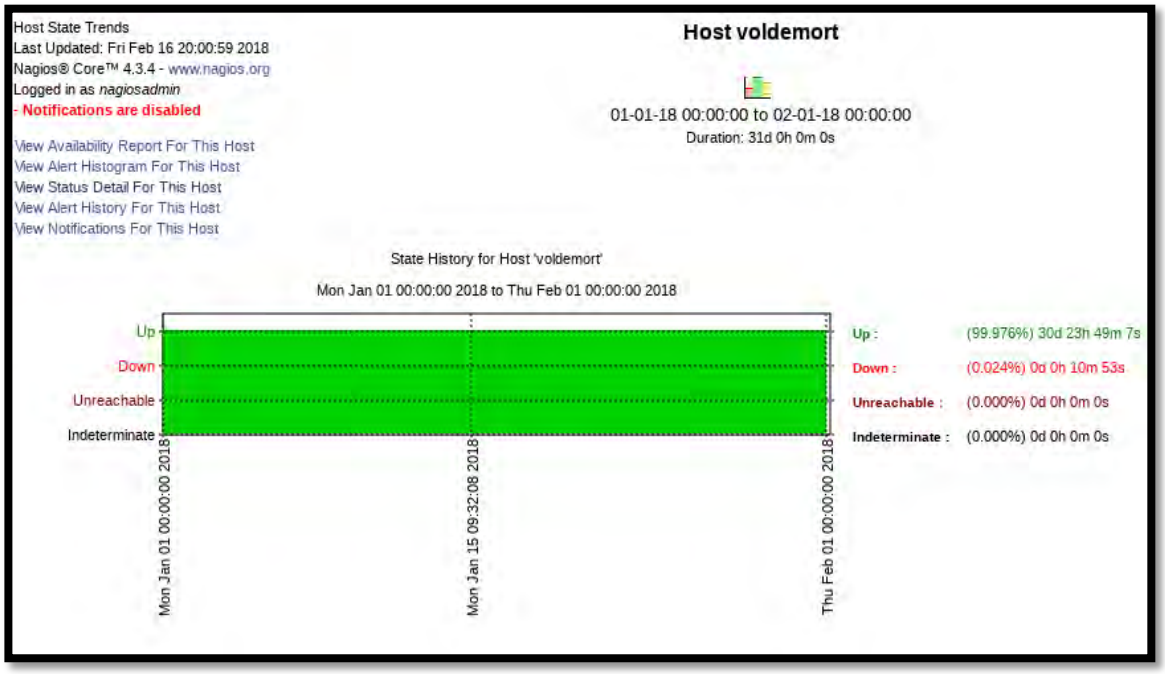


Figura CR 16. Grafica de historial de estado de servidor voldemort.

Los resultados obtenidos del servidor azkaban son similares a los del servidor voldemort, la Figuras CR 17 muestra como el servidor ha trabajado de forma contínua durante todo el mes, ya que casi la mayor parte del tiempo un 99.978% su estado a sido Up (Arriba) y una minima un 0.022% Down (Abajo).

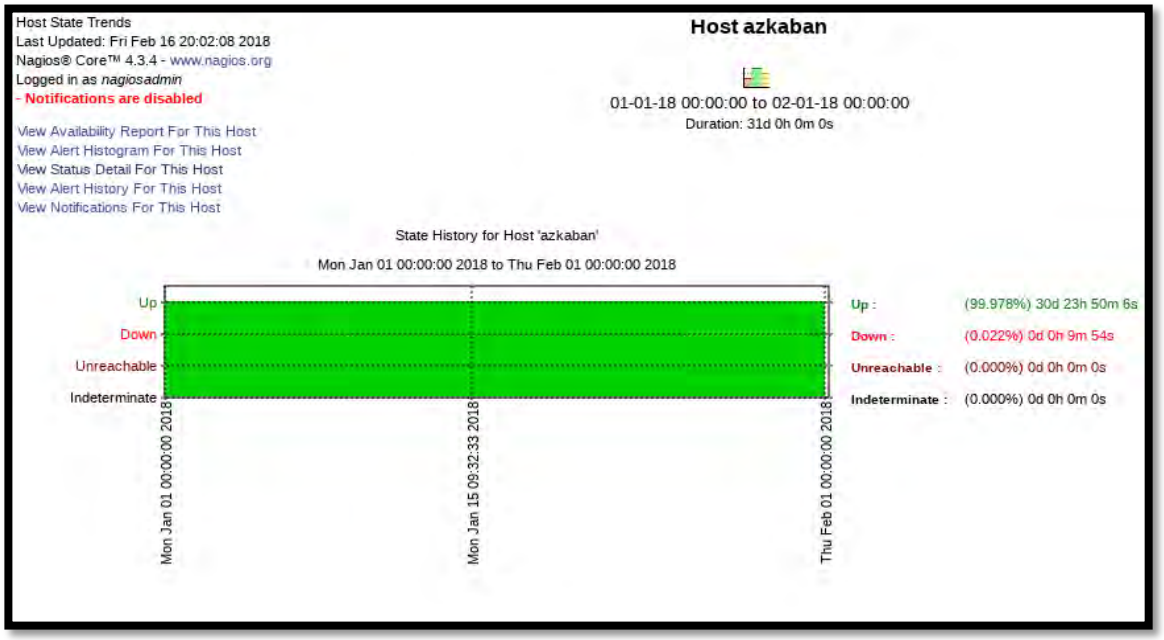


Figura CR 17. Gráfica de historial de estado de servidor azkaban.

Alerts:

- Alert History

El reporte de Alert History (historial de alertas) proporciona un registro de alertas históricas para hosts y servicios.

En la Figura CR 18 se observa las alertas producidas durante el día, se pueden realizar filtros de la información que ayudan tener más claridad del comportamiento de alertas de equipos y servicios monitoreados por Nagios.

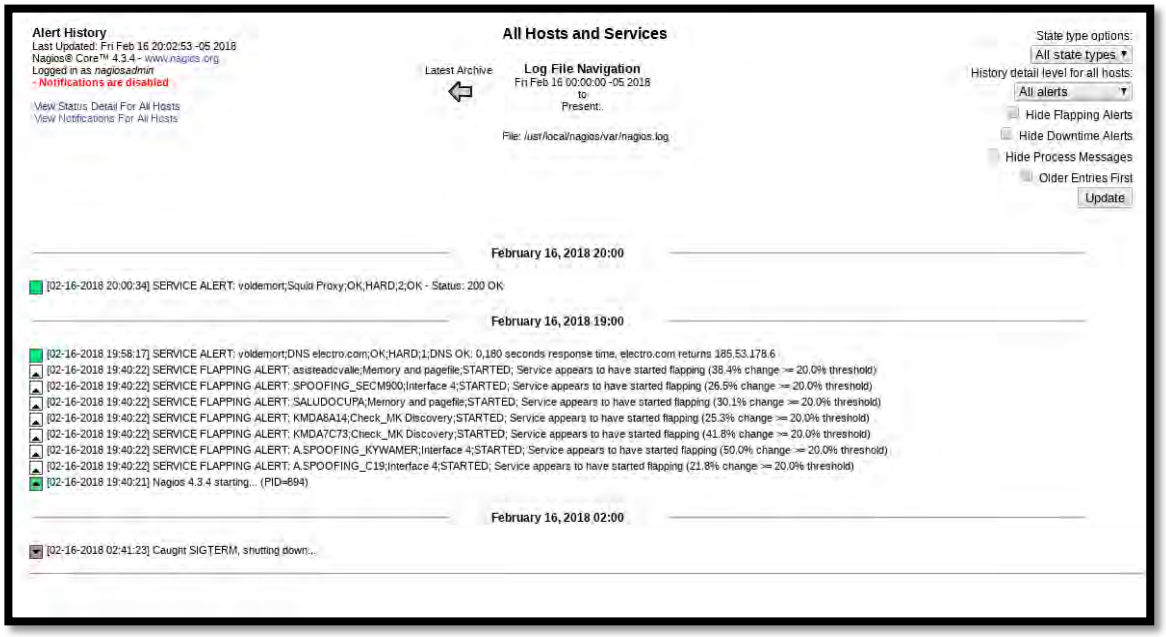
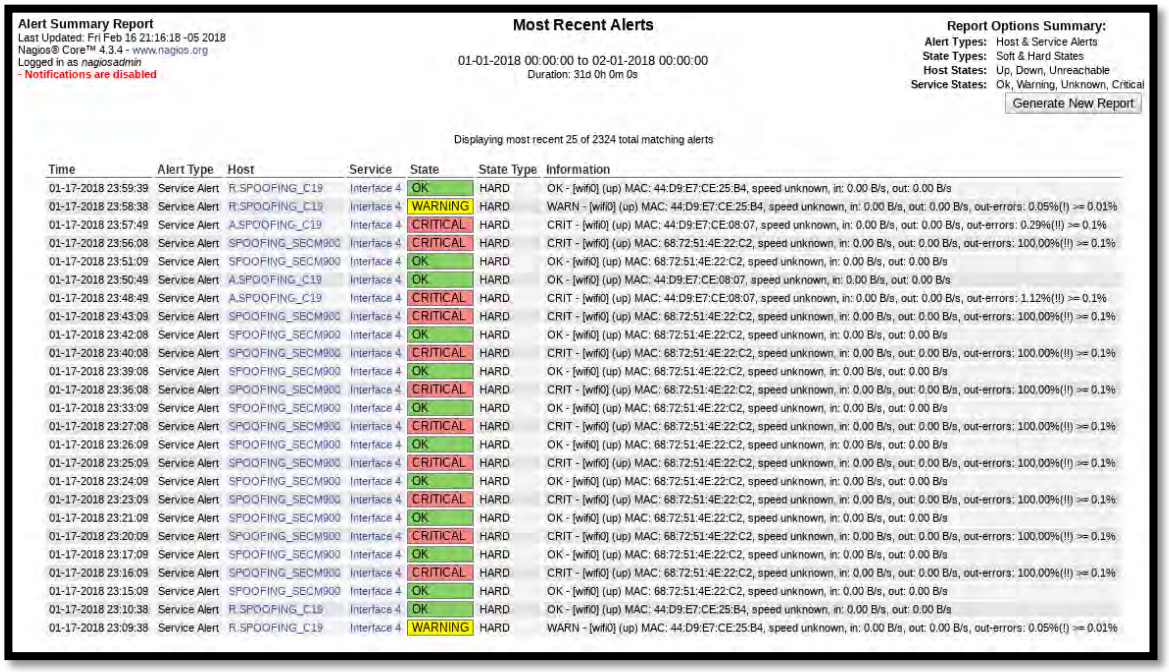


Figura CR 18. Resultados de historial de alertas de todos los host y servicios.

- Alert Summary

El reporte de Alert Summary (resumen de alertas), proporciona un informe de los principales productores de alertas. Esto es útil para determinar que equipos o servicios son los que causan la mayor cantidad de problemas en la infraestructura de red.

A continuación, se muestra los resultados recientes de cambios de estado de las últimas veinticinco alertas generadas tanto por equipos como por servicios.



Alert Summary Report
Last Updated: Fri Feb 16 21:16:18 -05 2018
Nagios® Core™ 4.3.4 - www.nagios.org
Logged in as nagiosadmin
- Notifications are disabled

Most Recent Alerts

01-01-2018 00:00:00 to 02-01-2018 00:00:00
Duration: 31d 0h 0m 0s

Report Options Summary:
Alert Types: Host & Service Alerts
State Types: Soft & Hard States
Host States: Up, Down, Unreachable
Service States: Ok, Warning, Unknown, Critical

Generate New Report

Displaying most recent 25 of 2324 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
01-17-2018 23:59:39	Service Alert	R.SPOOFING_C19	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 44:D9:E7:CE:25:B4, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:58:38	Service Alert	R.SPOOFING_C19	Interface 4	WARNING	HARD	WARN - [wifi0] (up) MAC: 44:D9:E7:CE:25:B4, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 0.05%(!) >= 0.01%
01-17-2018 23:57:49	Service Alert	A.SPOOFING_C19	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 44:D9:E7:CE:08:07, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 0.29%(!!) >= 0.1%
01-17-2018 23:56:08	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:51:09	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:50:49	Service Alert	A.SPOOFING_C19	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 44:D9:E7:CE:08:07, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:48:49	Service Alert	A.SPOOFING_C19	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 44:D9:E7:CE:08:07, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 1.12%(!!) >= 0.1%
01-17-2018 23:43:09	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:42:08	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:40:08	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:39:08	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:36:08	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:33:09	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:27:08	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:26:09	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:25:09	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:24:09	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:23:09	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:21:09	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:20:09	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:17:09	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:16:09	Service Alert	SPOOFING_SECM900	Interface 4	CRITICAL	HARD	CRIT - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 100.00%(!!) >= 0.1%
01-17-2018 23:15:09	Service Alert	SPOOFING_SECM900	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 68:72:51:4E:22:C2, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:10:38	Service Alert	R.SPOOFING_C19	Interface 4	OK	HARD	OK - [wifi0] (up) MAC: 44:D9:E7:CE:25:B4, speed unknown, in: 0.00 B/s, out: 0.00 B/s
01-17-2018 23:09:38	Service Alert	R.SPOOFING_C19	Interface 4	WARNING	HARD	WARN - [wifi0] (up) MAC: 44:D9:E7:CE:25:B4, speed unknown, in: 0.00 B/s, out: 0.00 B/s, out-errors: 0.05%(!) >= 0.01%

Figura CR 19. Resumen de las utimas 25 alertas generadas por Nagios.

- Alert Histogram

El reporte Alert Histogram (histograma de alerta) proporciona un gráfico de frecuencia de las alertas de host y servicio. Útil para ver cuándo las alertas ocurren con mayor frecuencia para un host o servicio en particular.

La siguiente gráfica, Figura CR 20, muestra que durante el dia cuatro (4) al seis (6) de enero de 2018 hubo eventos UP (arriba) y Down (abajo) consecutivos en el servidor voldemort, esto debido a que en estos días se apago dos veces el servidor Nagios y se prendio una vez.

Por otro lado, evidencia que desde el día doce (12) al dieciséis (16) de enero de 2018, el servidor Nagios estuvo apagado.

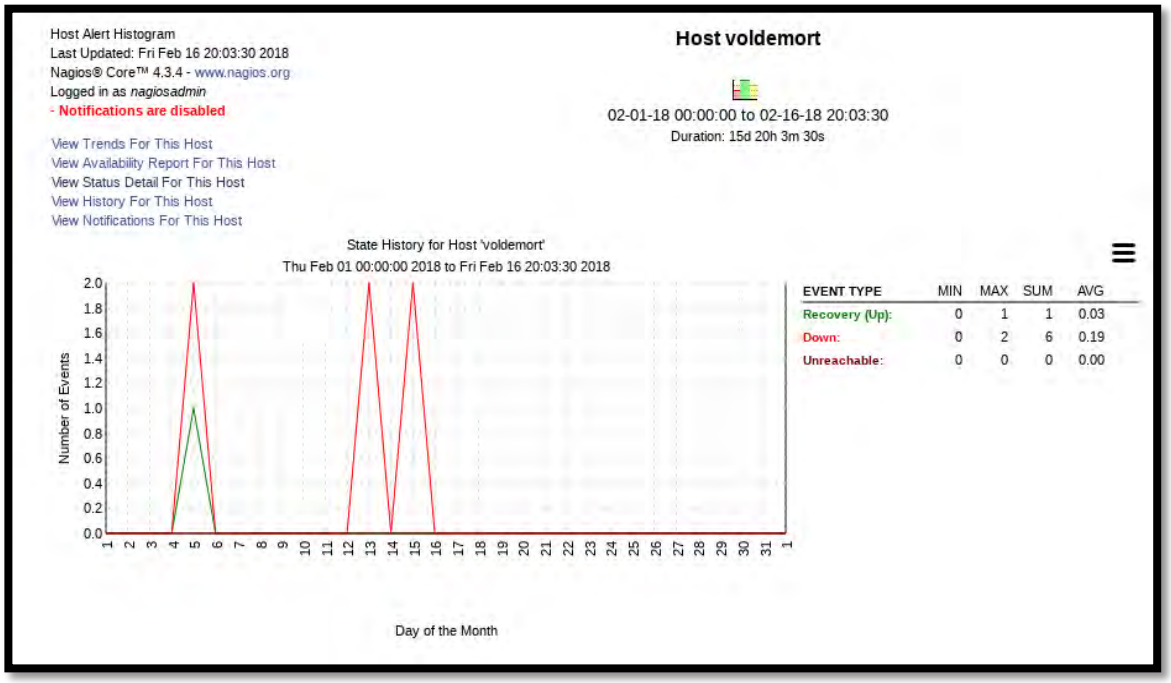


Figura CR 20. Gráfico de frecuencia de alertas de host y servicios del servidor voldemort.

La siguiente gráfica, Figura CR 21, muestra que durante el dia catorce (14) al dieciséis (16) de enero de 2018 hubo eventos UP (arriba) y Down (abajo) consecutivos en el servidor azkaban, esto debido a que en estos días se apagó dos veces el servidor Nagios y se prendio una vez.

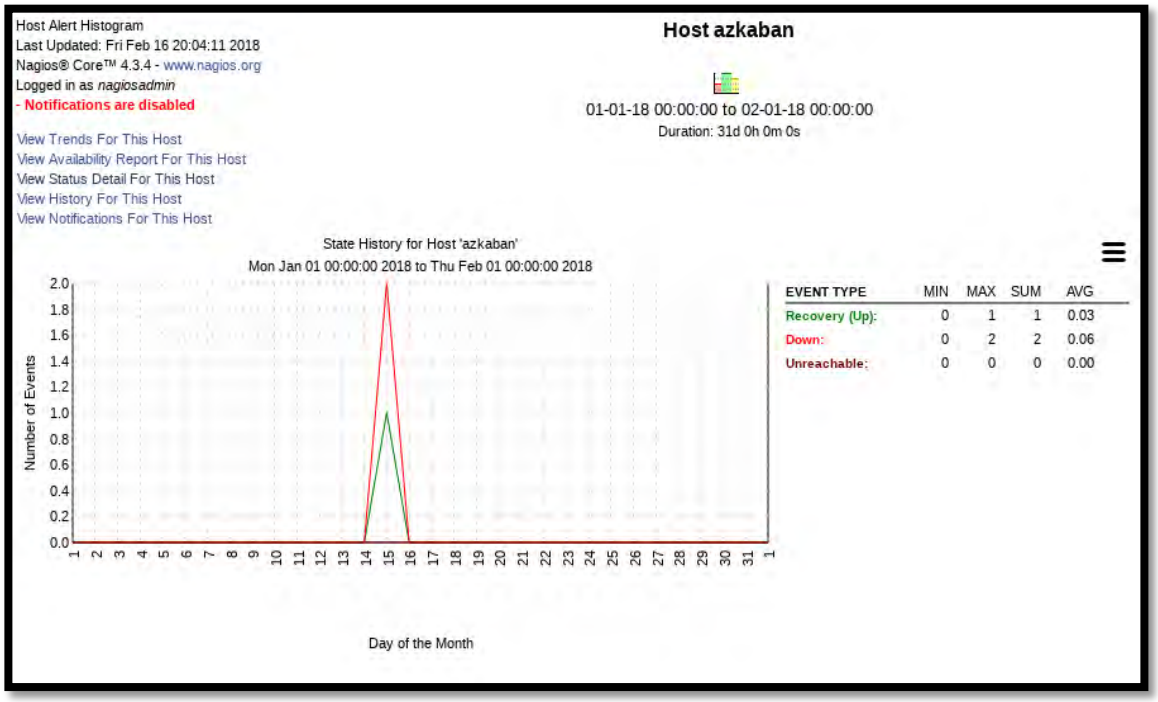


Figura CR 21. Gráfico de frecuencia de alertas de host y servicios del servidor azkaban.

Nota: cabe resaltar que no fueron los servidores azkaban y voldemor los que estuvieron fuera de servicio durante los tiempos precisados en las gráficas, si no el servidor Nagios.

Notifications: el reporte de Notifications (notificaciones), proporciona un registro histórico de las notificaciones de host y servicio que se han enviado a los contactos.

En este caso no se encontraron notificaciones en la fecha establecida. Los resultados suministrados en este informe son directamente recolectados de los datos obtenidos de archivos .log que se encuentran en la ruta **/usr/local/nagios/var/archives/**



Figura CR 22. Reporte de notificaciones de host y servicios a contactos.

Event Log: el reporte Event Log (registro de eventos) permite la opción de ver los eventos que ocurren dentro del core de Nagios.

Los datos son suminstrados por el archivo nagios.log que se encuentra en la ruta **/usr/local/nagios/var/nagios.log**

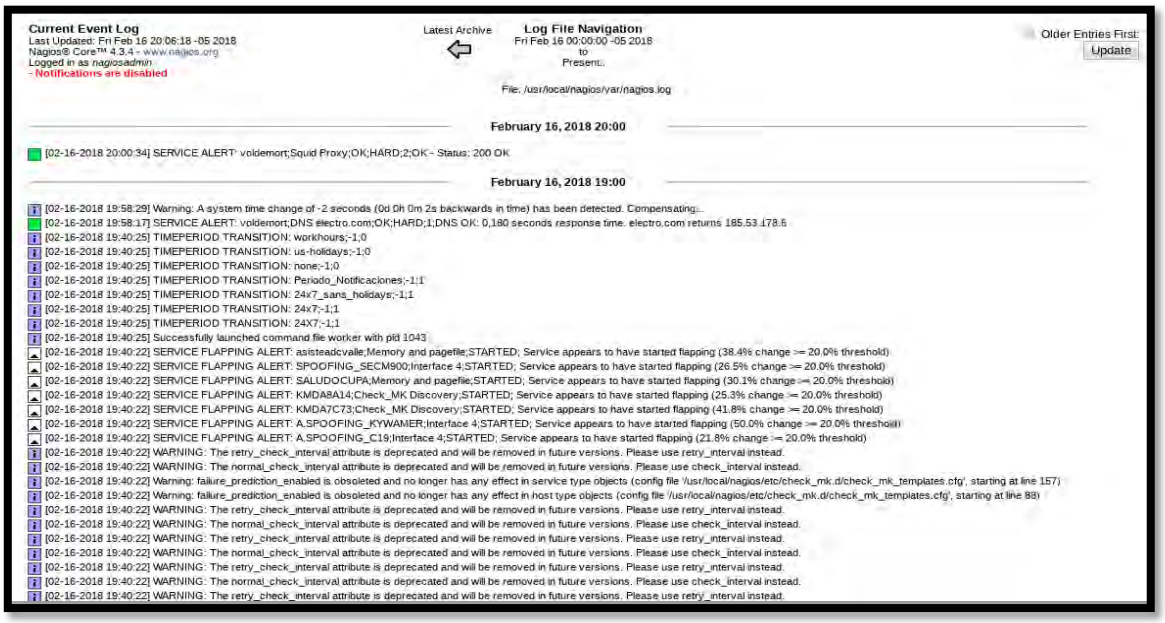


Figura CR 23. Reporte de servicios de eventos Nagios.

Análisis de reportes cvs generados en availability: anteriormente se había dicho que los reportes cvs generados en Availability son mas detatellados que los que se generan en la página web y formato pdf, en estos archivos se describe muchos mas campos, donde no solo se encuentra el porcentaje de tiempo, si no también el tiempo en segundos y diferentes estados que maneja un equipo y/o servicio.

- Total de equipos en estado up y down

El primer análisis realizado fue del total de equipos que se monitorearon en la empresa con respecto al tiempo de funcionamiento. Los datos se extrajeron del archivo cvs (Anexo P. Resultados de reporte en archivo .cvs avail individual all hots.), en una tabla en hoja de calculo Exel, estos datos corresponden al tiempo total (en segundos), en que los equipos monitoredos estuvieron en estado Up (arriba) y Down (abajo).

La figura Figura CR 24, muestra el comportamiento en estado UP de los equipos durante el mes de enero de 2018. De la gráfica se puede inferir que una gran cantidad de equipos que en promedio deberían funcionar solamente 8 horas al día, al mes 248 horas, tienen un uso de aproximadamente 18.6 horas al día es decir que en el mes de enero estuvieron en funcionamiento 576 horas, 24 de los 31 días del mes.

También se puede observar que los equipos como los servidores, radioenlaces y algunos equipos importantes, están teniendo un funcionamiento continuo. Hay otros equipos que no están en funcionamiento, esto puede ser debido a varias causas, por mensionar las mas comunes, puede ser que el equipo antes del mes de enero pasó a mantenimiento y no esté en funcionamiento, que el equipo este funcionando y no se le instaló el agente para poder ser moniteado por Nagios, o que hubo un cambio de equipo, entre otras.

En contraste la Figura CR 25, muestra el comportamiento del estado DOWN de los equipos durante el mismo mes. De la gráfica se puede decir que tiene el comportamiento contrario a la anterior, se observa que una gran mayoría de equipos han estado muy poco tiempo apagados, aproximadamente 6 horas al día, a excepción de los servidores y radioenlaces y algunos equipos que tienen un funcionamiento continuo durante el mes. Además, se puede observar, equipos que han estado fuera de funcionamiento, el motivo puede ser que el equipo este funcionando y no se le instaló el agente para poder ser moniteado por Nagios, o que hubo un cambio de equipo, o que el equipo antes del mes de enero pasó a mantenimiento y no esté en funcionamiento,

Tiempo de equipos en estado Up:

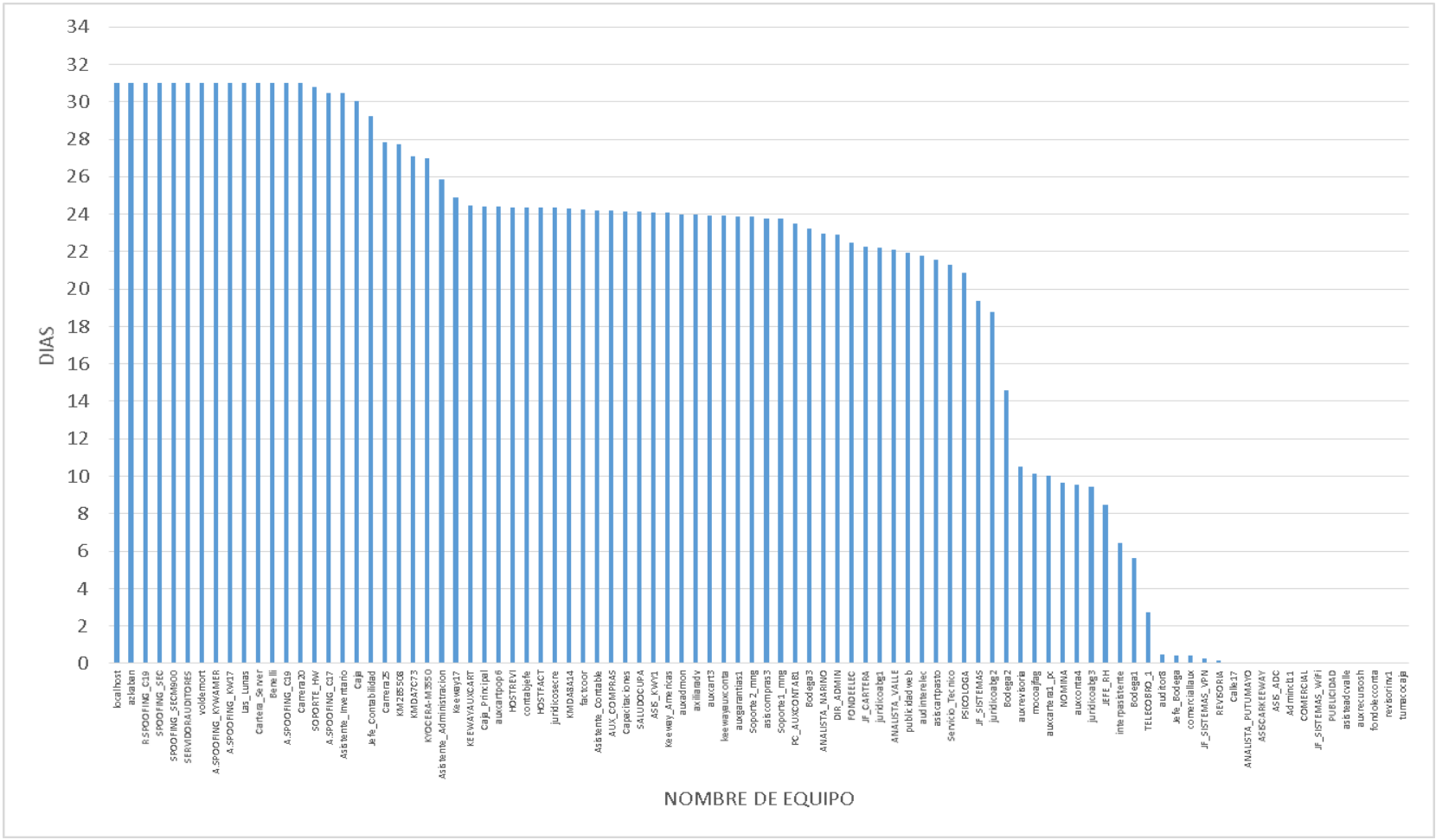


Figura CR 24. Gráfica, tiempo de equipos en estado UP, mes de enero 2018.

Tiempo de equipos en estado DOWN:

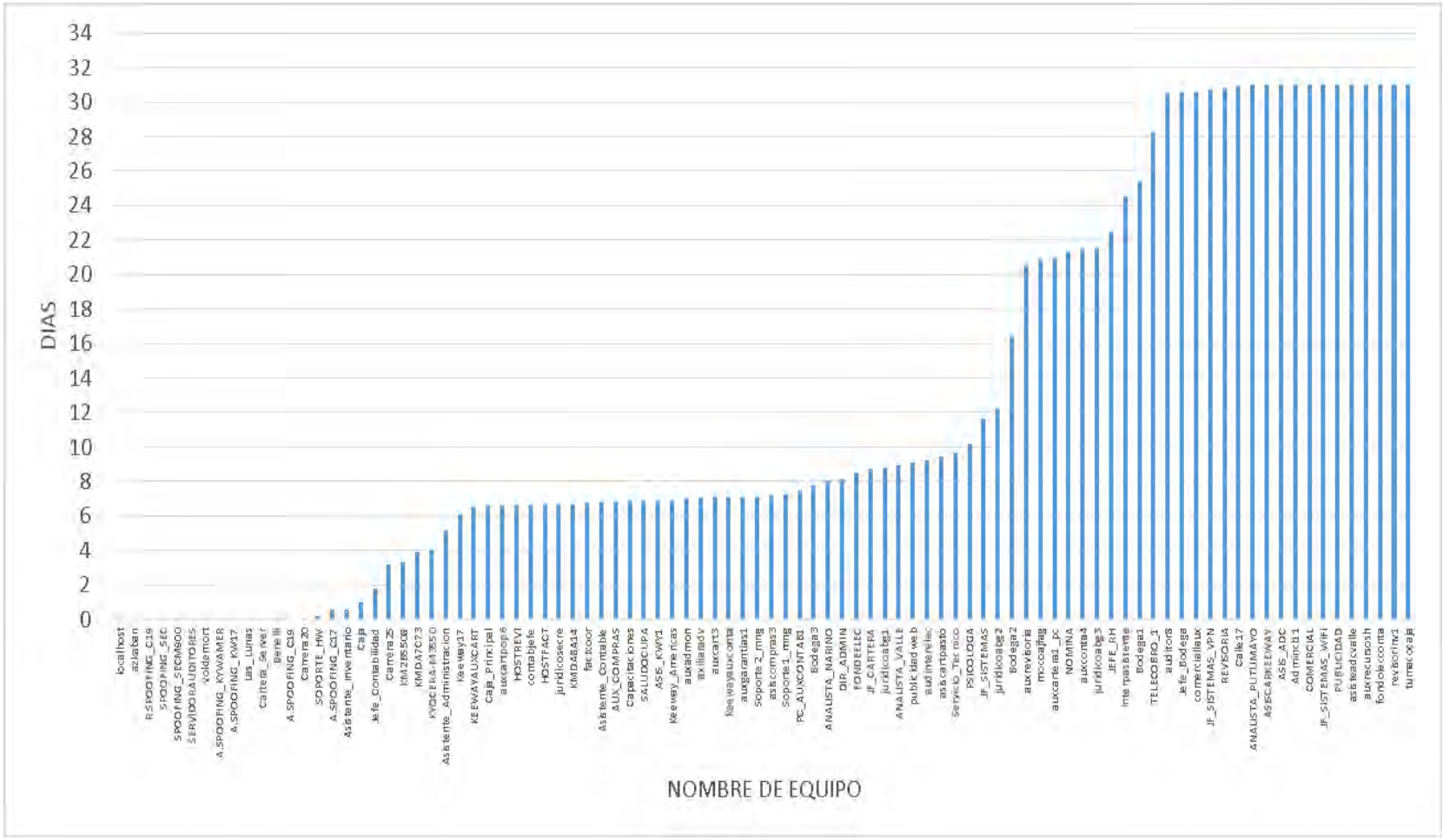


Figura CR 25. Gráfica, tiempo de equipos en estado UP, mes de enero 2018.

- Estado de servicios en servidor azkaban y voldemort

El segundo análisis realizado fue del comportamiento de estado (OK, CRITICAL, WARNING, UNKNOWN, UNDETERMINED) de cada uno de los servicios monitoreados en cada uno de los equipos de la empresa. Los datos se extrajeron del archivo cvs (Anexo Q. Resultados de reporte en archivo .cvs avail all service servidores Azkaban y Voldemort.), en una tabla en hoja de calculo Exel. Estos datos corresponden al tiempo total (segundos), en que los servicios de cada uno de los equipos se mantuvieron en un estado en particular.

Para más información en cuanto a tipos de estados en host y servicios visitar[47].

Nota: los estados WARNING, UNKNOWN, UNDETERMINED, no se utilizaron en el análisis de servicios del servidor azkaban debido a que el tiempo total de registro fue cero (0). Por el mismo motivo, el estado UNDETERMINED no fue utilizado en el análisis de servicios del servidor voldemort.

- Servidor Azkaban

La Figura CR 26*,* muestra el comportamiento en estado OK (satisfactorio) de los servicios del servidor azkaban, monitoreados por Nagios durante el mes de enero de 2018. Se muestra como durante este mes el servidor, en cuanto a servicios no tuvo problemas, solamente pequeñas interferencia en los servicios **Check_MK**, **OpenFire**, **SSH** y **FTP**, que no afectaron los procesos informáticos dentro de la empresa. En general se puede decir que el servidor azkaban tuvo un comportamiento casi perfecto en los servicios monitoriados, ya que en las fallas minimas en los servicios anteriormente mensionados, se evidencia en promedio un funcionamiento constante durante 30.99 dias de los 31 días del mes. El resto de servicios tuvieron un trabajo pleno de 31 de los 31 dias monitoreados.

La Figura CR 27, muestra un contraste opuesto a la anterior, ya que se observa el comportamiento en estado CRITICAL (critico), de los servicios **Check_MK**, **OpenFire**, **SSH** y **FTP**, instalados en el servidor azkaban. En este sentido, se observa que durante el mes de enero el servicio **Check_MK** tuvo un aproximado de once minutos de comportamiento CRITICAL, el servicio OpenFire ocho minutos, el servicio **SSH** y el **FTP** de nueve minutos. El motivo de tal estado en estos servicios puede obedecer a varios factores, el principal es que los servicios sobrepasen los valores predeterminados colocados por el administrador a la hora de definir los topes que deben tener, teniendo en cuenta variables como tiempo, estado del puerto (activo, inactivo), estado de protocolo (activo, inactivo), ping, entre otros. Otro motivo se puede deber a niveles pico de consumo de banda en los días de cierre de mes, cortes de energia, problemas hardware, entre otros.

[47] Nagios, Op. Cit.

Tiempo en estado ok de servicios en servidor AZKABAN:

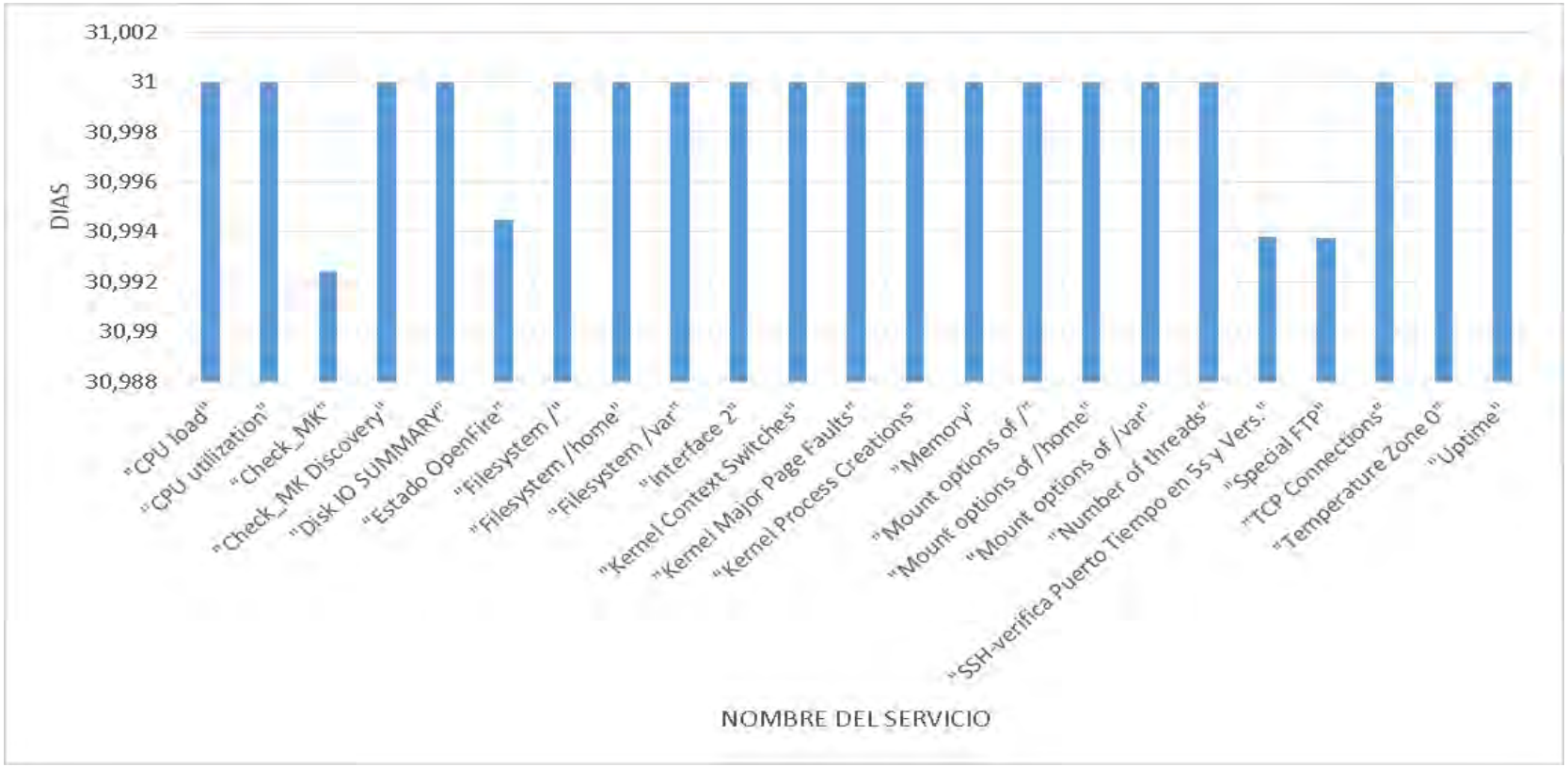


Figura CR 26. Estado OK de servicios en servidor azkaban en el mes de enero de 2018. R

Tiempo en estado critical de servicios en servidor AZKABAN:

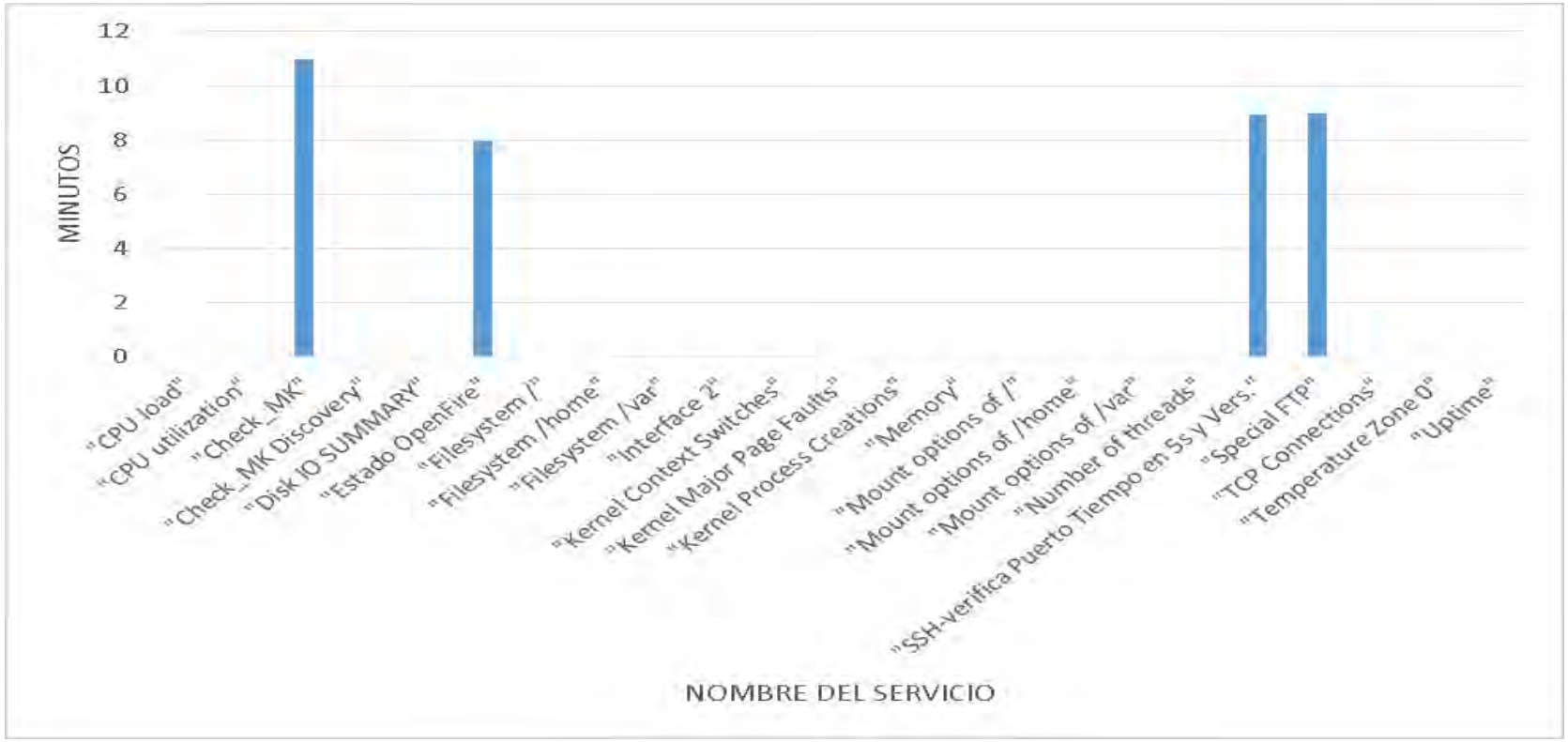


Figura CR 27. Estado CRITICAL de servicios en servidor azkaban en el mes de enero de 2018.

- Servidor Voldemort

La Figura CR 28*,* muestra el comportamiento en estado OK (satisfactorio) de los servicios del servidor voldemort monitoreados por Nagios, durante el mes de enero de 2018. Se muestra como durante este mes el servidor, en cuanto a servicios no tuvo mayores inconvenientes que afectacen los procesos informáticos dentro de la empresa.

Según lo observado en la gráfica, Figura CR 28, los servicios **DNS, Filesystem /datosbd, Filesystem /media/usb y Mount option of /media/usb**, tuvieron estados diferentes a OK. Los servicios Check_MK, Apache, SSH Y Squid tuvieron pequeñas interferencias que en general no son significativas ya que en promedio trabajaron 30.99 días de los 31 días del mes. El resto de servicios tuvieron un trabajo óptimo de 31 días de los 31 días monitoreados.

En la Figura CR 29, se observa como dos de los servicios del servidor voldemort, **DNS y Filesystem /datobd**, tuvieron estados WARNING (advertencia). El servcio **DNS** estuvo durante casi el total de los 31 días del mes en estado WARNING, el motivo de este estado se devio a que el servicio excedió el nivel de respuesta configurado en diez segundos, pero no superó el tope de quince segundos configurado para el estado CRITICAL. Por su parte el servicio Filesystem /datosbd, estuvo durante un poco más de 16 días en estado WARNING, esto debido a que exedió el nivel de uso de espacio de la particion de un 85%, pero no superó el tope de 90% para un estado CRITICAL.

En la Figura CR 30, se puede observar como dos servicios **Filesystem /media/usb y Mount options of /media/usb**, han estado durante 30 días en estado UNKNOWN (desconocido), esto debido a que la particion /media/usb fue creada y montada, pero Nagios no ha encontrado ningun tipo de actividad relacionado durante el mes de monitoreo.

Por último, las Figuras CR 31 y CR 32, muestran el resultado de los servicios en estado CRITICAL (critico), del servidor voldemort. En la *Figura CR 31* se oberva un grafica ampliada en cuanto al rango de tiempo (días), en donde el servicio **Filesystem /datosbd** estuvo aproximadamente 14 días y medio en tal estado, esto debido a que exedió el nivel de uso de espacio de la particion de un 90%. En la *Figura CR 32* se hace una disminución en la escala de tiempo (minutos), en donde se evidencia que los servicios estuvieron en estado CRITICAL durante el mes de enero. **Check_MK** once minutos, **DNS** once minutos, **Apache** nueve minutos**, SSH** nueve minutos y **Squid** aproximadamente nueve minutos y medio. El motivo de tal estado en estos servicios puede obedecer a varios factores, el principal es que los servicios sobrepasen los valores predeterminados colocados por el administrador a la hora de definir los topes variables de chequeo. Otro motivo se puede deber a niveles pico de consumo de banda en los días de cierre de mes, cortes de energia, problemas hardware, entre otros.

Tiempo en estado ok de servicios en servidor VOLDEMORT:

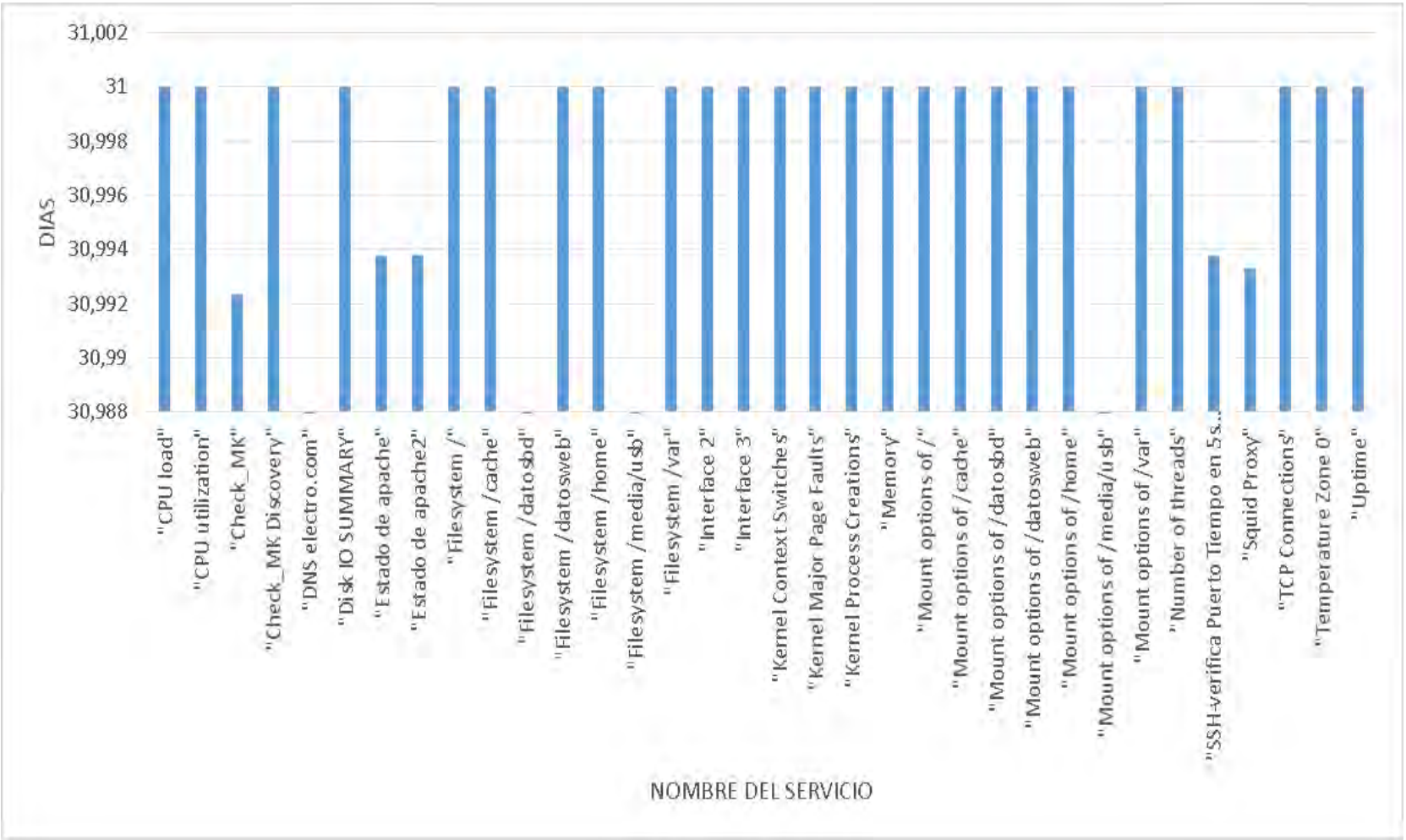


Figura CR 28. Estado OK de servicios en servidor voldemort en el mes de enero de 2018.

Tiempo en estado warning de servicios en servidor VOLDEMORT:

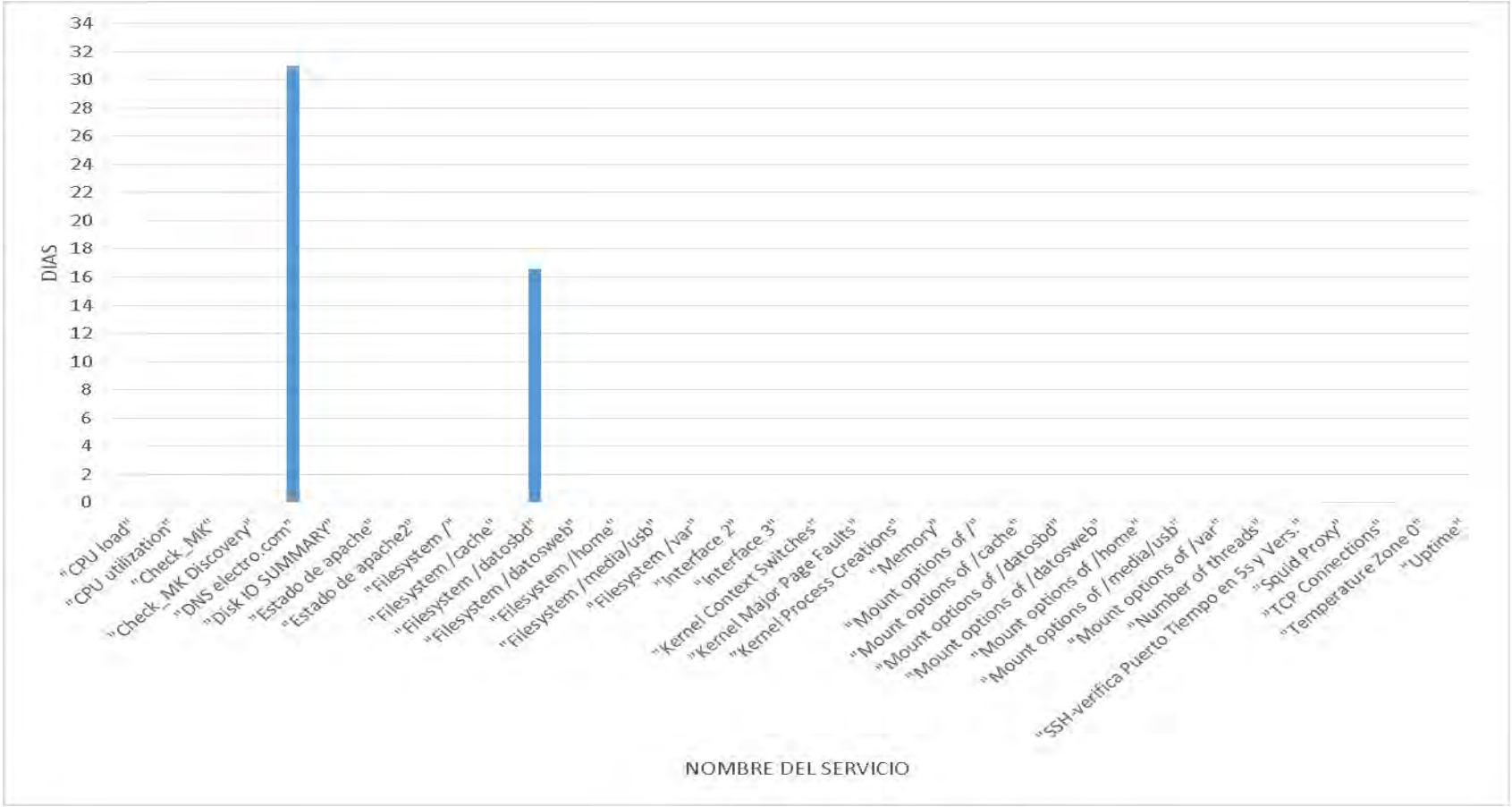


Figura CR 29. Estado WARNING de servicios en servidor voldemort en el mes de enero de 2018.

Tiempo en estado unknown de servicios en servidor VOLDEMORT:

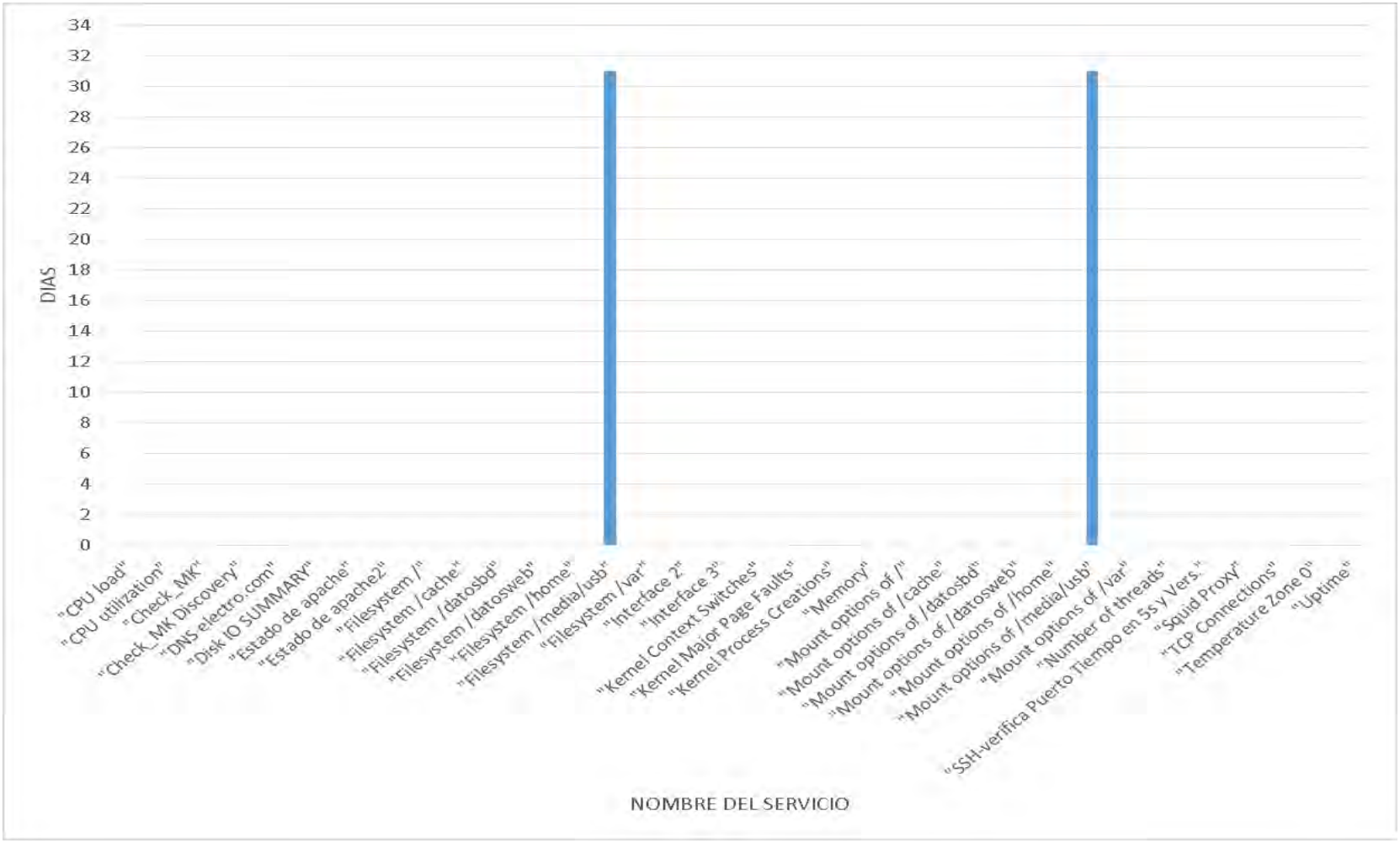


Figura CR 30. Estado UNKNOWN de servicios en servidor voldemort en el mes de enero de 2018.

Tiempo en estado critical de servicios en servidor VOLDEMORT:

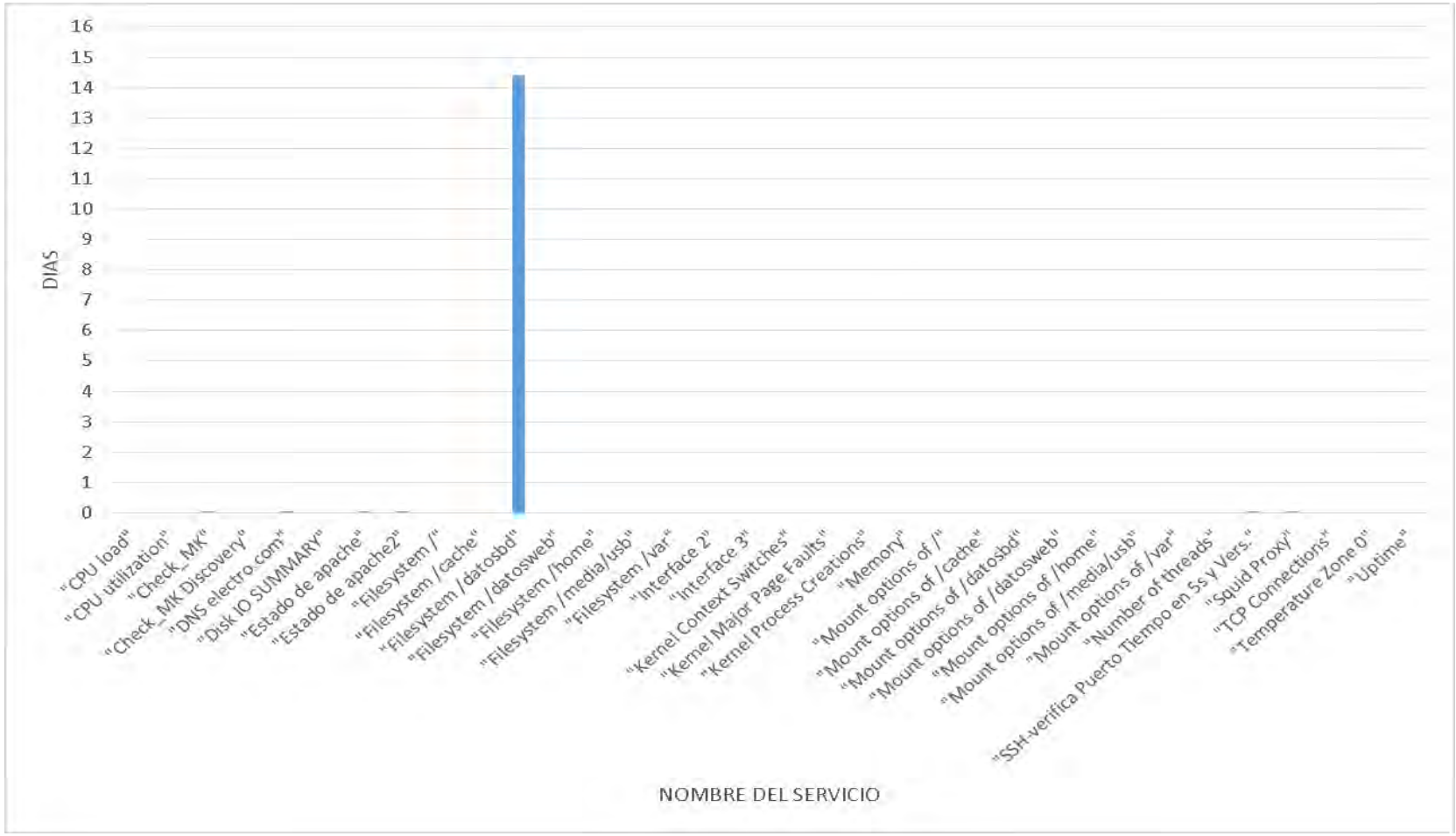


Figura CR 31. Estado CRITICAL de servicios en servidor voldemort en el mes de enero de 2018.

Tiempo en estado critical de servicios en servidor VOLDEMORT:

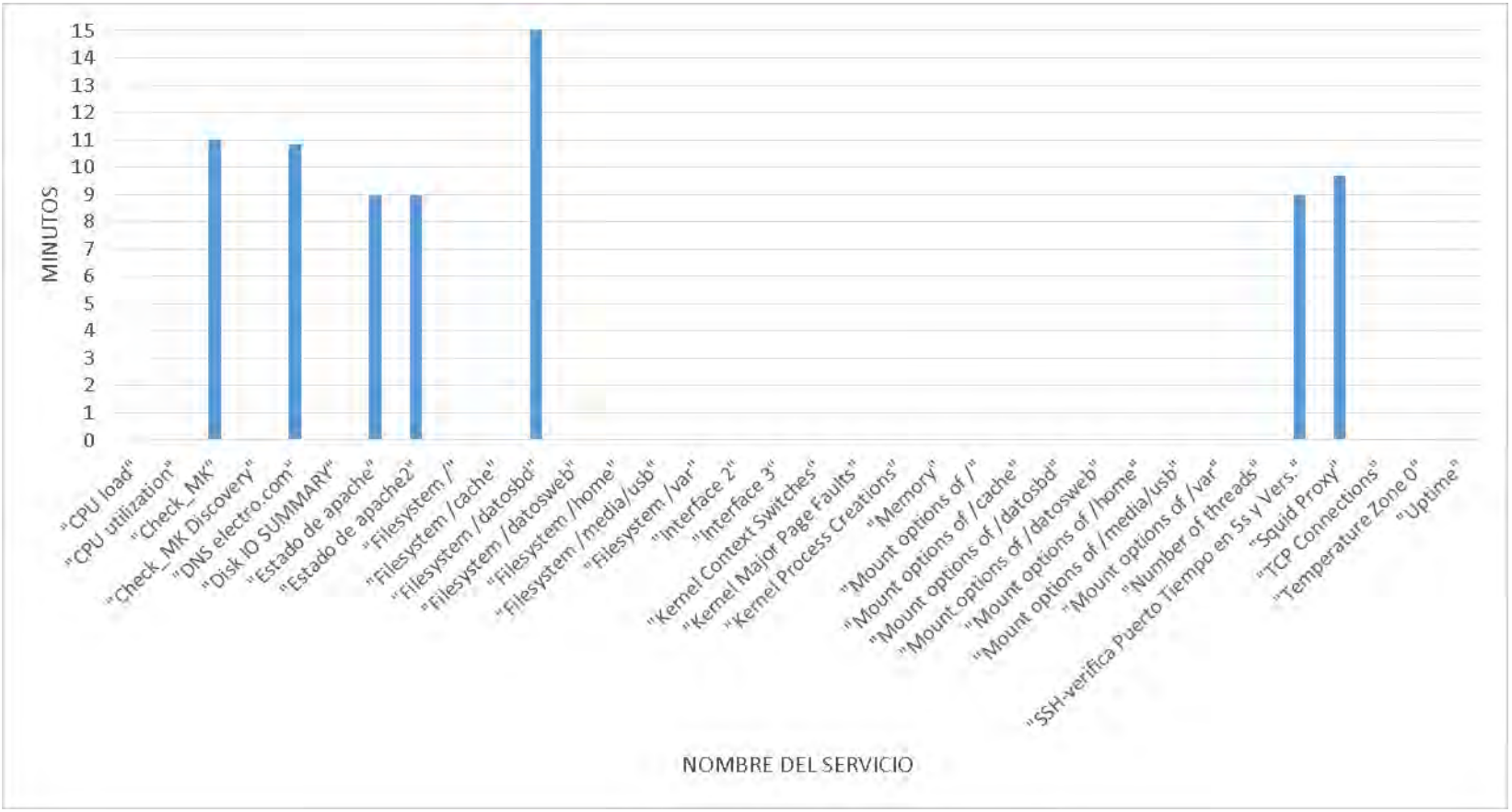


Figura CR 32. Estado CRITICAL de servicios en servidor voldemort en el mes de enero de 2018.

9.8.6 Actualización de la suite de monitoreo. Una actividad a tener en cuenta es la actualización de las versiones de las herramientas que componen la suite de monitoreo, es algo muy importante para que el trabajo pueda permanecer en óptimo funcionamiento a través del tiempo. Las versiones se pueden tener dos a tres veces en el año.

El proceso de actualización de las versiones hace parte de la investigacion realizada por los integrantes de este trabajo.

Se recomienda hacer un respaldo de la configuración antes de realizar las actualizaciones.

Actualización versión de Nagios core: para mas información sobre este tema visitar (Nagios org, 2017).

Se descarga desde la fuente.

```
cd /tmp
wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.3.4.tar.gz
```

Se Descomprime y se compila

```
tar xzf nagioscore.tar.gz
cd /nagioscore-nagios-4.3.4/
./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

Se ejecutan los comandos siguientes:

```
make all
make install
```

Se debe modificar el archivo config.inc.php ubicado en la ruta /usr/local/nagios/share/

```
nano /usr/local/nagios/share/config.inc.php
```

Dentro del archivo se modifica la linea donde dice: *$cfg['cgi_base_url']='/nagios/cgi-bin';*

Por:

```
$cfg['cgi_base_url']='/site01/nagios/cgi-bin';
```

Se reinicia Nagios.

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

Actualización versión de check_mk: para mas información sobre este tema visitar (Kettner GmbH, 2017).

Se descarga desde la fuente.

```
cd /tmp
wget -O check_mk-1.2.8p26.tar.gz http://mathias-kettner.com/download/check_mk-1.2.8p26.tar.gz
```

Se descomprime y se compila.

```
tar zxfv check_mk-1.2.8p26.tar.gz
cd check_mk-1.2.8p26
./setup.sh
```

Esta configuración se hizo al momento de instalar por primera vez check_mk. Se da enter a todas las opciones, si es necesario se podrá verificar la configuración para mayor seguridad.

NOTA: Si se ha hecho actualización previa de Nagios, se debe cambiar la versión de nagios de la anterior a la actual cuando se llegue a la siguiente opción.

Así:

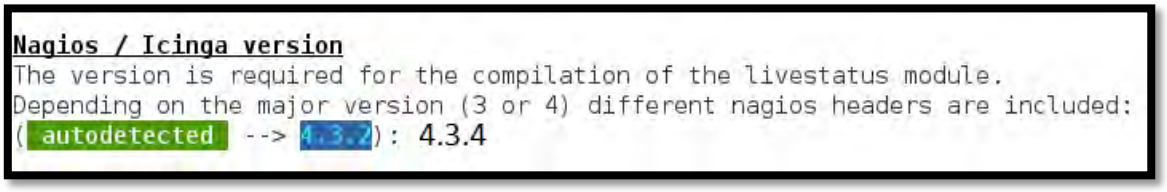


Figura ACH 1. Definición de rutas de instalación.

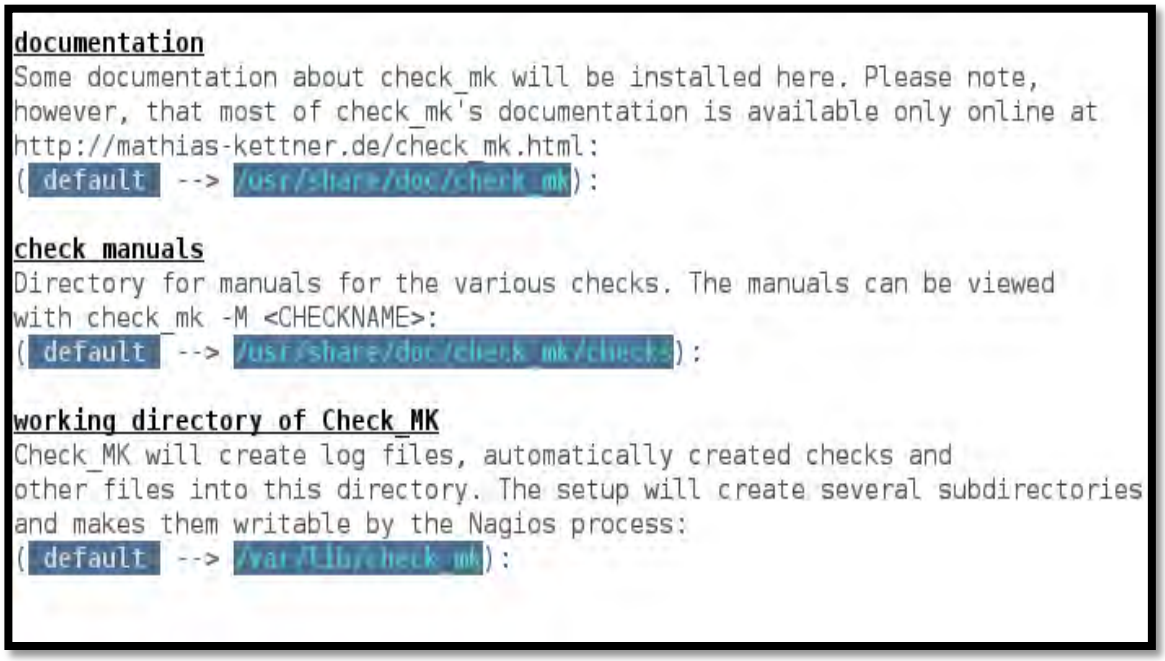


Figura ACH 2. Definición de rutas de instalación.

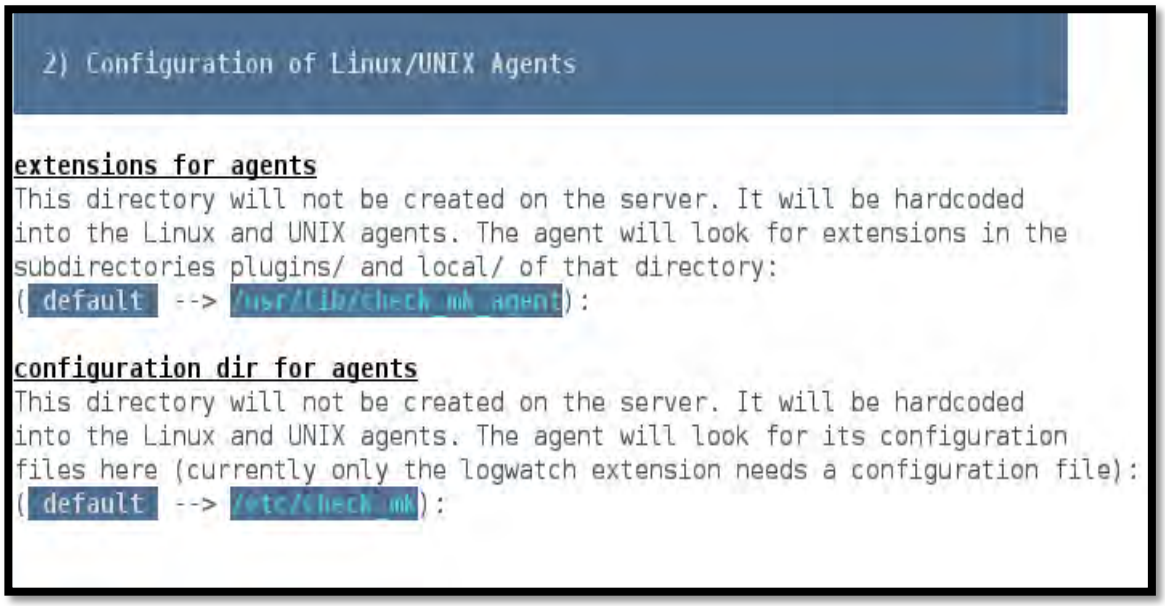


Figura ACH 3. Definición de rutas de instalación.

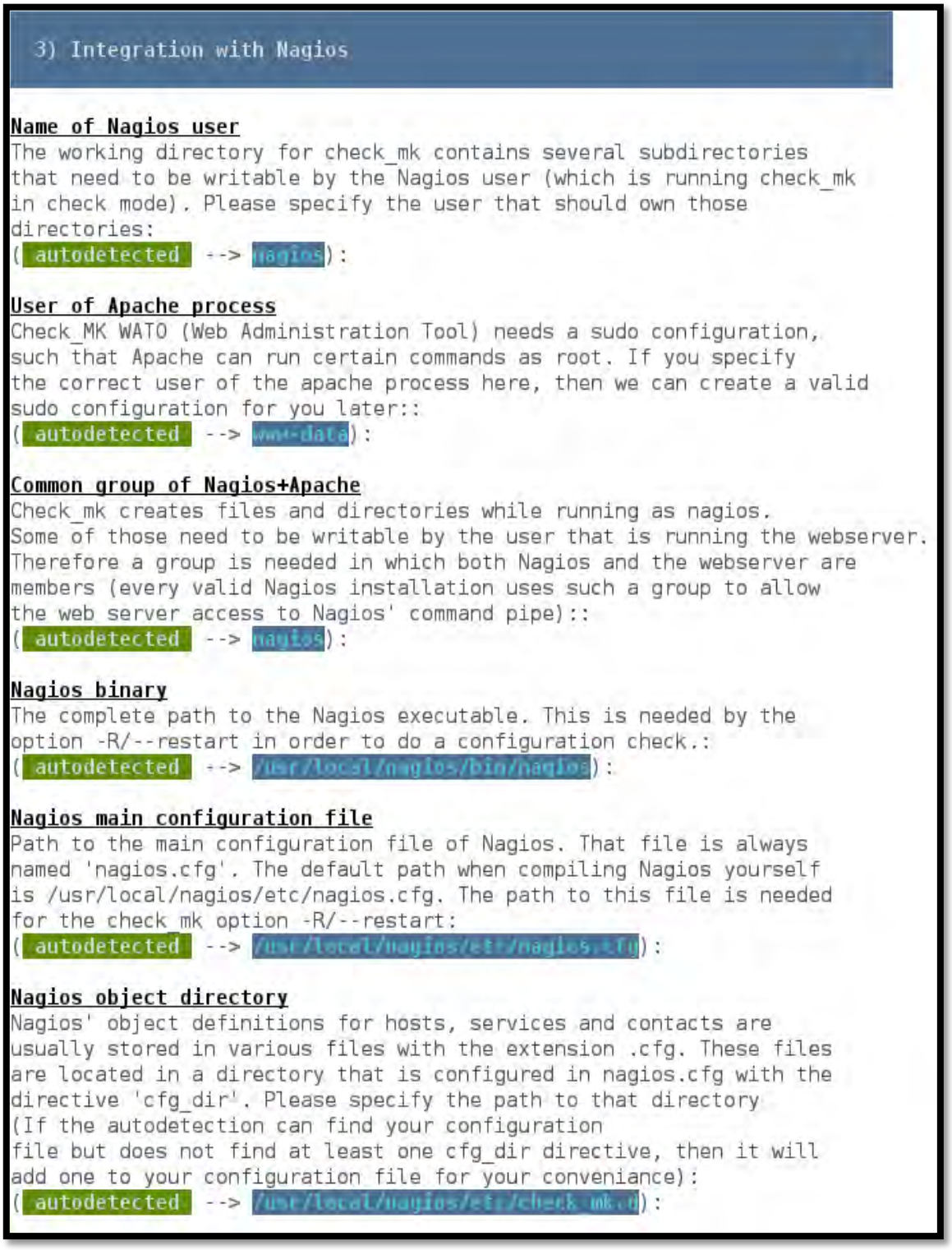


Figura ACH 4. Definición de rutas de instalación.

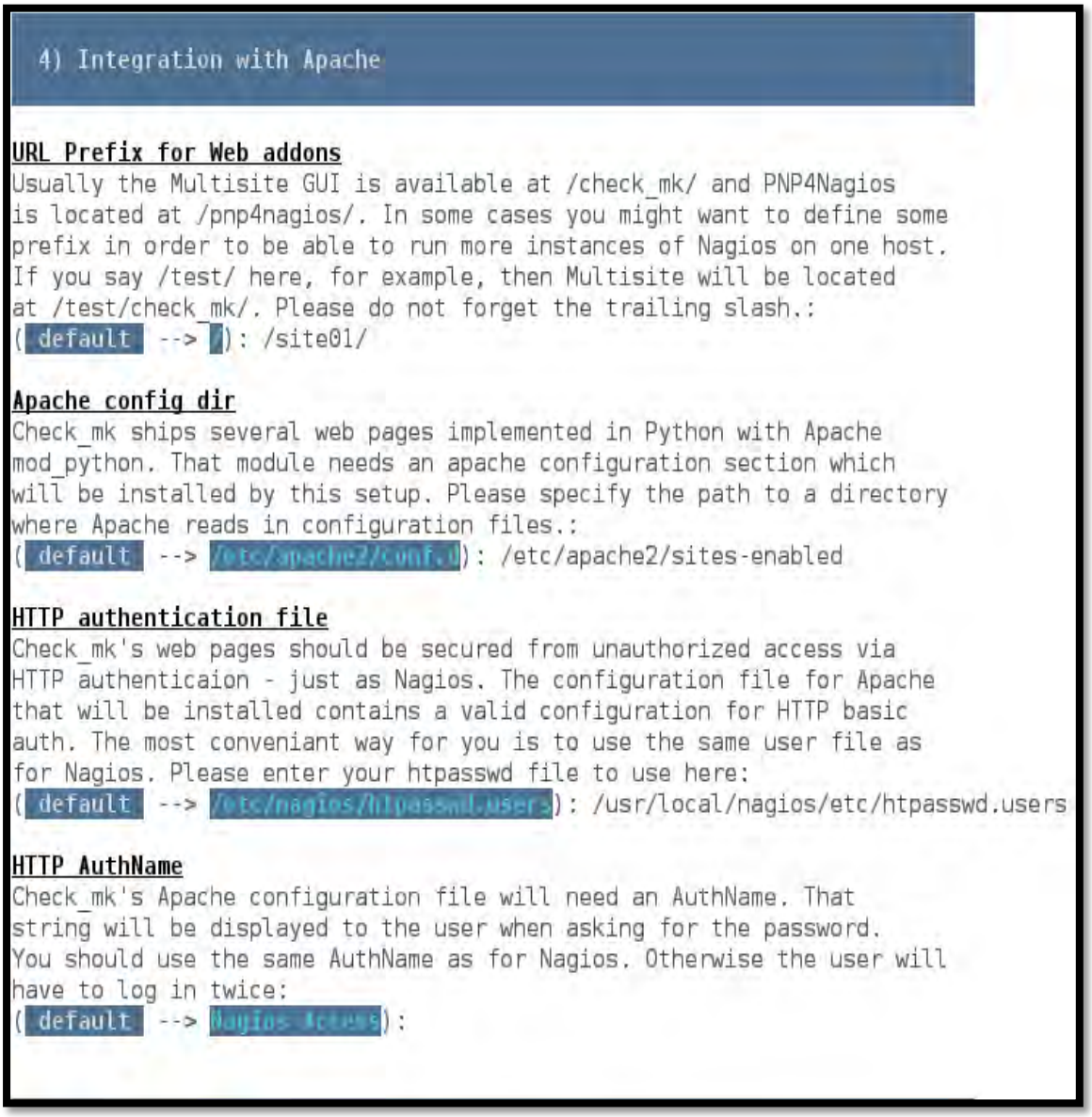


Figura ACH 5. Definición de rutas de instalación

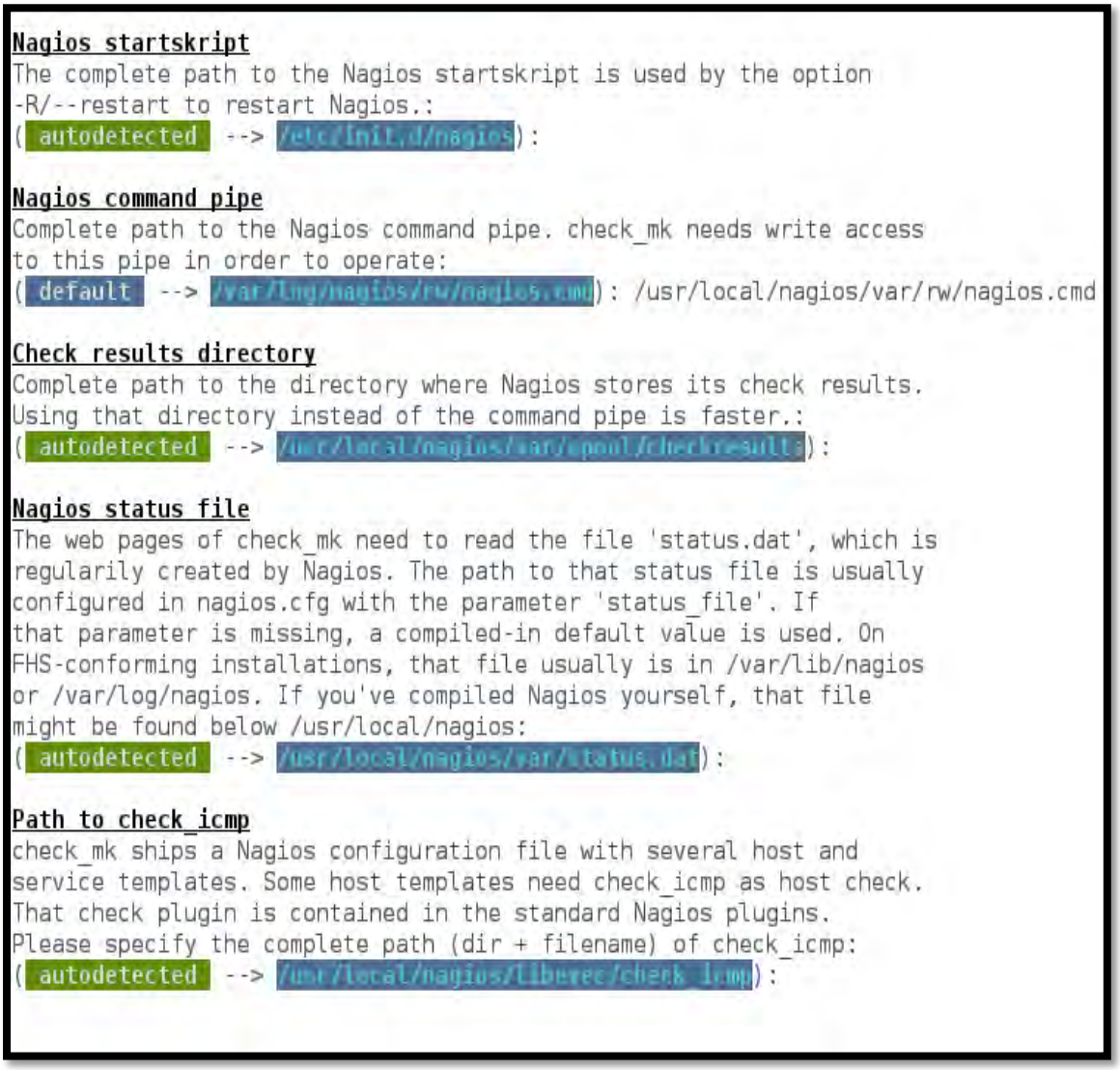


Figura ACH 6. Definición de rutas de instalación.



Figura ACH 7. Definición de rutas de instalación.

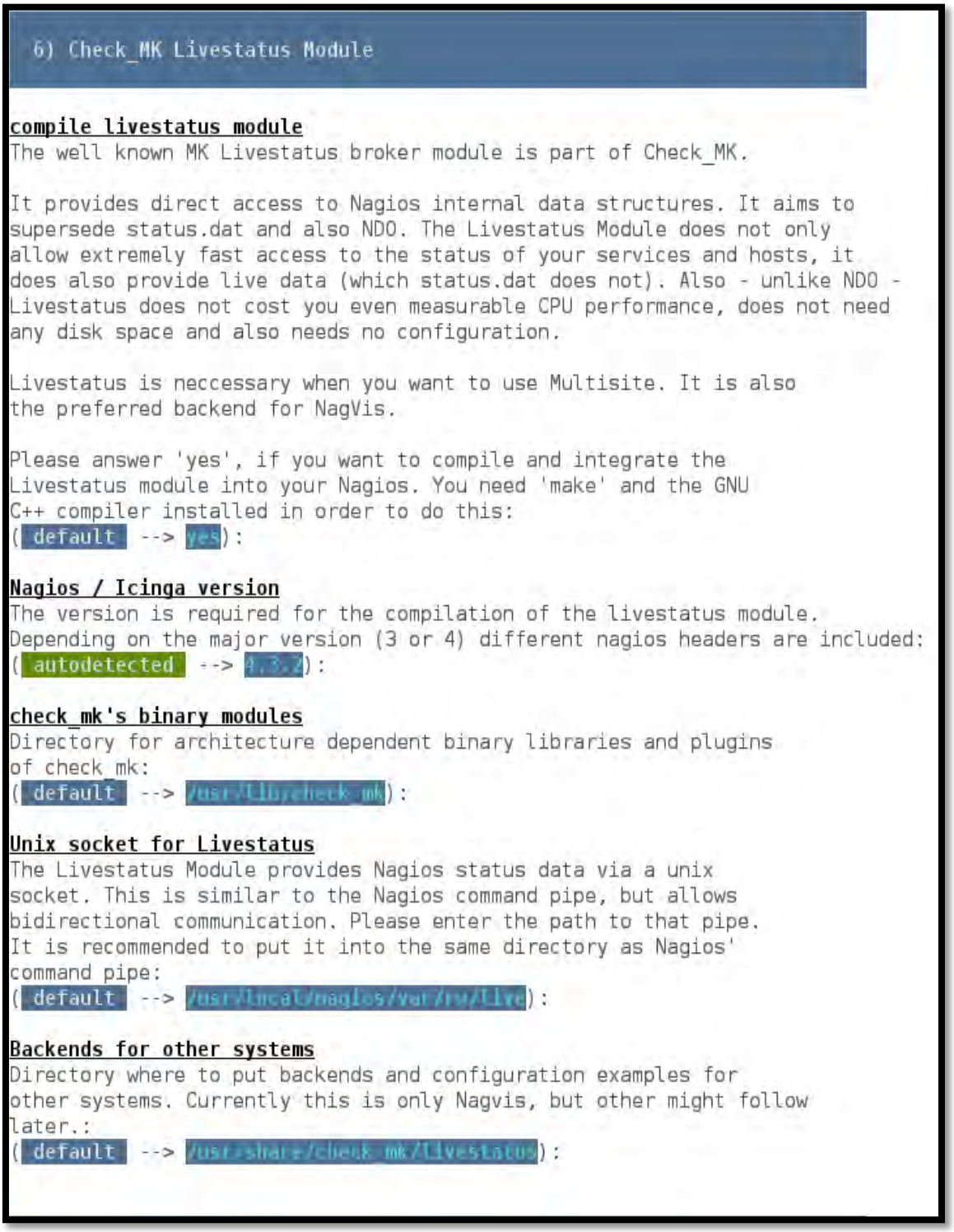


Figura ACH 8. Definición de rutas de instalación.



Figura ACH 9. Definición de rutas de instalación

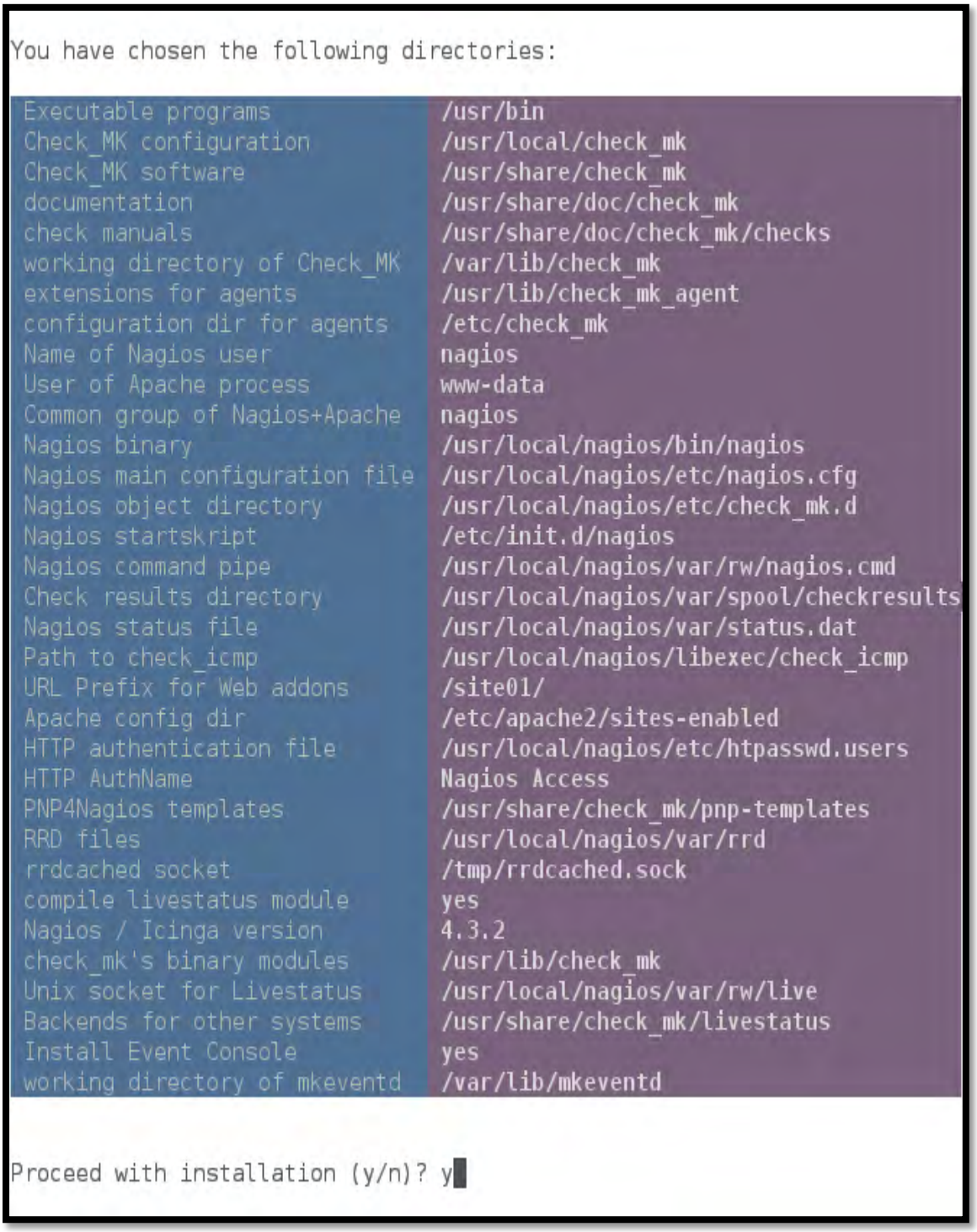


Figura ACH 10. Definición de rutas de instalación.

Se reinicia este servicio.

```
/etc/init.d/mkeventd restart
```

Actualización versión de PNP4Nagios: para mas información sobre este tema visitar (Linge, 2012).

Se descarga desde la fuente.

```
cd /tmp
wget -O pnp4nagios-0.6.26.tar.gz
https://sourceforge.net/projects/pnp4nagios/files/latest/download
```

Se descomprime y se compila.

```
tar zxfv pnp4nagios-0.6.26.tar.gz
cd pnp4nagios-0.6.26/
./configure --with-httpd-conf=/etc/apache2/sites-enabled   --
sysconfdir=/usr/local/pnp4nagios --with-base-url=/site01/pnp4nagios
```

Se ejecutan los siguientes comandos:

```
make all
make fullinstall
```

Es necesario eliminar el archivo “install.php”, para que se muestren las gráficas.

```
rm /usr/local/pnp4nagios/share/install.php
```

Se reinicia el servicio.

```
/etc/init.d/npcd restart
```

Actualización versión de Nagvis: para mas información sobre este tema visitar (Nagvis.org, 2013).

Se descarga desde la fuente.

```
cd /tmp
wget -O nagvis-1.9.5.tar.gz http://www.nagvis.org/share/nagvis-1.9.5.tar.gz
```

Se descomprime y se compila.

```
tar xvzf nagvis-1.9.5.tar.gz
cd nagvis-1.9.5
./install.sh
```

Se Dejan todas las opciones por defecto dando enter.

Al finalizar la instalación aparecerá lo siguiente:

```
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/nagios -p /usr/local/nagvis -l
"unix:/usr/local/nagios/var/rw/live" -b mklivestatus -u www-data -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/nagvis/etc/nagvis.ini.php
| - Configure NagVis via browser
|   <http://localhost/site01/nagvis/config.php>
| - Initial admin credentials:
|     Username: admin
|     Password: admin
```

Se reinicia el servicio de apache.

```
/etc/init.d/apache2 restart
```

9.9 INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR ESPEJO

9.9.1 Instalación y configuración de la herramienta rsync con ssh. Para tener el servicio de monitoreo siempre disponible se realizó un servidor espejo del servidor original, si hay un problema en elservidor original se puede colocar en funcionamiento el servidpr espejo mientras se solucionan las fallas.

Medinte Rsync se pudo lograr el objetivo de tener en funcionmiento el servidor espejo.

Rsync para transferir archivos bajo Linux: para mas información sobre Rsync visitar (nixCraft, 2017).

Se llama:

PC1 = al servidor donde está alojado Nagios, servidor principal, al que se le realizara la réplica.

PC2 = al servidor espejo, este va a ser el servidor de respaldo del servidor principal Nagios.

Todo en este tutorial tanto en PC1 como en PC2 se realizó como súper usuario.

```
Su
```

Rsync y ssh deben estar instalados en PC1 y PC2.

```
apt-get update
apt-get install rsync
apt-get install openssh-server openssh-client
```

Rsync no proporciona ninguna seguridad durante la transferencia de datos, se recomienda utilizar rsync en la sesión ssh. Esto permite una conexión remota segura.

Configuración conexión ssh sin password: para mas información sobre configuración de SSH visitar (Toro, 2000).

Se ingresa el siguiente comando en el servidor PC1 para crear las keys pública y privada.

```
ssh-keygen -b 4096 -t rsa
```

Mostrará algo como esto:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
0a:94:43:ac:8f:f2:0d:a2:9a:d0:f8:60:4f:9b:74:d9 root@debian1205
The key's randomart image is:
+---[RSA 4096]----+
|   ..            |
|   ...           |
|   .+            |
|  .. .           |
|   o.   S        |
```

```
|ooo ..o.                 |
|==.= o.E                 |
|++= =                    |
|+ .+                     |
+--------------------+
```

Se da enter a todas las opciones.

Luego en el servidor PC2 se habilita el permiso de acceso como root mediante ssh.

En el archivo *sshd_config* que se encuentra en la ruta */etc/ssh/*

```
nano /etc/ssh/sshd_config
```

Se edita lo siguiente:

```
.
.
.
# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes

RSAAuthentication yes
.
.
.
```

Por:

```
# Authentication:
LoginGraceTime 120
#PermitRootLogin without-password
PermitRootLogin yes
AllowUsers root@ip_servidor_principal
StrictModes yes

RSAAuthentication yes
```

Se reinicia el servicio ssh.

```
service ssh restart
```

Una vez se cambian los permisos en PC2 se procede a enviar la llave pública desde PC1.

```
ssh-copy-id root@ip_servidor_espejo
```

Aparecerá algo como lo siguiente. Donde se coloca el password de root de PC2.

```
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.170.123's password:
```

Una vez ingresado el password aparecera lo siguiente:

```
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.170.123'"
and check to make sure that only the key(s) you wanted were added.
```

Opciones de comando rsync de Comman:

--delete: Eliminar los archivos que no existen en el remitente (sistema).
-v: Verbose (intente -vvpara obtener información más detallada).
-e "ssh options”: Especifica el shell ssh como remoto.
-a: Modo de archivo.
-r: Recurse en directorios.
-z: Comprimir datos de archivo.

Script para sincronización de los servidores desde pc1: se ingresa como root y se ingresa la contraseña, ubicandose en la raíz.

```
su
cd
```

En la terminal se escribe lo siguiente:

```
cd $HOME && touch script.sh && chmod +x script.sh
```

Creará el script en la carpeta personal.

Luego se ingresa el siguiente comando:

```
cd $HOME && echo '#!/usr//bin/expect' > script.sh && echo '# -*- ENCODING: UTF-8 -*-' >> script.sh
```

Antes de editar el script es necesario instalar *expect.* Para esto se ingresa el siguiente comando:

```
apt-get install expect
```

Posteriormente se edita el script.sh.

```
cd
nano script.sh
```

Para el siguiente script se tomó como referencia el script encontrado en (Aceror, 2011).

Nota: El script fue editado mediante investigación realizada por los integrantes de este trabajo, para cumplir con el objetivo de hacer la replica espejo del servidor que contiene la suite de monitoreo.

Quedando de la siguiente manera:

```
#!/usr/bin/expect
# -*- ENCODING: UTF-8 -*-

  #La linea de arriba indica donde esta el programa expect
  spawn ssh root@192.168.170.123
  #Ahora sabemos que nos preguntará por el password del
  #usuario que hemos indicado
#!/usr/bin/expect
# -*-ENCODING: UTF-8-*-
# La linea de arriba indica donde esta el programa expect
#La linea de arriba indica donde esta el programa expect
spawn ssh root@192.168.170.251
#Ahora sabemos que nos preguntarÃ¡ por el password del
#usuario que hemos indicado
expect "*?assword:*"
#Ahora le enviamos los comandos que como root queremos
```

```
#que se ejecuten
send "systemctl stop nagios.service\r"
send "systemctl stop mkeventd.service\r"
send "systemctl stop npcd.service\r"
send "systemctl stop apache2.service\r"
#Cuando hemos terminado mandamos el comando exit para que
#salga
send "exit\r"
expect eof
#En las siguientes lineas se realiza la sincronizacion de los directorios
#del servidor remoto con el servidor local
#spawn rsync -rave "ssh -l root" --delete /usr/local/ 192.168.170.254:/usr/local/
#spawn rsync -rave "ssh -l root" --delete /usr/share/check_mk/
192.168.170.254:/usr/share/check_mk/
#spawn rsync -rave "ssh -l root" --delete /usr/share/doc/check_mk/
192.168.170.254:/usr/share/doc/check_mk/
#spawn rsync -rave "ssh -l root" --delete /usr/lib/check_mk/
192.168.170.254:/usr/lib/check_mk/
#spawn rsync -rave "ssh -l root" --delete /var/lib/check_mk/
192.168.170.254:/var/lib/check_mk/

spawn rsync -ravhe "ssh -l root" --delete /usr/local/check_mk/
192.168.170.251:/usr/local/check_mk/
spawn rsync -ravhe "ssh -l root" --delete /usr/local/pnp4nagios/
192.168.170.251:/usr/local/pnp4nagios/
spawn rsync -ravhe "ssh -l root" --delete /usr/local/nagios/
192.168.170.251:/usr/local/nagios/
spawn rsync -ravhe "ssh -l root" --delete /usr/local/nagvis/
192.168.170.251:/usr/local/nagvis/
spawn rsync -ravhe "ssh -l root" --delete /usr/local/ 192.168.170.251:/usr/local/
spawn rsync -ravhe "ssh -l root" --delete /usr/share/check_mk/
192.168.170.251:/usr/share/check_mk/
spawn rsync -ravhe "ssh -l root" --delete /usr/share/doc/check_mk/
192.168.170.251:/usr/share/doc/check_mk/
spawn rsync -ravhe "ssh -l root" --delete /usr/lib/check_mk/
192.168.170.251:/usr/lib/check_mk/
spawn rsync -ravhe "ssh -l root" --delete /var/lib/check_mk/
192.168.170.251:/var/lib/check_mk/
spawn ssh root@192.168.170.251
#Ahora sabemos que nos preguntarÃ¡ por el password del
#usuario que hemos indicado
expect "*?assword:*"
#Ahora le enviamos los comandos que como root queremos
#que se ejecuten
```

```
send "systemctl start nagios.service\r"
send "systemctl start mkeventd.service\r"
send "systemctl start npcd.service\r"
send "systemctl start apache2.service\r"
#Cuando hemos terminado mandamos el comando exit para que
#salga
send "exit\r"
expect eof
```

Nota: la dirección IP 192.168.170.123 se debe cambiar por la dirección IP del servidor espejo al cual se le va a realizar la réplica.

Ejecución del script con administrador de tareas crontab desde PC1: para mas información sobre crontab visitar (Geeky Theory, 2017).

Para observar que tareas se están ejecutando en crontab, se ingresa la siguiente línea:

```
sudo crontab -l
```

Para editar el contenido se ingresa el siguiente comando:

```
sudo crontab -e
```

Se programa la tarea, la cual va a ejecutar el script. Por ejemplo, el script se ejecutará de lunes a viernes cada 10 minutos.

La siguiente línea se coloca al final del archivo.

```
*/15 * * * 1-5 /root/script.sh
```

9.10 MANUAL DE FUNCIONAMIENTO DE CHECK_MK

Se realiza un manual de funcionamiento de la herramienta Check_Mk, debido a que es la herramienta que tiene más contacto con el usuario y requiere de un conocimiento mayor para su configuración y uso.

Dentro de la interface web de la herramienta de administración Check_Mk, se encuentra un área de navegación para acceder a las páginas oficiales de las cuatro herramientas que componen la suite de monitoreo, donde se encuentra toda la información necesaria para dar un buen uso de la suite implementada.

Para detallar el manual de funcionamiento mirar el

Anexo R. Manual Check_MK.

9.11 CAPACITACIÓN AL PERSONAL DEL ÁREA DE SISTEMAS

La capacitación de la suite de monitoreo se la realizó el dia 25 de enero de 2018 con el personal del área de sistemas que va a hacer uso de la suite. A la capacitación asistieron: ingeniero jefe del área de sistemas, ingeniero de telecomunicaciones, auxiliar de sistemas y el administrador desarrollador.

La duración de la capacitación fue de cuatro (4) horas, en donde se obtuvo un acta de capacitación la cual se encuentra en el Anexo S. Acta de capacitación personal área de sistemas. En esta se describe el objetivo de la capacitación y los temas tratados.



Figura CP 1. Imagen capacitación a personal del área de sistemas.



Figura CP 2. Imagen capacitación a personal del área de sistemas



Figura CP 3. Imagen capacitación a personal del área de sistemas.

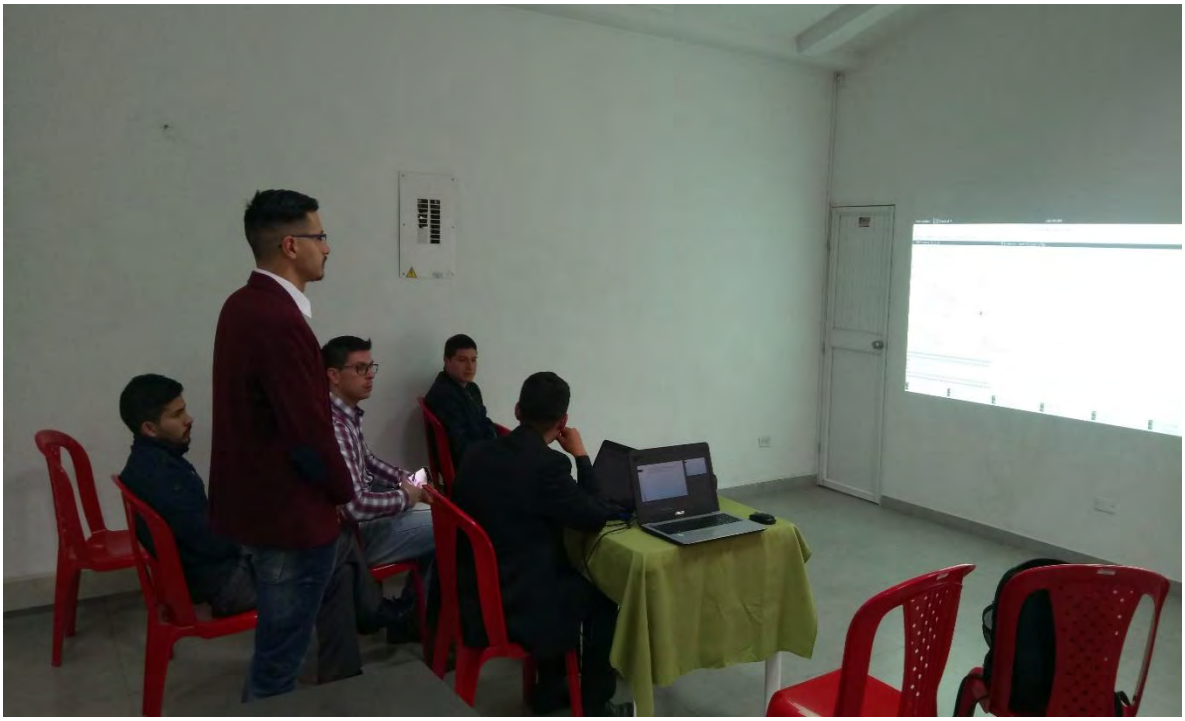


Figura CP 4. Imagen capacitación a personal del área de sistemas.

10. CONCLUSIONES

Mediante la implementación de la suite de monitoreo se logró cumplir el objetivo de brindar una herramienta de gestión a la red de datos de la empresa Electromillonaria, contribuyendo a la toma de decisiones, mejorando la calidad de su servicio.

Se cumplieron los objetivos planteados, obteniendo los resultados esperados.

El análisis de la red de datos da a conocer la necesidad que tienen las empresas de implementar herramientas que realicen un monitoreo continuo de sus componentes de red, para tener sus servicios siempre disponibles.

Para el desarrollo del trabajo se tomó como referencia una metodología de administración de redes de datos con el fin de obtener los resultados esperados planteados en el trabajo.

Se investigaron diferentes herramientas de monitoreo para cumplir los objetivos planteados para la empresa Electromillonaria. Por lo que se eligió la herramienta Nagios, al ser la más completa y tener la capacidad de ser potenciada por otras herramientas, logrando mejores resultados.

La suite de monitoreo está compuesta por herramientas desarrolladas bajo código abierto lo que permite mejorar su funcionamiento, por ejemplo, el desarrollo de plugins.

La suite de monitoreo tiene una interface web que permite una interacción directa entre el usuario y las herramientas, facilitando la configuración y visualización de los resultados del monitoreo a través de múltiples vistas y reportes.

Debido a la fácil escalabilidad de la suite de monitoreo, es posible que la empresa Electromillonaria monitoree todos los componentes de red, incluyendo las agencias sin importar su ubicación geográfica.

11. RECOMENDACIONES

Implementar la suite de monitoreo en sus últimas versiones y se utilizó los plugins requeridos hasta el momento. Sin embargo, es necesario sugerir algunas recomendaciones para tener en pleno funcionamiento la suite de monitoreo:

Conocer a profundidad las herramientas que componen la suite de monitoreo, debido a que estas cuentan con una gran cantidad de opciones que no fueron estudiadas durante el desarrollo del trabajo.

Conocer el manejo de plugins, debido a que estos permiten el monitoreo de múltiples servicios.

Tener actualizadas las versiones de las herramientas que componen la suite de monitoreo. Se recomienda que la empresa monitoree los servicios de red a través de Nagios.

Mantener actualizado el diagrama lógico y físico de la red de datos.

Tomar decisiones de acuerdo al análisis de la red de datos y los reportes obtenidos del monitoreo.

Instalar los agentes en los equipos cuando son formateados, e instalarlo en los nuevos componentes de la red de datos.

REFERENCIAS BIBLIOGRAFICAS

ESnet / Lawrence Berkeley National Laboratory. (23 de 06 de 2016). Iperf.fr. Obtenido de Iperf.fr: https://iperf.fr/

Sørensen, S. (2 de Diciembre de 2013). LO4D.COM . Obtenido de LO4D.COM : http://free-ip-tools.en.lo4d.com/

Aceror. (12 de Agosto de 2011). BLOG DE UN ADMINISTRADOR DE REDES LINUX. Obtenido de BLOG DE UN ADMINISTRADOR DE REDES LINUX: http://aceror.blogspot.com.co/2011/08/comandos-ssh-remotos-automaticos.html?m=1

Acuña Garcia, E., & Caicedo Urresta, V. M. (02 de 02 de 2017). Repositorio digital Universidad Técnica de Ambato. Recuperado el 02 de 02 de 2017, de http://repositorio.uta.edu.ec/bitstream/123456789/326/3/Tesis_t167si.pdf

Alvarez Cevallos, A. (01 de 04 de 2015). Repositorio digital Universidad Politécnica Salesiana Ecuador . Recuperado el 25 de 02 de 2017, de http://dspace.ups.edu.ec/bitstream/123456789/10298/1/UPS-GT001194.pdf

Arellano Ruiz, J. F., & Cuasquer Viveros, D. A. (01 de 01 de 2007). Biblioteca virtual Alverto Quijano Guerrero. Obtenido de Biblioteca virtual Alverto Quijano Guerrero: http://biblioteca.udenar.edu.co:8085/bibliotecavirtual/viewer.aspx?&var=70963

Black Duck Software, Inc. . (01 de 01 de 2013). Nagvis. Obtenido de Nagvis: http://nagvis.org/

Botero Arana, N. (01 de Junio de 2005). Pontificia Universidad Javeriana Bogotá. Obtenido de Pontificia Universidad Javeriana Bogotá: http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf

Cacti Group, Inc. (01 de 01 de 2017). Cacti the complite rrdtool based graphing solution. Obtenido de Cacti the complite rrdtool based graphing solution: http://cacti.net/

Cayuqueo, S. D. (14 de 07 de 2016). Cayu - Wiki de Sergio Cayuqueo. Recuperado el 02 de 02 de 2017, de http://cayu.com.ar/files/manuales-nagios.pdf

Combs, G. (2017 de Noviembre de 11). WIRESHARK. Obtenido de WIRESHARK: https://www.wireshark.org/

Cortazar Mejia, A., & Galindo Alvarez, L. A. (01 de 01 de 2009). Biblioteca virtual de UTB (Universidad Tecnologica de Bolivar). Recuperado el 017 de 02 de 27, de http://biblioteca.unitecnologica.edu.co/notas/tesis/0053945.pdf

de la fuente, T. (01 de 01 de 2017). https://blyx.com/. Recuperado el 6 de 02 de 2017, de https://blyx.com/public/docs/pila_OSI.pdf

Domínguez Dorado, M., & Zarandieta Morán, J. A. (01 de 05 de 2003). Manuel Domínguez Dorado ingeniería informática y dirección de proyectos. Obtenido de Manuel Domínguez Dorado ingeniería informática y dirección de proyectos: http://www.manolodominguez.com/wp-content/uploads/2016/10/20161007-M_Dominguez_Dorado-EvaluacionNagios1.pdf

Duque Padilla, A. S. (101 de 01 de 2011). Biblioteca virtual Universidad Católica de Pereira CDCH. Obtenido de Biblioteca virtual Universidad Católica de Pereira CDCH: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/3007/CDPEIST61.pdf?sequence=1

El blog educativo. (15 de Junio de 2017). Redes-Amenazas de internet. Obtenido de Redes-Amenazas de internet: https://charxavier.wordpress.com/redes-amenazas-de-internet-y-seguridad-en-redes/

FITEC Institucion de educacion superior. (01 de 01 de 2017). Tecnologia FITEC Institucion de educacion superior. Recuperado el 27 de 02 de 2017, de https://csudp.wikispaces.com/file/view/Topologias+de+Red.pdf

Forouzan, B. A. (2007). Transmisión de datos y redes de comunicaciones. Madrid: McGraw-hill/Interamericana de España S.A.U.

geekland . (1 de Enero de 2018). Instalar servidor LAMP. Obtenido de Instalar servidor LAMP: https://geekland.eu/instalar-un-servidor-web-lamp/

Geeky Theory. (11 de Junio de 2017). Aprende programación, desarrollo web y mucho más. Obtenido de Aprende programación, desarrollo web y mucho más: https://geekytheory.com/programar-tareas-en-linux-usando-crontab

Halsall, F. (1998). Comunicación de datos, redes de computadores y sistemas abiertos. Naucalpan de Juárez: Pearson educación.

JL Y RB S.A.S – ELECTROMILLONARIA. (10 de 08 de 2017). Electromillonaria. Obtenido de Electromillonaria: electromillonaria.co

Kettner GmbH, M. (25 de Octubre de 2017). MK Mathias Kettner. Obtenido de MK Mathias Kettner: http://mathias-kettner.com/index.html

Kettner, M. (26 de 09 de 2017). MK Mathias Kettner. Obtenido de MK Mathias Kettner: http://mathias-kettner.de/check_mk.html

Leon Garcia, A., & Widjaja, I. (2002). Redes de comunicación. Madrid: McGraw-Hill/Interamericana de España, S.A.U.

Linge, J. (15 de Marzo de 2012). PNP4Nagios. Obtenido de PNP4Nagios: http://docs.pnp4nagios.org/es/pnp-0.6/start

López, Á., & Novo, A. (2000). Protocolos de Internet diseño e implementacion en sistemas UNIX. Mexico D.F.: Alfaomega grupo editor , S.A. de C.V.

Macías Ríos, E., Rentería Anguiano, E., & Rangel Licea, V. (10 de 2009). Paginas personales en la web. Recuperado el 02 de 02 de 2017, de http://profesores.fi-b.unam.mx/victor/CCNA/Productos/Notas%20de%20Curso/Manual%20de%20la%20Asignatura%20de%20Redes%20de%20Datos%20I%20y%20II%20%20(avance%2050%25).pdf

Martínez Ramírez, S. (01 de 01 de 2016). Repositorio digital de la Facultad de Ingeniería - UNAM. Recuperado el 24 de 02 de 2017, de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/10527/Tesina.pdf?sequence=1

Mifsud Talón, E., & Lerma Blasco, R. (01 de Abril de 2013). Servicios en red. Mexico D.F, Mexico.

Monitoring Plugins Development Team. (15 de 03 de 2012). PNP4 NAGIOS. Obtenido de PNP4 NAGIOS: http://docs.pnp4nagios.org/es/pnp-0.6/start

Munin org. (22 de 01 de 2017). MUNIN. Obtenido de MUNIN: http://munin-monitoring.org/

Nagios Core. (01 de Enero de 2017). Host Checks. Obtenido de Host Checks: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/hostchecks.html

Nagios org. (01 de 01 de 2017). Nagios. Obtenido de Nagios: https://www.nagios.org/documentation/

Nagvis.org. (01 de Enero de 2013). Nagvis. Obtenido de Nagvis: http://nagvis.org/

nixCraft. (12 de Mayo de 2017). nixCraft. Obtenido de nixCraft: https://www.cyberciti.biz/tips/linux-use-rsync-transfer-mirror-files-directories.html

Ookla. (12 de Diciembre de 2017). SPEEDTEST. Obtenido de SPEEDTEST: http://www.speedtest.net/es

ORACLE. (01 de 01 de 2017). ORACLE help center. Recuperado el 02 de 02 de 2017, de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html

Pandora org. (01 de 01 de 2017). Pandora fms community. Obtenido de Pandora fms community: https://pandorafms.org/es/producto/introduccion-a-pandora-fms/

Primantech. (08 de 05 de 2012). PrimanTech Blog dedicado a la divulgación y ayuda sobre el mundo de las TIC. Obtenido de PrimanTech Blog dedicado a la divulgación y ayuda sobre el mundo de las TIC: http://primantech.blogspot.com.co/2012/05/nagios-instalacion-en-centos.html

Primo Guijarro, Á. (2012 de Febrero de 23). Servcios de mensajería instantanea. Ciudad Real, España.

S. Tanenbaum, A. (02 de 02 de 2017). Google academico. Recuperado el 02 de 02 de 2017, de https://books.google.es/books?hl=es&lr=&id=WWD-4oF9hjEC&oi=fnd&pg=PR18&dq=modelo+osi+capa&ots=XykbU9p6Ga&sig=523h8yuonKY38ufAVVCbXkcsfiI#v=onepage&q=modelo%20osi%20capa&f=false

Schuber, M., Bennett, D., Gines, J., Hay, A., & Strand, J. (01 de 01 de 2008). Nagios. Obtenido de Nagios: https://www.nagios.org/downloads/nagios-core/

SENA (Servicio Nacional de Aprendizaje). (01 de 01 de 2017). SENA titulada. Obtenido de SENA titulada: https://senaintro.blackboard.com/bbcswebdav/institution/semillas/217219_1_VIRTUAL/OAAPs/OAAP1/aa1/oa_disp_activos/utilidades/descargable.pdf

Stallings, W. (2008). Comunicaciones y Redes de Computadores. Madrid (España): Pearson Educacion, S.A.

Tanenbaum, A., & Wetherall, D. (2012). Redes de computadoras. Naucalpan de Juárez, Estado de México: Pearson.

Tarlogic Security. (1 de Enero de 2017). ACRYLIC WiFi. Obtenido de ACRYLIC WiFi: https://www.acrylicwifi.com/en/wlan-software/wifi-analyzer-acrylic-professional/

Tekmikro. (01 de 01 de 2017). Programación de microcontroladores PIC en mikroC PRO. Obtenido de Programación de microcontroladores PIC en mikroC PRO: http://programarpicenc.com/articulos/ethernet-ieee-8023-y-el-modelo-osi/

Toro, L. (15 de Octubre de 20). DesdeLinux. Obtenido de DesdeLinux: https://blog.desdelinux.net/ssh-sin-password-solo-3-pasos/

Universidad de Oviedo. (03 de 02 de 2017). Universidad de Oviedo área de ingeniería de sistemas y automática. Recuperado el 03 de 02 de 2017, de http://www.isa.uniovi.es/docencia/redes/Apuntes/tema5.pdf

Untiveros, S. (01 de 07 de 2004). AprendaRedes.com. Recuperado el 20 de 02 de 2017, de http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

Zabbix LLC. (01 de 01 de 2017). Zabbix. Obtenido de Zabbix: http://www.zabbix.com/

Zuleta Londoño, M. Á. (01 de 01 de 2013). Biblioteca virtual Universidad Católica de Pereira CDCH. Obtenido de Biblioteca virtual Universidad Católica de Pereira CDCH: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/2000/DDPAIST36.pdf?sequence=1

Anexos

Anexo A. Información de equipos.

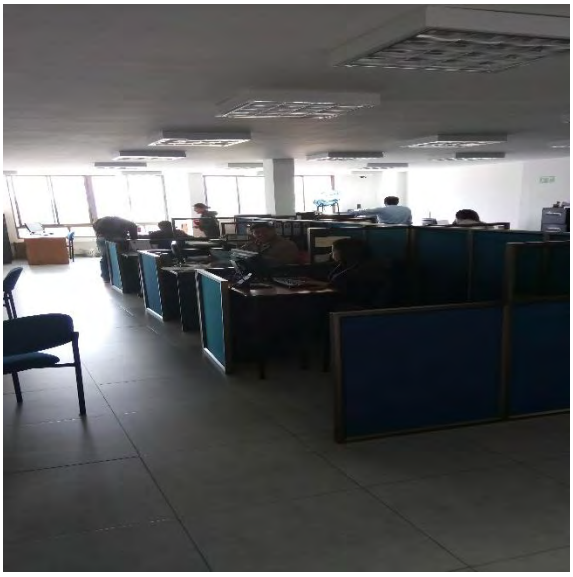
ÍNDICE

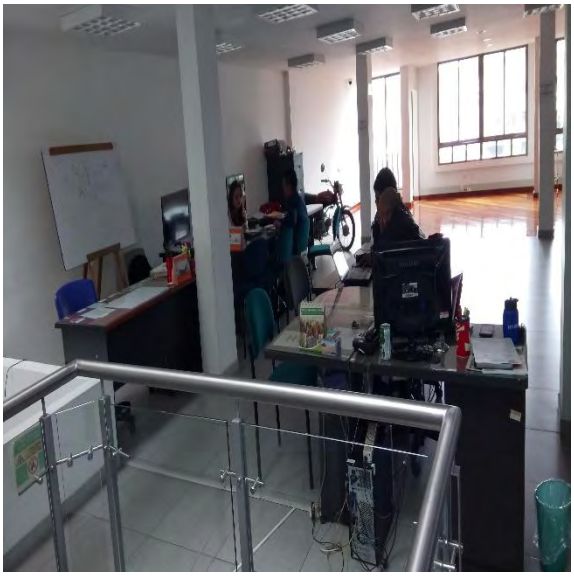
Pág.

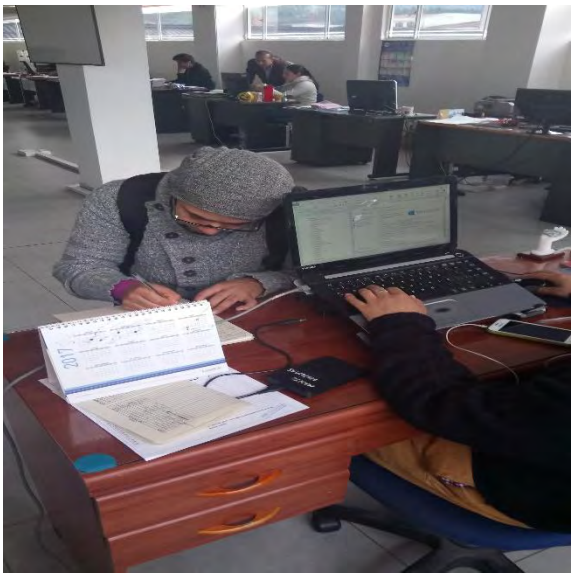
1. FOTOS RECOLECCIÓN DE INFORMACIÓN 241
2. EQUIPOS ÁREA DE ADMINISTRACIÓN 242
3. EQUIPOS ÁREA DE FACTURACIÓN 243
4. EQUIPOS ÁREA DE JURÍDICO 244
5. EQUIPOS ÁREA DE CARTERA 246
6. EQUIPOS ÁREA DE SISTEMAS 250
7. EQUIPOS ÁREA COMERCIAL 252
8. EQUIPOS ÁREA DE GERENCIA 254
9. EQUIPOS ÁREA DE CONTABILIDAD 254
10. EQUIPOS ÁREA DE REVISORÍA 257
11. EQUIPOS ÁREA INTERELEC 261
12. EQUIPOS ÁREA FONDELEC 262
13. EQUIPOS ÁREA DE PUBLICIDAD 263
14. EQUIPOS AGENCIA KEEWAY AMERICAS 263
15. EQUIPOS AGENCIA ELECTROMILLONARIA CARRERA 20 264
16. EQUIPOS AGENCIA KEEWAY CALLE 17 265
17. EQUIPOS AGENCIA ELECTROMILLONARIA CALLE 17 265
18. EQUIPOS AGENCIA ELECTROMILLONARIA CARRERA 25 265
19. EQUIPOS AGENCIA ELECTROMILLONARIA CARRERA 24 266
20. EQUIPOS AGENCIA ELECTROMILLONARIA CALLE 19 266
21. EQUIPOS AGENCIA BODEGA PRINCIPAL 268
22. EQUIPOS AGENCIA ELECTROMILLONARIA LAS LUNAS 270
23. RADIO ENLACES UBIQUITI 270
24. ROUTER PRINCIPAL ELECTROMILLONARIA 271
25. SERVIDORES DE RED ELECTROMILLONARIA 271
26. IMPRESORAS MULTIFUNCIONALES 272

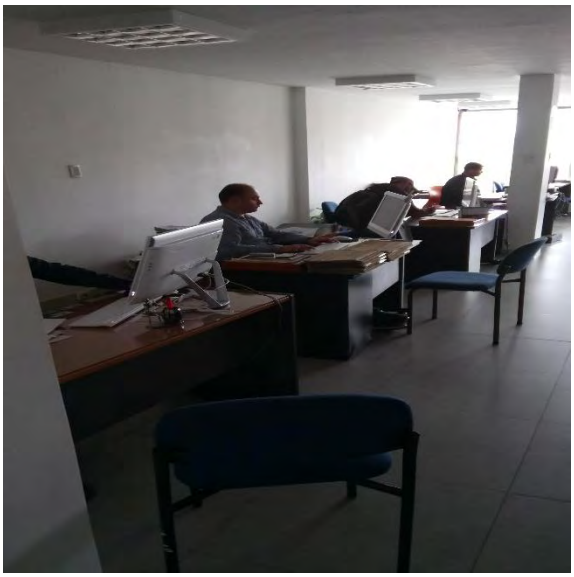
1. FOTOS RECOLECCIÓN DE INFORMACIÓN

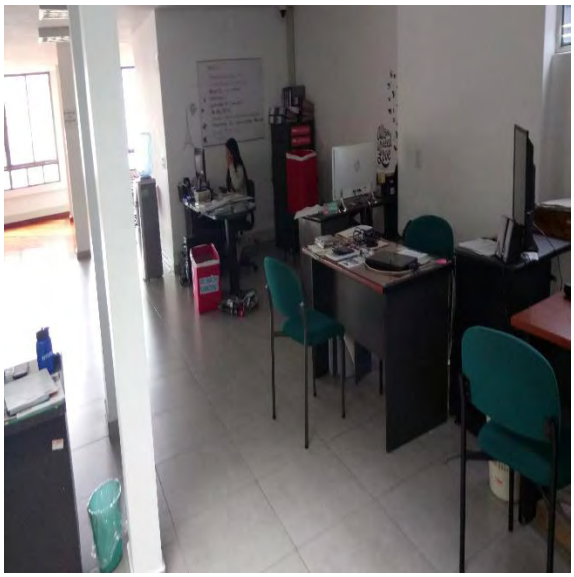












2. EQUIPOS ÁREA DE ADMINISTRACIÓN

DEPARTAMENTO ADMINISTRACION	
AREA	TALENTO HUMANO
ENCARGADO	
NOMBRE DE EQUIPO	SALUDOCUPA
GRUPO DE TRABAJO	ADMINISTRACION
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL PENTIUM CPU 3.0GHZ
MEMORIA RAM	1 GB
DISCO DURO	150 GB
IP	192.168.170.58
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO ADMINISTRACION	
AREA	RECURSOS HUMANOS
ENCARGADO	JHOANA MUÑOZ
NOMBRE DE EQUIPO	auxthumano
GRUPO DE TRABAJO	ADMINISTRACION
SISTEMA OPERATIVO	XP PROFESIONAL 2002 SERVIPACK
PROCESADOR	INTEL CELERON CPU 2.53GHZ
MEMORIA RAM	1GB
DISCO DURO	80GB
IP	192.168.170.60
MASCARA DE RED	24

GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO ADMINISTRACION	
AREA	RECURSO HUMANOS
ENCARGADO	JHOANA MUÑOZ
NOMBRE DE EQUIPO	coortalentoh
GRUPO DE TRABAJO	ADMINISTRACION
SISTEMA OPERATIVO	WINDOWS 7 PROFESIONAL
PROCESADOR	CORE i5 4ta generación 2.30GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.170.55
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6
DEPARTAMENTO ADMINISTRACION	
AREA	RECEPCION
ENCARGADO	LUIS ARMANDO LOPEZ
NOMBRE DE EQUIPO	auxrecursosh
GRUPO DE TRABAJO	ADMINISTRACION
SISTEMA OPERATIVO	XP PROFESIONAL 2002 SERVIPACK
PROCESADOR	INTEL CELERON 1.75GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.170.57
MASCARA DE RED	16
GATEWAY	192.168.170.1
DNS	192.168.170.6

3. EQUIPOS ÁREA DE FACTURACIÓN

DEPARTAMENTO FACTURACION	
AREA	FACTURACION
ENCARGADO	
NOMBRE DE EQUIPO	HOSTFACT
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 PROFESIONAL
PROCESADOR	INTEL CORE i5 2320 CPU 3.0GHZ
MEMORIA RAM	4GB
DISCO DURO	250GB
IP	192.168.170.42

MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO FACTURACION	
AREA	FACTURACION
ENCARGADO	
NOMBRE DE EQUIPO	Factcoor
GRUPO DE TRABAJO	INICIOMS
SISTEMA OPERATIVO	XP PROFESIONAL 2002 SERVIPACK
PROCESADOR	INTEL PENTIUM DUAL CPU 2.0 GHZ
MEMORIA RAM	1GB
DISCO DURO	150GB
IP	192.168.170.38
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6
DEPARTAMENTO FACTURACION	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	auxcartera1_pc
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	AMD E1-1500 1.48GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.37
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

4. EQUIPOS ÁREA DE JURÍDICO

DEPARTAMENTO JURIDICO	
AREA	JURIDICO
ENCARGADO	
NOMBRE DE EQUIPO	juridicoabg1
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i3 5ta generacion
MEMORIA RAM	4GB

DISCO DURO	500GB
IP	192.168.170.51
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6
DEPARTAMENTO JURIDICO	
AREA	JURIDICO
ENCARGADO	
NOMBRE DE EQUIPO	juridicosecre
GRUPO DE TRABAJO	JURIDICO
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i5 5tageneracion
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.49
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6
DEPARTAMENTO JURIDICO	
AREA	JURIDICO
ENCARGADO	ANDREA MARTINEZ
NOMBRE DE EQUIPO	juridicoabg2
GRUPO DE TRABAJO	JURIDICO
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i3 5ta generación
MEMORIA RAM	4 GB
DISCO DURO	500GB
IP	192.168.170.52
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO JURIDICO	
AREA	JURIDICO
ENCARGADO	
NOMBRE DE EQUIPO	USUARIO-PC
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 HOME PREMIUM
PROCESADOR	CORE i5 CPU 2.40GHZ
MEMORIA RAM	4GB
DISCO DURO	700GB
IP	192.168.170.50
MASCARA DE RED	24

GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO JURIDICO	
AREA	JURIDICO
ENCARGADO	
NOMBRE DE EQUIPO	juridicoABG3
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i3 5ta generación CPU 1.7GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.170.53
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

5. EQUIPOS ÁREA DE CARTERA

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	auxcart3
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 PROFESIONAL
PROCESADOR	AMD SEMPRON 2.21GHZ
MEMORIA RAM	2GB
DISCO DURO	150GB
IP	192.168.170.35
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	Kwyjfcart
GRUPO DE TRABAJO	KEEWAY
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON CPU 1.10GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB

IP	192.168.170.46
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	fernando_eraso
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 HOME BASIC
PROCESADOR	CORE i3 4ta generación CPU 2.53GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.170.143
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	TESORERIA
ENCARGADO	MARGARITA LOPEZ
NOMBRE DE EQUIPO	tesorería
GRUPO DE TRABAJO	ADMINISTRACION
SISTEMA OPERATIVO	WINDOWS 7 STARTER
PROCESADOR	PENTIUM DUAL CORE CPU 3.20 GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.43
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	TESORERIA
ENCARGADO	
NOMBRE DE EQUIPO	cajacobrador
GRUPO DE TRABAJO	CARTERA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	AMD CPU 1.48GHZ
MEMORIA RAM	2GB

DISCO DURO	100GB
IP	192.168.170.44
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	ASISCARKEEWAY
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	XP PROFESIONAL 2002
PROCESADOR	INTEL CELERON CPU 2.0GHZ
MEMORIA RAM	1GB
DISCO DURO	300GB
IP	192.168.170.45
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	asistcadcvalle
GRUPO DE TRABAJO	CARTERA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	AMD ATLON CPU 2.50GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.170.201
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	KEEWAYAUXCART
GRUPO DE TRABAJO	CARTERA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL ATOM CPU 1.66GHZ
MEMORIA RAM	1GB
DISCO DURO	150GB

IP	192.168.170.48
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	
NOMBRE DE EQUIPO	asiscartpasto
GRUPO DE TRABAJO	CARTERA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTAL ATOM CPU 1.66
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.31
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	FERNANDO ERASO
NOMBRE DE EQUIPO	carteracooradc
GRUPO DE TRABAJO	CARTERA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL PENTIUM DUAL CORE CPU 3.0GHZ
MEMORIA RAM	3GB
DISCO DURO	300GB
IP	192.168.170.150
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CARTERA	
AREA	CARTERA
ENCARGADO	FERNANDO ERASO
NOMBRE DE EQUIPO	MPSCARTERA
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	MULTIPOIN SERVER 2011
PROCESADOR	INTEL CORE i7 CPU 3.40GHZ

MEMORIA RAM	6GB
DISCO DURO	500GB
IP	192.168.170.150
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

6. EQUIPOS ÁREA DE SISTEMAS

DEPARTAMENTO SISTEMAS	
AREA	SISTEMAS
ENCARGADO	GUSTAVO PEREZ
NOMBRE DE EQUIPO	soporte
GRUPO DE TRABAJO	SISTEMAS
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON 2.53GHZ
MEMORIA RAM	2GB
DISCO DURO	320GB
IP	192.168.170.17
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO SISTEMAS	
AREA	SISTEMAS
ENCARGADO	GUSTAVO PEREZ
NOMBRE DE EQUIPO	auxsistemas3
GRUPO DE TRABAJO	SISTEMAS
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i3 1.7GHZ
MEMORIA RAM	4GB
DISCO DURO	1 TB
IP	192.168.170.27
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO SISTEMAS	
AREA	SISTEMAS
ENCARGADO	GUSTAVO PEREZ
NOMBRE DE EQUIPO	capacitaciones
GRUPO DE TRABAJO	SISTEMAS

SISTEMA OPERATIVO	WINDOWS 7 SERVIPACK
PROCESADOR	INTEL CELERON 2.6GHZ
MEMORIA RAM	2GB
DISCO DURO	200GB
IP	192.168.170.26
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6
DEPARTAMENTO SISTEMAS	
AREA	SISTEMAS
ENCARGADO	GUSTAVO PEREZ
NOMBRE DE EQUIPO	ING_WIN_10
GRUPO DE TRABAJO	SISTEMAS
SISTEMA OPERATIVO	WINDOWS 10
PROCESADOR	CORE i5 3ra generación 2.6GHZ
MEMORIA RAM	6GB
DISCO DURO	720GB
IP	192.168.170.11
MASCARA DE RED	22
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO SISTEMAS	
AREA	SISTEMAS
ENCARGADO	GUSTAVO PEREZ
NOMBRE DE EQUIPO	SISTEMAS10
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS XP 2002 SRVIPACK
PROCESADOR	INTEL CELERON 1.6GHZ
MEMORIA RAM	2GB
DISCO DURO	80GB
IP	192.168.170.25
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO SISTEMAS	
AREA	SISTEMAS
ENCARGADO	GUSTAVO PEREZ
NOMBRE DE EQUIPO	sysadmin_Pc
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i5 4ta generación 2.5GHZ

MEMORIA RAM	6GB
DISCO DURO	500GB
IP	192.168.170.24
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

7. EQUIPOS ÁREA COMERCIAL

DEPARTAMENTO COMERCIAL	
AREA	MERCADEO Y PUBLICIDAD
ENCARGADO	MERY HELEN SANCHEZ
NOMBRE DE EQUIPO	comercialaux
GRUPO DE TRABAJO	COMERCIAL
SISTEMA OPERATIVO	WINDOWS XP PROFESIONAL
PROCESADOR	AMD ATLOM DUAL CORE 2.51GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.170.70
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO COMERCIAL	
AREA	COMPRAS
ENCARGADO	MARIA CONSTANZA TORRES
NOMBRE DE EQUIPO	compras01pt
GRUPO DE TRABAJO	COMERCIAL
SISTEMA OPERATIVO	WINDOWS 10 HOME
PROCESADOR	AMD CPU 1.80GHZ
MEMORIA RAM	8GB
DISCO DURO	1TB
IP	192.168.170.160
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO COMERCIAL	
AREA	COMPRAS
ENCARGADO	MARIA CONSTANZA TORRES
NOMBRE DE EQUIPO	asiscomercial2
GRUPO DE TRABAJO	ADMINCALLE19

SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CORE i3 4ta generación CPU 3.07GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.71
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO COMERCIAL	
AREA	COMPRAS
ENCARGADO	MARIA CONSTANZA TORRES
NOMBRE DE EQUIPO	inventarios
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CORE i3 3ra generación CPU 2.10GHZ
MEMORIA RAM	3GB
DISCO DURO	300GB
IP	192.168.170.146
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6
DEPARTAMENTO COMERCIAL	
AREA	COMPRAS
ENCARGADO	MARIA CONSTANZA TORRES
NOMBRE DE EQUIPO	inventarios
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CORE i3 3ra generación CPU 2.10GHZ
MEMORIA RAM	3GB
DISCO DURO	300GB
IP	192.168.170.146
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

8. EQUIPOS ÁREA DE GERENCIA

DEPARTAMENTO GERENCIA	
AREA	GERENCIA
ENCARGADO	JESUS LOPEZ
NOMBRE DE EQUIPO	asiscompras3
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i3 3ra generación CPU 3.07GHZ
MEMORIA RAM	3GB
DISCO DURO	300GB
IP	192.168.170.76
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO GERENCIA	
AREA	PUBLICIDAD
ENCARGADO	
NOMBRE DE EQUIPO	ASISGERENCIA
GRUPO DE TRABAJO	GERENCIA
SISTEMA OPERATIVO	WINDOWS 10 HOME SINGLE LANGUAGE
PROCESADOR	INTELCORE i7 CPU 2.7GHZ
MEMORIA RAM	12GB
DISCO DURO	1TB
IP	192.168.170.75
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

9. EQUIPOS ÁREA DE CONTABILIDAD

DEPARTAMENTO CONTABILIDAD	
AREA	CONTABILIDAD
ENCARGADO	CARLOS BENAVIDES
NOMBRE DE EQUIPO	contadorkwy
GRUPO DE TRABAJO	CONTABILIDAD
SISTEMA OPERATIVO	WINDOWS 8.1PRO
PROCESADOR	CORE i3 5ta generación CPU 2.70GHZ

MEMORIA RAM	4GB
DISCO DURO	1TB
IP	192.168.170.85
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CONTABILIDAD	
AREA	CONTABILIDAD
ENCARGADO	CARLOS BENAVIDES
NOMBRE DE EQUIPO	auxadmon
GRUPO DE TRABAJO	ADMON
SISTEMA OPERATIVO	XP PROFESIONAL 2002 SERVIPACK
PROCESADOR	AMD ATLON DUAL CORE 2.51GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.170.79
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CONTABILIDAD	
AREA	CONTABILIDAD
ENCARGADO	CARLOS BENAVIDES
NOMBRE DE EQUIPO	contabjefe
GRUPO DE TRABAJO	CONTABILIDAD
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CORE i3 5ta genercion 1.70GHZ
MEMORIA RAM	4GB
DISCO DURO	1TB
IP	192.168.170.78
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CONTABILIDAD	
AREA	CONTABILIDAD
ENCARGADO	
NOMBRE DE EQUIPO	keewayauxconta
GRUPO DE TRABAJO	KEEWAY
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	AMD ATLON DUAL CORE 1.50GHZ

MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.170.84
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CONTABILIDAD	
AREA	CONTABILIDAD
ENCARGADO	
NOMBRE DE EQUIPO	auxconta4
GRUPO DE TRABAJO	CONTABILIDAD
SISTEMA OPERATIVO	XP PROFESIONAL 2002
PROCESADOR	INTEL CELERON CPU 2.60GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.82
MASCARA DE RED	16
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CONTABILIDAD	
AREA	CONTABILIDAD
ENCARGADO	
NOMBRE DE EQUIPO	PC_AUXCONTAB1
GRUPO DE TRABAJO	CONTABILIDAD
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	AMD CPU 1.48GHZ
MEMORIA RAM	4GB
DISCO DURO	300GB
IP	192.168.170.81
MASCARA DE RED	16
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO CONTABILIDAD	
AREA	CONTABILIDAD
ENCARGADO	
NOMBRE DE EQUIPO	Benelli
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 10 PRO
PROCESADOR	INTEL CORE i3 3.60GHZ
MEMORIA RAM	4GB

DISCO DURO	1TB
IP	192.168.170.87
MASCARA DE RED	16
GATEWAY	192.168.170.1
DNS	192.168.170.6

10. EQUIPOS ÁREA DE REVISORÍA

DEPARTAMENTO REVISORIA	
AREA	INTERELEC
ENCARGADO	VANESA RODRIGUEZ
NOMBRE DE EQUIPO	audinterelec
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	XP PROFESIONAL 2002
PROCESADOR	INTEL CORE 2 DUO CPU 2.66GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.170.108
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	FONDO DE EMPLEADOS
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	fondolecconta
GRUPO DE TRABAJO	REVISORIA
SISTEMA OPERATIVO	WINDOWS 8 PRO
PROCESADOR	INTEL CORE i3 5ta generación CPU 1.70GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.170.121
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	REVISORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	REVICAJAS2
GRUPO DE TRABAJO	INICIOMS

SISTEMA OPERATIVO	WINDOWS XP 2002
PROCESADOR	INTEL CELERON 2.53GHZ
MEMORIA RAM	512MB
DISCO DURO	40GB
IP	192.168.170.94
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	REVISORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	auxbancos
GRUPO DE TRABAJO	INICIOMS
SISTEMA OPERATIVO	WINDOWS XP 2002
PROCESADOR	INTEL CELERON CPU 2.0GHZ
MEMORIA RAM	1GB
DISCO DURO	40GB
IP	192.168.170.105
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	REVISORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	auxiliaradv
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 8.1 PRO
PROCESADOR	INTEL CELERON CPU 1.6GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.170.115
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	BANCOS
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	revisorcajas1
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 STARTER

PROCESADOR	PENTIUM DUALCORE CPU 3.20GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.103
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	BANCOS
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	AUXCAJAS11
GRUPO DE TRABAJO	REVISORIA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	AMD E1 CPU 1.40GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.170.104
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	BANCOS
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	revisorcajas2
GRUPO DE TRABAJO	REVISORIA
SISTEMA OPERATIVO	WINDOWS 7 STARTER
PROCESADOR	PENTIUM DUAL CORE CPU 3.20GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.170.102
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	REVISORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	auxrevisoria
GRUPO DE TRABAJO	REVISORIA
SISTEMA OPERATIVO	WINDOWS XP 2002 SERVIPACK2
PROCESADOR	INTEL CELERON CPU 2.13GHZ

MEMORIA RAM	1GB
DISCO DURO	80GB
IP	192.168.170.93
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	REVISORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	HOSTREVI
GRUPO DE TRABAJO	REVISORIA
SISTEMA OPERATIVO	WINDOWS 7 PROFESIONAL
PROCESADOR	INTEL CORE i3 CPU 3.1GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.170.100
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	AUDITORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	revisorinv1
GRUPO DE TRABAJO	REVISORIA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CORE i3 CPU 1.7GHZ
MEMORIA RAM	4GB
DISCO DURO	1TB
IP	192.168.170.99
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	AUDITORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	AUDINTERNA-PC
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON CPU 2.41GHZ
MEMORIA RAM	4GB

DISCO DURO	1TB
IP	192.168.170.109
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	AUDITORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	auditor8
GRUPO DE TRABAJO	REVISORIA
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON CPU 2.53GHZ
MEMORIA RAM	1GB
DISCO DURO	250GB
IP	192.168.170.96
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO REVISORIA	
AREA	AUDITORIA
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	revinv2
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS XP PROFESIONAL 2002
PROCESADOR	INTEL CELERON CPU 1.8GHZ
MEMORIA RAM	1GB
DISCO DURO	80GB
IP	192.168.170.120
MASCARA DE RED	16
GATEWAY	192.168.170.1
DNS	192.168.170.6

11. EQUIPOS ÁREA INTERELEC

DEPARTAMENTO INTERELEC	
AREA	INTERELEC
ENCARGADO	VANESA RODRIGUEZ
NOMBRE DE EQUIPO	interpasistente
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE

PROCESADOR	AMD CPU 1.48GHZ
MEMORIA RAM	2GB
DISCO DURO	150GB
IP	192.168.170.62
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

DEPARTAMENTO INTERELEC	
AREA	INTERELEC
ENCARGADO	VANESA RODRIGUEZ
NOMBRE DE EQUIPO	abogado3_PC
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL PENTIUM DUAL CPU 2.40GHZ
MEMORIA RAM	2GB
DISCO DURO	200GB
IP	192.168.170.152
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

12. EQUIPOS ÁREA FONDELEC

DEPARTAMENTO FONDELEC	
AREA	FONDO DE EMPLEADOS
ENCARGADO	ROCIO BURBANO
NOMBRE DE EQUIPO	fondolecadm
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 8 PRO
PROCESADOR	INTEL CORE i3 5ta generación CPU 1.70GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.170.110
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

13. EQUIPOS ÁREA DE PUBLICIDAD

DEPARTAMENTO PUBLICIDAD	
AREA	PUBLICIDAD
ENCARGADO	
NOMBRE DE EQUIPO	publicidadweb
GRUPO DE TRABAJO	COMERCIAL
SISTEMA OPERATIVO	WINDOWS 10 HOME SINGLE LANGUAGE
PROCESADOR	INTELCORE i7 CPU 2.81GHZ
MEMORIA RAM	8GB
DISCO DURO	2TB
IP	192.168.170.68
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

14. EQUIPOS AGENCIA KEEWAY AMERICAS

AGENCIA KEEWAY AMERICAS	
AREA	VENTAS
ENCARGADO	ADRIANA MARIA OCAMPO
NOMBRE DE EQUIPO	Kamericasvtas
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON CPU 3.0GHZ
MEMORIA RAM	2GB
DISCO DURO	230GB
IP	192.168.169.46
MASCARA DE RED	21
GATEWAY	192.168.169.1
DNS	192.168.170.6

AGENCIA KEEWAY AMERICAS	
AREA	CAJA
ENCARGADO	ADRIANA MARIA OCAMPO
NOMBRE DE EQUIPO	Kamericascaja
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 PROFESIONAL
PROCESADOR	CORE i5 2320 CPU 3.0GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB

IP	192.168.169.45
MASCARA DE RED	22
GATEWAY	192.168.169.1
DNS	192.168.170.6

15. EQUIPOS AGENCIA ELECTROMILLONARIA CARRERA 20

AGENCIA CARRERA 20 (VPN)	
AREA	CAJA
ENCARGADO	LEYDY BURBANO
NOMBRE DE EQUIPO	Cra20WMSIS3
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS MULTI POINT SERVER 2011
PROCESADOR	CORE i5 CPU 3.2GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.171.81
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA CARRERA 20 (VPN)	
AREA	ADMINISTRACION
ENCARGADO	
NOMBRE DE EQUIPO	Cra20WMSIS3
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	MULTIPOIN SERVER 2011
PROCESADOR	INTEL CORE i7 CPU 3.40GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.171.126
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

16. EQUIPOS AGENCIA KEEWAY CALLE 17

AGENCIA KEEWAY CALLE 17	
AREA	CAJA
ENCARGADO	CAROL ANDREA BENAVIDES
NOMBRE DE EQUIPO	Keeway17caja
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL ATOM CPU 1.66GHZ
MEMORIA RAM	2GB
DISCO DURO	500GB
IP	192.168.169.35
MASCARA DE RED	22
GATEWAY	192.168.170.1
DNS	192.168.170.6

17. EQUIPOS AGENCIA ELECTROMILLONARIA CALLE 17

AGENCIA ELECTROMILLONARIA CALLE 17 (VPN)	
AREA	CAJA
ENCARGADO	CARLOS BURBANO
NOMBRE DE EQUIPO	servercl17
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CORE i5 CPU 3.2GHZ
MEMORIA RAM	4GB
DISCO DURO	370GB
IP	192.168.171.126
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

18. EQUIPOS AGENCIA ELECTROMILLONARIA CARRERA 25

AGENCIA CARRERA 25 (VPN)	
AREA	CAJA
ENCARGADO	
NOMBRE DE EQUIPO	CRA25WMSI51
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS MULTIPOINT SERVER 2012
PROCESADOR	INTEL PENTIUM CPU 3.0GHZ

MEMORIA RAM	4GB
DISCO DURO	160GB
IP	192.168.171.93
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

19. EQUIPOS AGENCIA ELECTROMILLONARIA CARRERA 24

AGENCIA CARRERA 24	
AREA	VENTAS
ENCARGADO	
NOMBRE DE EQUIPO	ASISTECRA24
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON 1.86GHZ
MEMORIA RAM	2GB
DISCO DURO	120GB
IP	192.168.170.116
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA CARRERA 24	
AREA	CAJA
ENCARGADO	
NOMBRE DE EQUIPO	CAJACRA24
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON 1.86GHZ
MEMORIA RAM	2GB
DISCO DURO	120GB
IP	192.168.170.117
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

20. EQUIPOS AGENCIA ELECTROMILLONARIA CALLE 19

AGENCIA CALLE 19	
AREA	INVENTARIO
ENCARGADO	

NOMBRE DE EQUIPO	asistente19
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON 1.48GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.169.12
MASCARA DE RED	16
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA CALLE 19	
AREA	CAJA
ENCARGADO	
NOMBRE DE EQUIPO	cajacl19
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON 1.48GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.169.10
MASCARA DE RED	16
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA CALLE 19	
AREA	CONTABILIDAD
ENCARGADO	
NOMBRE DE EQUIPO	jefecontabcl19
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON 1.48GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.169.17
MASCARA DE RED	24
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA CALLE 19	
AREA	CONTABILIDAD
ENCARGADO	
NOMBRE DE EQUIPO	auxcontab2

GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON 1.48GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.169.18
MASCARA DE RED	16
GATEWAY	192.168.169.1
DNS	192.168.170.6

21. EQUIPOS AGENCIA BODEGA PRINCIPAL

AGENCIA BODEGA PRINCIPAL (VPN)	
AREA	SERVICIO TECNICO
ENCARGADO	JUAN CARLOS MANTILLA
NOMBRE DE EQUIPO	serviciotecnico
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 10 PRO
PROCESADOR	CORE i5 4ta generación 2.30GHZ
MEMORIA RAM	4GB
DISCO DURO	1TB
IP	192.168.171.131
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA BODEGA PRINCIPAL (VPN)	
AREA	BODEGA
ENCARGADO	ALVARO DAVILA
NOMBRE DE EQUIPO	BODEGA1
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON CPU 3.0GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.171.149
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA BODEGA PRINCIPAL (VPN)	
AREA	BODEGA

ENCARGADO	ALVARO DAVILA
NOMBRE DE EQUIPO	BODEGA2
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON CPU 3.0GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.171.112
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA BODEGA PRINCIPAL (VPN)	
AREA	BODEGA
ENCARGADO	ALVARO DAVILA
NOMBRE DE EQUIPO	BODEGA3
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	INTEL CELERON CPU 3.0GHZ
MEMORIA RAM	2GB
DISCO DURO	300GB
IP	192.168.171.113
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

AGENCIA BODEGA PRINCIPAL (VPN)	
AREA	BODEGA PRINCIPAL
ENCARGADO	ALVARO DAVILA
NOMBRE DE EQUIPO	logisticacoord
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS 7 ULTIMATE
PROCESADOR	CORE i3 CPU 3.0GHZ
MEMORIA RAM	4GB
DISCO DURO	500GB
IP	192.168.171.34
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

22. EQUIPOS AGENCIA ELECTROMILLONARIA LAS LUNAS

AGENCIA LAS LUNAS (VPN)	
AREA	CAJA
ENCARGADO	
NOMBRE DE EQUIPO	cajalaunas
GRUPO DE TRABAJO	
SISTEMA OPERATIVO	WINDOWS MULTIPOINT SERVER 2012
PROCESADOR	INTEL PENTIUM CPU 3.0GHZ
MEMORIA RAM	4GB
DISCO DURO	160GB
IP	192.168.171.37
MASCARA DE RED	21
GATEWAY	192.168.170.1
DNS	192.168.170.6

23. RADIO ENLACES UBIQUITI

RADIO ENLACES UBIQUITI				
AGENCIA	**NOMBRE**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**	**IP LOCAL**
PRINCIPAL	RADIO-ENLACE PPAL C19	SISTEMAS	R. SPOOFING_C19	192.168.169.1
PRINCIPAL	RADIO-ENLACE PPAL SECTORIAL	SISTEMAS	SPOOFING_SEC	192.168.169.3
PRINCIPAL	RADIO-ENLACE PPAL SECTORIAL_M900	SISTEMAS	SPOOFING_SECM900	192.168.169.4
AG.CALLE19	RADIO-ENLACE AG.CALLE19	SISTEMAS	A.SPOOFING_C19	192.168.169.2
KWY CALLE17	RADIO-ENLACE AG. KWY CALLE17	SISTEMAS	A.SPOOFING_KWY17	192.168.169.31

KWY AMERICAS	RADIO-ENLACE AG. KWY AMERICAS	SISTEMAS	A.SPOOFING_KWYAMER	192.168.169.41
AG.CALLE17	RADIO-ENLACE AG. CALLE17	SISTEMAS	A.SPOOFING_C17	192.168.169.51

24. ROUTER PRINCIPAL ELECTROMILLONARIA

ROUTER ELECTROMILLONARIA				
AGENCIA	**NOMBRE**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**	**IP LOCAL**
PRINCIPAL	ROUTER TELEFONICA	SISTEMAS		192.168.170.1

25. SERVIDORES DE RED ELECTROMILLONARIA

SERVIDORES ELECTROMILLONARIA				
AGENCIA	**NOMBRE**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**	**IP LOCAL**
PRINCIPAL	SERVER VPN ENDIAN	SISTEMAS	SLYTHERIN	192.168.171.1
PRINCIPAL	SERVER SIIGO PAL	SISTEMAS	SIIGO PPAL	192.168.170.4
PRINCIPAL	SERVER DOCUMENTOS	SISTEMAS		192.168.170.5
PRINCIPAL	SERVER FIREWALL-PROXY-WEB	SISTEMAS	VOLDEMORT	192.168.170.6
PRINCIPAL	SERVER SPARK-FTP	SISTEMAS	AZKABAN	192.168.170.7
PRINCIPAL	SERVER BODEGA SIIGO	SISTEMAS	SIIGO	192.168.170.8
PRINCIPAL	SERVER REMOTO LAN1	SISTEMAS	REMOTO	192.168.170.9

PRINCIPAL	SERVER BASE DE DATOS	SISTEMAS	GRYFFINDOR	192.168.170.10
AG. CALLE19	SERVER FISCAL	SISTEMAS		192.168.169.15
AG. CALLE19	SERVER REMOTO FISCAL	SISTEMAS		192.168.169.16
PRINCIPAL	SERVER DE REMOTO LAN2	SISTEMAS	REMOTO	192.168.170.20

26. IMPRESORAS MULTIFUNCIONALES

IMPRESORAS MULTIFUNCIONALES				
AGENCIA	**NOMBRE**	**DEPARTAMENTO**	**NOMBRE DE EQUIPO**	**IP LOCAL**
PRINCIPAL	MULTIFUNCIONAL 2do PISO (JURIDICO)	SISTEMAS		192.168.170.111
PRINCIPAL	MULTIFUNCIONAL 2do PISO (ADMIN)	SISTEMAS		192.168.170.112
PRINCIPAL	MULTIFUNCIONAL 3re PISO	SISTEMAS		192.168.170.113
PRINCIPAL	MULTIFUNCIONAL 4to PISO	SISTEMAS		192.168.170.114

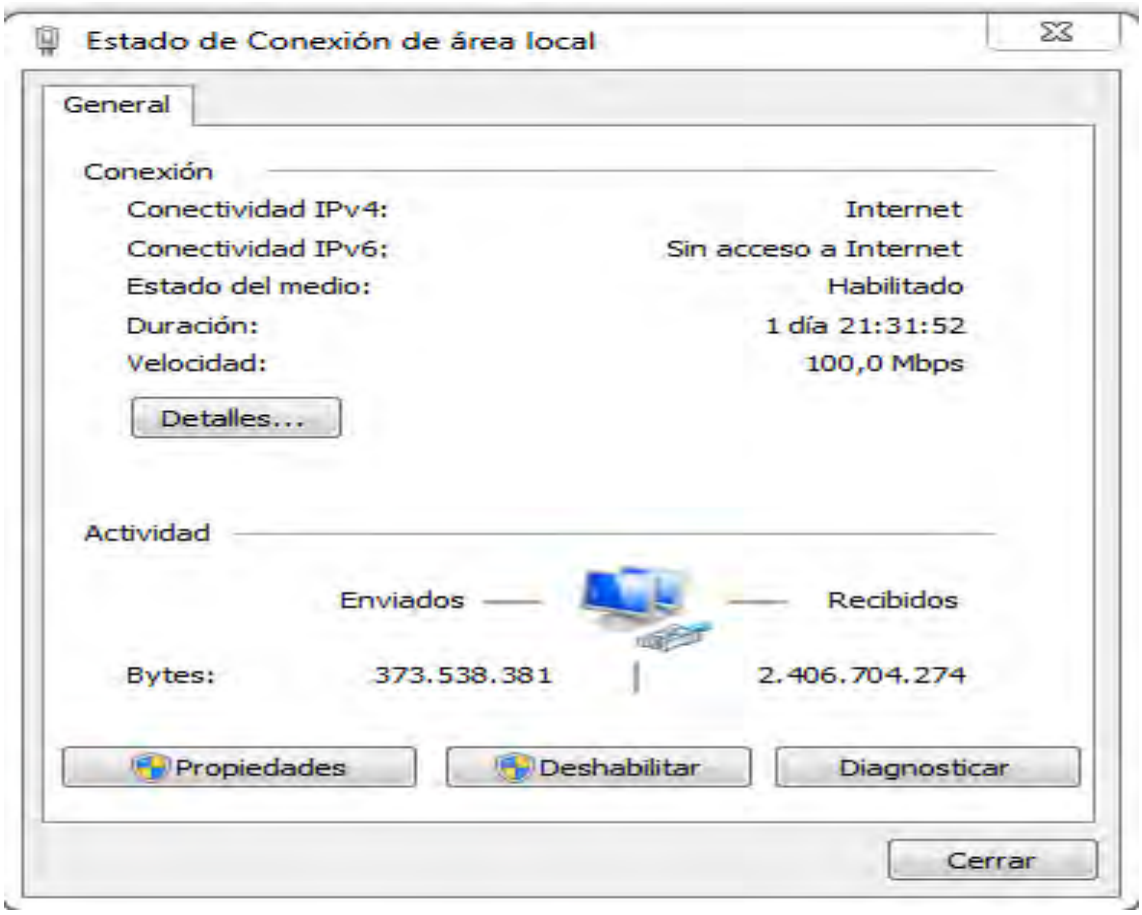
Anexo B. Analisis de la red de datos.

ÍNDICE

1. TARJETA DE RED ETHERNET 274
2. ANALISIS CON SPEEDTEST 276
3. ANALISIS CON IPERF3 277
4. ANÁLISIS CON ACRYLIC WI-FI PROFESSIONAL 278
5. ANÁLISIS CON WIRESHARK 280
6. ANALISIS CON IP TOOLS 284

1. TARJETA DE RED ETHERNET

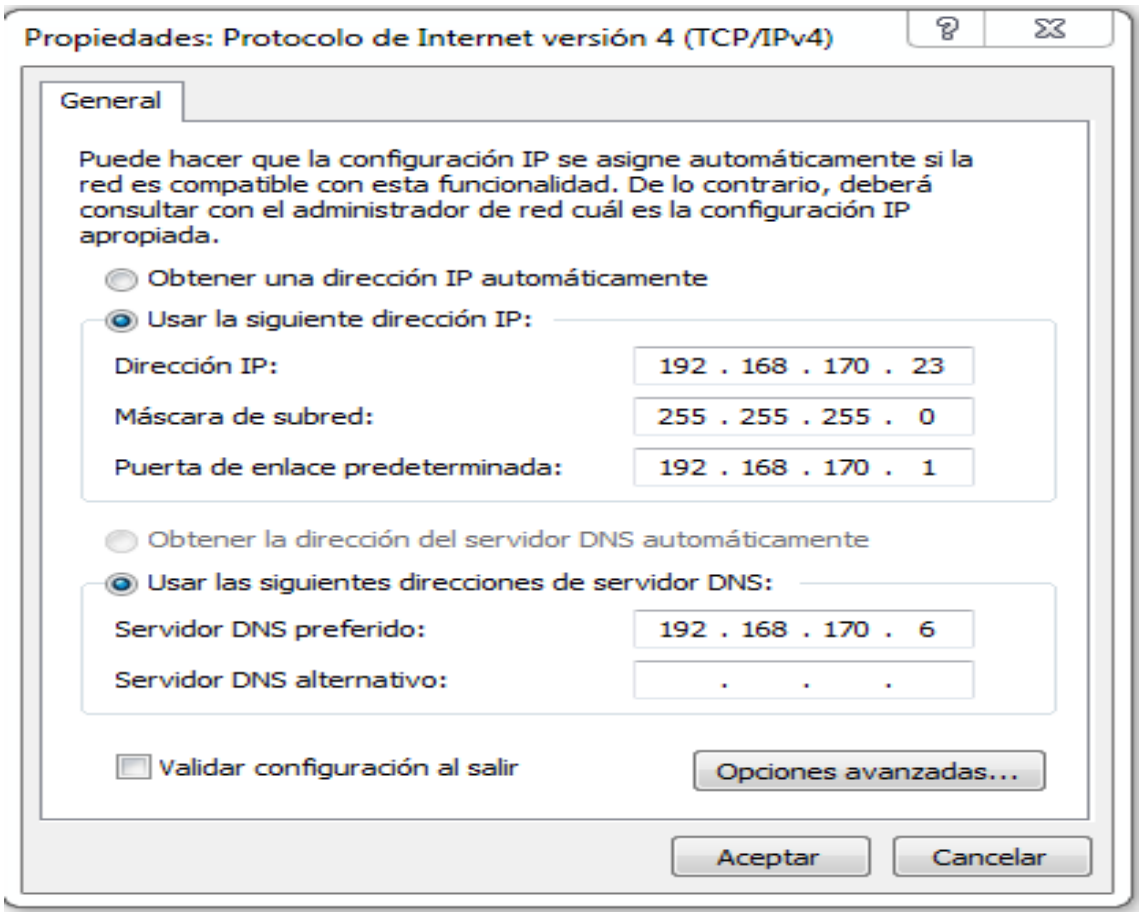
La tarjeta de red Ethernet del servidor Nagios tiene una velocidad de transmisión de 100 Mbps.



La red de la empresa es la 192.168.168.0 con mascara de red 255.255.252.0 con 1024 IP disponibles distribuidas en 4 pools de IP que son:

192.168.168.1 – 192.168.168.255
192.168.169.1 – 192.168.169.255
192.168.170.1 – 192.168.170.255
192.168.171.1 – 192.168.171.255

La configuracion IP en la empresa es de forma manual.


Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)
General
Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.
Obtener una dirección IP automáticamente
Usar la siguiente dirección IP:
Dirección IP: 192 . 168 . 170 . 23
Máscara de subred: 255 . 255 . 255 . 0
Puerta de enlace predeterminada: 192 . 168 . 170 . 1
Obtener la dirección del servidor DNS automáticamente
Usar las siguientes direcciones de servidor DNS:
Servidor DNS preferido: 192 . 168 . 170 . 6
Servidor DNS alternativo: . . .
Validar configuración al salir
Opciones avanzadas...
Aceptar
Cancelar

2. ANALISIS CON SPEEDTEST

Con la herramienta SpeedTest se midió la velocidad de Ping, descarga, subida y fluctuación de la red de datos de la empresa. Los resultados varian un poco dependiendo de la distancia del servidor que contesta la petición.
los resultados obtenidos son:



3. ANALISIS CON IPERF3

Se utilizó la herramienta Iperf3 que es una herramienta para mediciones activas de ancho de banda máximo alcanzable en redes IP.

Se hace una medición de ancho de banda con el protocolo TCP. Los resultados obtenidos son:

Intervalo 60 segundos, Transferencia 678MBytes y Ancho de Banda de 11.3 MBytes/sec.



Se hace una medición de ancho de banda con el protocolo UDP.
Los resultados obtenidos son:
Intervalo 10 segundos, Transferencia 1.25 MBytes, Ancho de Banda de 0.12 MBytes/sec, Jitter 0.610 ms, Datagramas perdidos 0 y Datagramas enviados 159.

El Jitter se considera como una señal de ruido no deseada. Variabilidad temporal durante él envió de señales digitales.

```
C:\iPerf>iperf3.exe -c 192.168.170.165 -p5201 -fM -V -u
iperf 3.1.3
CYGWIN_NT-6.1 PCJFSISTEMAS 2.5.1(0.297/5/3) 2016-04-21 22:14 x86_64
Time: Fri, 09 Feb 2018 20:32:31 GMT
Connecting to host 192.168.170.165, port 5201
      Cookie: PCJFSISTEMAS.1518208351.242283.7baf7
[  4] local 192.168.170.23 port 57718 connected to 192.168.170.165 port 5201
Starting Test: protocol: UDP, 1 streams, 8192 byte blocks, omitting 0 seconds, 10 second test
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec   392 KBytes  0.38 MBytes/sec  49
[  4]   1.00-2.00   sec  80.0 KBytes  0.08 MBytes/sec  10
[  4]   2.00-3.00   sec  80.0 KBytes  0.08 MBytes/sec  10
[  4]   3.00-4.00   sec  80.0 KBytes  0.08 MBytes/sec  10
[  4]   4.00-5.00   sec  80.0 KBytes  0.08 MBytes/sec  10
[  4]   5.00-6.00   sec  80.0 KBytes  0.08 MBytes/sec  10
[  4]   6.00-7.00   sec   104 KBytes  0.10 MBytes/sec  13
[  4]   7.00-8.00   sec   128 KBytes  0.12 MBytes/sec  16
[  4]   8.00-9.00   sec   128 KBytes  0.12 MBytes/sec  16
[  4]   9.00-10.00  sec   128 KBytes  0.12 MBytes/sec  16
- - - - - - - - - - - - - - - - - - - - - - - - -
Test Complete. Summary Results:
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec  1.25 MBytes  0.12 MBytes/sec  0.610 ms  0/159 (0%)
[  4] Sent 159 datagrams
CPU Utilization: local/sender 1.8% (0.8%u/1.1%s), remote/receiver 0.0% (0.0%u/0.0%s)

iperf Done.

C:\iPerf>
```

4. ANÁLISIS CON ACRYLIC WI-FI PROFESSIONAL

Con la herramienta Acrylic wi-Fi Professional se analizó la red inalámbrica de la empresa.

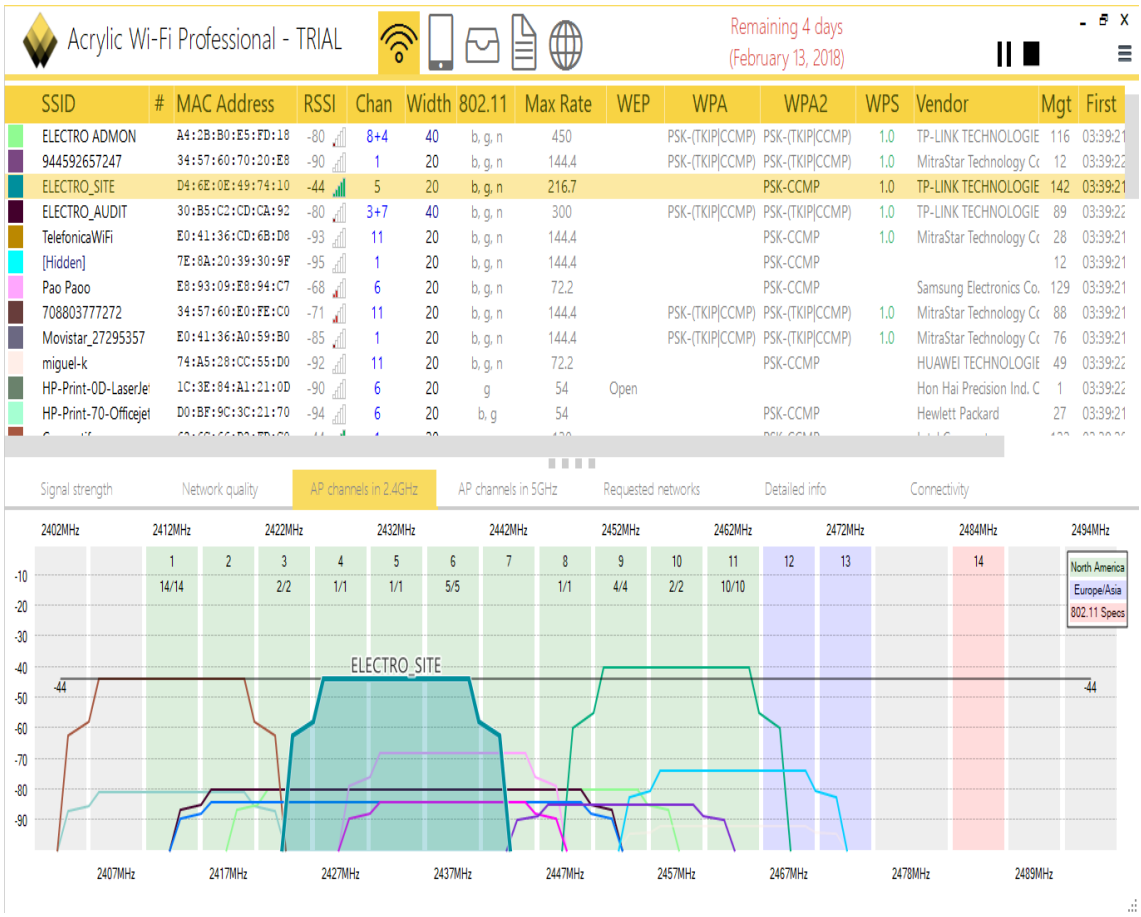
Los resultados obtenidos son: Indicador de fuerza de la señal recibida (RSSI) -44 dBm, Canal 5, estándar wifi b,g,n, seguridad WPA2 y Vendedor TP-Link TECHNOLOGIE.

RSSI: Se presenta en escala de 0 a -100 expresada en dBm, entre más cerca este a cero es mejor la intensidad de señal recibida.

Canal: Entre más redes inalámbricas existan mayor probabilidad de sufrir interferencias, a veces es necesario cambiar de canal. La frecuencia de red

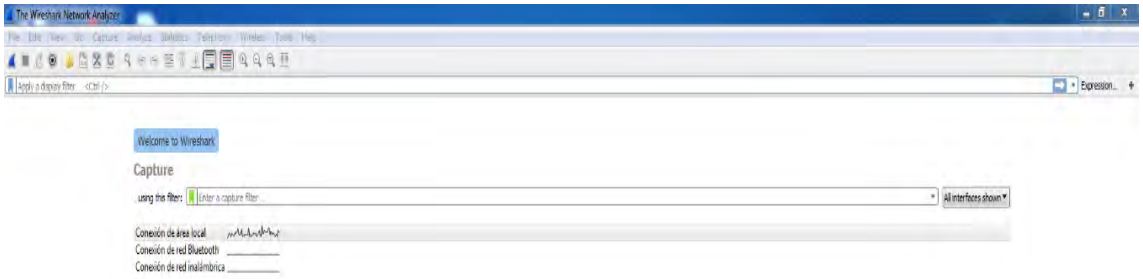
inalámbrica de la empresa es de 2.4 GHz. De acuerdo al resultado obtenido el canal elegido es el correcto.

802.11b/g/n: son los más aceptados actualmente a nivel mundial con una velocidad de trasferencia teórica de 11.54 y 300Mbit/s respectivamente.
WPA2: Protocolo de seguridad inalámbrica que proporciona fuertes datos de protección y control de acceso a la red.

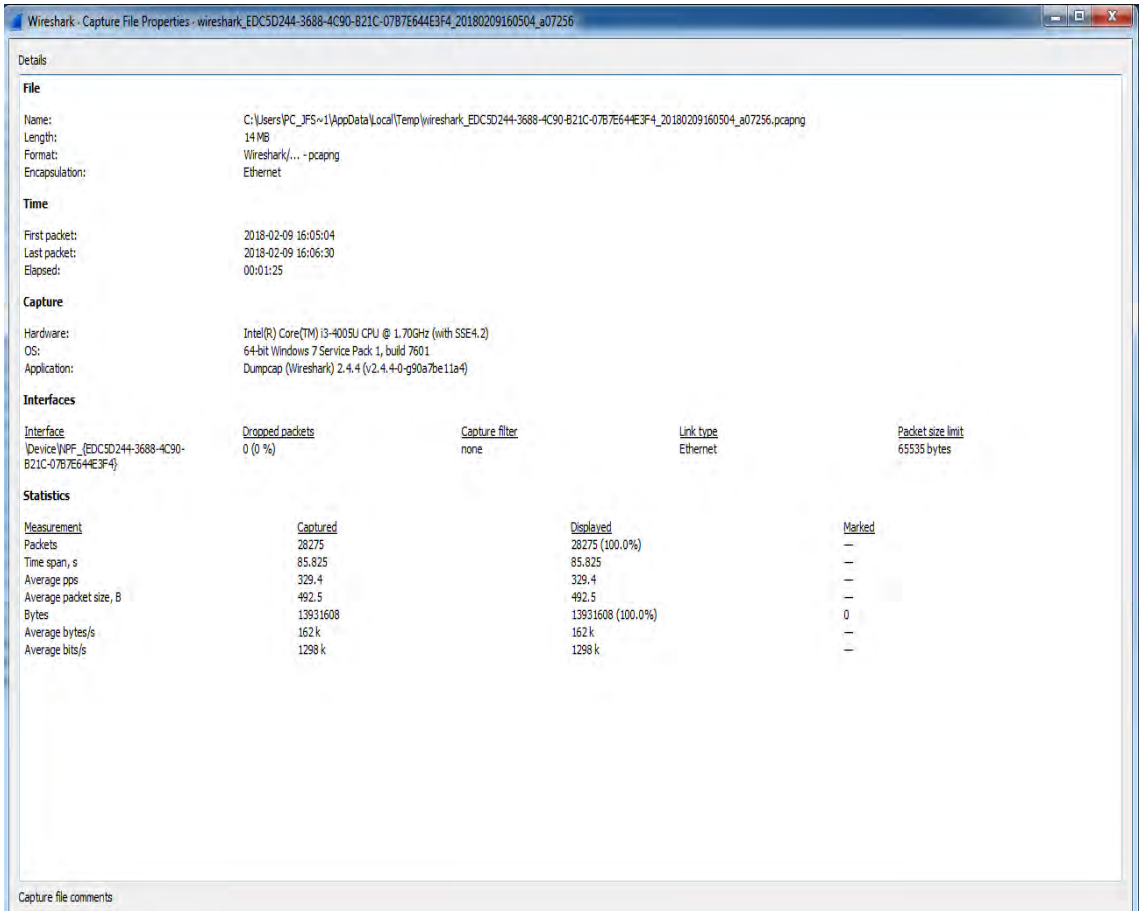


5. ANÁLISIS CON WIRESHARK

Con la herramienta Wireshark, que es un analizador de paquetes se analizó el tráfico de la red en un lapso corto de tiempo.
Se muestran las interfaces de red activas. La que presenta tráfico de red es la red local Ethernet.

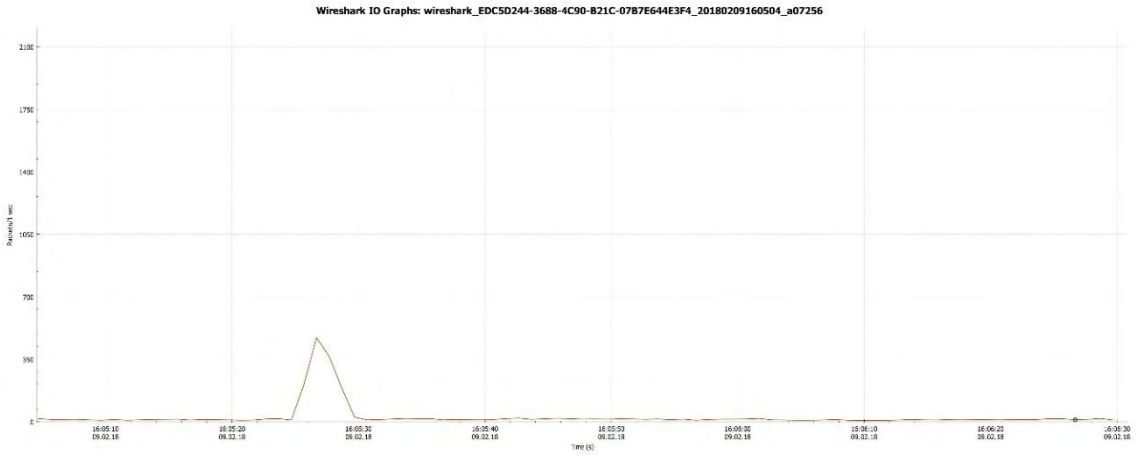


Se obtuvieron los siguientes resultados:

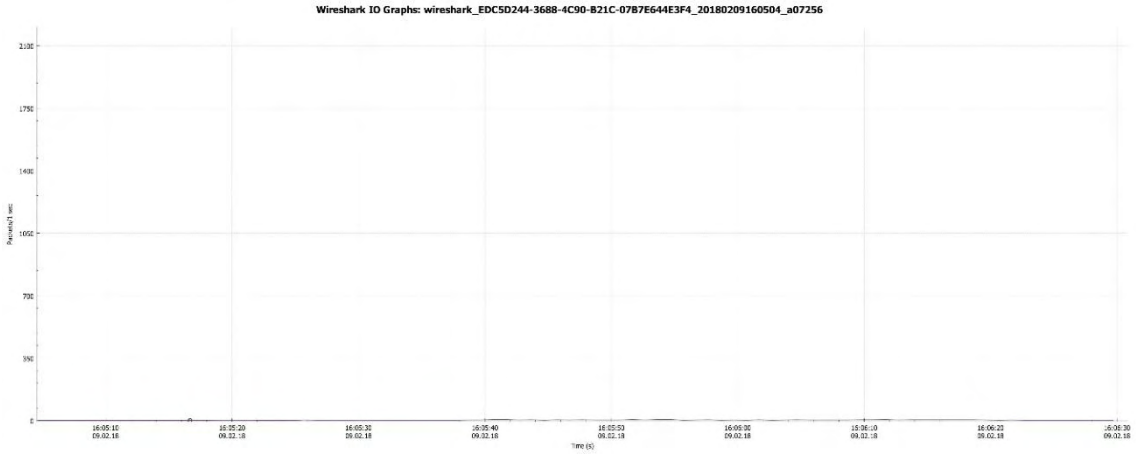


Mediante graficas de Paquetes/1sec, se muestra el comportamiento de diferentes protocolos durante el tiempo de captura.

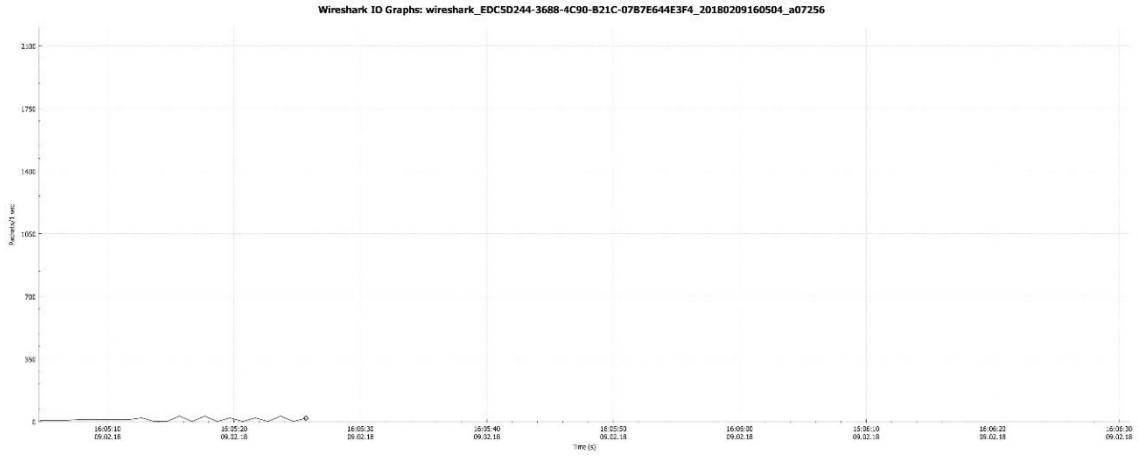
A continuación, se muestra el comportamiento protocolo ARP.



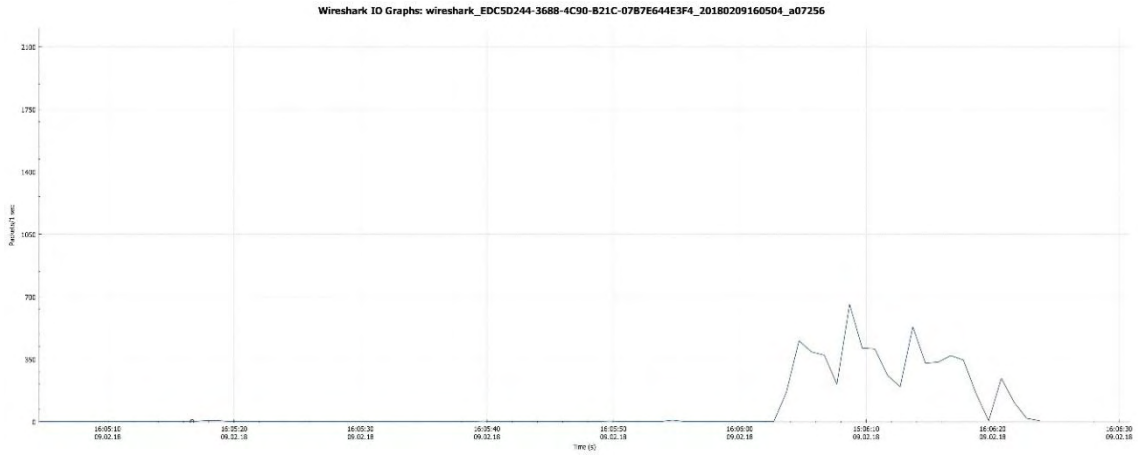
En seguida, se muestra el comportamiento protocolo ICMP.



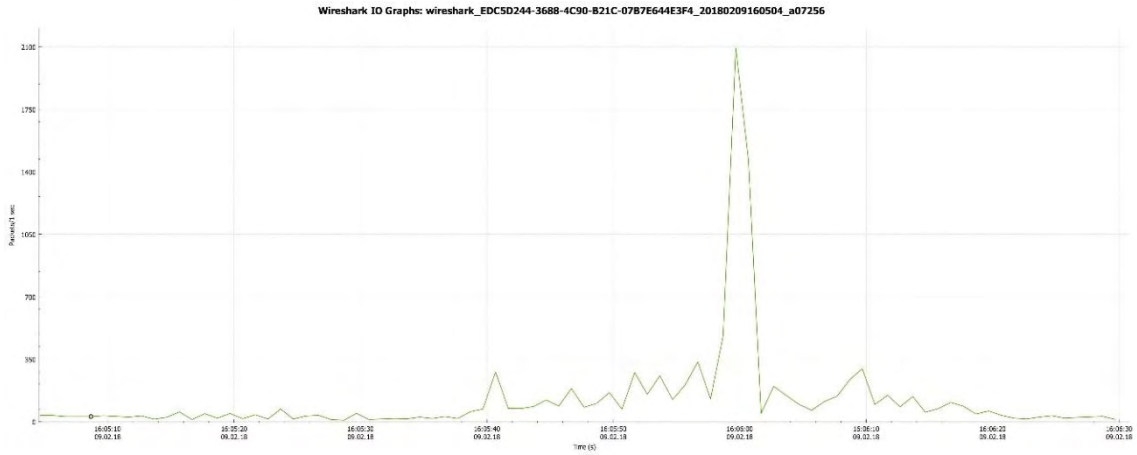
En seguida, se muestra el comportamiento protocolo SNMP.



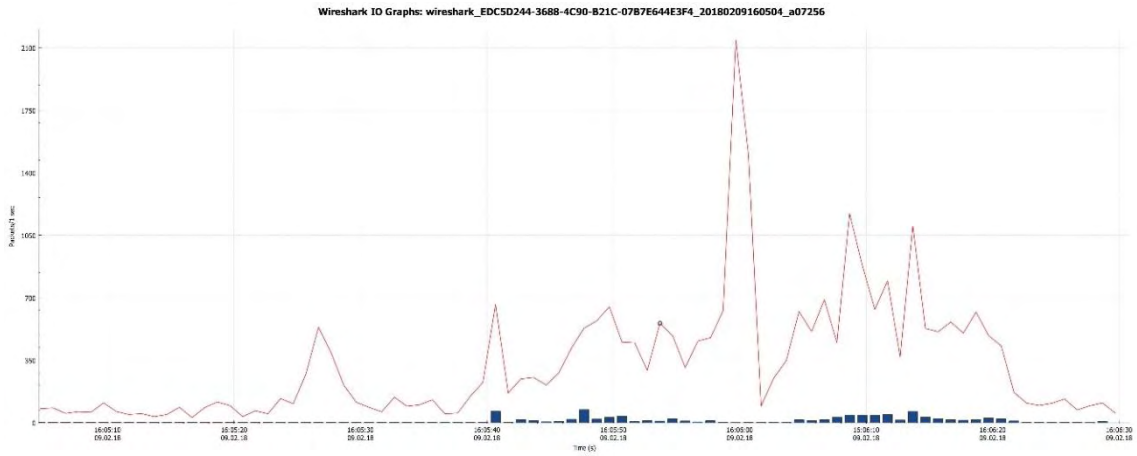
A continuación, se muestra el comportamiento protocolo TCP.



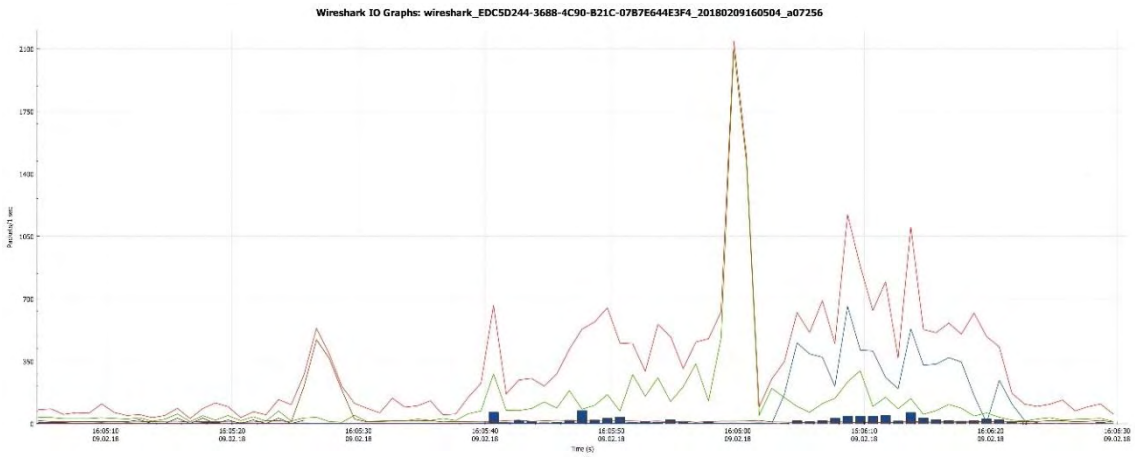
En seguida, se muestra el comportamiento protocolo UDP.



A continuación, se muestra el comportamiento total del tráfico de red, con errores TCP.



Por último, se muestra el comportamiento de todos los protocolos anteriormente graficados.



6. ANALISIS CON IP TOOLS

Con la herramienta free IP Tools se hizo un analisis de IP activas y escaneo de Puertos.
La empresa tiene un rango de IP de 1024 lo que permite la disponiblilidad de muchas IP para la ampliacion de la red de datos. La sub red 192.168.168.0 no esta en uso.

las IP que responden al ping en la sub red 192.168.169.0 son 20 de 255.

*	192.168.169.244		Pedido sobrepasado en tiempo	
*	192.168.169.246		Pedido sobrepasado en tiempo	
*	192.168.169.250		Pedido sobrepasado en tiempo	
*	192.168.169.249		Pedido sobrepasado en tiempo	
*	192.168.169.248		Pedido sobrepasado en tiempo	
*	192.168.169.253		Pedido sobrepasado en tiempo	
*	192.168.169.252		Pedido sobrepasado en tiempo	
*	192.168.169.254		Pedido sobrepasado en tiempo	
*	192.168.169.251		Pedido sobrepasado en tiempo	
*	192.168.169.255		Pedido sobrepasado en tiempo	
*	192.168.169.4		Respuesta Echo	0/0/1
*	192.168.169.1		Respuesta Echo	0/0/1
*	192.168.169.3		Respuesta Echo	0/1/2
*	192.168.169.5		Respuesta Echo	0/1/2
*	192.168.169.2		Respuesta Echo	3/7/12
*	192.168.169.10		Respuesta Echo	6/7/8
*	192.168.169.12		Respuesta Echo	5/6/7
*	192.168.169.11		Respuesta Echo	4/6/8
*	192.168.169.15		Respuesta Echo	4/9/19
*	192.168.169.17		Respuesta Echo	3/3/3
*	192.168.169.16		Respuesta Echo	2/7/15
*	192.168.169.18		Respuesta Echo	3/7/15
*	192.168.169.20		Respuesta Echo	3/12/26
*	192.168.169.35		Respuesta Echo	3/4/5
*	192.168.169.31		Respuesta Echo	2/4/7
*	192.168.169.36		Respuesta Echo	2/3/5
*	192.168.169.41		Respuesta Echo	121/170/252
*	192.168.169.51		Respuesta Echo	74/100/121
*	192.168.169.57		Respuesta Echo	2/11/19
*	192.168.169.61		Respuesta Echo	61/76/92

las IP que responden al ping en la sub red 192.168.170.0 son 82 de 255

Reporte: Ping

Generado en 9/02/2018 a 5:08:07 p. m. por Free IP Tools.

#	Dirección IP	Hostname	Msj de Respuesta	Tiempo de Respuesta
*	192.168.170.4		Respuesta Echo	0/0/0
*	192.168.170.1		Respuesta Echo	0/0/0
*	192.168.170.9		Respuesta Echo	0/0/1
*	192.168.170.10		Respuesta Echo	0/0/1
*	192.168.170.8		Respuesta Echo	0/0/1
*	192.168.170.7		Respuesta Echo	0/0/1
*	192.168.170.6		Respuesta Echo	0/0/0
*	192.168.170.20		Respuesta Echo	0/0/0
*	192.168.170.17		Respuesta Echo	0/0/1
*	192.168.170.25		Respuesta Echo	0/0/0
*	192.168.170.23		Respuesta Echo	0/0/1
*	192.168.170.21		Respuesta Echo	0/0/1
*	192.168.170.30		Respuesta Echo	0/0/1
*	192.168.170.29		Respuesta Echo	0/0/1
*	192.168.170.26		Respuesta Echo	0/0/1
*	192.168.170.27		Respuesta Echo	0/1/2
*	192.168.170.32		Respuesta Echo	0/1/1
*	192.168.170.31		Respuesta Echo	1/1/1
*	192.168.170.33		Respuesta Echo	1/1/1
*	192.168.170.35		Respuesta Echo	2/3/5
*	192.168.170.36		Respuesta Echo	0/0/0
*	192.168.170.38		Respuesta Echo	0/0/0
*	192.168.170.37		Respuesta Echo	0/0/0
*	192.168.170.42		Respuesta Echo	0/0/0
*	192.168.170.41		Respuesta Echo	0/0/0
*	192.168.170.45		Respuesta Echo	0/0/0
*	192.168.170.44		Respuesta Echo	0/1/2
*	192.168.170.49		Respuesta Echo	0/0/1
*	192.168.170.48		Respuesta Echo	0/0/1
*	192.168.170.51		Respuesta Echo	0/0/1
*	192.168.170.53		Respuesta Echo	0/0/0
*	192.168.170.54		Respuesta Echo	0/0/1
*	192.168.170.56		Respuesta Echo	1/1/1
*	192.168.170.60		Respuesta Echo	0/0/1
*	192.168.170.62		Respuesta Echo	0/1/2
*	192.168.170.68		Respuesta Echo	0/0/0
*	192.168.170.67		Respuesta Echo	0/1/2
*	192.168.170.75		Respuesta Echo	0/0/0
*	192.168.170.71		Respuesta Echo	0/1/1
*	192.168.170.78		Respuesta Echo	0/0/0
*	192.168.170.76		Respuesta Echo	0/0/1
*	192.168.170.85		Respuesta Echo	0/0/1

*	192.168.170.81		Respuesta Echo	0/0/1
*	192.168.170.84		Respuesta Echo	0/0/1
*	192.168.170.87		Respuesta Echo	0/0/0
*	192.168.170.88		Respuesta Echo	0/0/1
*	192.168.170.90		Respuesta Echo	0/1/4
*	192.168.170.93		Respuesta Echo	0/0/0
*	192.168.170.97		Respuesta Echo	0/0/0
*	192.168.170.100		Respuesta Echo	0/0/1
*	192.168.170.103		Respuesta Echo	0/0/1
*	192.168.170.101		Respuesta Echo	0/1/1
*	192.168.170.104		Respuesta Echo	1/1/1
*	192.168.170.102		Respuesta Echo	0/1/3
*	192.168.170.108		Respuesta Echo	0/0/1
*	192.168.170.110		Respuesta Echo	0/0/1
*	192.168.170.109		Respuesta Echo	0/1/2
*	192.168.170.111		Respuesta Echo	0/0/1
*	192.168.170.113		Respuesta Echo	0/0/1
*	192.168.170.112		Respuesta Echo	0/0/1
*	192.168.170.114		Respuesta Echo	0/0/1
*	192.168.170.115		Respuesta Echo	0/1/3
*	192.168.170.117		Respuesta Echo	0/0/1
*	192.168.170.119		Respuesta Echo	0/0/1
*	192.168.170.116		Respuesta Echo	0/0/1
*	192.168.170.118		Respuesta Echo	0/0/1
*	192.168.170.135		Respuesta Echo	0/0/1
*	192.168.170.133		Respuesta Echo	0/1/2
*	192.168.170.144		Respuesta Echo	0/1/2
*	192.168.170.148		Respuesta Echo	0/0/1
*	192.168.170.147		Respuesta Echo	1/2/2
*	192.168.170.149		Respuesta Echo	1/1/2
*	192.168.170.152		Respuesta Echo	0/1/2
*	192.168.170.153		Respuesta Echo	1/1/1
*	192.168.170.151		Respuesta Echo	1/1/2
*	192.168.170.165		Respuesta Echo	0/0/0
*	192.168.170.170		Respuesta Echo	0/0/1
*	192.168.170.172		Respuesta Echo	0/1/3
*	192.168.170.184		Respuesta Echo	0/0/1
*	192.168.170.202		Respuesta Echo	0/0/0
*	192.168.170.203		Respuesta Echo	0/0/0
*	192.168.170.205		Respuesta Echo	0/0/0
*	192.168.170.204		Respuesta Echo	0/0/0
*	192.168.170.240		Respuesta Echo	1/2/4
*	192.168.170.255		Respuesta Echo	0/0/0
*	192.168.170.2		Pedido sobrepasado en tiempo	
*	192.168.170.3		Pedido sobrepasado en tiempo	

Las IP que responden al ping en la sub red 192.168.171.0 son 2 de 255

*	192.168.171.227		Pedido sobrepasado en tiempo	0/104/208
*	192.168.171.230		Pedido sobrepasado en tiempo	
*	192.168.171.228		Pedido sobrepasado en tiempo	
*	192.168.171.226		Pedido sobrepasado en tiempo	
*	192.168.171.231		Pedido sobrepasado en tiempo	0/157/314
*	192.168.171.234		Pedido sobrepasado en tiempo	
*	192.168.171.235		Pedido sobrepasado en tiempo	
*	192.168.171.232		Pedido sobrepasado en tiempo	
*	192.168.171.233		Pedido sobrepasado en tiempo	
*	192.168.171.238		Pedido sobrepasado en tiempo	
*	192.168.171.240		Pedido sobrepasado en tiempo	
*	192.168.171.239		Pedido sobrepasado en tiempo	
*	192.168.171.237		Pedido sobrepasado en tiempo	
*	192.168.171.236		Pedido sobrepasado en tiempo	
*	192.168.171.244		Pedido sobrepasado en tiempo	
*	192.168.171.241		Pedido sobrepasado en tiempo	
*	192.168.171.245		Pedido sobrepasado en tiempo	
*	192.168.171.242		Pedido sobrepasado en tiempo	
*	192.168.171.243		Pedido sobrepasado en tiempo	
*	192.168.171.246		Pedido sobrepasado en tiempo	0/166/332
*	192.168.171.248		Pedido sobrepasado en tiempo	
*	192.168.171.250		Pedido sobrepasado en tiempo	
*	192.168.171.247		Pedido sobrepasado en tiempo	
*	192.168.171.249		Pedido sobrepasado en tiempo	
*	192.168.171.255		Pedido sobrepasado en tiempo	
*	192.168.171.251		Pedido sobrepasado en tiempo	
*	192.168.171.253		Pedido sobrepasado en tiempo	
*	192.168.171.254		Pedido sobrepasado en tiempo	
*	192.168.171.1		Respuesta Echo	0/0/1
*	192.168.171.38		Respuesta Echo	236/244/252

Se hace un scaneo de puertos por cada sub red.

Se hace un scaneo de puertos por cada sub red. Se observa que la mayoria de los componentes escaneados tienen los mismos puertos abiertos, varia el analisis en los servidores de red, impresoras multifuncionales y radioenlaces. Ademas, muchas de las IP no estan en uso y algunos hosts estan apagados.

A continuación, se muestra el componentes de la sub red 192.168.169.0

Reporte: PortScan

Generado en 9/02/2018 a 6:28:39 p. m. por Free IP Tools.

Dirección IP	Puertos Abiertos	Nro. De Puertos Cerrados	Nro. De Puertos Silenciosos
192.168.169.30	smtp;pop3;nntp;imap	N/A	N/A
192.168.169.37	smtp;pop3;nntp;imap	N/A	N/A
192.168.169.10	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.11	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.12	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.17	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.35	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.36	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.55	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.15	smtp;http;pop3;nntp;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.1	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.2	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.3	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.4	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.5	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.31	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.41	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.51	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.61	smtp;http;pop3;nntp;imap;https	N/A	N/A
192.168.169.6	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.7	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.8	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.9	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.13	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.14	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.19	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.21	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.22	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.23	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.24	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.25	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.26	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.27	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.28	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.29	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.32	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.33	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.34	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.38	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.39	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.40	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.42	smtp;http;pop3;nntp;imap	N/A	N/A

192.168.169.43	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.44	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.47	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.48	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.49	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.50	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.52	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.53	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.54	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.56	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.57	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.58	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.59	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.60	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.169.18	smtp;http;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.45	smtp;http;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.46	smtp;http;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.16	ftp;smtp;http;pop3;nntp;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.169.20	ftp;smtp;http;pop3;nntp;netbios-ssn;imap;https;microsoft-ds	N/A	N/A

En seguida, se muestra los componentes de la sub red 192.168.170.0

Reporte: PortScan

Generado en 9/02/2018 a 6:20:33 p. m. por Free IP Tools.

Dirección IP	Puertos Abiertos	Nro. De Puertos Cerrados	Nro. De Puertos Silenciosos
192.168.170.255		N/A	N/A
192.168.170.111	ftp;smtp;http;pop3;nntp;netbios-ssn;imap;https;microsoft-ds	N/A	N/A
192.168.170.112	ftp;smtp;http;pop3;nntp;netbios-ssn;imap;https;microsoft-ds	N/A	N/A
192.168.170.113	ftp;smtp;http;pop3;nntp;netbios-ssn;imap;https;microsoft-ds	N/A	N/A
192.168.170.114	ftp;smtp;http;pop3;nntp;netbios-ssn;imap;https;microsoft-ds	N/A	N/A
192.168.170.7	ftp;smtp;pop3;nntp;imap	N/A	N/A
192.168.170.8	ftp;telnet;smtp;domain;pop3;sunrpc;nntp;netbios-ssn;imap;microsoft-ds;login	N/A	N/A
192.168.170.6	smtp;domain;http;pop3;sunrpc;nntp;netbios-ssn;imap;microsoft-ds;3128	N/A	N/A
192.168.170.21	smtp;http;pop3;nntp;epmap;netbios-ssn;imap;https;microsoft-ds	N/A	N/A
192.168.170.85	smtp;http;pop3;nntp;epmap;netbios-ssn;imap;https;microsoft-ds	N/A	N/A
192.168.170.147	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.149	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.151	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.153	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.202	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.203	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.205	smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.22	smtp;http;pop3;sunrpc;nntp;netbios-ssn;imap;https;microsoft-ds	N/A	N/A
192.168.170.33	smtp;pop3;nntp;epmap;imap;microsoft-ds	N/A	N/A
192.168.170.42	smtp;pop3;nntp;epmap;imap;microsoft-ds	N/A	N/A
192.168.170.88	smtp;pop3;nntp;epmap;imap;microsoft-ds	N/A	N/A
192.168.170.154	smtp;pop3;nntp;epmap;imap;microsoft-ds	N/A	N/A
192.168.170.9	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.11	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.17	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.20	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.25	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.26	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.27	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.29	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.30	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.31	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.32	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.36	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.37	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.38	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.41	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.44	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.45	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.48	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.49	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.51	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A

192.168.170.181	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.182	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.183	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.185	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.186	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.187	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.188	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.189	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.190	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.191	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.192	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.193	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.194	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.195	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.196	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.197	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.198	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.199	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.200	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.201	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.204	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.206	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.207	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.208	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.209	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.210	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.211	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.212	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.213	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.214	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.215	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.216	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.217	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.218	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.219	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.220	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.221	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.222	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.223	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.224	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.225	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.226	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.227	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.228	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.229	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.230	smtp;pop3;nntp;imap	N/A	N/A

192.168.170.16	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.18	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.19	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.23	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.24	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.28	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.34	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.39	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.40	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.43	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.46	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.47	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.50	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.52	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.55	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.57	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.58	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.59	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.61	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.63	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.64	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.65	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.66	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.67	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.69	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.70	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.72	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.73	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.74	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.77	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.80	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.82	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.83	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.86	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.89	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.91	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.92	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.94	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.95	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.96	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.98	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.99	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.105	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.106	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.107	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.118	smtp;pop3;nntp;imap	N/A	N/A

192.168.170.53	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.54	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.56	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.60	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.62	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.68	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.71	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.75	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.76	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.78	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.79	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.81	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.84	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.87	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.90	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.97	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.100	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.101	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.102	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.103	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.104	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.108	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.109	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.110	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.115	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.116	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.117	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.133	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.141	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.144	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.148	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.150	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.165	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.167	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.170	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.171	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.172	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.184	smtp;pop3;nntp;epmap;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.2	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.3	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.5	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.12	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.13	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.14	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.15	smtp;pop3;nntp;imap	N/A	N/A

192.168.170.231	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.232	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.233	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.234	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.235	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.236	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.237	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.238	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.239	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.241	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.242	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.243	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.244	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.245	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.246	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.247	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.248	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.249	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.250	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.251	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.252	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.253	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.254	smtp;pop3;nntp;imap	N/A	N/A
192.168.170.10	smtp;pop3;nntp;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.35	smtp;pop3;nntp;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.93	smtp;pop3;nntp;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.119	smtp;pop3;nntp;netbios-ssn;imap;microsoft-ds	N/A	N/A
192.168.170.240	telnet;smtp;http;pop3;nntp;imap	N/A	N/A
192.168.170.1	telnet;smtp;pop3;nntp;imap	N/A	N/A
192.168.170.4	telnet;smtp;pop3;nntp;imap	N/A	N/A

En seguida, se muestra los componentes de la sub red 192.168.171.0.

Reporte: PortScan

Generado en 9/02/2018 a 6:29:40 p. m. por Free IP Tools.

Dirección IP	Puertos Abiertos	Nro. De Puertos Cerrados	Nro. De Puertos Silenciosos
192.168.171.1	smtp;domain;http;pop3;nntp;imap	N/A	N/A

Reporte: PortScan

Generado en 9/02/2018 a 6:30:13 p. m. por Free IP Tools.

Dirección IP	Puertos Abiertos	Nro. De Puertos Cerrados	Nro. De Puertos Silenciosos
192.168.171.38	smtp;http;pop3;nntp;imap	N/A	N/A

Con los resultados obtenidos del análisis se concluye que, se puede hacer un plan para mejorar el estado y disponibilidad de la red de datos. Además, cabe destacar que la empresa cuenta con personal capacitado para la gestión de redes de datos.

Anexo C. Resultado acotado de análisis con herramienta Wireshark.

```
      1 0.000000       fe80::5d94:ff76:e322:cd36 ff02::1:fffd:6597      ICMPv6
86     Neighbor Solicitation for fe80::bde9:8222:6fd:6597 from
10:60:4b:90:0c:db
Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: HewlettP_90:0c:db (10:60:4b:90:0c:db), Dst:
IPv6mcast_ff:fd:65:97 (33:33:ff:fd:65:97) Internet Protocol Version 6,
Src: fe80::5d94:ff76:e322:cd36, Dst: ff02::1:fffd:6597
Internet Control Message Protocol v6
      2 0.042482       192.168.170.143        239.255.255.250        SSDP     175    M-SEARCH *
      HTTP/1.1
Frame 2: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
Ethernet II, Src: LiteonTe_4f:28:28 (94:e9:79:4f:28:28), Dst:
IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) Internet Protocol Version 4,
Src: 192.168.170.143, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 59770, Dst Port: 1900
Simple Service Discovery Protocol
      3 0.073092       192.168.169.55         239.255.255.250        IGMPv2   60     Membership
      Report group 239.255.255.250
Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Ubiquiti_86:ba:11 (68:72:51:86:ba:11), Dst:
IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) Internet Protocol Version 4,
Src: 192.168.169.55, Dst: 239.255.255.250
Internet Group Management Protocol
      4 0.093903       192.168.170.40         192.168.170.255        NBNS
92     Name query NB WPAD<00> Frame 4: 92 bytes on wire (736 bits), 92
bytes captured (736 bits) on interface 0
Ethernet II, Src: LcfcHefe_e2:58:3a (c8:5b:76:e2:58:3a),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Internet Protocol
Version 4, Src: 192.168.170.40, Dst: 192.168.170.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
      5 0.094823       fe80::245a:3cf9:e786:2dd5 ff02::1:3             LLMNR    84     Standard
      query 0x665f A wpad
Frame 5: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: LcfcHefe_e2:58:3a (c8:5b:76:e2:58:3a), Dst:
IPv6mcast_01:00:03 (33:33:00:01:00:03) Internet Protocol Version 6,
Src: fe80::245a:3cf9:e786:2dd5, Dst: ff02::1:3
User Datagram Protocol, Src Port: 63691, Dst Port: 5355
Link-local Multicast Name Resolution (query)
      6 0.094826       192.168.170.40         224.0.0.252            LLMNR    64     Standard
      query 0x665f A wpad
Frame 6: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
Ethernet II, Src: LcfcHefe_e2:58:3a (c8:5b:76:e2:58:3a), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.170.40, Dst: 224.0.0.252
User Datagram Protocol, Src Port: 63691, Dst Port: 5355
Link-local Multicast Name Resolution (query)
      7 0.095822       fe80::245a:3cf9:e786:2dd5 ff02::1:3             LLMNR    84     Standard
      query 0xbae2 AAAA wpad
Frame 7: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: LcfcHefe_e2:58:3a (c8:5b:76:e2:58:3a), Dst:
IPv6mcast_01:00:03 (33:33:00:01:00:03) Internet Protocol Version 6,
Src: fe80::245a:3cf9:e786:2dd5, Dst: ff02::1:3
User Datagram Protocol, Src Port: 49337, Dst Port: 5355
Link-local Multicast Name Resolution (query)
      8 0.095824       192.168.170.40         224.0.0.252            LLMNR    64     Standard
      query 0xbae2 AAAA wpad
```

```
Frame 8: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
Ethernet II, Src: LcfcHefe_e2:58:3a (c8:5b:76:e2:58:3a), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.170.40, Dst: 224.0.0.252
User Datagram Protocol, Src Port: 49337, Dst Port: 5355
Link-local Multicast Name Resolution (query)
      9 0.098767       Ibm_2c:6f:93          Broadcast             ARP      60     Who has
      192.168.171.149? Tell 192.168.170.20
Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Ibm_2c:6f:93 (40:f2:e9:2c:6f:93),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution
Protocol (request)
     10 0.098769       Ibm_2c:6f:92          Broadcast             ARP      60     Who has
     192.168.171.149? Tell 192.168.170.9
Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Ibm_2c:6f:92 (40:f2:e9:2c:6f:92),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution
Protocol (request)
     11 0.113668       fe80::9584:37b1:9418:cccf ff02::1:fffd:6597      ICMPv6
86     Neighbor Solicitation for fe80::bde9:8222:6fd:6597 from
00:ff:79:28:0f:0d
Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: 00:ff:79:28:0f:0d (00:ff:79:28:0f:0d), Dst:
IPv6mcast_ff:fd:65:97 (33:33:ff:fd:65:97) Internet Protocol Version 6,
Src: fe80::9584:37b1:9418:cccf, Dst: ff02::1:fffd:6597
Internet Control Message Protocol v6
     12 0.128062       192.168.170.141       239.255.255.250       SSDP     175    M-SEARCH *
     HTTP/1.1
Frame 12: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
Ethernet II, Src: Universa_55:e9:7d (e0:2a:82:55:e9:7d), Dst:
IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) Internet Protocol Version 4,
Src: 192.168.170.141, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 57515, Dst Port: 1900
Simple Service Discovery Protocol
     13 0.184207       BiostarM_9a:e0:22     Broadcast             ARP      60     Who has
     192.168.170.1? Tell 192.168.170.29
Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: BiostarM_9a:e0:22 (00:30:67:9a:e0:22),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution
Protocol (request)
     14 0.215142       fe80::11f6:b023:96e5:736f ff02::c               SSDP     208    M-SEARCH
     * HTTP/1.1
Frame 14: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0
Ethernet II, Src: 00:ff:a9:b8:94:af (00:ff:a9:b8:94:af), Dst:
IPv6mcast_0c (33:33:00:00:00:0c) Internet Protocol Version 6,
Src: fe80::11f6:b023:96e5:736f, Dst: ff02::c
User Datagram Protocol, Src Port: 50334, Dst Port: 1900

Simple Service Discovery Protocol
     15 0.218763       192.168.170.23        192.168.170.113       SNMP     160    get-request
     1.3.6.1.2.1.43.8.2.1.18.1.1
1.3.6.1.2.1.43.8.2.1.18.1.2 1.3.6.1.2.1.43.8.2.1.18.1.3 1.3.6.1.2.1.43.8.2.1.18.1.4
1.3.6.1.2.1.43.8.2.1.18.1.5
Frame 15: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
Ethernet II, Src: AioLcdPc_7d:83:4a (00:25:ab:7d:83:4a), Dst:
KyoceraD_2b:55:08 (00:17:c8:2b:55:08) Internet Protocol Version 4,
Src: 192.168.170.23, Dst: 192.168.170.113
User Datagram Protocol, Src Port: 59797, Dst Port: 161
Simple Network Management Protocol
```

```
     16 0.224079       192.168.170.113       192.168.170.23        SNMP     160    get-response
     1.3.6.1.2.1.43.8.2.1.18.1.1
1.3.6.1.2.1.43.8.2.1.18.1.2 1.3.6.1.2.1.43.8.2.1.18.1.3 1.3.6.1.2.1.43.8.2.1.18.1.4
1.3.6.1.2.1.43.8.2.1.18.1.5
Frame 16: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
Ethernet II, Src: KyoceraD_2b:55:08 (00:17:c8:2b:55:08), Dst:
AioLcdPc_7d:83:4a (00:25:ab:7d:83:4a) Internet Protocol Version 4,
Src: 192.168.170.113, Dst: 192.168.170.23
User Datagram Protocol, Src Port: 161, Dst Port: 59797
Simple Network Management Protocol
     17 0.224361       192.168.170.23        192.168.170.113       SNMP     142    get-request
     1.3.6.1.2.1.43.8.2.1.18.1.1
1.3.6.1.2.1.43.8.2.1.18.1.2 1.3.6.1.2.1.43.8.2.1.18.1.3 1.3.6.1.2.1.43.8.2.1.18.1.4
Frame 17: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: AioLcdPc_7d:83:4a (00:25:ab:7d:83:4a), Dst:
KyoceraD_2b:55:08 (00:17:c8:2b:55:08) Internet Protocol Version 4,
Src: 192.168.170.23, Dst: 192.168.170.113
User Datagram Protocol, Src Port: 59797, Dst Port: 161
Simple Network Management Protocol
     18 0.231318       192.168.170.113       192.168.170.23        SNMP     142    get-response
     1.3.6.1.2.1.43.8.2.1.18.1.1
1.3.6.1.2.1.43.8.2.1.18.1.2 1.3.6.1.2.1.43.8.2.1.18.1.3 1.3.6.1.2.1.43.8.2.1.18.1.4
Frame 18: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: KyoceraD_2b:55:08 (00:17:c8:2b:55:08), Dst:
AioLcdPc_7d:83:4a (00:25:ab:7d:83:4a) Internet Protocol Version 4,
Src: 192.168.170.113, Dst: 192.168.170.23
User Datagram Protocol, Src Port: 161, Dst Port: 59797
Simple Network Management Protocol
     19 0.231697       192.168.170.23        192.168.170.113       SNMP     124    get-request
     1.3.6.1.2.1.43.8.2.1.18.1.1
1.3.6.1.2.1.43.8.2.1.18.1.2 1.3.6.1.2.1.43.8.2.1.18.1.3
Frame 19: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
Ethernet II, Src: AioLcdPc_7d:83:4a (00:25:ab:7d:83:4a), Dst:
KyoceraD_2b:55:08 (00:17:c8:2b:55:08) Internet Protocol Version 4,
Src: 192.168.170.23, Dst: 192.168.170.113
User Datagram Protocol, Src Port: 59797, Dst Port: 161
Simple Network Management Protocol
     20 0.236518       192.168.170.113       192.168.170.23        SNMP     151    get-response
     1.3.6.1.2.1.43.8.2.1.18.1.1
1.3.6.1.2.1.43.8.2.1.18.1.2 1.3.6.1.2.1.43.8.2.1.18.1.3
Frame 20: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
Ethernet II, Src: KyoceraD_2b:55:08 (00:17:c8:2b:55:08), Dst:
AioLcdPc_7d:83:4a (00:25:ab:7d:83:4a) Internet Protocol Version 4,
Src: 192.168.170.113, Dst: 192.168.170.23
User Datagram Protocol, Src Port: 161, Dst Port: 59797
Simple Network Management Protocol
     21 0.240135       192.168.171.95        224.0.0.252           LLMNR    68     Standard
     query 0xaf69 A Jefecali
Frame 21: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Ethernet II, Src: 00:ff:d3:c4:e3:bf (00:ff:d3:c4:e3:bf), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.171.95, Dst: 224.0.0.252
User Datagram Protocol, Src Port: 51022, Dst Port: 5355
Link-local Multicast Name Resolution (query)
     22 0.240937       fe80::2900:ba19:dc87:c48e ff02::1:3             LLMNR    88     Standard
     query 0xaf69 A Jefecali
Frame 22: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
```

```
Ethernet II, Src: 00:ff:d3:c4:e3:bf (00:ff:d3:c4:e3:bf), Dst:
IPv6mcast_01:00:03 (33:33:00:01:00:03) Internet Protocol Version 6,
Src: fe80::2900:ba19:dc87:c48e, Dst: ff02::1:3
User Datagram Protocol, Src Port: 57956, Dst Port: 5355
Link-local Multicast Name Resolution (query)
     23 0.254228       fe80::6505:9ac:d48a:768b ff02::16              ICMPv6   90     Multicast
     Listener Report Message v2
Frame 23: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv6mcast_16 (33:33:00:00:00:16) Internet Protocol Version 6,
Src: fe80::6505:9ac:d48a:768b, Dst: ff02::16
Internet Control Message Protocol v6
     24 0.267201       192.168.170.21         192.168.170.255        UDP      170    60894 →
     50007 Len=128
Frame 24: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
Ethernet II, Src: HewlettP_c0:a9:19 (a0:48:1c:c0:a9:19), Dst:
Broadcast (ff:ff:ff:ff:ff:ff) Internet Protocol Version 4,
Src: 192.168.170.21, Dst: 192.168.170.255
User Datagram Protocol, Src Port: 60894, Dst Port: 50007
Data (128 bytes)
0000  4a b5 7f e5 21 43 bd f3 2d 9e da ff f9 b6 b3 37   J...!C..-......7
0010  82 f6 c4 bd f2 a0 21 72 b1 4c b7 87 58 67 ca 70   ......!r.L..Xg.p
0020  30 e0 91 17 7d 91 88 ab 19 9f fb c7 08 b1 75 4c   0...}.........uL
0030  f5 8e 16 d8 57 a9 68 db cc ba 47 4c 72 0c 60 47   ....W.h...GLr.`G
0040  a4 e9 9e 34 83 11 c3 22 c5 b9 53 f4 77 0a 0b e0   ...4..."..S.w...
0050  1d f5 13 96 a4 b7 57 bb 5a 0e 61 f8 8a ba 02 89   ......W.Z.a.....
0060  b8 ba f5 87 09 1e 62 b7 26 64 cb 70 23 f7 9a 94   ......b.&d.p#...
0070  55 18 f0 c4 12 ba f4 45 14 7e 4d f3 3a 4d 58 0f   U......E.~M.:MX.
     25 0.268651       HewlettP_5f:39:de      Broadcast              ARP      60     Who has
     192.168.1.170?  Tell 192.168.170.6
Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0Ethernet II,
Src: HewlettP_5f:39:de (00:1e:0b:5f:39:de), Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address
Resolution Protocol (request)
     26 0.272653       HewlettP_5f:39:de      Broadcast              ARP      60     Who has
     192.168.170.178?  Tell 192.168.170.6
Frame 26: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: HewlettP_5f:39:de (00:1e:0b:5f:39:de),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution
Protocol (request)
     27 0.278982       fe80::6505:9ac:d48a:768b ff02::16              ICMPv6   90     Multicast
     Listener Report Message v2
Frame 27: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv6mcast_16 (33:33:00:00:00:16) Internet Protocol Version 6,
Src: fe80::6505:9ac:d48a:768b, Dst: ff02::16
Internet Control Message Protocol v6
     28 0.279862       192.168.170.165        224.0.0.252            IGMPv2   60     Membership
     Report group 224.0.0.252
Frame 28: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.170.165, Dst: 224.0.0.252
Internet Group Management Protocol
     29 0.280792       192.168.170.165        224.0.0.252            IGMPv2   60     Membership
     Report group 224.0.0.252
Frame 29: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
```

```
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.170.165, Dst: 224.0.0.252
Internet Group Management Protocol
     30 0.280834       fe80::6505:9ac:d48a:768b ff02::16              ICMPv6   90     Multicast
     Listener Report Message v2
Frame 30: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv6mcast_16 (33:33:00:00:00:16) Internet Protocol Version 6,
Src: fe80::6505:9ac:d48a:768b, Dst: ff02::16
Internet Control Message Protocol v6
     31 0.280836       fe80::6505:9ac:d48a:768b ff02::16              ICMPv6   90     Multicast
     Listener Report Message v2
Frame 31: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv6mcast_16 (33:33:00:00:00:16) Internet Protocol Version 6,
Src: fe80::6505:9ac:d48a:768b, Dst: ff02::16
Internet Control Message Protocol v6
     32 0.280839       192.168.170.165       224.0.0.2             IGMPv2   60     Leave Group
     224.0.0.252
Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv4mcast_02 (01:00:5e:00:00:02) Internet Protocol Version 4,
Src: 192.168.170.165, Dst: 224.0.0.2
Internet Group Management Protocol
     33 0.280840       192.168.170.202       224.0.0.252           IGMPv2   60     Membership
     Query, specific for group
224.0.0.252
Frame 33: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Tp-LinkT_e5:fd:18 (a4:2b:b0:e5:fd:18), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.170.202, Dst: 224.0.0.252
Internet Group Management Protocol
     34 0.281808       fe80::6505:9ac:d48a:768b ff02::1:3             LLMNR    88
Standard query 0x46a9 ANY SISTEMAS Frame 34: 88 bytes on wire (704 bits), 88 bytes
captured (704 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv6mcast_01:00:03 (33:33:00:01:00:03) Internet Protocol Version 6,
Src: fe80::6505:9ac:d48a:768b, Dst: ff02::1:3
User Datagram Protocol, Src Port: 64686, Dst Port: 5355
Link-local Multicast Name Resolution (query)
     35 0.282755       192.168.170.165       224.0.0.252           LLMNR    68
Standard query 0x46a9 ANY SISTEMAS Frame 35: 68 bytes on wire (544 bits), 68 bytes
captured (544 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.170.165, Dst: 224.0.0.252
User Datagram Protocol, Src Port: 64686, Dst Port: 5355
Link-local Multicast Name Resolution (query)
     36 0.282761       192.168.170.165       239.255.255.250       SSDP     179    M-SEARCH *
     HTTP/1.1
Frame 36: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) Internet Protocol Version 4,
Src: 192.168.170.165, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 57728, Dst Port: 1900
Simple Service Discovery Protocol
     37 0.325946       192.168.170.23        224.0.0.252           IGMPv2   46     Membership
     Report group 224.0.0.252
Frame 37: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
```

```
Ethernet II, Src: AioLcdPc_7d:83:4a (00:25:ab:7d:83:4a), Dst:
IPv4mcast_fc (01:00:5e:00:00:fc) Internet Protocol Version 4,
Src: 192.168.170.23, Dst: 224.0.0.252
Internet Group Management Protocol
     38 0.337533       fe80::9584:37b1:9418:cccf ff02::c               SSDP     208    M-SEARCH
     * HTTP/1.1
Frame 38: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0
Ethernet II, Src: 00:ff:79:28:0f:0d (00:ff:79:28:0f:0d), Dst:
IPv6mcast_0c (33:33:00:00:00:0c) Internet Protocol Version 6,
Src: fe80::9584:37b1:9418:cccf, Dst: ff02::c
User Datagram Protocol, Src Port: 59048, Dst Port: 1900
Simple Service Discovery Protocol
     39 0.344361       fe80::6505:9ac:d48a:768b ff02::16              ICMPv6   90     Multicast
     Listener Report Message v2
Frame 39: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: QuantaCo_36:3e:f0 (04:7d:7b:36:3e:f0), Dst:
IPv6mcast_16 (33:33:00:00:00:16) Internet Protocol Version 6,
Src: fe80::6505:9ac:d48a:768b, Dst: ff02::16

     40 0.356284       fe80::79ba:d568:8039:6bea ff02::1:fff4:dc74      ICMPv6   86     Neighbor
     Solicitation for fe80::529f:
27ff:fef4:dc74 from 00:ff:63:58:d6:fe
Frame 40: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: 00:ff:63:58:d6:fe (00:ff:63:58:d6:fe), Dst:
IPv6mcast_ff:f4:dc:74 (33:33:ff:f4:dc:74) Internet Protocol Version 6,
Src: fe80::79ba:d568:8039:6bea, Dst: ff02::1:fff4:dc74
Internet Control Message Protocol v6
     41 0.383761       Pegatron_2e:35:74     Broadcast             ARP      60     Who has
     192.168.170.47? Tell 192.168.170.42
Frame 41: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Pegatron_2e:35:74 (38:60:77:2e:35:74),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution
Protocol (request)
     42 0.386623       HewlettP_c1:3a:ce     Broadcast             ARP      60     Who has
     192.168.170.82? Tell 192.168.4.1
Frame 42: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: HewlettP_c1:3a:ce (b4:b5:2f:c1:3a:ce),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution
Protocol (request)
     43 0.387457       Pegatron_ba:a0:d1     Broadcast             ARP      60     Who has
     192.168.170.95? Tell 192.168.170.100
Frame 43: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Pegatron_ba:a0:d1 (e0:69:95:ba:a0:d1),
Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution
Protocol (request)
```

Anexo D. Instalación y configuración servidor DNS bind9.

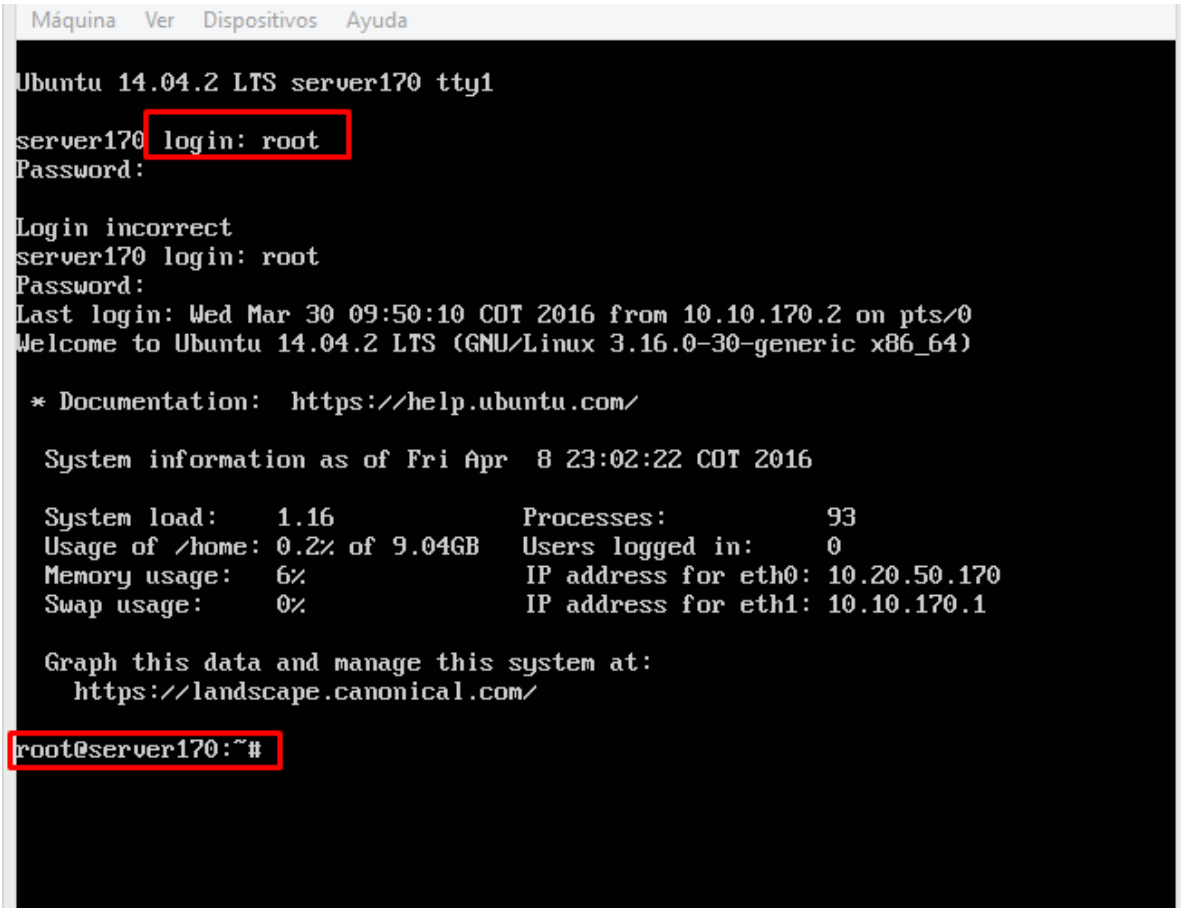
ÍNDICE

Pág.

1. INSTALACION Y CONFIGURACION DE BIND9 304
2. RESOLUCION DIRECTA 311
3. RESOLUCION INVERSA 313

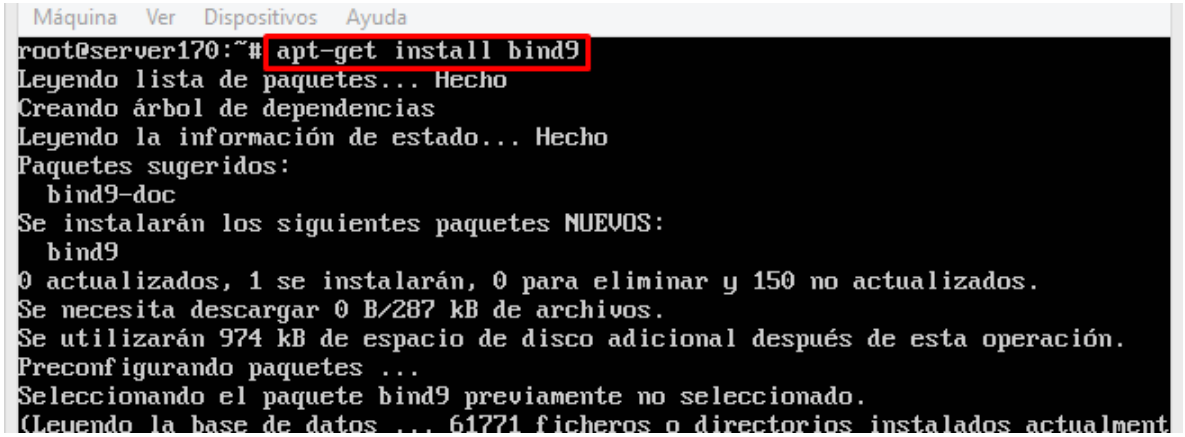
1. INSTALACION Y CONFIGURACION DE BIND9

En primer lugar, se accede al servidor, en este caso se ingresa como **root** tal como se observa en la siguiente imagen.

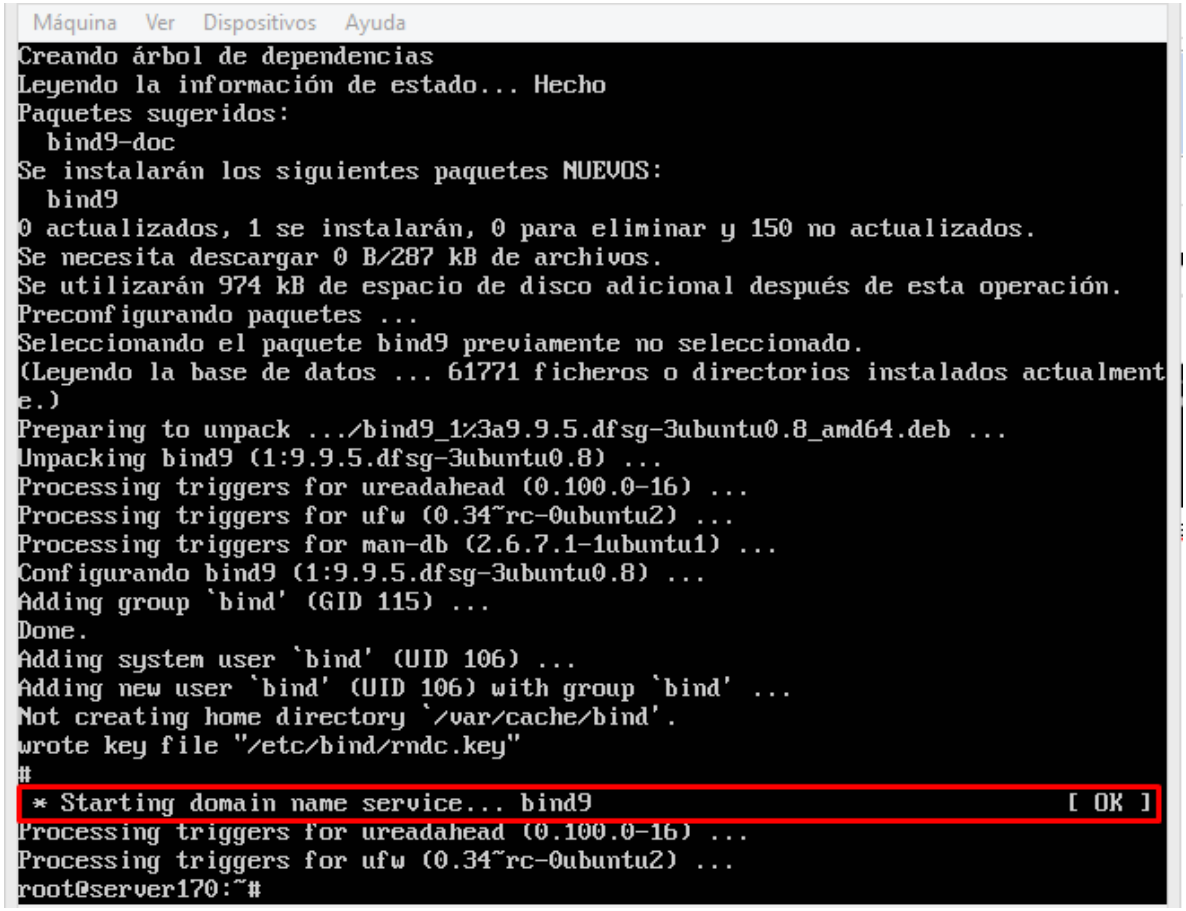


Se configura BIND9 para disponer de un servidor DNS en una intranet, que resuelva dominios internos. El servidor DNS se encargará de resolver esos dominios en sus respectivas IPs, además de resolver otros dominios de Internet como “google.com”.

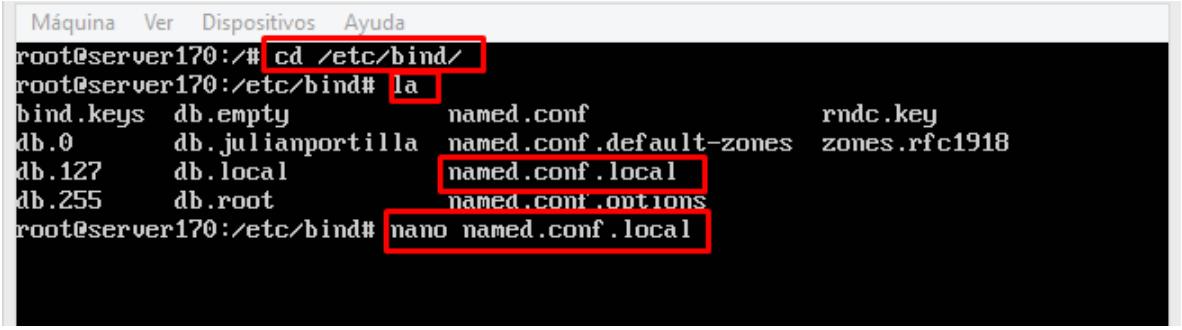
Ahora, se instala bin9 en nuestro servidor.



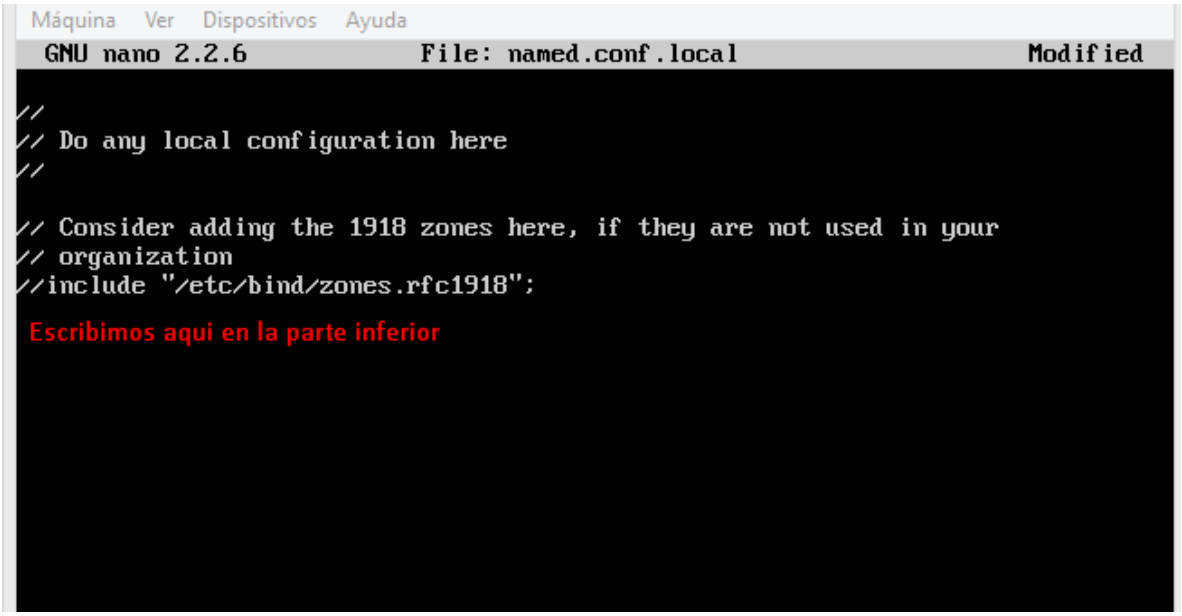
Al finalizar la instalación de bind9 el servicio debe aparecer como **OK**



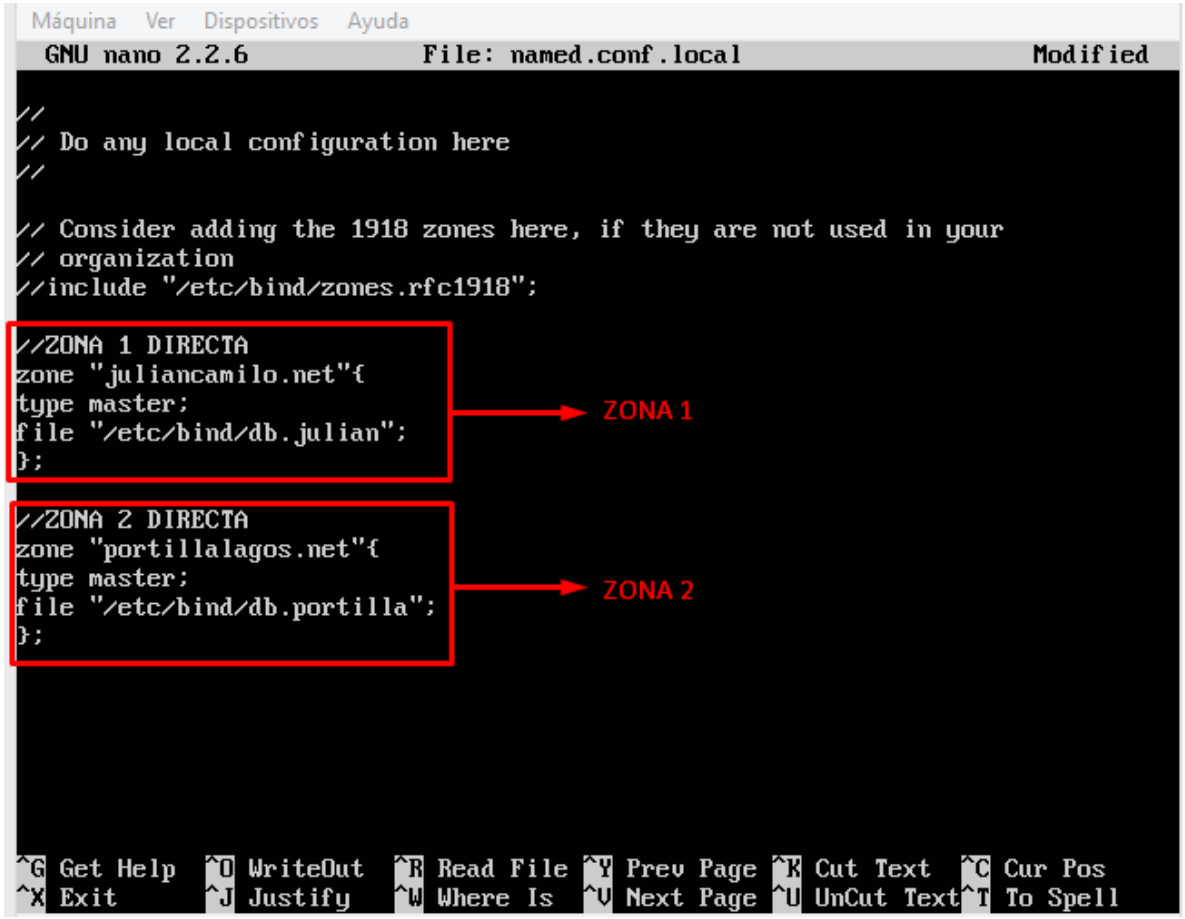
Para dirigirse a los archivos de configuración de bind9 se va hacia la carpeta bind que se encuentra en la ruta **/etc/bind,** en esta carpeta se edita el archivo **named.conf.local**



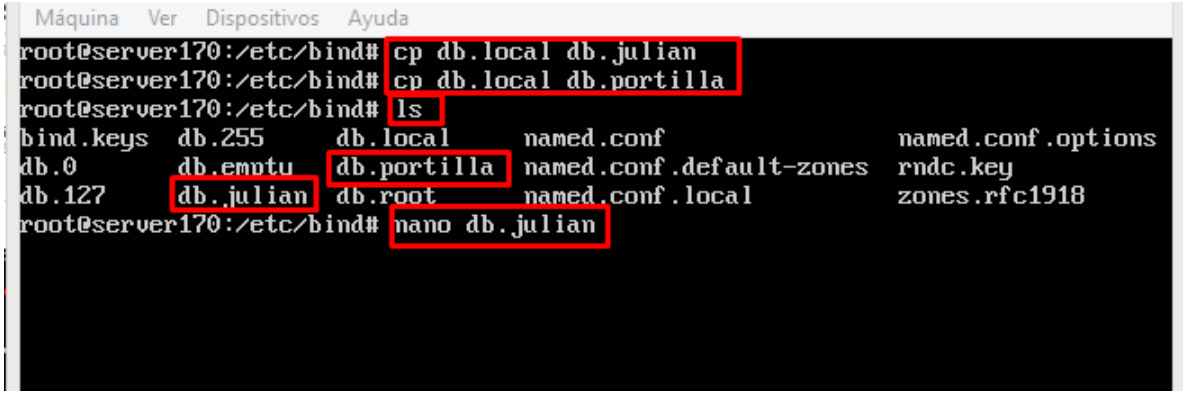
Para editar este archivo se lo hace en la parte inferior, esto como para dar orden al archivo.



Se colocan las zonas directas de los dominios **juliancamilo.net** y **portillalagos.net**

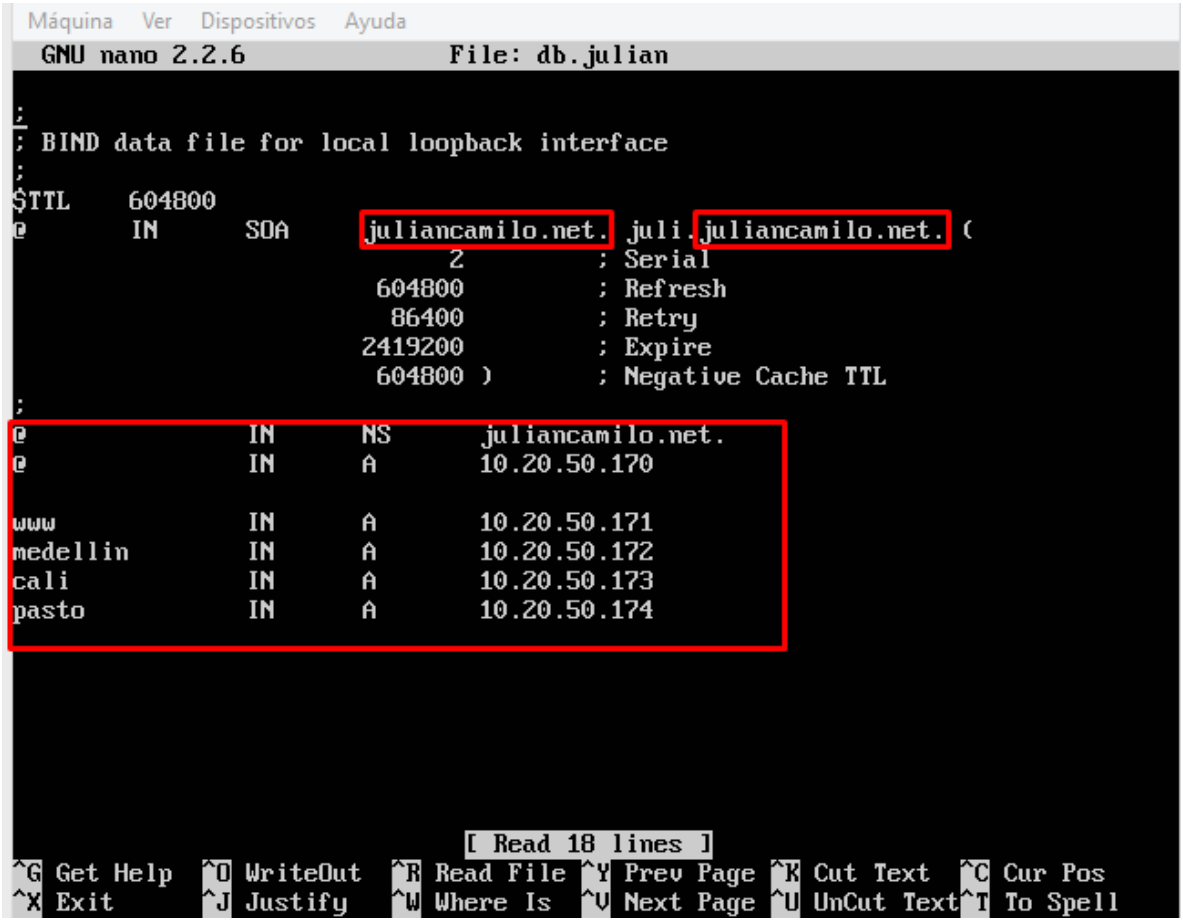


Luego se crea a partir del archivo **db.local** los archivos **db.julian** y **db.portilla,** en estos archivos se configura el DNS.



Ya dentro del archivo **db.julian** se cambia en donde dice **localhost** por el nombre de dominio, en este caso por **juliancamilo.net.**

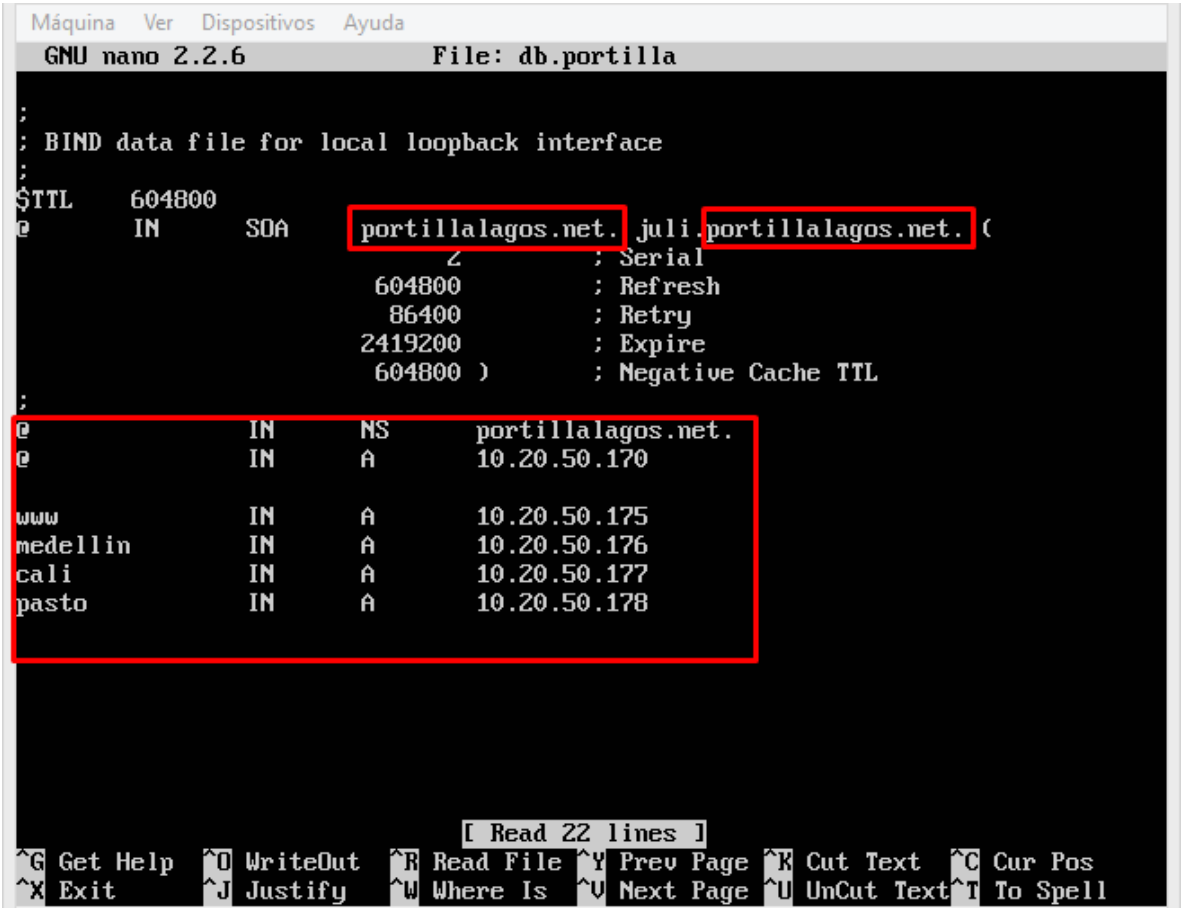
Además del cambio del nombre de dominio se registra en cada uno de los dominios a los hosts “medellin”, “cali” y “pasto”. Asignando una IP diferente a cada host. Se guardan los cambios.



Ahora se edita el archivo **db.portilla**



Ya dentro del archivo **db.portilla** se camba en donde dice **localhost** por el nombre de dominio, en este caso por **portillalagos.net.**
Además del cambio del nombre de dominio se registra en cada uno de los dominios a los hosts “medellin”, “cali” y “pasto”. Asignando una IP diferente a cada host.
Se Guardan los cambios.



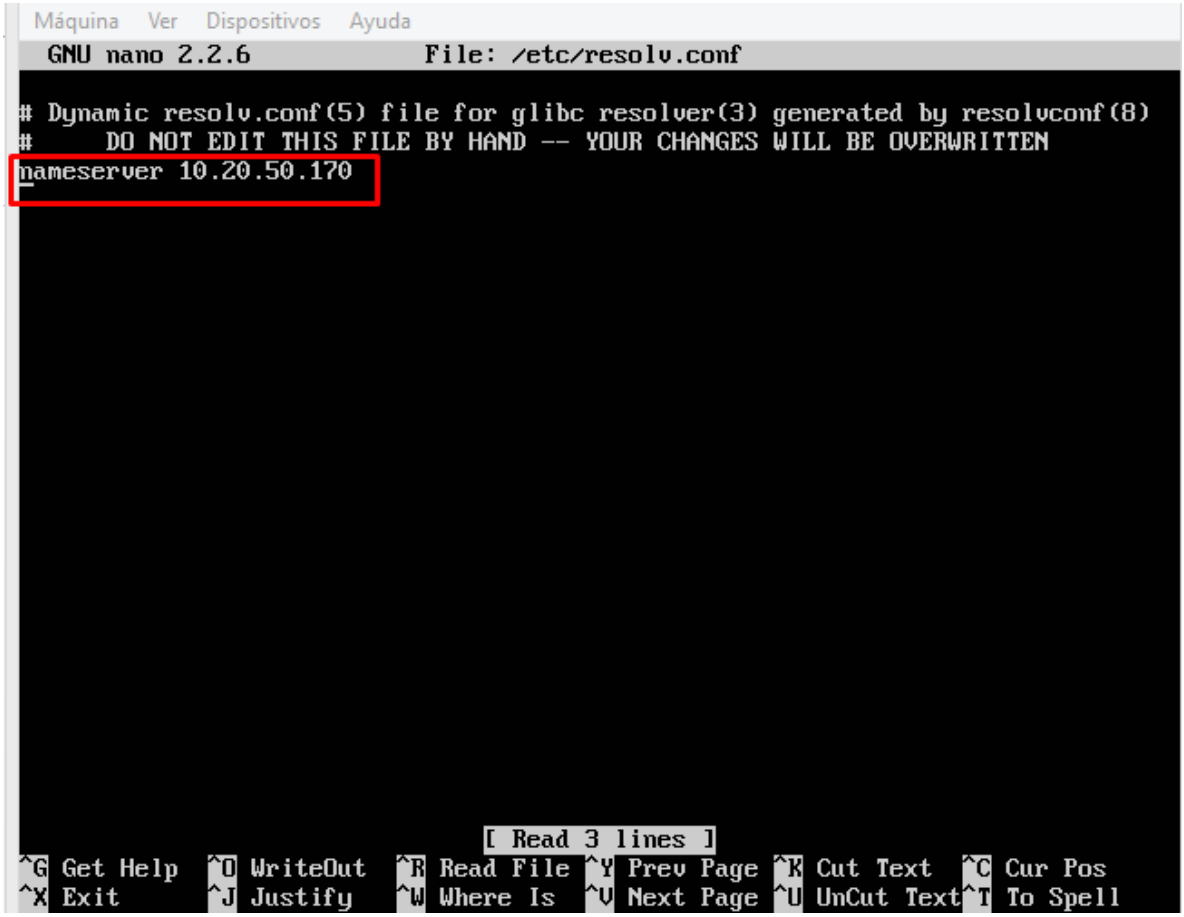
Al terminar la configuración de los anteriores archivos, se procede a reiniciar el servicio de **bin9,** se debe tener en cuenta que tanto el **Stopping** como el **Starting** estén en **OK.**



A continuación se edita el archivo **resolv.conf,** en el cual se coloca el dominio de nuestro servidor.

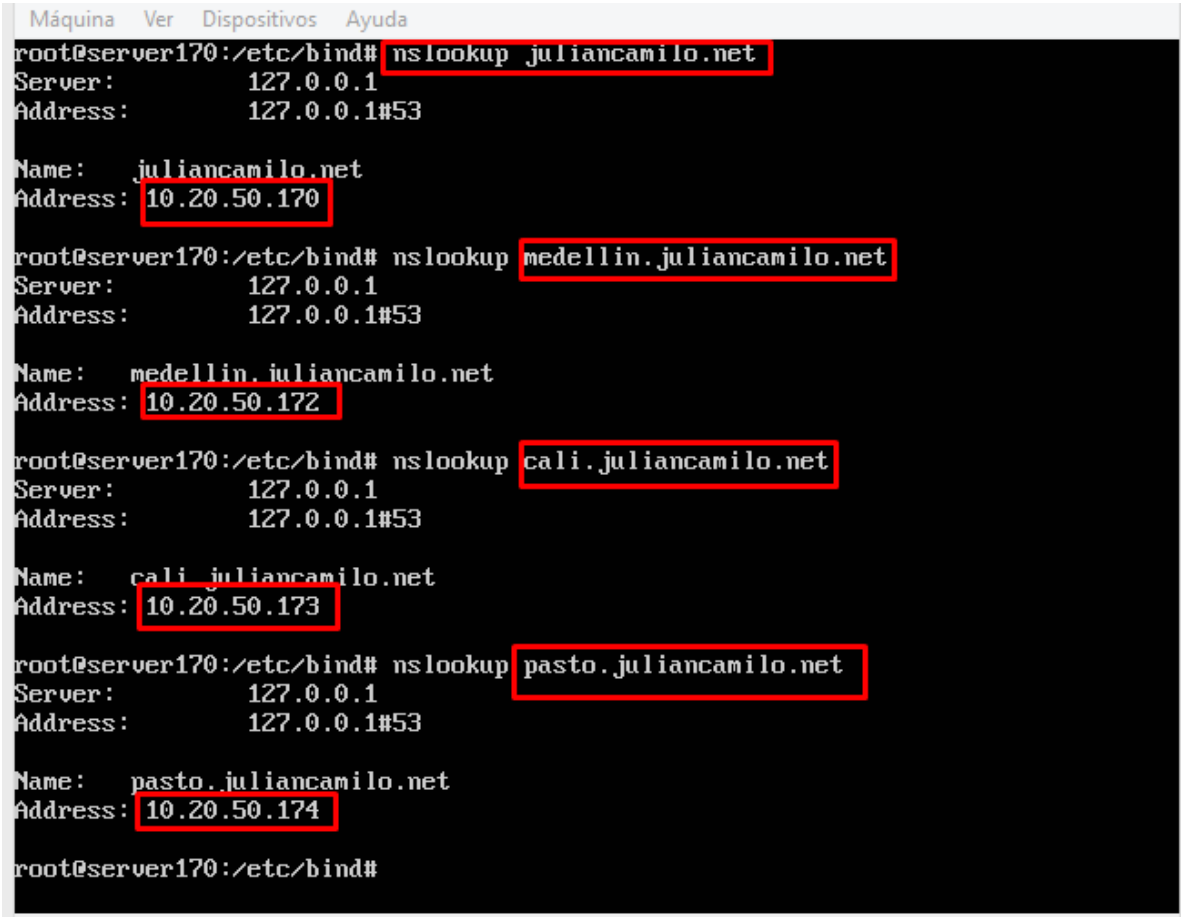


Ya dentro del archivo se coloca la dirección IP de nuestro servidor DNS, mediante la línea **nameserver 10.20.50.170**

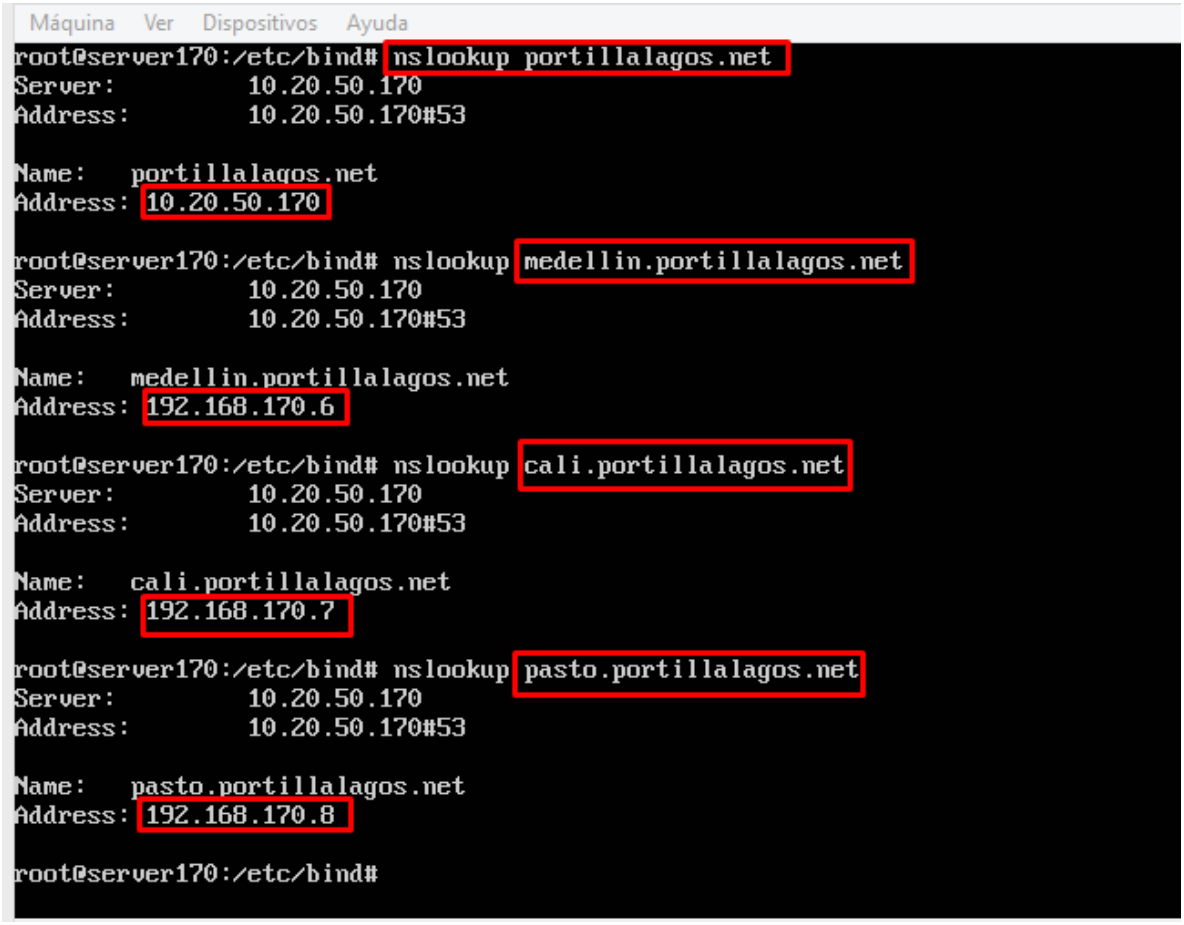


2. RESOLUCION DIRECTA

La resolución directa fue previamente configurada mediante la configuración del archivo **named.conf.local** realizada en el punto anterior. Para visualizar que IP fue asignada al dominio **juliancamilo.net, medellin.juliancamilo.net, cali.juliancamilo.net, pasto.juliancamilo.net,** se debe anteponer el comando **nslookup.**



De igual manera para los dominios **portillalagos.net, medellin.portillalagos.net, cali.portillalagos.net, pasto.portillalagos.net**

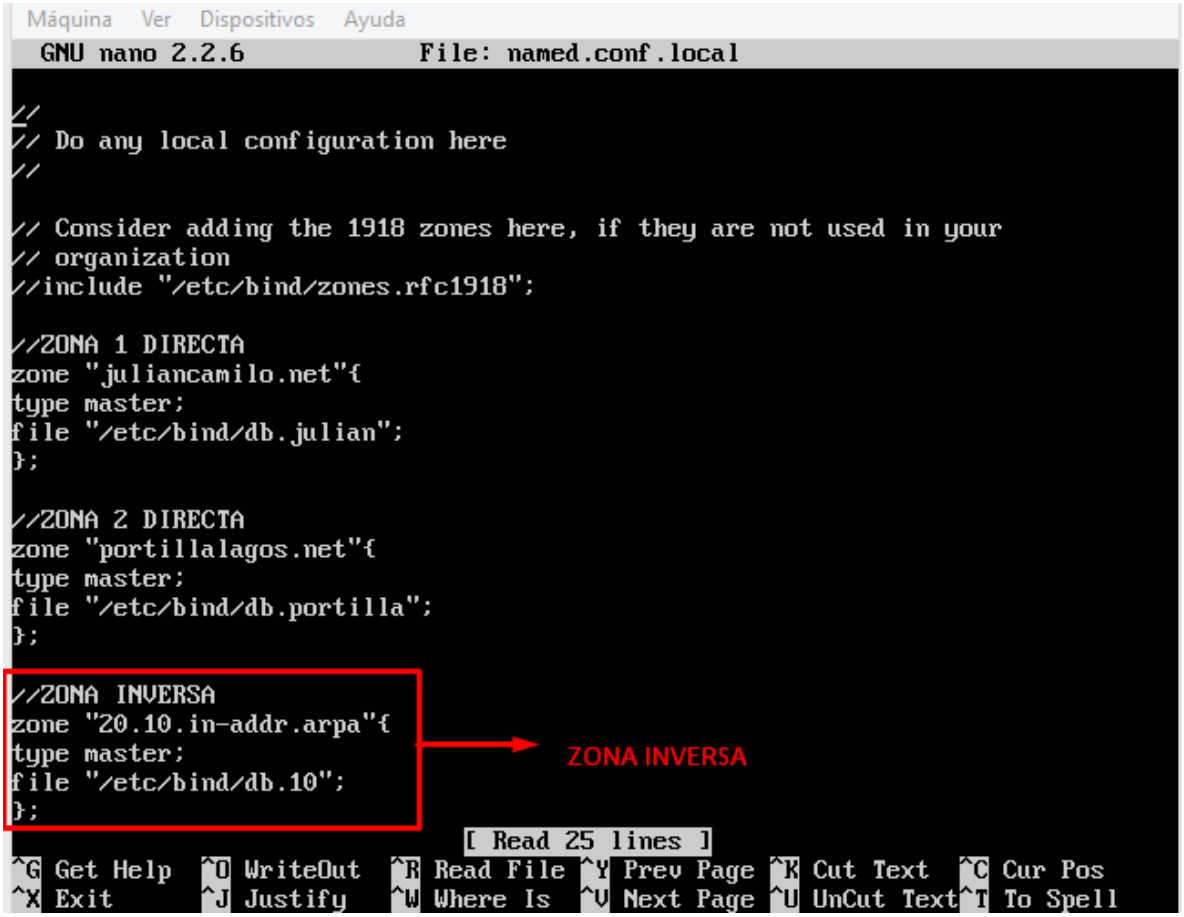


3. RESOLUCION INVERSA

Para la configuración de resolución inversa se edita el archivo **named.conf.local**



Ya dentro de este archivo se configura la zona inversa, tal y como se muestra en la siguiente imagen.



Posteriormente se crea un archivo el cual va a ser la base de datos donde se encuentran los diferentes registros de la zona inversa, este archivo se crea a partir del archivo **db.127**. Una vez creado lo se edita con **nano.**

```
Máquina  Ver  Dispositivos  Ayuda
root@server170:/etc/bind# cp db.127 db.10
root@server170:/etc/bind# ls
bind.keys   db.255     db.portilla               named.conf.local
db.0        db.empty   db.root                   named.conf.options
db.10       db.julian  named.conf                rndc.key
db.127      db.local   named.conf.default-zones  zones.rfc1918
root@server170:/etc/bind# nano db.10_
```

Ya dentro del archivo en este caso **db.10,** se cambia **localhost** por en nombre de dominio en este caso **juliancamilo.net.** El registro PTR es el registro de recurso (RR) de un dominio que define las direcciones IP de todos los sistemas en una notación invertida.

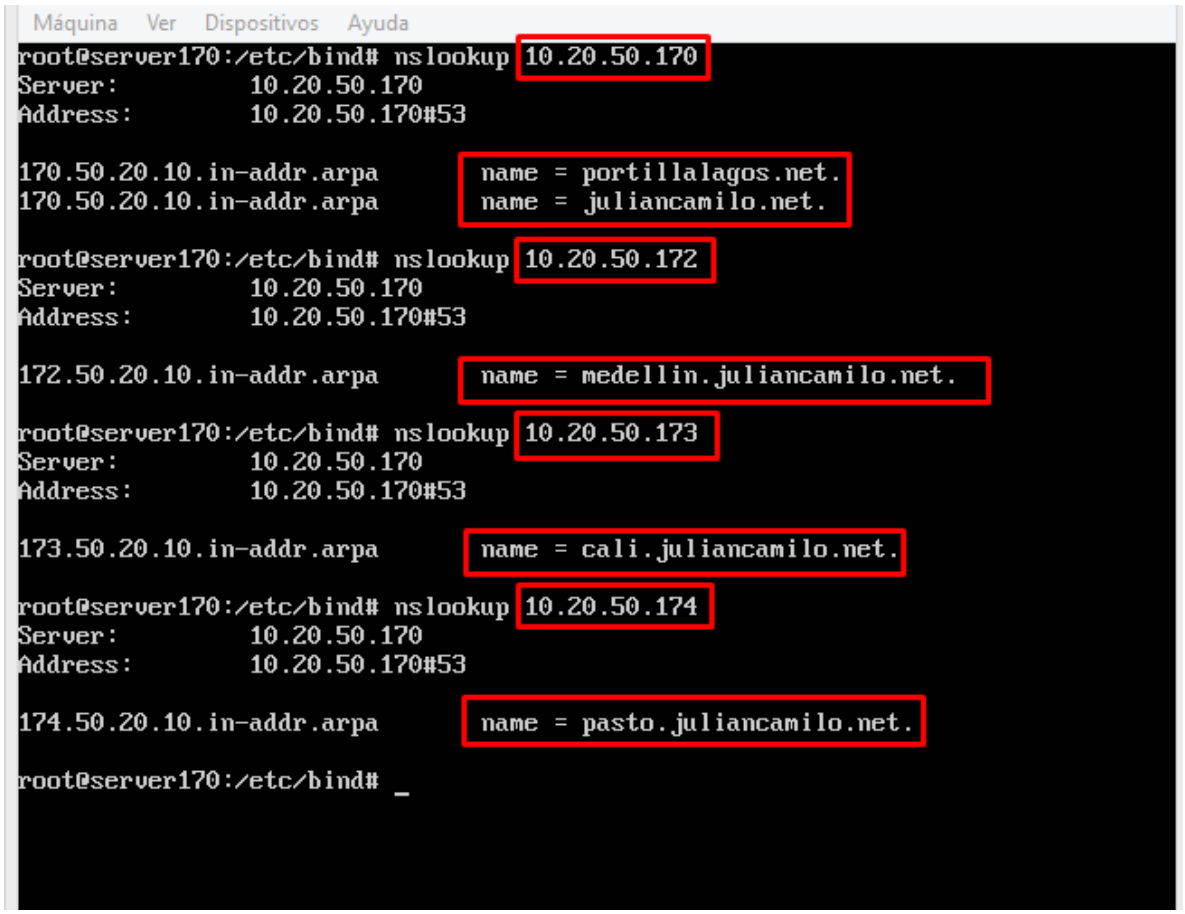
```
Máquina  Ver  Dispositivos  Ayuda
 GNU nano 2.2.6                File: db.10

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     juliancamilo.net. juli.juliancamilo.net. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      juliancamilo.net.
170.50  IN      PTR     juliancamilo.net.
172.50  IN      PTR     medellin.juliancamilo.net.
173.50  IN      PTR     cali.juliancamilo.net.
174.50  IN      PTR     pasto.juliancamilo.net.

@       IN      NS      portillalagos.net.
170.50  IN      PTR     portillalagos.net.
176.50  IN      PTR     medellin.portillalagos.net.
177.50  IN      PTR     cali.portillalagos.net.
178.50  IN      PTR     pasto.portillalagos.net.

                [ Read 26 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Una vez hecha la configuración de los anteriores archivos mediante el comando **nslookup** se verifica como colocando la dirección IP da el nombre de dominio.


Máquina Ver Dispositivos Ayuda
root@server170:/etc/bind# nslookup 10.20.50.170
Server: 10.20.50.170
Address: 10.20.50.170#53
170.50.20.10.in-addr.arpa name = portillalagos.net.
170.50.20.10.in-addr.arpa name = juliancamilo.net.
root@server170:/etc/bind# nslookup 10.20.50.172
Server: 10.20.50.170
Address: 10.20.50.170#53
172.50.20.10.in-addr.arpa name = medellin.juliancamilo.net.
root@server170:/etc/bind# nslookup 10.20.50.173
Server: 10.20.50.170
Address: 10.20.50.170#53
173.50.20.10.in-addr.arpa name = cali.juliancamilo.net.
root@server170:/etc/bind# nslookup 10.20.50.174
Server: 10.20.50.170
Address: 10.20.50.170#53
174.50.20.10.in-addr.arpa name = pasto.juliancamilo.net.
root@server170:/etc/bind#

Anexo E. Instalación y configuración de servidor web Apache.

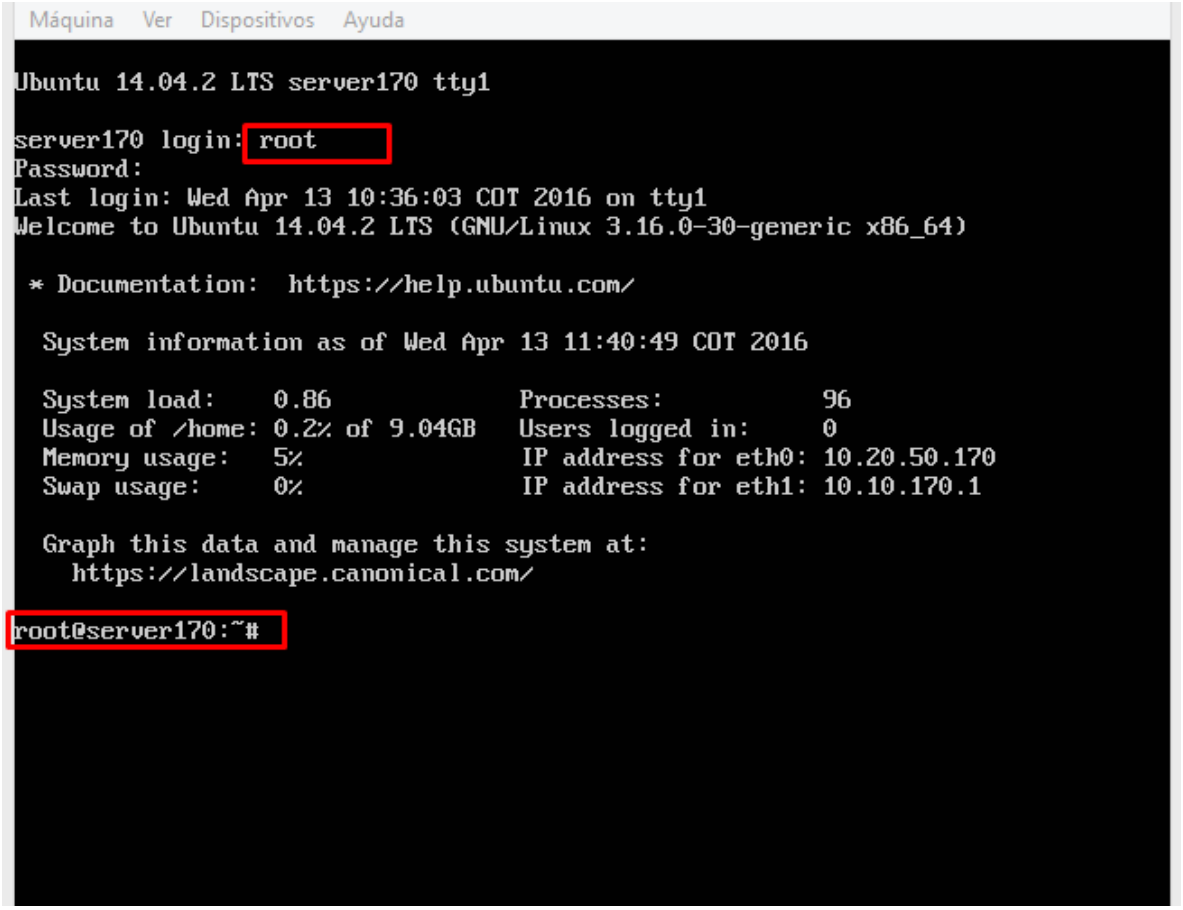
ÍNDICE

Pág.

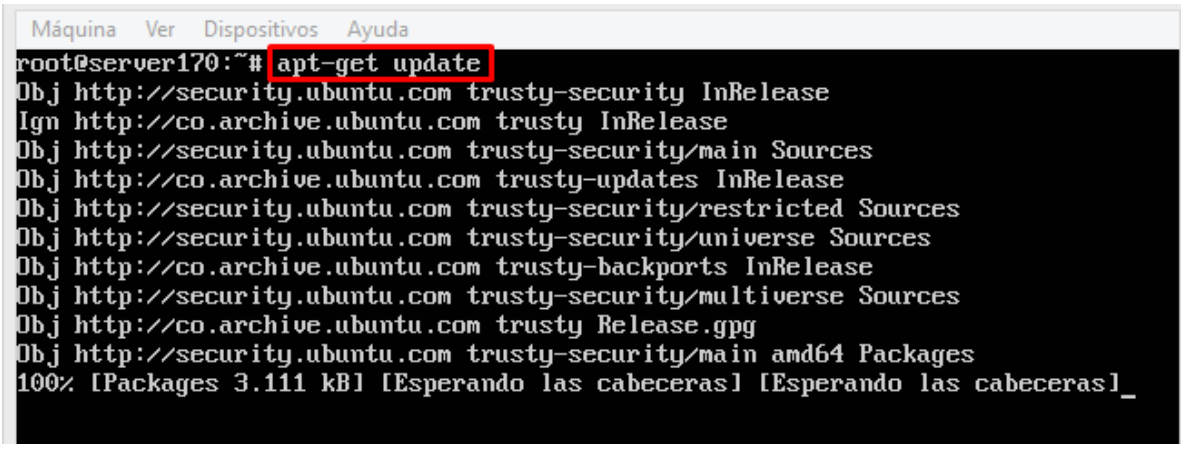
1. INSTALACION Y CONFIGURACION DE APACHE 317
2. MODIFICACION DE PUERTO 322
3. AUTENTICACION EN APACHE 324

1. INSTALACION Y CONFIGURACION DE APACHE

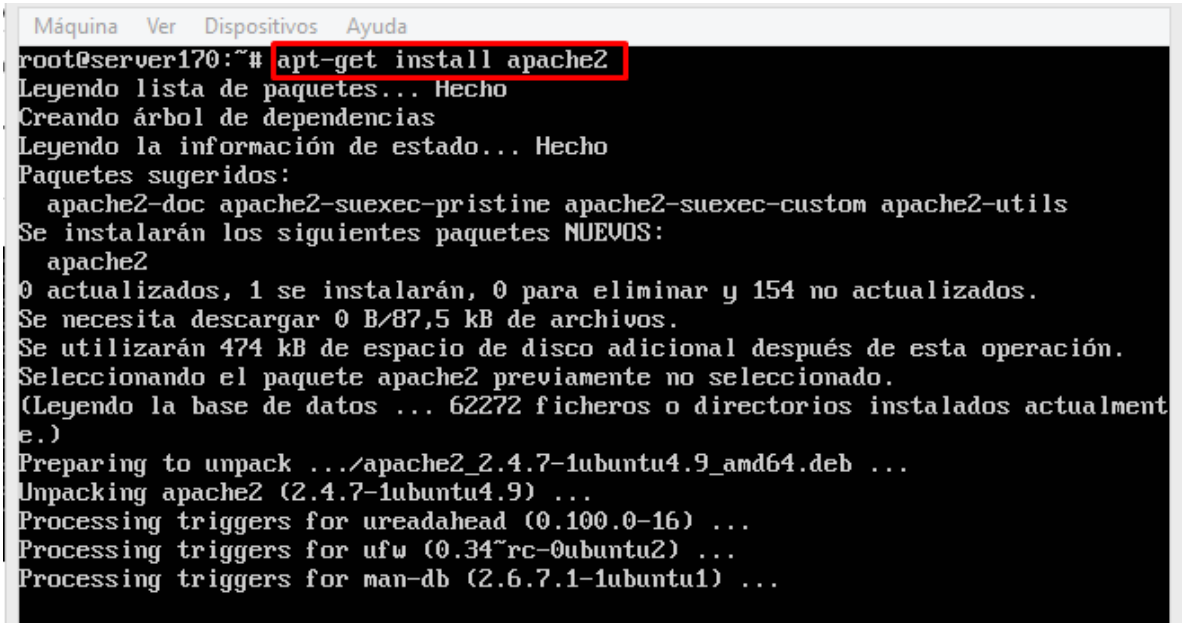
En primer lugar, se ingresa al servidor Ubuntu como usuario root.



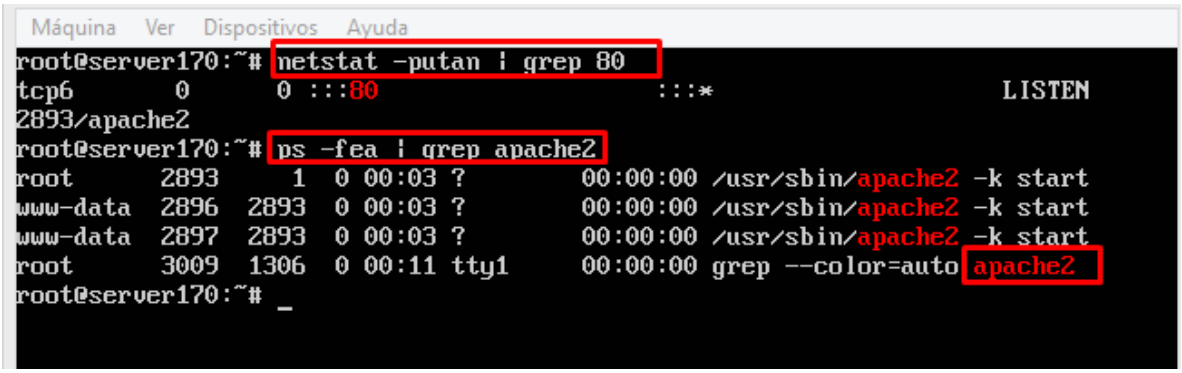
Actualizar los repositorios del servidor con el comando apt-get update.



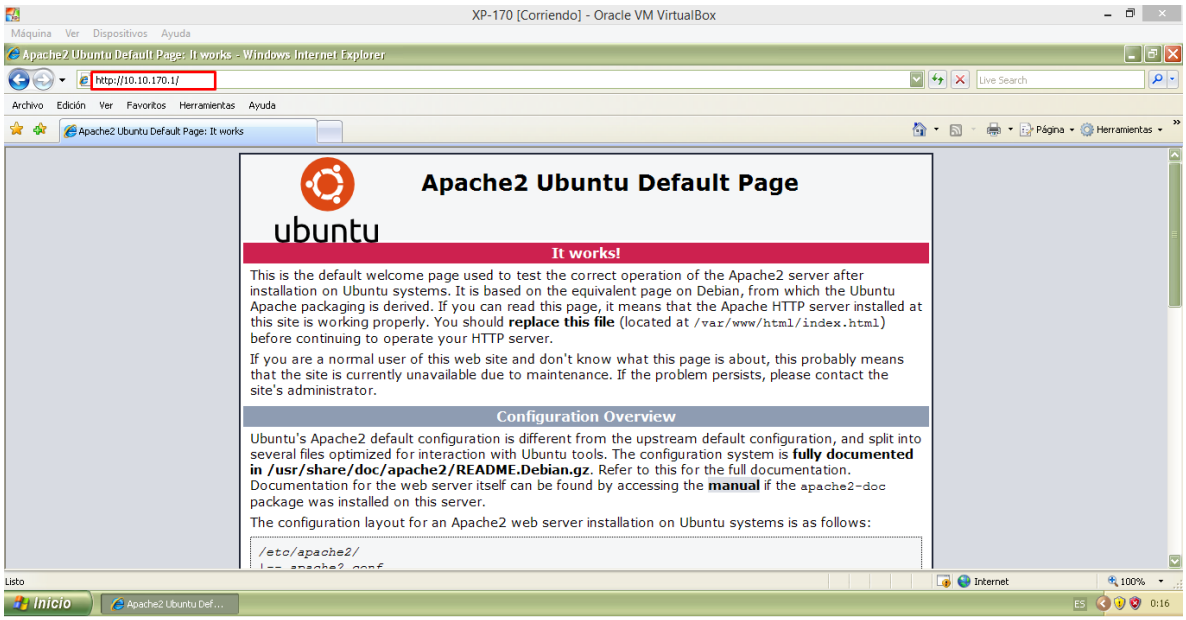
Instalar el servidor web apache con el comando apt-get install apache2.



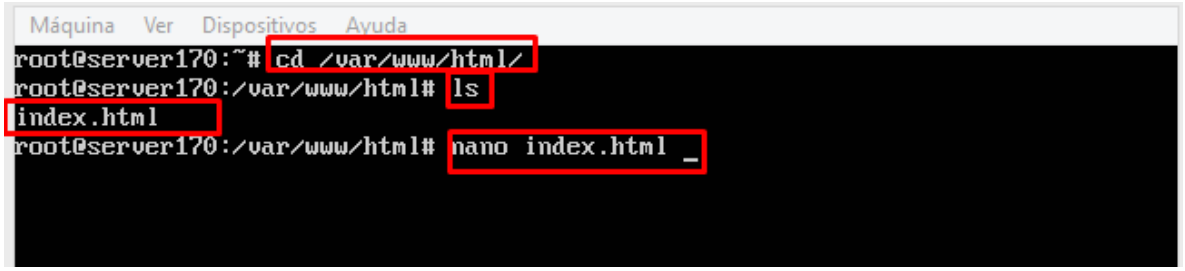
Una vez instalado se verifica que el puerto 80 por defecto está escuchando, como también que el proceso se apache2 está corriendo, tal y como se muestra en la imagen.



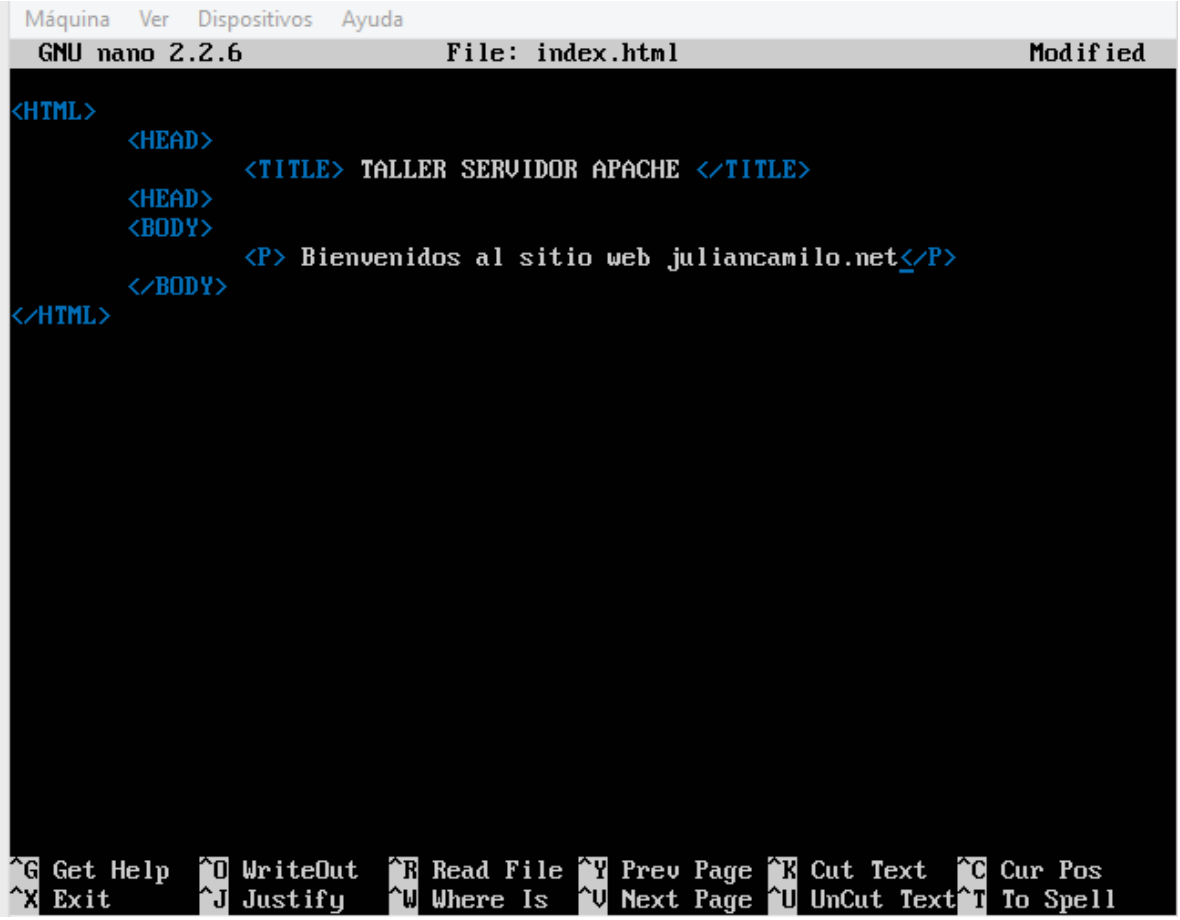
Se puede verificar que el servidor está corriendo colocando en la url de la maquina XP que se encuentra en red con el servidor Ubuntu, la puerta de enlace, en este caso la 10.10.10701.



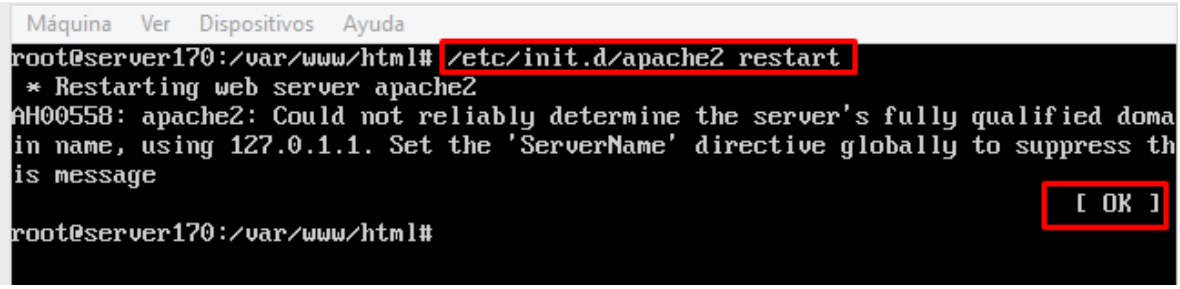
Luego, se accede a la direccion /var/www/html/ , donde se crea un archivo index.html, para hacer una página web básica.



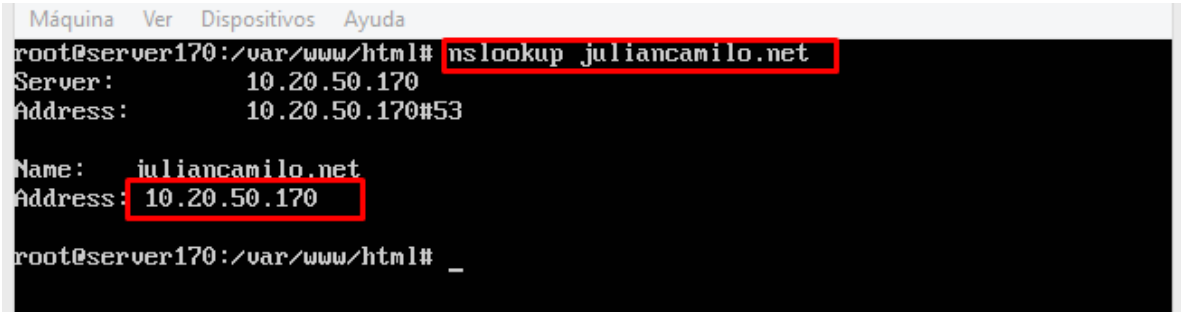
Dentro del archivo se escribe el código básico de la página tal como se muestra en la siguiente imagen.



Una vez hecho lo anterior se debe reiniciar el servidor web para que los cambios sean aplicados.



Se Verifica que el dominio esté funcionando de forma adecuada, esto mediante el comando nslookup nombre_dominio, si está bien configurado, nos devolverá la dirección IP del servidor DNS, tal como se muestra en la siguiente imagen.



Se verifica colocando el nombre del dominio en la url de la máquina XP, mostrara la página de bienvenida creada anteriormente.

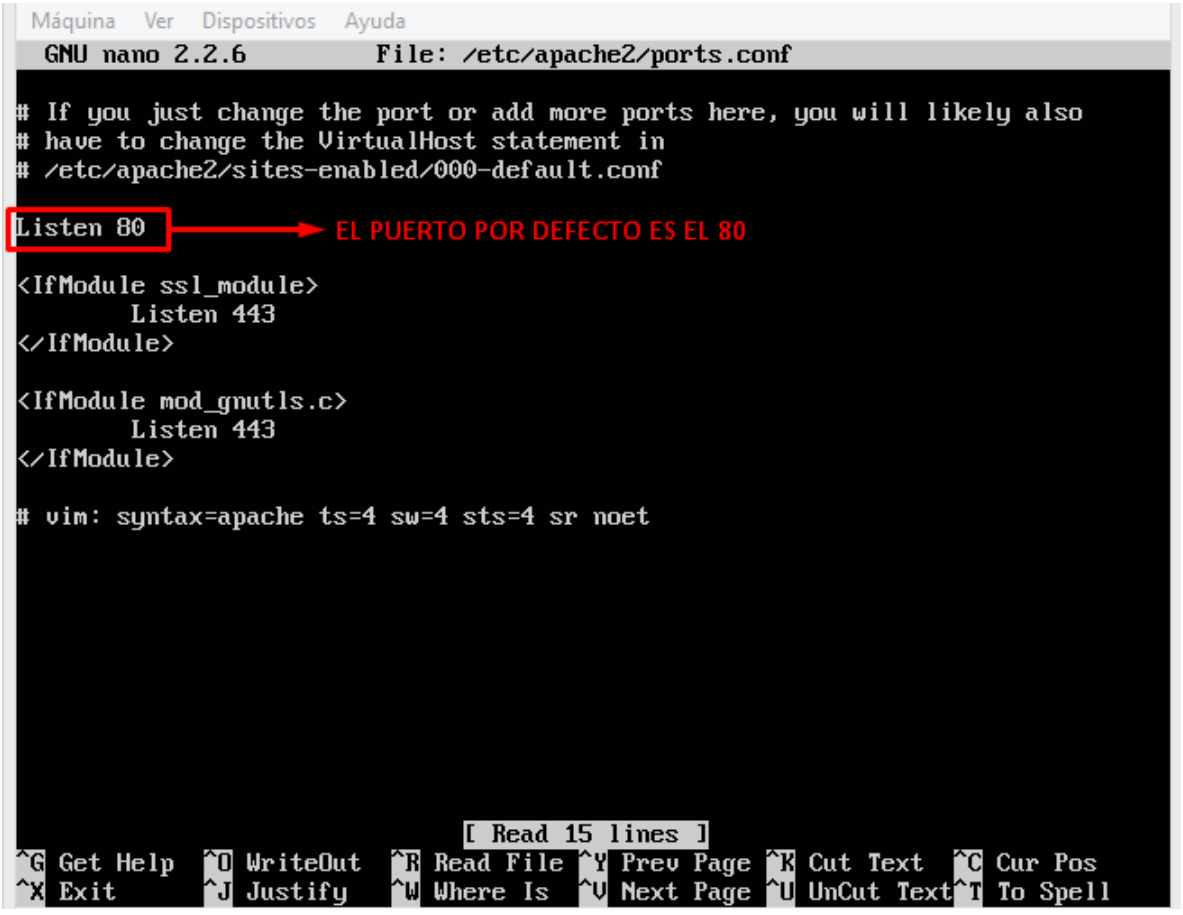


2. MODIFICACION DE PUERTO

Para esto se edita el archivo ports.conf, este archivo se encuentra en la ruta /etc/apache2/



Al ingresar al archivo se observa que el puerto por defecto que trabaja Apache es el 80.



Se modifica el puerto, teniendo en cuenta que hay:

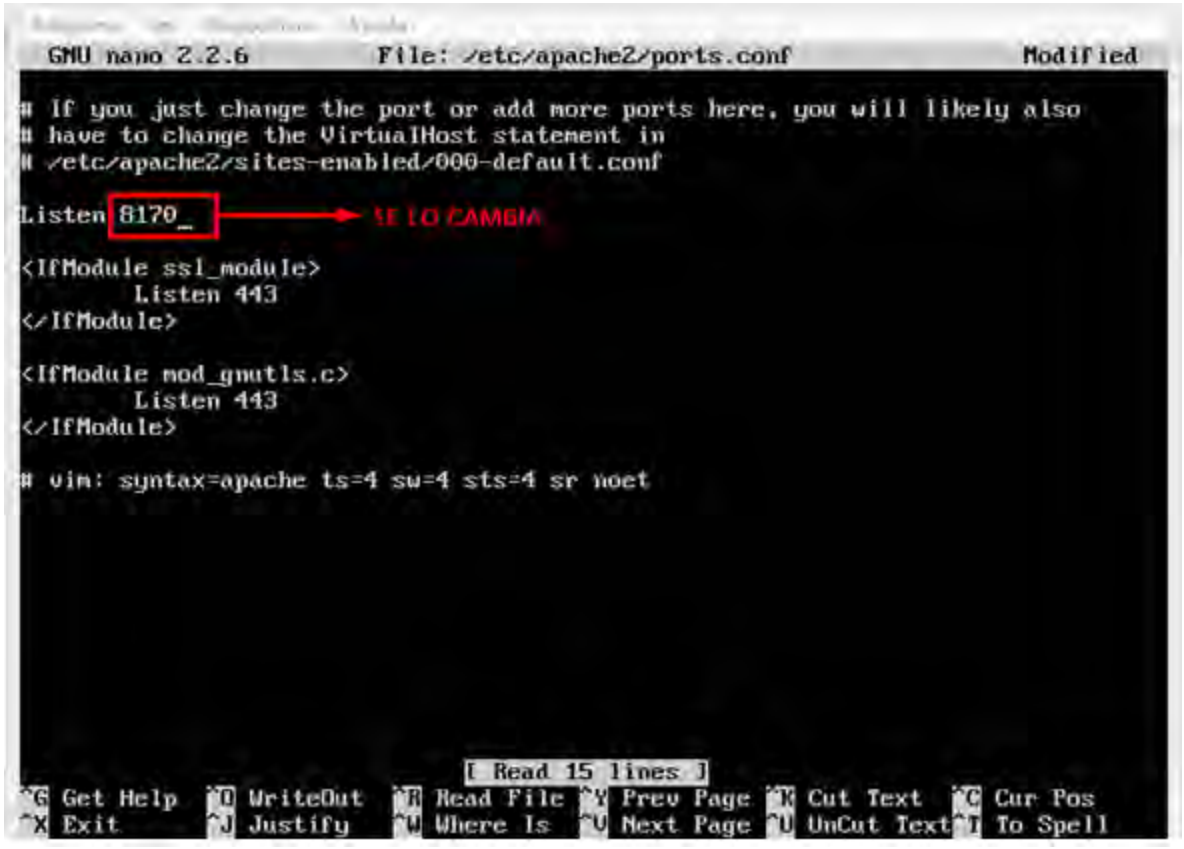
- Puertos bien conocidos: Los puertos inferiores al 1024 son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos" como por ejemplo HTTP (servidor Web), POP3/SMTP (servidor

de e-mail) y Telnet. Si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.

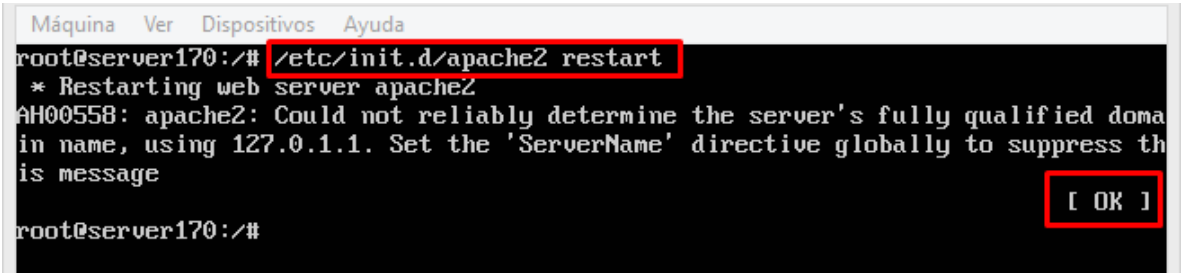
- Puertos registrados: Los comprendidos entre 1024 (0400 en hexadecimal) y 49151 (BFFF en hexadecimal) son denominados "registrados" y pueden ser usados por cualquier aplicación. Existe una lista pública en la web del IANA donde se puede ver qué protocolo usa cada uno de ellos.

- Puertos dinámicos o privados: Los comprendidos entre los números 49152 (C000 en hexadecimal) y 65535 (FFFF en hexadecimal) son denominados dinámicos o privados, normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Son usados en conexiones peer to peer (P2P).

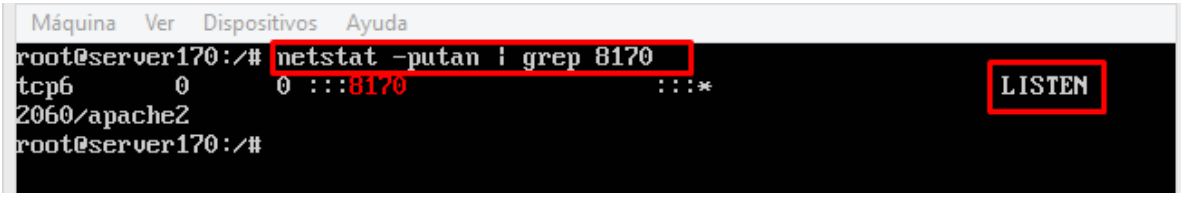
En este caso se cambia el puerto por el 8170.



Se reinicia el servicio de Apache.



Verificar que el puerto haya sido modificado de la siguiente manera:



3. AUTENTICACION EN APACHE

Para esto se edita el archivo julian.conf así:



Dentro del archivo se aumenta lo que se encuentra en el cuadro de la siguiente imagen.

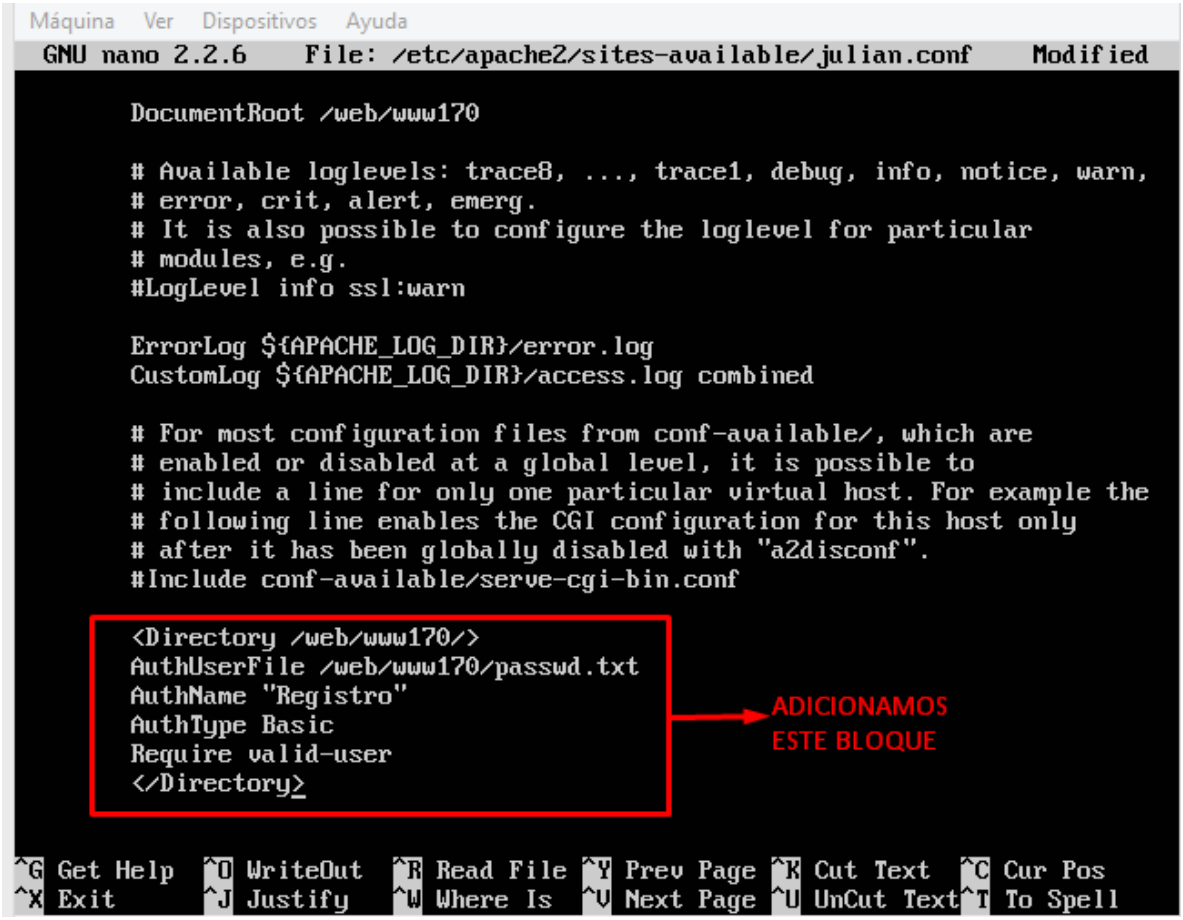
La directiva AuthUserFile establece la ruta al archivo de contraseña que se acaba de crear con htpasswd. Si tiene un gran número de usuarios, sería bastante lento buscar por medio de un archivo en texto plano para autentificar al usuario en cada solicitud. Apache también tiene la capacidad de almacenar la información del usuario en archivos rápidos de bases de datos.

La directiva AuthName establece el Dominio (Realm) a usar en la autentificación. El dominio (realm) cumple dos funciones importantes. Primero, el cliente frecuentemente presenta esta información al usuario como parte del cuatro de diálogo para la contraseña. Segundo, es usado por el cliente para determinar qué contraseña enviar para un área autentificada dada.

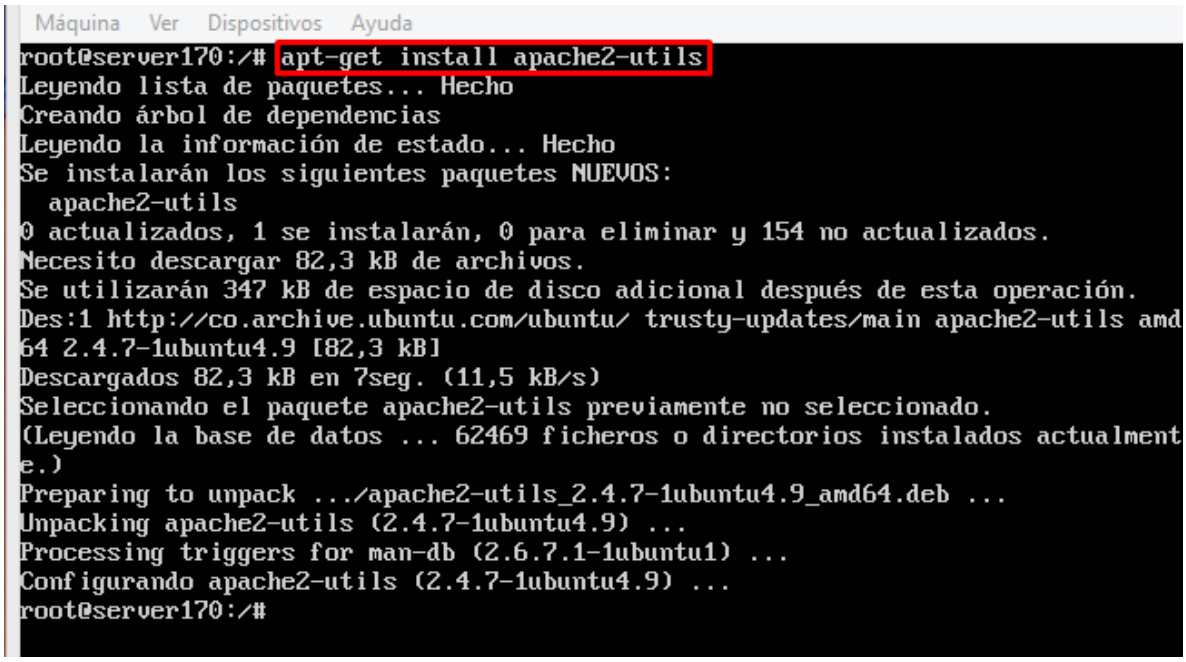
La directiva AuthType selecciona el método que se va a usar para autentificar al usuario. El método más común es Basic, y éste método está implementado en mod_auth. Es importante ser consciente, sin embargo, de que la autentificación Básica envía la contraseña desde el cliente hasta el navegador sin encriptar. Por lo

tanto, este método no debería ser usado para información altamente sensible. Apache soporta otro método de autentificación: AuthType Digest. Este método está implementado en mod_auth_digest y es mucho más seguro. Sólo las versiones más recientes de clientes soportan la autentificación del tipo Digest.

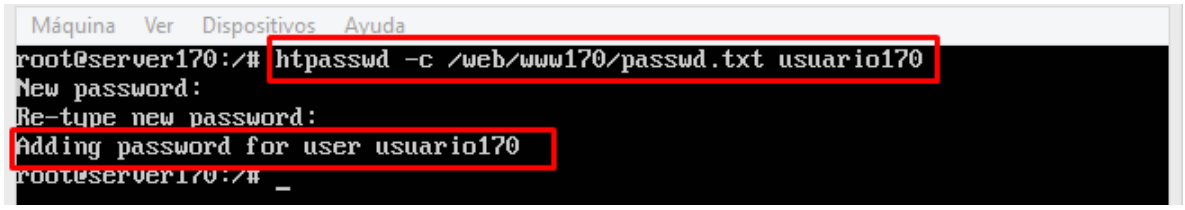
Finalmente, la directiva Require proporciona la parte de la autorización del proceso estableciendo el usuario al que se le permite acceder a esa área del servidor.



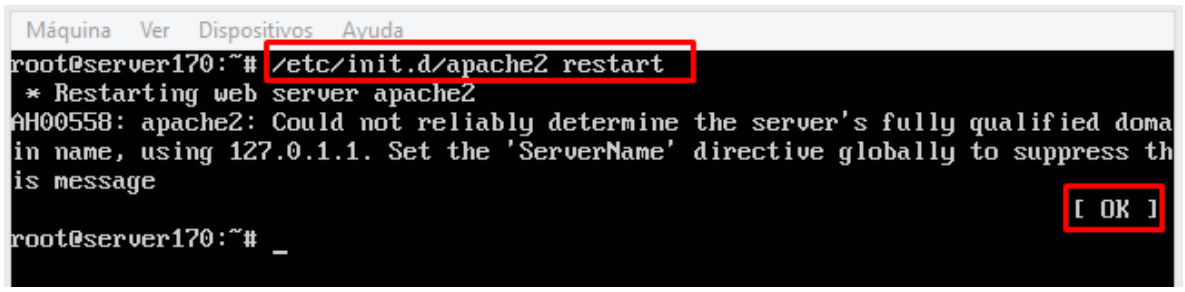
Para crear un archivo de contraseñas, se utiliza la utilidad htpasswd que viene con Apache. Si no la tiene es necesario descargarla así:



Crear el archivo con la utilidad htpasswd, esta pedirá la contraseña y luego la confirmación de la misma, así:

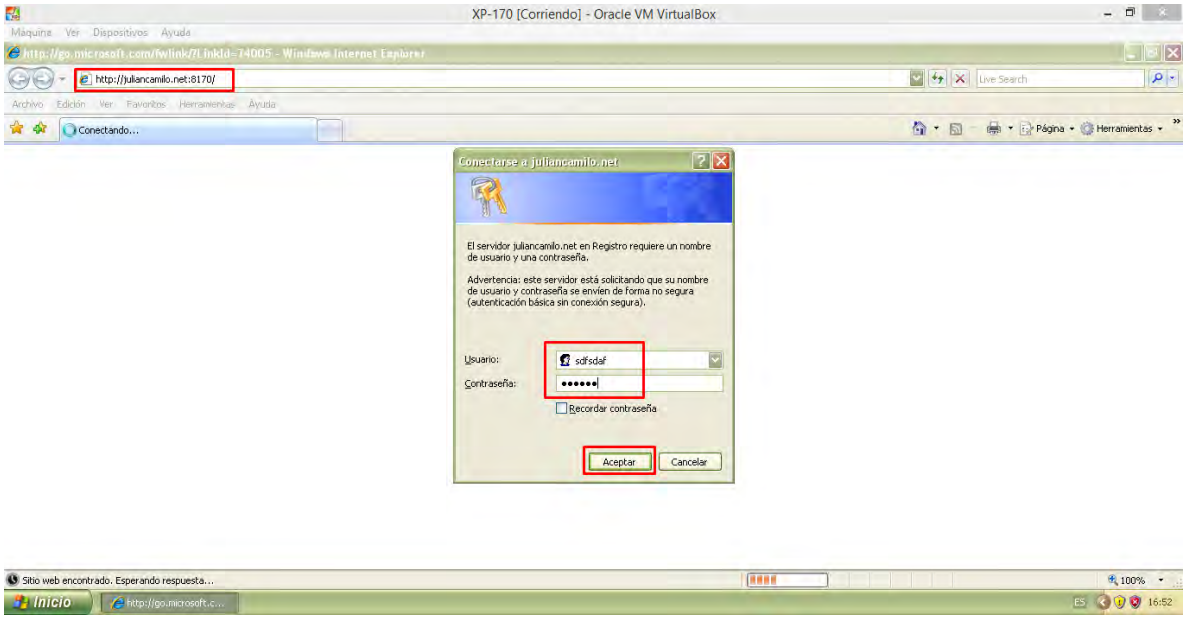


Una vez hecho lo anterior se reinicia el servicio de Apache2.

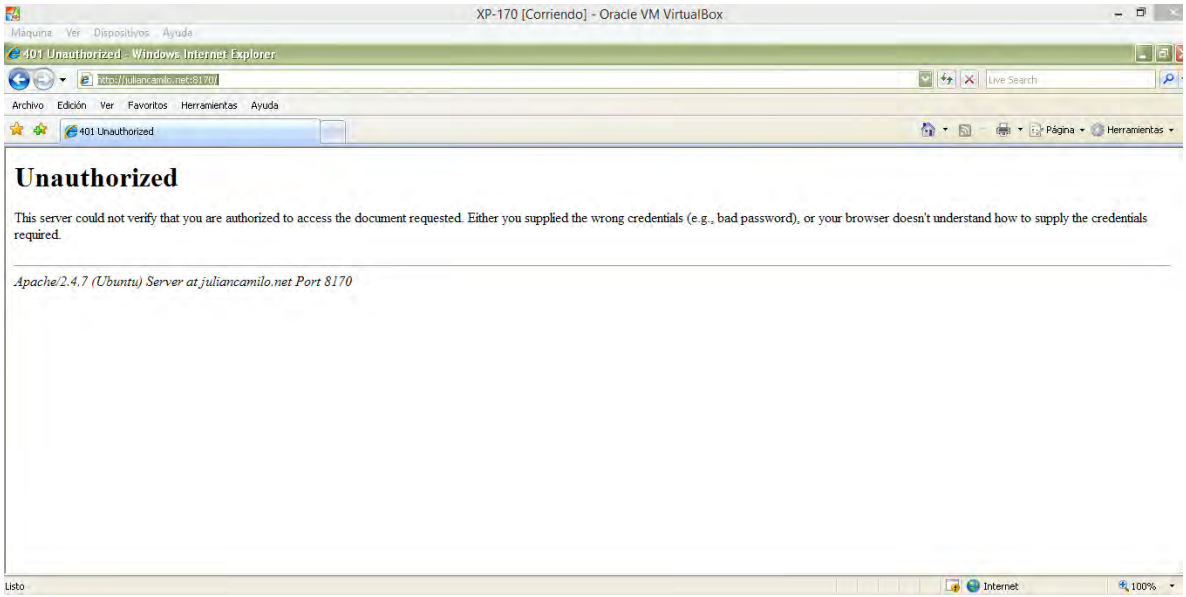


Para verificar lo anteriormente hecho, se ingresa a la maquina XP y se coloca en la URL el nombre de dominio seguido del puerto en este caso juliancamilo.net:8170, se observa para ingresar a los archivos dentro del dominio es necesario registrarse.

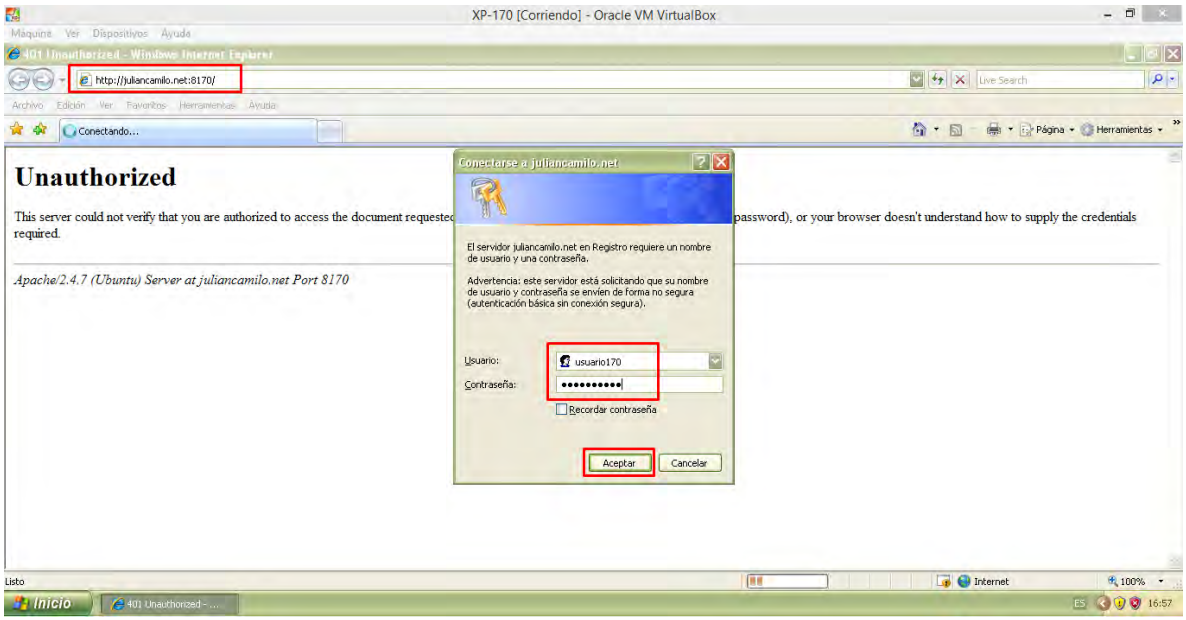
El usuario puede equivocarse hasta 3 veces de lo contrario aparecerá un mensaje de error.



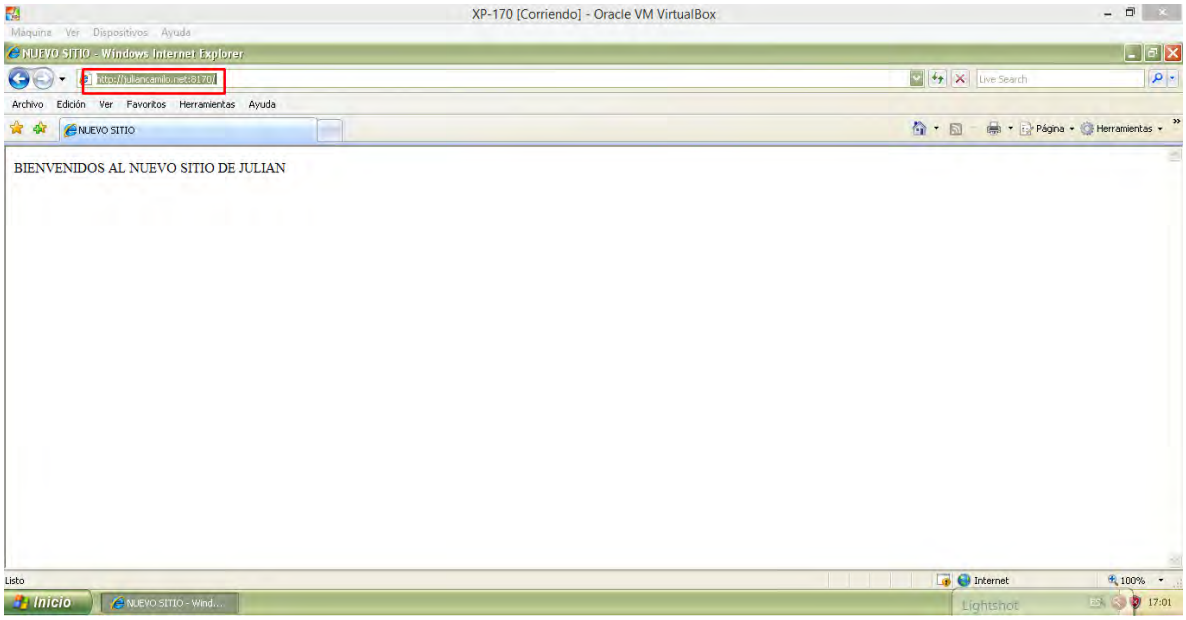
En la siguiente imagen se muestra el mensaje de error.



Digitar el usuario y la contraseña correctos.



Se observa como se accede a la página de bienvenida creada dentro del directorio raíz.



Anexo F. Instalación y configuración de servidor proxy SQUID.

ÍNDICE

Pág.

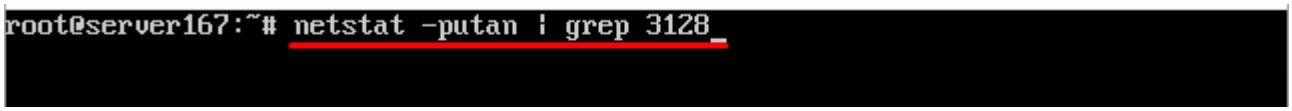
1. INSTALACIÓN SQUID Y CONFIGURACION DE SQUID 330
2. ALGUNAS CONFIGURACIONES BÁSICAS DE SQUID 330
3. RESTRICCIONES DE USO 335

1. INSTALACIÓN SQUID Y CONFIGURACION DE SQUID

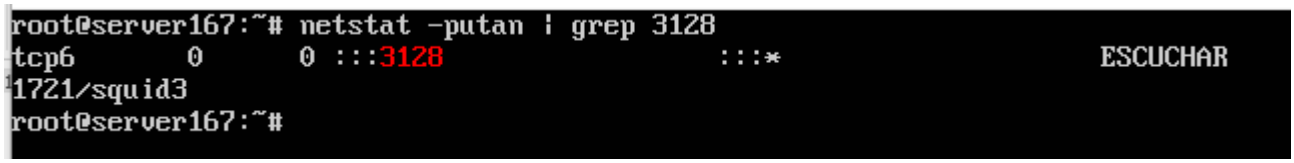
Para descargar e instalar el paquete, en una terminal, se debe escribir el comando: apt-get install squid3, esperar la confirmación de la instalación, aceptar y esperar a que termine la instalación.



Una vez instalado SQUID se confirma que el servicio este corriendo, para esto se utiliza la siguiente línea de comandos: netstat –putan | grep 3128



Y se verifica que efectivamente el servidor SQUID está funcionando y se encuentra activo escuchando por su correspondiente puerto predeterminado 3128

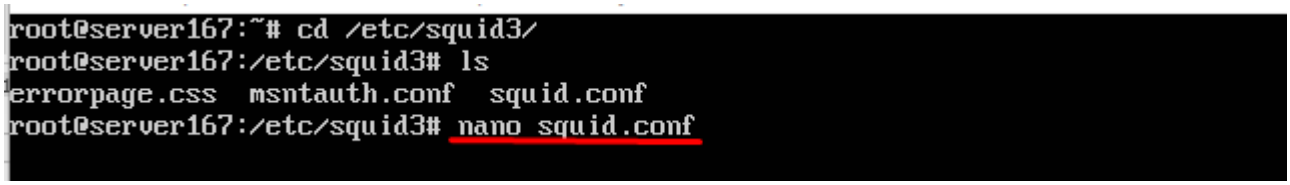


2. ALGUNAS CONFIGURACIONES BÁSICAS DE SQUID

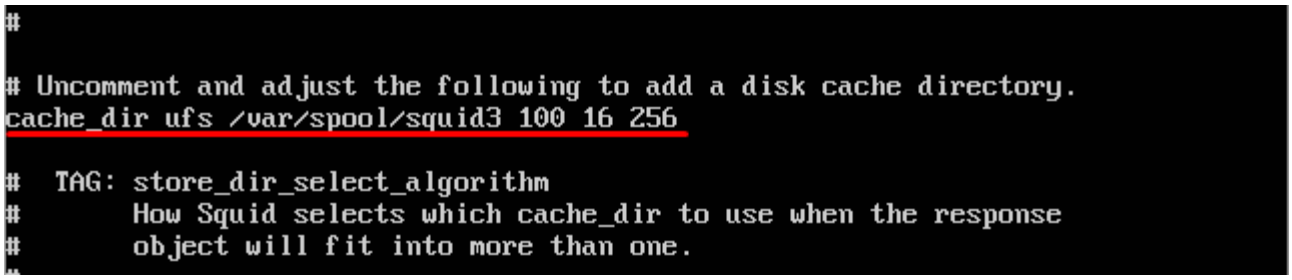
Para lograr que el servidor SQUID permita a los clientes conectarse a internet se debe modificar algunos parámetros en su archivo de configuración que se encuentra en la ubicación /etc/squid3. Lo primero que se hace es cambiarse al directorio donde se encuentra el archivo de configuración de SQUID con el siguiente comando: cd /etc/squid3



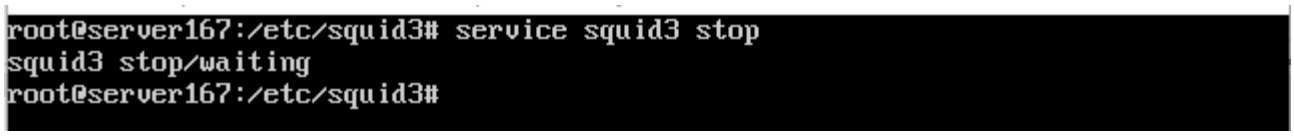
Ahora con un editor, se abre el archivo de configuración squid.conf.



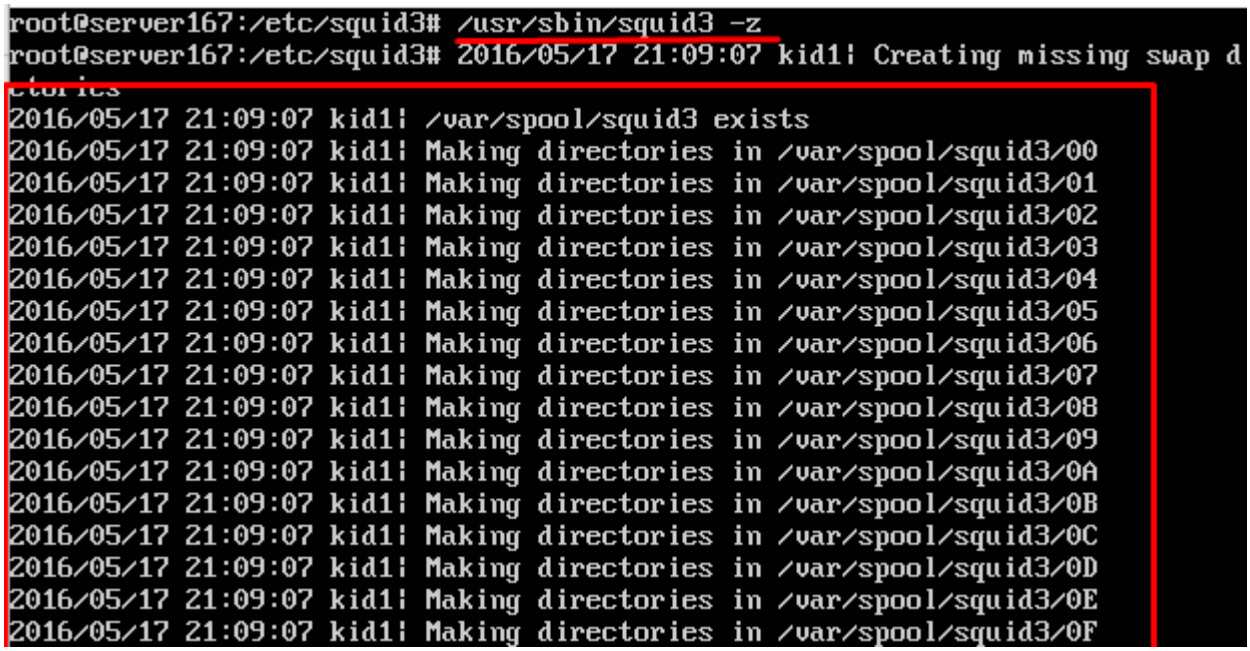
Ahora, presionando control + w, se debe buscar el parámetro cache_dir, se debe descomentar. Quedando como se muestra en la imagen siguiente:



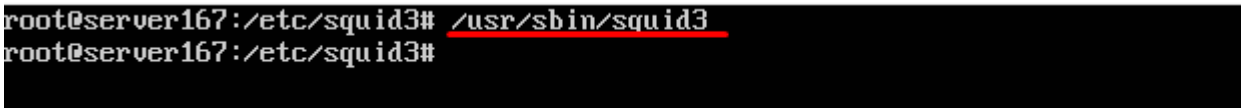
Se guardan los cambios con **control + o,** y se sale del editor con control + x. Ahora se detiene el servicio con el comando service squid3 stop para construir los directorios de la cache.



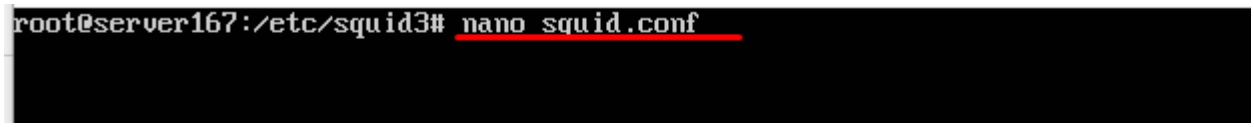
El siguiente comando crea los directorios para la memoria cache del servidor: /usr/sbin/squid3 –z



Se Vuelve a iniciar SQUID con el comando /usr/sbin/squid3

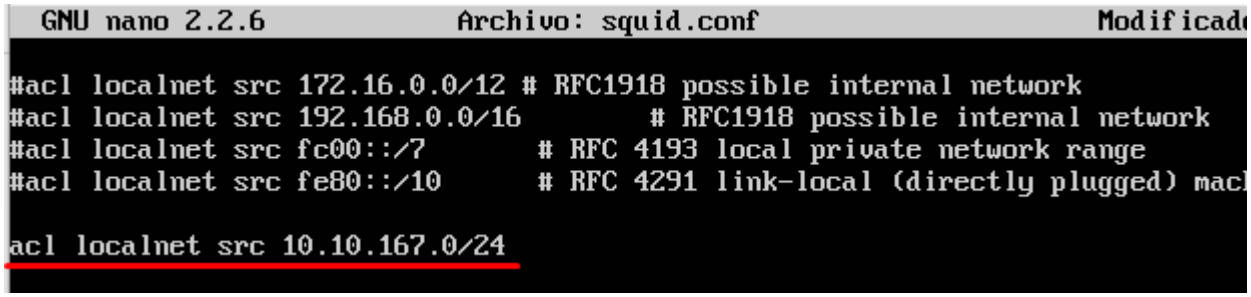


El próximo paso es crear una Lista de Control de Acceso loa cual será la que permita la conectividad a internet de las maquinas clientes. Para esto se vuelve a editar el archivo de configuración de SSQUID: squid.conf



Dentro de este archivo se debe crear las listas de acceso (acl) y las reglas de acceso (http_access) de la siguiente manera:

acl localnet src 10.10.167.0/24 con esto se crea la lista de acceso con el nombre localnet

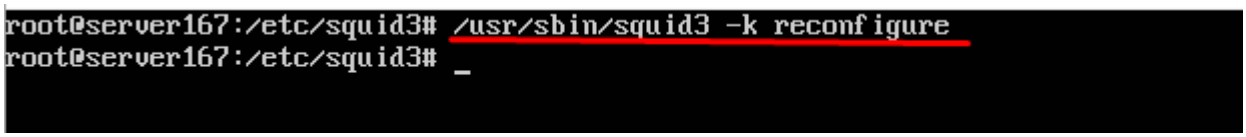


Ahora se da acceso mediante la creación de la regla. Para ello se escribe en el mismo fichero, ahora en la sección donde dice: INSERT YOUR RULE(s) HERE TO ALLOW ACCESS FROM YOUR CLIENTS.

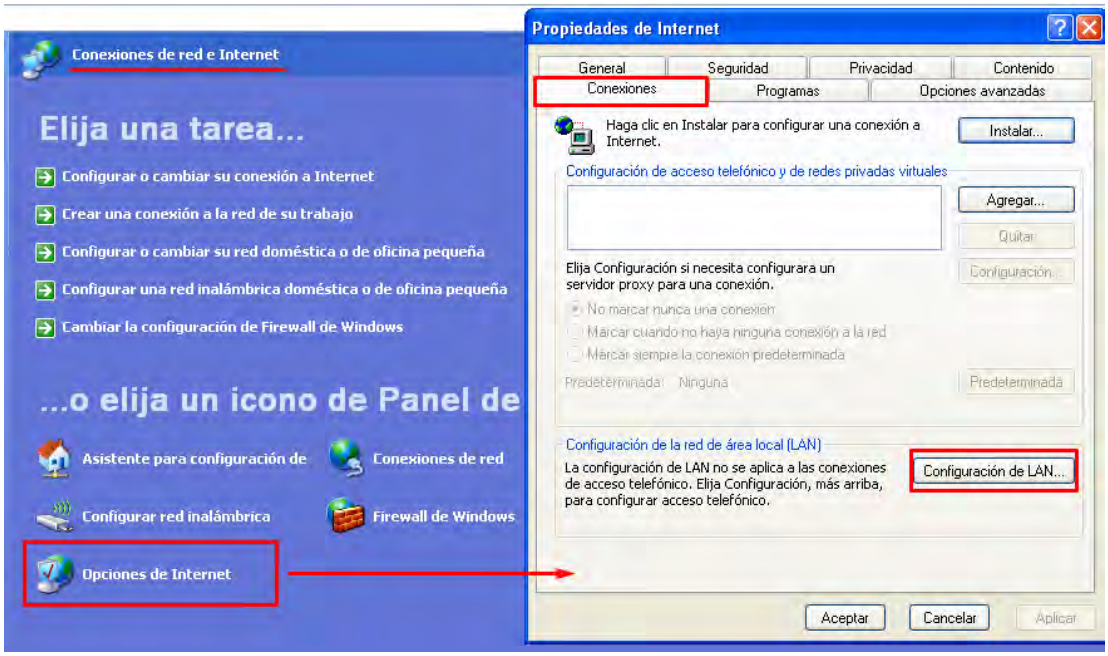
http_access allow localnet con esto se le indica al servidor que permita el acceso a toda la red.



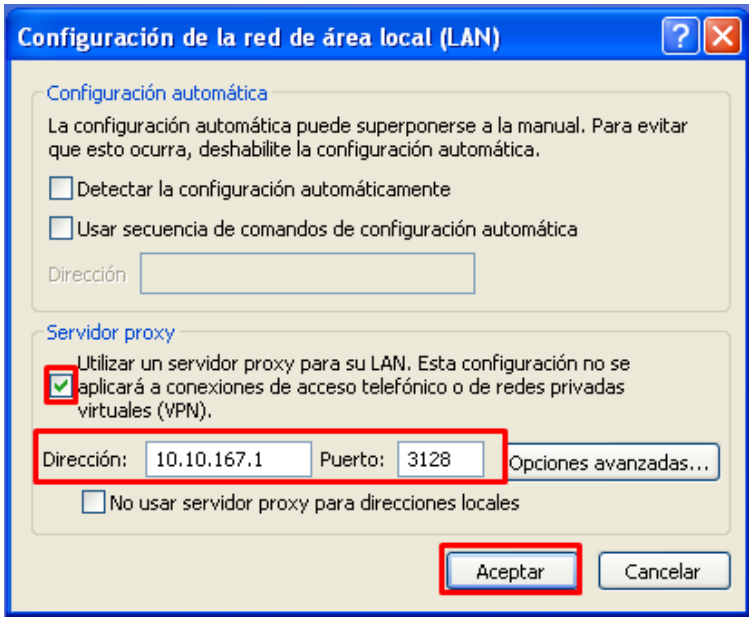
Como SQUID no se reinicia porque no es una buena práctica desconectar a los clientes, entonces se procede a reconfigurar el servicio con el comando:
/usr/sbin/squid3 –k reconfigure



Como la configuración del proxy no es transparente, entonces se debe configurar manualmente para los navegadores del cliente (Windows XP). Para esto se accede a **Conexiones de red e Internet** en el panel de control y se selecciona **Opciones de Internet**, aquí se ubica a la pestaña de conexiones y se hace clic en el botón de la parte inferior **Configuración de LAN**.



Se habilita la opción para **Utilizar un servidor proxy para su LAN….** Y se ingresa los valores de los campos tal como se muestra en la siguiente imagen:



3. RESTRICCIONES DE USO

Ahora se configura algunas restricciones de uso en el servidor Squid, para que el registro de actividad del sistema sea mucho más amplio.

Restricción Por Dominio.

Para restringir un dominio, en el directorio /etc/squid3 se crea el archivo restringido donde se agregarán los dominios a restringir.



Luego se agrega la acl en el archivo de configuración squid.conf

```
acl pagBloq dstdomain "/etc/squid3/restringidos.txt"
```

Se crea la regla que le dé acceso a la acl anterior:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

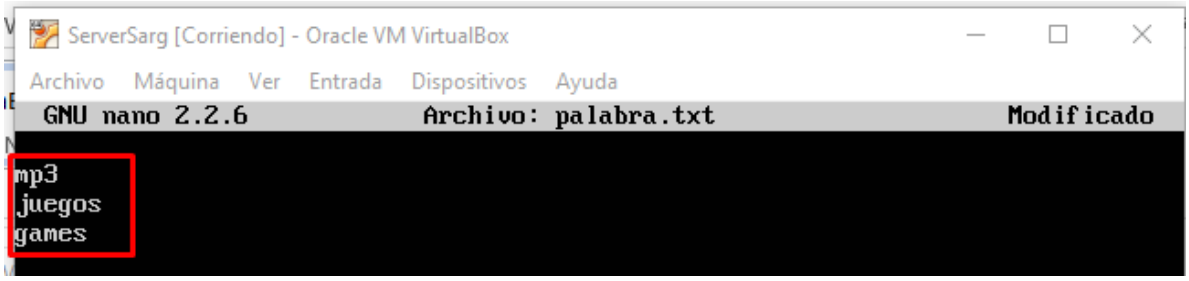
http_access deny pagBloq
```

Guardar los cambios, salir del editor y reconfigurar SQUID.

```
root@server167:/etc/squid3# /usr/sbin/squid3 -k reconfigure
root@server167:/etc/squid3# _
```

Restricción Por Palabra.

Para denegar el acceso por palabra en el directorio squid3 se debe crear un archivo, se lo llamará palabra.txt y en este es donde se agregarán las palabras a restringir. Para nuestro caso se restringe la palabra mp3, juegos y games.



Después de guardar los cambios del archivo palabra.txt y salir del editor, se procede a realizar la restricción en el archivo de configuración de SQUID, utilizando el parámetro url_regex tal como se muestra en la siguiente imagen:

```
acl palBloq url_regex "/etc/squid3/palabra.txt"
```

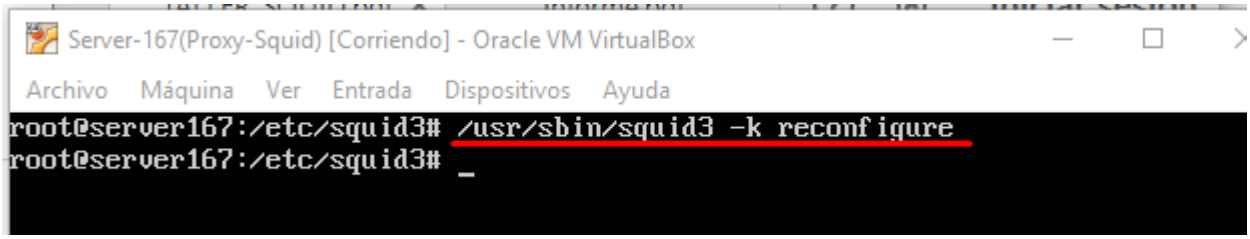
Crear la regla que le dé acceso a la acl anterior:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

http_access deny pagBloq

http_access deny palBloq
```

Guardar los cambios, salir del editor y reconfigurar SQUID.

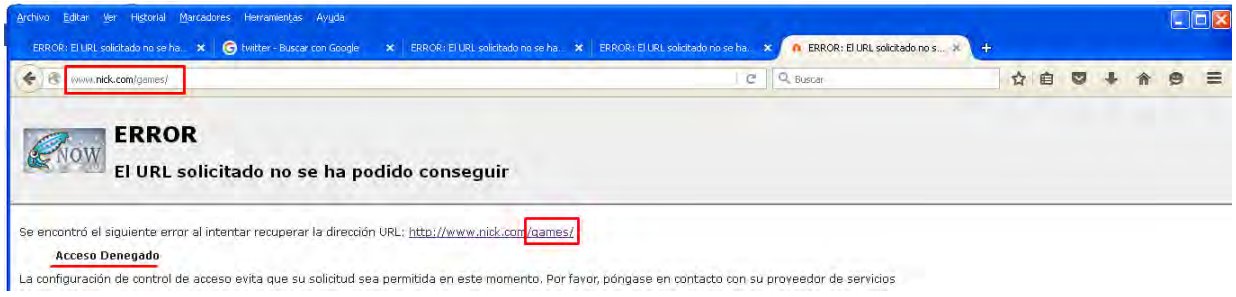


El servidor Proxy está configurado y listo para usarse.

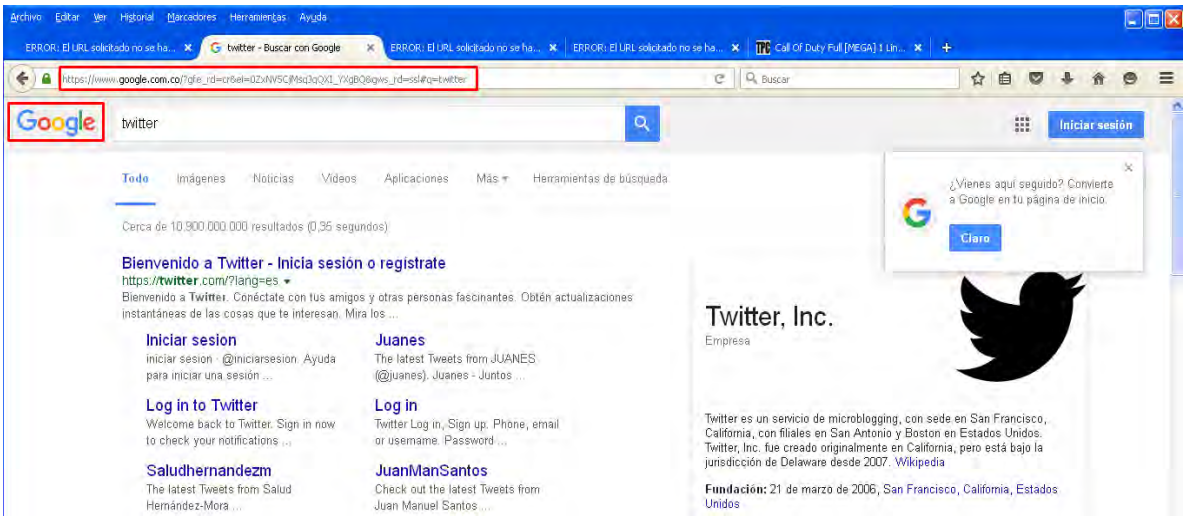
Restricción por dominio:



Restricción por palabra:



Acceso permitido:



Anexo G. Instalación y configuración de servidor ftp.

ÍNDICE

Pág.

1. INSTALACIÓN DE VSFTPD 340
2. CONFIGURACIÓN DE SERVIDOR FTP 341
3. CLIENTE FILEZILLA EN WINDOWS 344

1. INSTALACIÓN DE VSFTPD

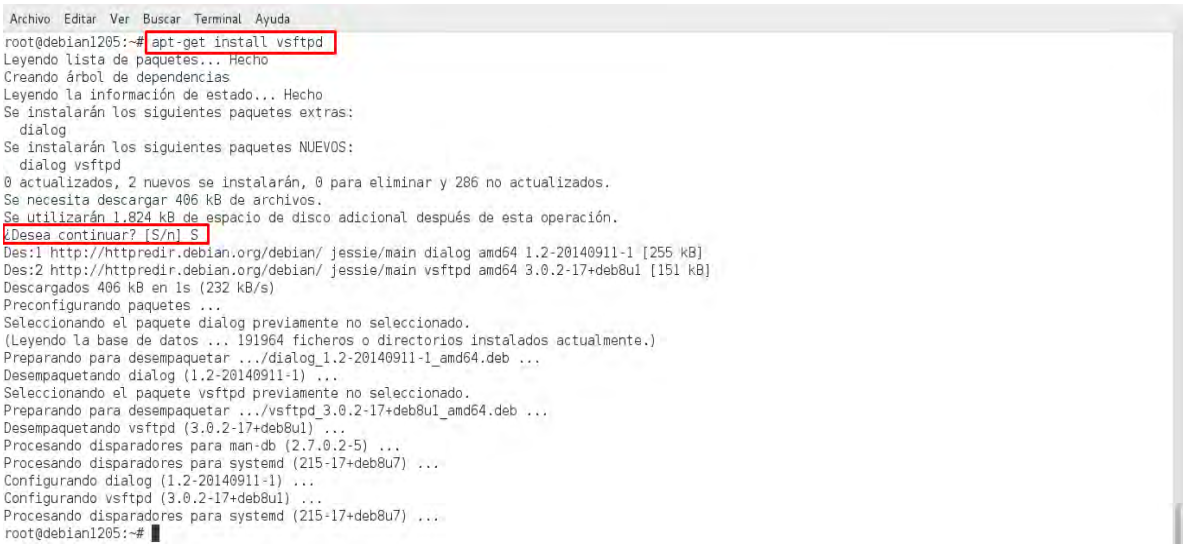
Se actualizan los repositorios para instalar la última versión de VSFTPD.

```
apt-get update
```

Se instala el servidor ftp con VSFTPD con el siguiente comando:

```
apt-get install vsftpd
```

Mostrará lo siguiente:



Mediante el siguiente comando se verifica la instalación del servidor FTP.

```
netstat -putona | grep vsftpd
```

Mostrará lo siguiente:



2. CONFIGURACIÓN DE SERVIDOR FTP

Se ingresa al directorio de /etc para poder renombrar y editar el archivo vsftpd.conf

```
cd /etc
```

Se renombra el archivo de configuración del servidor FTP para guardar la copia original y hacer un nuevo archivo con los parámetros de configuración del servidor.

```
mv vsftpd.conf vsftpd.conf.save
```

Se crea el archivo vsftpd.conf que tiene la configuración del servidor FTP.

```
nano vsftpd.conf
```

El archivo vsftpd.conf contendrá lo siguiente:

```
#Fichero de configuracion de VSFTPD

#configuracion general

ftpd_banner="Bienvenidos al servidor FTP de SISTEMAS"

#Configuracion de los usuarios locales

local_enable=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list

#Configuracion de los usuarios anonimos

anonymous_enable=NO

#Configuracion de transferencia

connect_from_port_20=YES
data_connection_timeout=120

#Modo standalone

listen=YES

#Nombre del servicio PAM
```

```
pam_service_name=vsftpd

#Puerto FTP

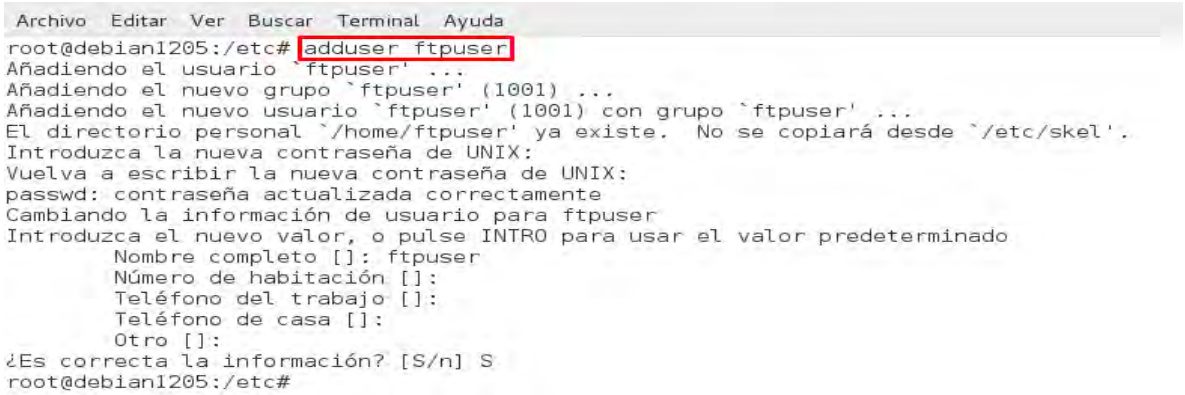
listen_port=22
```

NOTA: en este caso se cambió el puerto por defecto de FTP por el puerto 22, debido a que este puerto estaba siendo ocupado por otra aplicación.

Se crea un usuario para el ingreso al servidor FTP.

```
adduser ftpuser
```

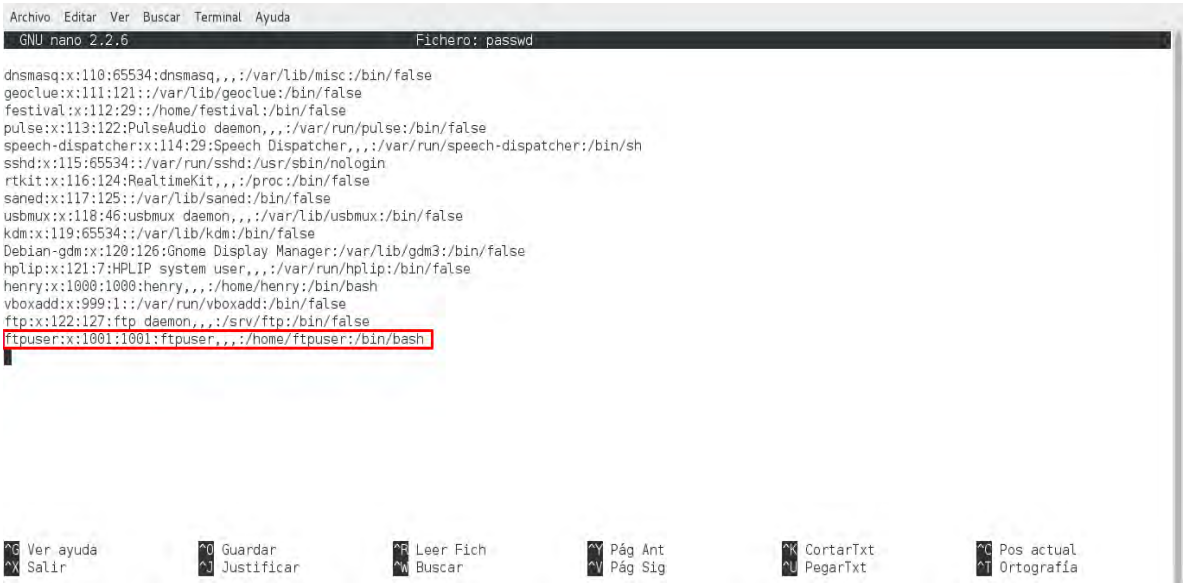
Mostrará lo siguiente:



Con el siguiente comando se verifica que el usuario haya sido creado.

```
nano passwd
```

Mostrará lo siguiente:



Se crea el archivo vsftpd.chroot_list , que contiene los usuarios que podrán ingresar al servidor FTP.

```
nano vsftpd.chroot_list
```

En el archivo se coloca lo siguiente:

```
ftpuser
```

Así:



Se inicia el servicio VSFTPD con el siguiente comando:

```
/etc/init.d/vsftpd start
```

Mostrará lo siguiente:

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@debian1205:/etc# /etc/init.d/vsftpd start
[ ok ] Starting vsftpd (via systemctl): vsftpd.service.
root@debian1205:/etc#
```

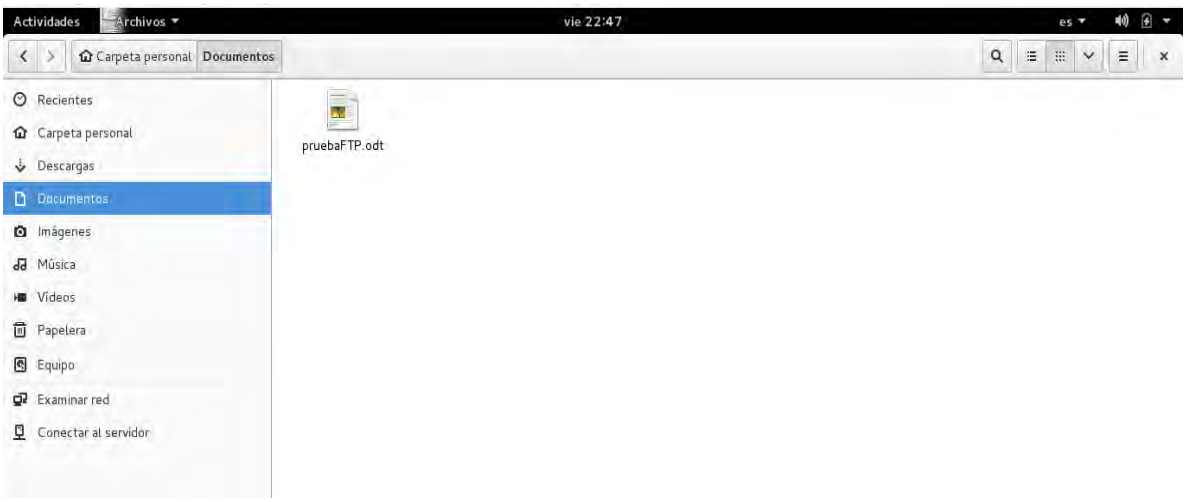
Se reinicia el servicio VSFTPD con el siguiente comando:

```
/etc/init.d/vsftpd restart
```

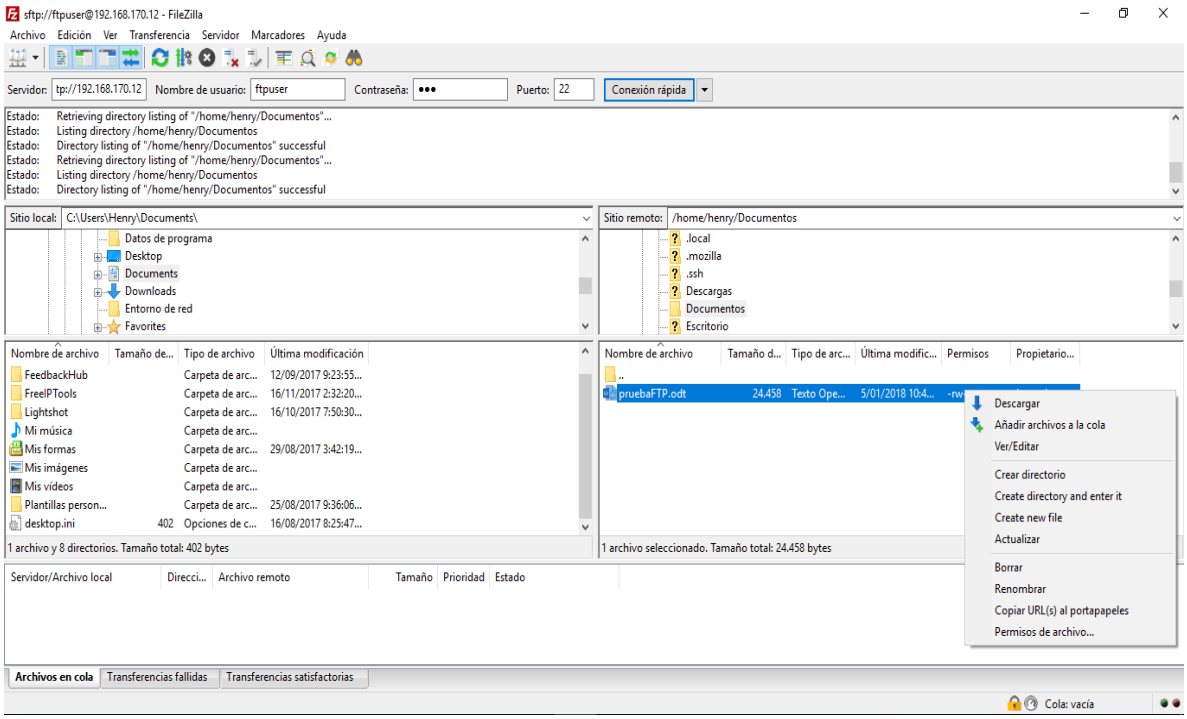
3. CLIENTE FILEZILLA EN WINDOWS

Se hace una demostración con la aplicación filezilla en windows.

Se tiene un documento en el servidor FTP en la carpeta documentos y se quiere descargar este documento en un equipo Windows.



En Filezilla se ingresa la IP del servidor FTP, el nombre del usuario, la contraseña del usuario y el puerto y se da Enter. Si los datos ingresados son correctos se tiene conexión al servidor FTP y se puede tener acceso a las funcionalidades que presta este Servidor.


sftp://ftpuser@192.168.170.12 - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Servidor: tp://192.168.170.12 Nombre de usuario: ftpuser Contraseña: ••• Puerto: 22 Conexión rápida
Estado: Retrieving directory listing of "/home/henry/Documentos"...
Estado: Listing directory /home/henry/Documentos
Estado: Directory listing of "/home/henry/Documentos" successful
Estado: Retrieving directory listing of "/home/henry/Documentos"...
Estado: Listing directory /home/henry/Documentos
Estado: Directory listing of "/home/henry/Documentos" successful
Sitio local: C:\Users\Henry\Documents\
Datos de programa
Desktop
Documents
Downloads
Entorno de red
Favorites
Sitio remoto: /home/henry/Documentos
.local
.mozilla
.ssh
Descargas
Documentos
Escritorio
Nombre de archivo Tamaño de... Tipo de archivo Última modificación
FeedbackHub Carpeta de arc... 12/09/2017 9:23:55...
FreeIPTools Carpeta de arc... 16/11/2017 2:32:20...
Lightshot Carpeta de arc... 16/10/2017 7:50:30...
Mi música Carpeta de arc...
Mis formas Carpeta de arc... 29/08/2017 3:42:19...
Mis imágenes Carpeta de arc...
Mis vídeos Carpeta de arc...
Plantillas person... Carpeta de arc... 25/08/2017 9:36:06...
desktop.ini 402 Opciones de c... 16/08/2017 8:25:47...
1 archivo y 8 directorios. Tamaño total: 402 bytes
Nombre de archivo Tamaño d... Tipo de arc... Última modific... Permisos Propietario...
..
pruebaFTP.odt 24.458 Texto Ope... 5/01/2018 10:4... -rw
1 archivo seleccionado. Tamaño total: 24.458 bytes
Descargar
Añadir archivos a la cola
Ver/Editar
Crear directorio
Create directory and enter it
Create new file
Actualizar
Borrar
Renombrar
Copiar URL(s) al portapapeles
Permisos de archivo...
Servidor/Archivo local Direcci... Archivo remoto Tamaño Prioridad Estado
Archivos en cola Transferencias fallidas Transferencias satisfactorias
Cola: vacía

Anexo H. Instalación y configuración de servidor ssh.

ÍNDICE

Pág.

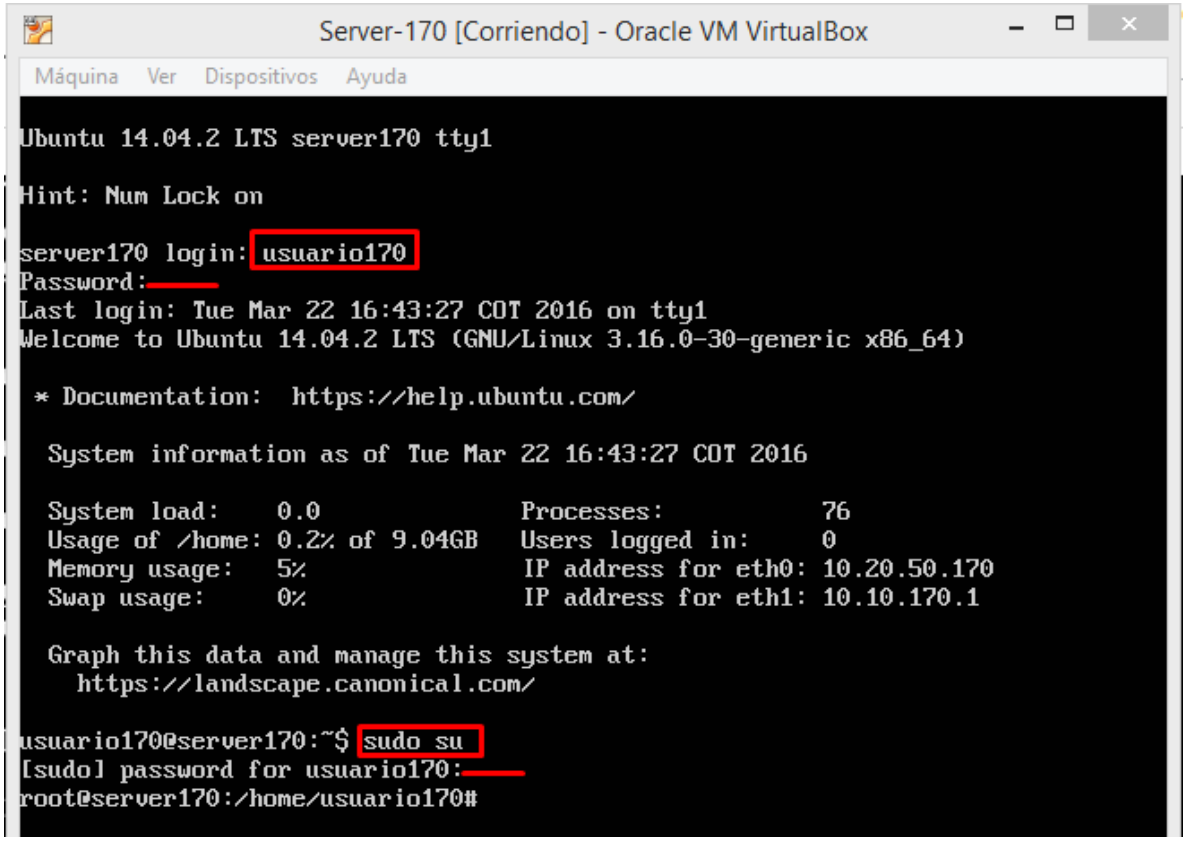
1. CREACION DE USUARIO Y ACCESO CON CLIENTE PUTTY 347

2. CONFIGURACION DE ADMISION Y DENEGACION DE ACCESO USUARIO ROOT 352

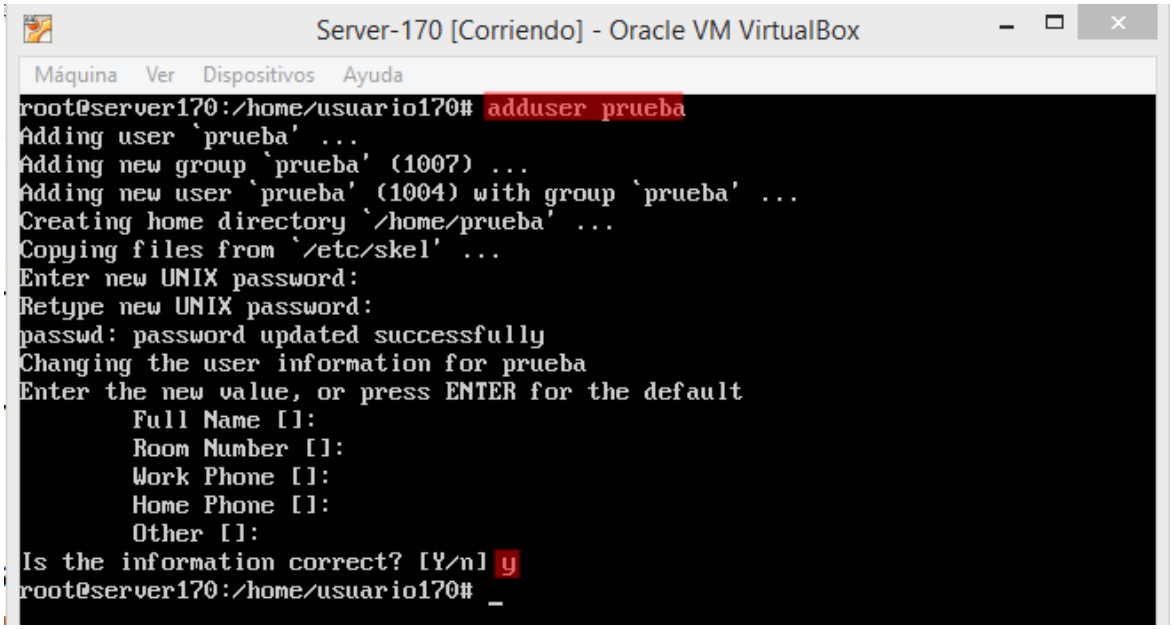
3. CONFIGURACION DE AUTENTICACION DE USUARIOS 361

1. CREACION DE USUARIO Y ACCESO CON CLIENTE PUTTY

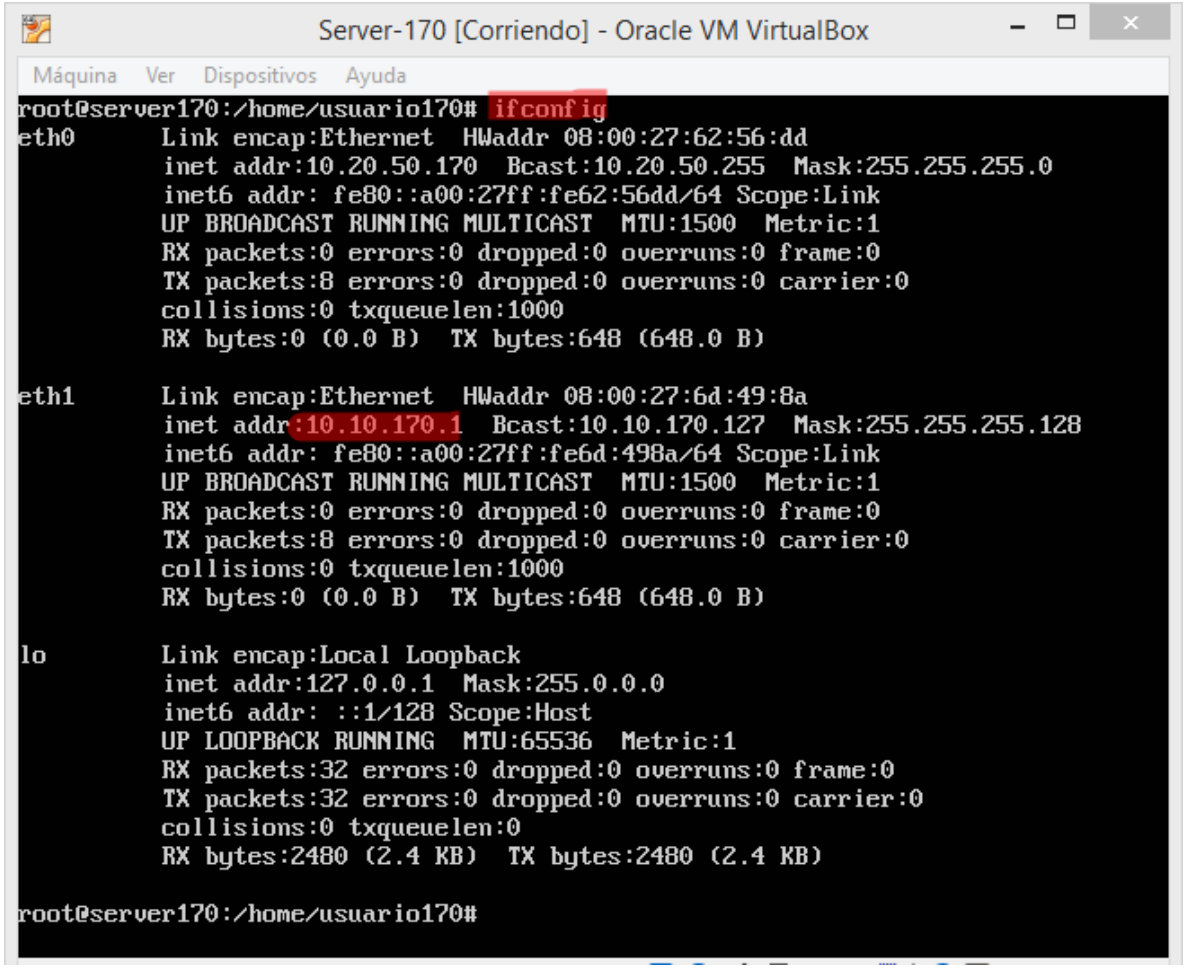
Se inicia con logearse con el usuario, en este caso como **usuario170** en el servidor Linux, una vez se logea se accede como súper usuario mediante el comando **sudo su.**



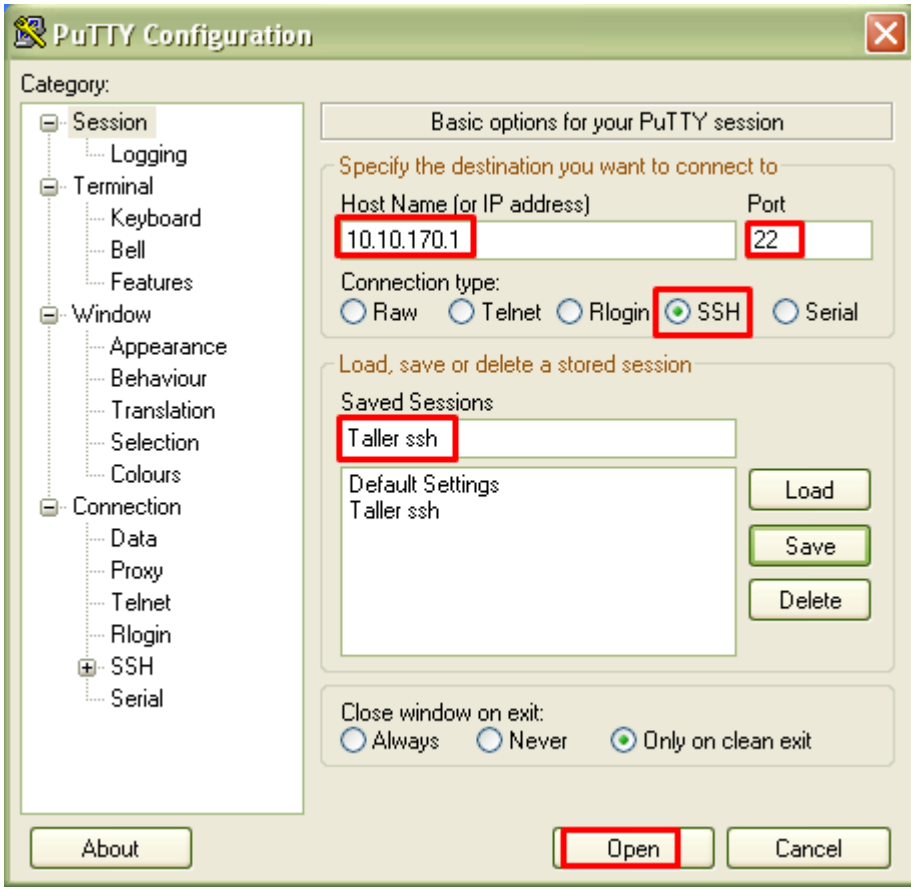
Posteriormente, se crea el usuario prueba con el comando **adduser** tal y como se muestra en la siguiente imagen, se le asigna la clave 123.



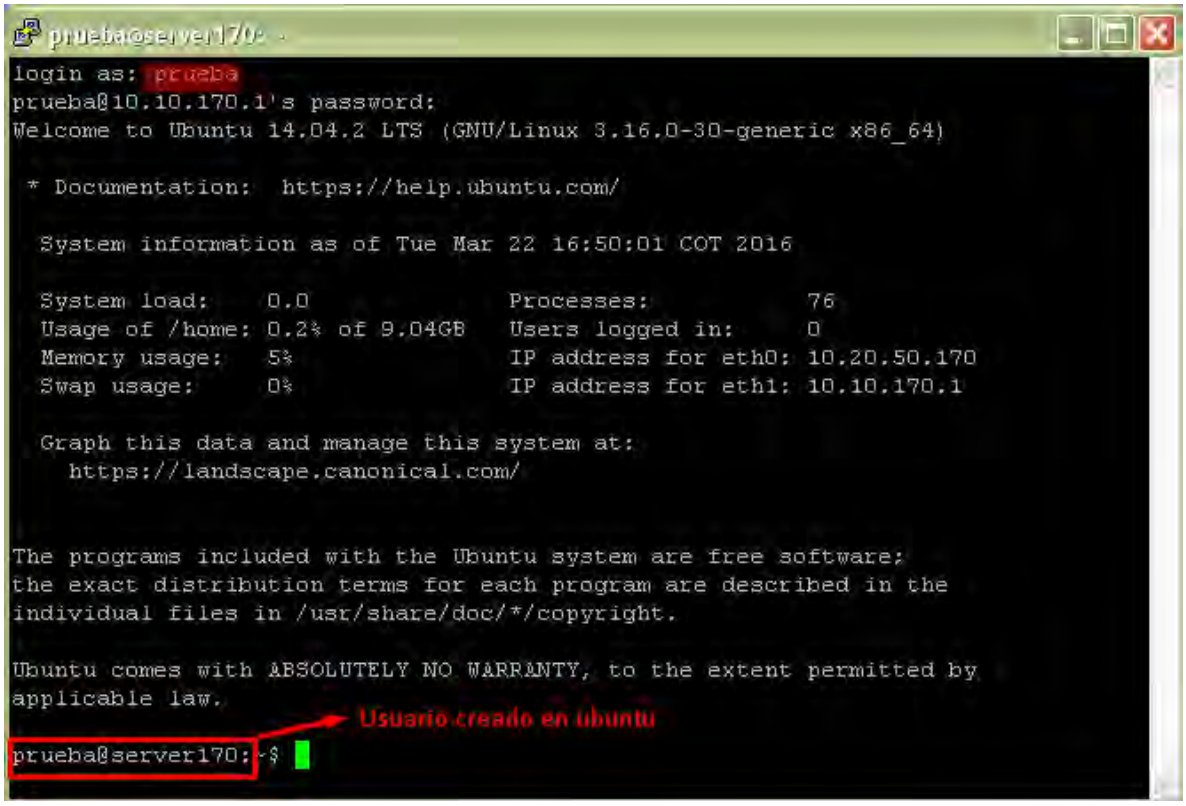
Una vez creado, mediante el comando **ifconfig** se observa la dirección IP de la máquina, en este caso se utiliza la dirección IP de la tarjeta **eth1.**



Luego, se ingresa remotamente con **PuTTY** ingresando la direccion IP del equipo al que se quiere acceder, el puerto que viene por defecto es el 22, se puede guardar la sesión de los equipos que se quiera acceder en **Save Sessions,** se asigna un nombre a la sesión y se guarda, se da doble clic sobre la sesión guardada y continuar.

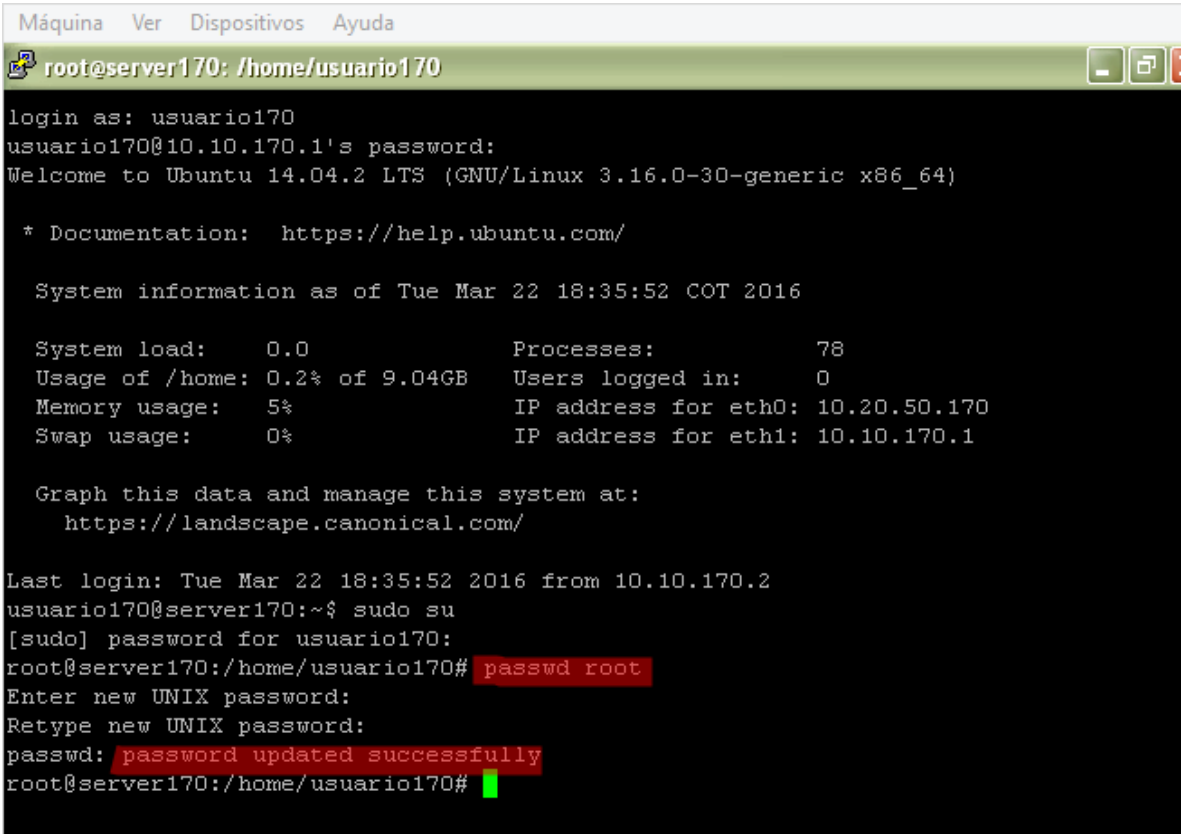


Posteriormente, se abrirá una ventana desde la cual se administra el servidor, aquí se ingresa el usuario y posteriormente la contraseña del usuario, de esta manera se accede al servidor.

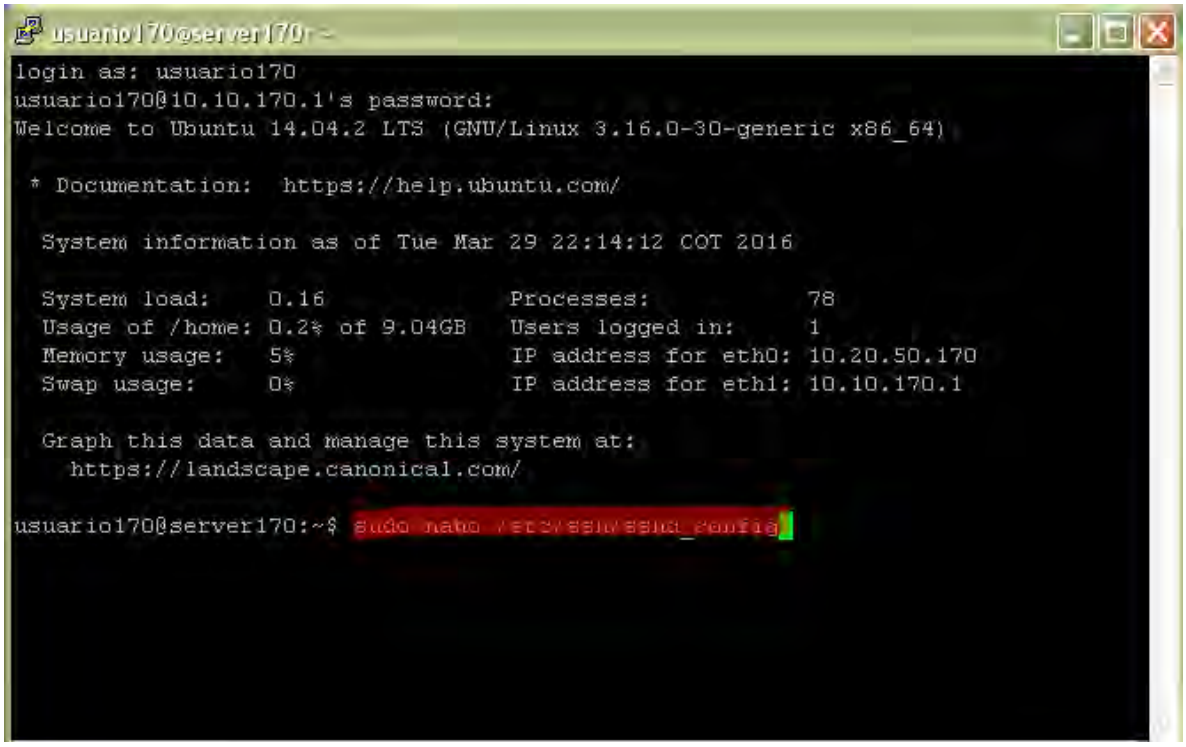


2. CONFIGURACION DE ADMISION Y DENEGACION DE ACCESO USUARIO ROOT

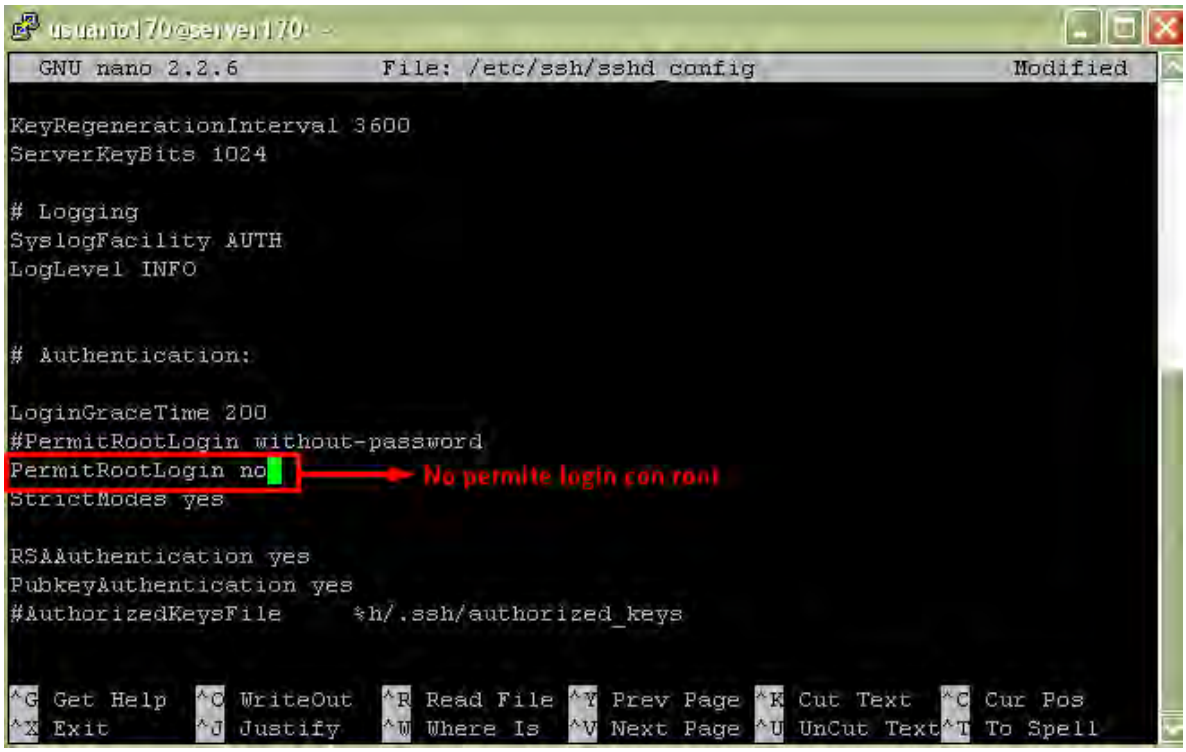
Por defecto, el usuario **root** no se encuentra con login, para el desarrollo de este punto es necesario colocárselo, para esto se utiliza el comando **passwd root** el cual permite asignarle una contraseña al usuario **root.**



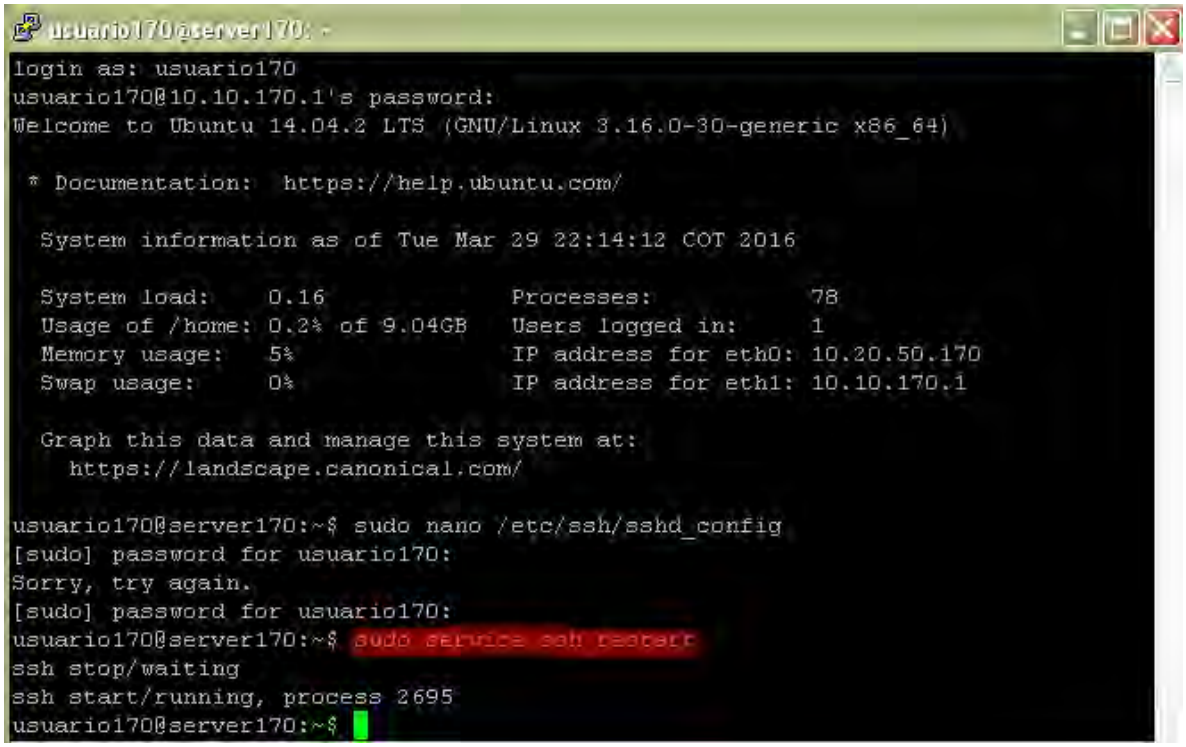
Posteriormente, se edita el archivo **sshd_config** con el editor **nano** el cual se encuentra en la rota **/etc/ssh/**



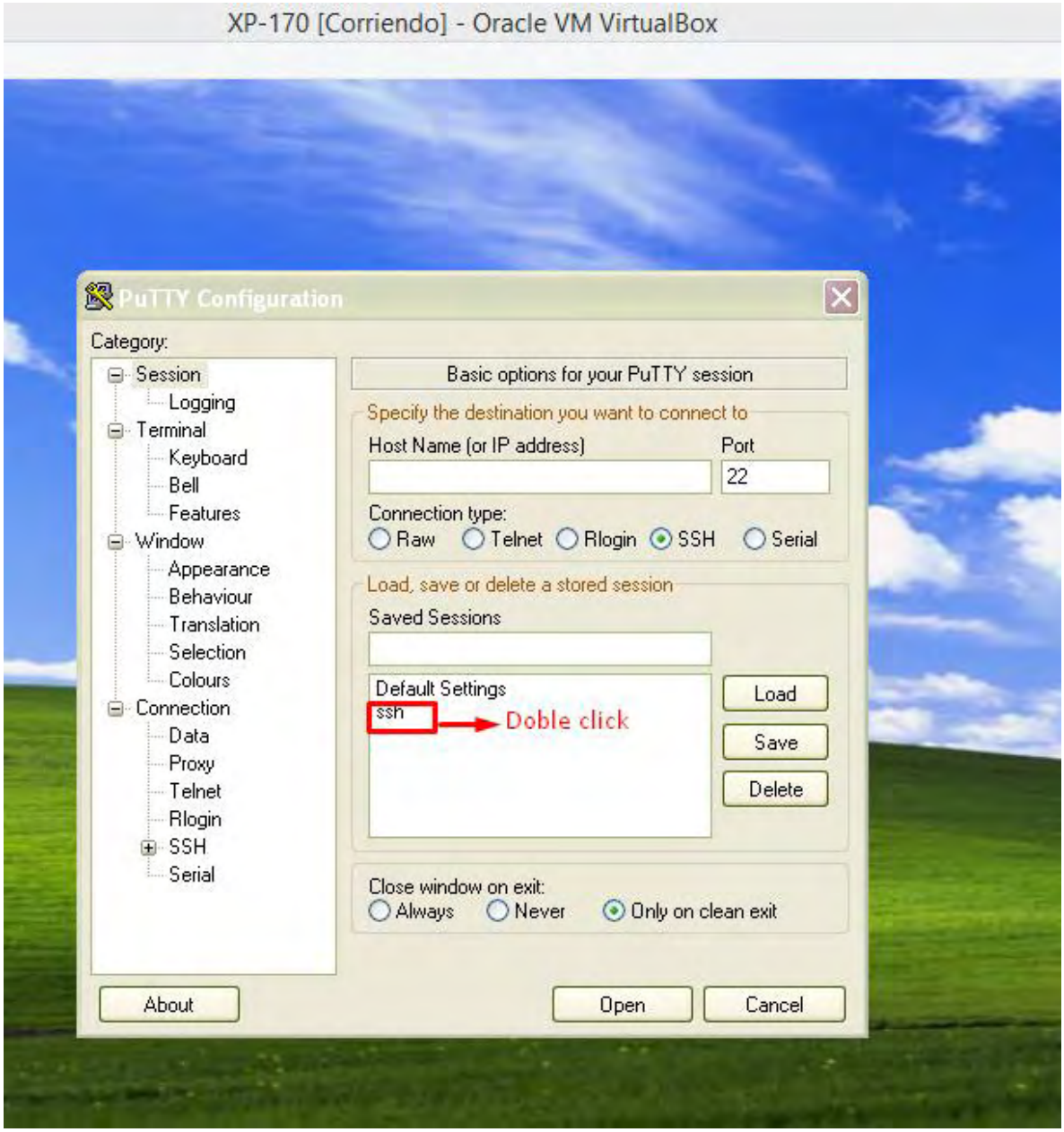
Ahora, para no permitir logearse desde ninguna maquina como usuario root, hay que encontrar la línea **PermitRootLogin** y se le aumenta la palabra **no** quedando **PermitRootLogin no,** se guarda los cambios y continuar.



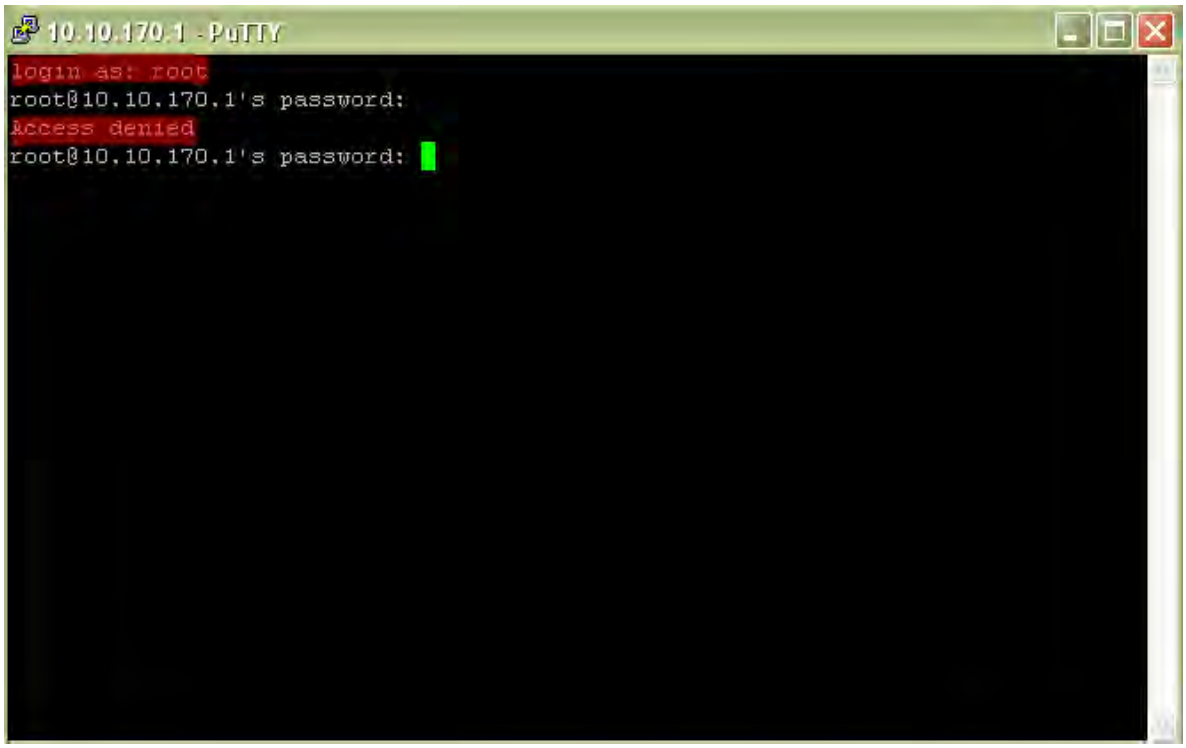
Es necesario resetear el servicio de SSH para aplicar los cambios, para esto se utiliza el comando **sudo service ssh restart.**



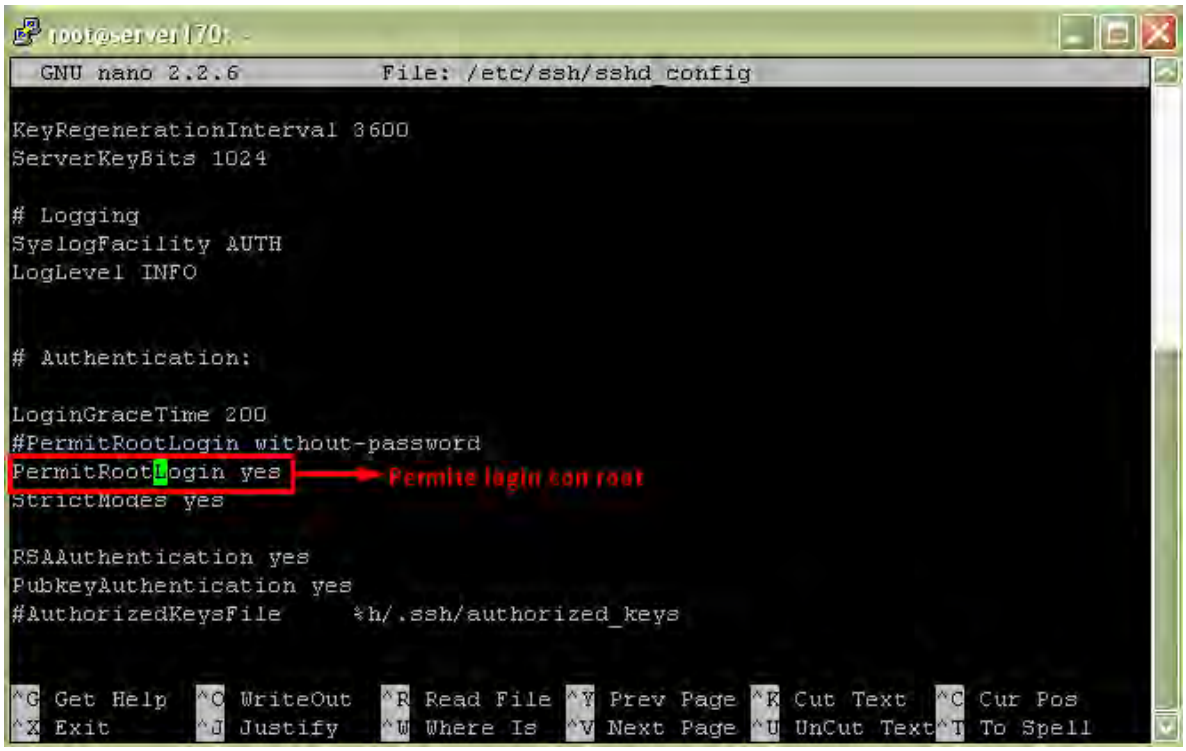
Luego, se ingresa nuevamente a **PuuTY.**



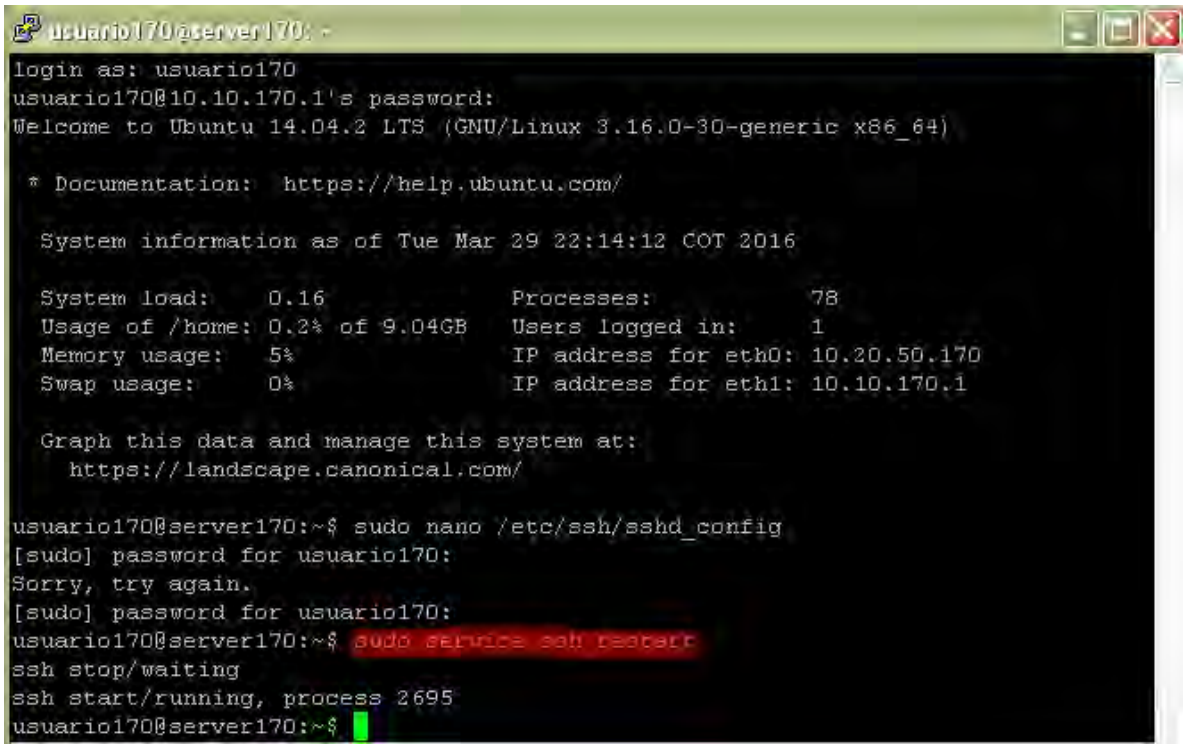
Y al logearse como root no se tendra acceso, tal y como se muestra en la siguiente imagen.



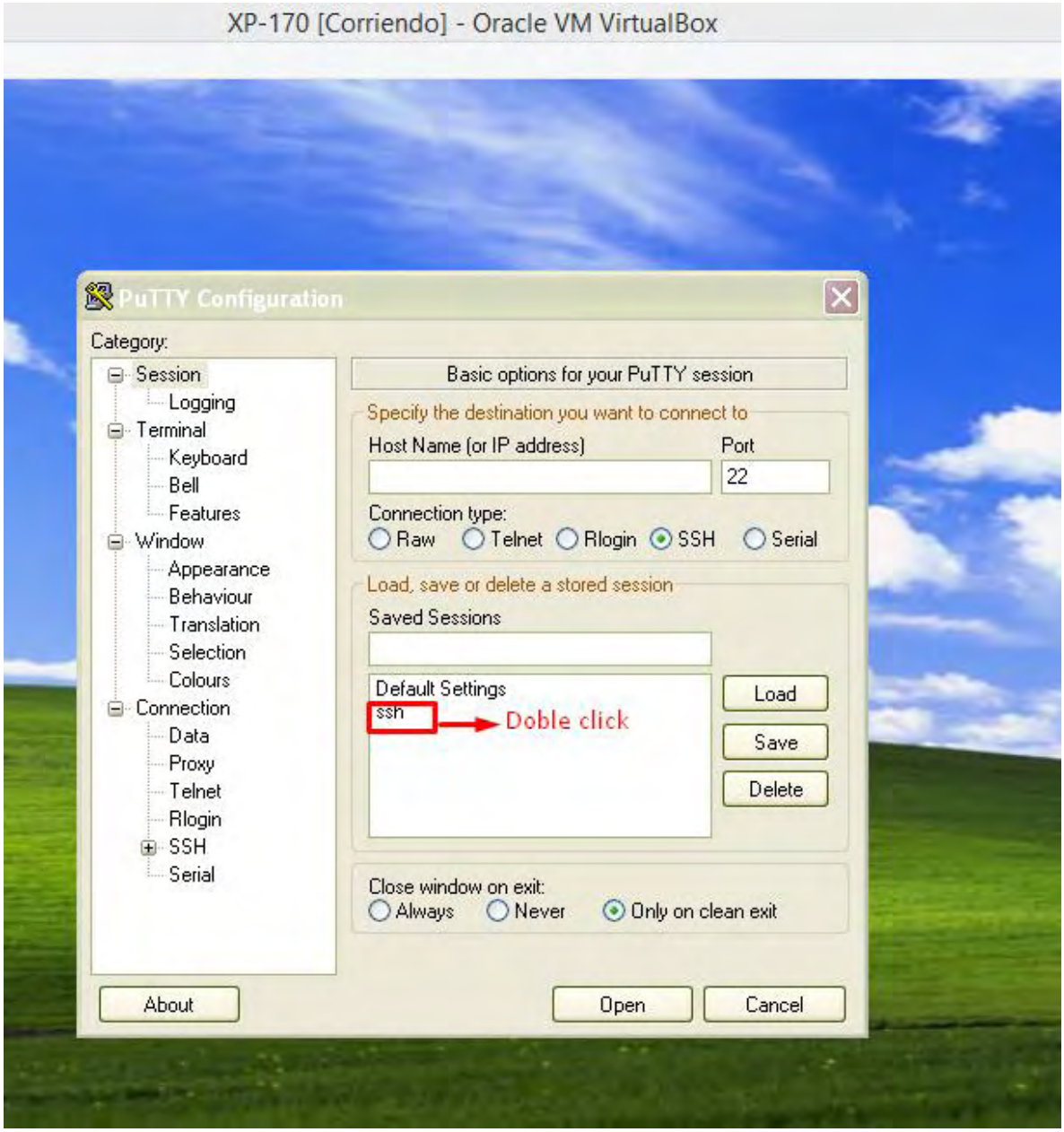
Por otro lado, si se quiere que remotamente se puedan conectar como root, aunque no es recomendable por razones de seguridad, se debe dirigir nuevamente al archivo **sshd_config** y la línea **PermitRootLogin yes.**



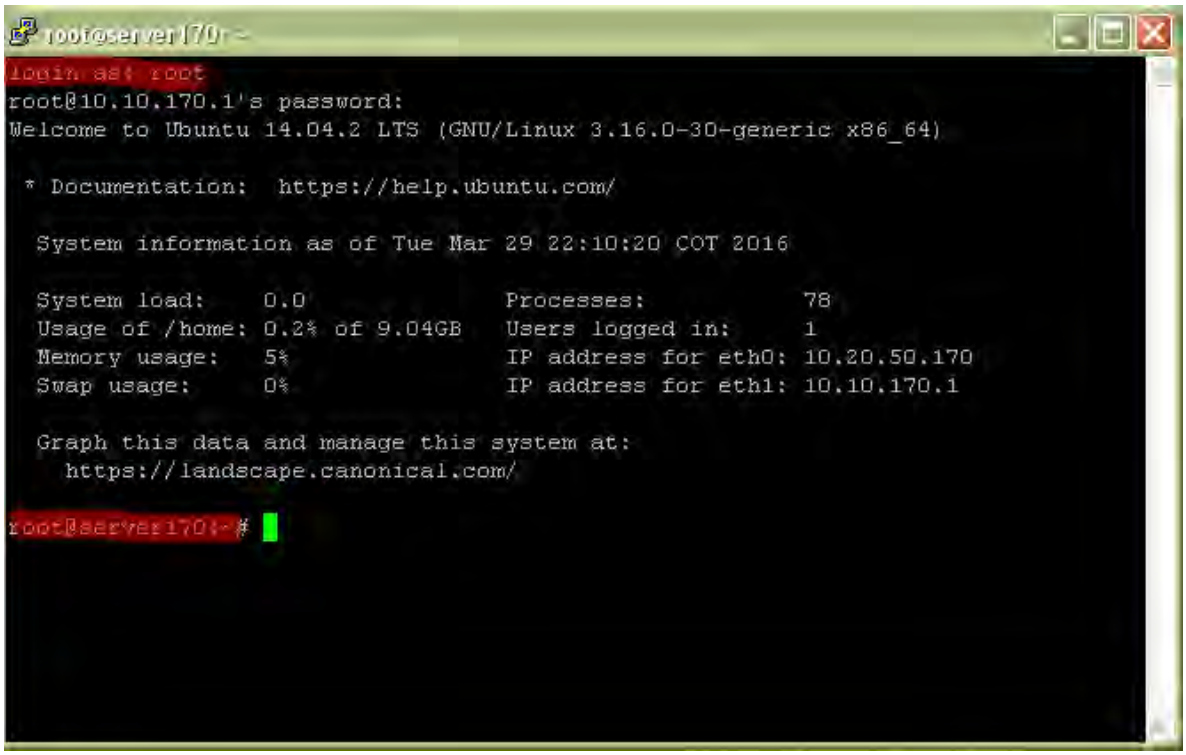
Se reinicia el servicio de SSH para aplicar los cambios, para esto se utiliza el comando **sudo service ssh restart.**



Se ingresa nuevamente a **PuuTY.**



Y al logearse como root se tendra acceso, tal y como se muestra en la siguiente imagen.



3. CONFIGURACION DE AUTENTICACION DE USUARIOS

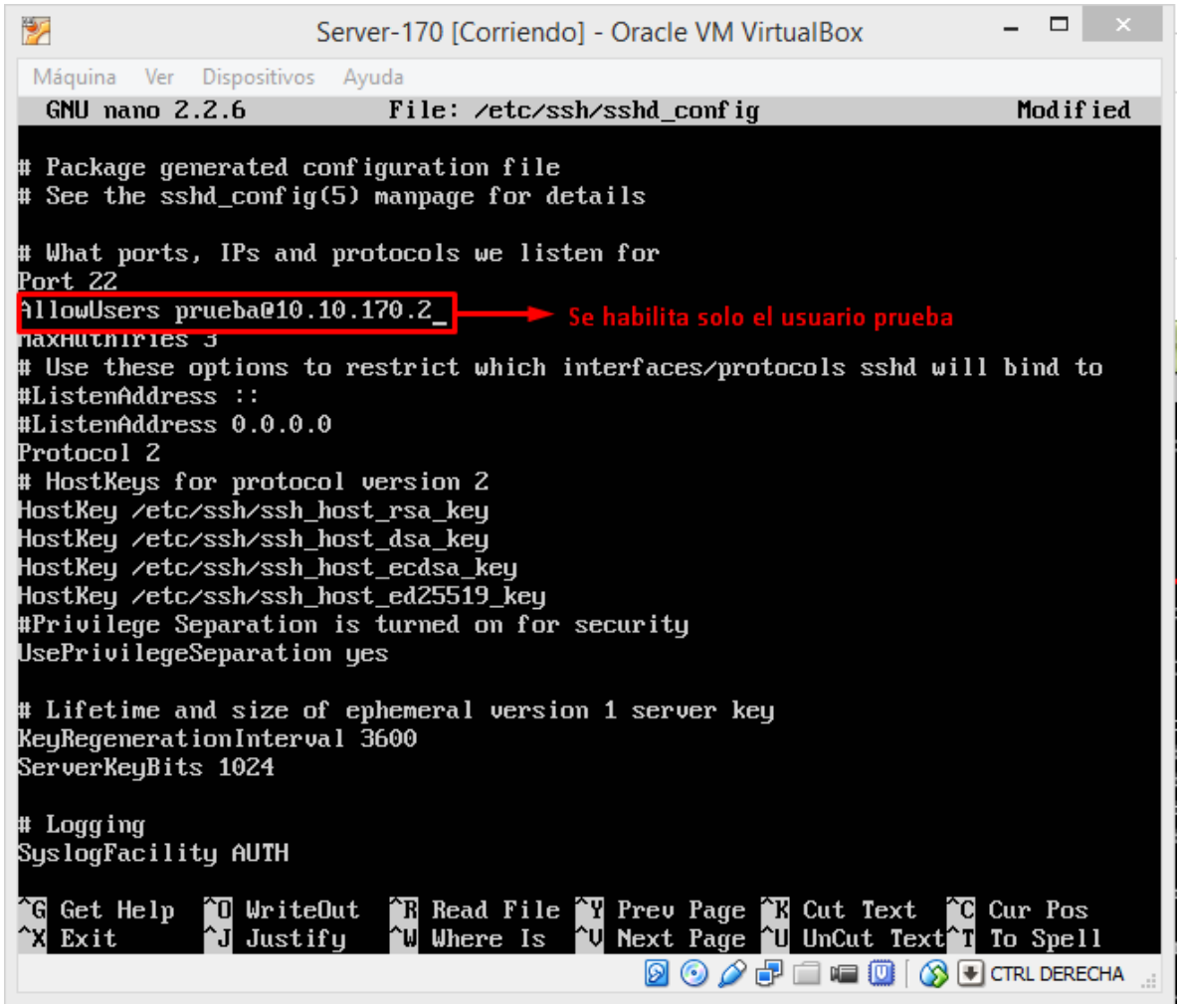
Configurar el servidor SSH para que solo permita la autenticación de los usuarios que se le indique.

Para esto se debe editar el archivo **sshd_config** como se muestra en la siguiente imagen:



Para realizar la autenticación de los usuarios que se deseen, es necesario aumentar la línea **AllowUsers nombre_usuario,** con esta línea en sistemas donde se tiene varios usuarios, quizás existan varios que solo pueden acceder desde la LAN por ejemplo, o quizás solo desde ciertos equipos. O incluso que solo desde su PC puedan trabajar en Linux por lo que no hay razón para que se conecten remotamente vía ssh. Con esta directiva se puede indicar los usuarios que pueden ingresar vía ssh.

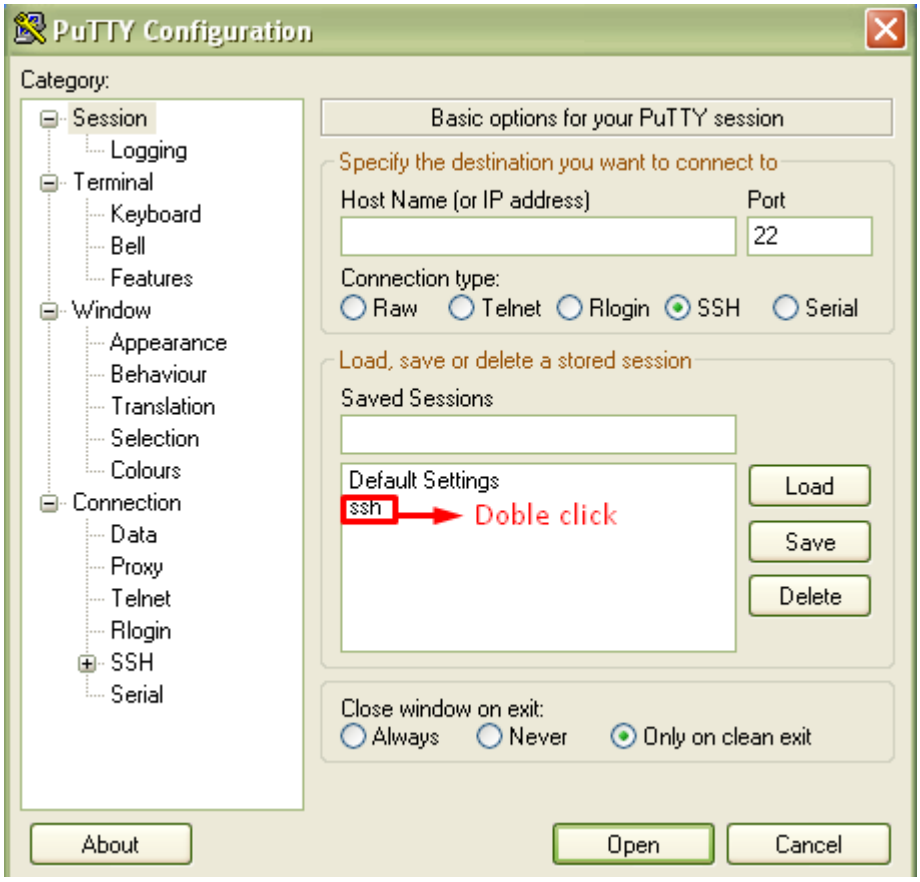
En la siguiente imagen se muestra como se habilita para que solo se registre en el sistema el usuario prueba.



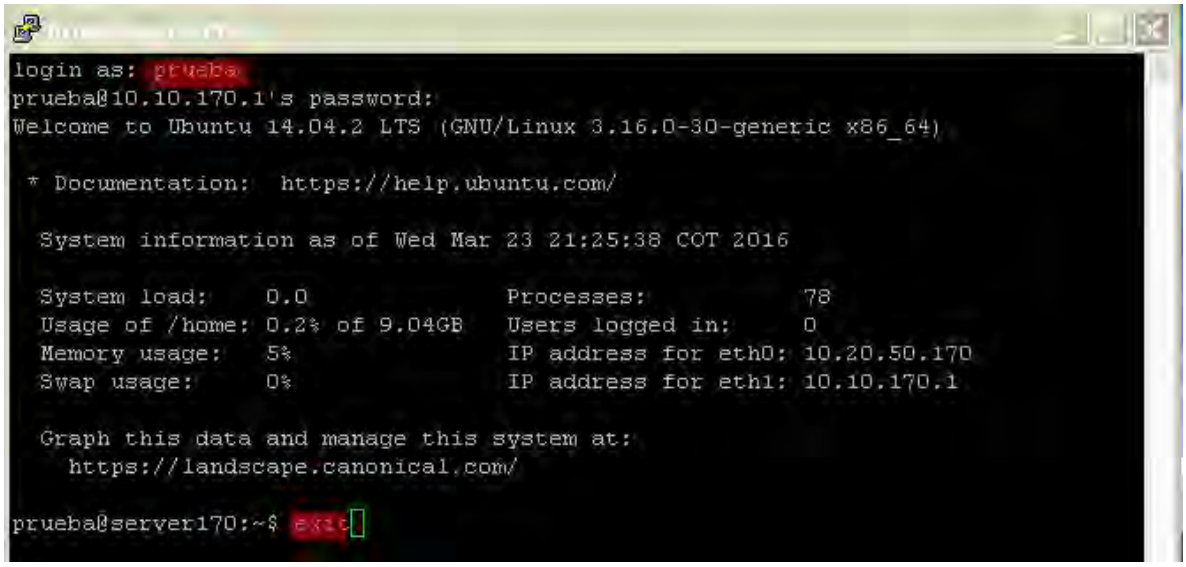
Para que la configuración de resultado es necesario reiniciar el servicio SSH como se muestra a continuación. Una vez reiniciado el servicio se sale de **PuuTY** tal como se muestra en la siguiente imagen.



Para comprobar que el usuario **prueba** puede ingresar al servidor remotamente, se ingresa nuevamente a **PuuTY.**



Se coloca el usuario **prueba** con su clave y se verifica que el usuario puede ingresar. Una vez comprobado el ingreso se sale de **PuTY.**



Para verificar que únicamente se puede ingresar el usuario **prueba** al servidor, se ingresa al usuario **usuario170** para mirar que no puede logearse.

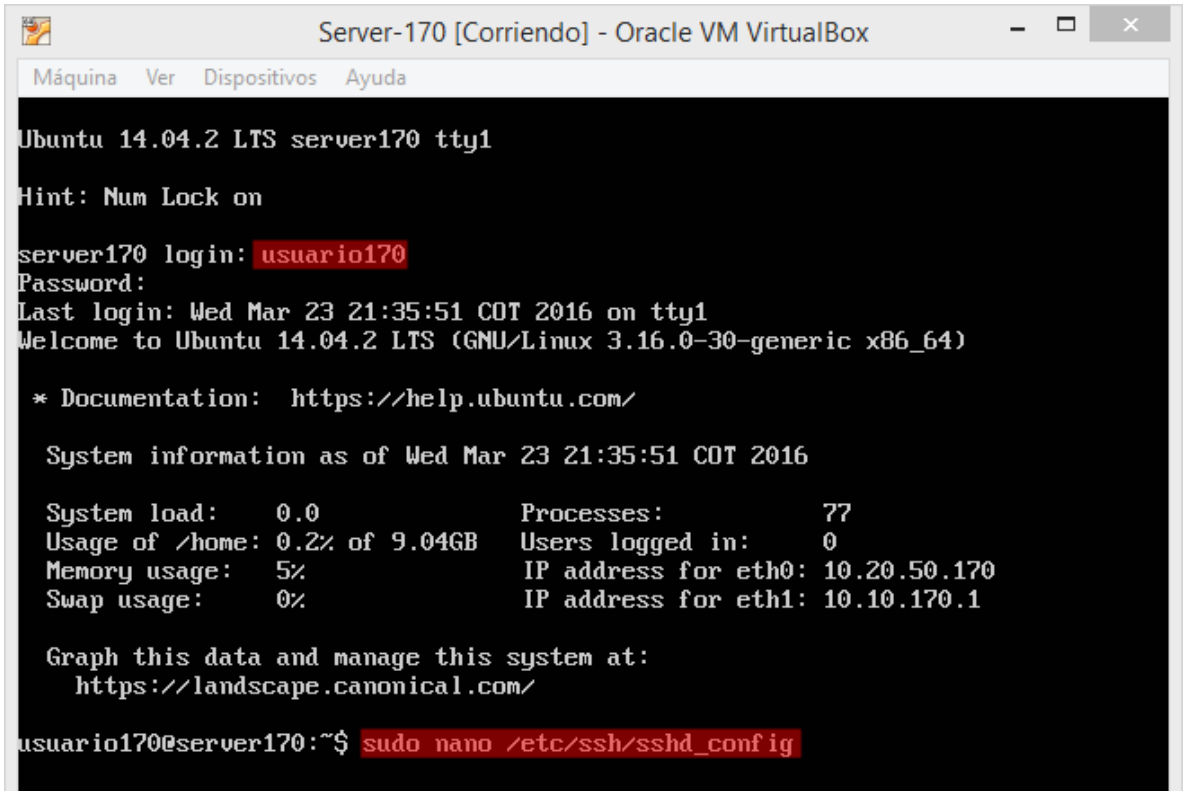
Para esto se ingresa nuevamente a **PuuTY.**



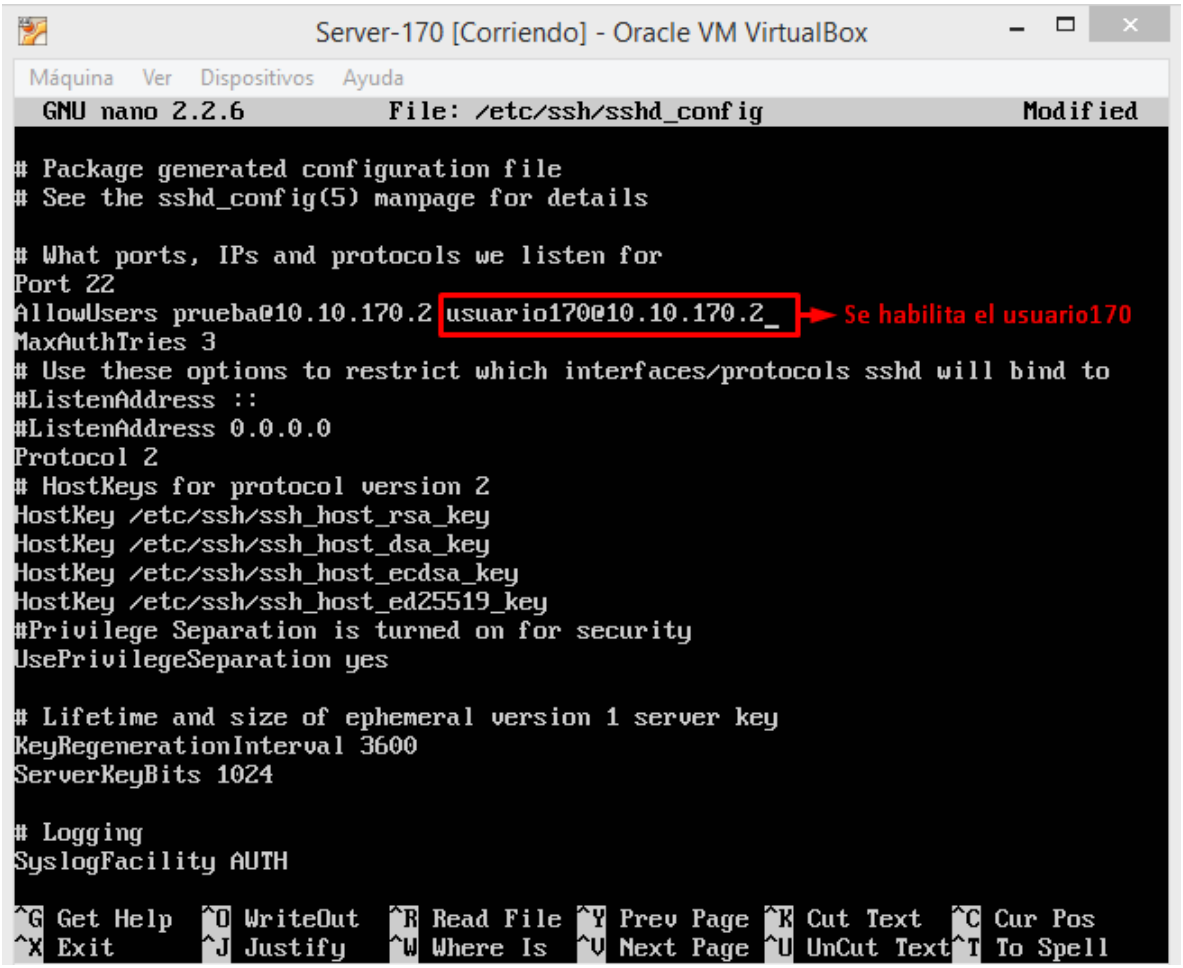
Se logea como usuario **usuario170,** y se observa en la siguiente imagen como el acceso es denegado.



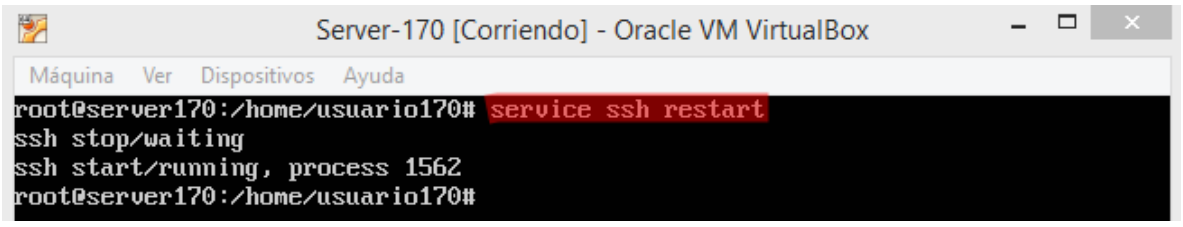
Para poder habilitar al **usuario170** es necesario colocarlo editando el archivo **sshd_config.**



Una vez en el archivo **sshd_config,** se aumenta la línea **AllowUser prueba, usuario170,** para que el usuario puede logearse remotamente en **PuuTY.**



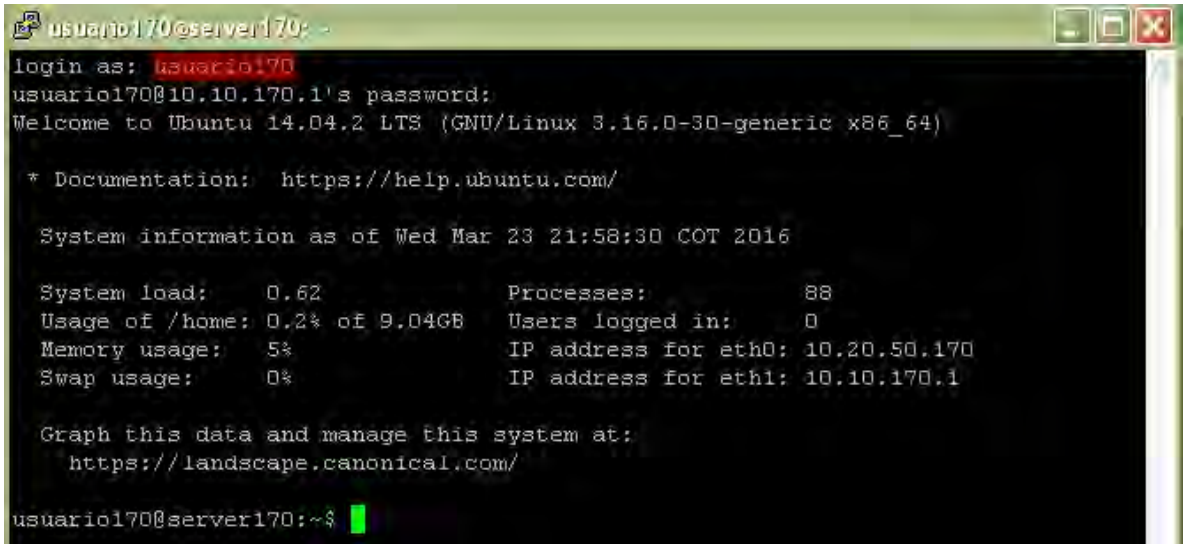
Ya modificado el archivo **sshd_config** se reinicia el servicio SSH.



Posteriormente, se ingresa a nuestro equipo donde se administra remotamente al servidor mediante **PuuTY.**


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
ssh
Doble click
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

Por último, se logea como **usuario170** y se verifica como el usuario puede acceder al servidor.



Anexo I. Instalación y configuración de servidor chat OPEN FIRE.

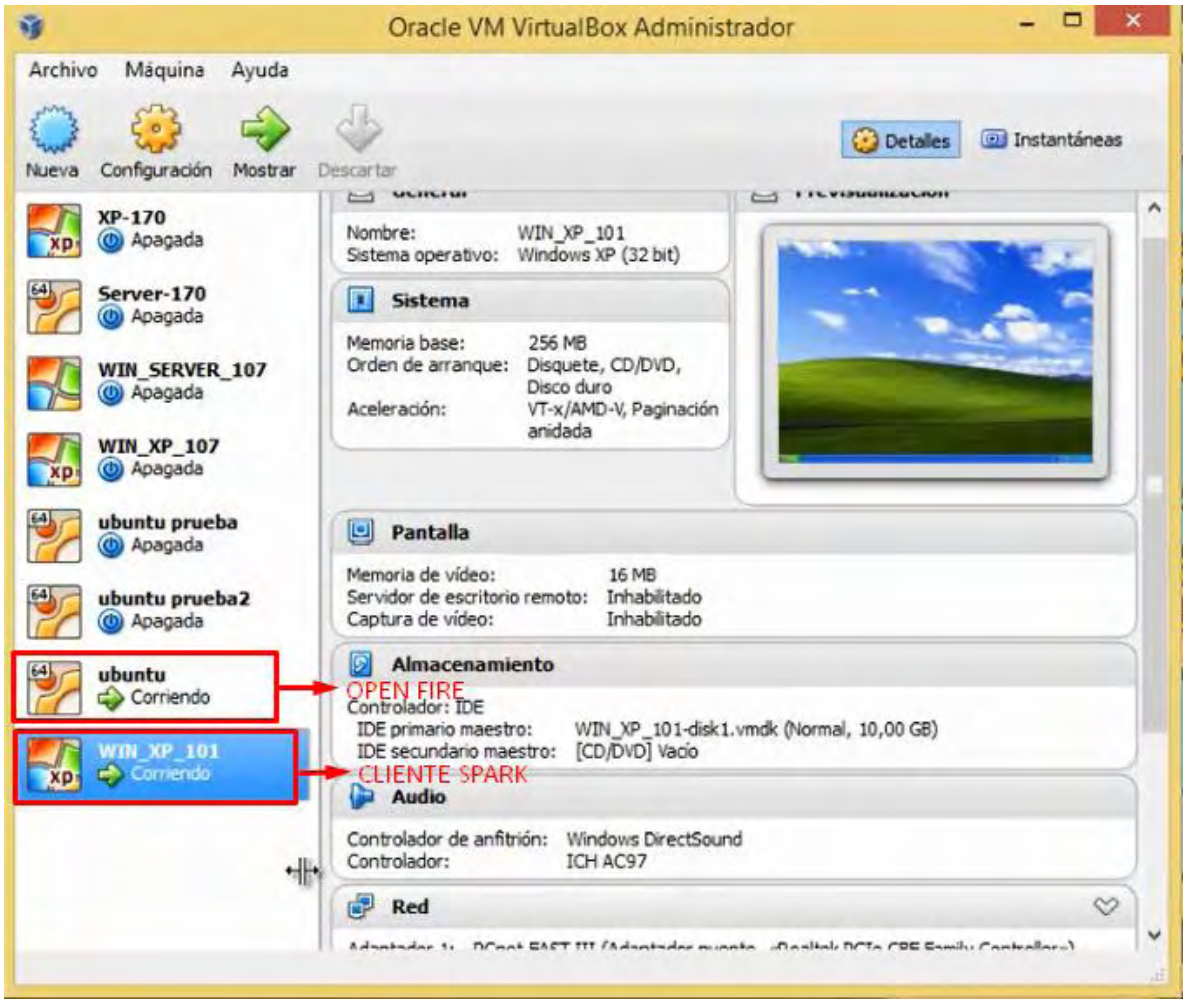
ÍNDICE

Pág.

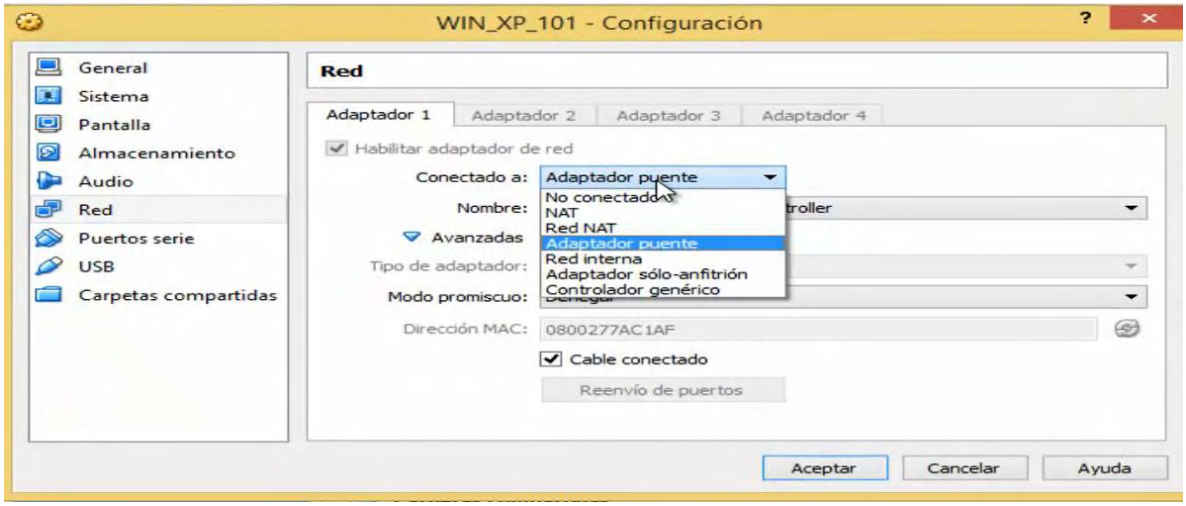
1. REQUERIMIENTOS SOFTWARE 371
2. INSTALACION SERVIDOR OPENFIRE 376
3. CONFIGURACION BASICA DE OPENFIRE 379
4. CONFIGURACION AVANZADA DE OPENFIRE 382
5. INSTALACION DE CLIENTES Y PRUEBA DE COMUNICACIÓN 388

1. REQUERIMIENTOS SOFTWARE

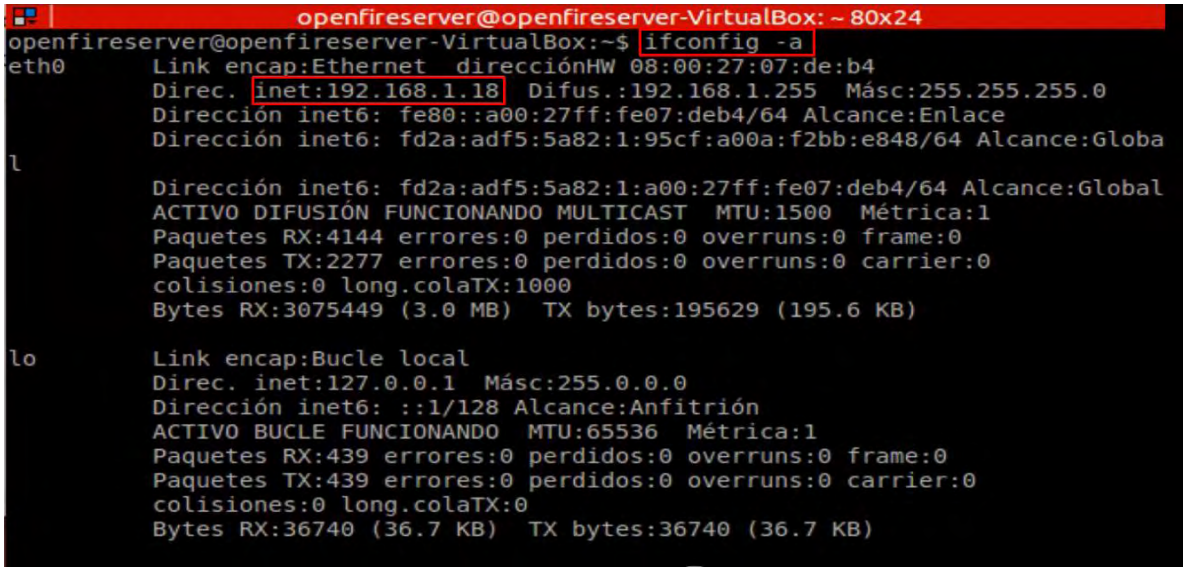
Para este caso se tienen tres máquinas, dos virtuales y una física, la primera máquina virtual es Ubuntu donde se instalará el servidor OPENFIRE, la segunda una Windows xp donde se instalará el cliente SPARK, y la maquina física, donde está corriendo Virtual Box, se instalará de igual manera el cliente SPARK.



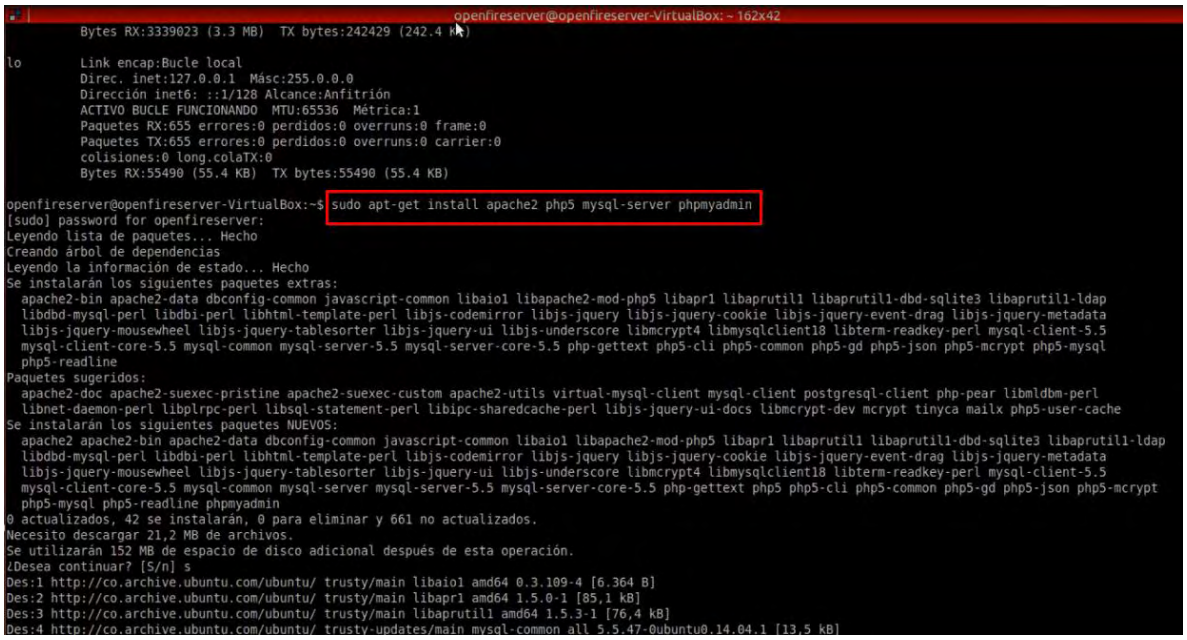
Se debe de tener en cuenta que las maquinas deben estar en adaptador puente para su funcionamiento.



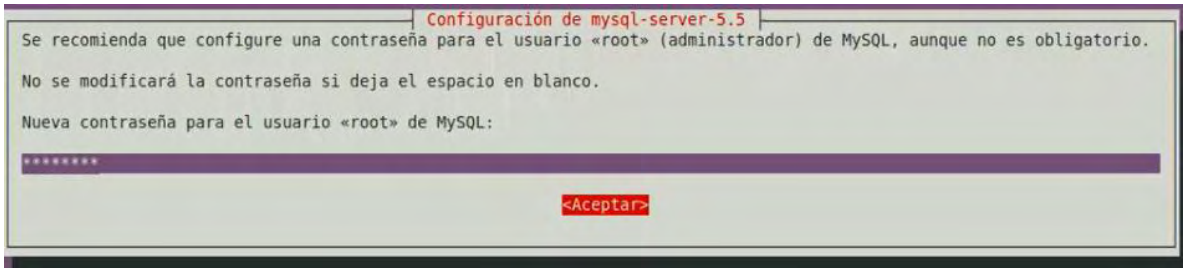
Una vez hecho lo anterior, se ingresa a la maquina Ubuntu donde se instalara los requerimientos software y el servidor OPENFIRE, se abre una terminal, se coloca el comando *ifconfig –a* y se verifica que la dirección IP está asignada, para este caso la dirección IP es la de la tarjeta de red *eth0.*



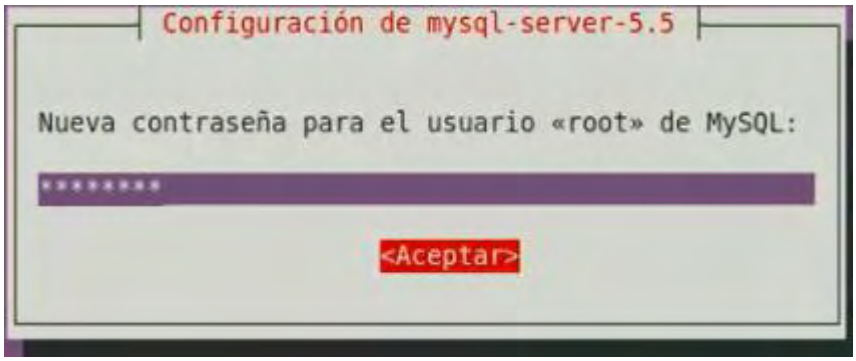
Luego se realiza la instalación de apache2, php5, mysql server y phpmyadmin, con el siguiente comando:



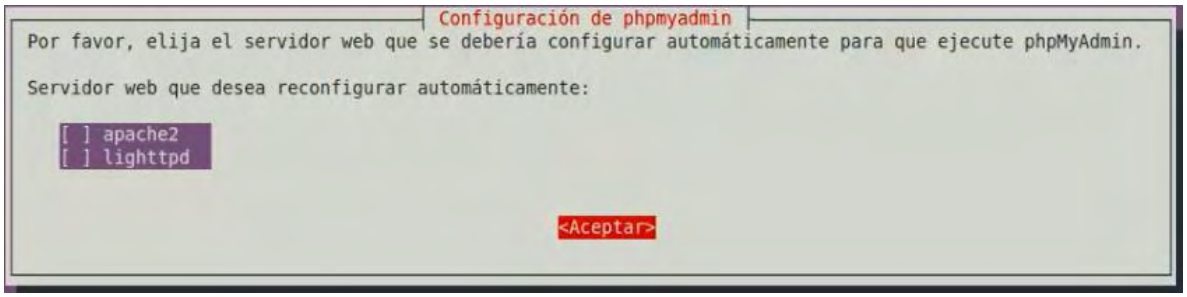
En seguida aparecerá una ventana donde se coloca la contraseña para el usuario root de mysql server.



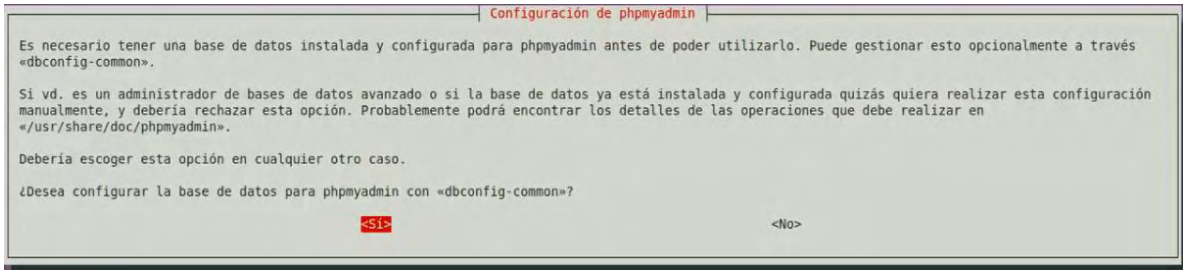
Se confirma la contraseña.



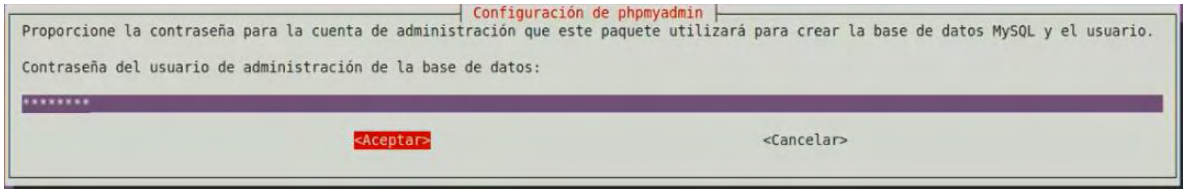
Luego aparecerá la siguiente ventana donde se elige el servidor web que se utilizara para la ejecución de phpmyadmin.



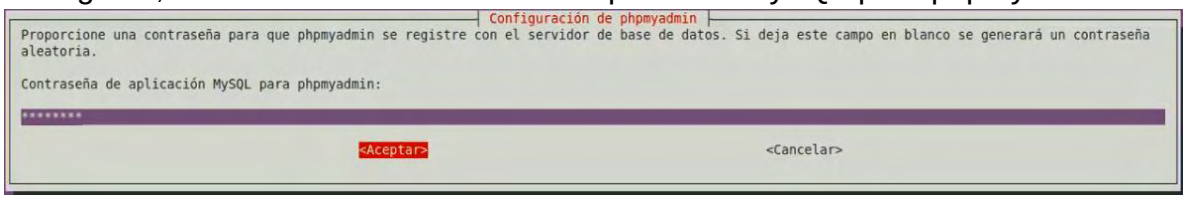
Enseguida aparecerá la siguiente ventana, donde se configurará la base de datos para phpmyadmin, se escoge la opción *Sí.*



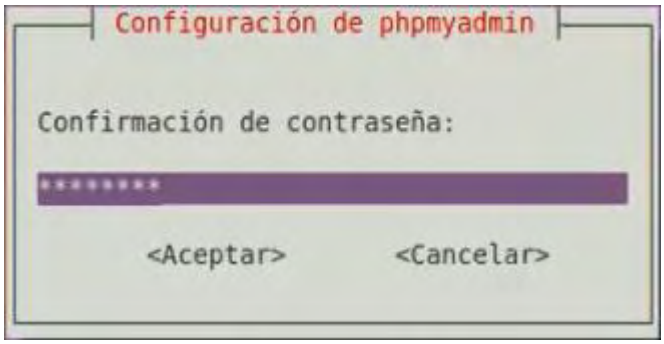
Luego, se coloca la contraseña del usuario administrador de la base de datos.



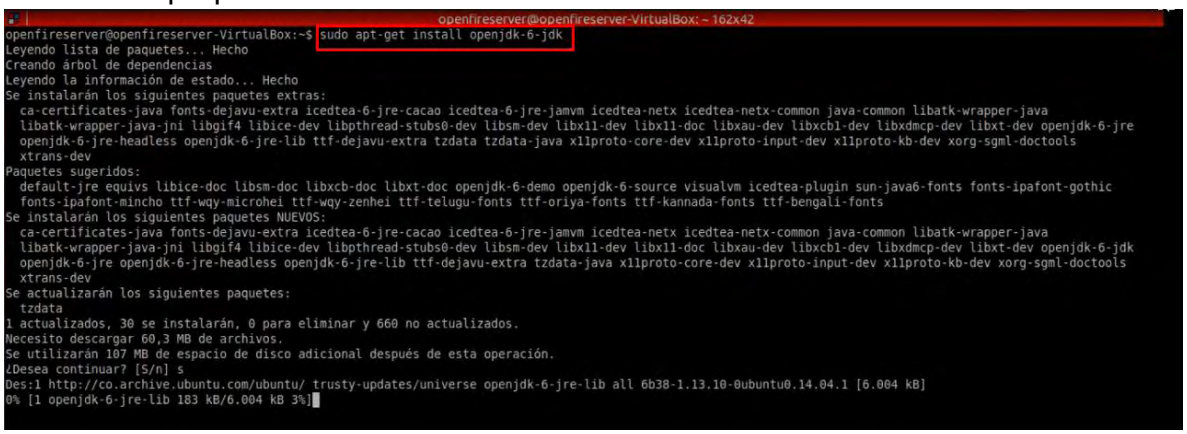
Enseguida, se coloca una contraseña de aplicación MySQL para phpmyadmin.



Se confirma la contraseña.

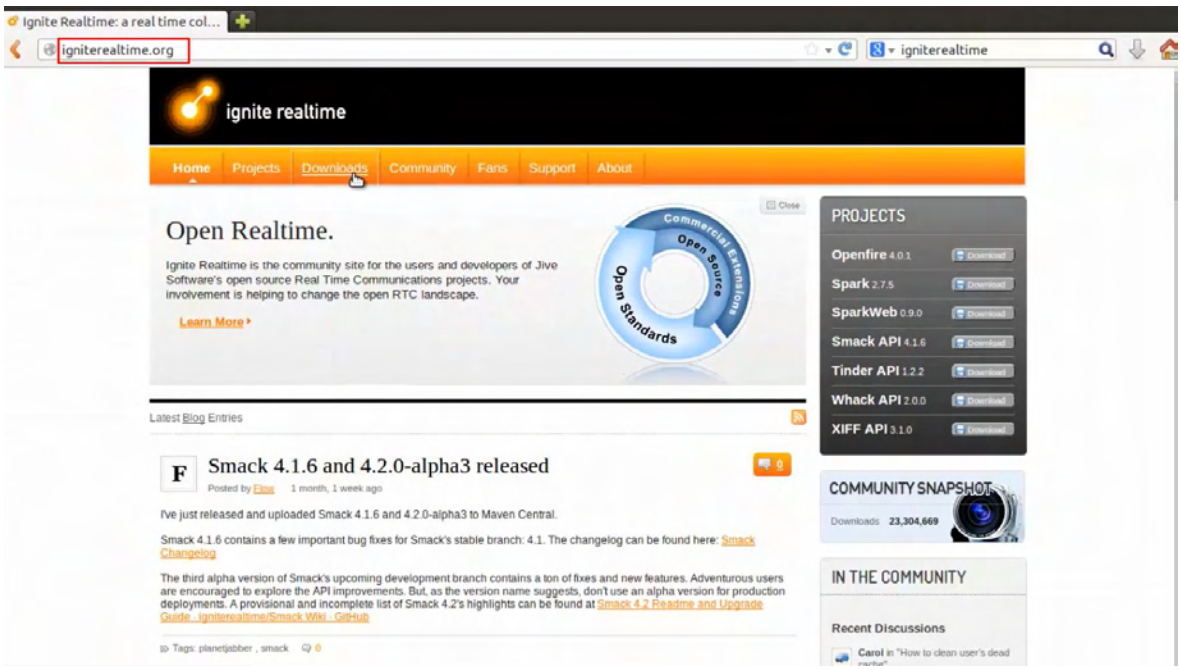


En seguida se procede a la instalación de openjdk, con el siguiente comando se instalara el paquete.

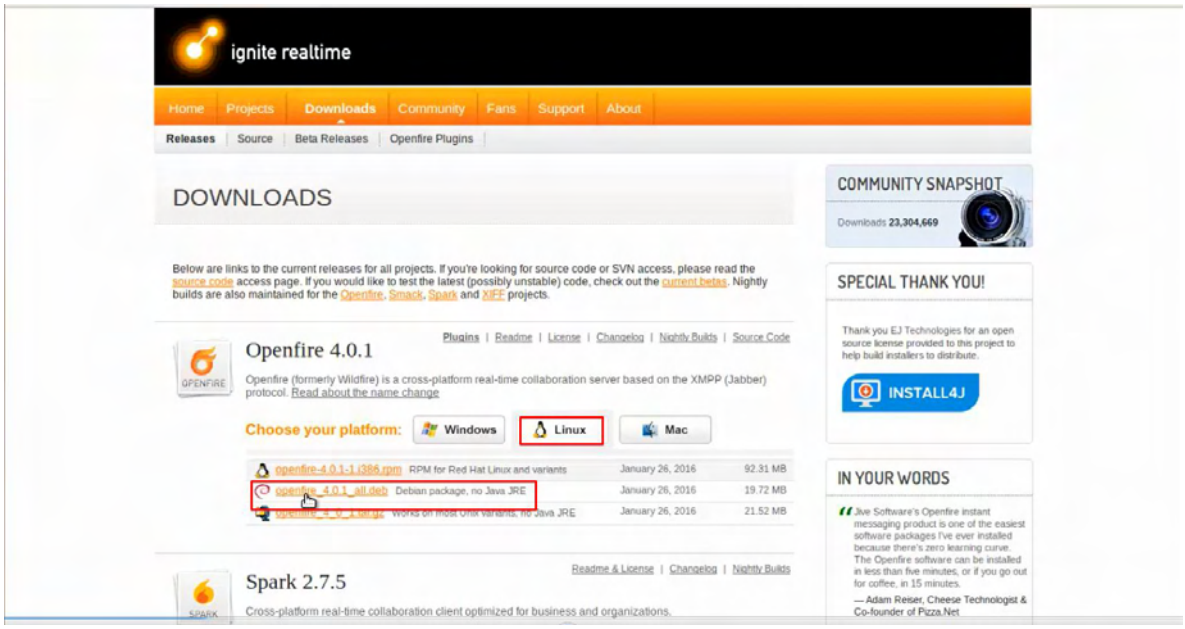


2. INSTALACION SERVIDOR OPENFIRE

Para la instalación de OPENFIRE se debe dirigir a la página oficial y elegir la opción de **Downloads**.



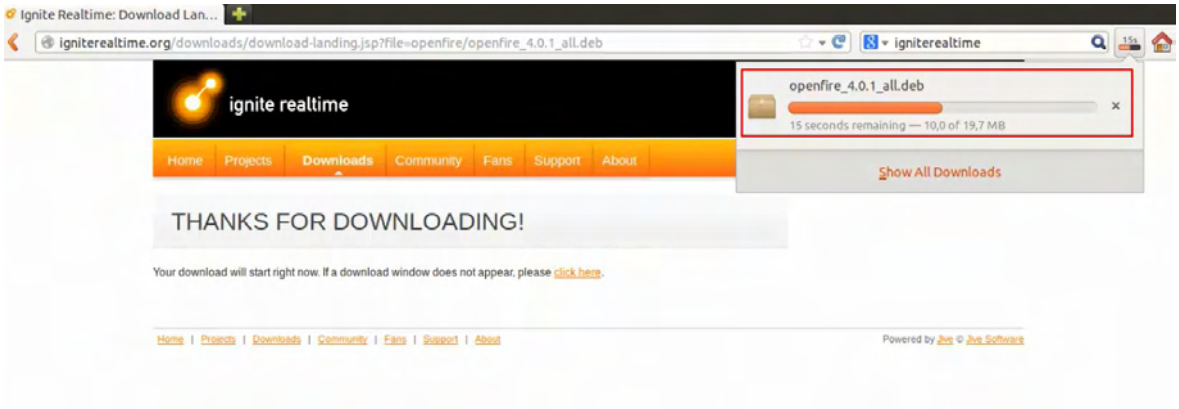
Una vez en descargas se da clic sobre el botón Linux y posteriormente el paquete **.deb de OPENFIRE**.



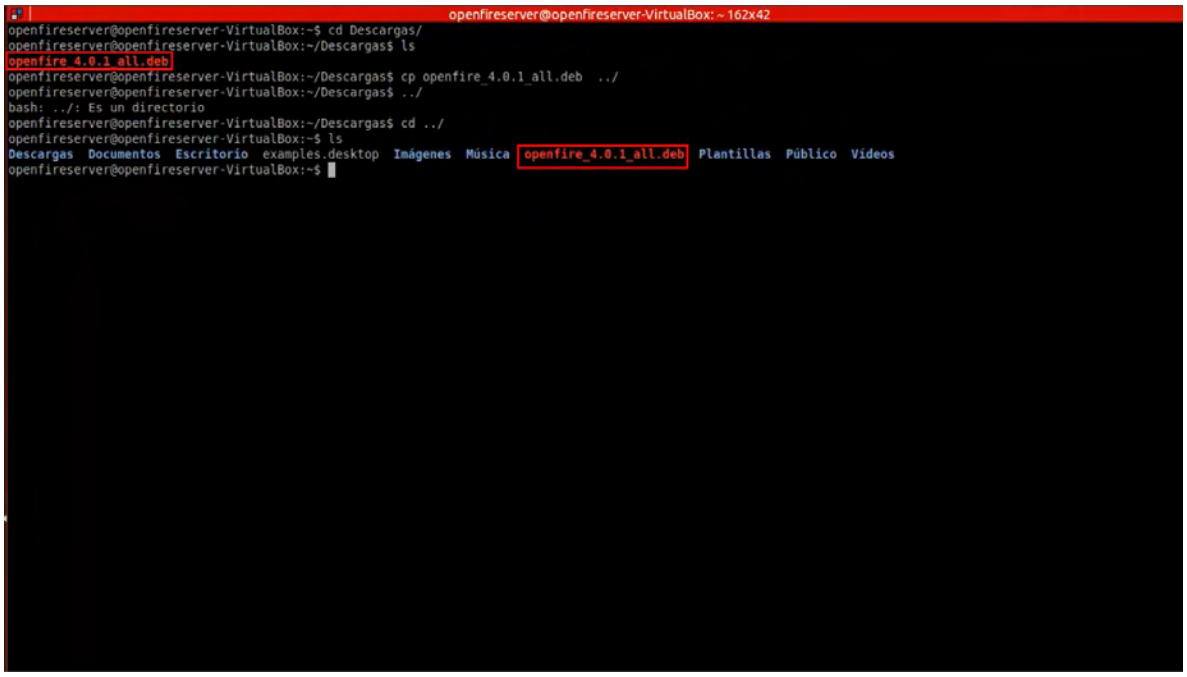
Se abrirá el administrador de descargas.



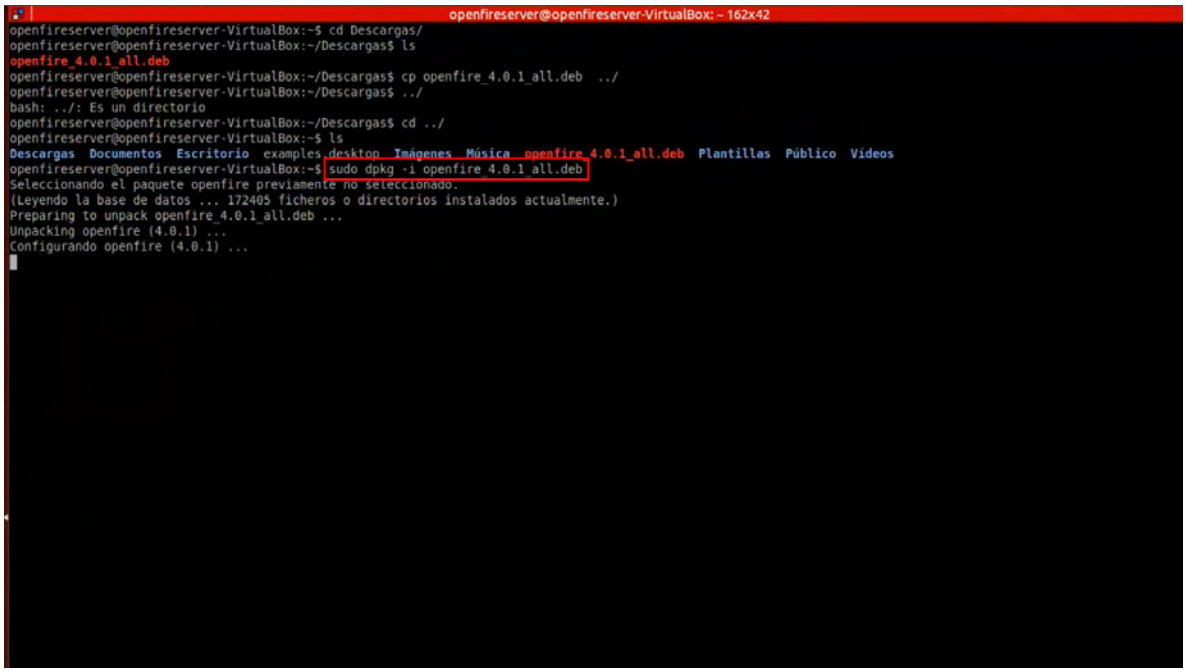
Y empezará la descarga.



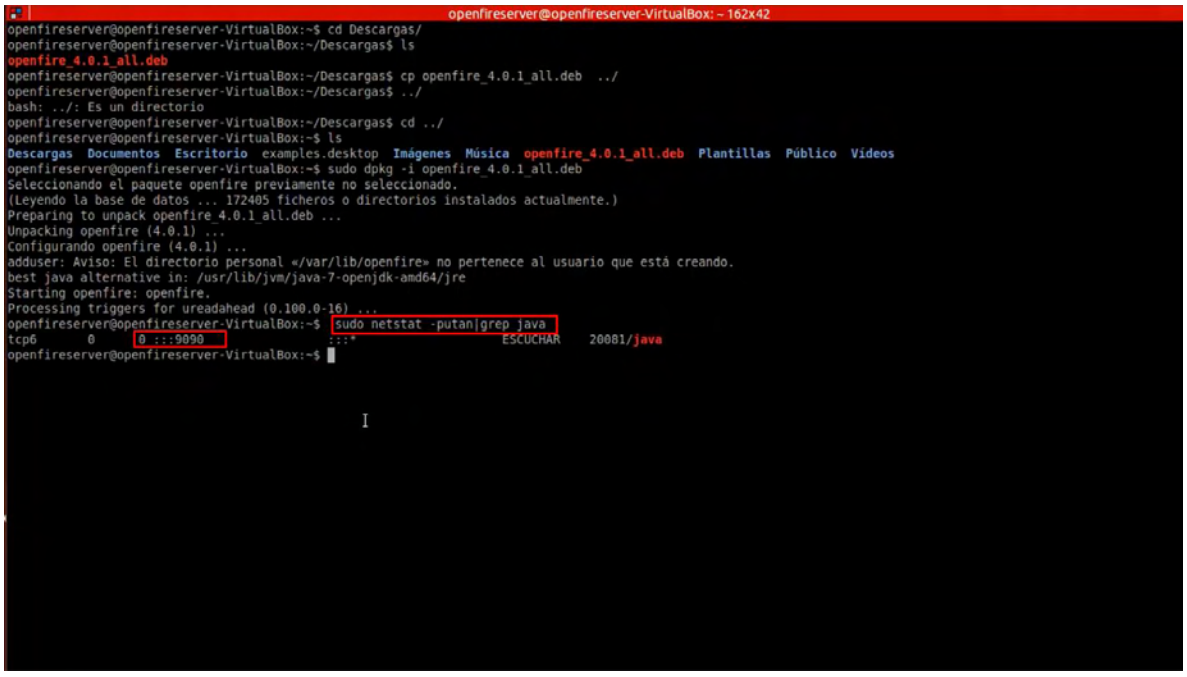
Luego en la consola, se ubica en la ruta de Descargas y se copia el archivo en otra carpeta, esto es opcional, en este caso se copió en la carpeta del usuario.



Ahora se desempaqueta el archivo con el siguiente comando:

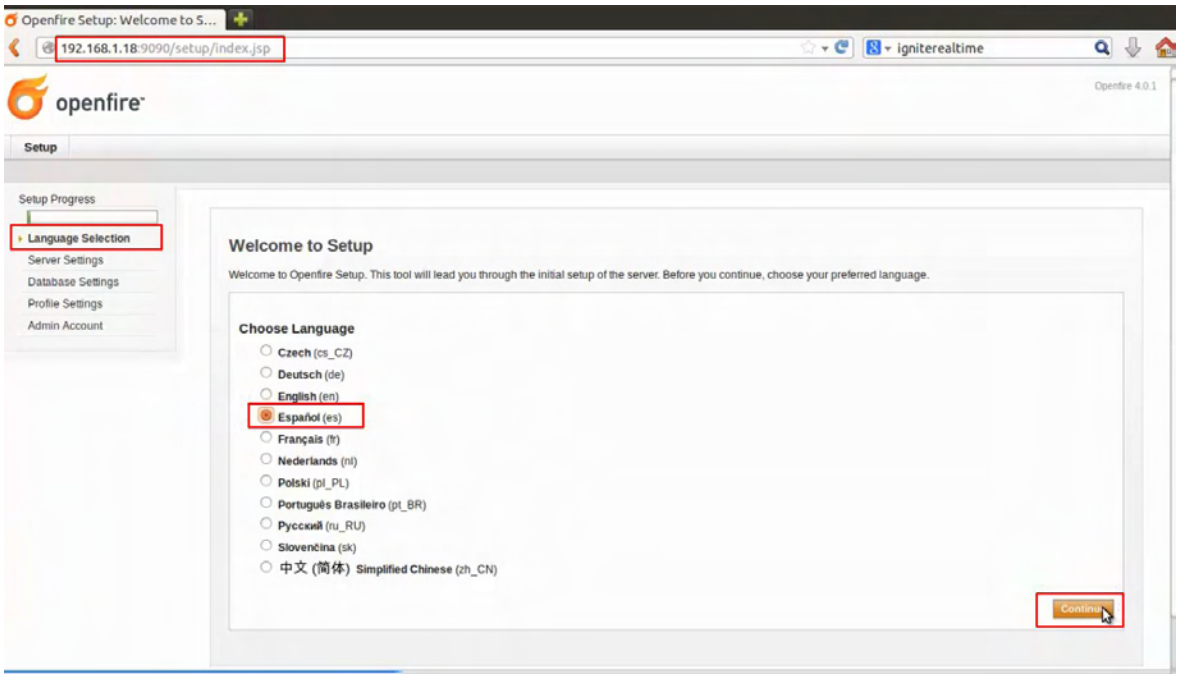


Una vez hecho lo anterior se verifica el funcionamiento de OPENFIRE, con el siguiente comando:

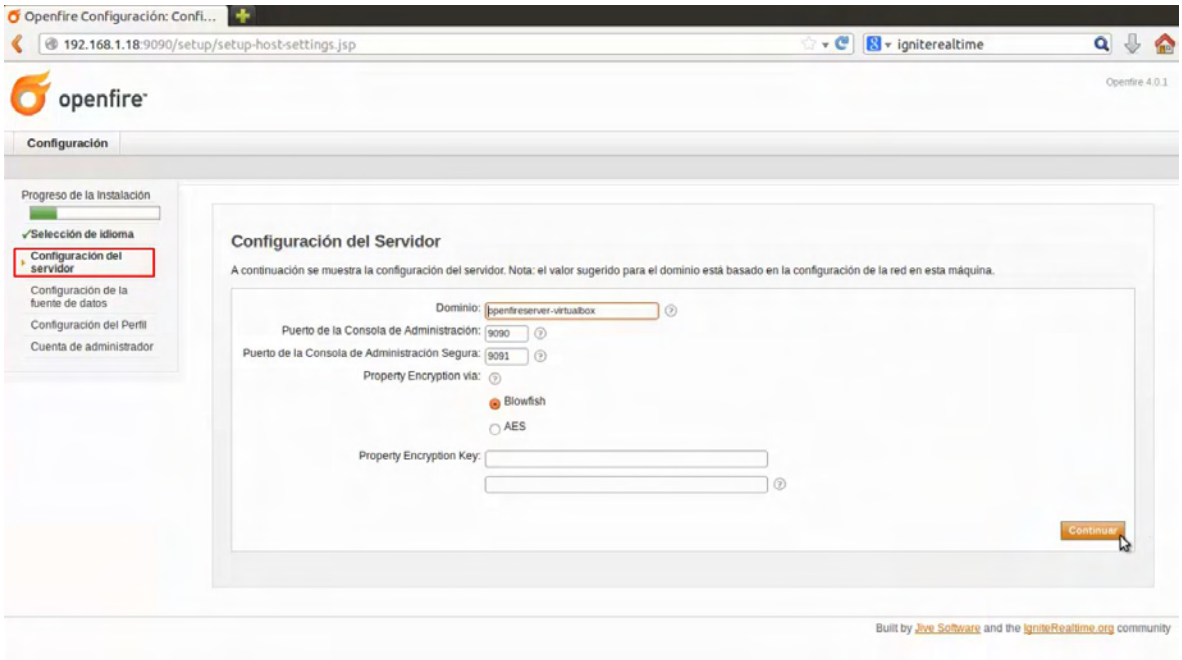


3. CONFIGURACION BASICA DE OPENFIRE

A continuación, se mostrará la configuración básica del servidor OPENFIRE, para esto se debe ingresar a un navegador, y en la url colocar la dirección IP del servidor ip, (direccion_ip_servidor:9090), en esta primera pantalla escoger el idioma con el que trabajará el servidor.



En Configuración del servidor se deja todo por defecto.



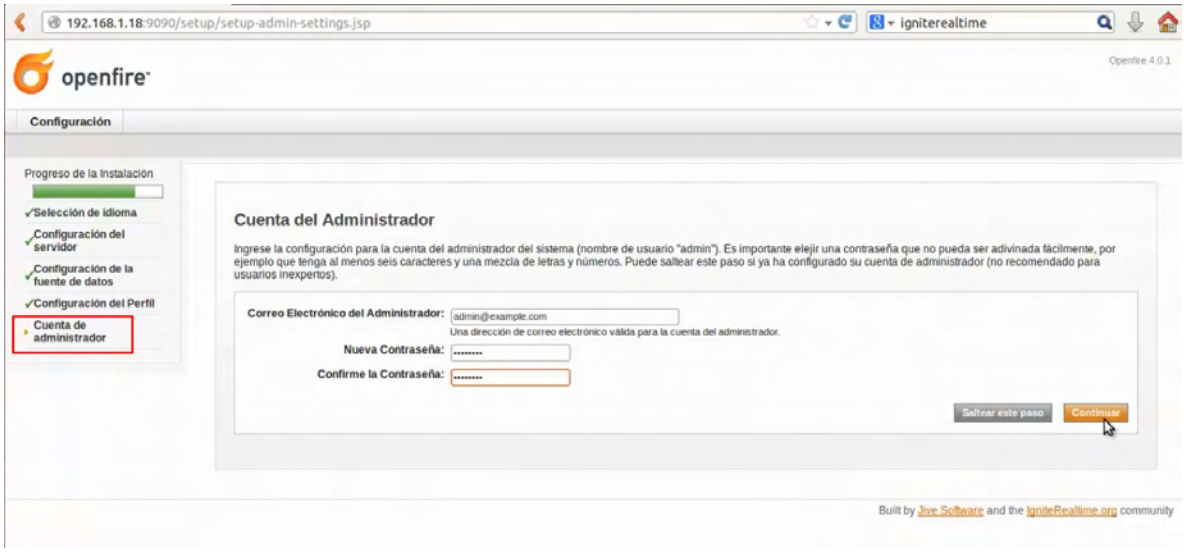
En **Configuración de la fuente de datos** se elige la **Base de datos interna**.



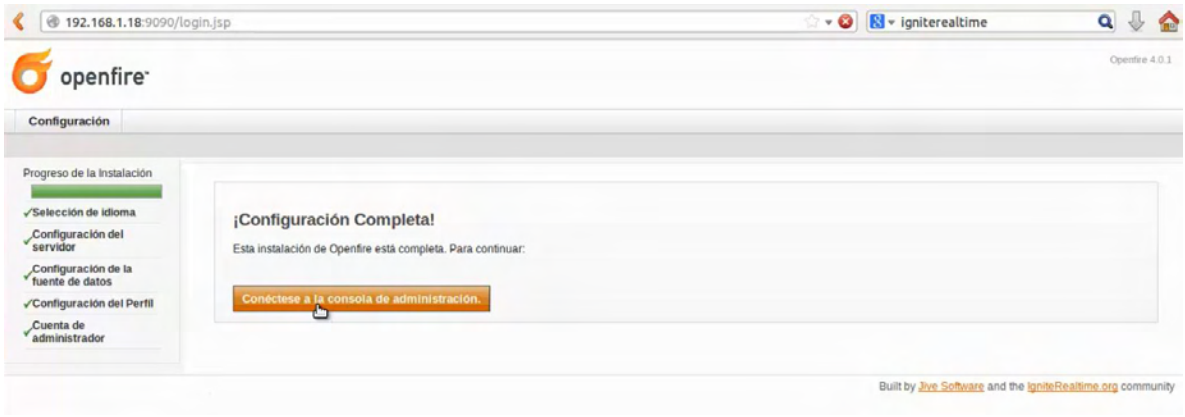
En **Configuración del Perfil** *se* deja la opción **Por defecto**.



En **Cuenta de administrador**, *se* coloca el correo electrónico del administrador y una contraseña.

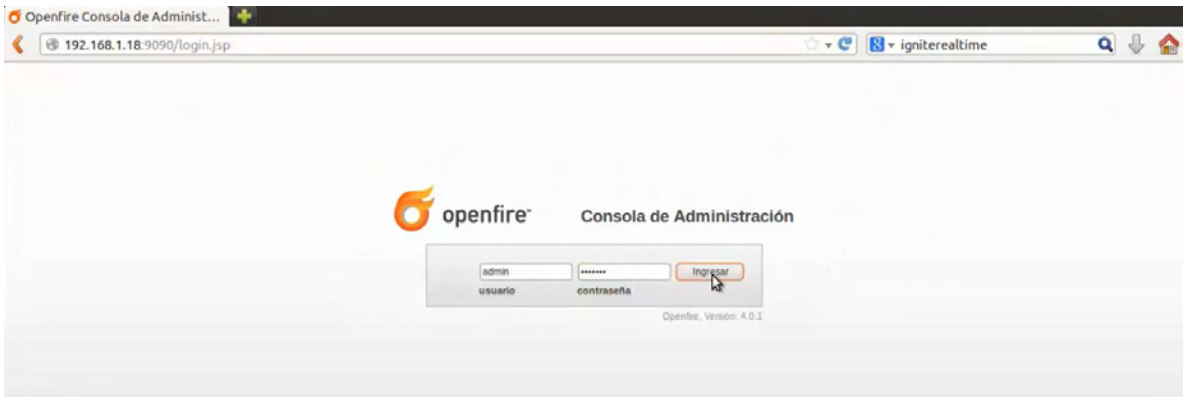


Por último, aparecerá una pantalla donde notificará que la configuración fue completada. Se da clic en **Conectarse a la consola de administración**.

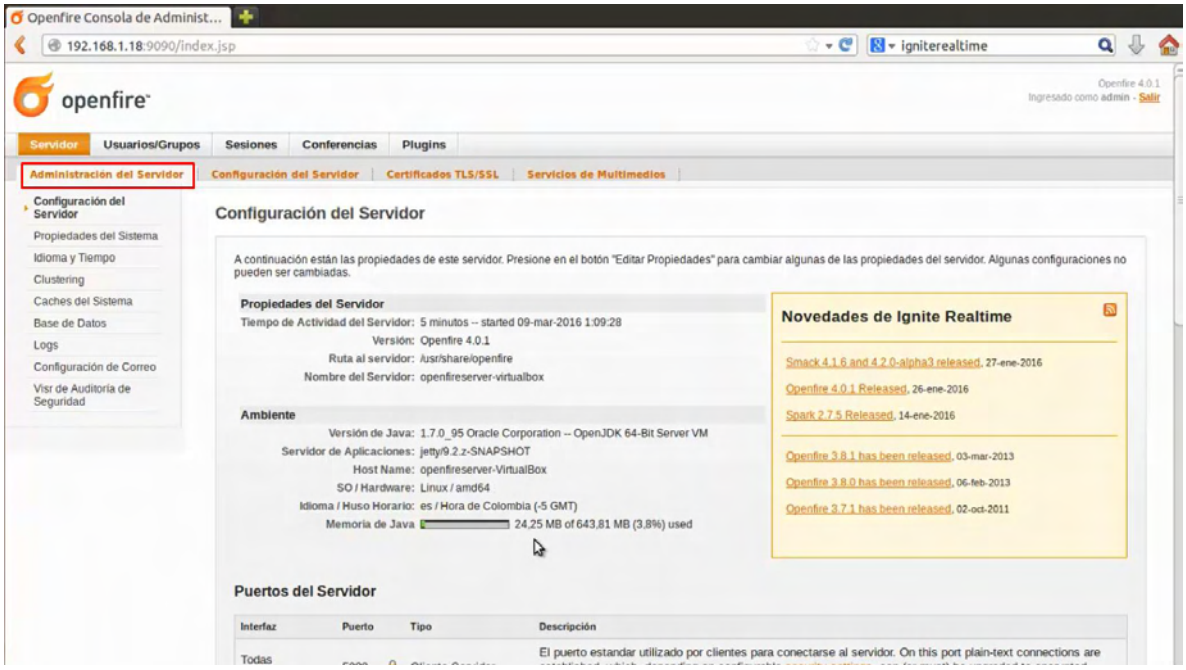


4. CONFIGURACIÓN AVANZADA DE OPENFIRE

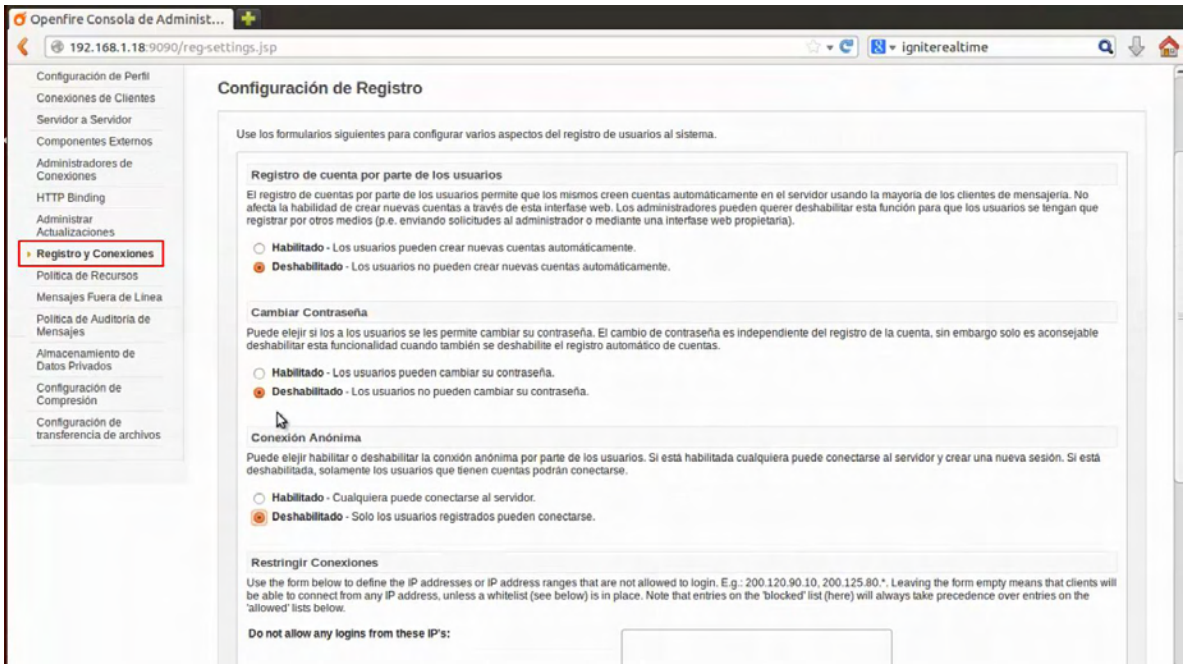
Para ingresar a la configuración avanzada es necesario logearse, por defecto el usuario es **admin** y la contraseña se la colocó en el anterior paso.



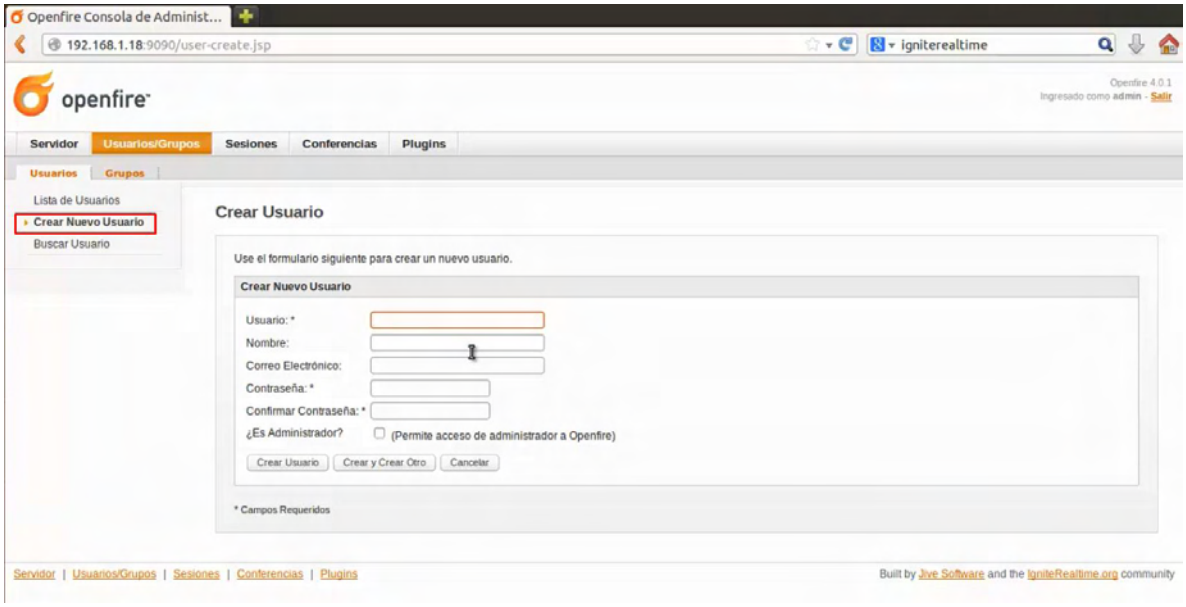
En el botón Servidor, en el sub botón **Administración del servidor** muestra una descripción general de las propiedades del servidor.



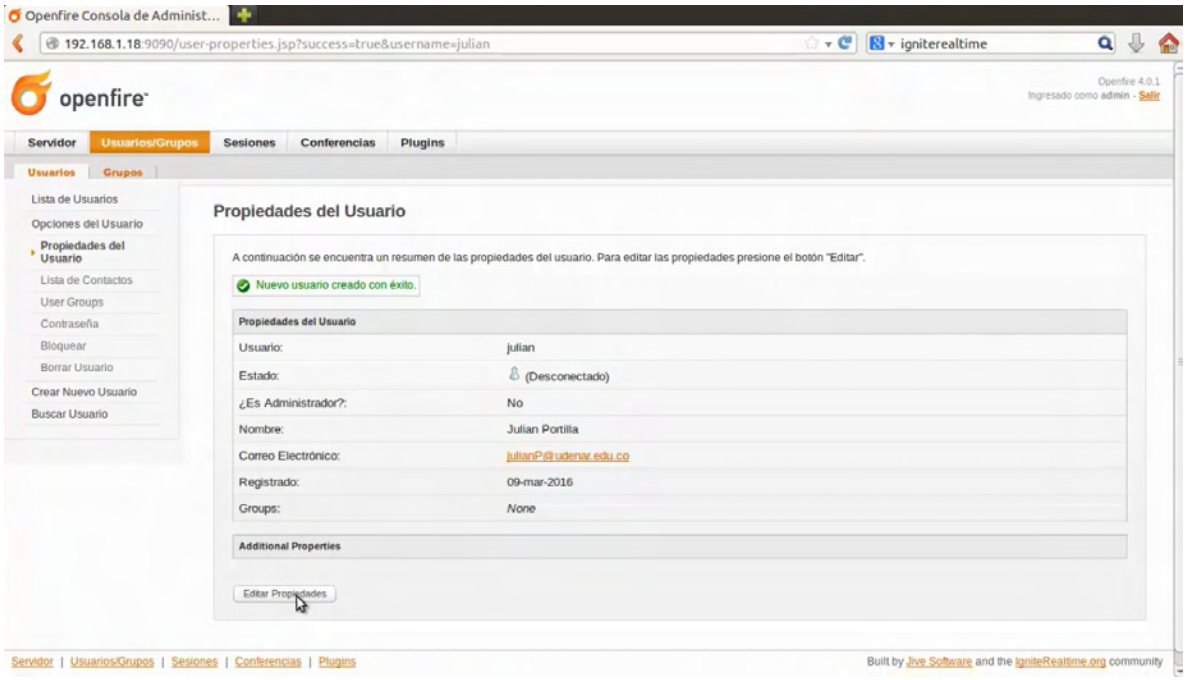
Ahora en el sub botón **Configuración del servidor** en la pestaña **Registro y conexiones**, se dan los perfiles para los usuarios que se vayan a crear. Para este caso se configuró de la siguiente manera. Al final se da clic en el botón **Guardar configuración**.



En el botón **Usuarios/Grupos**, en el sub botón **Usuarios**, en la pestaña se pueden crear usuarios con sus respectivas contraseñas y darles o denegarles permiso de administrador.

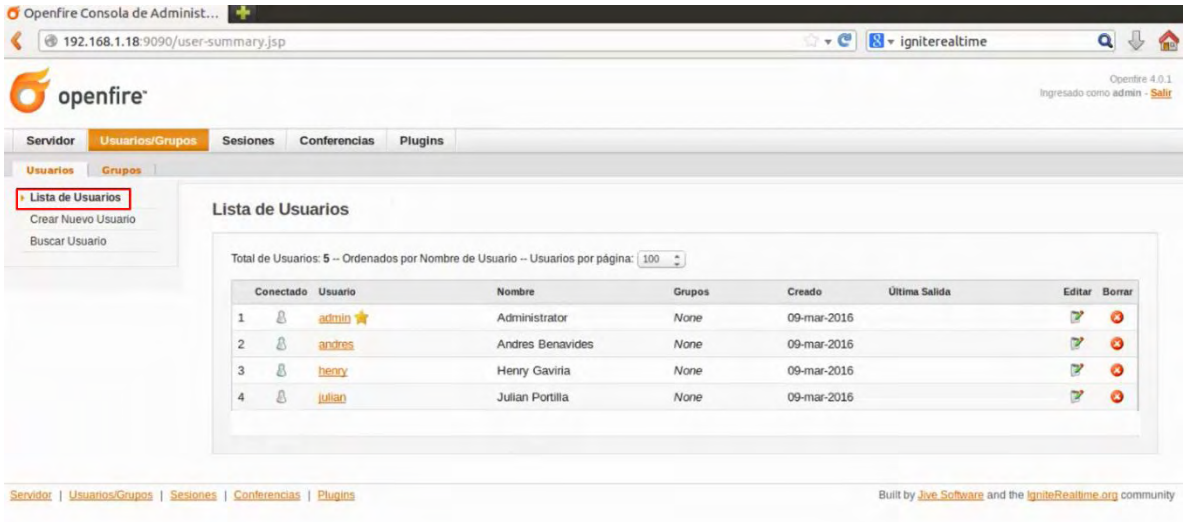


Al momento de crear el usuario aparecerá una ficha con las características del usuario.

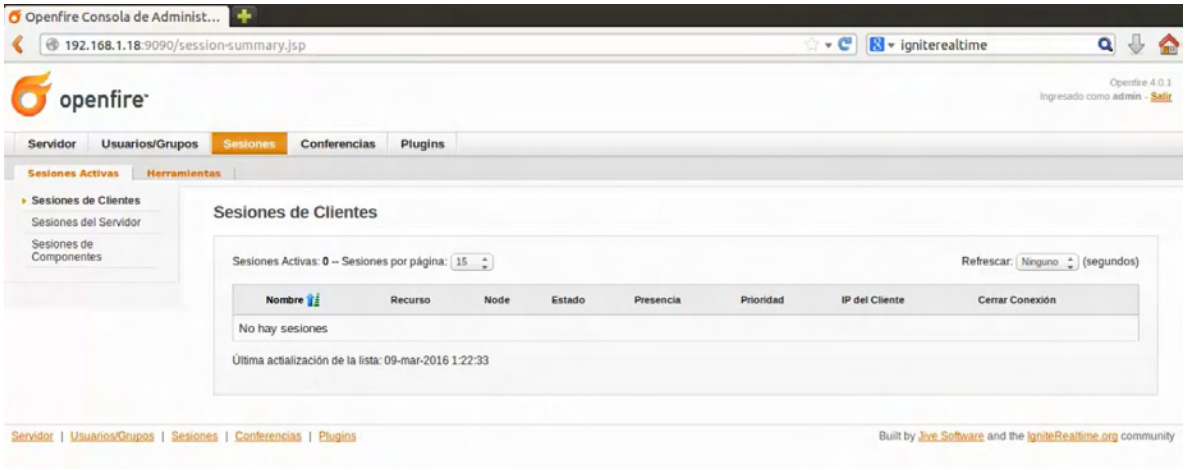


Para mirar los usuarios que se han creado se debe dirigir hacia la pestaña **Lista de Usuarios**, donde se listan los usuarios creados.

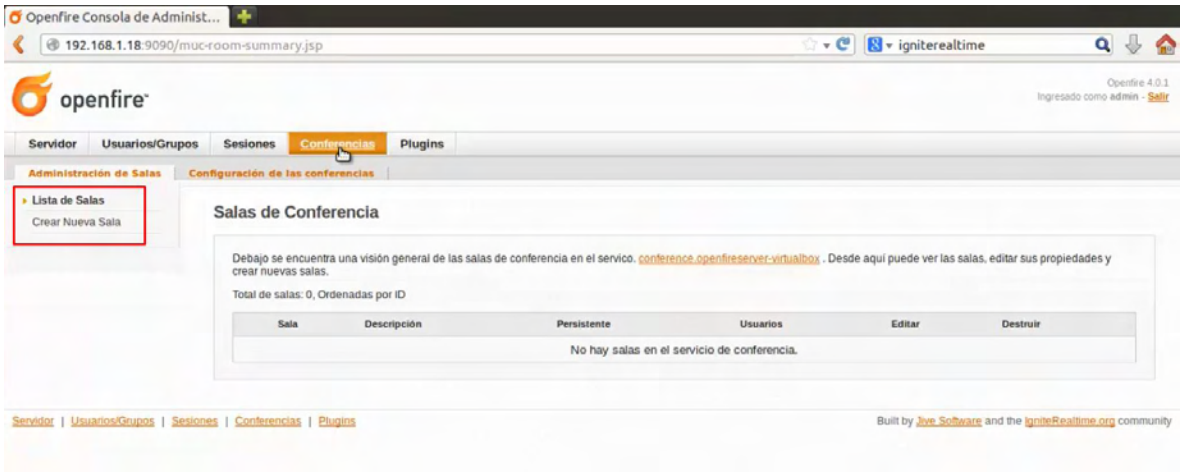
También se pueden crear grupos en los cuales se asignarán usuarios previamente creados.



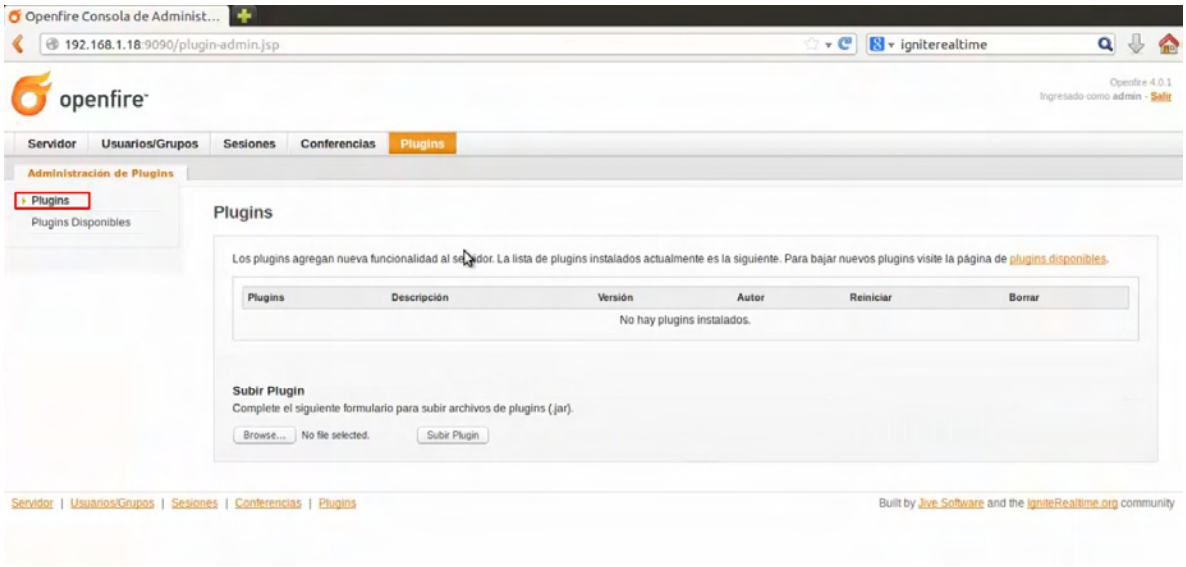
En sesiones se puede observar cuantas sesiones tanto de clientes, de servidor como de componentes se encuentran activas, en este caso como no se ha iniciado ningún cliente se encuentra en cero.



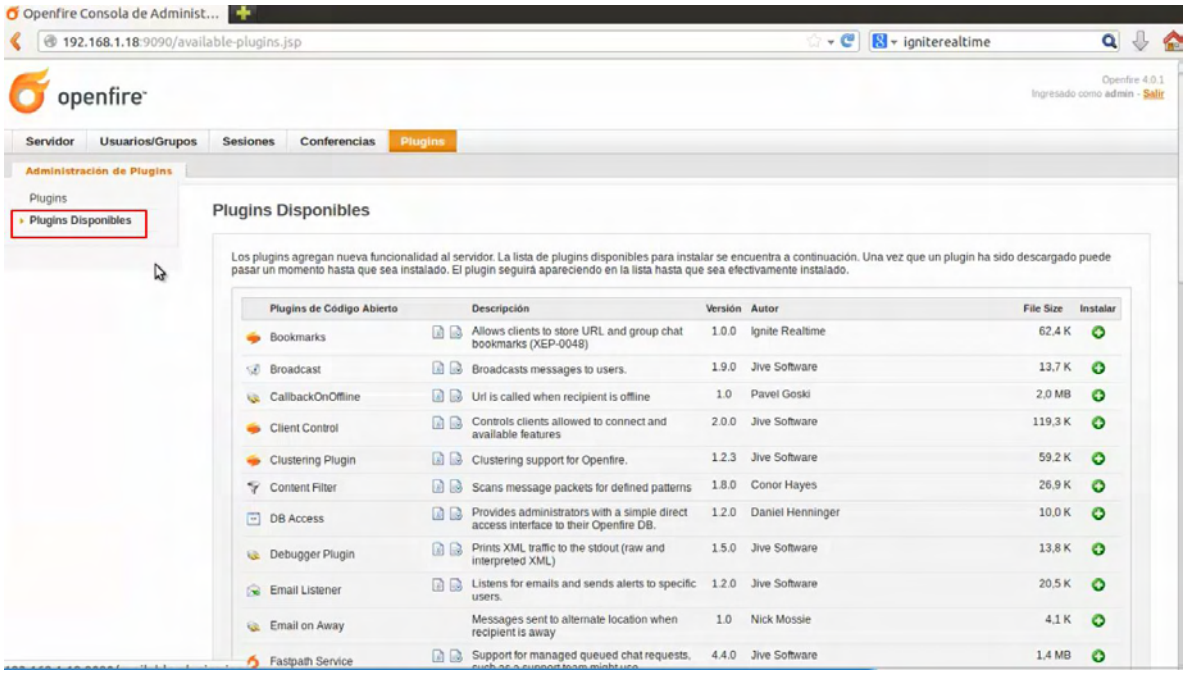
En el botón conferencias se puede crear salas de chat y sus respectivas configuraciones.



En el último, botón **Plugins** en la pestaña **Plugins**, se deberían listar los complementos que se hayan descargado para dar mejoras al servidor, en este caso como no se ha descargado ninguno, la lista se encuentra vacía.



En la siguiente pestaña **Plugins Disponibles**, se observan una lista de plugins que se pueden descargar.

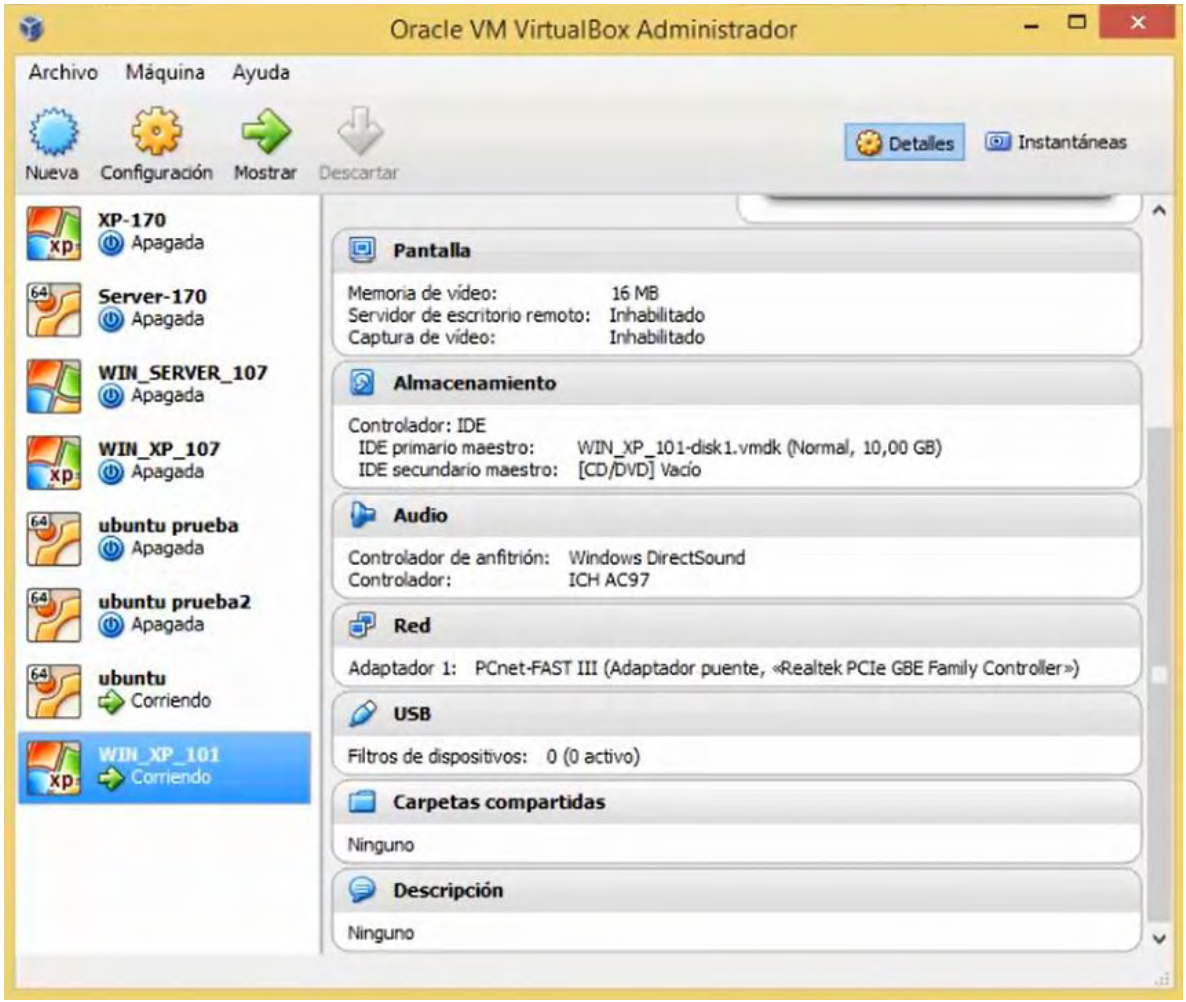


Por último, al hacer esta configuración se cierra el navegador y se abre una terminal, en esta se verifica que el servidor está corriendo y que además del puerto 9090 se habilitaron otros, tal como se muestra a continuación.

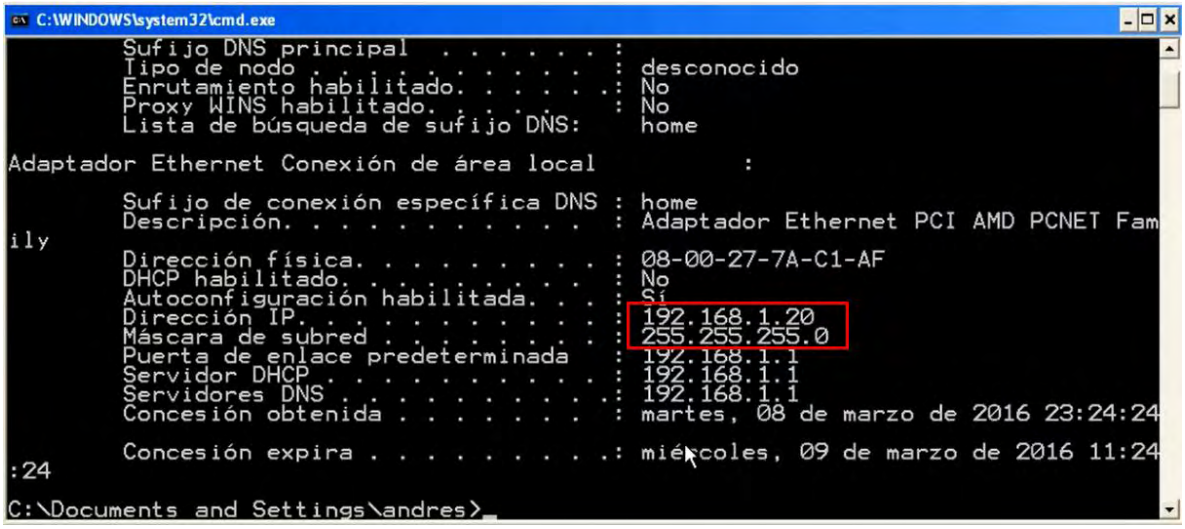


5. INSTALACIÓN DE CLIENTES Y PRUEBA DE COMUNICACIÓN

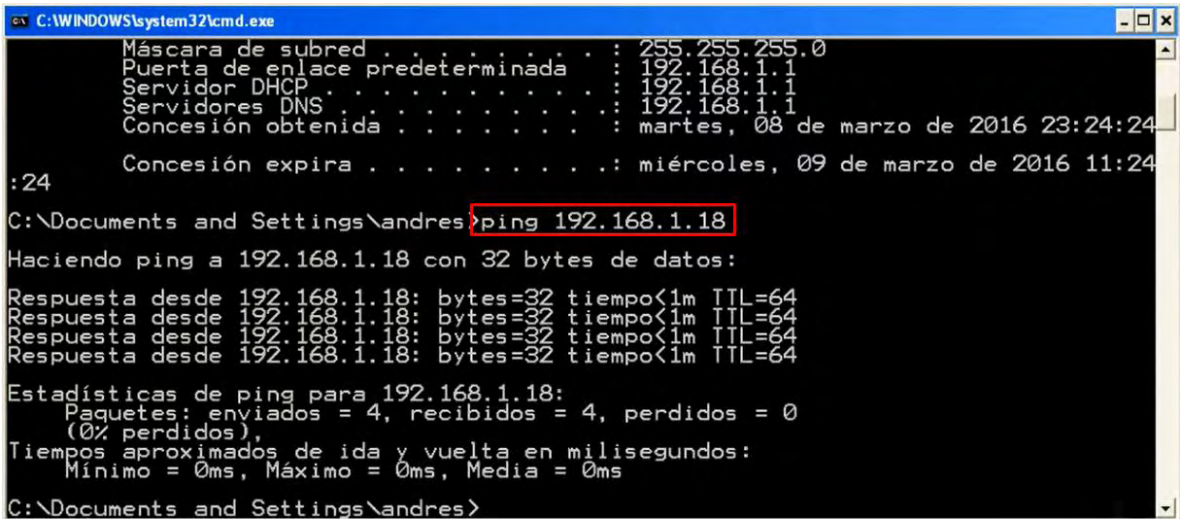
Para hacer la prueba del servidor chat con los clientes, en primer lugar, se cambia de máquina virtual, en este caso se abre una maquina Windows xp.



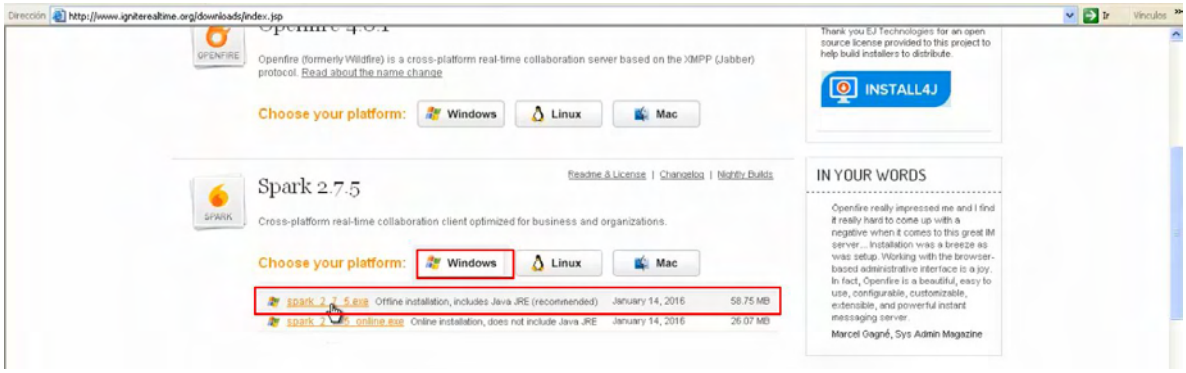
Una vez dentro de la máquina, se abre una consola y se coloca el comando **ipconfig /all** con el cual se verifica la dirección ip, la cual debe estar en el rango ip del servidor.



Posteriormente se realiza un ping al servidor chat OPENFIRE para verificar si hay conexión.



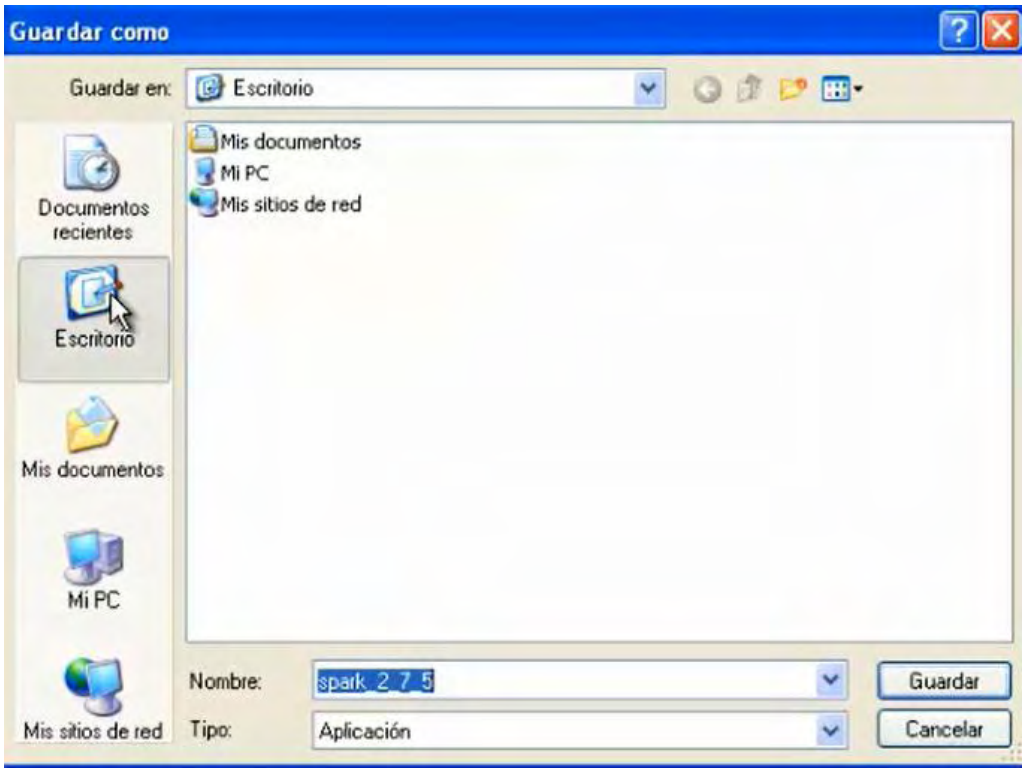
Se abre un navegador y se debe ubicar en la página de descarga de la aplicación de clientes para Windows para el servidor chat.


Openfire (formerly Wildfire) is a cross-platform real-time collaboration server based on the XMPP (Jabber) protocol. Read about the name change
Choose your platform:
Windows
Linux
Mac
INSTALL4J
Spark 2.7.5
Readme & License | Changelog | Nightly Builds
Cross-platform real-time collaboration client optimized for business and organizations.
Choose your platform:
Windows
Linux
Mac
spark_2_7_5.exe Offline installation, includes Java JRE (recommended) January 14, 2016 58.75 MB
spark_2_7_5_online.exe Online installation, does not include Java JRE January 14, 2016 26.07 MB
IN YOUR WORDS
Openfire really impressed me and I find it really hard to come up with a negative when it comes to this great IM server... Installation was a breeze as was setup. Working with the browser-based administrative interface is a joy. In fact, Openfire is a beautiful, easy to use, configurable, customizable, extensible, and powerful instant messaging server.
Marcel Gagné, Sys Admin Magazine

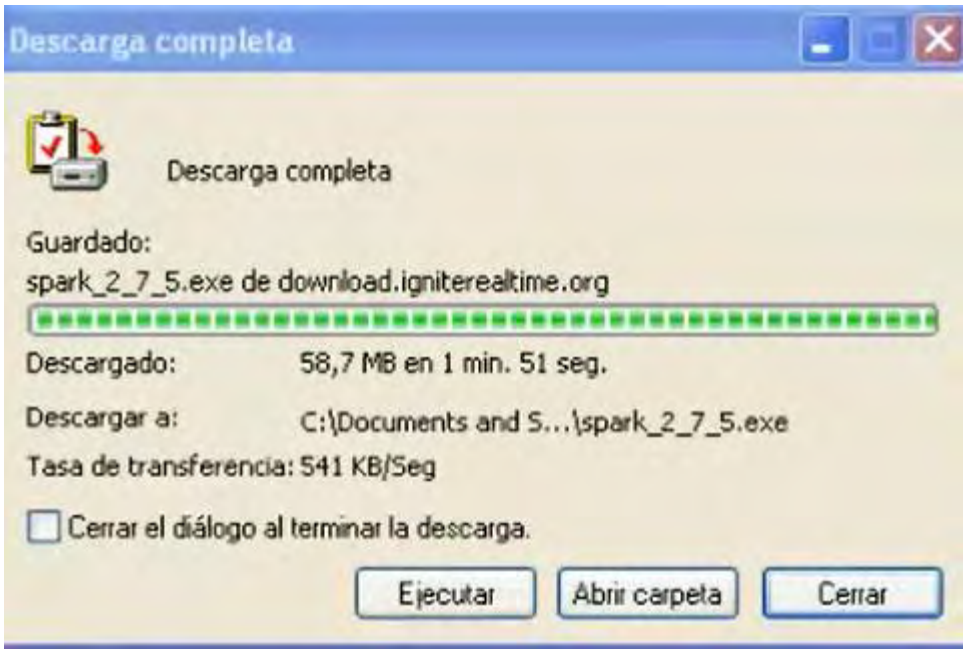
Se guarda.


Descarga de archivo - Advertencia de seguridad
¿Desea ejecutar o guardar este archivo?
Nombre: spark_2_7_5.exe
Tipo: Aplicación, 58,7 MB
De: download.igniterealtime.org
Ejecutar
Guardar
Cancelar
Los archivos procedentes de Internet pueden ser útiles, pero este tipo de archivo puede dañar potencialmente su equipo. Si no confía en el origen, no ejecute ni guarde este software. ¿Cuál es el riesgo?

Se guarda en **Escritorio**.



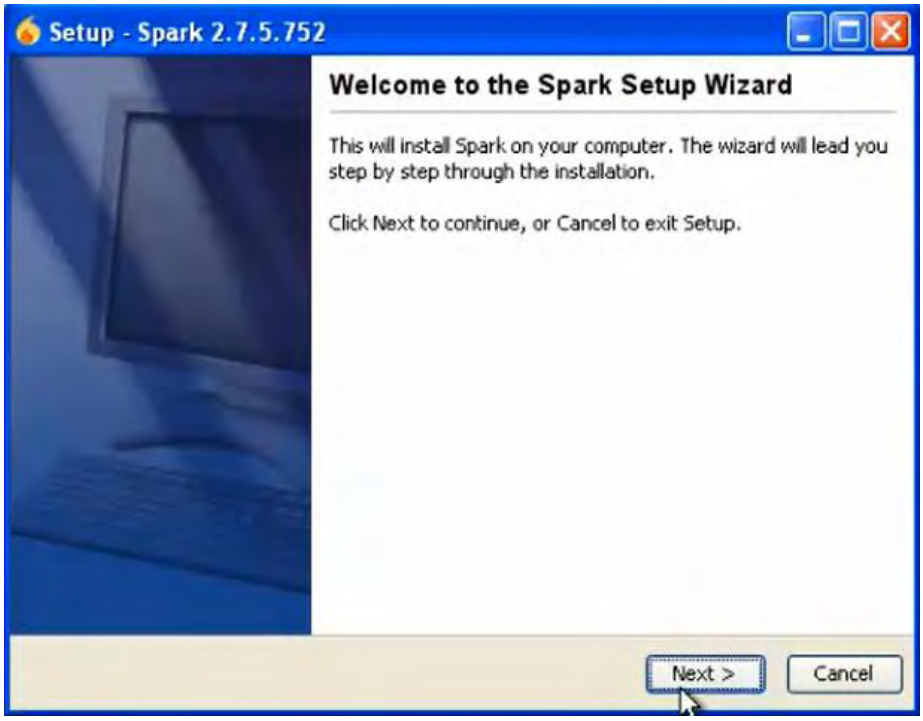
Esperar la descarga y dar en **Ejecutar**.



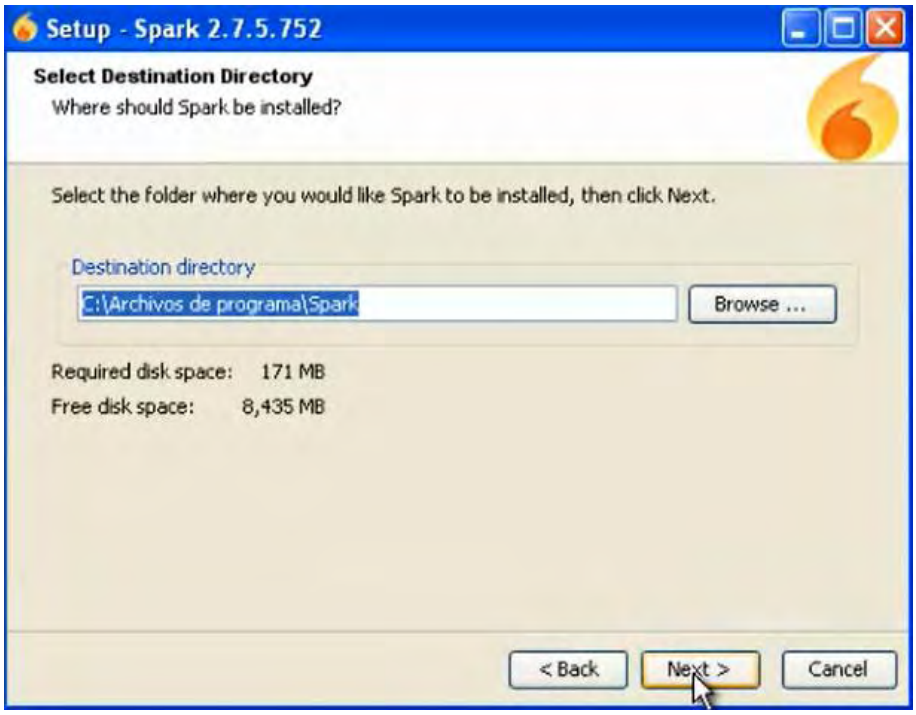
Aparecerá la siguiente ventana.



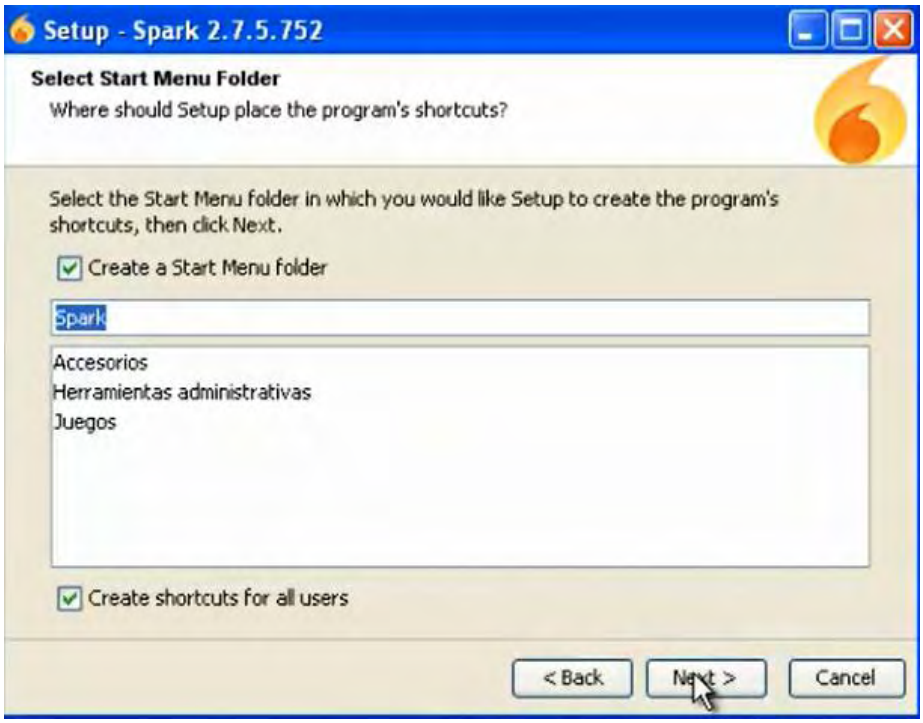
Luego la siguiente, dar clic en **Next**.



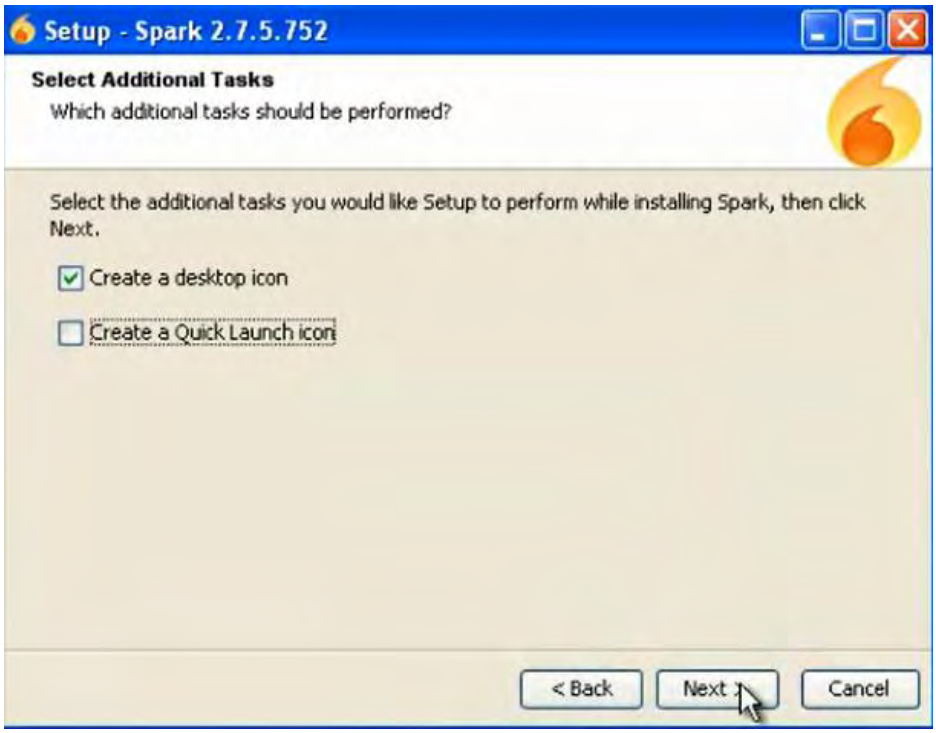
En la siguiente, nuevamente dar clic en **Next**.



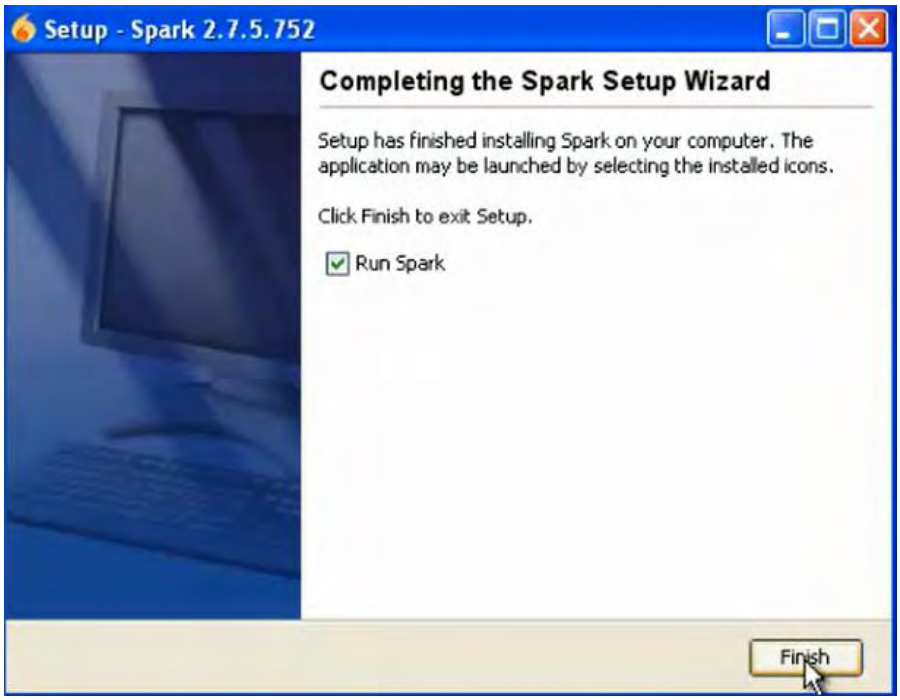
De igual manera, a continuación, dar clic en **Next**.



De igual manera, se dar clic en **Next**.



Por último, dar clic en **Finish**.



Al terminar la instalación del cliente, aparecerá la ventana de autenticación donde se coloca el **Nombre de usuario**, la **Contraseña** y la dirección ip del **Servidor**. El *Nombre de usuario* y la *Contraseña* son las que se registrarón previamente en el servidor. Luego de ingresar las credenciales aparecerá una ventana donde muestra que el usuario está en línea.





De igual manera, en la maquina física se instala y se coloca las credenciales de un cliente creado en el servidor. Una vez autenticado aparecerá el usuario en línea.


Spark
Spark Instant Messenger
Nombre de usuario
andres
Contraseña
Servidor
192.168.1.18
Guardar contraseña
Login automático
Login as invisible
Cuentas
Avanzado
Login


Spark
Spark Contactos Acciones Ayuda
andres
En línea
Contactos
Conferencias
Buscar otras personas en el servidor.

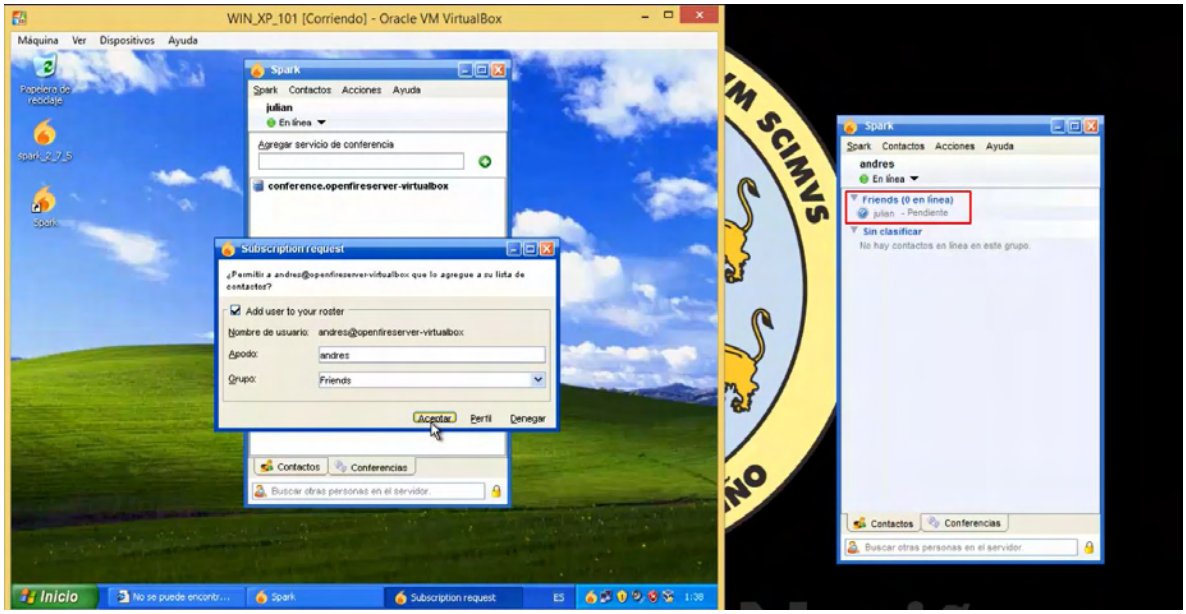
Luego de instalar e ingresar las credenciales en cada una de las maquinas, en uno de los clientes en este caso en el usuario **Andres** se agrega al usuario **Julian**, se da clic en el botón **Contactos** y se elige la opción **Agregar contacto**.



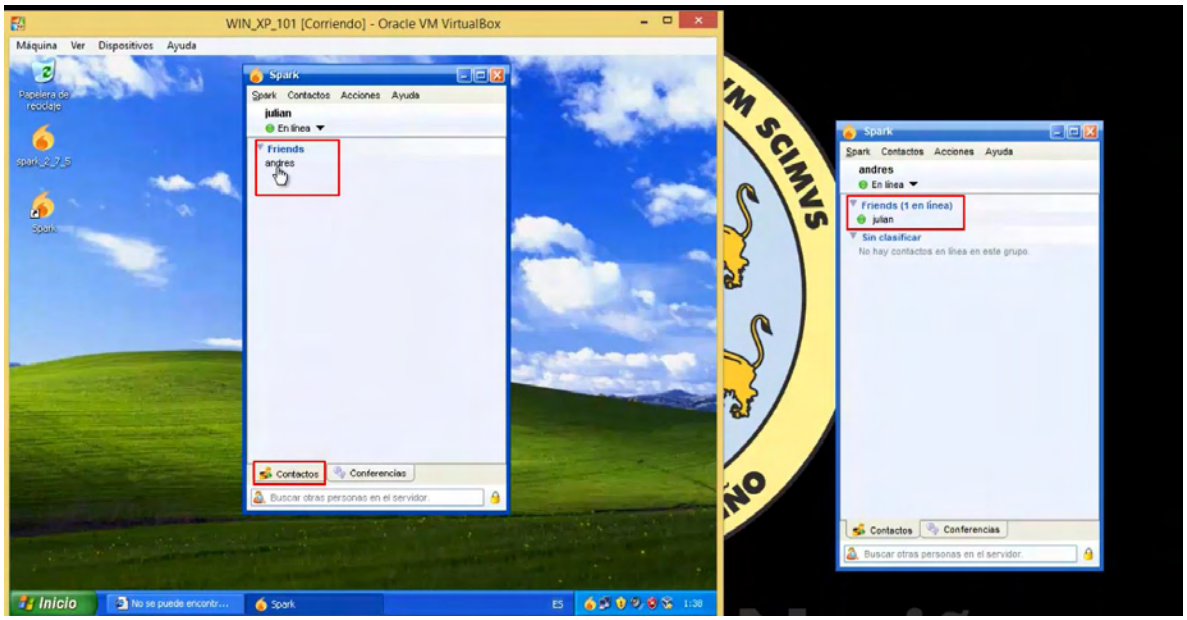
Aparecerá una ventana donde se coloca el *Nombre de usuario* que se va a agregar, si tiene un **Apodo** se coloca y se escoge el grupo.



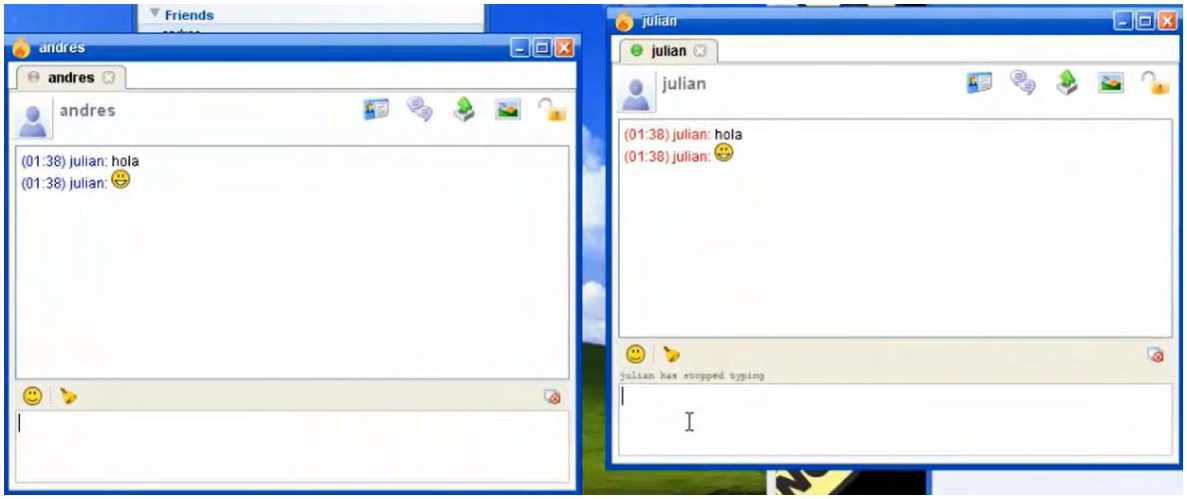
Inmediatamente llega la solicitud al usuario **Julian** en donde se la da clic en **Aceptar**.



Una vez aceptada la solicitud el usuario **Andres**, aparecerá en los contactos del usuario **Julian** y viceversa.



Por último, una vez realizado lo anterior los usuarios podrán comunicarse vía chat.



Anexo J. Instalación y configuración de servidor de correo postfix.

ÍNDICE

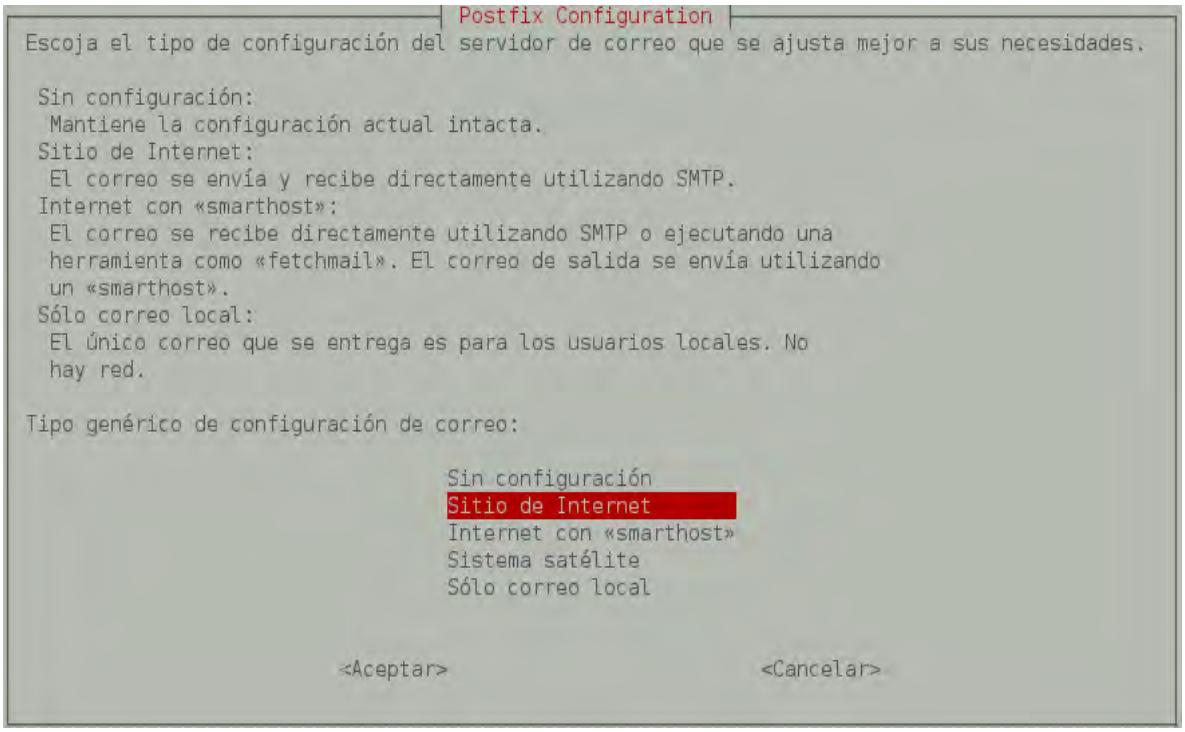
Pág.

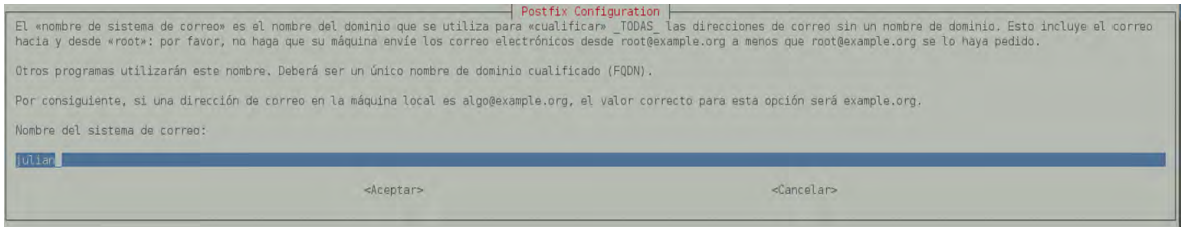
1. INSTALACION Y CONFIGURACION DE SERVIDOR DE CORREO POSTFIX 401
1.1 AUTENTICACIÓN 402
1.2 CERTIFICACIÓN 403
1.3 FUNCIONAMIENTO 403
2. CONFIGURACION DE ALERTAS POR EMAIL CON NAGIOS 405
3. CONFIGURACION DE ALERTAS POR EMAIL CON CHECK_MK 411

1. INSTALACION SERVIDOR DE CORREO POSTFIX

Nota: Este es un requisito previo para poder generar notificaciones a través de correo electrónico con Nagios o Check_mk.

apt-get update
apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules





Luego se edita el fichero /etc/postfix/main.cf

```
nano /etc/postfix/main.cf
```

Se debe comentar la siguiente linea *myorigin = /etc/mailname*

```
#myorigin = /etc/mailname
```

Dentro del mismo archivo se añade las siguientes líneas al final del archivo:

```
relayhost = [smtp.gmail.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
smtp_use_tls = yes
smtp_tls_CAfile = /etc/postfix/cacert.pem
```

Se comenta la línea donde se encuentra “relayhost =” al inicio del archivo para que no quede duplicado.

En resumen, se le dice a postfix que utilice relayhost para conectarse al servidor de Gmail, que utilice smtp_sasl_password_maps para extraer los datos de conexión SASL y que utilice smtp_tls_CAfile como certificado para la conexión segura.

1.1 AUTENTICACIÓN

Se debe crear el archivo /etc/postfix/sasl/passwd con el siguiente contenido:

```
nano /etc/postfix/sasl/passwd
```

```
[smtp.gmail.com]:587 [CUENTA]@gmail.com:[CONTRASEÑA]
```

Donde **[CUENTA]** es la cuenta de correo que va a enviar las notificaciones.
Y **[CONTRASEÑA]** es la contraseña del correo que va a enviar las notificaciones.

Y se protege adecuadamente con:

```
chmod 600 /etc/postfix/sasl/passwd
```

Seguidamente, hay que transformar el archivo a un fichero indexado de tipo hash mediante la instrucción:

```
postmap /etc/postfix/sasl/passwd
```

Lo que creará el fichero passwd.db en /etc/postfix/sasl/

```
cd /etc/postfix/sasl/
ls
```

Mostrará los siguientes archivos:

```
passwd          passwd.db
```

1.2 CERTIFICACIÓN

Se debe tener instalados los certificados SSL de las autoridades certificadoras, esto ya fue instalado en la instalación inicial del servidor de correo POSTFIX. Con el siguiente comando: “apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules”.
Para añadir la autoridad certificadora Equifax (la que certifica correos de Gmail) al fichero de certificados que utilizará postfix, se ejecuta el siguiente comando en una consola de root:

```
cat /etc/ssl/certs/Equifax_Secure_CA.pem > /etc/postfix/cacert.pem
```

1.3 FUNCIONAMIENTO

Finalmente, se reinicia postfix para aplicar los cambios.

```
/etc/init.d/postfix restart
```

Se comprueba el funcionamiento por consola. Se ejecuta el siguiente comando para monitorear el comportamiento del correo (como root):

```
tail -f /var/log/mail.log
```

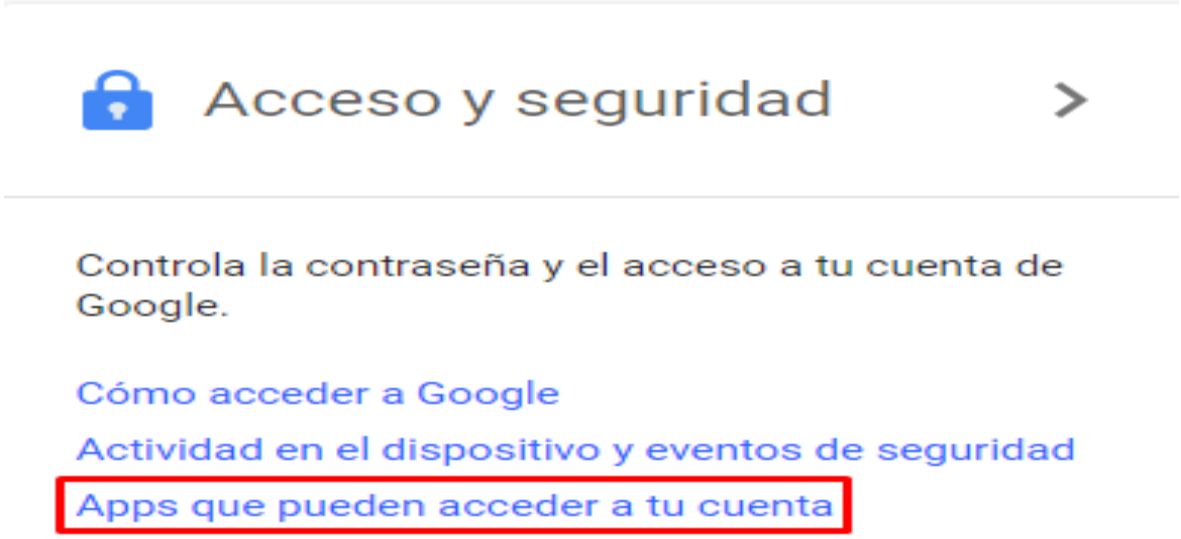
Otra opción de comprobar el funcionamiento es enviando un correo de prueba.

```
echo "Probando Postfix" | mail -s "Prueba Postfix" [CUENTA]@gmail.com
```

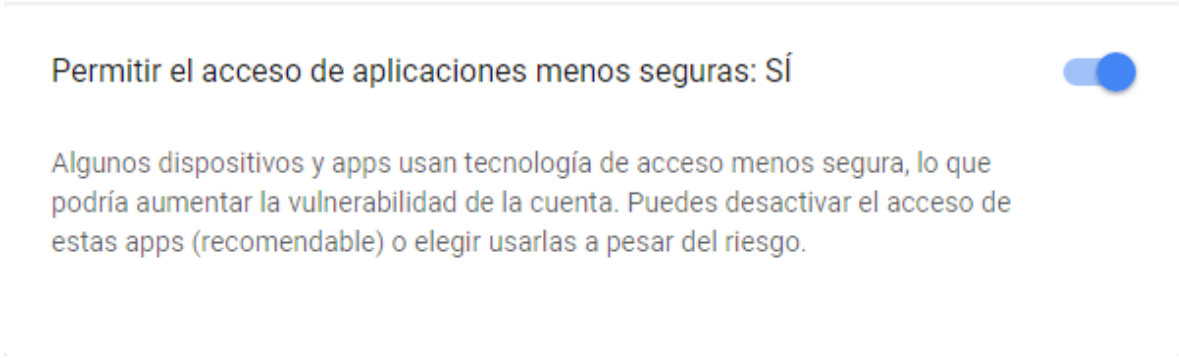
Para recibir las notificaciones por gmail es necesario realizar la siguiente configuracion a la cuenta de correo que va a recibirlas.
Se ingresa a gmail y se elige la opción mi cuenta.



En la opción Acceso y seguridad se elige Apps que pueden acceder a tu cuenta.



Se activa la opción de permitir el acceso de aplicaciones menos seguras.
Así ya se podrá recibir emails desde la suite de monitoreo.



2. CONFIGURACIÓN DE ALERTAS POR EMAIL CON NAGIOS

Se definen los contactos de email donde se recibirán las notificaciones mediante Nagios. Ingresando al siguiente fichero:

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

En email se ingresan los contactos. Quedará de la siguiente manera:

```
##############################################################################
#
# CONTACTS
#
##############################################################################

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

define contact{
        contact_name            nagiosadmin             ; Short name of user
        use                     generic-contact         ; Inherit default values from
generic-contact template        (defined above)
        alias                   Nagios Admin            ; Full name of user

        email                   nagioselectromillonaria@gmail.com   ; <<*****
CHANGE THIS TO YOUR EMAIL ADDRESS ******
        }

##############################################################################
##############################################################################
```

```
##############################################################################
```

NOTA: Si se desea colocar más contactos se ingresan separados con comas (,). Además, solo se pueden ingresar emails de servidor Gmail, debido a que el servidor de correo POSTFIX fue configurado para este tipo de emails.

Se edita el fichero commands,cfg ubicado en la ruta:

```
/usr/local/nagios/etc/objects/commands.cfg
```

Se editan los siguientes parámetros: 'notify-host-by-email' y 'notify-service-by-email' en estos parámetros se debe sustituir:

/usr/bin/ por /usr/bin/mailx

Quedando de la siguiente manera:

```
# 'notify-host-by-email' command definition
define command{
        command_name    notify-host-by-email
        command_line    /usr/bin/mailx "%b" "***** Nagios *****\n\nNotification Type:
$NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddre$
        }

# 'notify-service-by-email' command definition
define command{
        command_name    notify-service-by-email
        command_line    /usr/bin/mailx "%b" "***** Nagios *****\n\nNotification Type:
$NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTNAME$\$
        }
```

Se ingresa al siguiente fichero para verificar que estén activas las notificaciones.

```
/usr/local/nagios/etc/nagios.cfg
```

Se verifica que se encuentren activas así: enable_notifications=1

```
# NOTIFICATIONS OPTION
# This determines whether or not Nagios will sent out any host or
# service notifications when it is initially (re)started.
# Values: 1 = enable notifications, 0 = disable notifications
```

```
enable_notifications=1
```

Luego se procede a reiniciar nagios para guardar las modificaciones.

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

Nagios por defecto informa todos los estados de los hosts y sus servicios (Discos duros, memoria, ram, CPU, http, ftp, etc.). Cuando un host se encuentra apagado manda una notificación del tipo DOWN (d) y cuando éste vuelva a responder mandara una de Recovery (r).

En cuando a los servicios, envía notificaciones de estado Warning (“w”), Critical (c), Uknow (u) y recovery (r).

Se edita el siguiente fichero para configurar las notificaciones a nuestras necesidades.

Comprobamos que se tengan las notificaciones activadas para los host o servicios de un host (esto se hace dentro del apartado HOST ó SERVICES).

```
/usr/local/nagios/etc/objects/templates.cfg
```

Se configura las notificaciones para todos los host Linux.

```
# Linux host definition template - This is NOT a real host, just a template!

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           heck-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
                                        ; Note that the notification_period variable is being
overridden from
```

```
                                    ; the value that is inherited from the generic-host
template!
        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!
        }
```

Se configura las notificaciones para todos los host Windows.

```
# Windows host definition template - This is NOT a real host, just a template!

define host{
        name                    windows-server  ; The name of this host template
        use                     generic-host    ; Inherit default values from the generic-
host template
        check_period            24x7            ; By default, Windows servers are
monitored round the clock
        check_interval          5               ; Actively check the server every 5 minutes
        retry_interval          1               ; Schedule host check retries at 1 minute
intervals
        max_check_attempts      10              ; Check each server 10 times (max)
        check_command           check-host-alive        ; Default command to check if
servers are "alive"
        notification_period     24x7            ; Send notification out at any time - day or
night
        notification_interval   30              ; Resend notifications every 30 minutes
        notification_options    d,r             ; Only send notifications for specific host
states
        contact_groups          admins          ; Notifications get sent to the admins by
default
        hostgroups              windows-servers ; Host groups that Windows servers
should be a member of
        register                0               ; DONT REGISTER THIS - ITS JUST A
TEMPLATE
        }
```

Se configura las notificaciones para todos los servicios.

```
# Generic service definition template - This is NOT a real service, just a template!
```

```
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           0                   ; 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
        check_interval                  5               ; Check the service every 10
minutes under normal conditions
        retry_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!
        }
```

Si se desea configurar las notificaciones a un equipo en especial, se lo hace a cada máquina en el fichero de configuración en este caso servicios.cfg. Este fichero fue creado en este trabajo.

```
/usr/local/nagios/etc/objects/servicios.cfg
```

El siguiente ejemplo muestra la configuración de las notificaciones a un equipo específico.

```
#ssh

define service {
        use                             generic-service     ; Inherit default values from a
template
        host_name                       azkaban
        service_description             SSH-verifica Puerto Tiempo en 5s y Vers.
        check_command                   check_ssh!-p 5707!-t 5!-r "OpenSSH_6.6.1p1"
        notifications_enabled           1
        notification_options            w,c,r
        #notification_interval          5
        check_interval                  1
        #max_check_attempts             2
    }
```

NOTA: si se desea controlar la configuración de todos los hosts y servicios al mismo tiempo, se lo hace desde el fichero /usr/local/nagios/etc/objects/templates.cfg.

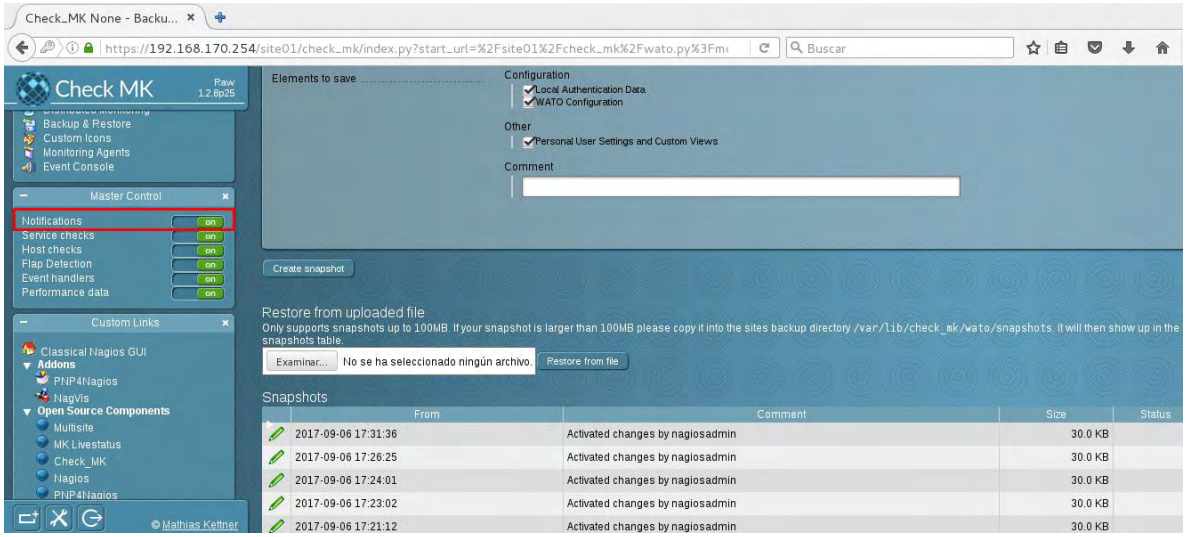
Si se tiene alguna excepción para un host o un servicio, se edita uno por uno el fichero de cada máquina a la que se desee asignar parámetros diferentes.

Luego se procede a reiniciar nagios para guardar las modificaciones.

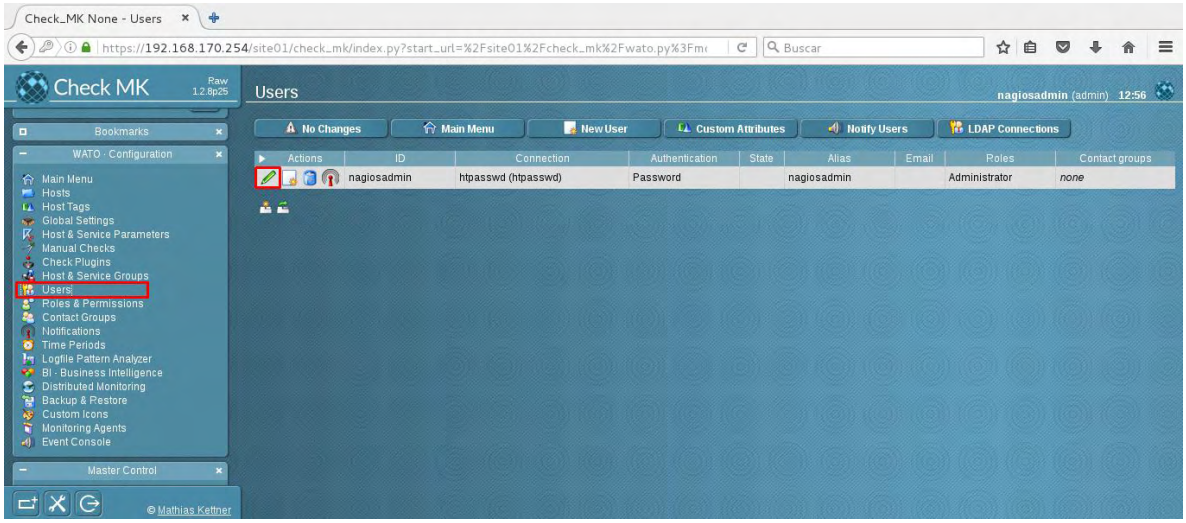
```
/etc/init.d/nagios restart
```

3. CONFIGURACIÓN DE ALERTAS POR EMAIL CON CHECK_MK

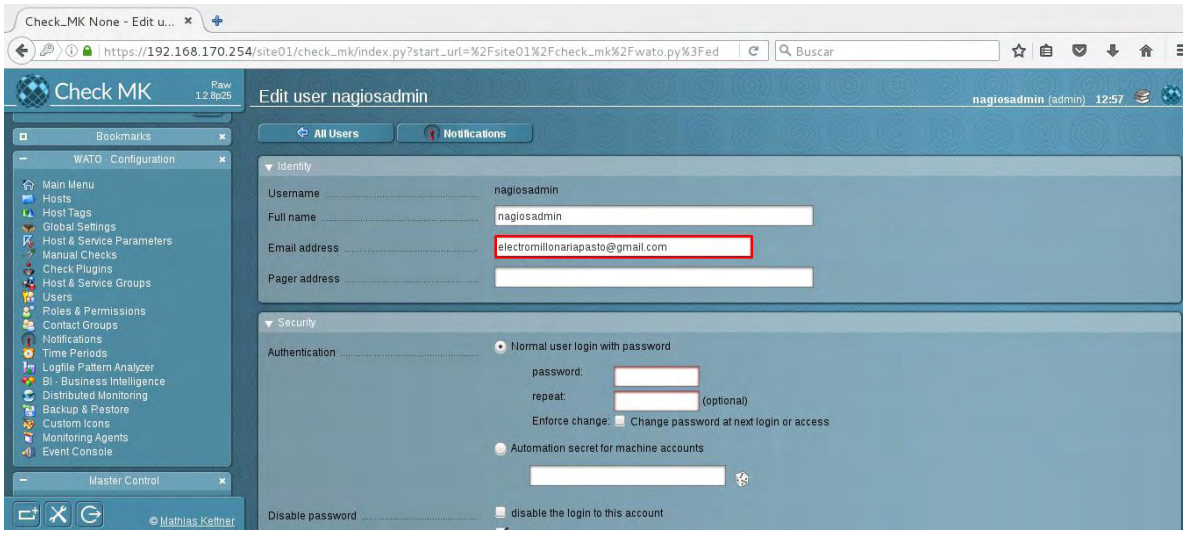
En la interface web de check_mk en la parte de opciones de configuracion se activa la opción Notifications.



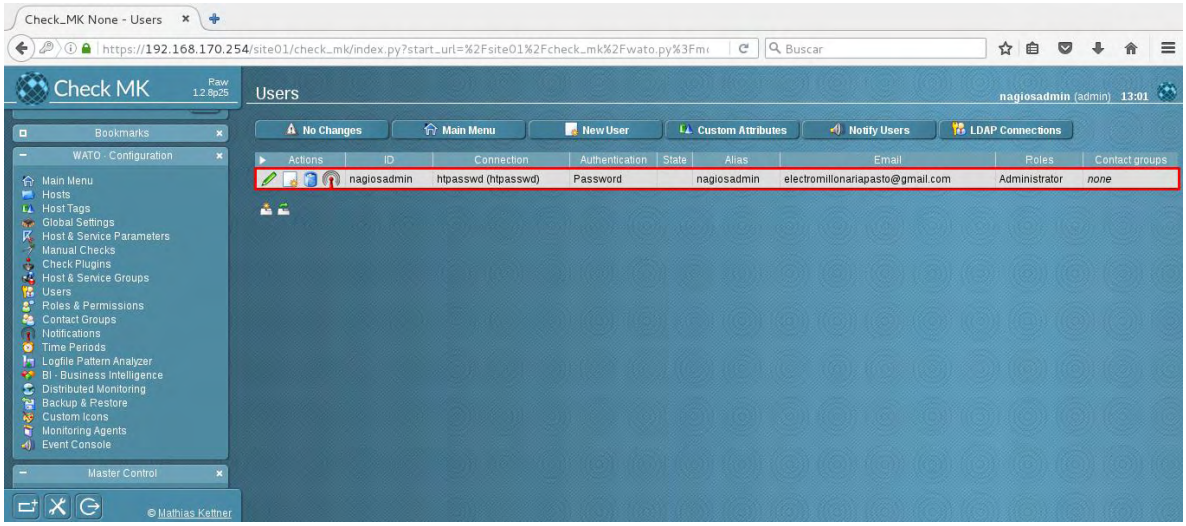
Se crean los usuarios que van a administrar la suite de monitoreo, en este caso solo se tiene el usuario nagiosadmin, se edita el perfil.



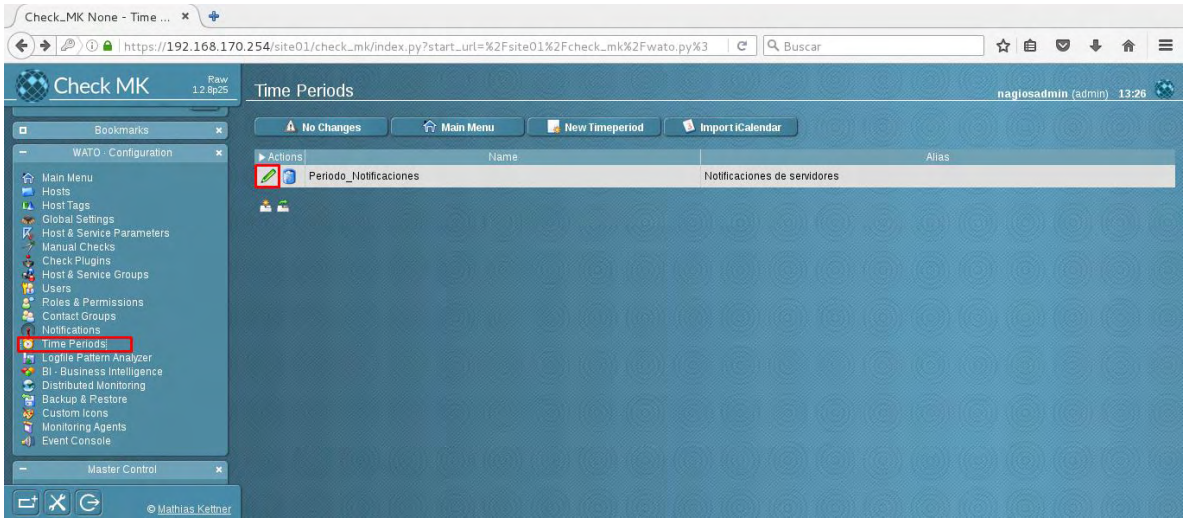
Se ingresa el email del usuario en la casilla Email address para recibir las notificaciones.



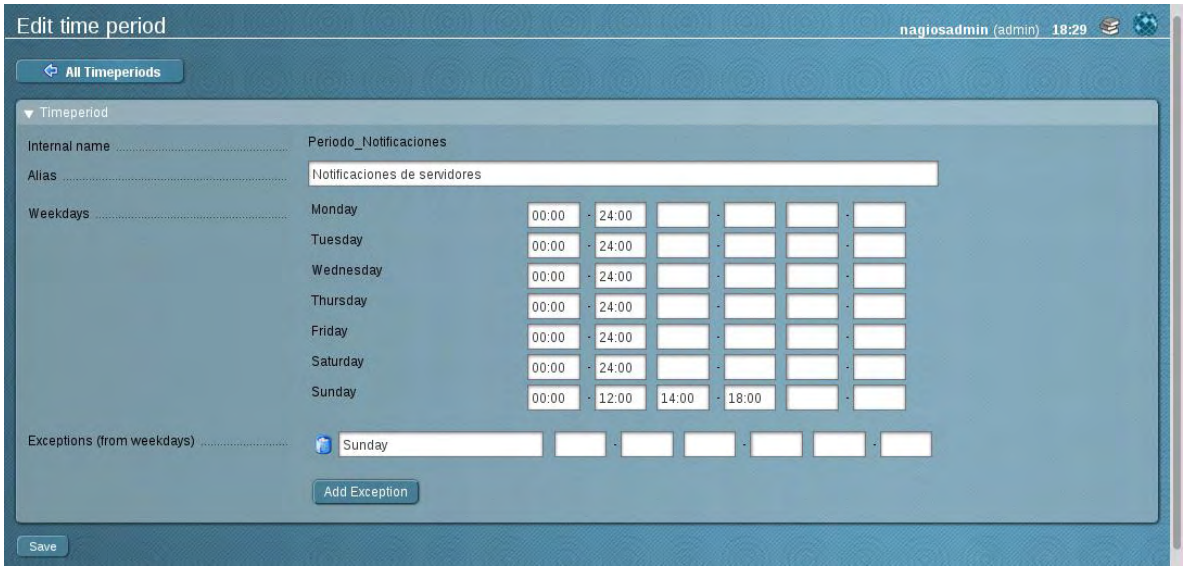
Se guardan los cambios quedando así:



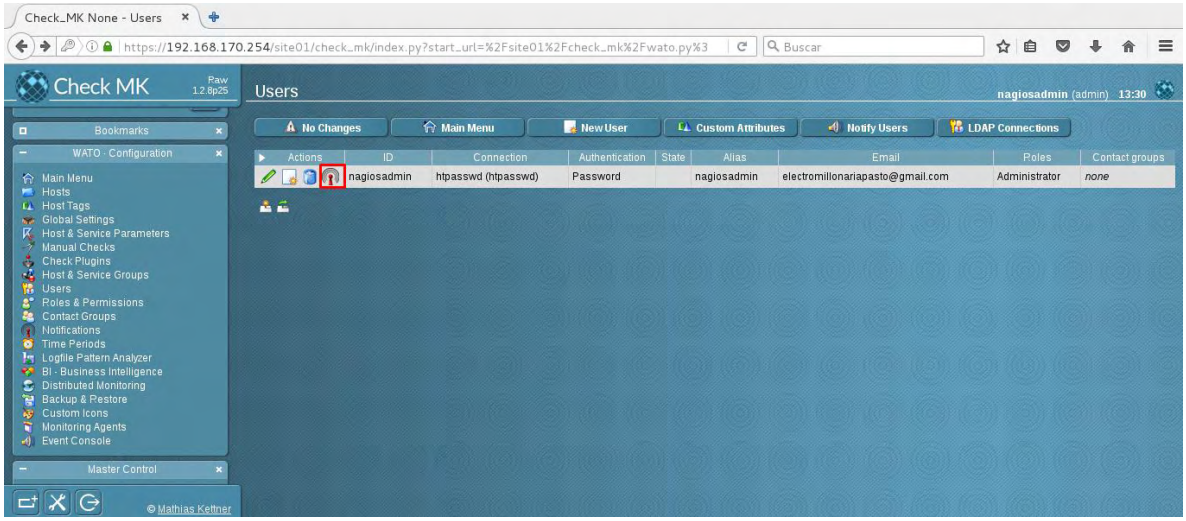
En la opción Time Periods se pueden crear periodos para las notificaciones.



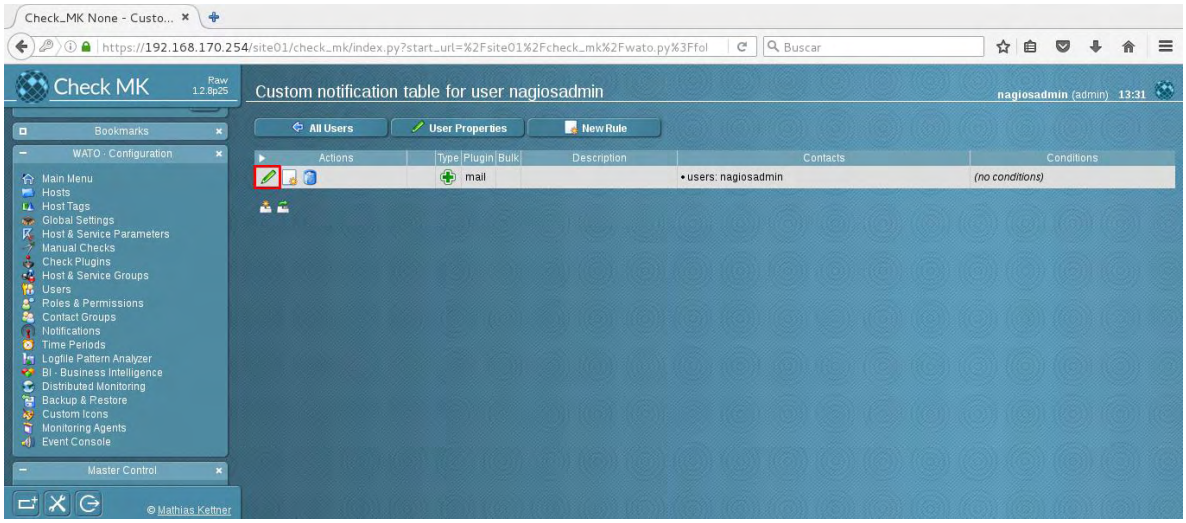
En este caso se crea un Timeperiod especificando que no se realicen notificaciones el día domingo y que sea 24X7 los demás días.



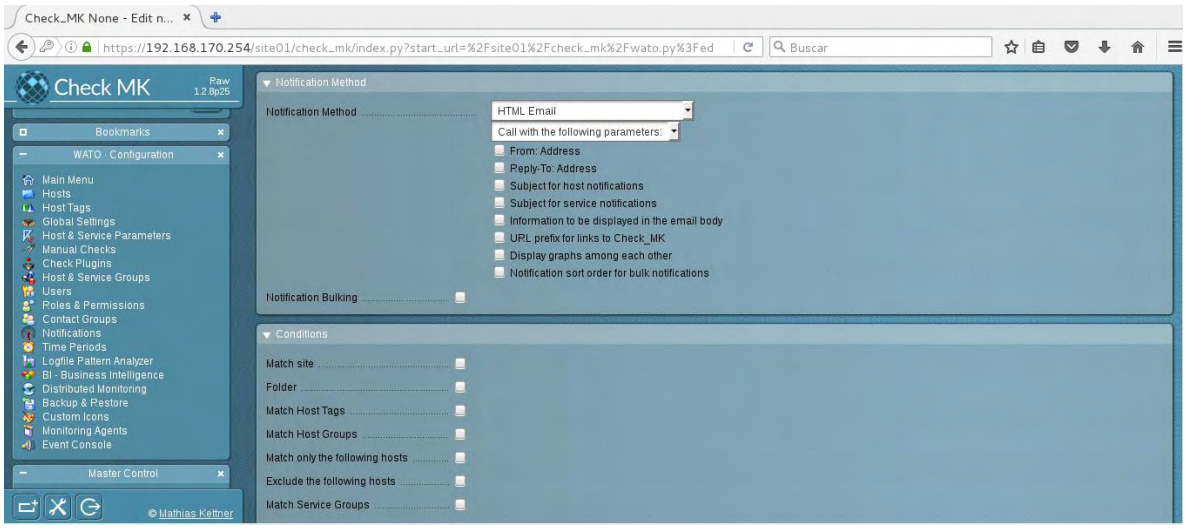
Se guardan cambios y se procede a configurar las notificaciones para este usuario.



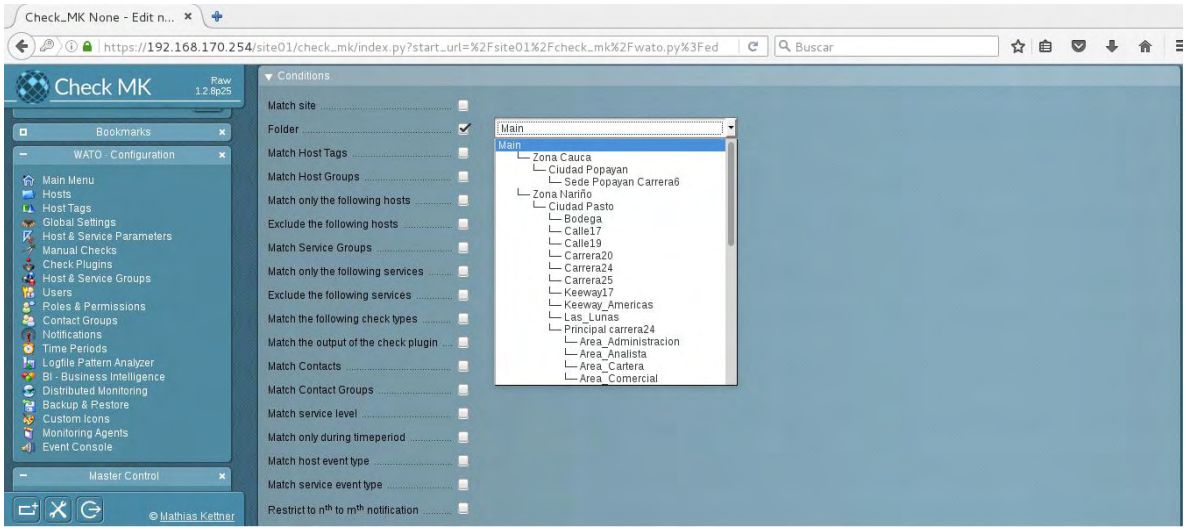
Se edita la configuración de notificaciones.



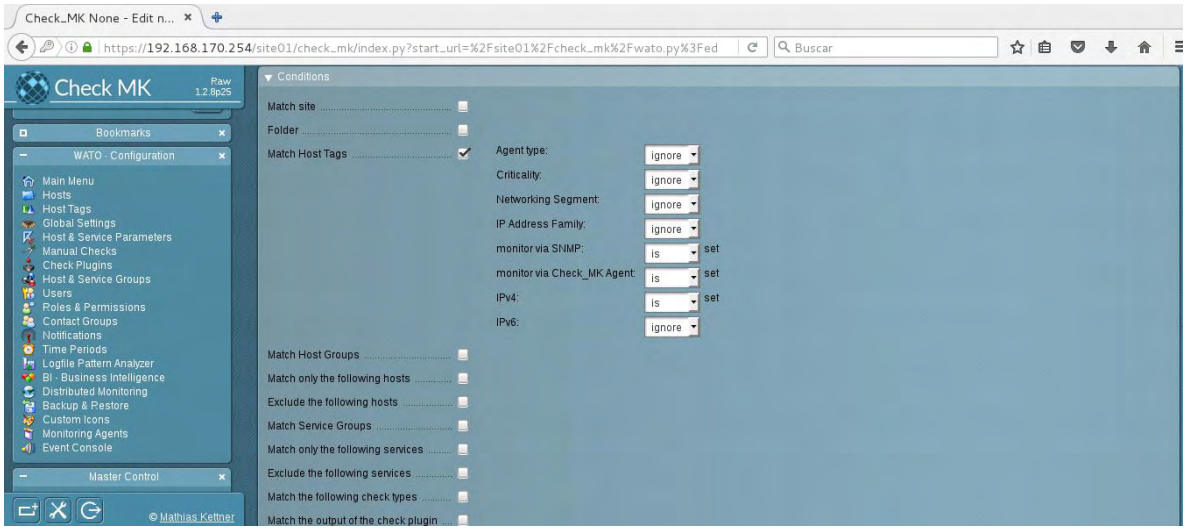
Se elige el método de envío en este caso HTML Email.



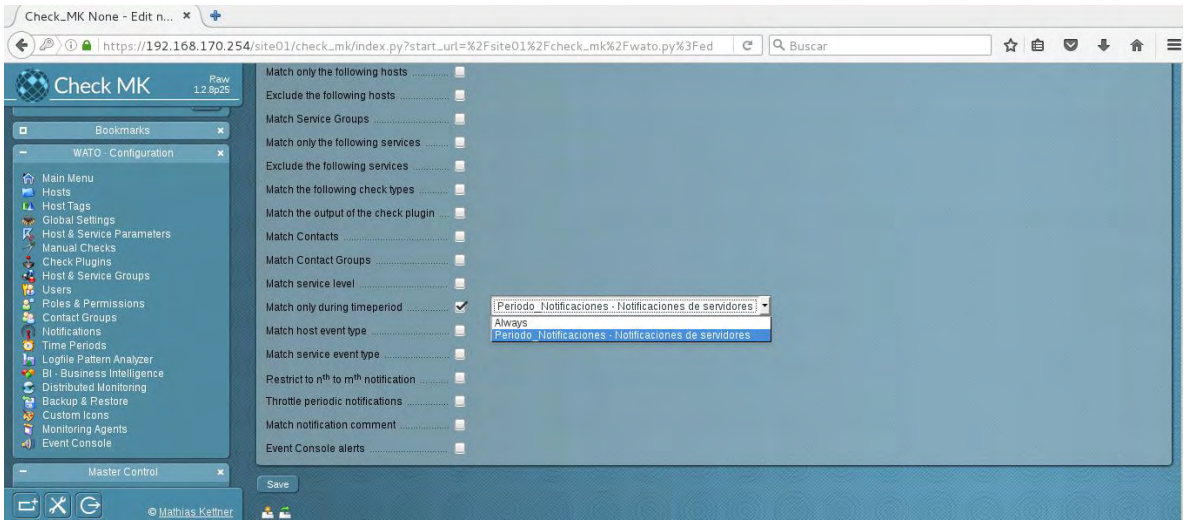
Se elige el folder donde se encuentran los equipos que van a generar las notificaciones, si se desea de todos se escoge la opción Main.



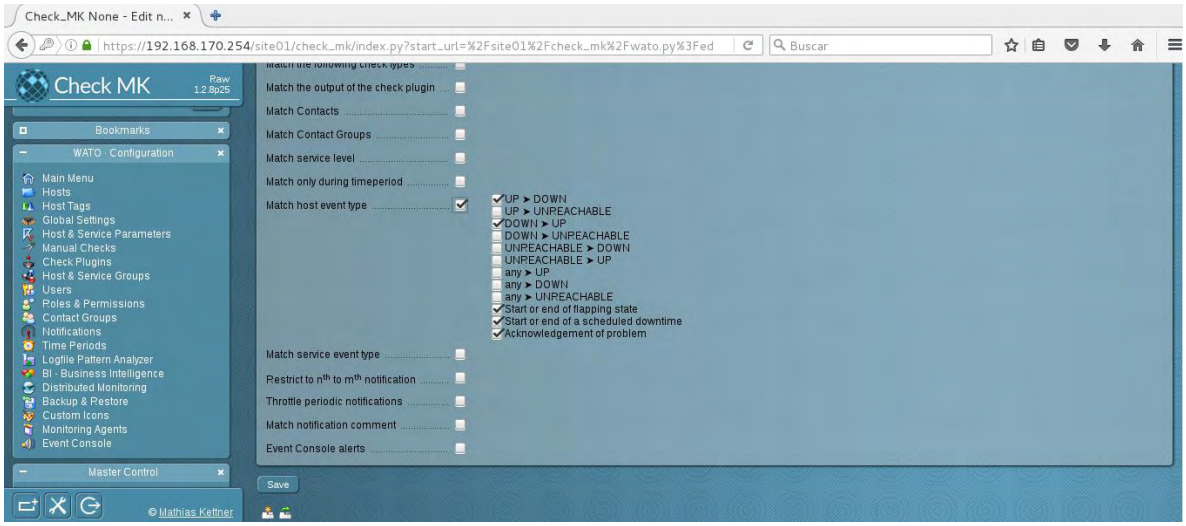
Se elige las etiquetas de monitoreo, en este trabajo son: SNMP, Check_Mk_Agent e IPv4.



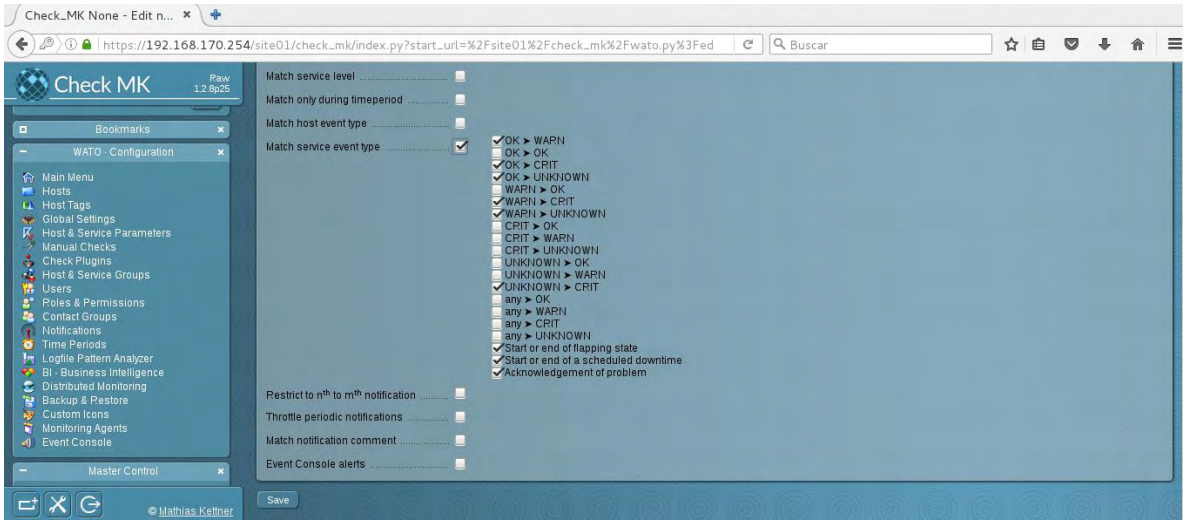
Se elige el Timeperiod creado o se deja por defecto para que sea 24X7.



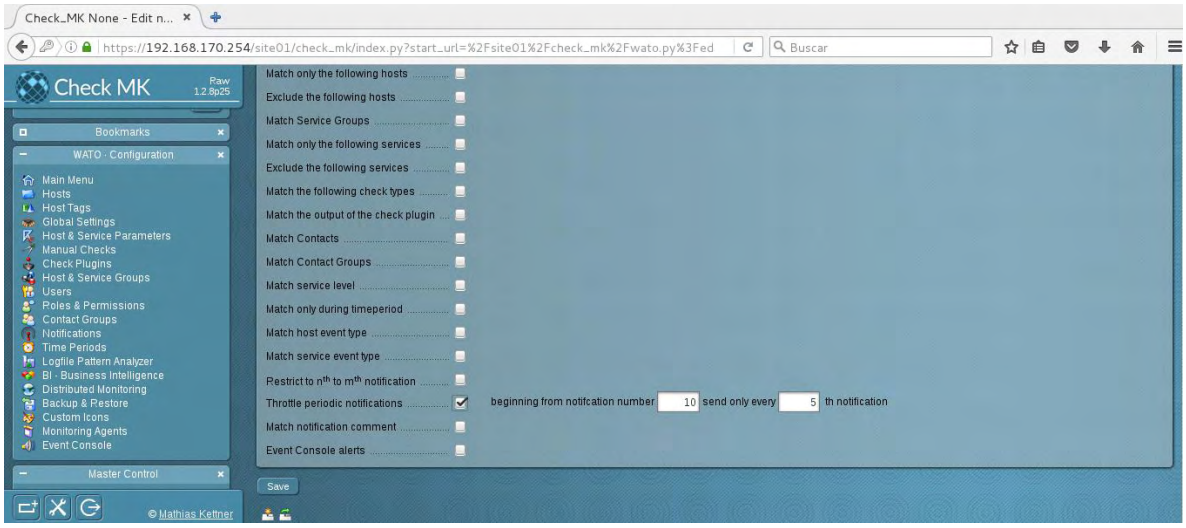
Se elige el cambio de estado en el que se desee enviar notificaciones, por ejemplo, cuanto un host pasa de UP a DOWN se enviara una notificación. Esta configuración es para el estado de los host.



Se elige el cambio de estado en el que se desee enviar notificaciones, por ejemplo, cuanto un servicio pasa de OK a CRIT se enviara una notificación. Esta configuración es para el estado de los servicios.



Se elige la frecuencia de las notificaciones y se procede a guardar los cambios.



Anexo K. Implementación de la suite de monitoreo en entorno virtual.

ÍNDICE

Pág.

1. REQUERIMIENTOS HARDWARE Y SOFTWARE DE LA MAQUINA VIRTUAL 421
1.1 REQUERIMIENTOS HARDWARE 421
1.2 REQUERIMIENTOS SOFTWARE 421
2 INSTALACIÓN DE LA SUITE DE MONITOREO 431
2.1 INSTALACIÓN Y CONFIGURACIÓN DE NAGIOS 431
2.1.1 instalación de NRPE en maquina Linux 439
2.1.2 instalación de Nrpe en servidor Nagios: 448
2.1.3 Instalación agente nsclient++ en maquina Windows. Se descargan desde el siguiente link “http://nsclient.org/download/” 451
2.2 INSTALACIÓN Y CONFIGURACIÓN DE CHECK_MK 460
2.2.1 Vinculación de Nagios con Check_MK. 472
2.2.2 Instalación de Check_mk_agent en máquina Windows 478
2.2.3 Instalación de check_mk_agent en máquina Linux. 487
2.2.4 Instalación de check_mk_agent en máquina remota Windows 488
2.3 INSTALACIÓN Y CONFIGURACIÓN DE NAGVIS 495
2.3.1 Vinculación de ingreso desde Nagvis a Nagios. 498
2.4 INSTALACIÓN Y CONFIGURACIÓN DE PNP4NAGIOS 501
2.4.1 Vinculación de PNP4Nagios con Nagios. 509
3. CONFIGURACIÓN DE SEGURIDAD EN LA SUITE DE MONITOREO 512
3.1 CONFIGURACIÓN DE SEGURIDAD CON PROTOCOLO SSL 512
3.1.1 Modificación de archivos de configuración en apache Nagios, Check_mk, Nagvis, PNP4Nagios. 514
3.2 Configuración de seguridad mediante restricción ip 522
3.2.1 Restricción de acceso por IP en apache 2.4.10: 523

3.2.2 Restricción de acceso por IP en apache 2.2.22: 527
3.2.3 Prueba de acceso y denegación por IP: 532

1. REQUERIMIENTOS HARDWARE Y SOFTWARE DE LA MAQUINA VIRTUAL

1.1 REQUERIMIENTOS HARDWARE

La implementación de la suite de monitoreo en entorno virtual se realizó sobre:

- Nombre del dispositivo: Debian_SuiteMonitoreo
- Memoria: 4 GiB
- Procesador:
- Gráficos: Intel Haswell Mobile
- Sistema Base: Debian GNU/Linux 8 (jessie) 64-bit
- Disco: 30 GB
- GNOME: Versión 3.14.1

1.2 REQUERIMIENTOS SOFTWARE

Todos los pasos en Debian requieren ejecutarse como root. Para convertirse en root simplemente ejecute:

```
Su
```

Todos los comandos a partir de este punto serán como root.

Actualizamos repositorios mediante el comando.

```
apt-get update
apt-get upgrade
```

- Instalar lamp en debian

LAMP es una combinación de sistema operativo y pila de software de código abierto. El acrónimo LAMP provino de las primeras letras de L inux, una base de datos HTTP Server, M ySQL o M ariaDB, y P HP / P erl / P ython. Este tutorial describe cómo instalarlo en una distribución de Debian Jessie, pero debería funcionar en la versión anterior de Debian y derivados.

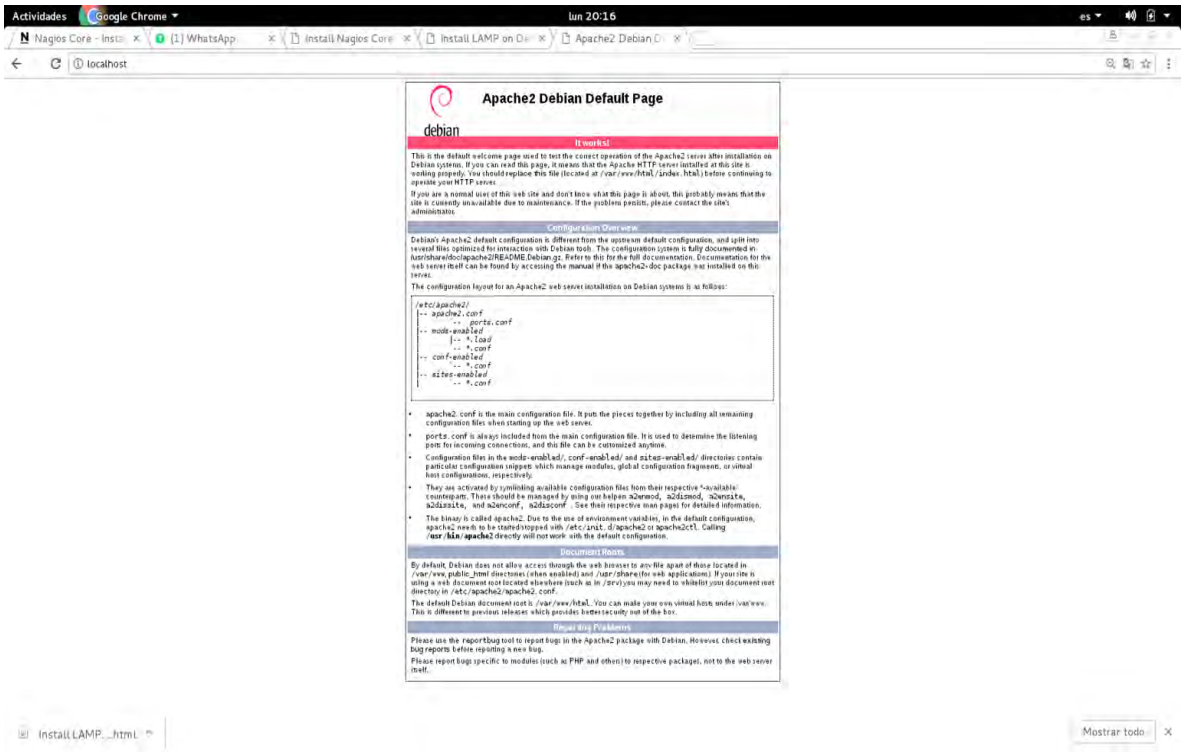
- Instalación de apache

Apache es un servidor web multiplataforma de código abierto. Proporciona una gama completa de funciones de servidor web, incluyendo CGI, SSL y dominios virtuales.

Para instalar Apache, ingrese:

```
apt-get install apache2
```

Prueba Apache:
Abra su navegador web y navege a http://localhost/ o http://server-ip-address/. Otra forma de probar apache es colocando los siguientes comandos:




```
netstat -putan | grep 80
```

Debe aparecer algo como esto:

```
tcp6       0      0 :::80                   :::*                    LISTEN      8235/apache2
udp6       0      0 :::60806                :::*                                451/rpc.statd
```

O colocando

```
ps -fea | grep apache2
```

Debe hacer algo como esto:

```
root      8235     1  0 18:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8238  8235  0 18:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8239  8235  0 18:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8240  8235  0 18:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8241  8235  0 18:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8242  8235  0 18:44 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8243  8235  0 18:44 ?        00:00:00 /usr/sbin/apache2 -k start
root      9031  2038  0 19:48 pts/0    00:00:00 grep apache2
```

- Instalación de mariadb

En los sistemas Debian, se recomienda encarecidamente instalar el paquete ' python-software-properties ' antes de dirigirse a la instalación de MariaDB desde los repositorios oficiales.

```
apt-get install python-software-properties
```

A continuación, importe y registe la clave GPG, lo que permite a apt verificar la integridad de las descargas del software.

```
apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 0xcbcb082a1bb943db
```

Al final aparecera algo como lo siguiente:

```
gpg: solicitando clave 1BB943DB de hkp servidor keyserver.ubuntu.com
gpg: clave 1BB943DB: clave pública "MariaDB Package Signing Key <package-signing-key@mariadb.org>" importada
gpg: Cantidad total procesada: 1
gpg:                importadas: 1
```

Ahora, agregue el siguiente repositorio oficial de MariaDB a su archivo sources.list, usando el siguiente comando.
El siguiente comando para debian 7 wheezy

```
add-apt-repository 'deb http://mariadb.biz.net.id/repo/10.1/debian wheezy main'
```

El siguiente comando para debian 8 jessie

```
add-apt-repository 'deb http://mariadb.biz.net.id/repo/10.1/debian jessie main'
```

Si agrega un error de lanzamiento de repositorio como " add-apt-repository: command not found ", debe instalar 'software-properties-common' como se muestra

a continuación.

```
apt-get install software-properties-common
```

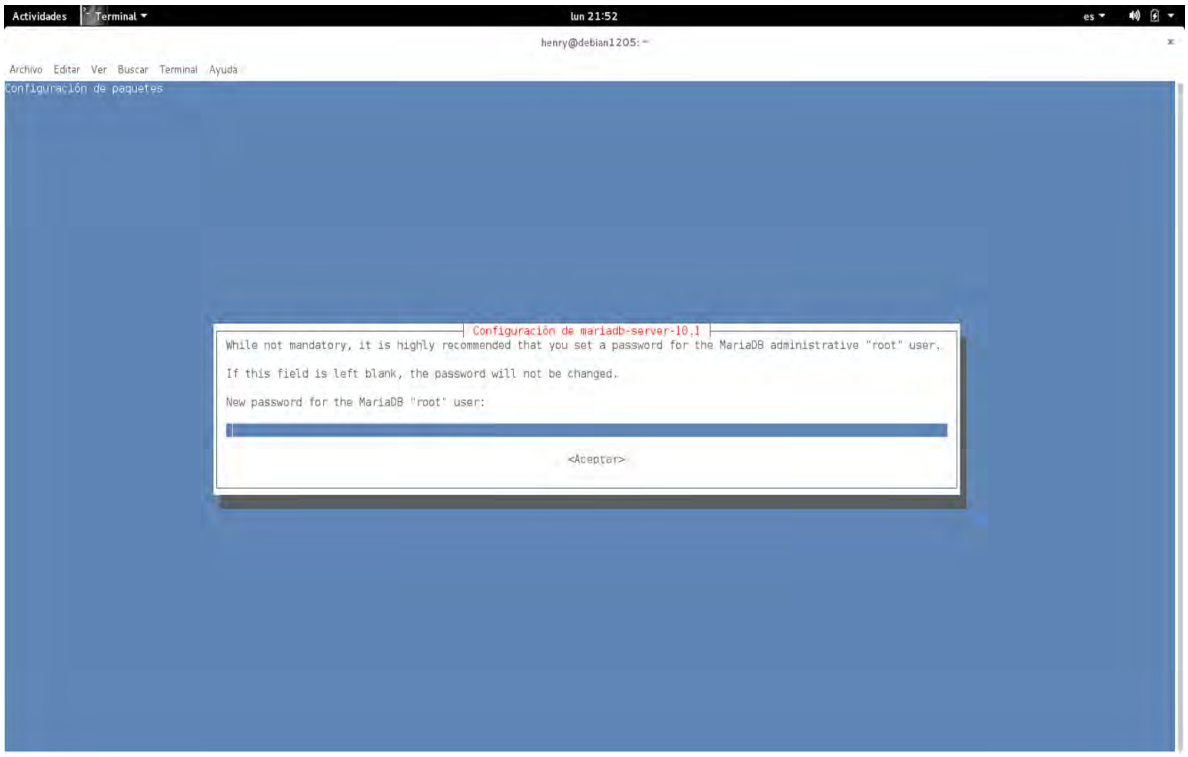
Actualice la lista de paquetes disponibles en el sistema.

```
apt-get update
```

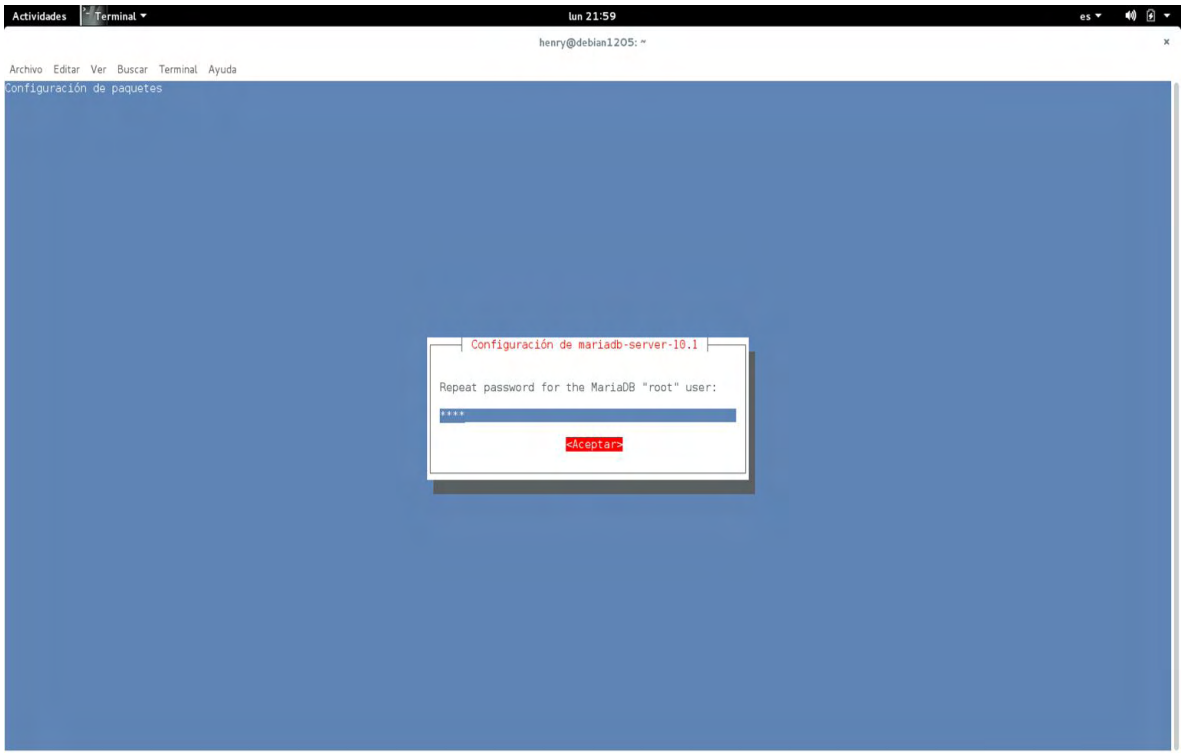
Por último, instale MariaDB Server y Client, utilizando los siguientes comandos.

```
apt-get install mariadb-server mariadb-client
```

Aparecerá una ventana en donde debemos colocar el password “root” user para MariaDB.



Luego, aparecerá otra pantalla donde confirmamos la contraseña



Si la instalación se realiza sin problemas, compruebe la versión de MariaDB instalada.

```
mysql –V
```

Debe aparecer algo como lo siguiente:

```
mysql  Ver 15.1 Distrib 10.1.13-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2
```

Inicie sesión en MariaDB utilizando root (No recomendado), seguido de contraseña.

```
mysql -u root –p
```

Mostrara algo como lo siguiente:

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
```

```
Server version: 10.1.13-MariaDB-1~jessie mariadb.org binary distribution

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

NOTA: 'none', significa que no se ha seleccionado ninguna base de datos actualmente.

Para salir de mysql presionar.

```
CTRL+C
```

Nota importante: En Ubuntu 15.10 / 15.04, MariaDB no le pedirá que configure la contraseña del usuario root durante la instalación.

Además, no puede establecer la contraseña manualmente utilizando el siguiente comando:

```
mysql_secure_installation
```

Se lanzará el siguiente error. (¡¡OJO ESTO SOLAMENTE PARA UBUNTU!!)

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL
MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.
Enter current password for root (enter for none):
ERROR 1698 (28000): Access denied for user 'root'@'localhost'
Enter current password for root (enter for none):
```

Para corregir este error, inicie sesión en mysql sin contraseña como usuario root:

```
mysql -u root
```

A continuación, ejecute los siguientes comandos uno por uno en el prompt mysql:

```
use mysql;
```

```
update user set plugin='' where User='root';
```

```
flush privileges;
```

```
\q
```

Si no le aparece el error, obvié lo anterior y continué desde el siguiente comando.

Ahora, establezca la base de datos administrativo "root" contraseña de usuario utilizando el comando. Pulse Intro y vaya con la configuración predetermina

```
mysql_secure_installation
```

Aparecerá algo como lo siguiente.

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.
Enter current password for root (enter for none):
OK, successfully used password, moving on...
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.
Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!
By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.
```

```
Remove anonymous users? [Y/n]
 ... Success!
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.
Disallow root login remotely? [Y/n]
 ... Success!
By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.
Remove test database and access to it? [Y/n]
 - Dropping test database...
ERROR 1008 (HY000) at line 1: Can't drop database 'test'; database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!
Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.
Reload privilege tables now? [Y/n]
 ... Success!
Cleaning up...
All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.
Thanks for using MariaDB!
```

Compruebe si mariadb está funcionando o no, usando el siguiente comando:

```
service mysql status
```

Mostrará algo como lo siguiente:

En debian 7 wheezy

```
[info] /usr/bin/mysqladmin  Ver 9.1 Distrib 10.1.25-MariaDB, for debian-linux-gnu on
x86_64
Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Server version          10.1.25-MariaDB-1~wheezy
Protocol version    10
Connection          Localhost via UNIX socket
UNIX socket         /var/run/mysqld/mysqld.sock
Uptime:                 12 min 2 sec

Threads: 1  Questions: 487  Slow queries: 0  Opens: 196  Flush tables: 2  Open
```

```
tables: 27  Queries per second avg: 0.674.
```

En debian8 jessie

```
mariadb.service - MariaDB database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled)
  Drop-In: /etc/systemd/system/mariadb.service.d
           └─migrated-from-my.cnf-settings.conf
   Active: active (running) since lun 2016-04-11 11:13:16 EDT; 22min ago
 Main PID: 25965 (mysqld)
   Status: "Taking your SQL requests now..."
   CGroup: /lxc/410/system.slice/mariadb.service

abr 11 11:13:16 nagios-master mysqld[25965]: 2016-04-11 11:13:16 140007725565696 [Note] InnoDB: Dumping buffer pool(s) not yet started
abr 11 11:13:16 nagios-master mysqld[25965]: 2016-04-11 11:13:16 140008488851392 [Note] Plugin 'FEEDBACK' is disabled.
abr 11 11:13:16 nagios-master mysqld[25965]: 2016-04-11 11:13:16 140008488851392 [Note] Server socket created on IP: '127.0.0.1'.
abr 11 11:13:16 nagios-master mysqld[25965]: 2016-04-11 11:13:16 140008488851392 [Note] Reading of all Master_info entries succeded
abr 11 11:13:16 nagios-master mysqld[25965]: 2016-04-11 11:13:16 140008488851392 [Note] Added new Master_info '' to hash table
abr 11 11:13:16 nagios-master mysqld[25965]: 2016-04-11 11:13:16 140008488851392 [Note] /usr/sbin/mysqld: ready for connections.
abr 11 11:13:16 nagios-master mysqld[25965]: Version: '10.1.13-MariaDB-1~jessie'  socket: '/var/run/mysqld/mysqld.sock'  port: 3306  mariadb.org binary distribution
abr 11 11:13:16 nagios-master mysqld[26001]: Checking for corrupt, not cleanly closed and upgrade needing tables.
abr 11 11:13:16 nagios-master /etc/mysql/debian-start[26011]: Upgrading MySQL tables if necessary.
abr 11 11:13:16 nagios-master systemd[1]: Started MariaDB database server.
```

- Instalación de php

PHP (siglas en inglés recurrentes para PHP: Hypertext Preprocessor) es un lenguaje de programación de uso general de código abierto ampliamente utilizado que es especialmente adecuado para el desarrollo web y puede ser incorporado en HTML.
Instalar PHP con el siguiente comando:

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

Para probar PHP, cree un archivo de muestra "testphp.php" en la carpeta raíz del documento Apache.

```
nano /var/www/html/testphp.php
```

Adicionar las siguientes lineas:

```
<?php
phpinfo();
?>
```

Reiniciar el servicio apache2.

Para debia7 wheezy

```
service apache2 restart
```

Para debian8 jessie

```
systemctl restart apache2
```

Se ingresa a **http://server-ip-address/testphp.php**. Se mostrará todos los detalles acerca de php como la versión, fecha de compilación y comandos, etc.



Si se quiere instalar todos los módulos php a la vez, ingrese el comando **sudo apt-get install php*** y reinicie el servicio apache2. Para verificar los módulos, abra el navegador web y navegue hasta **http://server-ip-address/testphp.php** . Podrá ver todos los módulos php instalados.

2 INSTALACIÓN DE LA SUITE DE MONITOREO

2.1 INSTALACIÓN Y CONFIGURACIÓN DE NAGIOS

- Requisitos previos

Realizar estos pasos para instalar los paquetes de requisitos previos.

```
apt-get update
apt-get install -y autoconf gcc libc6 make wget unzip apache2 apache2-utils php5 libgd2-xpm-dev
```

- Descargar del paquete Nagios desde la fuente

```
cd /tmp
```

```
wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.3.2.tar.gz
```

```
tar xzf nagioscore.tar.gz
```

- Compilar

```
cd /tmp/nagioscore-nagios-4.3.2/
```

```
./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

Nos mostrara algo como lo siguiente.

```
*** Configuration summary for nagios 4.3.2 2017-05-09 ***:

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

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

Review the options above for accuracy.  If they look okay,
type 'make all' to compile the main program and CGIs.
```

```
make all
```

- Crear usuario y grupo

Esto crea el usuario y grupo nagios. El usuario www-data también se agrega al grupo nagios.

```
useradd nagios
usermod -a -G nagios www-data
```

- Instalar binarios

Este paso instala los archivos binarios, CGI y archivos HTML.

```
make install
```

- Instalar Service / Daemon

Esto instala los archivos de servicio o daemon y también los configura para que se inicien al arrancar.
===== Debian 7.x =====

```
make install-init
update-rc.d nagios defaults
```

===== Debian 8.x =====

```
make install-init
systemctl enable nagios.service
```

La información sobre los servicios de arranque y parada se explicará más adelante.

- Instalar command mode

Esto instala y configura el archivo de comandos externo.

```
make install-commandmode
```

- Instalar archivos de configuración

Esto instala los archivos de configuración * SAMPLE *. Estos son necesarios ya que Nagios necesita algunos archivos de configuración para permitir que se inicie.

```
make install-config
```

- Instalar archivos de configuración de Apache

Esto instala los archivos de configuración del servidor web Apache y configura la configuración de Apache.

```
make install-webconf
a2enmod rewrite
a2enmod cgi
```

- Configurar Firewall

Se permite el tráfico entrante del puerto 80 en el firewall local para que pueda acceder a la interfaz web Nagios Core.

```
iptables -I INPUT -p tcp --destination-port 80 -j ACCEPT
apt-get install -y iptables-persistent
```

Se debe responder sí a guardar las reglas existentes

- Crear cuenta de usuario nagiosadmin

Se debe crear una cuenta de usuario de Apache para poder iniciar sesión en Nagios.

El siguiente comando creará una cuenta de usuario llamada nagiosadmin y se le pedirá que proporcione una contraseña para la cuenta.

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

Nota: Cuando se agregue usuarios adicionales en el futuro, deberá quitar -c del comando anterior, de lo contrario reemplazará al usuario existente de nagiosadmin (y cualquier otro usuario que haya agregado).

- Iniciar Apache Web Server

===== Debian 7.x =====

Se reinicia porque ya se está ejecutando.

```
service apache2 restart
```

===== Debian 8.x =====

Se reinicia porque ya se está ejecutando.

```
systemctl restart apache2.service
```

- Iniciar Service / Daemon

Este commando inicia Nagios Core

===== Debian 7.x =====

```
service nagios start
```

===== Debian 8.x =====

```
systemctl start nagios.service
```

- Test Nagios

Nagios se está ejecutando, para confirmar esto es necesario iniciar sesión en la Interfaz Web de Nagios.

Se debe apuntar el navegador web a la dirección IP o FQDN de su servidor Nagios Core, por ejemplo:

```
http://10.25.5.143/nagios

http://core-013.domain.local/nagios
```

Se pedirá un nombre de usuario y una contraseña. El nombre de usuario es nagiosadmin (lo creo en un paso anterior) y la contraseña es la que proporciono anteriormente.

Una vez que se haya iniciado sesión, se presenta la interfaz de Nagios. Congratulations you have installed Nagios Core.

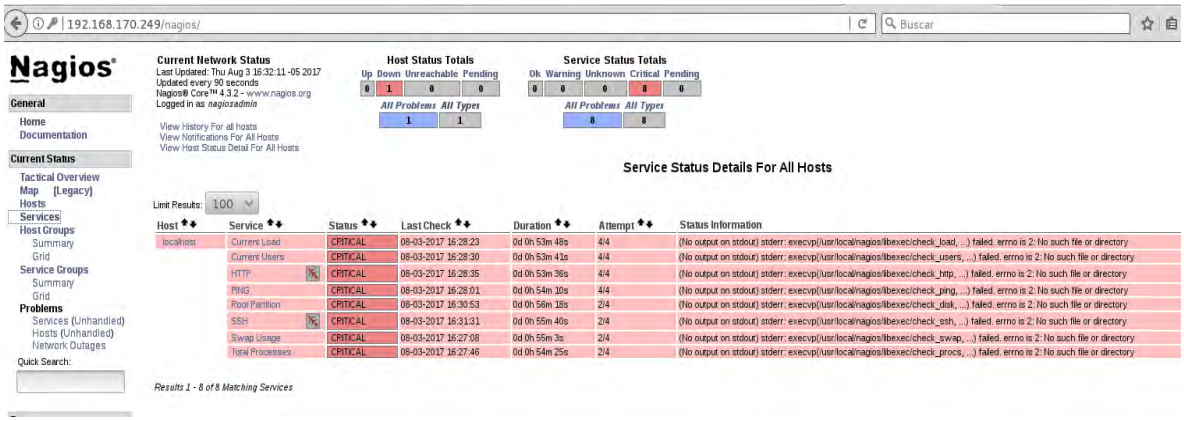
Para comprobar que la autenticación se esta realizando se puede ingresar al log de inicio de sesión de Nagios ubicado en /var/log/apache2/error.log.

```
nano /var/log/apache2/error.log
```

Mostrará algo como lo siguiente.

```
[Thu Aug 17 19:22:04.810056 2017] [mpm_prefork:notice] [pid 27257] AH00169: caught SIGTERM, shutting down
[Thu Aug 17 19:22:05.930804 2017] [mpm_prefork:notice] [pid 4493] AH00163: Apache/2.4.10 (Debian) configured -- resuming normal operations
[Thu Aug 17 19:22:05.930872 2017] [core:notice] [pid 4493] AH00094: Command line: '/usr/sbin/apache2'
```

Nota: Actualmente sólo se instalado el motor Nagios Core. Se notará algunos errores bajo los anfitriones y los servicios según las líneas de:



(No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_load, ...) failed. errno is 2: No such file or directory

Estos errores se resolverán una vez se instale Nagios Plugins, que se trata en el siguiente paso.

- Instalación de los Nagios plugins

Nagios Core necesita plugins para funcionar correctamente. Los siguientes pasos le ayudarán a instalar Nagios Plugins.

Nota: Estos pasos instalan nagios-plugins 2.2.1. Las versiones más recientes están disponibles en el futuro y se pueden utilizar las siguientes etapas de instalación. Para más información dirigirse a GitHub (https://github.com/nagios-plugins/nagios-plugins/releases), para todas las versiones disponibles.

Se debe tener en cuenta que los siguientes pasos instalan la mayoría de los

complementos que vienen en el paquete Nagios Plugins. Sin embargo, hay algunos complementos que requieren otras bibliotecas que no están incluidas en esas instrucciones. Consultar el siguiente artículo de KB para obtener instrucciones detalladas de instalación:

Documentación – Instalación de Nagios Plugin desde el origen (https://support.nagios.com/kb/article.php?id=569)

- Prerequisitos

Se debe tener instalados los siguientes paquetes.

```
apt-get install -y autoconf gcc libc6 libmcrypt-dev make libssl-dev wget bc gawk dc build-essential snmp libnet-snmp-perl gettext
```

- Descargando la fuente

```
cd /tmp
wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz
tar zxf nagios-plugins.tar.gz
```

- Compile + Install

```
cd /tmp/nagios-plugins-release-2.2.1/
./tools/setup
./configure
make
make install
```

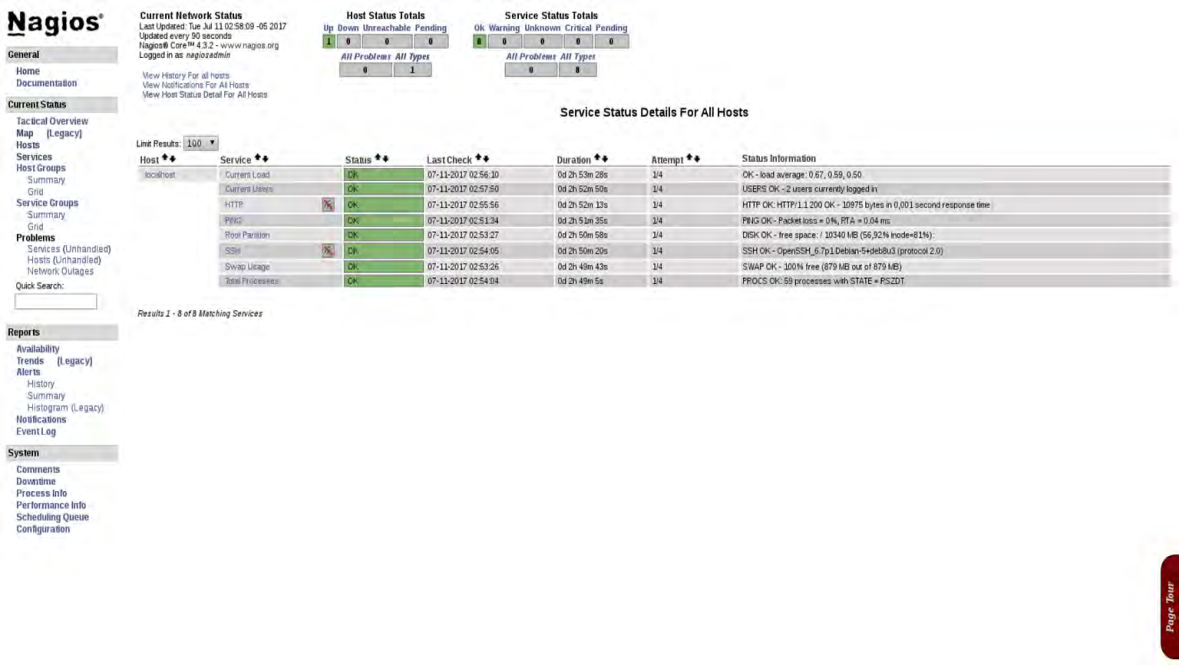
- Test plugins

Apuntar al navegador web a la dirección IP o FQDN del servidor Nagios Core, por ejemplo:

```
http://10.25.5.143/nagios

http://core-013.domain.local/nagios
```

Dirigirse a un objeto de host o servicio y "Reorganizar la siguiente comprobación" en el menú Comandos. El error anteriormente debería desaparecer y la salida correcta aparecerá en la pantalla.



- Comandos de Service / Daemon

Diferentes distribuciones de Linux tienen diferentes métodos de starting / stopping / restarting / status Nagios.
===== Debian 7.x =====

service nagios start
service nagios stop
service nagios restart
service nagios status

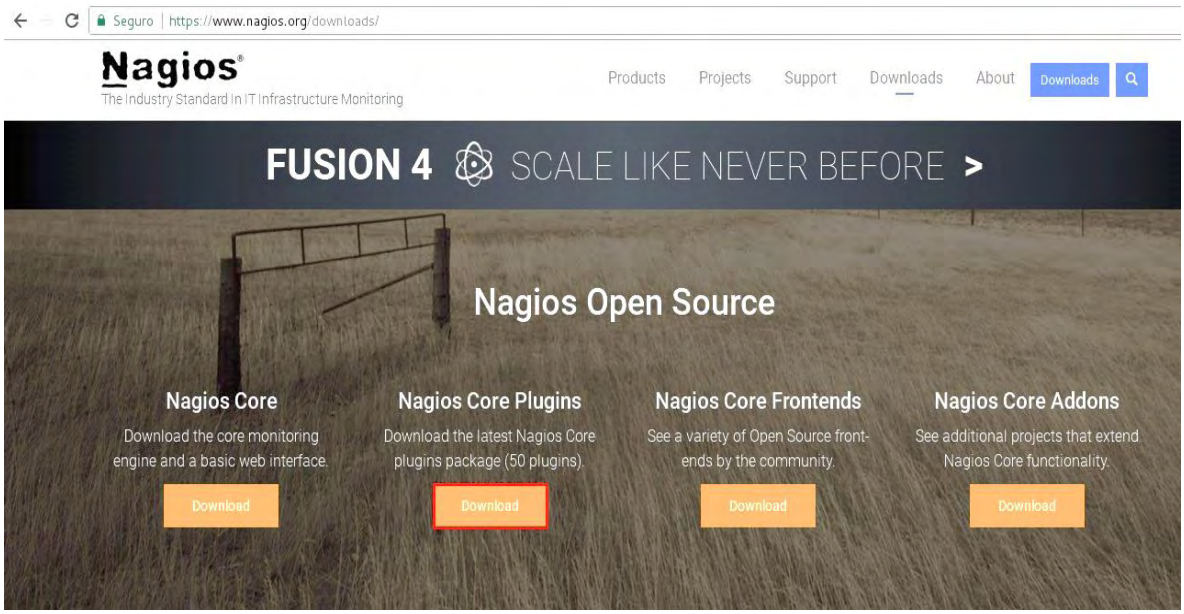
===== Debian 8.x =====

systemctl start nagios.service
systemctl stop nagios.service
systemctl restart nagios.service
systemctl status nagios.service

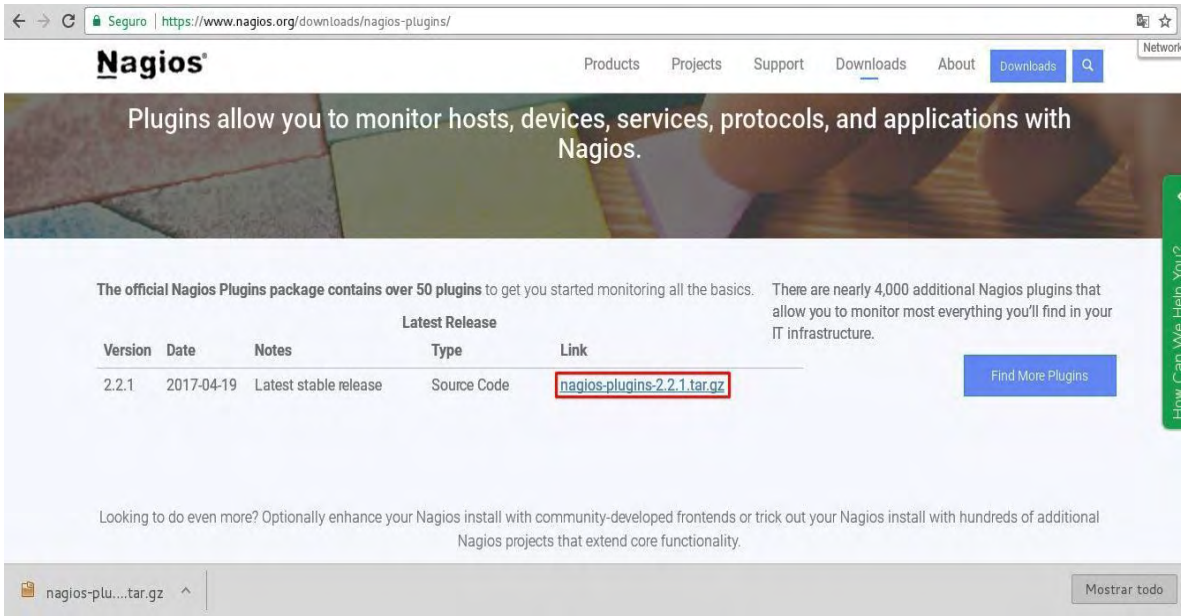
2.1.1 instalación de NRPE en maquina Linux. Toda la configuración se hace como (root)

```
su
```

En el siguiente link se encontra los plugins de Nagios core ”https://www.nagios.org/downloads/”



En esta página se descargan los plugins de Nagios core.



O se pueden descargar directamente con el siguiente comando:

```
cd   /tmp/
```

```
wget https://www.nagios.org/downloads/nagios-plugins-2.2.1.tar.gz
```

Se accede al directorio donde se encuentran descargados los plugins.

```
root@debian1205:/tmp# ls
nagios-plugins-2.2.1.tar.gz
root@debian1205:/tmp#
```

Se descomprime al archivo

```
tar xzf nagios-plugins-2.2.1.tar.gz
```

Quedando los dos archivos

```
root@debian1205:/tmp# ls
nagios-plugins-2.2.1  nagios-plugins-2.2.1.tar.gz
root@debian1205:/home/henry/Descargas#
```

Se ingresa dentro del archivo nagios-plugins-2.2.1

```
cd nagios-plugins-2.2.1
```

Se actualizan los repositorios para poder instalar paquetes necesarios.

```
apt-get update
```

Se crea el usuario Nagios

```
/usr/sbin/useradd nagios
```

Se crea la contraseña para el usuario Nagios

```
passwd nagios
```

Se instala los paquetes de seguridad y el demonio de NRPE que es xinetd.

```
apt-get install libssl-dev xinetd
```

Se compila y se instalan los plugins con los siguientes comandos:

```
./configure
```

```
make
```

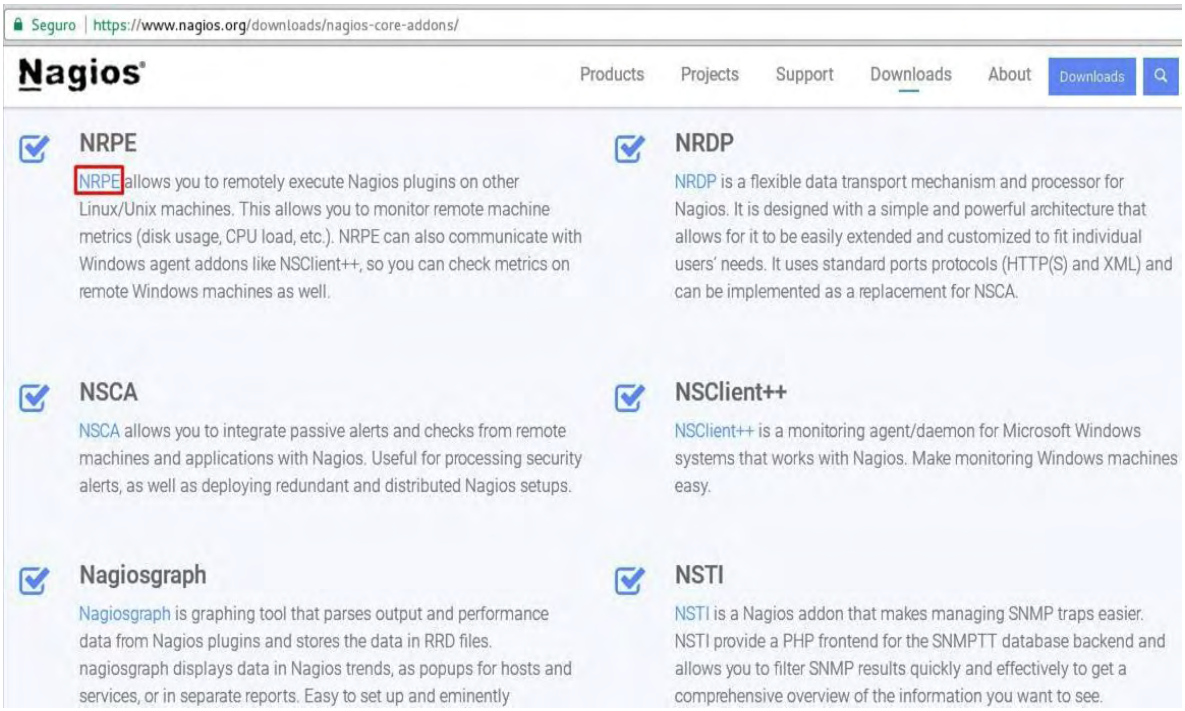
```
make install
```

Se dan los permisos al directorio donde se encuentran los complementos (plugins) de Nagios.

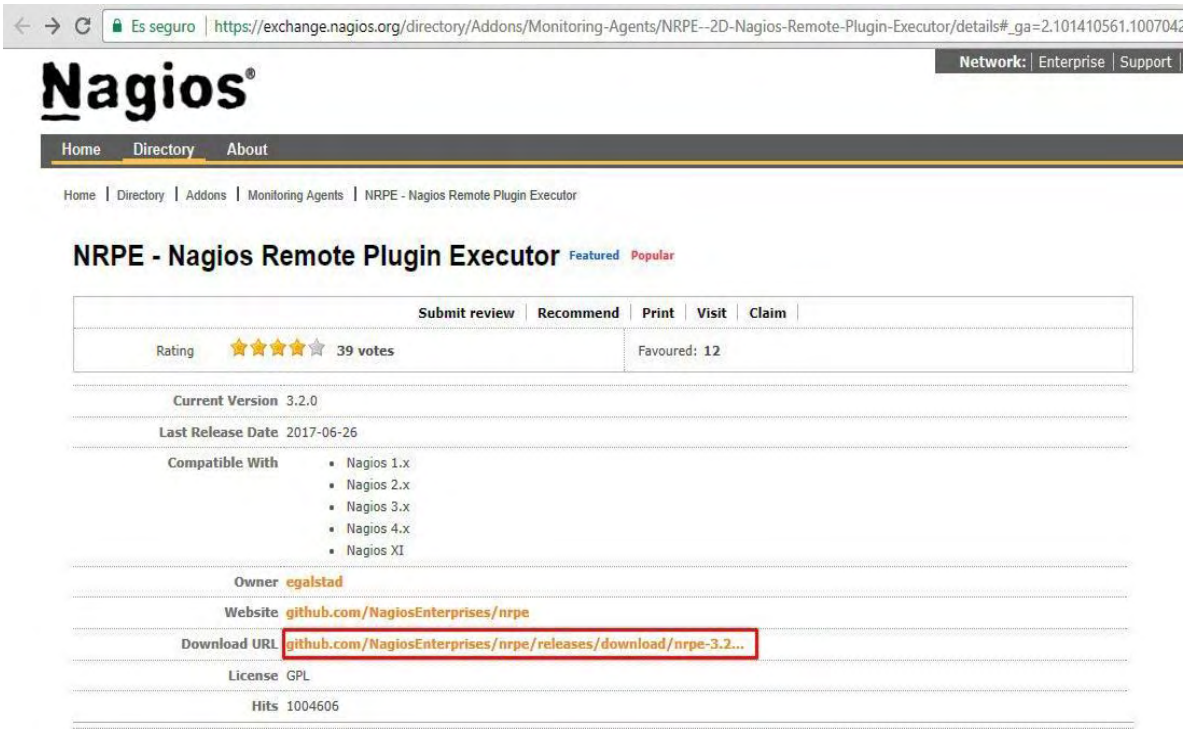
```
chown nagios.nagios /usr/local/Nagios
```

```
chown -R nagios.nagios /usr/local/nagios/libexec
```

En el siguiente link se encuentra el plugin NRPE https://www.nagios.org/downloads/nagios-core-addons/



En el link Download URL se descarga el plugin NRPE.



O se lo puede descargar directamente con el siguiente comando:

```
cd  /tmp/
```

```
wget http://sourceforge.net/projects/nagios/files/nrpe-3.x/nrpe-3.2.0/nrpe-3.2.0.tar.gz
```

```
root@debian1205:/tmp# ls
nagios-plugins-2.2.1  nagios-plugins-2.2.1.tar.gz  nrpe-3.2.0.tar.gz
root@debian1205:/tmp#
```

Se descomprime el archivo.

```
tar xzf nrpe-3.2.0.tar.gz
```

```
root@debian1205:/tmp# ls
nagios-plugins-2.2.1              nrpe-3.2.0
nagios-plugins-2.2.1.tar.gz  nrpe-3.2.0.tar.gz
root@debian1205:/tmp#
```

Estando en la ruta donde se descargó el plugin de NRPE, se accede a “nrpe-3.2.0”.

```
cd nrpe-3.2.0
```

Se compila el plugin NRPE con seguridad para proteger la comunicación entre el servidor Nagios y los host remotos. Este comando es para sistema operativo de 64bits si fuese de 32bits se cambia “x86_64-linux-gnu” por “i386”

```
./configure --with-ssl=/usr/bin/openssl --with-ssl-lib=/usr/lib/x86_64-linux-gnu/
```

```
make all
```

Se instala el plugin de NRPE

```
make install
```

Se instala el archivo de configuración del plugin NRPE.

```
make install-config
```

El siguiente comando permite que NRPE ejecute conexión con Xinetd.

```
make install-inetd
```

Mostrará lo siguiente:

```
root@debian1205:/tmp/nrpe-3.2.0# make install-inetd
/usr/bin/install -c -m 644 startup/default-xinetd /etc/xinetd.d/nrpe
***** MAKE SURE 'nrpe 5666/tcp' IS IN YOUR /etc/services FILE
root@debian1205:/home/henry/Descargas/nrpe-3.2.0#
```

Es necesario reiniciar el demonio de NRPE con los siguientes comandos:

```
service xinetd restart
```

```
systemctl reload xinetd
```

```
systemctl enable nrpe && systemctl start nrpe
```

Se prueba que el demonio está corriendo.

```
netstat -at | egrep "nrpe|5666"
```

Debe mostrar lo siguiente:

```
root@debian1205:/tmp/nrpe-3.2.0# netstat -at | egrep "nrpe|5666"
tcp        0      0 *:nrpe                  *:*                     LISTEN
tcp6       0      0 [::]:nrpe               [::]:*                  LISTEN
root@debian1205:/home/henry/Descargas/nrpe-3.2.0#
```

Se hace una prueba de comunicación con el localhost

```
/usr/local/nagios/libexec/check_nrpe -H localhost
```

Mostrará lo siguiente:

```
NRPE v3.2.0
```

Es necesario permitir el acceso de NRPE con el NRPE del servidor por el puerto (5666). Esto se hace con el siguiente comando:

```
iptables -A INPUT -p tcp --dport 5666 -j ACCEPT
```

Se ingresa al siguiente archivo para modificarlo añadiendo en la línea “allowed_hosts” la IP del servidor Nagios permitiendo la conexión.

```
nano /usr/local/nagios/etc/nrpe.cfg
```

Quedará de la siguiente manera:

```
GNU nano 2.2.6                  Fichero: /usr/local/nagios/etc/nrpe.cfg

# Note: The daemon only does rudimentary checking of the client's IP
# address.  I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

allowed_hosts=127.0.0.1, 192.168.170.250

# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed.  This option only works
# if the daemon was configured with the --enable-command-args configure script
```

```
# option.
#
# *** ENABLING THIS OPTION IS A SECURITY RISK! ***
# Read the SECURITY file for information on some of the security implications
# of enabling this variable.
#
# Values: 0=do not allow arguments, 1=allow command arguments

dont_blame_nrpe=0
```

Se ingresa al siguiente archivo para modificarlo añadiendo en la línea “only_from” la IP del servidor Nagios.

```
nano /etc/xinetd.d/nrpe
```

Quedará de la siguiente manera:

```
  GNU nano 2.2.6                    Fichero: /etc/xinetd.d/nrpe

# default: off
# description: NRPE (Nagios Remote Plugin Executor)
service nrpe
{
    disable         = yes
    socket_type     = stream
    port            = 5666
    wait            = no
    user            = nagios
    group           = nagios
    server          = /usr/local/nagios/bin/nrpe
    server_args     = -c /usr/local/nagios/etc/nrpe.cfg --inetd
    only_from       = 127.0.0.1 192.168.170.250
    log_on_success  =
}
```

Se comprueba que el servicio nrpe se encuentre en este archivo.

```
nano /etc/services
```

```
GNU nano 2.2.6                    Fichero: /etc/services
```

```
xtell           4224/tcp                    # xtell server
fax             4557/tcp                    # FAX transmission service (old)
hylafax         4559/tcp                    # HylaFAX client-server protocol (new)
distmp3         4600/tcp                    # distmp3host daemon
munin           4949/tcp        lrrd        # Munin
enbd-cstatd     5051/tcp                    # ENBD client statd
enbd-sstatd     5052/tcp                    # ENBD server statd
pcrd            5151/tcp                    # PCR-1000 Daemon
noclog          5354/tcp                    # noclogd with TCP (nocol)
noclog          5354/udp                    # noclogd with UDP (nocol)
hostmon         5355/tcp                    # hostmon uses TCP (nocol)
hostmon         5355/udp                    # hostmon uses UDP (nocol)
rplay           5555/udp                    # RPlay audio service
nrpe            5666/tcp                    # Nagios Remote Plugin Executor
nsca            5667/tcp                    # Nagios Agent - NSCA
mrtd            5674/tcp                    # MRT Routing Daemon
bgpsim          5675/tcp                    # MRT Routing Simulator
canna           5680/tcp                    # cannaserver
syslog-tls      6514/tcp                    # Syslog over TLS [RFC5425]
sane-port       6566/tcp    sane saned      # SANE network scanner daemon
```

Es necesario reiniciar el servicio nrpe con los siguientes comandos

```
service nrpe restart
```

```
/etc/init.d/xinetd restart
```

```
systemctl daemon-reload
```

Se verifica el estado del servicio NRPE

```
service nrpe status
```

Deberá mostrar lo siguiente:

```
root@debian1205:/home/henry/Descargas/nrpe-3.2.0# service nrpe status
● nrpe.service - Nagios Remote Plugin Executor
   Loaded: loaded (/lib/systemd/system/nrpe.service; enabled)
   Active: active (running) since mar 2017-07-11 20:36:06 -05; 22s ago
     Docs: http://www.nagios.org/documentation
  Process: 2564 ExecStopPost=/bin/rm -f /usr/local/nagios/var/nrpe.pid
(code=exited, status=0/SUCCESS)
```

```
 Main PID: 2568 (nrpe)
   CGroup: /system.slice/nrpe.service
           └─2568 /usr/local/nagios/bin/nrpe -c /usr/local/nagios/etc/nrpe.cfg -f

jul 11 20:36:06 debian1205 systemd[1]: Started Nagios Remote Plugin Executor.
jul 11 20:36:06 debian1205 nrpe[2568]: Starting up daemon
jul 11 20:36:06 debian1205 nrpe[2568]: Server listening on 0.0.0.0 port 5666.
jul 11 20:36:06 debian1205 nrpe[2568]: Server listening on :: port 5666.
jul 11 20:36:06 debian1205 nrpe[2568]: Listening for connections on port 5666
jul 11 20:36:06 debian1205 nrpe[2568]: Allowing connections from: 127.0.0.1,
192.168.170.250
root@debian1205:/home/henry/Descargas/nrpe-3.2.0#
```

Se comprueba el estado del demonio de NRPE Xinetd.

```
/etc/init.d/xinetd status
```

Mostrará lo siguiente:

```
root@debian1205:/home/henry/Descargas/nrpe-3.2.0# /etc/init.d/xinetd status
● xinetd.service - LSB: Starts or stops the xinetd daemon.
   Loaded: loaded (/etc/init.d/xinetd)
   Active: active (running) since mar 2017-07-11 20:36:12 -05; 5min ago
  Process: 2579 ExecStop=/etc/init.d/xinetd stop (code=exited,
status=0/SUCCESS)
  Process: 2506 ExecReload=/etc/init.d/xinetd reload (code=exited,
status=0/SUCCESS)
  Process: 2584 ExecStart=/etc/init.d/xinetd start (code=exited,
status=0/SUCCESS)
   CGroup: /system.slice/xinetd.service
           └─2594 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inetd_compat -
inetd_ipv6

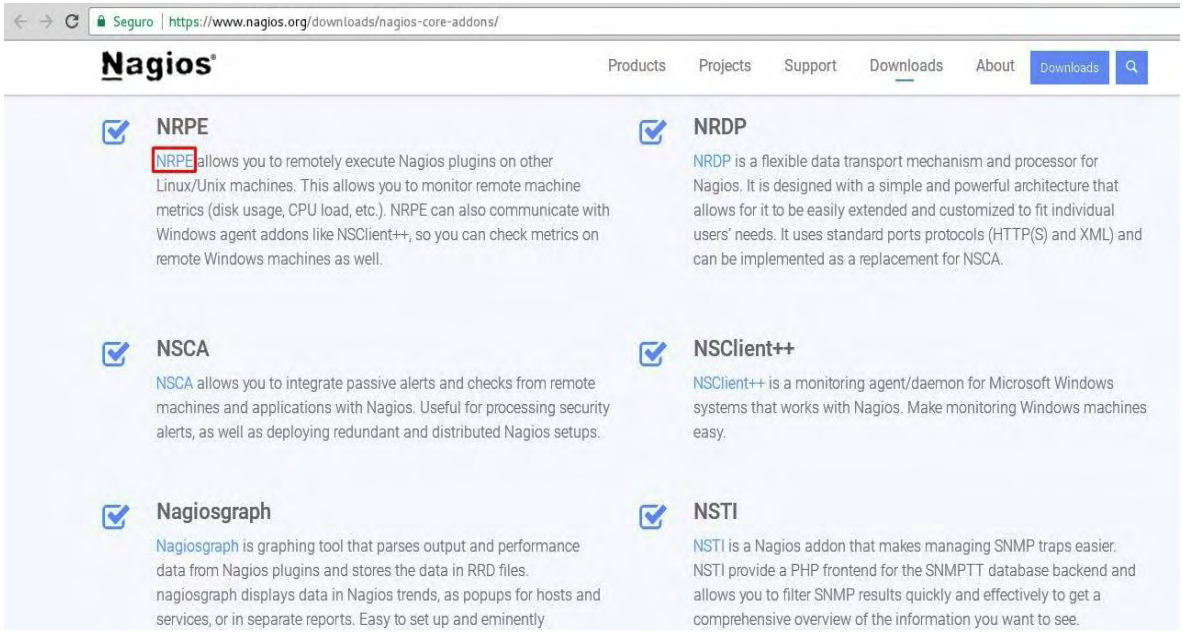
jul 11 20:36:12 debian1205 xinetd[2594]: removing daytime
jul 11 20:36:12 debian1205 xinetd[2594]: removing discard
jul 11 20:36:12 debian1205 xinetd[2594]: removing discard
jul 11 20:36:12 debian1205 xinetd[2594]: removing echo
jul 11 20:36:12 debian1205 xinetd[2594]: removing echo
jul 11 20:36:12 debian1205 xinetd[2594]: removing nrpe
jul 11 20:36:12 debian1205 xinetd[2594]: removing time
jul 11 20:36:12 debian1205 xinetd[2594]: removing time
jul 11 20:36:12 debian1205 xinetd[2594]: xinetd Version 2.3.15 started with libwrap
loadavg options compiled in.
```

```
jul 11 20:36:12 debian1205 xinetd[2594]: Started working: 0 available services
root@debian1205:/home/henry/Descargas/nrpe-3.2.0#
```

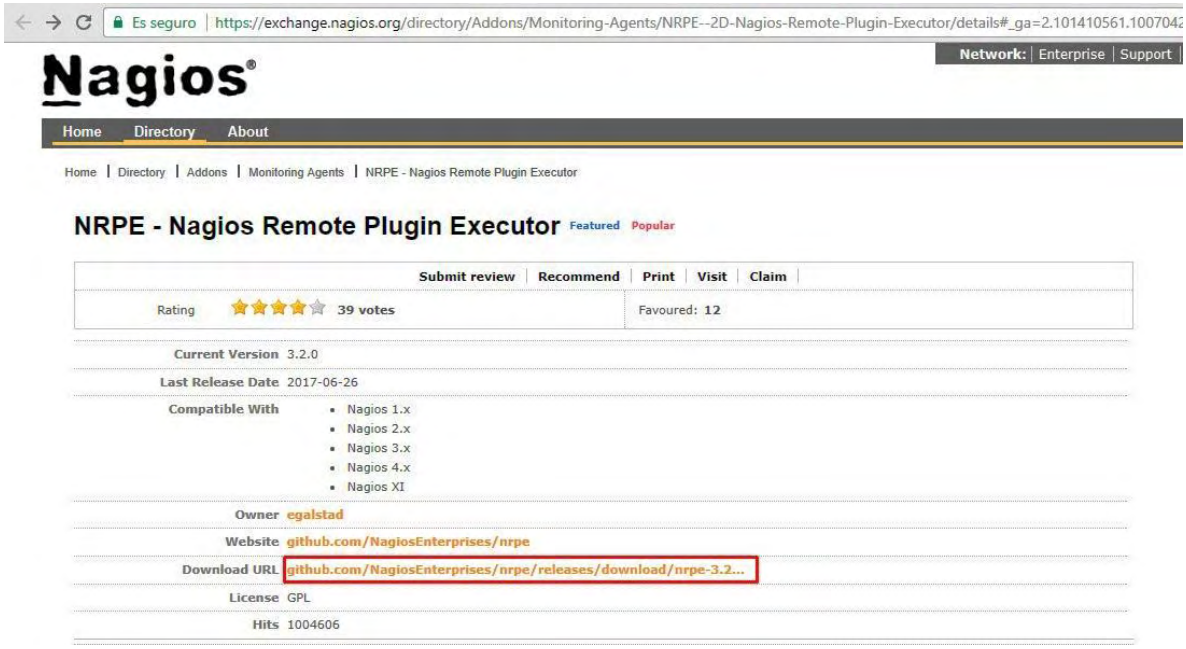
2.1.2 instalación de Nrpe en servidor Nagios:

Paginas referentes:
https://itiramos.wordpress.com/2015/05/20/nagios-instalacion-de-nrpe-en-host-y-cliente/

En el siguiente link se encuentra el plugin NRPE
https://www.nagios.org/downloads/nagios-core-addons/



Nos dirigimos al siguiente link y descargamos el plugin NRPE.



Podemos descargarlo directamente así.

```
cd /tmp/
wget http://sourceforge.net/projects/nagios/files/nrpe-3.x/nrpe-3.2.0/nrpe-3.2.0.tar.gz
```

Descomprimimos el paquete con el siguiente comando

```
tar xzf nrpe-3.2.0.tar.gz
```

Accedemos al archivo de nrpe-3.2.0 asi:

```
cd nrpe-3.2.0
```

Compilamos NRPE con los siguientes comandos.

```
./configure --with-ssl=/usr/bin/openssl --with-ssl-lib=/usr/lib/x86_64-linux-gnu
make all
```

- Instalación de plugin NRPE

```
make install-plugin
```

Verificamos la comunicación del demonio NRPE, aparecera algo como lo siguiente.

```
/usr/local/nagios/libexec/check_nrpe -H 192.168.170.0
```

Debe aparecer lo siguiente.

```
NRPE v3.2.0
```

“192.168.170.0” se remplaza por una dirección IP de un host remoto que ya tenga instalado el plugin NRPE (cliente) instalado para verificar la conexión.

Es necesario crear una definición del comando en el archivo de objetos de Nagios que se encuentra en la siguiente ruta “/usr/local/nagios/etc/”.
Editamos el siguiente archivo:

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Deberá quedar definido de la siguiente manera:

```
define command{
 command_name check_nrpe
 command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
 }
```

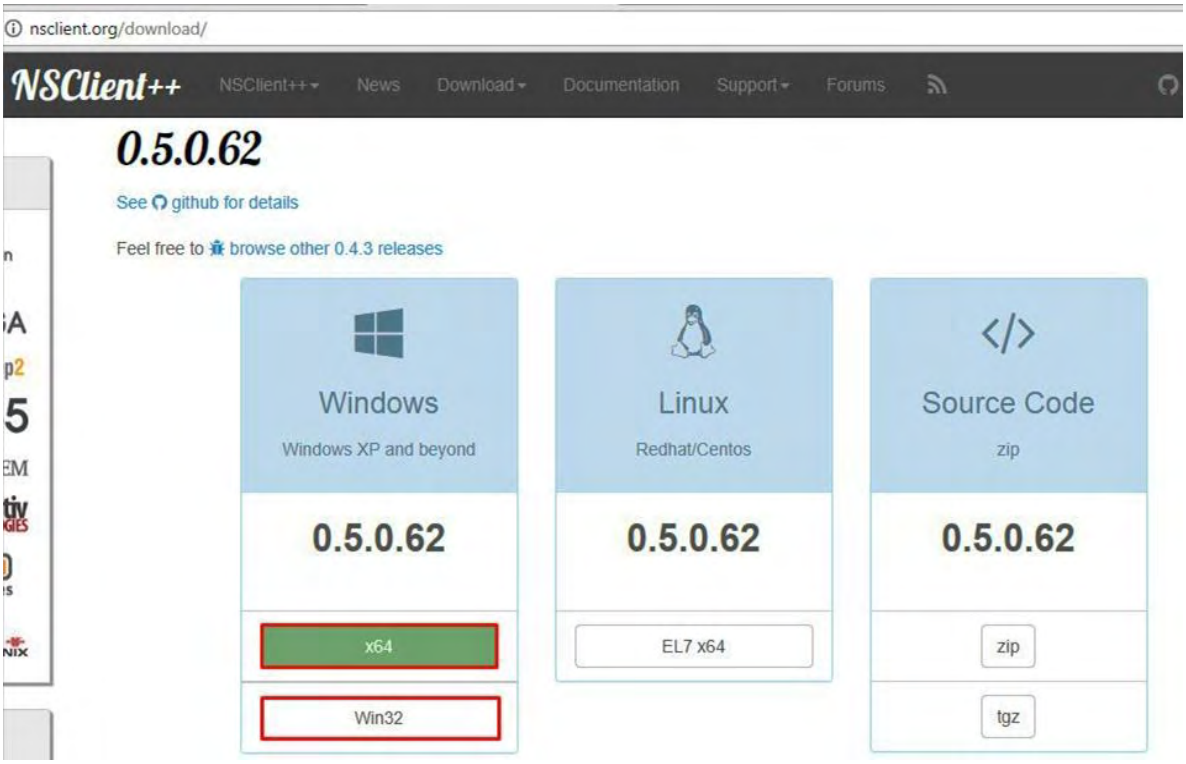
Primero se debe comprobar que no haya errores en la configuración con el siguiente comando:

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

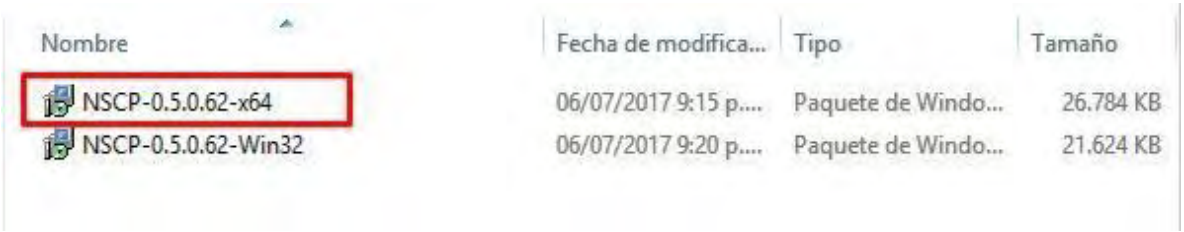
NOTA: Si se obtiene algún error se debe corregir antes de reiniciar Nagios para que no se guarde con errores, cada vez que se realicen cambios en la configuración de Nagios se recomienda utilizar este comando de verificación antes de efectuar los cambios.
Finalmente se reinicia Nagios para guardar cambios, con los siguientes comandos:

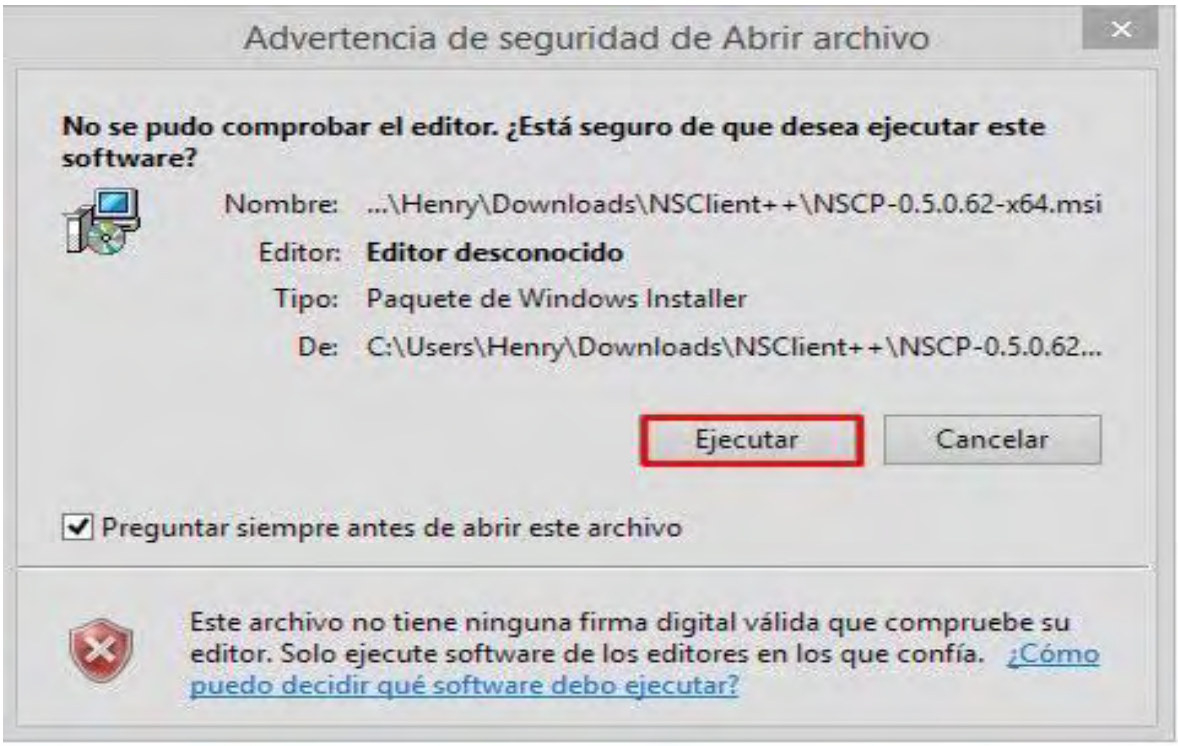
```
service nagios restart
/etc/init.d/nagios restart
```

2.1.3 Instalación agente nsclient++ en maquina Windows. Se descargan desde el siguiente link “http://nsclient.org/download/”

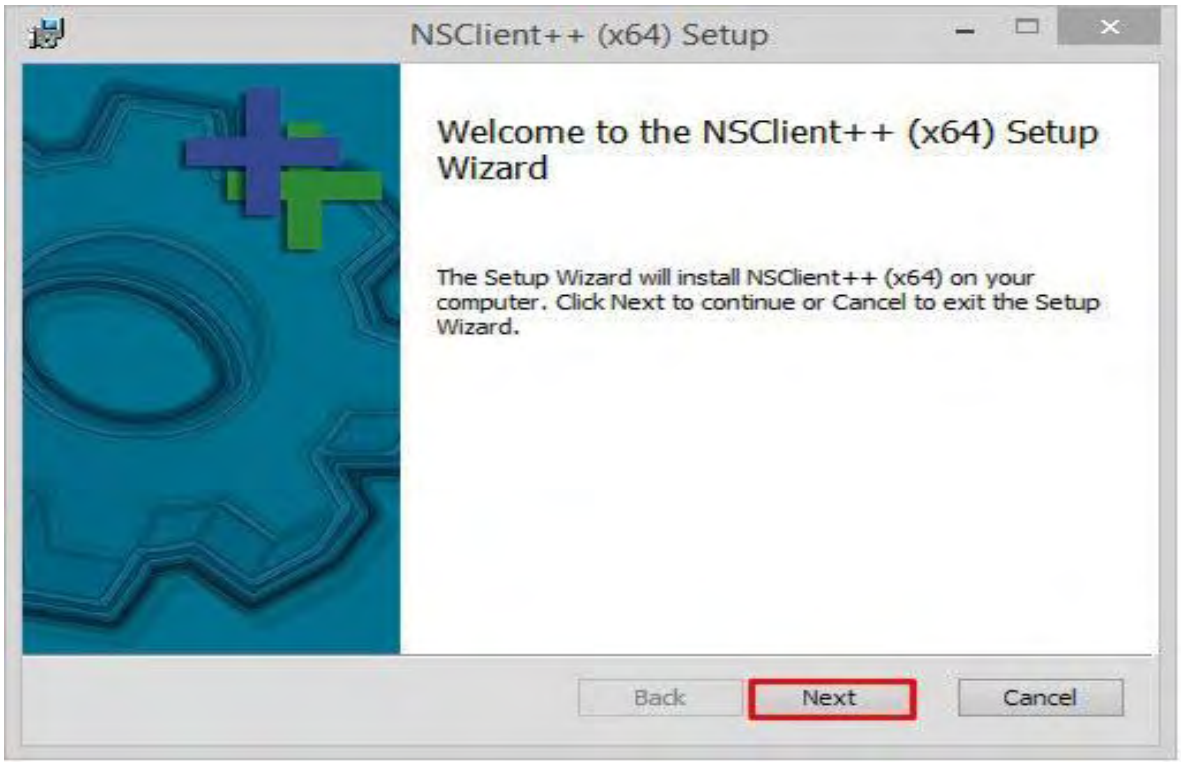


Se ejecuta el instalador dependiendo del tipo de Sistema.
NOTA: estos pasos son los mismos para sistemas operativos basados en 64 y 32 bits

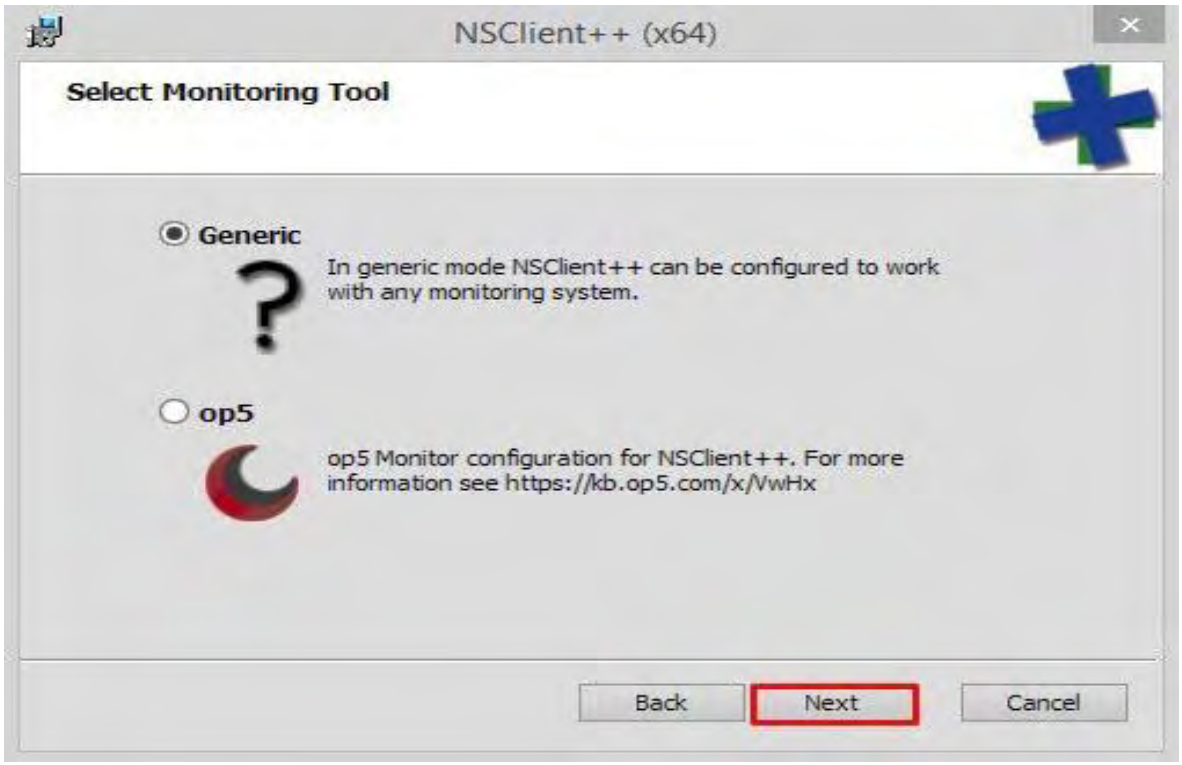



Advertencia de seguridad de Abrir archivo
No se pudo comprobar el editor. ¿Está seguro de que desea ejecutar este software?
Nombre: ...\Henry\Downloads\NSClient++\NSCP-0.5.0.62-x64.msi
Editor: Editor desconocido
Tipo: Paquete de Windows Installer
De: C:\Users\Henry\Downloads\NSClient++\NSCP-0.5.0.62...
Ejecutar
Cancelar
Preguntar siempre antes de abrir este archivo
Este archivo no tiene ninguna firma digital válida que compruebe su editor. Solo ejecute software de los editores en los que confía. ¿Cómo puedo decidir qué software debo ejecutar?

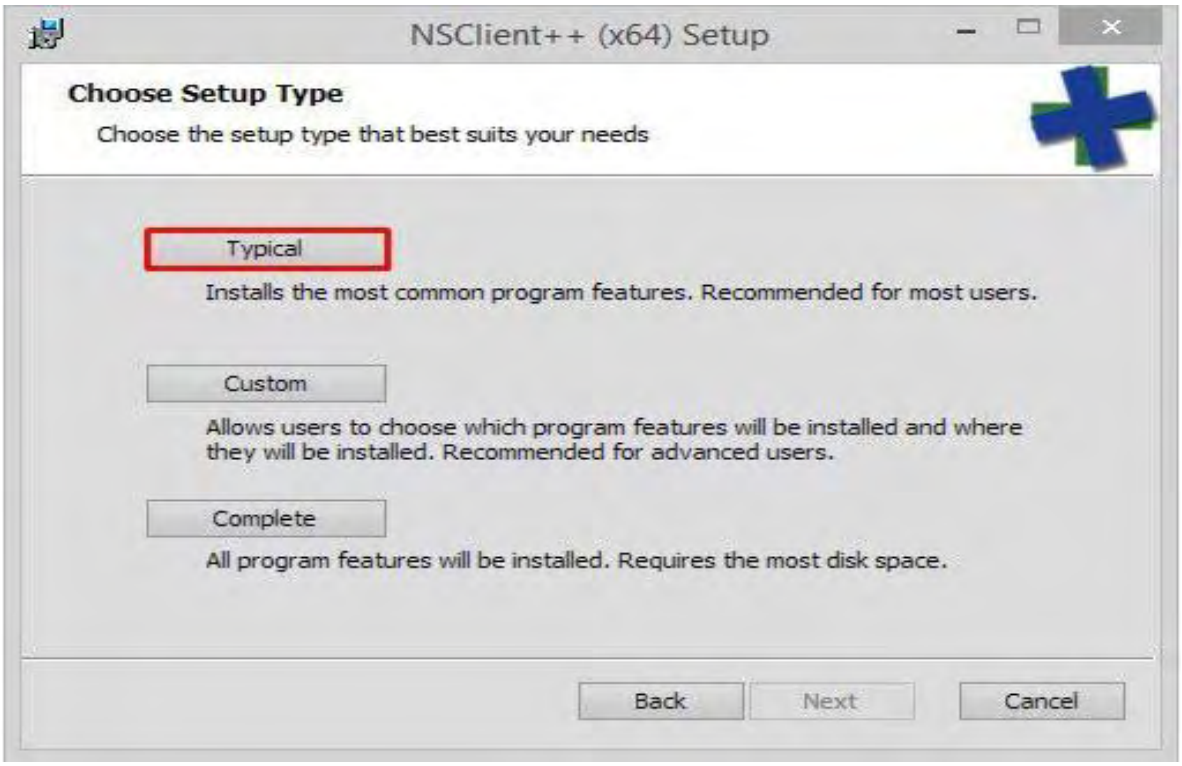
Se da en la opción **Next**.



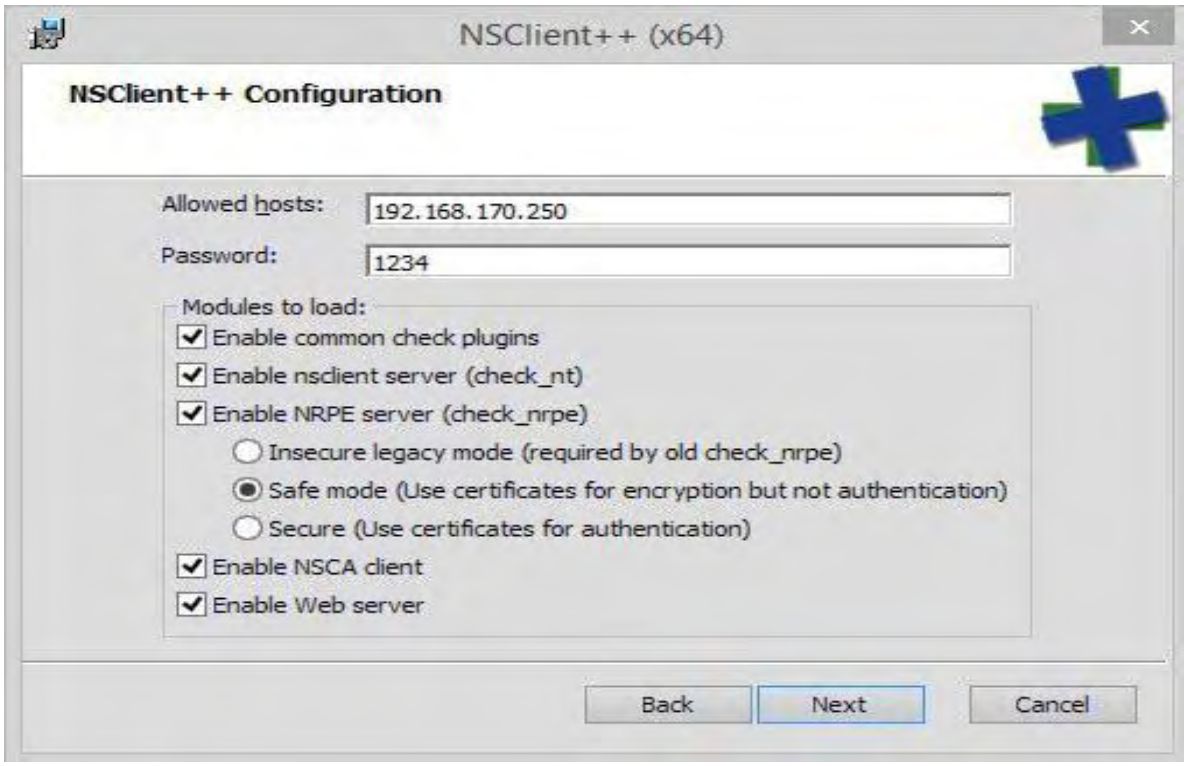
Se instala con la configuración genérica.



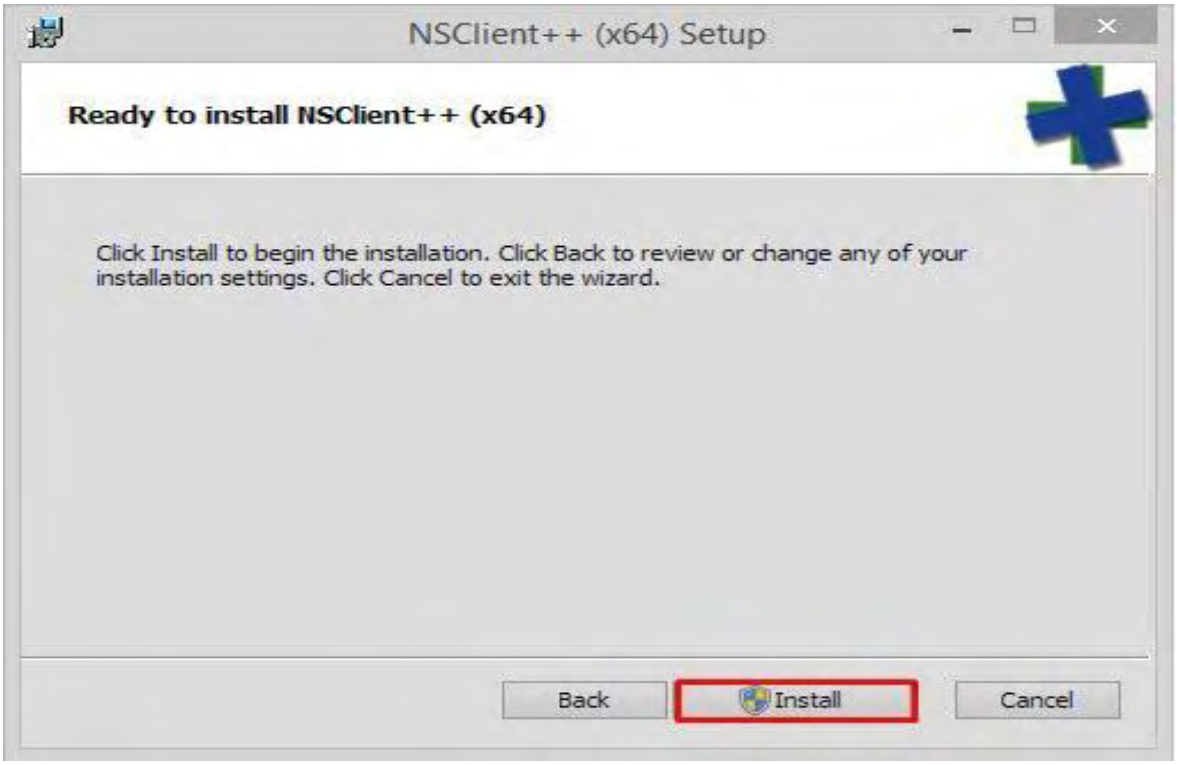
Se elige el tipo de configuración Típica.



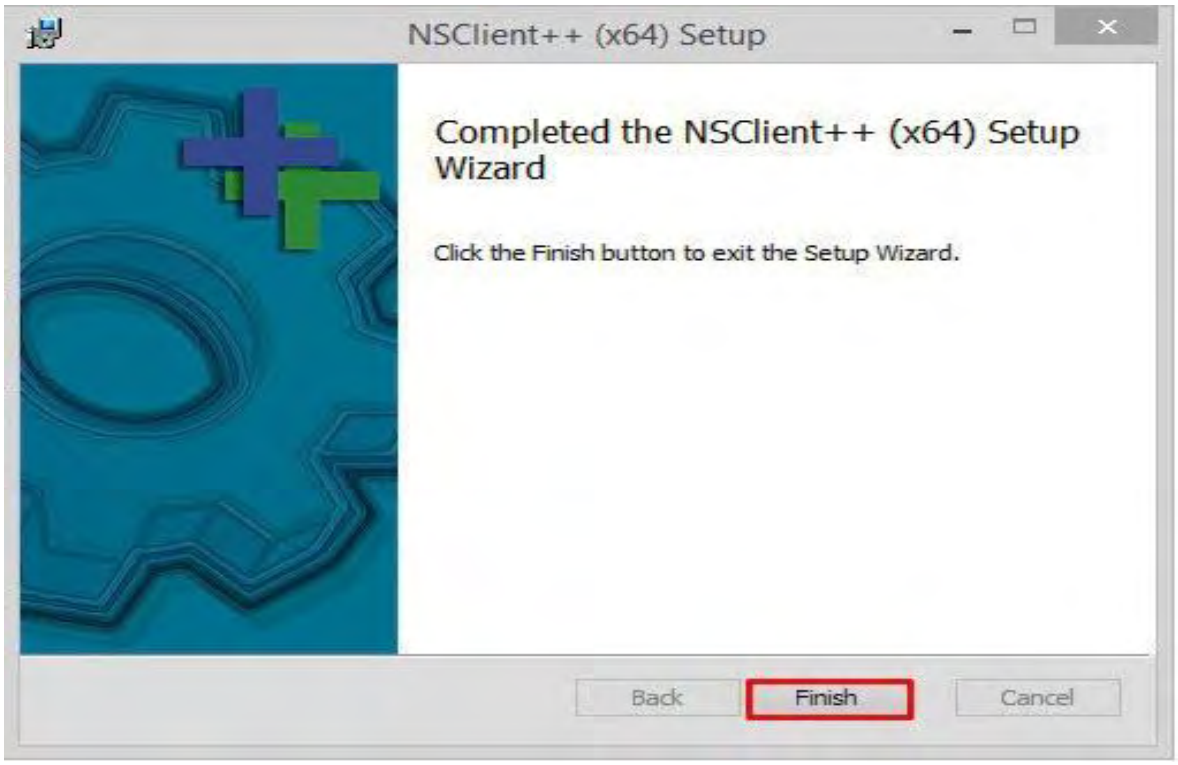
En Allowed hosts se coloca la IP del servidor Nagios y en Password se coloca la contraseña la cual se colocará en la configuración del servidor Nagios con lo cual podrá reconocer al host. Se habilitan los módulos que se requieran para el monitoreo.



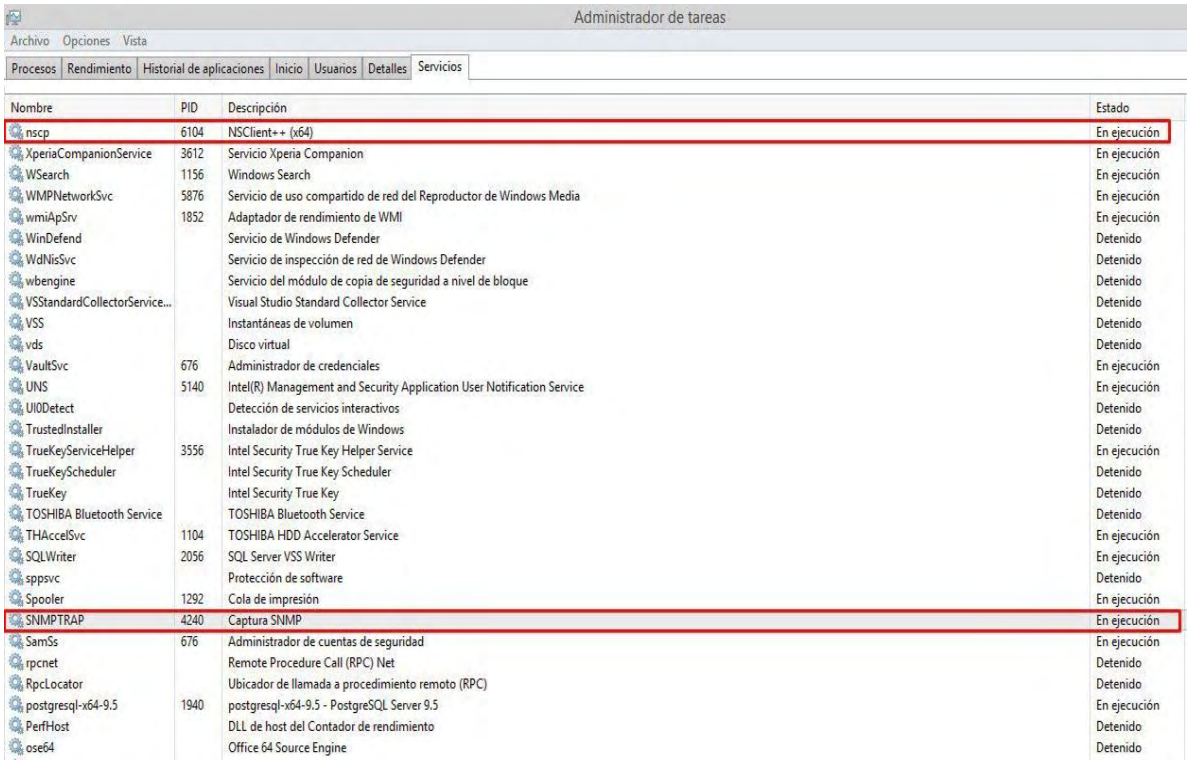
Luego de terminar la configuración para la instalación, se procede a instalar.



Se finaliza la instalación.



Luego se verifica en el administrador de tareas que el servicio **nscp** este en ejecución juntamente con el servicio **SNMP TRAP**.



Nombre	PID	Descripción	Estado
nscp	6104	NSClient++ (x64)	En ejecución
XperiaCompanionService	3612	Servicio Xperia Companion	En ejecución
WSearch	1156	Windows Search	En ejecución
WMPNetworkSvc	5876	Servicio de uso compartido de red del Reproductor de Windows Media	En ejecución
wmiApSrv	1852	Adaptador de rendimiento de WMI	En ejecución
WinDefend		Servicio de Windows Defender	Detenido
WdNisSvc		Servicio de inspección de red de Windows Defender	Detenido
wbengine		Servicio del módulo de copia de seguridad a nivel de bloque	Detenido
VSStandardCollectorService...		Visual Studio Standard Collector Service	Detenido
VSS		Instantáneas de volumen	Detenido
vds		Disco virtual	Detenido
VaultSvc	676	Administrador de credenciales	En ejecución
UNS	5140	Intel(R) Management and Security Application User Notification Service	En ejecución
UI0Detect		Detección de servicios interactivos	Detenido
TrustedInstaller		Instalador de módulos de Windows	Detenido
TrueKeyServiceHelper	3556	Intel Security True Key Helper Service	En ejecución
TrueKeyScheduler		Intel Security True Key Scheduler	Detenido
TrueKey		Intel Security True Key	Detenido
TOSHIBA Bluetooth Service		TOSHIBA Bluetooth Service	Detenido
THAccelSvc	1104	TOSHIBA HDD Accelerator Service	En ejecución
SQLWriter	2056	SQL Server VSS Writer	En ejecución
sppsvc		Protección de software	Detenido
Spooler	1292	Cola de impresión	En ejecución
SNMPTRAP	4240	Captura SNMP	En ejecución
SamSs	676	Administrador de cuentas de seguridad	En ejecución
rpcnet		Remote Procedure Call (RPC) Net	Detenido
RpcLocator		Ubicador de llamada a procedimiento remoto (RPC)	Detenido
postgresql-x64-9.5	1940	postgresql-x64-9.5 - PostgreSQL Server 9.5	En ejecución
PerfHost		DLL de host del Contador de rendimiento	Detenido
ose64		Office 64 Source Engine	Detenido

2.2 INSTALACIÓN Y CONFIGURACIÓN DE CHECK_MK

Se lo puede descargar directamente desde (http://mathias-kettner.com/check_mk_download_source.html), para más información visitar el sitio web (http://mathias-kettner.com/check_mk.html).

Para la descarga se coloca el siguiente comando.

```
wget -O /tmp/check_mk-1.2.8p25.tar.gz http://mathias-kettner.com/download/check_mk-1.2.8p25.tar.gz
```

- Prerequisitos

Se instala algunas dependencias para los gráficos

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

- Instalación Check_MK

Nota. Para compilar check_mk se debe tener al menos 700Mb de RAM. Si no, puede aparecer un error como: g++: internal compiler error: Killed (program cc1plus)

```
cd /tmp/
tar zxfv check_mk-1.2.8p25.tar.gz
cd check_mk-1.2.8p25
./setup.sh
```

Se deja todo por defecto excepto por estas opciones.

```
Check_MK configuration
( default  --> /etc/check_mk): /usr/local/check_mk

Nagios command pipe
( default  --> /var/log/nagios/rw/nagios.cmd): /usr/local/nagios/var/rw/nagios.cmd

URL Prefix for Web addons
( default  --> /): /site01/

Apache config dir
( default  --> /etc/apache2/conf.d): /etc/apache2/sites-enabled
```

```
HTTP authentication file
( default  --> /etc/nagios/htpasswd.users): /usr/local/nagios/etc/htpasswd.users

RRD files
( default  --> /var/lib/nagios/rrd): /usr/local/nagios/var/rrd

Install Event Console
( default  --> no): yes
```



Welcome to Check_MK. This setup will install Check_MK into user defined directories. If you run this script as root, installation paths below /usr will be suggested. If you run this script as non-root user paths in your home directory will be suggested. You may override the default values or just hit enter to accept them.

Your answers will be saved to /root/.check_mk_setup.conf and will be reused when you run the setup of this or a later version again. Please delete that file if you want to delete your previous answers.

* Found running Nagios process, autodetected 16 settings.

1) Installation directories of check_mk

Executable programs
Directory where to install executable programs such as check_mk itself. This directory should be in your search path ($PATH). Otherwise you always have to specify the installation path when calling check_mk:
(default --> /usr/bin):

Check_MK configuration
Directory where check_mk looks for its main configuration file main.mk. An example configuration file will be installed there if no main.mk is present from a previous version:
(default --> /etc/check_mk): /usr/local/check_mk

Check_MK software
The base directory for the software installation of Check_MK. This directory will get the subdirectories checks, modules, web, locale and agents. Note: in previous versions it was possible to specify each of those directories separately. This is no longer possible:
(default --> /usr/share/check_mk):

documentation
Some documentation about check_mk will be installed here. Please note,
however, that most of check_mk's documentation is available only online at
http://mathias-kettner.de/check_mk.html:
(default --> /usr/share/doc/check_mk):

check_manuals
Directory for manuals for the various checks. The manuals can be viewed
with check_mk -M <CHECKNAME>:
(default --> /usr/share/doc/check_mk/checks):

working directory of Check_MK
Check_MK will create log files, automatically created checks and
other files into this directory. The setup will create several subdirectories
and makes them writable by the Nagios process:
(default --> /var/lib/check_mk):

2) Configuration of Linux/UNIX Agents

extensions for agents
This directory will not be created on the server. It will be hardcoded
into the Linux and UNIX agents. The agent will look for extensions in the
subdirectories plugins/ and local/ of that directory:
(default --> /usr/lib/check_mk_agent):

configuration dir for agents
This directory will not be created on the server. It will be hardcoded
into the Linux and UNIX agents. The agent will look for its configuration
files here (currently only the logwatch extension needs a configuration file):
(default --> /etc/check_mk):

3) Integration with Nagios

Name of Nagios user
The working directory for check_mk contains several subdirectories
that need to be writable by the Nagios user (which is running check_mk
in check mode). Please specify the user that should own those
directories:
(autodetected --> nagios):

User of Apache process
Check_MK WATO (Web Administration Tool) needs a sudo configuration,
such that Apache can run certain commands as root. If you specify
the correct user of the apache process here, then we can create a valid
sudo configuration for you later::
(autodetected --> www-data):

Common group of Nagios+Apache
Check_mk creates files and directories while running as nagios.
Some of those need to be writable by the user that is running the webserver.
Therefore a group is needed in which both Nagios and the webserver are
members (every valid Nagios installation uses such a group to allow
the web server access to Nagios' command pipe)::
(autodetected --> nagios):

Nagios binary
The complete path to the Nagios executable. This is needed by the
option -R/--restart in order to do a configuration check.:
(autodetected --> /usr/local/nagios/bin/nagios):

Nagios main configuration file
Path to the main configuration file of Nagios. That file is always
named 'nagios.cfg'. The default path when compiling Nagios yourself
is /usr/local/nagios/etc/nagios.cfg. The path to this file is needed
for the check_mk option -R/--restart:
(autodetected --> /usr/local/nagios/etc/nagios.cfg):

Nagios object directory
Nagios' object definitions for hosts, services and contacts are
usually stored in various files with the extension .cfg. These files
are located in a directory that is configured in nagios.cfg with the
directive 'cfg_dir'. Please specify the path to that directory
(If the autodetection can find your configuration
file but does not find at least one cfg_dir directive, then it will
add one to your configuration file for your conveniance):
(autodetected --> /usr/local/nagios/etc/check_mk.d):

Nagios startskript
The complete path to the Nagios startskript is used by the option
-R/--restart to restart Nagios.:
(autodetected --> /etc/init.d/nagios):

Nagios command pipe
Complete path to the Nagios command pipe. check_mk needs write access
to this pipe in order to operate:
(default --> /var/log/nagios/rw/nagios.cmd): /usr/local/nagios/var/rw/nagios.cmd

Check results directory
Complete path to the directory where Nagios stores its check results.
Using that directory instead of the command pipe is faster.:
(autodetected --> /usr/local/nagios/var/spool/checkresults):

Nagios status file
The web pages of check_mk need to read the file 'status.dat', which is
regularily created by Nagios. The path to that status file is usually
configured in nagios.cfg with the parameter 'status_file'. If
that parameter is missing, a compiled-in default value is used. On
FHS-conforming installations, that file usually is in /var/lib/nagios
or /var/log/nagios. If you've compiled Nagios yourself, that file
might be found below /usr/local/nagios:
(autodetected --> /usr/local/nagios/var/status.dat):

Path to check_icmp
check_mk ships a Nagios configuration file with several host and
service templates. Some host templates need check_icmp as host check.
That check plugin is contained in the standard Nagios plugins.
Please specify the complete path (dir + filename) of check_icmp:
(autodetected --> /usr/local/nagios/libexec/check_icmp):

4) Integration with Apache

URL Prefix for Web addons

Usually the Multisite GUI is available at /check_mk/ and PNP4Nagios
is located at /pnp4nagios/. In some cases you might want to define some
prefix in order to be able to run more instances of Nagios on one host.
If you say /test/ here, for example, then Multisite will be located
at /test/check_mk/. Please do not forget the trailing slash.:
(default --> /): /site01/

Apache config dir

Check_mk ships several web pages implemented in Python with Apache
mod_python. That module needs an apache configuration section which
will be installed by this setup. Please specify the path to a directory
where Apache reads in configuration files.:
(default --> /etc/apache2/conf.d): /etc/apache2/sites-enabled

HTTP authentication file

Check_mk's web pages should be secured from unauthorized access via
HTTP authenticaion - just as Nagios. The configuration file for Apache
that will be installed contains a valid configuration for HTTP basic
auth. The most conveniant way for you is to use the same user file as
for Nagios. Please enter your htpasswd file to use here:
(default --> /etc/nagios/htpasswd.users): /usr/local/nagios/etc/htpasswd.users

HTTP AuthName

Check_mk's Apache configuration file will need an AuthName. That
string will be displayed to the user when asking for the password.
You should use the same AuthName as for Nagios. Otherwise the user will
have to log in twice:
(default --> Nagios Access):

---

5) Integration with PNP4Nagios 0.6

PNP4Nagios templates

Check_MK ships templates for PNP4Nagios for most of its checks.
Those templates make the history graphs look nice. PNP4Nagios
expects such templates in the directory pnp/templates in your
document root for static web pages:
(default --> /usr/share/check_mk/pnp-templates):

RRD files

Configure the directory PNP4Nagios stores the RRD database files in:
(default --> /var/lib/nagios/rrd): /usr/local/nagios/var/rrd

rrdcached socket

If you use the rrdcached to process performance data from Nagios,
you can configure the socket of the rrdcached here to make the prediction
feature use it:
(default --> /tmp/rrdcached.sock):

6) Check_MK Livestatus Module

compile livestatus module
The well known MK Livestatus broker module is part of Check_MK.

It provides direct access to Nagios internal data structures. It aims to supersede status.dat and also NDO. The Livestatus Module does not only allow extremely fast access to the status of your services and hosts, it does also provide live data (which status.dat does not). Also - unlike NDO - Livestatus does not cost you even measurable CPU performance, does not need any disk space and also needs no configuration.

Livestatus is neccessary when you want to use Multisite. It is also the preferred backend for NagVis.

Please answer 'yes', if you want to compile and integrate the Livestatus module into your Nagios. You need 'make' and the GNU C++ compiler installed in order to do this:
(default --> yes):

Nagios / Icinga version
The version is required for the compilation of the livestatus module. Depending on the major version (3 or 4) different nagios headers are included:
(autodetected --> 4.3.4):

check_mk's binary modules
Directory for architecture dependent binary libraries and plugins of check_mk:
(default --> /usr/lib/check_mk):

Unix socket for Livestatus
The Livestatus Module provides Nagios status data via a unix socket. This is similar to the Nagios command pipe, but allows bidirectional communication. Please enter the path to that pipe. It is recommended to put it into the same directory as Nagios' command pipe:
(default --> /usr/local/nagios/var/rw/live):

Backends for other systems
Directory where to put backends and configuration examples for other systems. Currently this is only Nagvis, but other might follow later.:
(default --> /usr/share/check_mk/livestatus):



Install Event Console

The Check_MK Event Console is a full featured event processing module that integrates with Multisite. It has an own daemon and several methods for retrieving events. It even has an integrated syslog daemon. Please answer 'yes', if you want to enable the Event Console.:

(default --> no): yes

working directory of mkeventd

The Event Console Daemon will store status and historic data in this directory.:

(default --> /var/lib/mkeventd):

```
You have chosen the following directories:

Executable programs                /usr/bin
Check_MK configuration             /usr/local/check_mk
Check_MK software                  /usr/share/check_mk
documentation                      /usr/share/doc/check_mk
check manuals                      /usr/share/doc/check_mk/checks
working directory of Check_MK      /var/lib/check_mk
extensions for agents              /usr/lib/check_mk_agent
configuration dir for agents       /etc/check_mk
Name of Nagios user                nagios
User of Apache process             www-data
Common group of Nagios+Apache      nagios
Nagios binary                      /usr/local/nagios/bin/nagios
Nagios main configuration file     /usr/local/nagios/etc/nagios.cfg
Nagios object directory            /usr/local/nagios/etc/check_mk.d
Nagios startskript                 /etc/init.d/nagios
Nagios command pipe                /usr/local/nagios/var/rw/nagios.cmd
Check results directory            /usr/local/nagios/var/spool/checkresults
Nagios status file                 /usr/local/nagios/var/status.dat
Path to check_icmp                 /usr/local/nagios/libexec/check_icmp
URL Prefix for Web addons          /site01/
Apache config dir                  /etc/apache2/sites-enabled
HTTP authentication file           /usr/local/nagios/etc/htpasswd.users
HTTP AuthName                      Nagios Access
PNP4Nagios templates               /usr/share/check_mk/pnp-templates
RRD files                          /usr/local/nagios/var/rrd
rrdcached socket                   /tmp/rrdcached.sock
compile livestatus module          yes
Nagios / Icinga version            4.3.2
check_mk's binary modules          /usr/lib/check_mk
Unix socket for Livestatus         /usr/local/nagios/var/rw/live
Backends for other systems         /usr/share/check_mk/livestatus
Install Event Console              yes
working directory of mkeventd      /var/lib/mkeventd

Proceed with installation (y/n)? y
```

Al final aparecerá.

```
Installation completed successfully.
Please restart Nagios and Apache in order to update/active check_mk's web pages.

You can access the new Multisite GUI at http://localhost/site01/check_mk/
```

Ahora añadimos el daemon CMK al arrancar y reiniciamos todos los servicios.

Para debian7 wheezy.

```
service mkeventd start
service apache2 restart
service nagios restart
service mkeventd restart
```

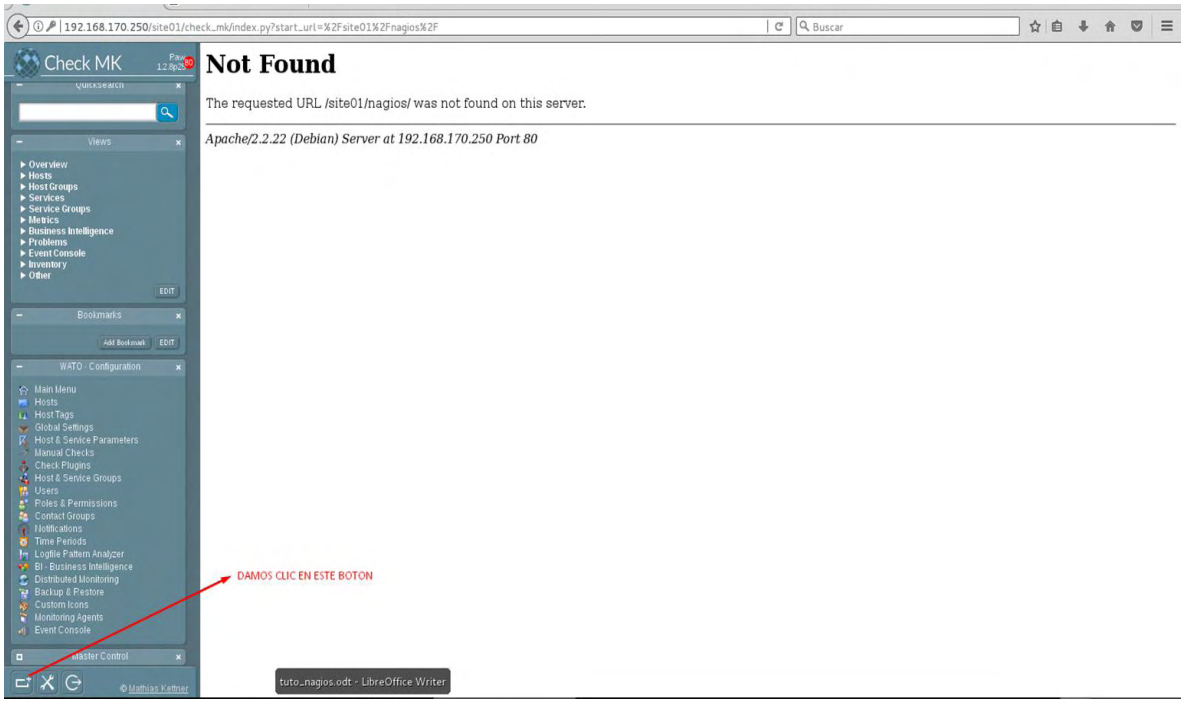
Para debian8 jessie

```
systemctl enable mkeventd
systemctl restart apache2
systemctl restart nagios
systemctl restart mkeventd
```

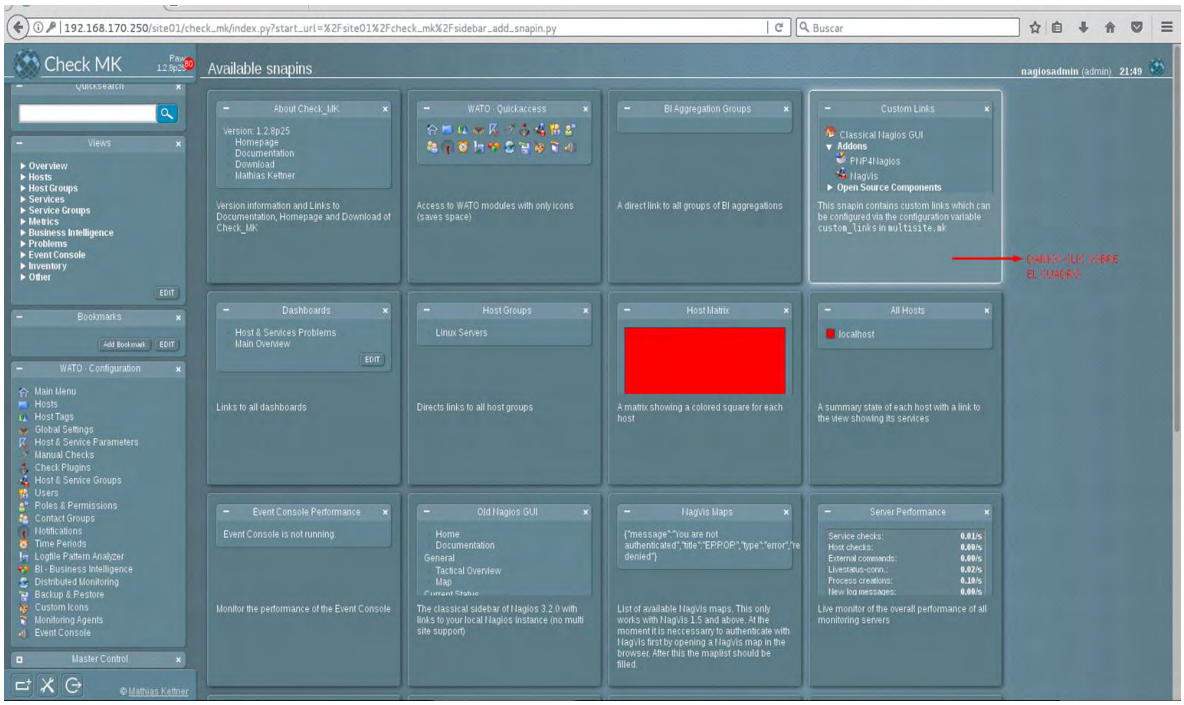
Y comprobamos en el navegador.

```
http://nagios-server-ip/site01/check_mk/
```

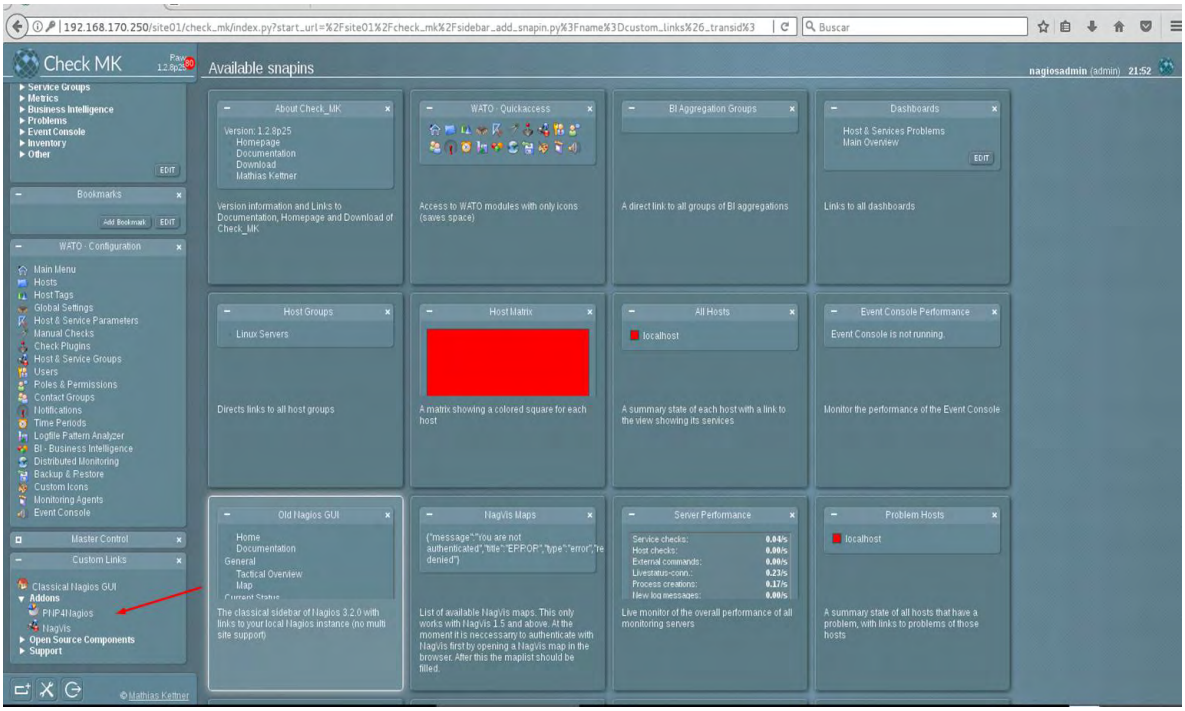
2.2.1 Vinculación de Nagios con Check_MK. En primer lugar, se debe dirigir hacia dar clic sobre el botón que se muestra en la siguiente imagen.



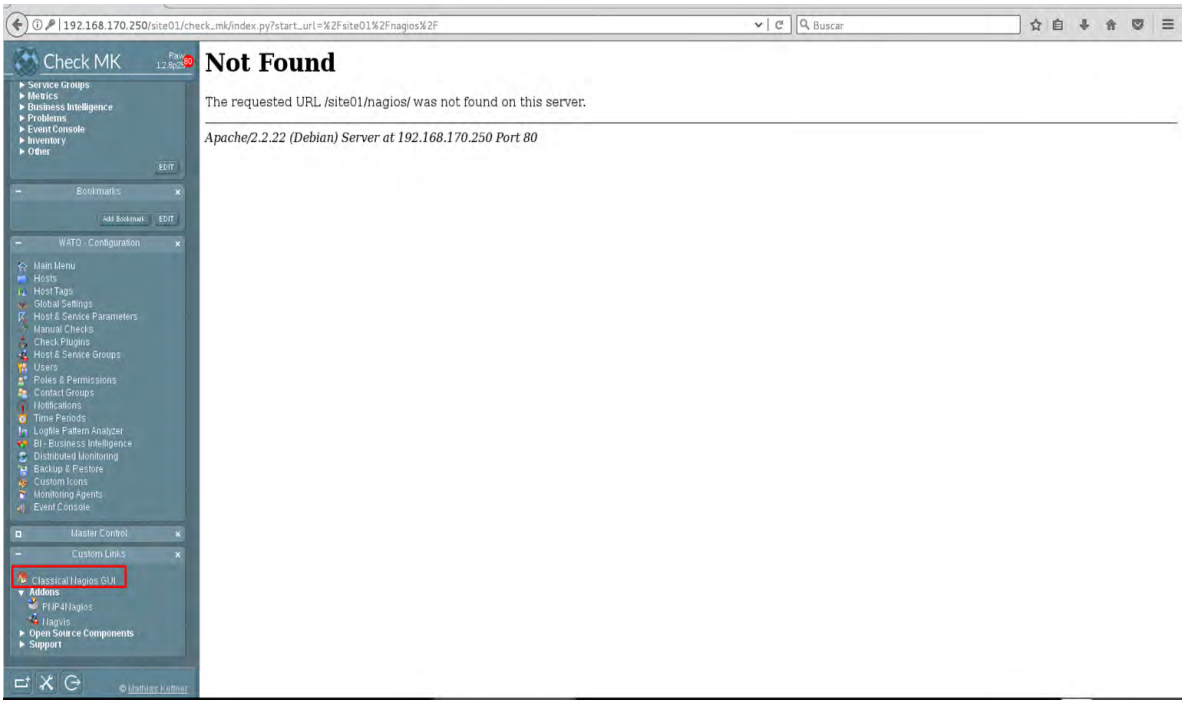
Esto permite agregar snapins al sidebar o barra lateral. Dando clic sobre uno de los recuadros.


192.168.170.250/site01/check_mk/index.py?start_url=%2Fsite01%2Fcheck_mk%2Fsidebar_add_snapin.py
Buscar
Check MK
Available snapins
nagiosadmin (admin) 21:49
Quicksearch
Views
Overview
Hosts
Host Groups
Services
Service Groups
Metrics
Business Intelligence
Problems
Event Console
Inventory
Other
EDIT
Bookmarks
Add Bookmark
EDIT
WATO - Configuration
Main Menu
Hosts
Host Tags
Global Settings
Host & Service Parameters
Manual Checks
Check Plugins
Host & Service Groups
Users
Roles & Permissions
Contact Groups
Notifications
Time Periods
Logfile Pattern Analyzer
BI - Business Intelligence
Distributed Monitoring
Backup & Restore
Custom Icons
Monitoring Agents
Event Console
Master Control
© Mathias Kettner
About Check_MK
Version: 1.2.8p25
Homepage
Documentation
Download
Mathias Kettner
Version information and Links to Documentation, Homepage and Download of Check_MK
WATO - Quickaccess
Access to WATO modules with only icons (saves space)
BI Aggregation Groups
A direct link to all groups of BI aggregations
Custom Links
Classical Nagios GUI
Addons
PNP4Nagios
Nagvis
Open Source Components
This snapin contains custom links which can be configured via the configuration variable custom_links in multisite.mk
Dashboards
Host & Services Problems
Main Overview
EDIT
Links to all dashboards
Host Groups
Linux Servers
Directs links to all host groups
Host Matrix
A matrix showing a colored square for each host
All Hosts
localhost
A summary state of each host with a link to the view showing its services
Event Console Performance
Event Console is not running.
Monitor the performance of the Event Console
Old Nagios GUI
Home
Documentation
General
Tactical Overview
Map
The classical sidebar of Nagios 3.2.0 with links to your local Nagios instance (no multi site support)
Nagvis Maps
{"message":"You are not authenticated","title":"EPROP","type":"error","re
denied"}
List of available NagVis maps. This only works with NagVis 1.5 and above. At the moment it is neccessary to authenticate with NagVis first by opening a NagVis map in the browser. After this the maplist should be filled.
Server Performance
Service checks: 0.01/s
Host checks: 0.00/s
External commands: 0.00/s
Livestatus-conn.: 0.02/s
Process creations: 0.10/s
New log messages: 0.00/s
Live monitor of the overall performance of all monitoring servers

En la siguiente imagen se muestra el snapin agregado en la barra lateral.



A continuación, damos clic sobre ***Classical Nagios GUI,*** y aparecerá el siguiente error. Esto debido a que no se encuentra vinculado con Nagios.



El error es debido a que 3 factores:

1. Nagios no se encuentra vinculado al site01 por lo tanto es necesario cambiar el archivo nagios.conf que se encuentra en la ruta /etc/apache2/sites-enabled/ de la siguiente manera:

```
nano /etc/apache2/sites-enabled/nagios.conf
```

Una vez dentro del archivo se debe modificar la linea *ScriptAlias /nagios/cgi-bin "/usr/local/nagios/sbin"* por:

```
ScriptAlias /site01/nagios/cgi-bin "/usr/local/nagios/sbin"
```

Como también se deba modificar la linea *Alias /nagios "/usr/local/nagios/share"* por:

```
Alias /site01/nagios "/usr/local/nagios/share"
```

2. Se debe modificar el archivo cgi.cfg ubicado en la ruta /usr/local/nagios/

```
nano /usr/local/nagios/etc/cgi.cfg
```

Una vez dentro del archivo modificamos la linea donde dice: *url_html_path=/nagios* por

```
url_html_path=/site01/nagios
```

3. Se debe modificar el archivo config.inc.php ubicado en la ruta /usr/local/nagios/share/

```
nano /usr/local/nagios/share/config.inc.php
```

Una vez dentro del archivo modificamos la linea donde dice: *$cfg['cgi_base_url']='/nagios/cgi-bin';* por:

```
$cfg['cgi_base_url']='/site01/nagios/cgi-bin';
```

Reiniciamos todos los servicios.

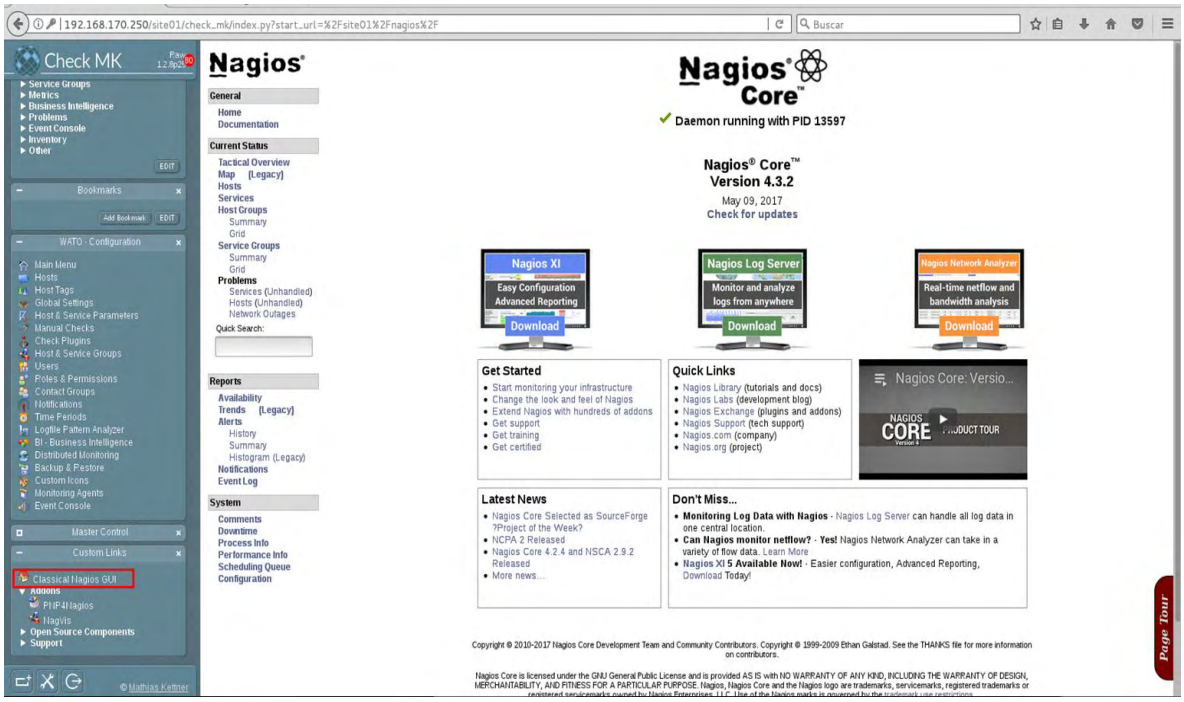
Para debian7 wheezy.

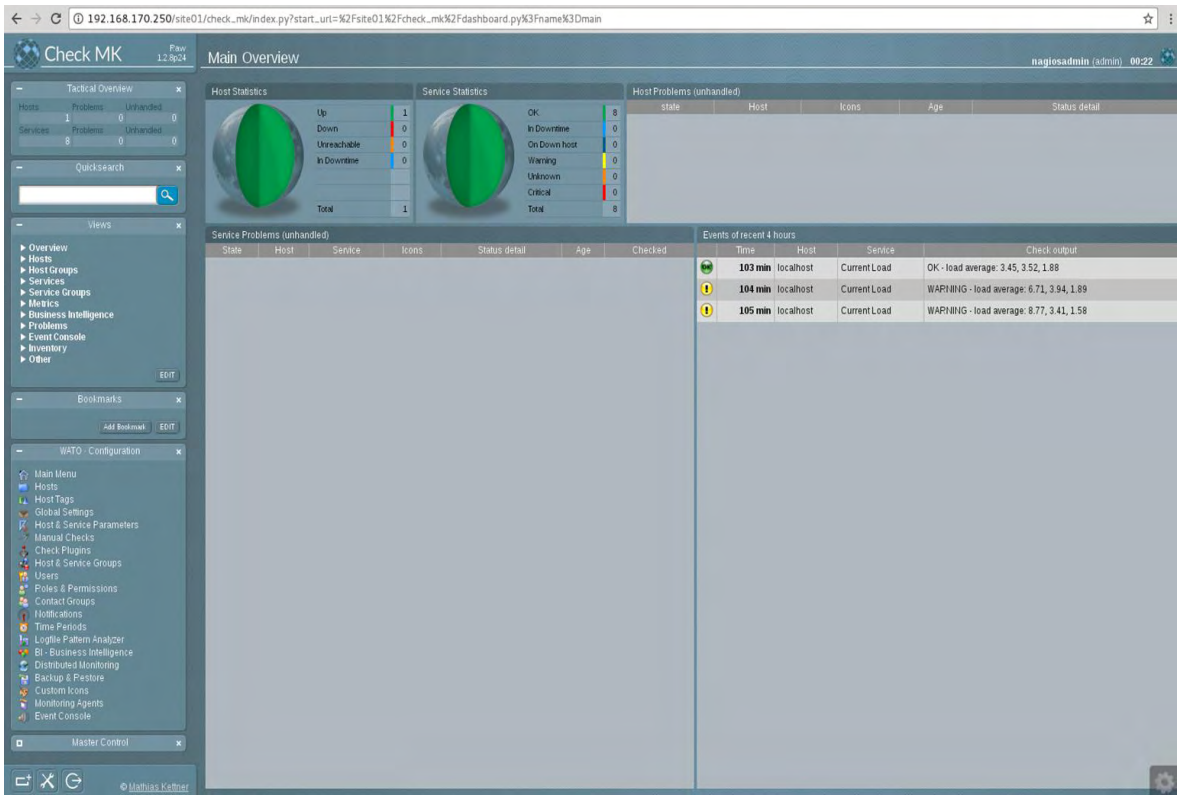
```
service mkeventd start
service apache2 restart
service nagios restart
service mkeventd restart
```

Para debian8 jessie

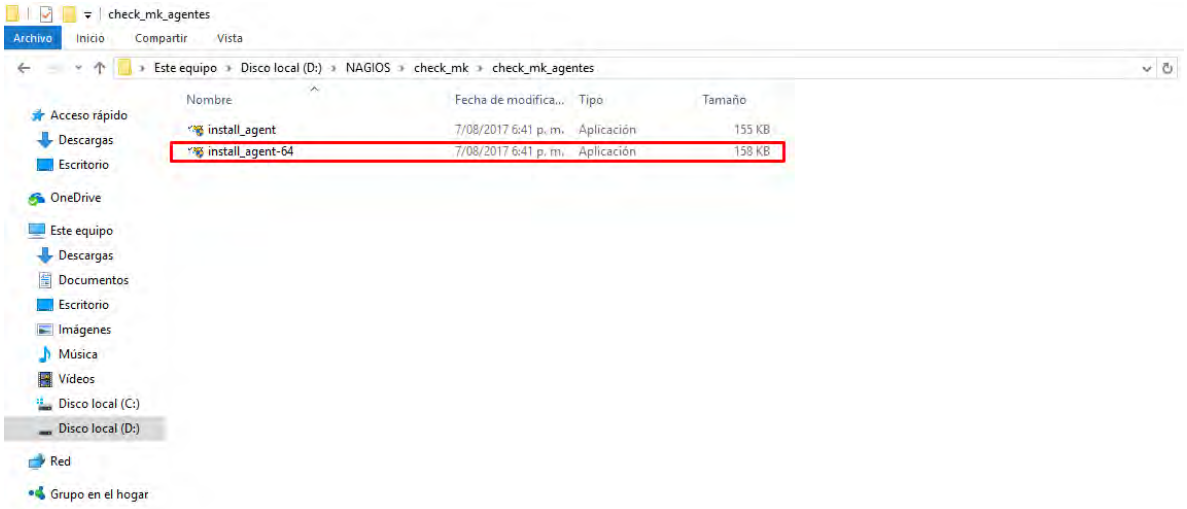
```
systemctl enable mkeventd
systemctl restart apache2
systemctl restart nagios
systemctl restart mkeventd
```

Ingresamos nuevamente a la pagina de check_mk y nos dirigimos al acceso de Nagios y debe dejarnos ingresar a la pagina de Nagios, con todas las funcionalidades de este.

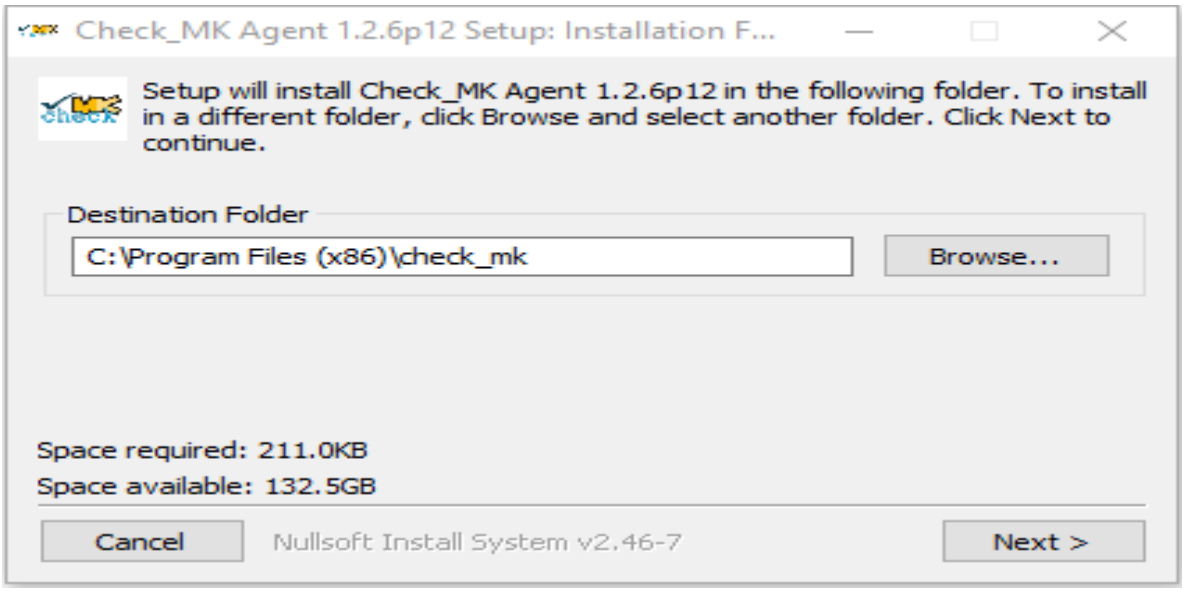

192.168.170.250/site01/check_mk/index.py?start_url=%2Fsite01%2Fnagios%2F
Buscar
Check MK
Service Groups
Metrics
Business Intelligence
Problems
Event Console
Inventory
Other
EDIT
Bookmarks
Add Bookmark
EDIT
WATO - Configuration
Main Menu
Hosts
Host Tags
Global Settings
Host & Service Parameters
Manual Checks
Check Plugins
Host & Service Groups
Users
Roles & Permissions
Contact Groups
Notifications
Time Periods
Logfile Pattern Analyzer
BI - Business Intelligence
Distributed Monitoring
Backup & Restore
Custom Icons
Monitoring Agents
Event Console
Master Control
Custom Links
Classical Nagios GUI
Addons
PNP4Nagios
NagVis
Open Source Components
Support
© Mathias Kettner
Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends (Legacy)
Alerts
History
Summary
Histogram (Legacy)
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration
Nagios Core
Daemon running with PID 13597
Nagios® Core™
Version 4.3.2
May 09, 2017
Check for updates
Nagios XI
Easy Configuration
Advanced Reporting
Download
Nagios Log Server
Monitor and analyze
logs from anywhere
Download
Nagios Network Analyzer
Real-time netflow and
bandwidth analysis
Download
Get Started
Start monitoring your infrastructure
Change the look and feel of Nagios
Extend Nagios with hundreds of addons
Get support
Get training
Get certified
Quick Links
Nagios Library (tutorials and docs)
Nagios Labs (development blog)
Nagios Exchange (plugins and addons)
Nagios Support (tech support)
Nagios.com (company)
Nagios.org (project)
Nagios Core: Versio...
NAGIOS
CORE
PRODUCT TOUR
Latest News
Nagios Core Selected as SourceForge ?Project of the Week?
NCPA 2 Released
Nagios Core 4.2.4 and NSCA 2.9.2 Released
More news...
Don't Miss...
Monitoring Log Data with Nagios - Nagios Log Server can handle all log data in one central location.
Can Nagios monitor netflow? - Yes! Nagios Network Analyzer can take in a variety of flow data. Learn More
Nagios XI 5 Available Now! - Easier configuration, Advanced Reporting, Download Today!
Copyright © 2010-2017 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors.
Nagios Core is licensed under the GNU General Public License and is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. Nagios, Nagios Core and the Nagios logo are trademarks, servicemarks, registered trademarks or
Page Tour



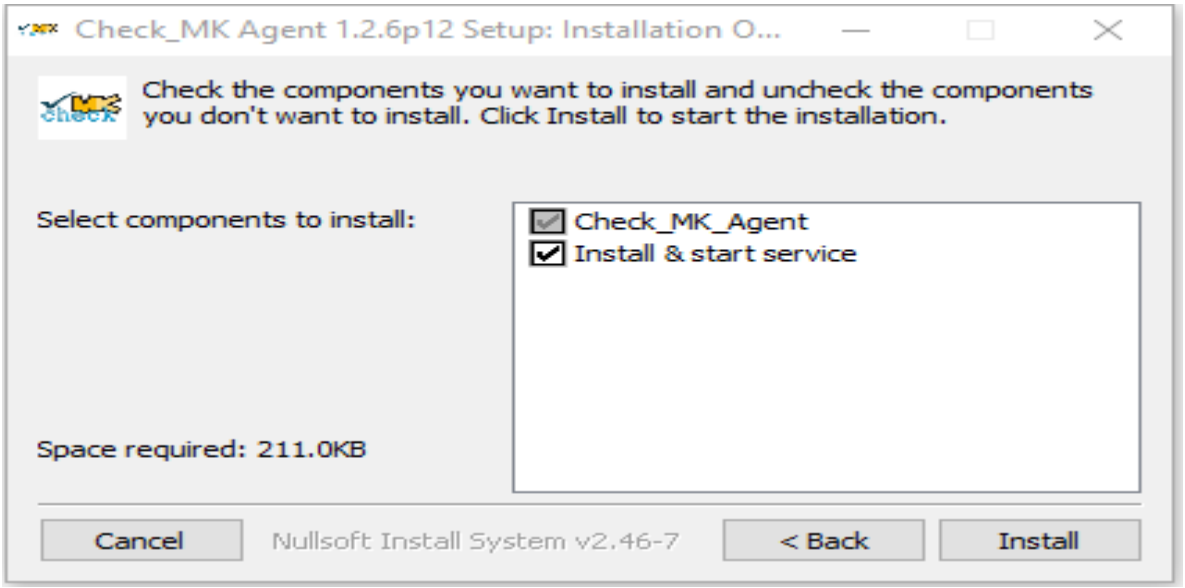
2.2.2 Instalación de Check_mk_agent en máquina Windows. Se debe ejecutar el instalador dependiendo del tipo de sistema operativo, sea 32bits o 64bits.



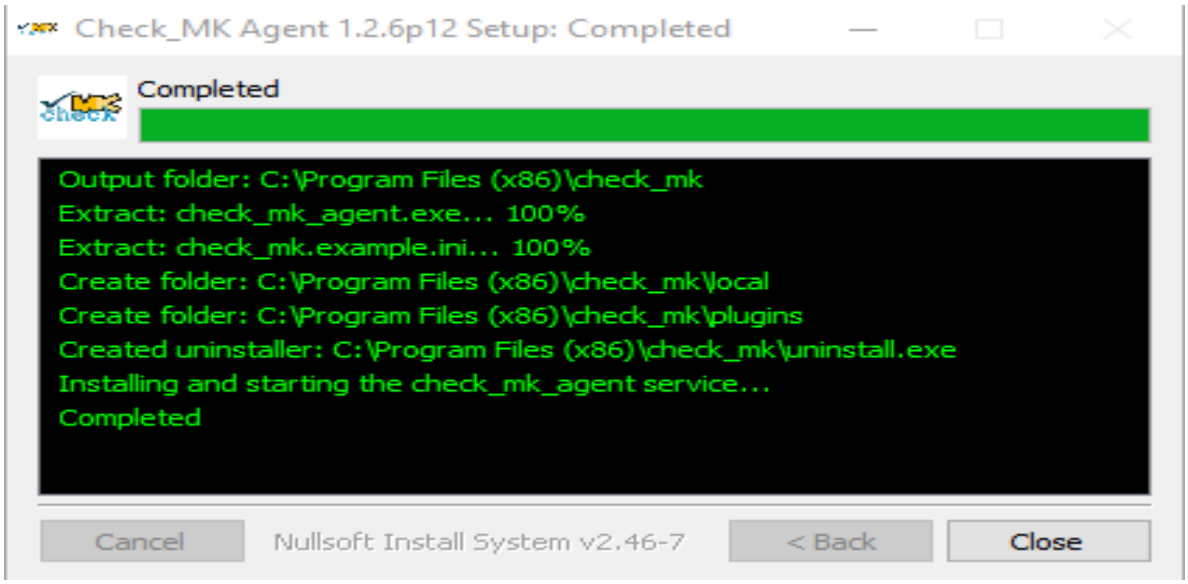
Se procede los pasos como indica el asistente de instalación.



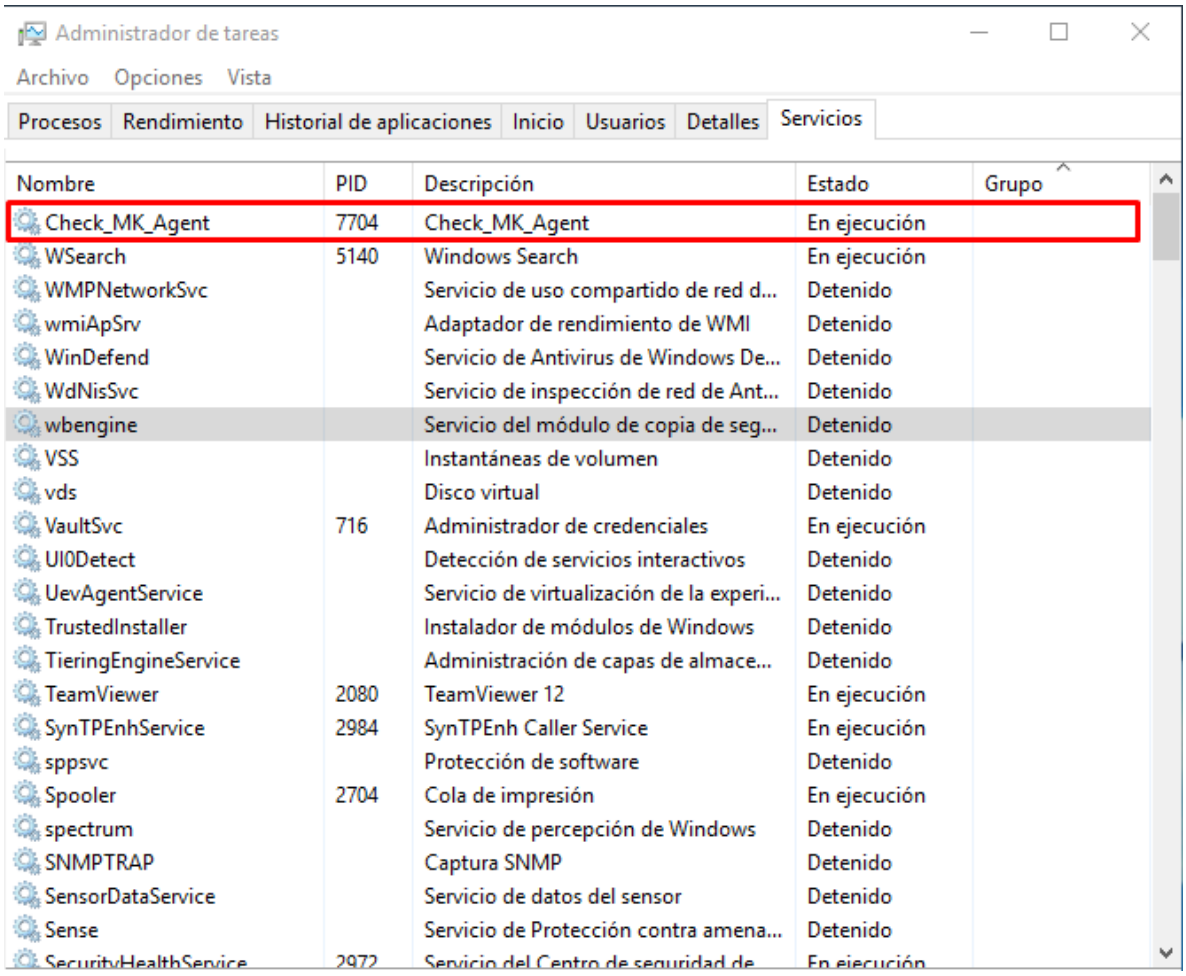
Se instala el programa cliente de monitoreo Check_MK_Agent



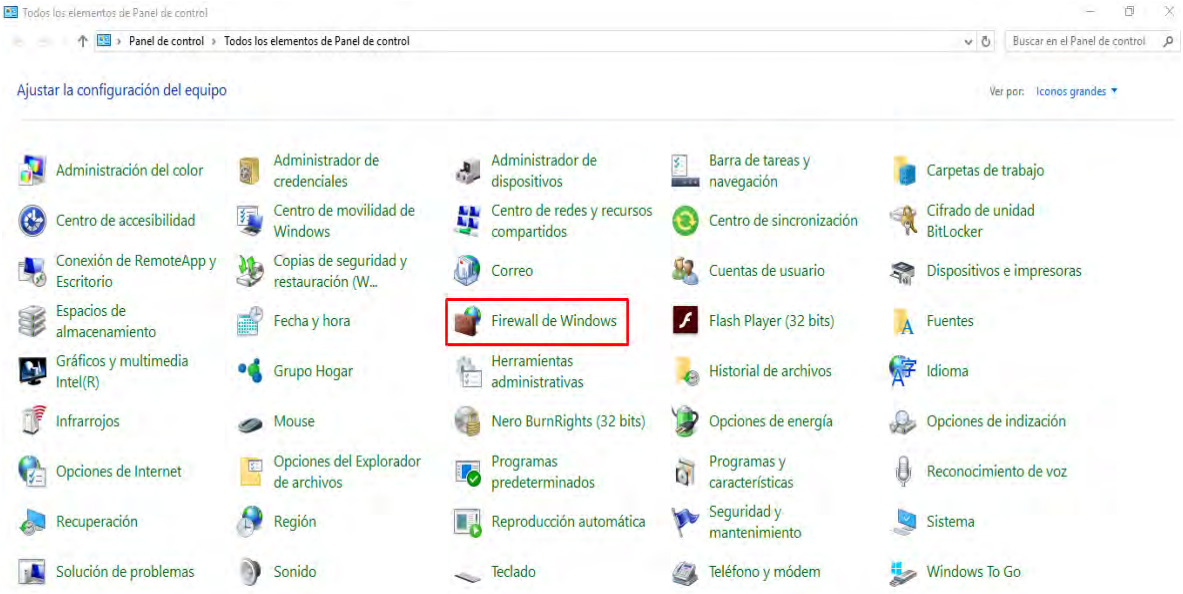
La instalación ha terminado, se cierra el asistente de instalación.



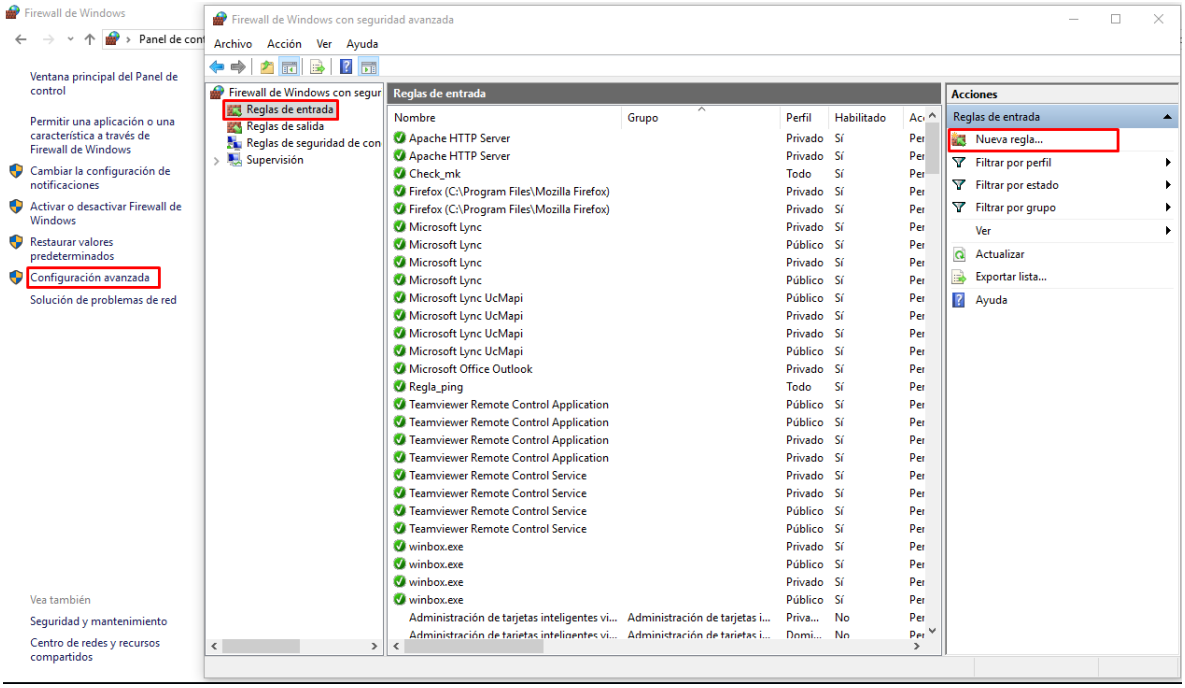
Se verifica que el servicio Check_MK_Agent esté en ejecución con el administrador de tareas.
NOTA: Para que el agente cliente se comunique con el agente servidor es necesario crear una regla de entrada en el Firewall de Windows.



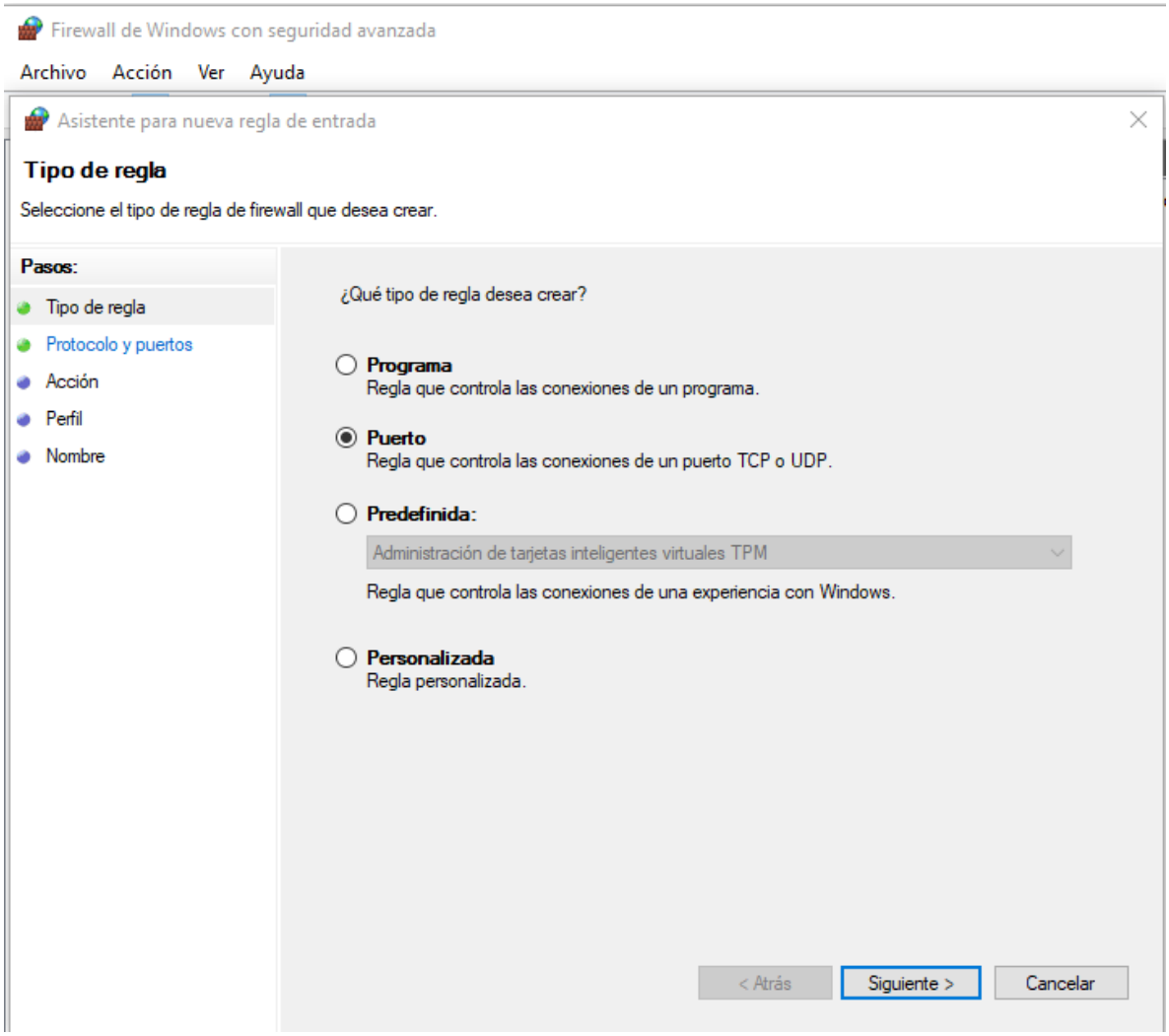
Se abre la configuración del Firewall de Windows en el panel de control.



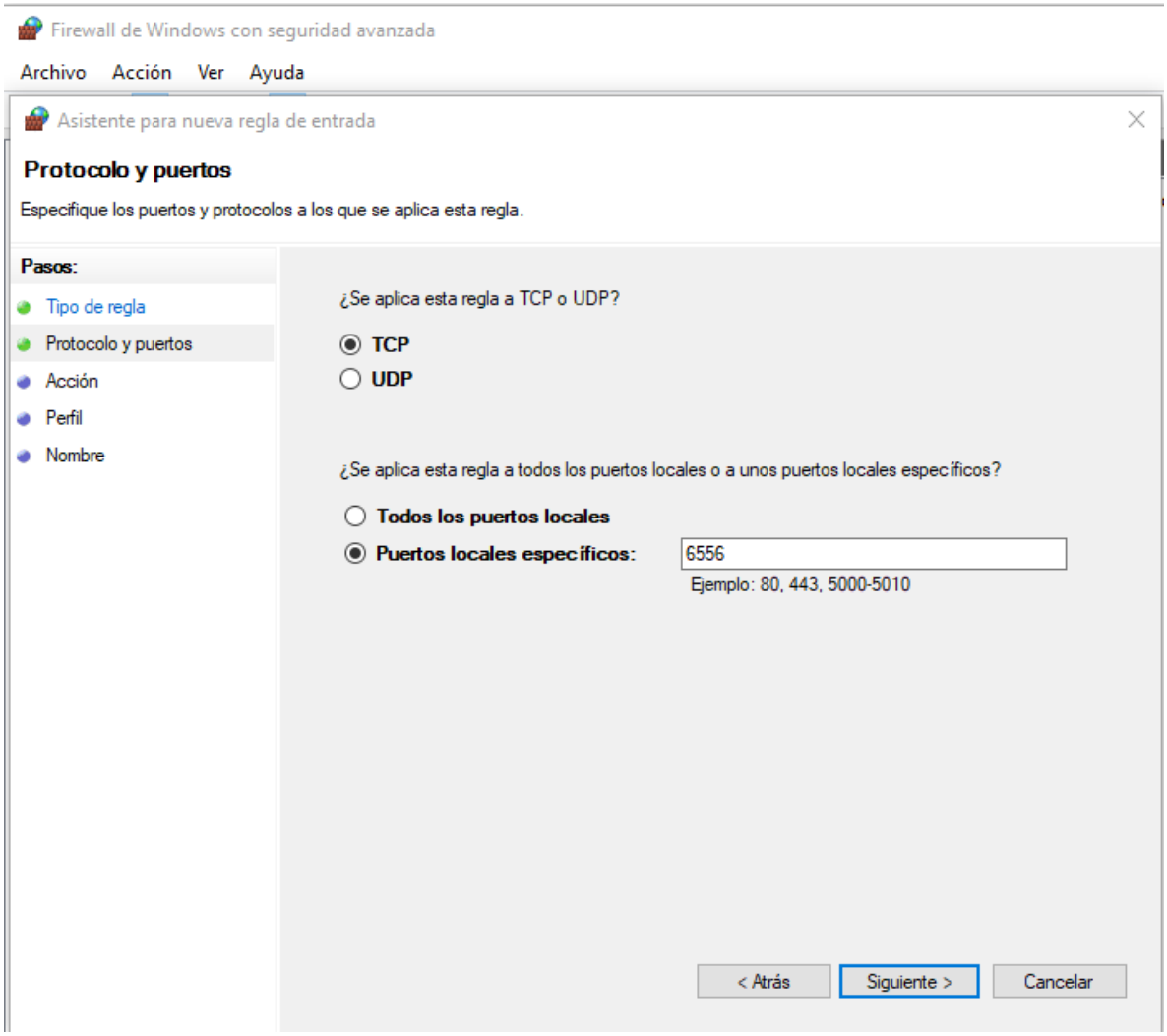
Se crea una nueva regla de entrada en la configuración avanzada.



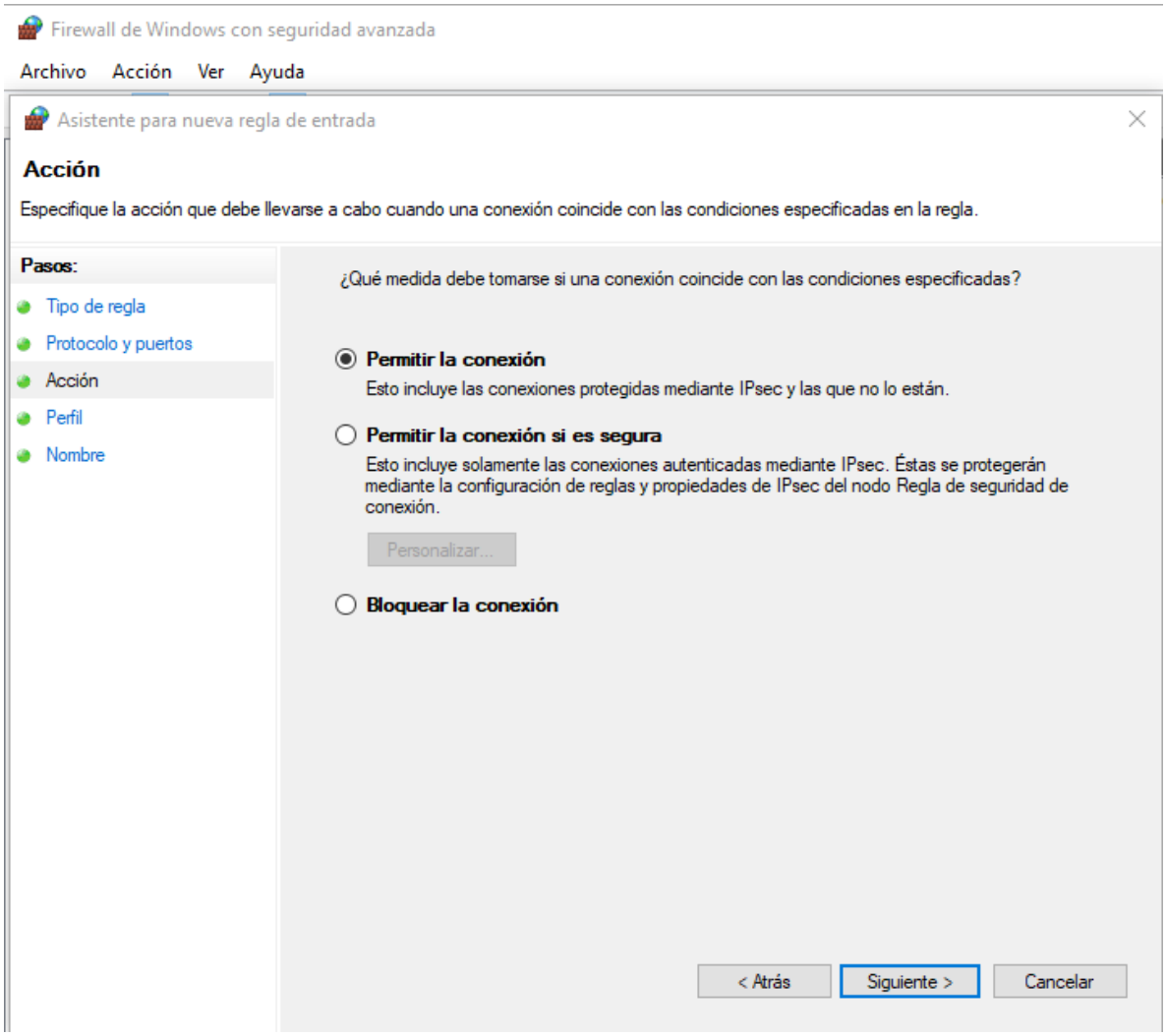
La regla será de tipo puerto.



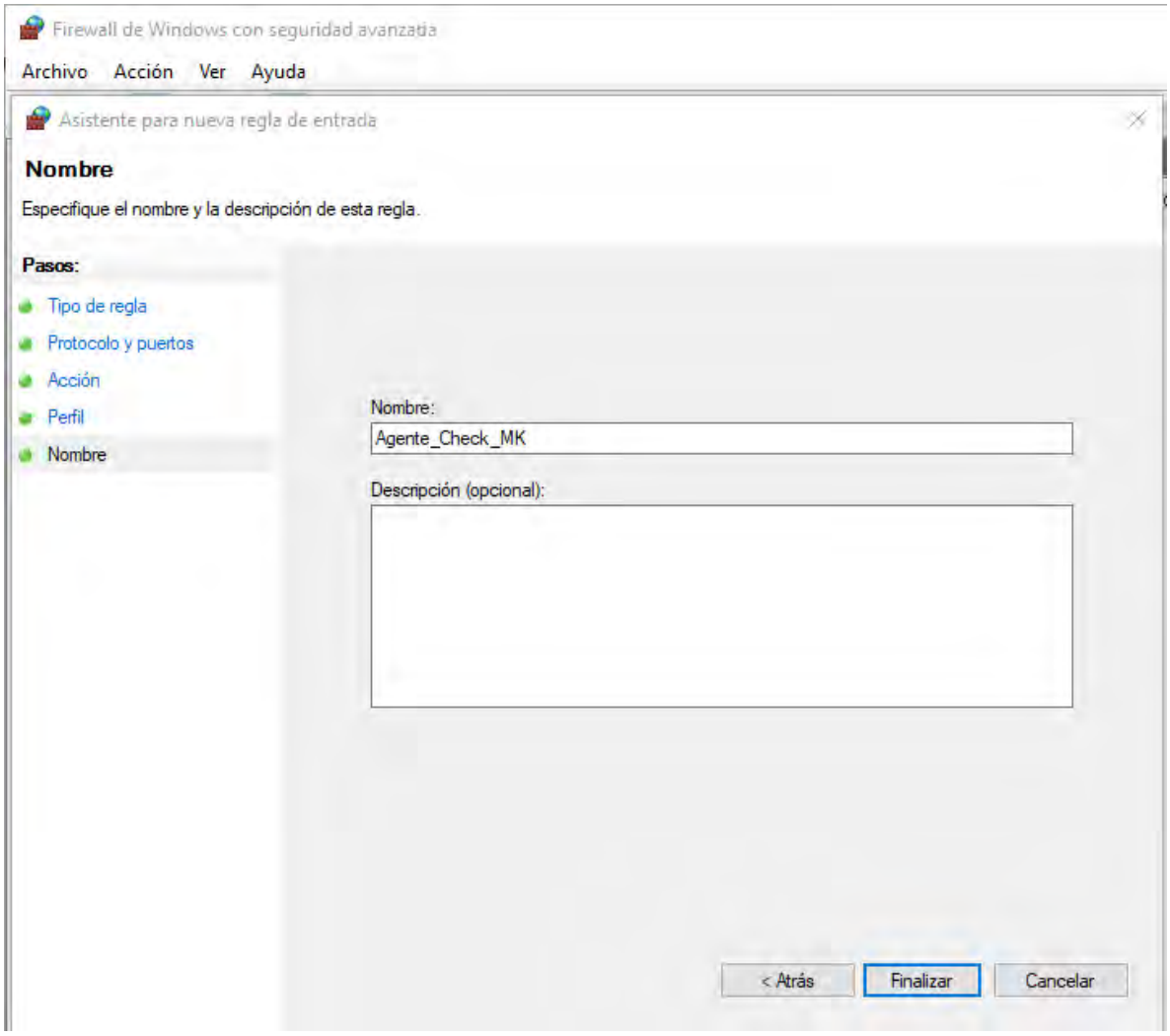
El puerto por donde escucha el agente cliente es 6556 con conexión TCP.



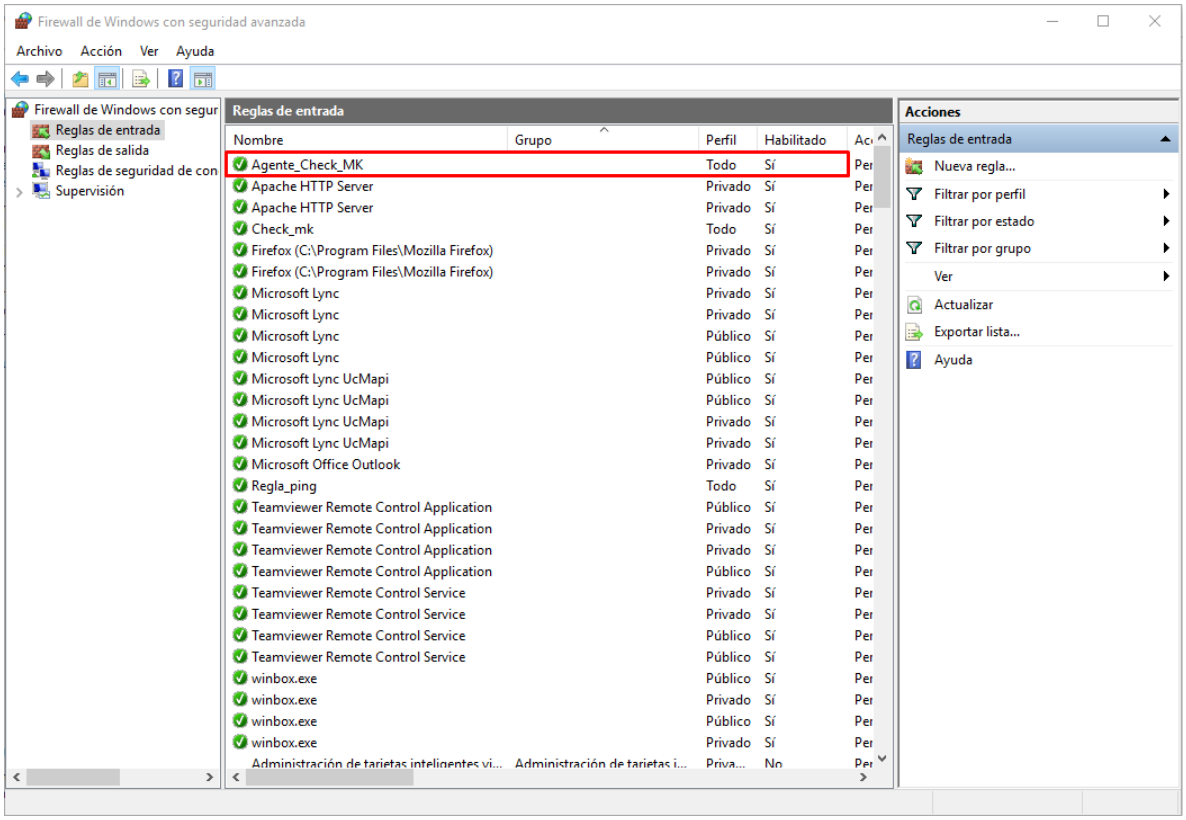
Se permite la conexión en la regla que se está creando.



Se da un nombre específico a la regla para poder identificarla. Se hace una conexión pública.



Se verifica que la regla está creada y habilitada.
Así termina el proceso de instalación del Agente de Check_MK para poder monitorear cualquier equipo Windows.



2.2.3 Instalación de check_mk_agent en máquina Linux. En la siguiente ruta se encuentra el agente “check-mk-agent_1.2.8p25-1_all.deb” que será instalado en las maquinas Linux para poder ser monitoreadas mediante check_mk.

```
cd /usr/share/check_mk/
```

Con el comando “ls” nos mostrara el contenido del directorio check_mk.

```
ls
```

Mostrará lo siguiente:

```
root@debian1205:/usr/share/check_mk/agents# ls
cfg_examples                      check_mk_agent.freebsd  check_mk_agent.netbsd   check-mk-agent.spec           mk-job.solaris  waitmax
check-mk-agent_1.2.8p25-1_all.deb check_mk_agent.hpux     check_mk_agent.openbsd  check_mk_caching_agent.linux  plugins         waitmax.c
check-mk-agent-1.2.8p25-1.noarch.rpm check_mk_agent.linux  check_mk_agent.openvms  CONTENTS                      sap             windows
check_mk_agent.aix                check_mk_agent.macosx   check_mk_agent.solaris  mk-job                        special         z_os
root@debian1205:/usr/share/check_mk/agents#
```

Antes de instalar el agente se debe instalar el paquete “xinetd” con el siguiente comando:

```
apt-get install xinetd
```

Luego se procede a instalar el agente con extensión “.deb” de la siguiente manera:

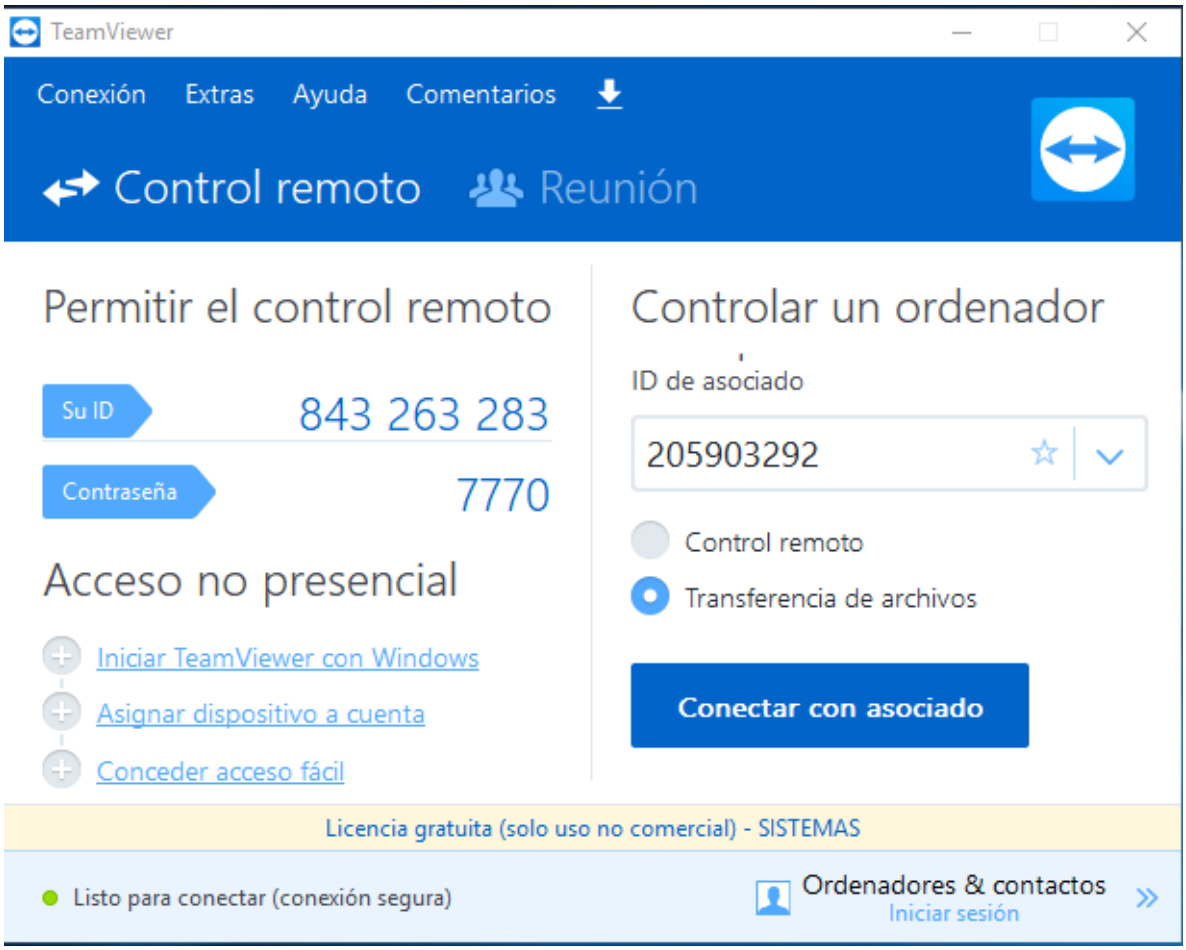
```
dpkg -i check-mk-agent_1.2.8p25-1_all.deb
```

Después de la instalación debe mostrar lo siguiente:

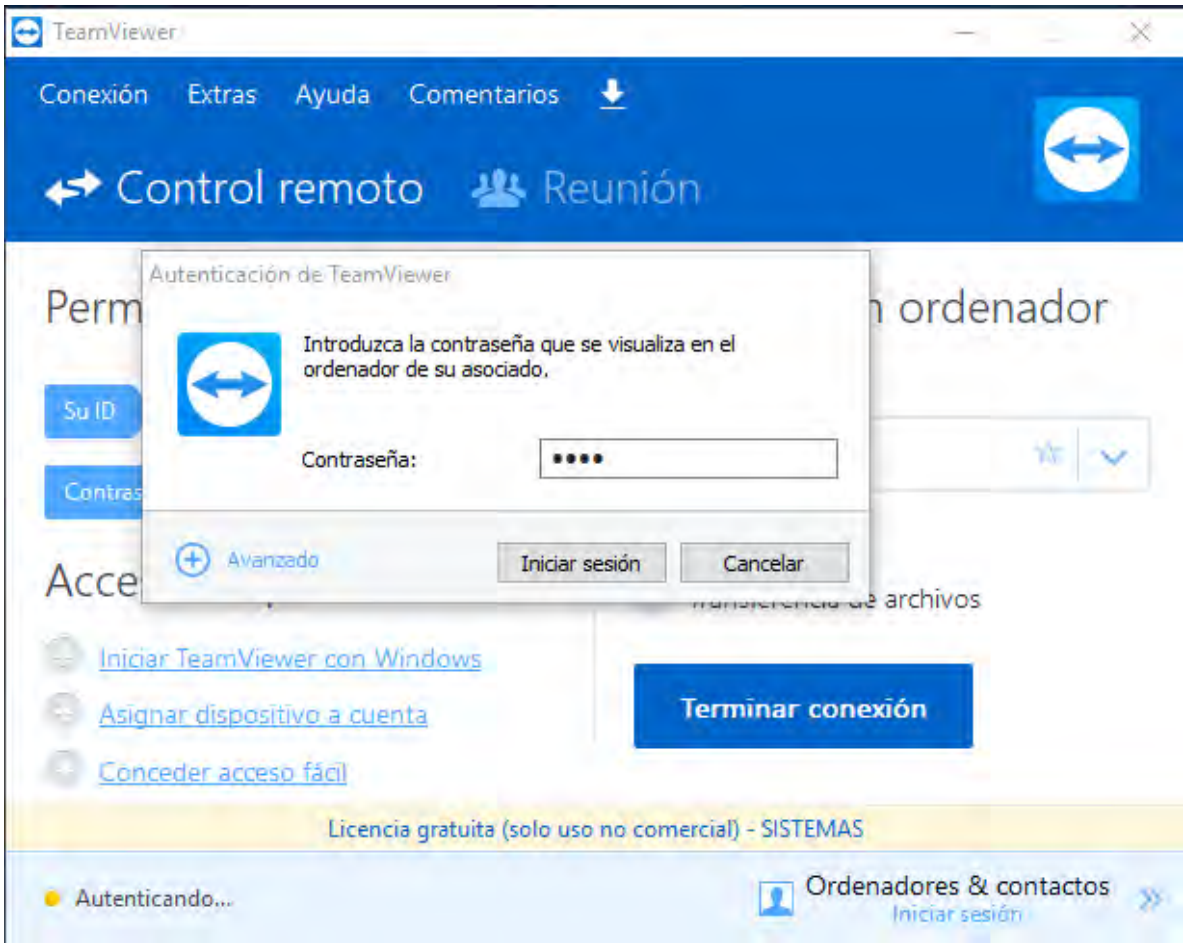
```
root@debian1205:/usr/share/check_mk/agents# dpkg -i check-mk-agent_1.2.8p25-1_all.deb
(Leyendo la base de datos ... 203578 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar check-mk-agent_1.2.8p25-1_all.deb ...
Desempaquetando check-mk-agent (1.2.8p25-1) sobre (1.2.8p25-1) ...
Reloading xinetd...
[ ok ] Reloading xinetd configuration (via systemctl): xinetd.service.
Configurando check-mk-agent (1.2.8p25-1) ...
Reloading xinetd...
[ ok ] Reloading xinetd configuration (via systemctl): xinetd.service.
root@debian1205:/usr/share/check_mk/agents#
```

2.2.4 Instalación de check_mk_agent en máquina remota Windows

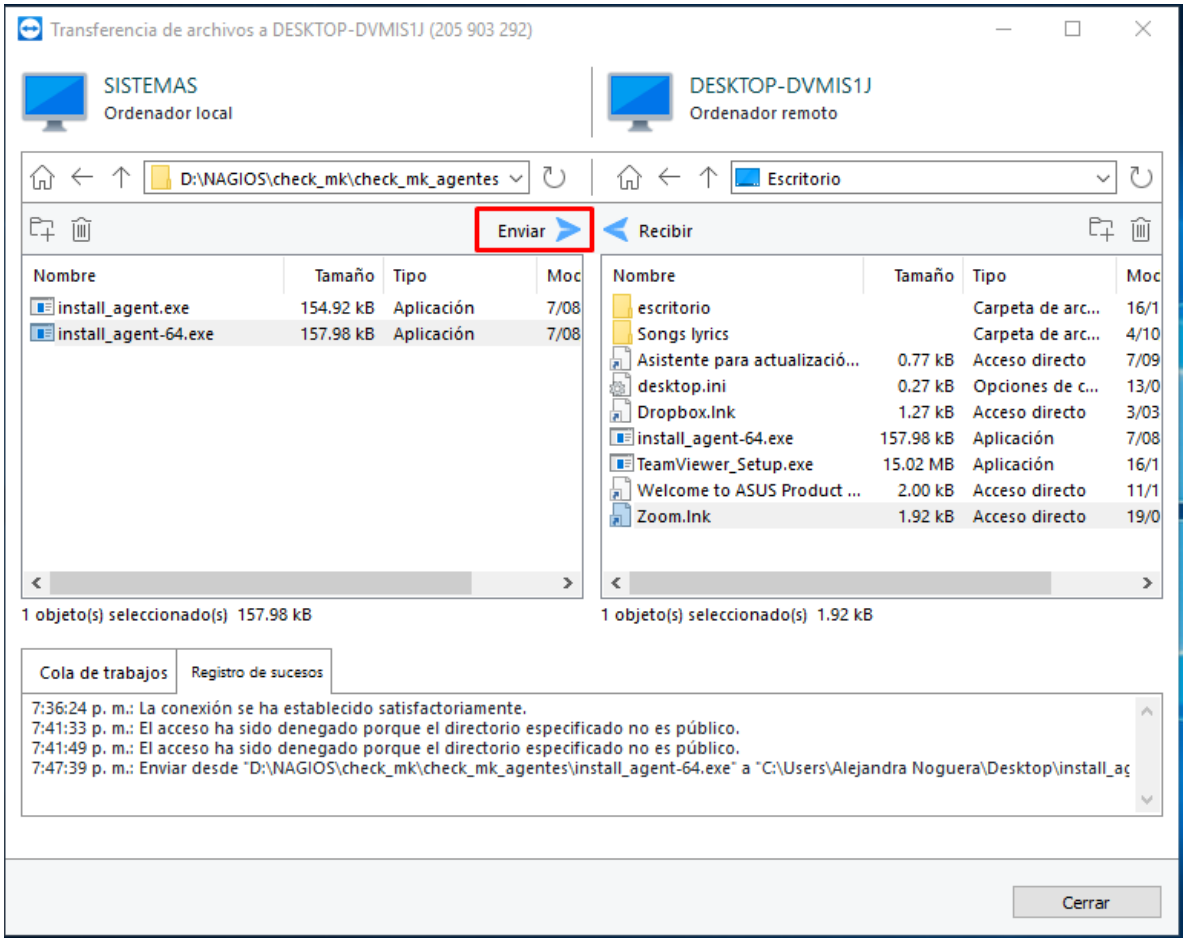
Se abre el programa de control remoto en este caso se utilizo la herramienta TeamViewer12 que se encuentra instalado en el computador principal del jefe del área de sistemas. Para enviar el instalador del agente cliente Check_MK_Agent, mediante la opción **Transferencia de archivos**. Se procede a conectarse con el asociando remoto.


TeamViewer
Conexión
Extras
Ayuda
Comentarios
Control remoto
Reunión
Permitir el control remoto
Su ID
843 263 283
Contraseña
7770
Acceso no presencial
Iniciar TeamViewer con Windows
Asignar dispositivo a cuenta
Conceder acceso fácil
Controlar un ordenador
ID de asociado
205903292
Control remoto
Transferencia de archivos
Conectar con asociado
Licencia gratuita (solo uso no comercial) - SISTEMAS
Listo para conectar (conexión segura)
Ordenadores & contactos
Iniciar sesión

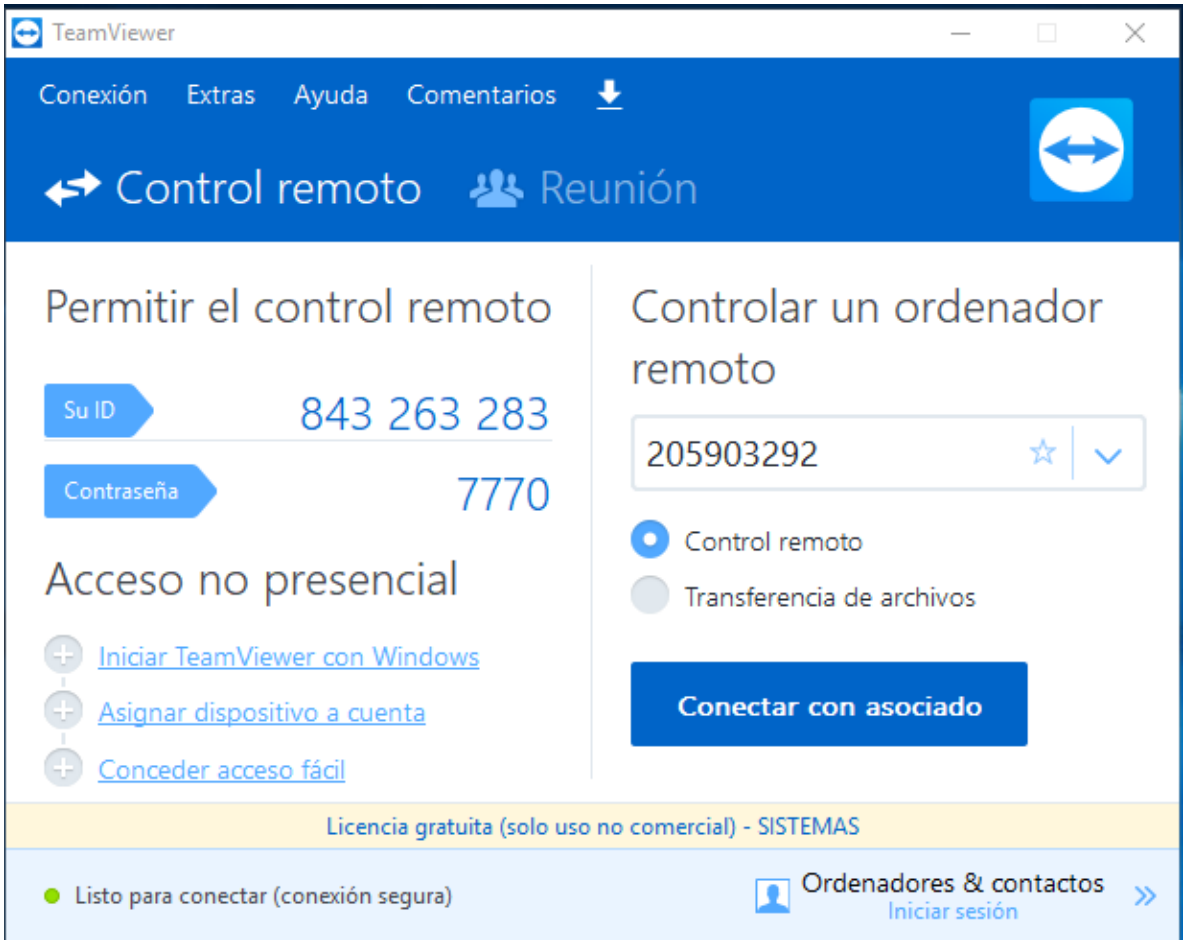
Se introduce la contraseña para establecer la conexión.



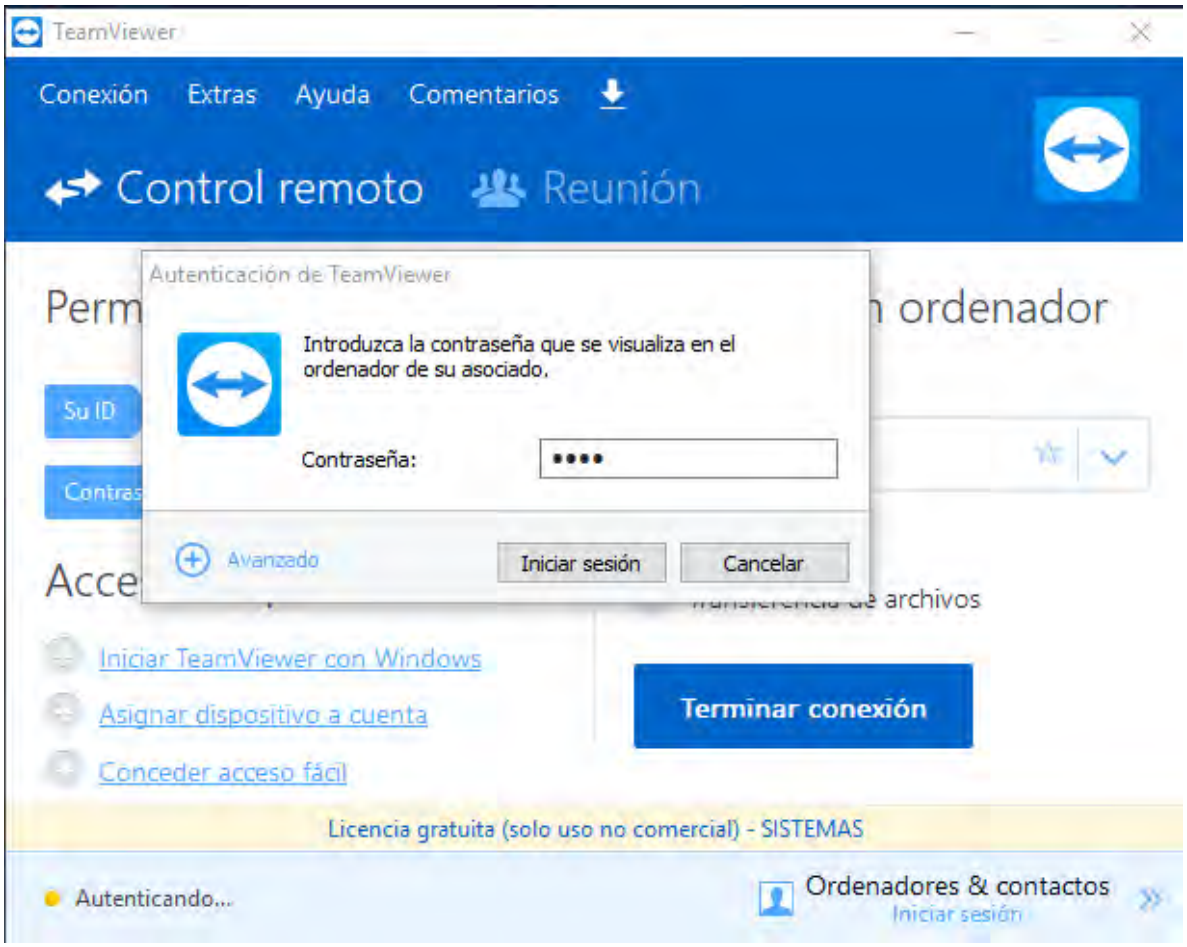
Se selecciona el archivo a enviar en el equipo local y se elige la ruta donde se recibirá el archivo en el equipo remoto y se da enviar.



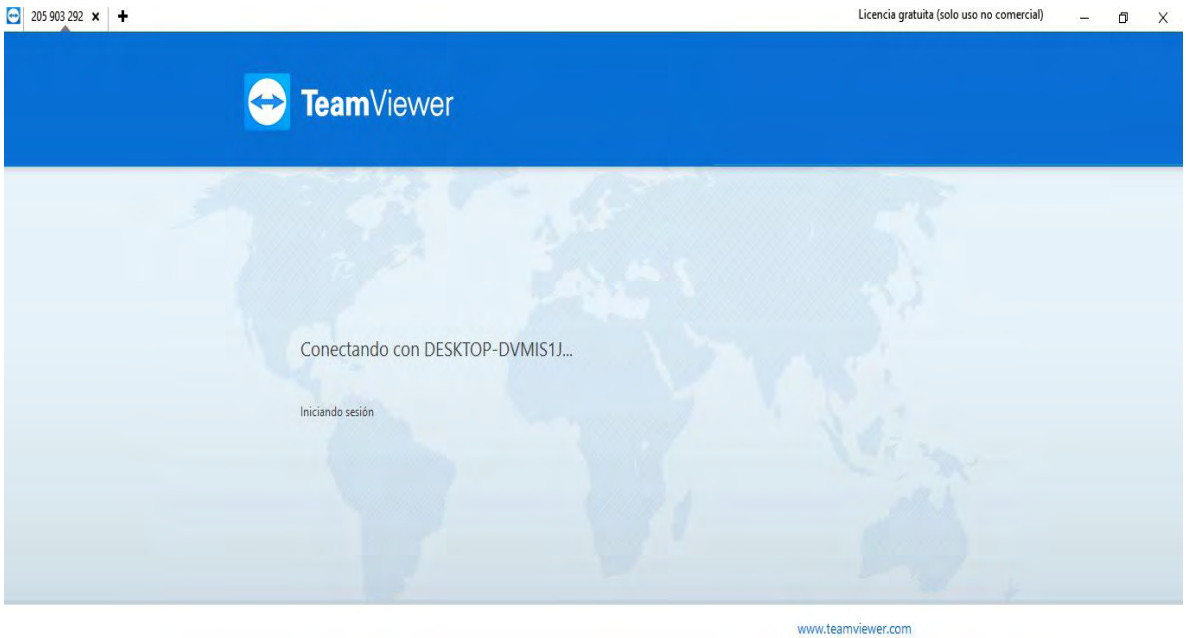
Luego de enviar el archivo, se elige la opción **Control remoto** para tener el control del asociado e instalar el agente cliente.



Se introduce la contraseña para establecer la conexión.



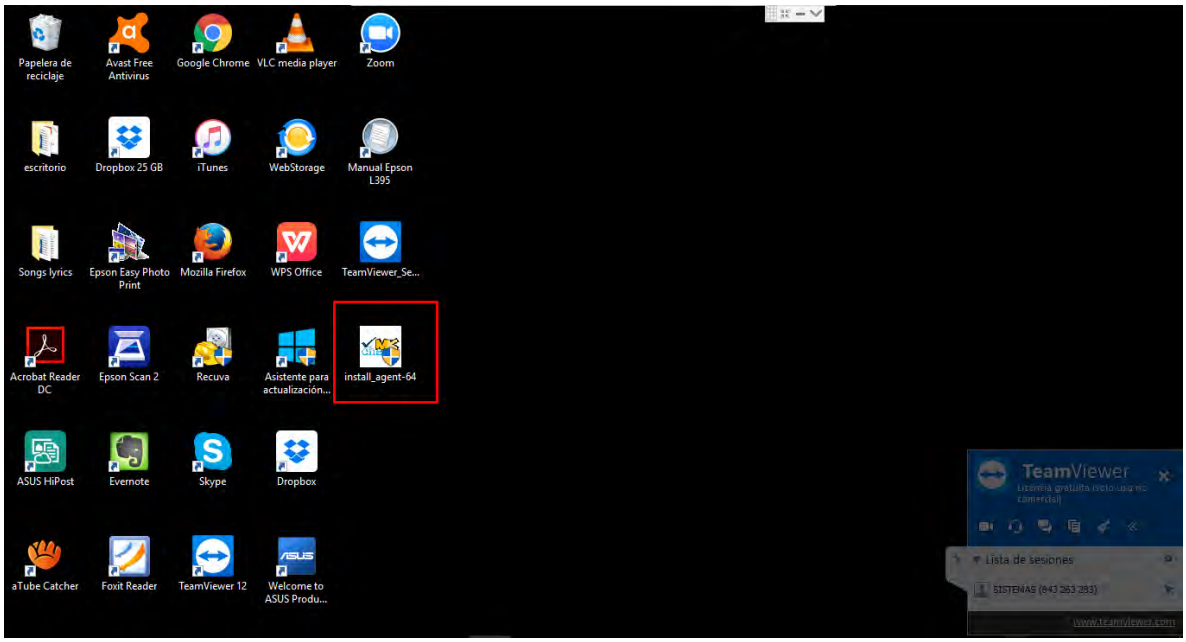
Aparecerá algo como lo siguiente y se establece la conexión remota.



Se muestra el escritorio del equipo remoto y el instalador a ejecutar.

NOTA: Luego se siguen los pasos realizados en el punto 18.2.2.4 ***INSTALACION DE AGENTE CLIENTE CHECK_MK EN EQUIPO WINDOWS.***

Este metodo de conexión remota se utilizó para instalar el agente cliente en los equipos remotos de las sedes Tumaco, Mocoa, Popayan, Yumbo y Cali.



2.3 INSTALACIÓN Y CONFIGURACIÓN DE NAGVIS

Se lo puede descargar directamente desde (http://www.nagvis.org/downloads), para más información visitar el sitio web (http://docs.nagvis.org/1.9/en_US/index.html).

Para la descarga colocamos el siguiente comando.

```
wget -O /tmp/nagvis-1.9.2.tar.gz http://www.nagvis.org/share/nagvis-1.9.2.tar.gz
```

- Prerequisitos

Instalamos algunas dependencias para gráficos.

```
apt-get install rsync php5-common libapache2-mod-php5 php5-cli php-gettext php5-cgi graphviz sqlite sqlite3 php5-sqlite libjson-xs-perl
```

- Instalación de Nagvis

```
cd /tmp/
tar xvzf nagvis-1.9.2.tar.gz
cd nagvis-1.9.2
./install.sh -W /site01/nagvis -w /etc/apache2/sites-enabled
```

Saldrá un mensaje de vienvenida como el siguiente.

```
+------------------------------------------------------------------------------+
| Welcome to NagVis Installer 1.9.2
+------------------------------------------------------------------------------+
| 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]: y
```

Dejamos toda la opción por defecto.

Al finalizar la instalación aparecerá lo siguiente.

```
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/nagios -p /usr/local/nagvis -l
"unix:/usr/local/nagios/var/rw/live" -b mklivestatus -u www-data -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/nagvis/etc/nagvis.ini.php
| - Configure NagVis via browser
|   <http://localhost/site01/nagvis/config.php>
| - Initial admin credentials:
|     Username: admin
|     Password: admin
```

Una vez que terminemos la instalación, tenemos que modificar el archivo de configuración de Apache para debian7 wheezy se encuentra en la ruta /etc/apache2/conf.d/nagvis.conf y en debian8 jessie en la ruta /etc/apache2/conf-available/nagvis.conf , cual sea el caso se debe modificar de la siguiente manera.

```
<Directory "/usr/local/nagvis/share">
Require all granted
Options FollowSymLinks
AllowOverride None
#Order allow,deny
#Allow from all
```

Ahora habilitamos la configuración de Nagvis y reiniciamos Apache.

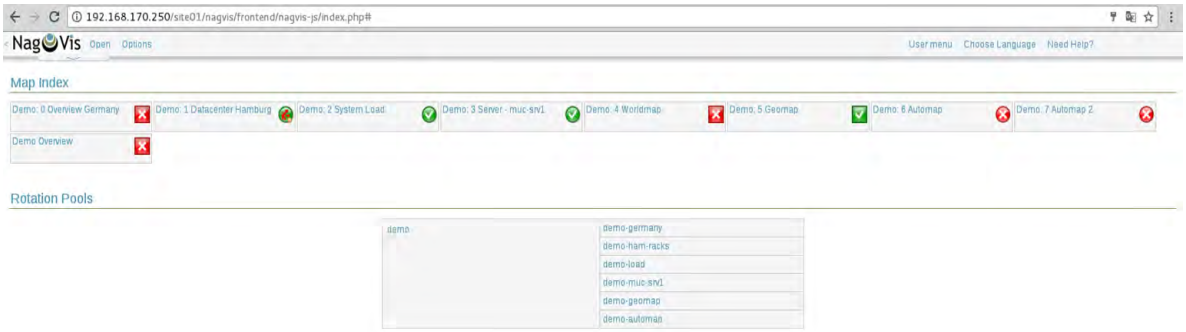
Para debian7 wheezy

```
ln -s /etc/apache2/conf.d/nagvis.conf /etc/apache2/sites-enabled/nagvis.conf
service apache2 restart
```

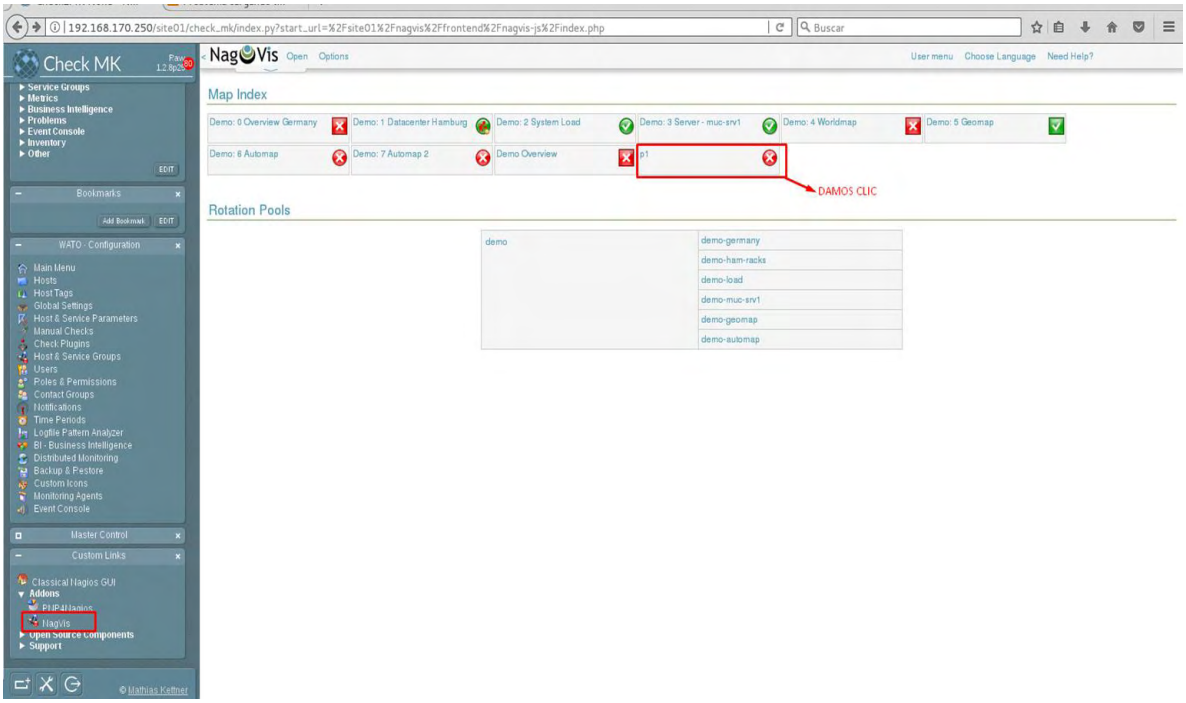
Para debian8 jessie

ln -s /etc/apache2/conf-available/nagvis.conf /etc/apache2/sites-enabled/nagvis.conf
systemctl restart apache2.service

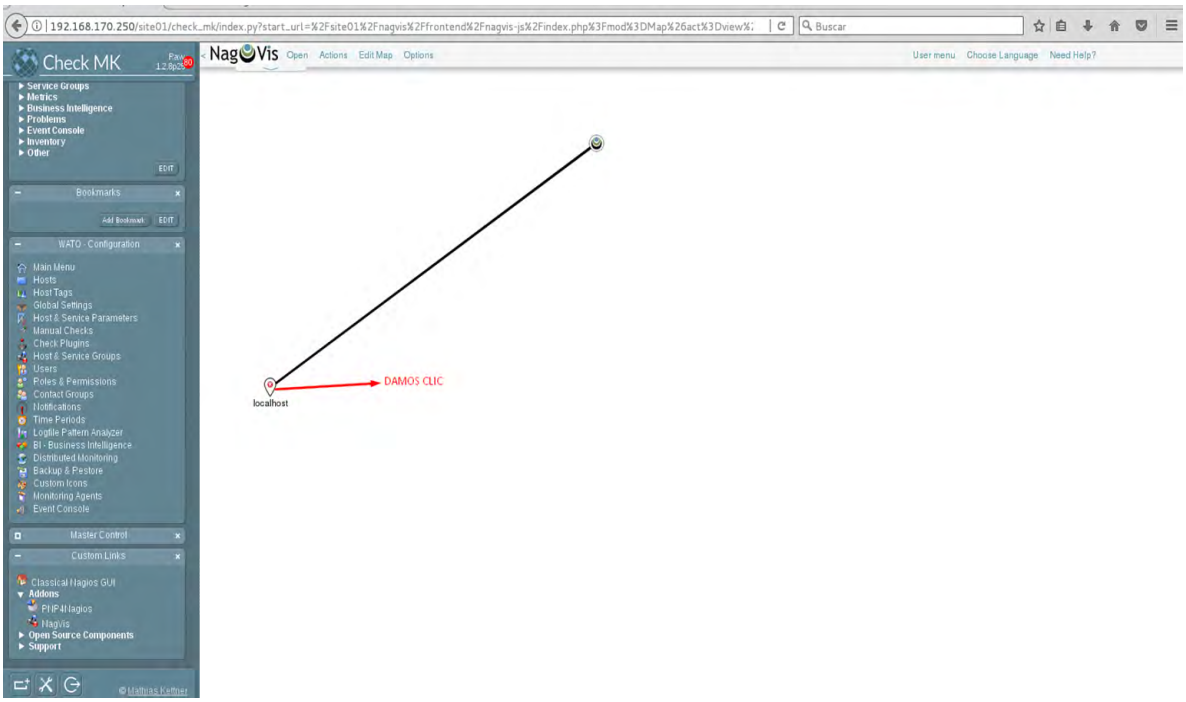
Y finalmente podemos acceder a Nagvis: http://nagios-server-ip/site01/nagvis (admin / admin por defecto, deberíamos cambiarlo en la primera entrada)
Encontraremos una gran cantidad de gráficos en ella. Para hacer un nuevo comienzo debemos eliminarlos a través del menú "Manage Map".



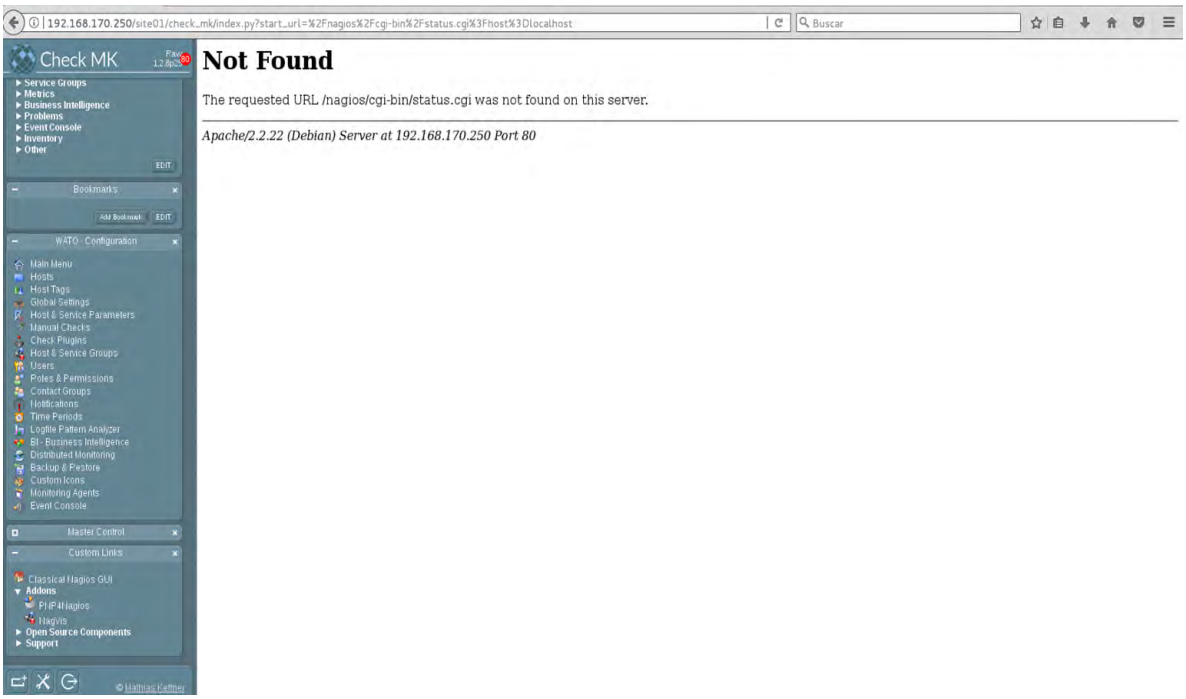
2.3.1 Vinculación de ingreso desde Nagvis a Nagios. Al ingresar a Nagvis, (previamente se creó un mapa básico en este caso llamado p1), damos clic sobre el mapa p1.



Nos mostrara el mapa creado, damos clic sobre el icono que representa en este caso a localhos.



Aparecerá el siguiente error.



El anterior error es debido a que se cambió la ruta /site01/ nagios en el archivo nagios.conf, esto afecta el vínculo de la nagvis con nagios.

Por lo tanto, se debe modficar el archivo nagvis.ini.php que se encuentra en la ruta /usr/local/nagvis/etc/

```
nano /usr/local/nagvis/etc/nagvis.ini.php
```

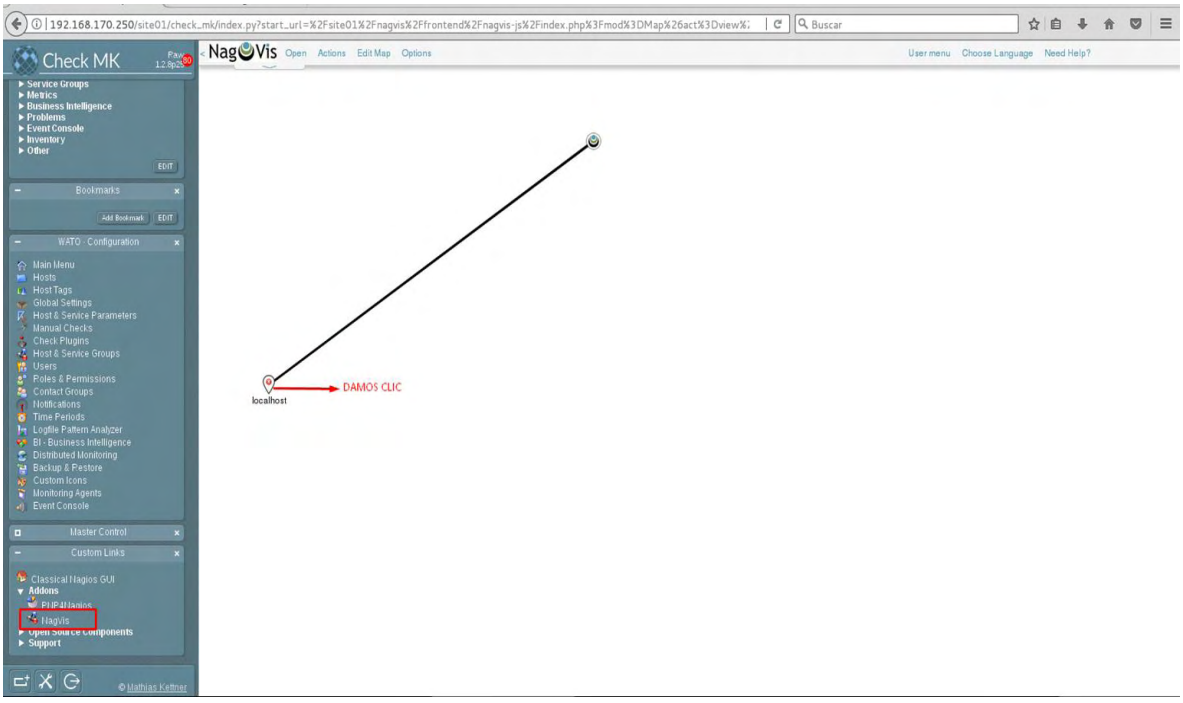
Una vez dentro del archivo modifcamos y descomentamos las siguiente linea. *;htmlcgi="/nagios/cgi-bin" por :*

```
; absolute html NagVis cgi path
htmlcgi="/site01/nagios/cgi-bin"
```

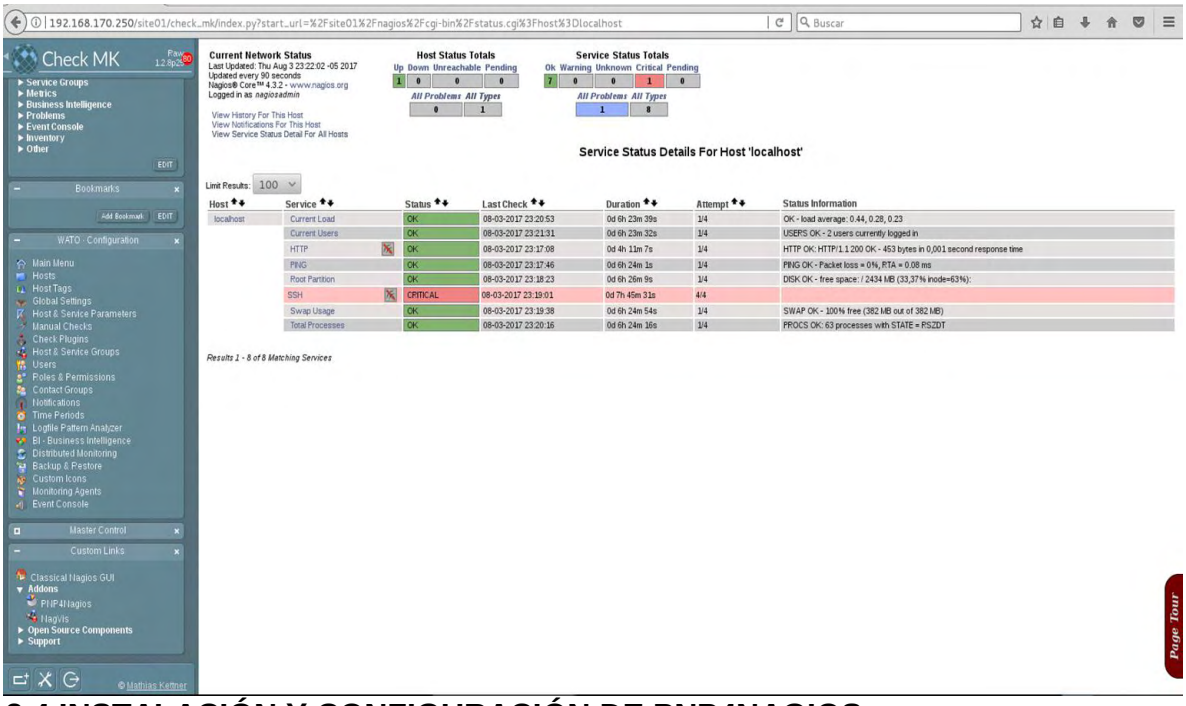
;htmlcgi="/nagios/cgi-bin" por:

```
; path to the cgi-bin of this backend
htmlcgi="/site01/nagios/cgi-bin"
```

Ingresamos nuevamente a Nagvis y nos dirigimos al mapa previamente creado y verificamos que ya se tiene la vinculación con Nagios



Mostrando los servicios que el host tiene configurado.



2.4 INSTALACIÓN Y CONFIGURACIÓN DE PNP4NAGIOS

- Descarga de software

Se lo puede descargar directamente desde (https://sourceforge.net/projects/pnp4nagios/), para mas informacion visitar el sitio web (https://docs.pnp4nagios.org/pnp-0.6/about#download), como sitio web sugerido (https://github.com/hashnao/pnp4nagios/tree/master/templates).

Para la descarga colocamos el siguiente comando.

```
wget -O /tmp/pnp4nagios-0.6.25.tar.gz
https://sourceforge.net/projects/pnp4nagios/files/latest/download
```

- Prerequisitos

Se debe instalar algunas dependencias para los gráficos.

```
apt-get install php5-gd librrds-perl rrdtool
```

- Instalación de PNP4Nagios

Ir al directorio donde se lo descargo (/tmp/), luego lo extraemos utilizado el comando.

```
cd /tmp/
tar zxfv pnp4nagios-0.6.25.tar.gz
```

Una vez extraido nos situamos en él.

```
cd pnp4nagios-0.6.25/
```

Luego colocamos los siguientes comandos.

```
./configure --with-httpd-conf=/etc/apache2/sites-enabled --
sysconfdir=/usr/local/pnp4nagios --with-base-url=/site01/pnp4nagios
```

Al final aparecerá lo siguiente.

```
*** Configuration summary for pnp4nagios-0.6.25 03-01-2015 ***

 General Options:
 ------------------------        -------------------
 Nagios user/group:                nagios nagios
 Install directory:              /usr/local/pnp4nagios
 HTML Dir:                       /usr/local/pnp4nagios/share
 Config Dir:                    /usr/local/pnp4nagios
 Location of rrdtool binary:       /usr/bin/rrdtool Version 1.4.8
 RRDs Perl Modules:                FOUND (Version 1.4008)
 RRD Files stored in:             /usr/local/pnp4nagios/var/perfdata
 process_perfdata.pl Logfile:      /usr/local/pnp4nagios/var/perfdata.log
 Perfdata files (NPCD) stored in:  /usr/local/pnp4nagios/var/spool

 Web Interface Options:
 ------------------------        -------------------
 HTML URL:                      http://localhost/site01/pnp4nagios
 Apache Config File:              /etc/apache2/sites-enabled/pnp4nagios.conf


 Review the options above for accuracy.  If they look okay,
 type 'make all' to compile.
```

Luego colocamos el siguiente comando.

```
make all
```

Al final aparecerá lo siguiente.

```
*** Compile finished ***

  make install
    - This installs the main program and HTML files

  make fullinstall
    - This installs the main program, runlevel scripts, config and HTML files

Enjoy.
```

Colocamos el siguiente comando.

```
make fullinstall
```

Al final aparecerá lo siguiente.

```
*** Configuration summary for pnp4nagios-0.6.25 03-01-2015 ***

  General Options:
  -------------------------       -------------------
  Nagios user/group:                nagios nagios
  Install directory:              /usr/local/pnp4nagios
  HTML Dir:                       /usr/local/pnp4nagios/share
  Config Dir:                    /usr/local/pnp4nagios
  Location of rrdtool binary:       /usr/bin/rrdtool Version 1.4.8
  RRDs Perl Modules:                FOUND (Version 1.4008)
  RRD Files stored in:             /usr/local/pnp4nagios/var/perfdata
  process_perfdata.pl Logfile:      /usr/local/pnp4nagios/var/perfdata.log
  Perfdata files (NPCD) stored in:  /usr/local/pnp4nagios/var/spool

  Web Interface Options:
  -------------------------       -------------------
  HTML URL:                       http://localhost/site01/pnp4nagios
  Apache Config File:               /etc/apache2/sites-enabled/pnp4nagios.conf



*** Main program, Scripts and HTML files installed ***
```

```
Enjoy.
```

Editamos el archivo Apache /etc/apache2/sites-enabled/pnp4nagios.conf y establecemos el PATH correcto para AuthUserFile y cambiamos AuthType Basic.

Ingresamos el siguiente comando.

```
nano /etc/apache2/sites-enabled/pnp4nagios.conf
```

```
AuthUserFile /usr/local/nagios/etc/htpasswd.users
```

Ahora reiniciamos Apache.

Para debian7 wheezy.

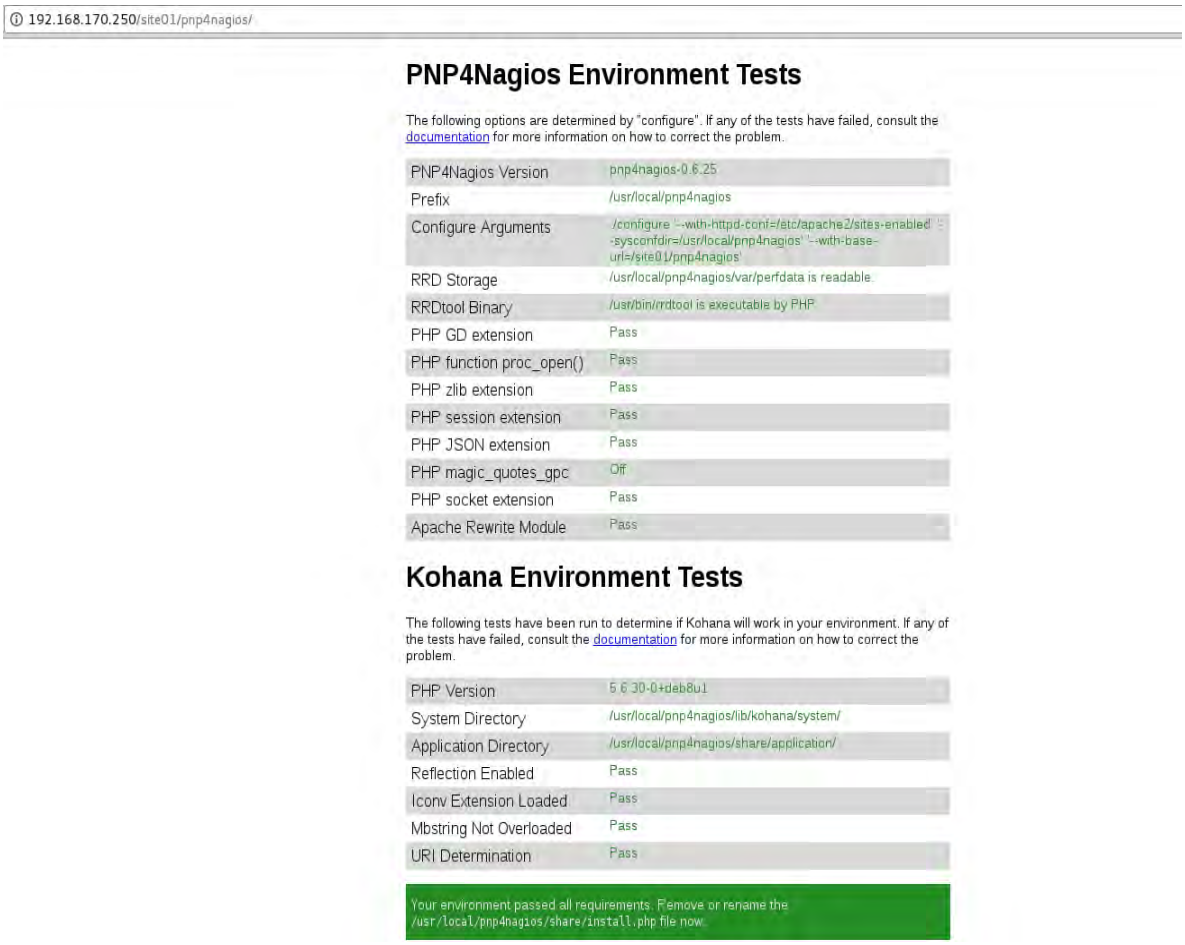
```
/etc/init.d/apache2 reload
```

Para debian8 jessie.

```
systemctl reload apache2
```

Verificamos la configuración de PNP4Nagios ingresando en el navegador:

```
http://nagios-server-ip/site01/pnp4nagios/
```



Al pie de la página se mostrará un aviso que dice: "Su entorno cumplió todos los requisitos. Elimine o cambie el nombre del archivo /usr/local/pnp4nagios/share/install.php".
Eliminamos el archivo.

```
rm /usr/local/pnp4nagios/share/install.php
```

- Configuración PNP4Nagios

PNP4Nagios permite una integración con Nagios. Vamos a usar "Bulk-Mode", ya que es la mejor forma disponible para Nagios 4.
Necesitamos copiar este fragmento al final del archivo /usr/local/nagios/etc/nagios.cfg (tenemos algunos ejemplos Dentro del directorio /usr/local/pnp4nagios/)

```
nano /usr/local/nagios/etc/nagios.cfg
```

Copiamos lo siguiente al final del archivo

```
# Bulk / NPCD mode
#
process_performance_data=1
# *** the template definition differs from the one in the original nagios.cfg
#
service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata
service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIME
T$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICE
PERFDATA::$SERVICE$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-perfdata-file
#
# *** the template definition differs from the one in the original nagios.cfg
#
host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$\tH
OSTNAME::$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHE
CKCOMMAND::$HOSTCHECKC$
host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file
# Load Livestatus Module
broker_module=/usr/lib/check_mk/livestatus.o /usr/local/nagios/var/rw/live
event_broker_options=-1
# added by setup.sh of check_mk
cfg_dir=/usr/local/nagios/etc/check_mk.d
```

Necesitamos copiar este fragmento al final del archivo /usr/local/nagios/etc/objects/misccommands.cfg (tenemos algunos ejemplos dentro del directorio /usr/local/pnp4nagios/)

```
nano /usr/local/nagios/etc/objects/misccommands.cfg
```

Ingresamos lo siguiente en el archivo que se va a crear.

```
# Bulk with NPCD mode
define command {
        command_name process-service-perfdata-file
        command_line /bin/mv /usr/local/pnp4nagios/var/service-perfdata
```

```
/usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$
}

define command {
        command_name process-host-perfdata-file
        command_line /bin/mv /usr/local/pnp4nagios/var/host-perfdata
/usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$
}
```

Y adicionamos esta línea justo después del bloque cfg_dir en el archivo /usr/local/nagios/etc/nagios.cfg:

```
nano /usr/local/nagios/etc/nagios.cfg
```

```
cfg_file=/usr/local/nagios/etc/objects/misccommands.cfg
```

Establecemos NPCD para iniciar el arranque.

Para debian7 wheezy

```
service npcd start
service npcd restart
```

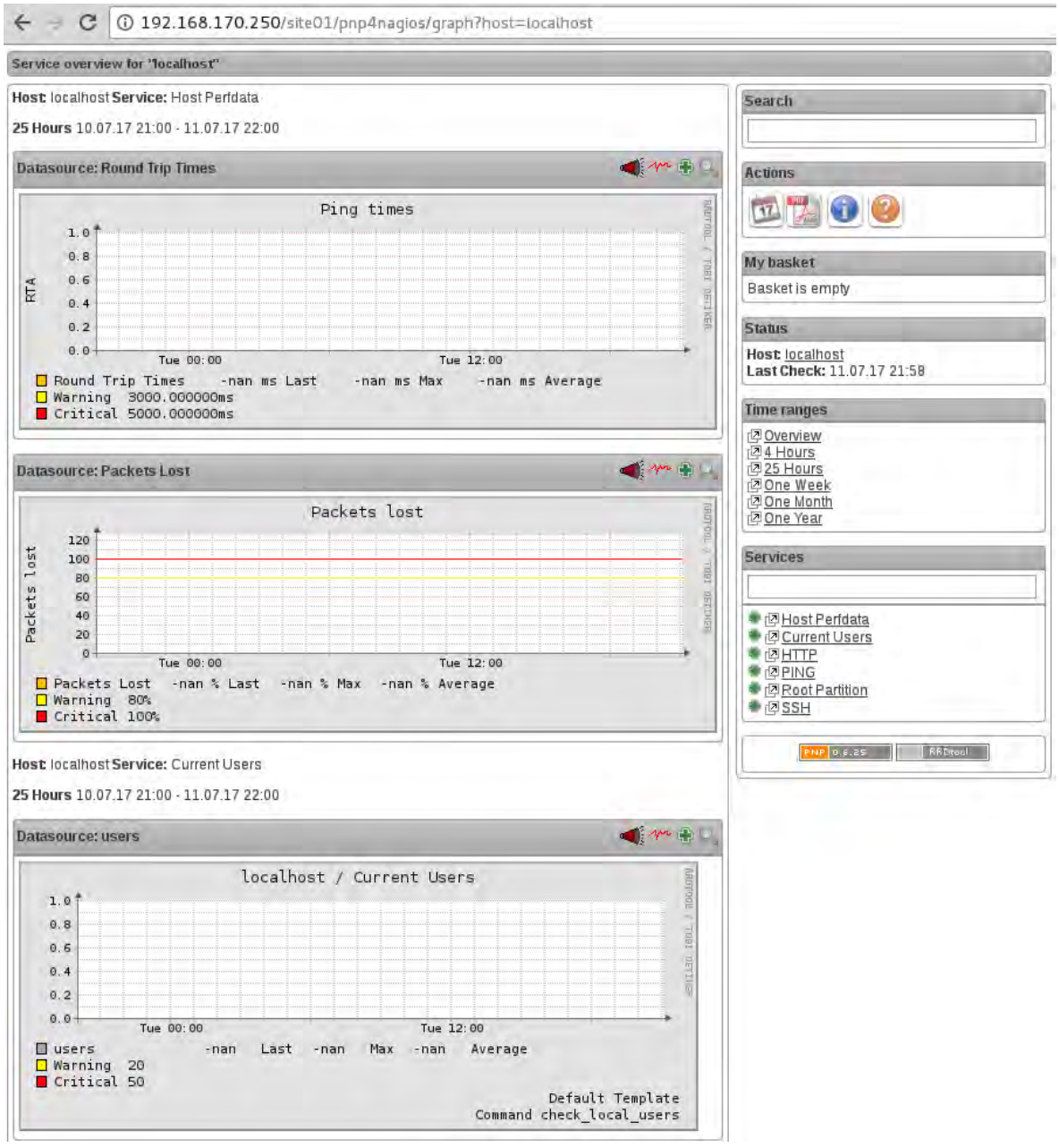
Para debian8 jessie

```
systemctl enable npcd.service
systemctl start npcd.service
systemctl restart nagios.service
```

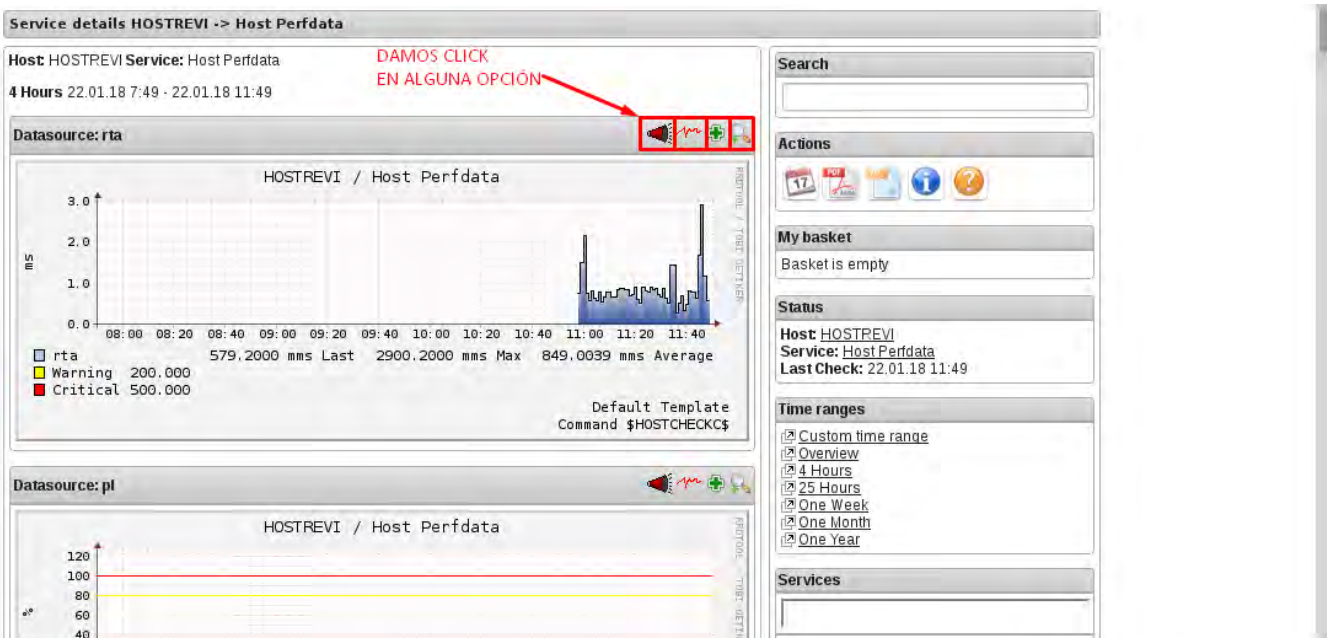
Ahora podemos comprobar de nuevo si todo está funcionando, colocamos en el navegador:

```
http://nagios-server-ip/site01/pnp4nagios/
```

Hasta este momento solamente se muestra las gráficas del localhost.


192.168.170.250/site01/pnp4nagios/graph?host=localhost
Service overview for 'localhost'
Host: localhost Service: Host Perfdata
25 Hours 10.07.17 21:00 - 11.07.17 22:00
Datasource: Round Trip Times
Ping times
RTA
1.0
0.8
0.6
0.4
0.2
0.0
Tue 00:00
Tue 12:00
Round Trip Times -nan ms Last -nan ms Max -nan ms Average
Warning 3000.000000ms
Critical 5000.000000ms
Datasource: Packets Lost
Packets lost
Packets lost
120
100
80
60
40
20
0
Tue 00:00
Tue 12:00
Packets Lost -nan % Last -nan % Max -nan % Average
Warning 80%
Critical 100%
Host: localhost Service: Current Users
25 Hours 10.07.17 21:00 - 11.07.17 22:00
Datasource: users
localhost / Current Users
1.0
0.8
0.6
0.4
0.2
0.0
Tue 00:00
Tue 12:00
users -nan Last -nan Max -nan Average
Warning 20
Critical 50
Default Template
Command check_local_users
Search
Actions
My basket
Basket is empty
Status
Host: localhost
Last Check: 11.07.17 21:58
Time ranges
Overview
4 Hours
25 Hours
One Week
One Month
One Year
Services
Host Perfdata
Current Users
HTTP
PING
Root Partition
SSH

2.4.1 Vinculación de PNP4Nagios con Nagios. Cuando se ingresa a PNP4Nagios a visualizar las gráficas, se observa que las opciones que están dentro de los cuadros rojos no tienen acceso a su funcionalidad. Estas opciones son importantes para realizar reportes.



Al momento de dar click a las opciones se muestra lo siguiente:



Para dar solución a este problema es necesario ubicarnos en la siguiente ruta:

```
cd /usr/local/pnp4nagios
```

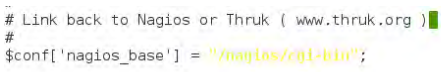
Dentro de la ruta es necesario modificar los archivos que estan marcados en color rojo.

```
root@debian1205:/usr/local/pnp4nagios# ls
background.pdf  config_local.php  lib                    nagios.cfg-sample  pnp4nagios_release          share
bin             config.php        libexec                npcd.cfg           process_perfdata.cfg        var
check_commands  config.php.0.6.25 man                    npcd.cfg.0.6.26    process_perfdata.cfg.0.6.26
config.d        config.php.0.6.26 misccommands.cfg-sample pages              rra.cfg-sample
root@debian1205:/usr/local/pnp4nagios#
```

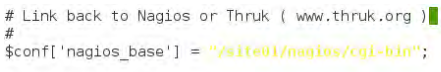
Se edita el archivo “config_local.php”.

```
nano config_local.php
```

En la línea donde se encuentra la ruta “/nagios/cgi-bin”.



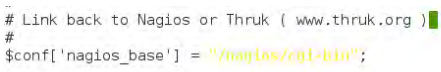
Se la edita por la ruta “/site01/nagios/cgi-bin”.



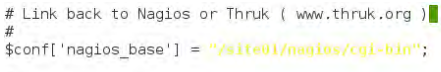
Luego se edita el archivo “config.php”.

```
nano config.php
```

En la línea donde se encuentra la ruta “/nagios/cgi-bin”.



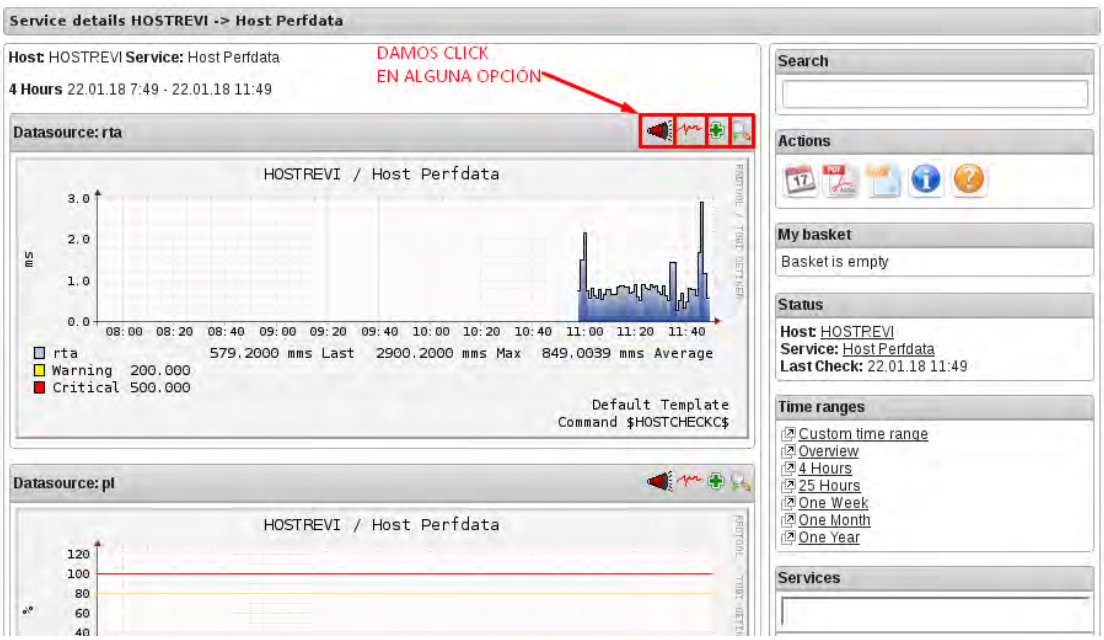
Se la edita por la ruta “/site01/nagios/cgi-bin”.



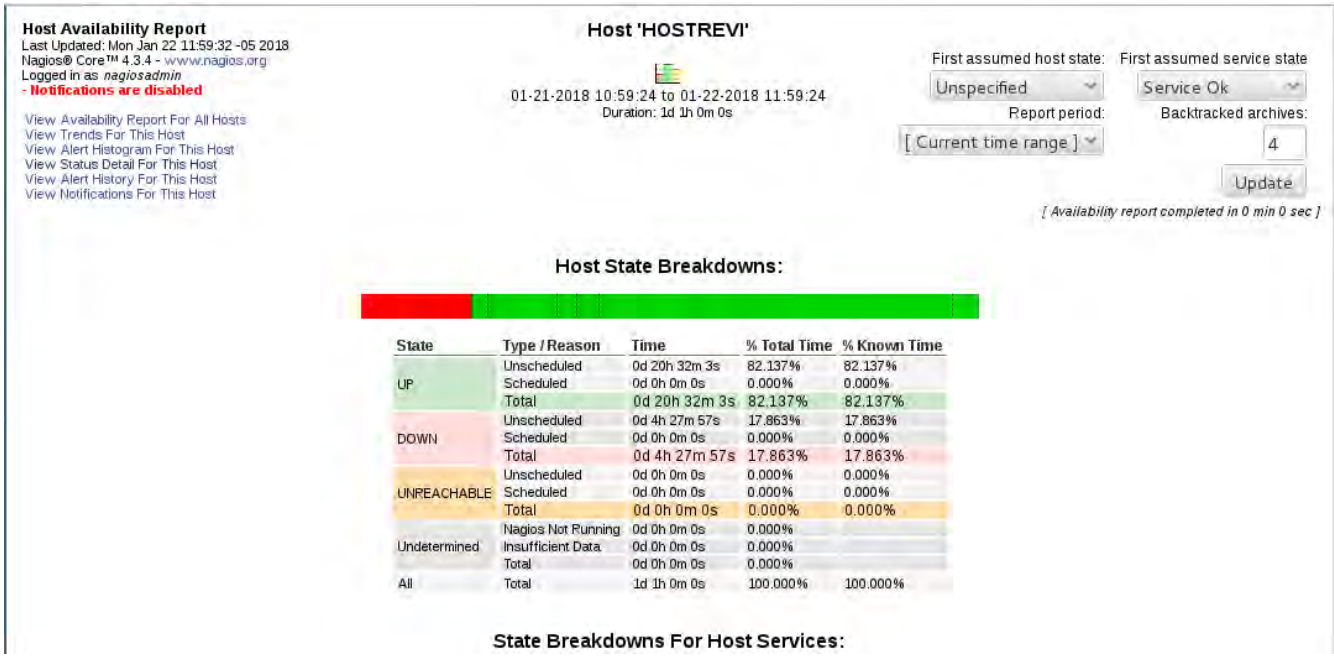
Luego de realizar los cambios y de guardarlos se reinicia el servicio npcd.

```
/etc/init.d/npcd restart
```

Se vuelve a dar click en las opciones de las gráficas de PNP4Nagios.



Se puede observar que ya se tiene acceso a sus funcionalidades.



3. CONFIGURACIÓN DE SEGURIDAD EN LA SUITE DE MONITOREO

3.1 CONFIGURACIÓN DE SEGURIDAD CON PROTOCOLO SSL

Páginas referentes:

https://www.ochobitshacenunbyte.com/2015/10/14/habilitar-https-servidor-web/

https://www.nanotutoriales.com/como-crear-un-certificado-ssl-de-firma-propia-con-openssl-y-apache-http-server

Instalar openssl y libssl-dev

```
apt-get install openssl
apt-get install libssl-dev
```

Se crea una llave privada que será utilizadapara la generación del certificado, esta llave le permite a nuestro certificado SSL ser implementado en cualquier servicio que requiera una conexión segura.
Se creará una llave de 1024bits

```
openssl genrsa -out server.key 1024
```

Aparecera lo siguiente.

```
Generating RSA private key, 1024 bit long modulus
.++++++
.....................................++++++
e is 65537 (0x10001)
```

- Crear un CSR (Certificate Signing Request)

Un CSR es la base para un certificado SSL, en el se definen los datos que son requeridos para poder generar dicho certificado.
Este se puede generar las veces que sea necesario si sucede algún error en la digitación de los datos, en esta parte se toma en cuenta la llave anteriormente creada.

```
openssl req -new -key server.key -out server.csr
```

En este caso se genero el CSR con los siguientes datos.

```
Country Name (2 letter code) [AU]:CO
State or Province Name (full name) [Some-State]:CO
Locality Name (eg, city) []:Pasto
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Electro
Organizational Unit Name (eg, section) []:Sistemas
Common Name (e.g. server FQDN or YOUR name) []:ES
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

- Generando el certificado SSL

Para generar el certificado SSL se va a necesitar la llave privada y el CSR que fueron creados anteriormente.

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Una vez generado aparecerá lo siguiente.

```
Signature ok
subject=/C=CO/ST=CO/L=Pasto/O=Electro/OU=Sistemas/CN=ES
Getting Private key
```

- Configuración del certificado ssl en Apache

Copiamos y renombramos el certificado y la llave en la ruta /etc/ssl/certs/

```
cp server.crt /etc/ssl/certs/ssl.crt
cp server.key /etc/ssl/certs/ssl.key
```

A continuación, se modifican los permisos del fichero creado.

```
chmod 600 /etc/ssl/certs/*
```

- Habilitar el modulo SSL en apache

Le debemos habilitar.

```
a2enmod ssl
```

Habilitamos plantilla web para conexión ssl

```
a2ensite default-ssl
```

Y reiniciamos el apache.

```
service apache reload
```

- Configuración de Apache para trabajar con ssl

Editamos el archivo default-ssl.

```
nano /etc/apache2/sites-available/default-ssl
```

Y modificamos las siguientes lineas.

SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem por:

```
SSLCertificateFile /etc/ssl/certs/ssl.crt
```

SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key por:

```
SSLCertificateKeyFile /etc/ssl/certs/ssl.key
```

Donde ssl.crt es el nombre del certifcado creado y ssl.key es el nombre de la llave creada.
Reiniciamos apache.

```
service apache2 reload
```

3.1.1 Modificación de archivos de configuración en apache Nagios, Check_mk, Nagvis, PNP4Nagios. Para forzar que las páginas sean accedidas de forma segura mediante https, es necesario modificar algunos archivos dentro en Apache.

- En Nagios

Ingresamos al archivos nagios.conf que se encuentra en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/nagios.conf
```

Descomentamos las líneas donde se encuentre, #SSLRequireSSL, quedando

```
SSLRequireSSL
```

Se debe tener en cuenta que en este archivo se encuentran dos líneas que se deben descomentar.

- En Check_MK

Ingresamos al archivos zzz_check_mk.conf que se encuentra en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/zzz_check_mk.conf
```

Adicionamos la linea SSLRequireSSL

```
<IfModule mod_python.c>
  Alias /site01/check_mk /usr/share/check_mk/web/htdocs
  <Directory /usr/share/check_mk/web/htdocs>
        AddHandler mod_python .py
        PythonHandler index
        PythonDebug Off
        DirectoryIndex index.py
        # Need Nagios authentification. Please edit the
        # following: Set AuthName and AuthUserFile to the
        # same value that you use for your Nagios configuration!
        SSLRequireSSL
        Order deny,allow
        allow from all
        AuthName "Nagios Access"
        AuthType Digest
        AuthUserFile /usr/local/nagios/etc/digest.users
        require valid-user....
…….....
…….....
```

- En Nagvis

Ingresamos al archivos nagvis.conf que se encuentra en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/nagvis.conf
```

Adicionamos la linea SSLRequireSSL

```
Alias /site01/nagvis "/usr/local/nagvis/share"

<Directory "/usr/local/nagvis/share">
  Options FollowSymLinks
  AllowOverride None
  SSLRequireSSL
  <IfModule mod_authz_core.c>
    # Apache >= 2.4
    Require all granted
  </IfModule>
  <IfModule !mod_authz_core.c>
    # Apache < 2.4
   # Order allow,deny
   # Allow from all
  </IfModule>
……..
……..
…….
```

- En PNP4Nagios

Ingresamos al archivo pnp4nagios.conf que se encuentra en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/pnp4nagios.conf
```

Adicionamos la linea SSLRequireSSL

```
Alias /site01/pnp4nagios "/usr/local/pnp4nagios/share"

<Directory "/usr/local/pnp4nagios/share">
        AllowOverride None
        SSLRequireSSL
        Order allow,deny
        Allow from all
        #
        # Use the same value as defined in nagios.conf
        #
        AuthName "Nagios Access"
```

```
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
……..
……..
…….
```

Por ultimo reiniciamos apache.

```
service apache2 restart
```

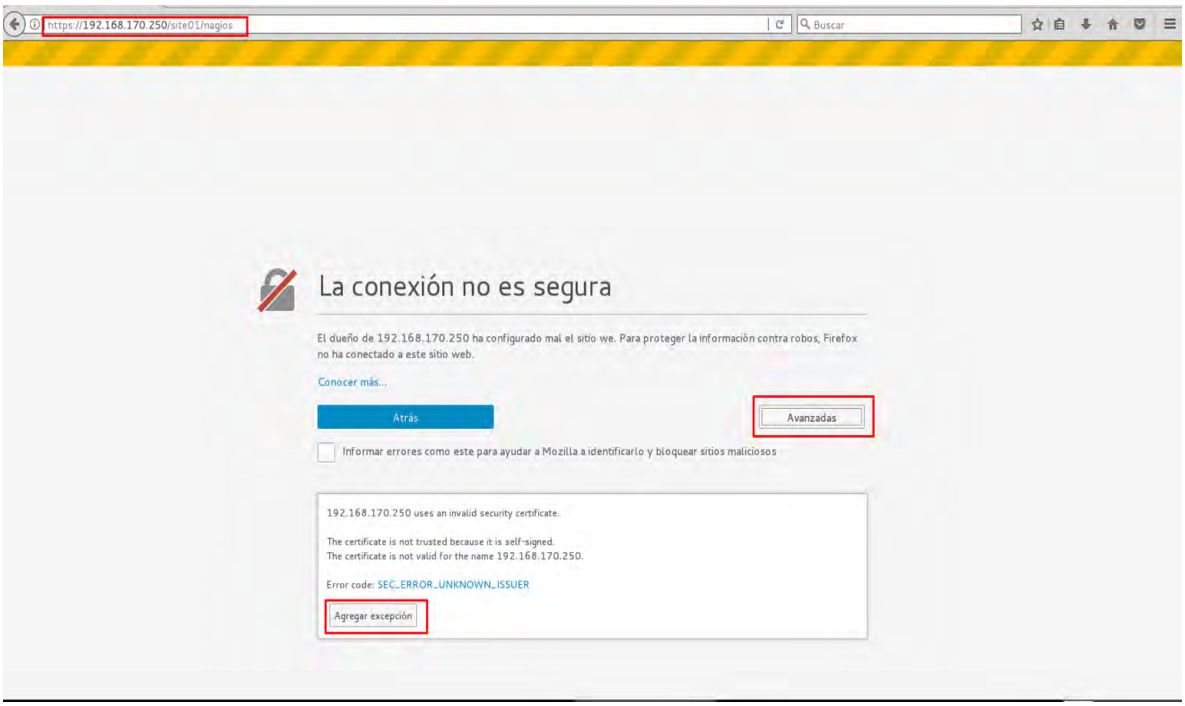
- Verificación del certificado SSL en un navegador

Una vez realizadas las anteriores modificaciones procedemos verificar el certificado ssl en este caso en firefox mozilla.

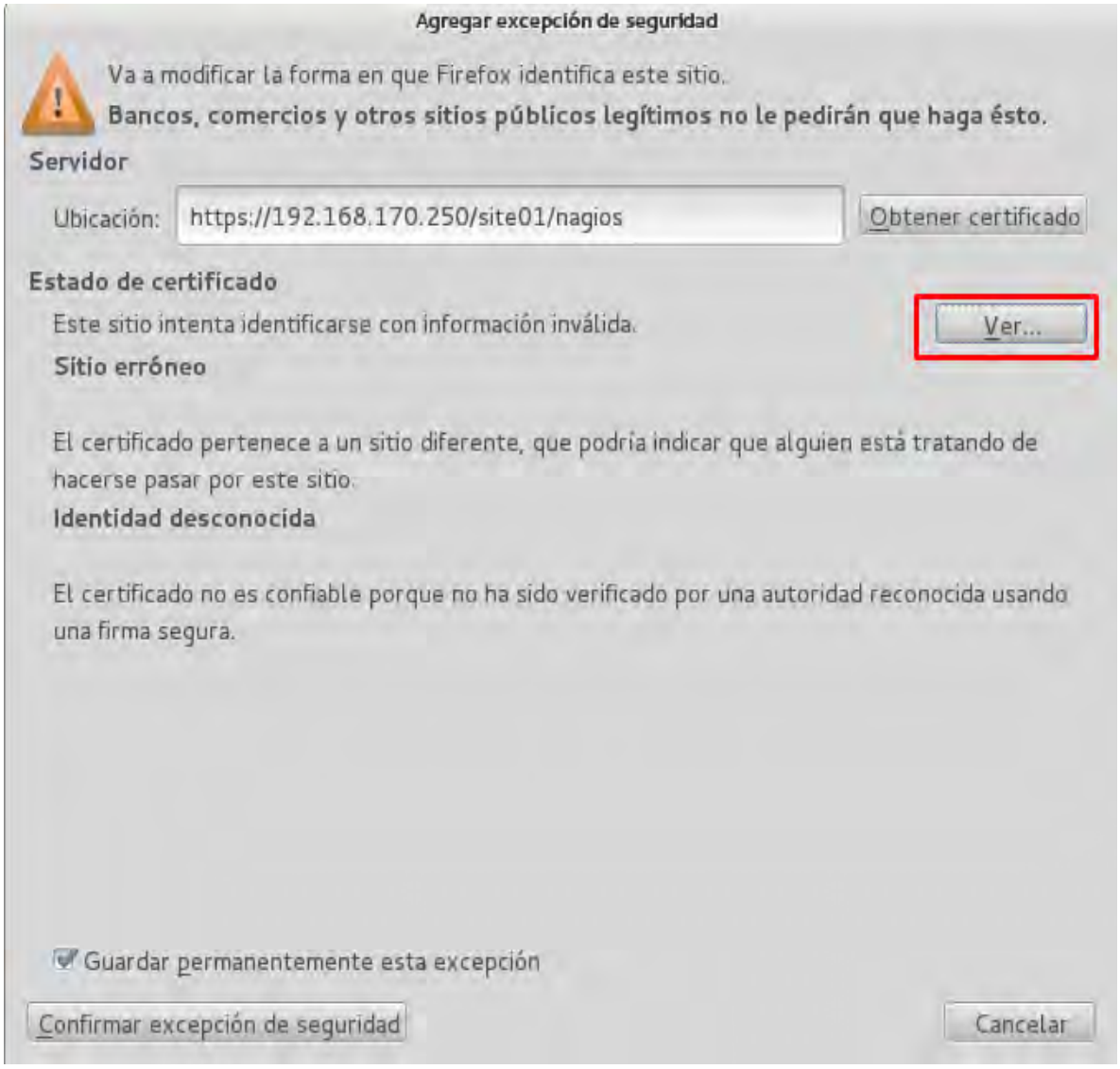
Ingresamos a uno de nuestros sitios en este caso a /site01/nagios con conexión http, para verificar que se forzó a una conexión segura https. Se mostrará el siguiente error.



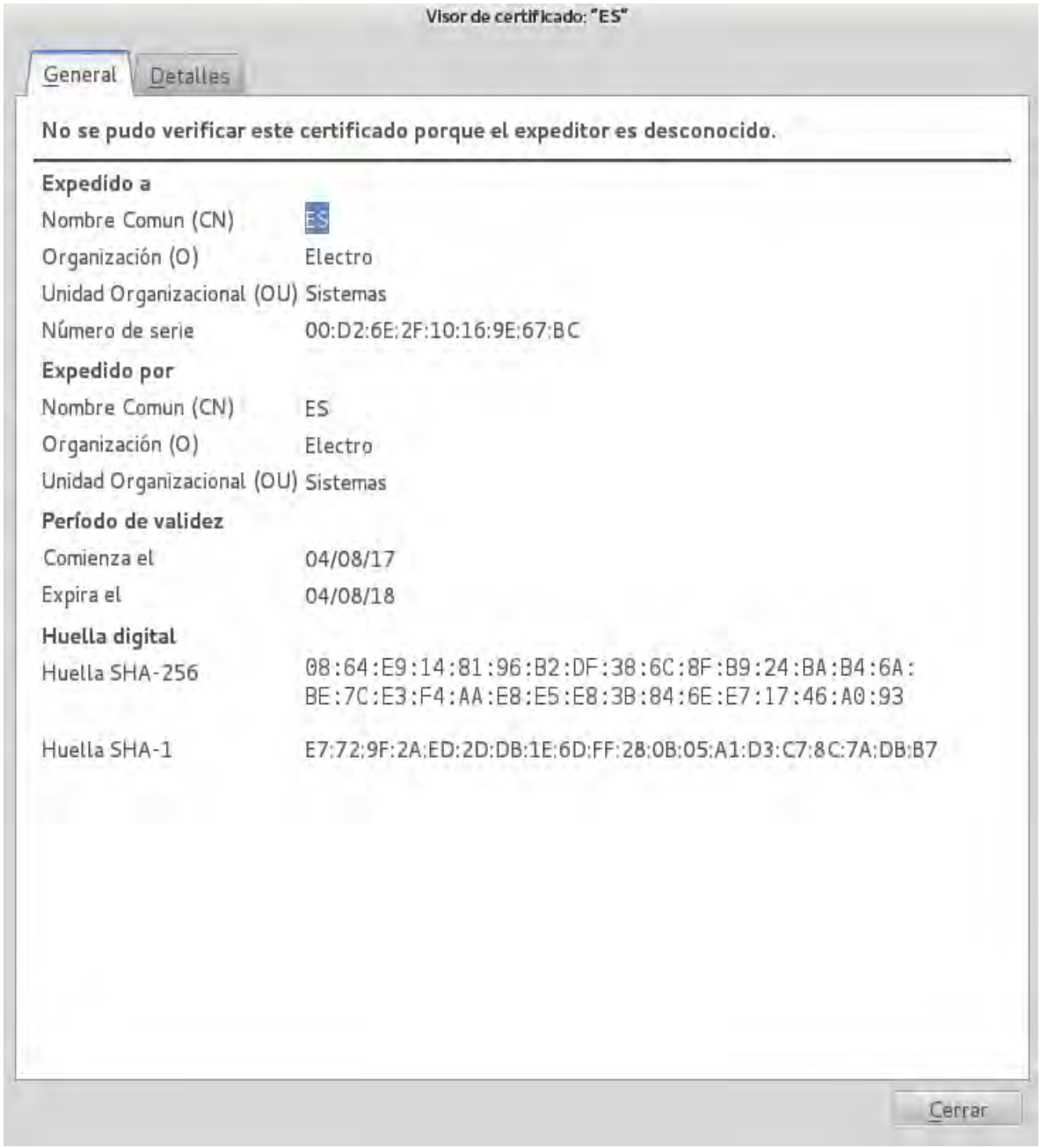
A continuación, se establece conexión de sitio colocando en la url *https:192.168.170.250/sites01/nagios* se mostrar una página como la de a continuación, en la cual damos clic sobre **Avanzadas** y posteriormente sobre **Agregar excepción**.


https://192.168.170.250/site01/nagios
Buscar
La conexión no es segura
El dueño de 192.168.170.250 ha configurado mal el sitio we. Para proteger la información contra robos, Firefox no ha conectado a este sitio web.
Conocer más...
Atrás
Avanzadas
Informar errores como este para ayudar a Mozilla a identificarlo y bloquear sitios maliciosos
192.168.170.250 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
The certificate is not valid for the name 192.168.170.250.
Error code: SEC_ERROR_UNKNOWN_ISSUER
Agregar excepción

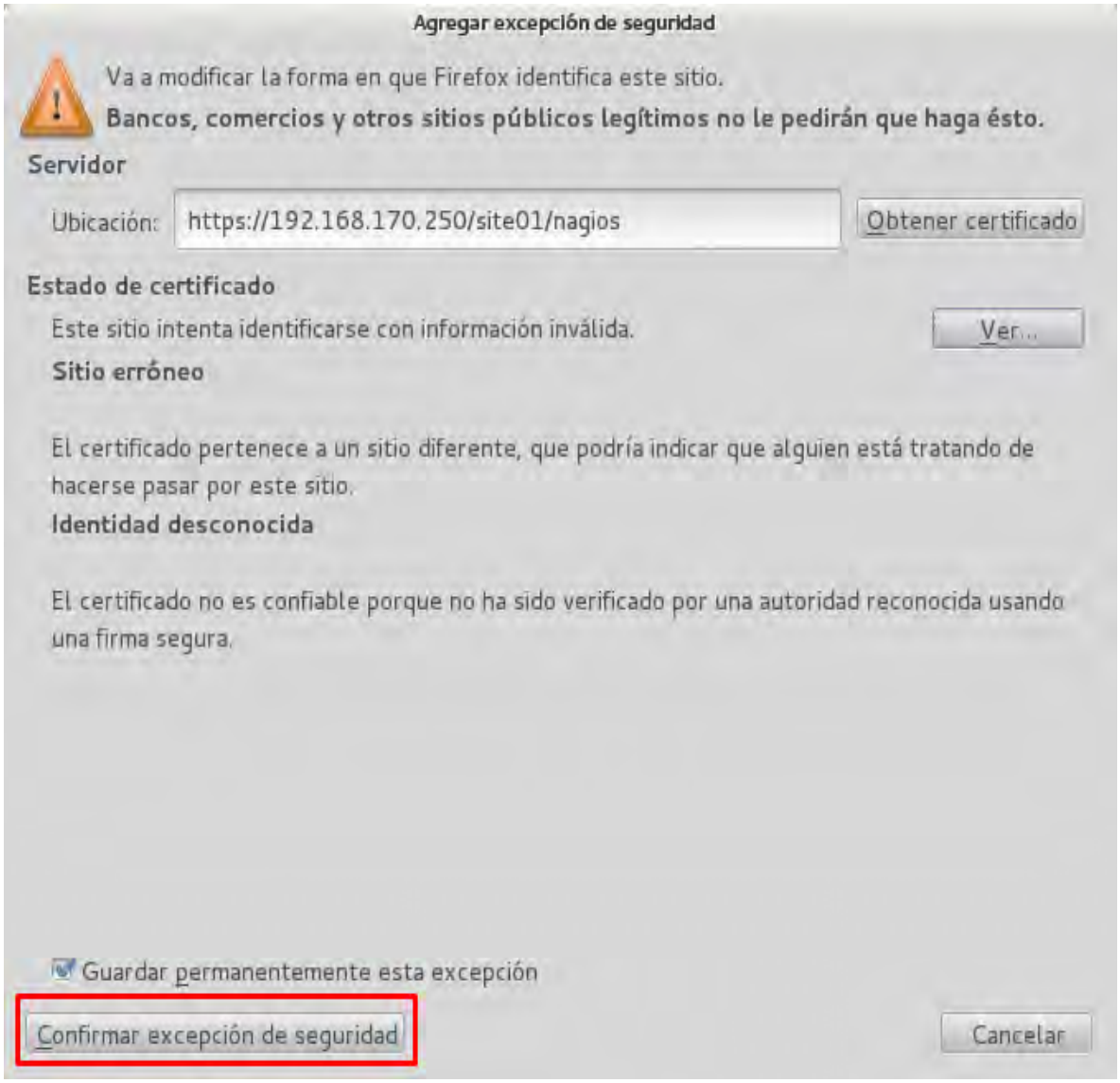
Luego, se abrirá una ventana donde automáticamente reconoce la dirección del certificado. Damos clic sobre *Ver* donde podemos ver la información del certificado generado.



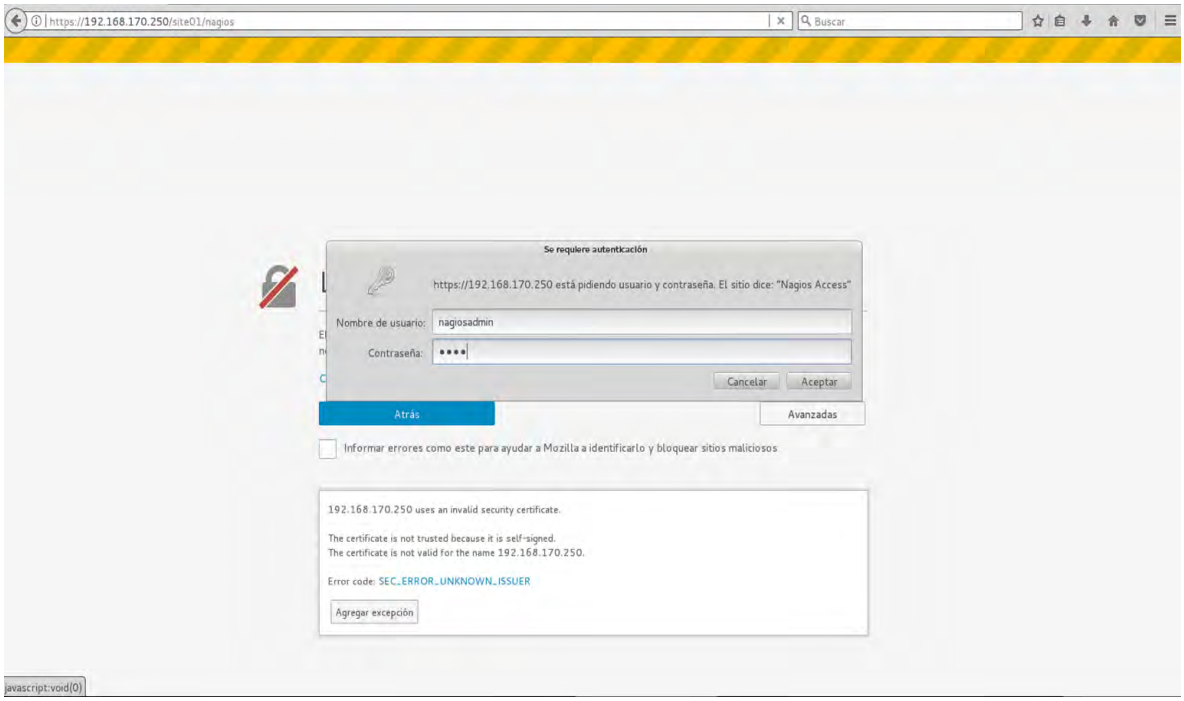
Enseguida, se abrirá una ventana donde muestra las características del certificado generado. Damos clic en *Cerrar.*



Luego, damos clic en *Confirmar excepción de seguridad.*



Se abrirá la ventana de registro donde nos pidira el **Nombre de usuario** y **Contraseña**.



Finalmente podremos acceder a nuestro sitio web de forma segura.



3.2 Configuración de seguridad mediante restricción ip

3.2.1 Restricción de acceso por IP en apache 2.4.10:

Páginas de referencia:

https://httpd.apache.org/docs/2.4/es/howto/access.html

Se accede a cada uno de los archivos de configuración de Nagios, Check_mk, Nagvis y PNP4Nagios en Apache, para modificar las reglas de acceso por IP.

Como primer paso verificamos que version de apache tenemos instalado.

```
apache2 -version
```

Mostrará lo siguiente.

```
Server version: Apache/2.4.10 (Debian)
```

- En Nagios

Ingresamos al archivo nagios.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/nagios.conf
```

Posteriormente se modifica las lineas donde se encuentre lo siguiente (en este caso dos veces):

```
…....
…....
…....
<IfVersion >= 2.3>
     <RequireAll>
        Require all granted
#        Require host 127.0.0.1

        AuthType Basic
        AuthName "Nagios Access"
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
     </RequireAll>
</IfVersion>
……
……
……
```

Por:

```
……
…..
…..
<IfVersion >= 2.3>
     <RequireAll>
#       Require all granted
#       Require host 127.0.0.1
       Require ip 192.168.170.250 192.168.170.0

        AuthType Basic
        AuthName "Nagios Access"
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
     </RequireAll>
  </IfVersion>
……
……
……
```

En directiva *Require ip* se definen las direcciones IP las cuales tendrán acceso al sitio web, por ejemplo el administrador del sitio.

- En Check_MK

Ingresamos al archivo zzz_check_mk.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/zzz_check_mk.conf
```

Posteriormente se modifica:

```
…….
…….
…….
 SSLRequireSSL
       Order deny,allow
       allow from all
       AuthName "Nagios Access"
       AuthType Basic
       AuthUserFile /usr/local/nagios/etc/htpasswd.users
       require valid-user
```

```
……
……
……
```

Por:

```
……
…..
…..
        SSLRequireSSL
        Order deny,allow
#       allow from all
        Deny from all
        Allow from 192.168.170.250 192.168.170.0
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        require valid-user
……
……
……
```

En directiva Allow from se definen las direcciones IP las cuales tendrán acceso al sitio web.

- En Nagvis

Ingresamos al archivo nagvis.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/nagvis.conf
```

Posteriormente se modifica:

```
……..
……..
……..
 <IfModule mod_authz_core.c>
   # Apache >= 2.4
   Require all granted
   Options FollowSymLinks
   AllowOverride None
  </IfModule>
……
```

```
……
……
```

Por:

```
……
…..
…..
<IfModule mod_authz_core.c>
    # Apache >= 2.4
#    Require all granted
    Require ip 192.168.170.250 192.168.170.0
    Options FollowSymLinks
    AllowOverride None
  </IfModule>
……
……
……
```

En directiva *Require ip* se definen las direcciones IP las cuales tendrán acceso al sitio web.

- En PNP4Nagios

Ingresamos al archivo pnp4nagios.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/pnp4nagios.conf
```

Posteriormente se modifica:

```
…….
…….
…….
  AllowOverride None
        SSLRequireSSL
        Order allow,deny
       Allow from all
        #
        # Use the same value as defined in nagios.conf
        #
        AuthName "Nagios Access"
```

```
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
……
……
……
```

Por:

```
……
…..
…..
 AllowOverride None
        SSLRequireSSL
        Order deny,allow
#       Allow from all
        Deny from all
        Allow from 192.168.170.250 192.168.170.0
        #
        # Use the same value as defined in nagios.conf
        #
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
……
……
……
```

En directiva *Allow from* se definen las direcciones IP las cuales tendrán acceso al sitio web.

3.2.2 Restricción de acceso por IP en apache 2.2.22:

Paginas de referencia:

https://httpd.apache.org/docs/2.4/es/howto/access.html

Se accede a cada uno de los archivos de configuración de Nagios, Check_mk, Nagvis y PNP4NAGIOS en apache, para modificar las reglas de acceso por IP.

Como primer paso verificamos que version de apache tenemos instalado.

```
apache2 -version
```

Mostrará lo siguiente.

```
Server version: Apache/2.2.22 (Debian)
```

- En Nagios

Ingresamos al archivo nagios.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/nagios.conf
```

Posteriormente se modifica las lineas donde se encuentre lo siguiente (en este caso dos veces):

```
…....
…....
…....
<IfVersion < 2.3>
      Order allow,deny
      Allow from all
#     Order deny,allow
#     Deny from all
#     Allow from 127.0.0.1

      AuthType Basic
      AuthName "Nagios Access"
      AuthUserFile /usr/local/nagios/etc/htpasswd.users
      Require valid-user
   </IfVersion>
……..
……..
……..
```

Por:

```
……..
…..
…..
<IfVersion < 2.3>
#       Order allow,deny
```

```
#     Allow from all
     Order deny,allow
     Deny from all
     Allow from 192.168.170.250 192.168.170.0

      AuthType Basic
      AuthName "Nagios Access"
      AuthUserFile /usr/local/nagios/etc/htpasswd.users
      Require valid-user
   </IfVersion>
……
……
……
```

En directiva *Allow from* se definen las direcciones IP las cuales tendrán acceso al sitio web, por ejemplo el administrador del sitio.

- En Check_MK

Ingresamos al archivo zzz_check_mk.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/zzz_check_mk.conf
```

Posteriormente se modifica:

```
…….
…….
…….
 SSLRequireSSL
        Order deny,allow
        allow from all
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        require valid-user
……
……
……
```

Por:

```
……
…..
```

```
…..
SSLRequireSSL
        Order deny,allow
#         allow from all
        Deny from all
        Allow from 192.168.170.250 192.168.170.0
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        require valid-user
……
……
……
```

En directiva Allow from se definen las direcciones IP las cuales tendrán acceso al sitio web.

- En Nagvis

Ingresamos al archivo nagvis.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/nagvis.conf
```

Posteriormente se modifica:

```
…….
…….
…….
 <IfModule !mod_authz_core.c>
    # Apache < 2.4
   #  Order allow,deny
   # Allow from all
     </IfModule>
……
……
……
```

Por:

```
……
…..
…..
<IfModule !mod_authz_core.c>
    # Apache < 2.4
```

```
  #  Order allow,deny
    Order deny,allow
  # Allow from all
   Deny from all
   Allow from 192.168.170.250 192.168.170.0
  </IfModule>
……
……
……
```

En directiva Allow from se definen las direcciones IP las cuales tendrán acceso al sitio web.

- En PNP4Nagios

Ingresamos al archivo pnp4nagios.conf ubicado en la ruta /etc/apache2/sites-enabled/

```
nano /etc/apache2/sites-enabled/pnp4nagios.conf
```

Posteriormente se modifica:

```
…….
…….
…….
  AllowOverride None
        SSLRequireSSL
        Order allow,deny
       Allow from all
        #
        # Use the same value as defined in nagios.conf
        #
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
……
……
……
```

Por:

```
……
```

```
…..
…..
 AllowOverride None
        SSLRequireSSL
        Order deny,allow
#       Allow from all
        Deny from all
        Allow from 192.168.170.250 192.168.170.0
        #
        # Use the same value as defined in nagios.conf
        #
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/nagios/etc/htpasswd.users
        Require valid-user
……..
……..
……..
```

En directiva *Allow from* se definen las direcciones IP las cuales tendrán acceso al sitio web.
Una vez realizado lo anterior procedemos reiniciar apache.

```
service apache2 restart
```

3.2.3 Prueba de acceso y denegación por IP:

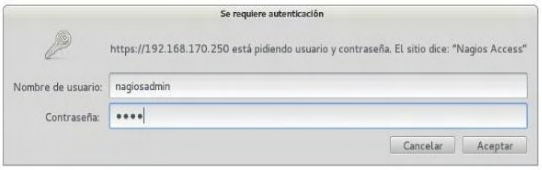
- Acceso al sitio web de Nagios

Al acceder con una IP que se encuentra en la directiva *Allow from,* el proceso de certificado se lleva a cabo de forma normal.



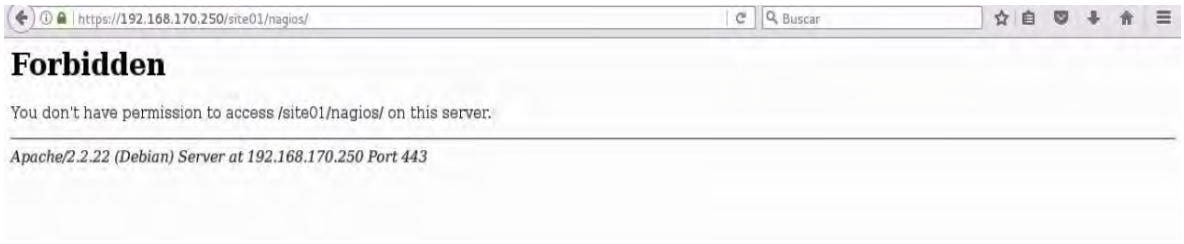
Ingresando al sitio web de forma segura, como se muestra en la siguiente imagen.





- Denegación de acceso al sitio web nagios

De lo contrario al acceder con una IP no definida en la directiva *Allow from,* se muestra la siguiente restricción.


https://192.168.170.250/site01/nagios/
Buscar
Forbidden
You don't have permission to access /site01/nagios/ on this server.
Apache/2.2.22 (Debian) Server at 192.168.170.250 Port 443

Anexo L. Dedifinición de servicios públicos y privados en Nagios.

ÍNDICE

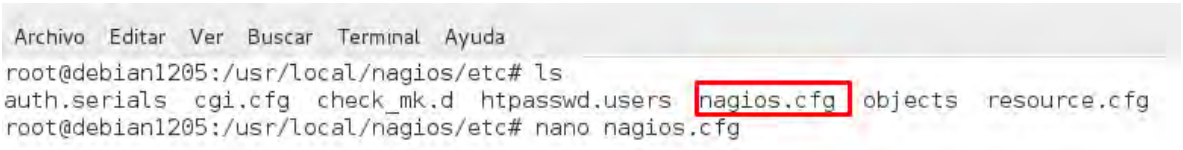
Pág.

1. SERVICIOS PRIVADOS 536
1.1 MAQUINA WINDOWS 536
1.2 MAQUINA LINUX 540
1.3 IMPRESORA 545
1.4 Switch 552
2. SERVICIOS PUBLICOS 558
2.1 SERVICIO SSH EN SERVIDOR AZKABAN Y VOLDEMORT 558
2.2 SERVICIO FTP EN SERVIDOR AZKABAN 561
2.3 SERVICIO DE MENSAJERIA INSTANTANEA (OPENFIRE) EN SERVIDOR AZKABAN 562
2.4 SERVICIO WEB (APACHE) SERVIDOR VOLDEMORT 564
2.5 SERVICIO PROXY (SQUID) SERVIDOR VOLDEMORT 567
2.6 SERVICIO DNS (BIND9) SERVIDOR VOLDEMORT 570

1. SERVICIOS PRIVADOS

Se mostrará la definición de servicios privados en equipos de cómputo Windows y Linux, como también de una impresora de red y un switch, para entender un poco la mecánica de Nagios es necesario tener en cuenta que este trabaja con directorios, subdirectorios y archivos, los directorios y subdirectorios son utilizados para llevar un orden cuando la red de datos a monitorear es muy grande, y en los archivos se define específicamente los host y servicios a monitorear.

Teniendo en cuenta lo anterior, existe el directorio /etc que se crea en la instalación de Nagios, en el que encuentra el archivo *nagios.cfg*.



Dentro de este existe el apartado (OBJETS CONFIGURATION FILE(S)), en donde se pueden crear tanto directorios como archivos. Existen ya creados algunos archivos los cuales utiliza Nagios al momento de realizar la instalación. Existen tanto directorios como archivos que se encuentran comentados para poder dar uso. O por otro lado se pueden crear directorios y archivos según las necesidades propias. Para llevar un orden especifico Nagios crea tanto los directorios como los archivos dentro del directorio */objects.*

Para la creación de los archivos y directorios Nagios utiliza la definición mediante rutas, en el caso de los archivos de la siguiente manera:

cfg_file=/usr/local/nagios/etc/objects/nombre_del_archivo

Y para los directorios:

cfg_dir=/usr/local/nagios/etc/objects/nombre_del_directorio

1.1 MAQUINA WINDOWS

Con todo lo anterior, dentro del archivo nagios.cfg por defecto ya viene definida la ruta para la creación del archivo que contendrá la definición y configuración de los servicios privados de la maquina Windows.

Se ingresa al archivo de la siguiente manera:

```
nano /usr/local/nagios/etc/nagios.cfg
```

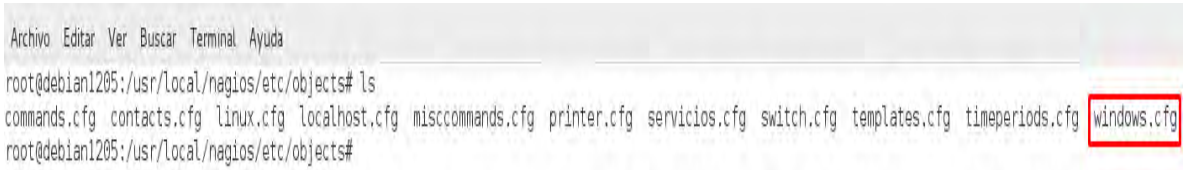
Se debe ubicar y descomentar la línea donde se encuentra definida la ruta para la creación del archivo windows.cfg.

Debe quedar de la siguiente manera.

```
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

Una vez definida la ruta se debe crear el archivo dentro del directorio */objects.*

```
cd /usr/local/nagios/etc/objects/
touch windows.cfg
```



Creado el archivo, se debe definir el comando del servicio, esto se hace en el archivo command.cfg, además de la contraseña al servidor Nagios, la misma que se definió al instalar el agente NSClient en la maquina Windows a monitorear. Se agrega el parámetro -s “la contraseña que se definió”. Para esto se debe editar el archivo commands.cfg

En la definición del comando en la línea *command_line* además de estar definido el parámetro de dirección de host (*-H $HOSTADDRESS$$*), deben estar definido como parámetro estático el puerto (*-p*) que en este caso es el 12489 y la contraseña (*-s*) la contraseña que se definió al instalar el agente NSClient. El argumento -v es una variable de chequeo no estática ($ARG1$), y un argumento dos ($ARG2$) utilizado por el plugin.

La definición debe quedar similar a lo siguiente.

```
# 'check_nt' command definition
define command{
        command_name    check_nt
        command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s 1234
-v $ARG1$ $ARG2$
        }
```

Definido el comando del servicio se procede a realizar la definición del host y de los servicios que se van a monitorear.
Nota: previamente se debe haber instalado el agente NSClient en los equipos Windows, si no se encuentra instalado no es posible realizar el monitoreo. Para

detalles sobre este tema dirigirse al apartado 18.2.1.3 del documento principal.

Se ingresa al archivo windows.cfg.

```
nano windows.cfg
```

Y se configura la definición del host Windows de la siguiente manera.

```
define host{
        use             windows-server  ; Inherit default values from a template
        host_name       winserver       ; The name we're giving to this host
        alias           My Windows Server       ; A longer name associated with the host
        address         192.168.170.0   ; IP address of the host
        }
```

Dentro del mismo archivo se realiza la definición de los servicios a supervisar.

A continuación, se define el servicio que se encarga de supervisar la versión de agente Nesciente.

```
define service{
        use                     generic-service
        host_name               winserver
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
```

A continuación, se define el servicio que se encarga de supervisar la carga de la CPU.

```
define service{
        use                     generic-service
        host_name               winserver
        service_description     CPU Load
        check_command           check_nt!CPULOAD!-l 5,80,90
        }
```

A continuación, se define el servicio de uso del disco C:\

```
define service{
        use                     generic-service
        host_name               winserver
        service_description     C:\ Drive Space
```

```
    check_command          check_nt!USEDDISKSPACE!-l c -w 80 -c 90
    }
```

Luego, se define el servicio del proceso de Explorer.exe

```
define service{
    use                    generic-service
    host_name              winserver
    service_description    Explorer
    check_command          check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
    }
```

Una vez terminado lo anterior verificamos que la configuración este correcta con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

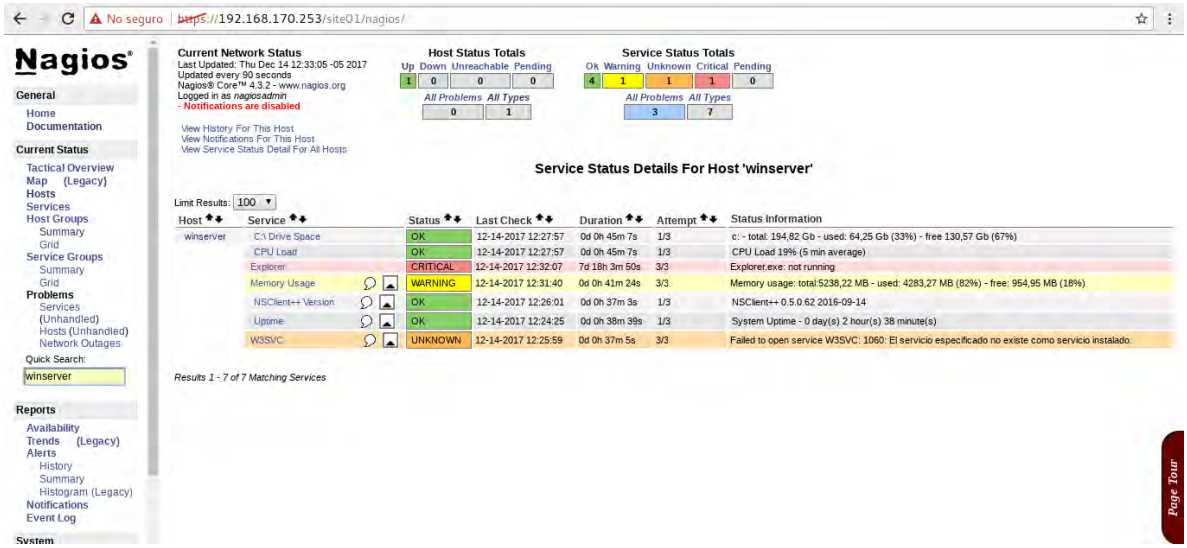
```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

Una vez terminada la definición y configuración, se ingresa a la página de administración de Nagios y podemos mirar la maquina con sus respectivos servicios públicos siendo monitoreados.



1.2 MAQUINA LINUX

La definición, configuración y puesta en marcha de los servicios privados de una maquina Linux es similar a la de una maquina Windows, en primer lugar, se debe editar el archivo *nagios.cfg* el cual por defecto ya viene definida la ruta para la creación del archivo que contendrá la definición y configuración de los servicios privados de la maquina Linux.

Se ingresa al archivo de la siguiente manera:

```
nano /usr/local/nagios/etc/nagios.cfg
```

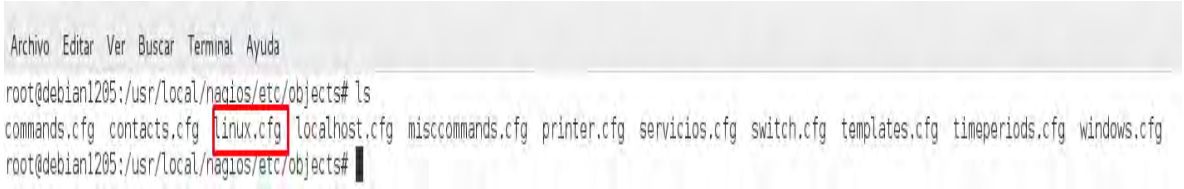
Se debe ubicar y descomentar la línea donde se encuentra definida la ruta para la creación del archivo linux.cfg.

Debe quedar de la siguiente manera.

```
cfg_file=/usr/local/nagios/etc/objects/linux.cfg
```

Una vez definida la ruta se debe crear el archivo dentro del directorio */objects.*

```
cd /usr/local/nagios/etc/objects/
touch linux.cfg
```



Creado el archivo, se debe definir el comando del servicio, esto se hace en el archivo command.cfg, en la definición del comando en la línea *command_line* se define como argumento no estático la dirección ip de la máquina Linux *(-H $HOSTADDRESS$)*, y el argumento (-c $ARG1$) el cual recibe el nombre del comando que debe ejecutar el daemon remoto.

La definición debe quedar similar a lo siguiente.

```
define command{
 command_name check_nrpe
 command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
 }
```

Creado el archivo se procede a realizar la definición del host y de los servicios que se van a monitorear.

Nota: previamente se debe haber instalado el agente NRPE en los equipos Linux, si no se encuentra instalado no es posible realizar el monitoreo. Para detalles sobre este tema dirigirse al punto 18.2.1.1 (INSTALACION DE NRPE EN MAQUINA LINUX) del documento principal.

Se edita el archivo linux.cfg.

```
nano linux.cfg
```

Y se configura la definición del host Linux de la siguiente manera.

```
define host{
                use linux-server            ; Inherit default values from a template
                host_name debian            ; The name we're giving to this server
                alias debian8               ; A longer name for the server
                address 192.168.170.252     ; IP address of the server
}
```

Dentro del mismo archivo se realiza la definición de los servicios a supervisar.

A continuación, se define el servicio de carga de la máquina.

```
define service{
        use generic-service
        host_name debian
        service_description CPU Load
        check_command check_nrpe!check_load
        }
```

En el siguiente servicio se monitorea el número de usuarios logeados en la máquina.

```
define service{
        use generic-service
        host_name debian
        service_description Current Users
        check_command check_nrpe!check_users
        }
```

En el siguiente servicio se monitorea el espacio libre en /dev/sda5 de la máquina.

```
define service{
        use generic-service
        host_name debian
        service_description /home /dev/sda5 Free Space
        check_command check_nrpe!check_sda5
        }
```

En el siguiente servicio se define el número total de procesos corriendo en la máquina.

```
define service{
        use generic-service
        host_name debian
        service_description Total Processes
        check_command check_nrpe!check_total_procs
        }
```

En el siguiente servicio se define los zombie_process corriendo en la maquina

```
define service{
        use generic-service
        host_name debian
        service_description Zombie Processes
        check_command check_nrpe!check_zombie_procs
```

```
        }
```

En el siguiente servicio se define el servicio de “ping” en la máquina local.

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               debian
        service_description         PING
          check_command                 check_ping!100.0,20%!500.0,60%
        }
```

A continuación, se define un servicio para verificar el espacio en disco de la partición raíz en la máquina local. Advertencia si <20% libre, crítico si <10% de espacio libre en la partición.

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               debian
        service_description         Root Partition
          check_command                 check_local_disk!20%!10%!/
        }
```

A continuación, se define un servicio para verificar el número de usuarios actualmente conectados en la máquina local. Advertencia si> 20 usuarios, crítico si> 50 usuarios.

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               debian
        service_description         Current Users
          check_command                 check_local_users!20!50
        }
```

A continuación, se define un servicio para verificar el número de procesos actualmente en ejecución en la máquina local. Advertencia si> 250 procesos, crítico si> 400 procesos.

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               debian
        service_description         Total Processes
          check_command                 check_local_procs!250!400!RSZDT
        }
```

A continuación, se define un servicio para verificar la carga en la máquina local.

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               debian
        service_description             Current Load
          check_command
          check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
        }
```

A continuación, se define un servicio para verificar el uso de intercambio de la máquina local. Crítico si menos del 10% del intercambio es gratis, advirtiendo si menos del 20% es gratis.

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               debian
        service_description             Swap Usage
          check_command                         check_local_swap!20!10
        }
```

Una vez terminado lo anterior verificamos que la configuración este correcta con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

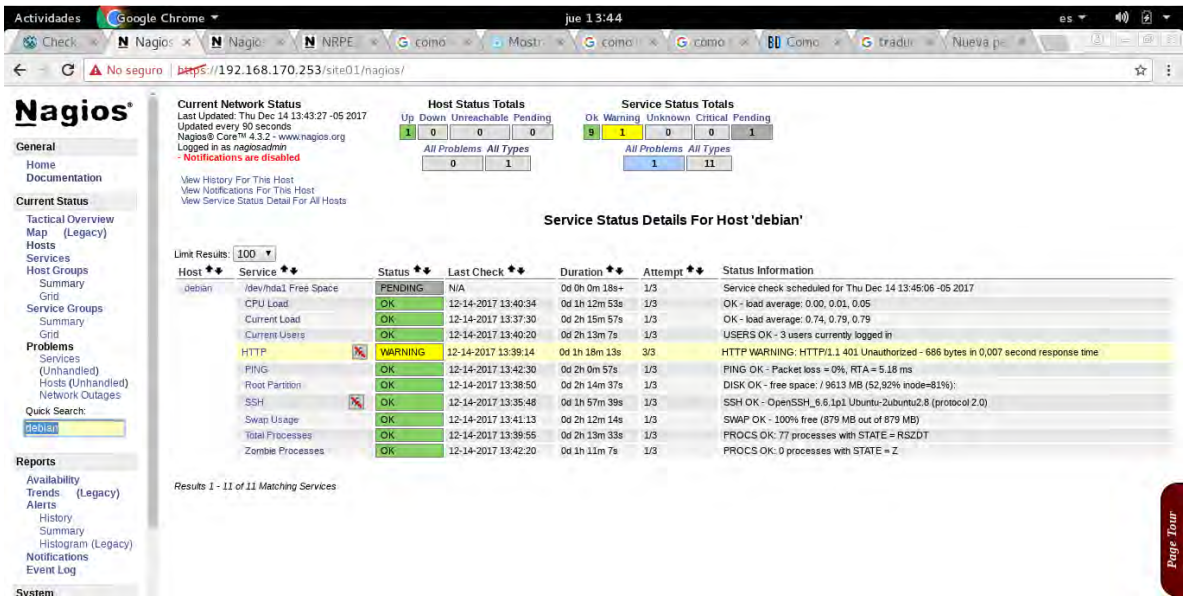
```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

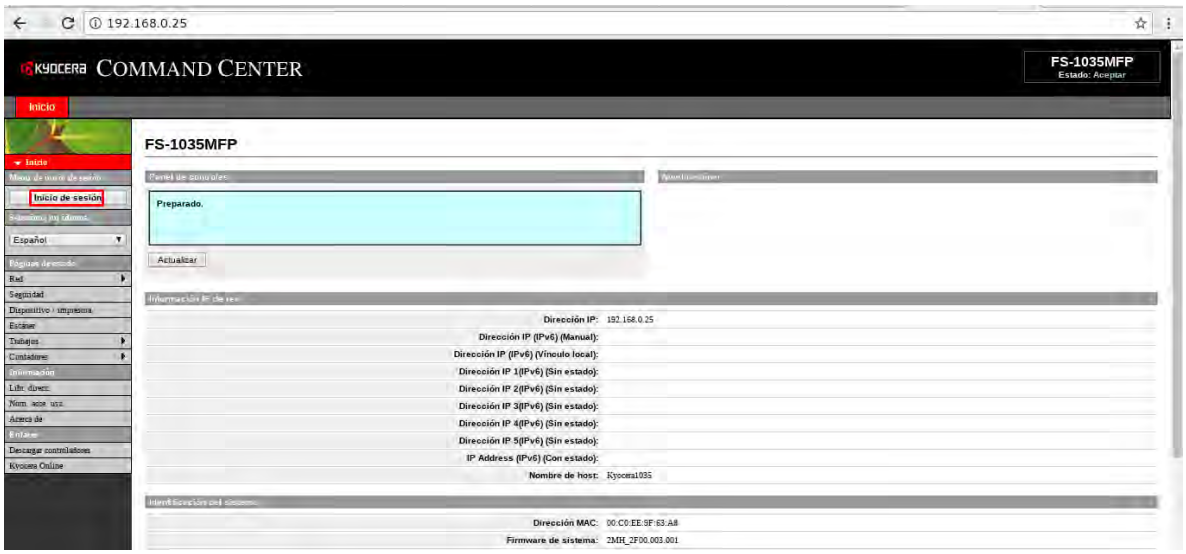
Una vez terminada la definición y configuración, se ingresa a la página de administración de Nagios y podemos mirar la maquina con sus respectivos servicios públicos siendo monitoreados.



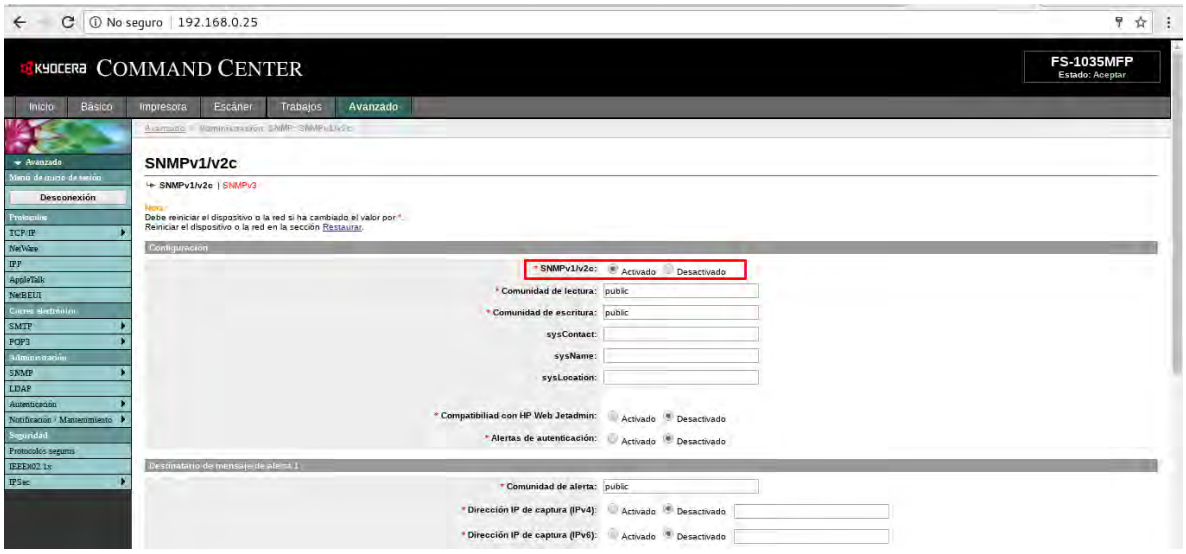
1.3 IMPRESORA

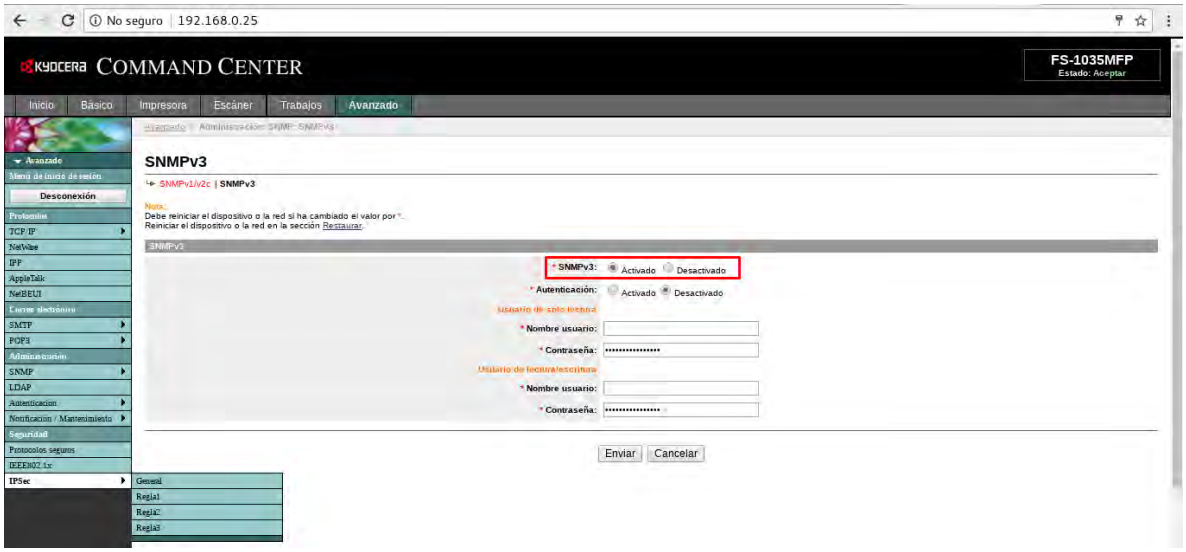
Para realizar el monitoreo de una impresora de red es necesario el protocolo SNMP en cualquiera de sus versiones, en este caso la impresora en red es una Kyocera FS-1035.
Ingresamos a la página de configuración de la impresora. Colocamos la dirección IP asignada a la impresora en la url de un navegador.

Una vez dentro de la página de configuración damos clic sobre el botón *Inicio de sesión.*



En la impresora se ha habilitado las versiones uno, dos, y tres del protocolo SNMP. Para la versión uno y dos se dejan como public.



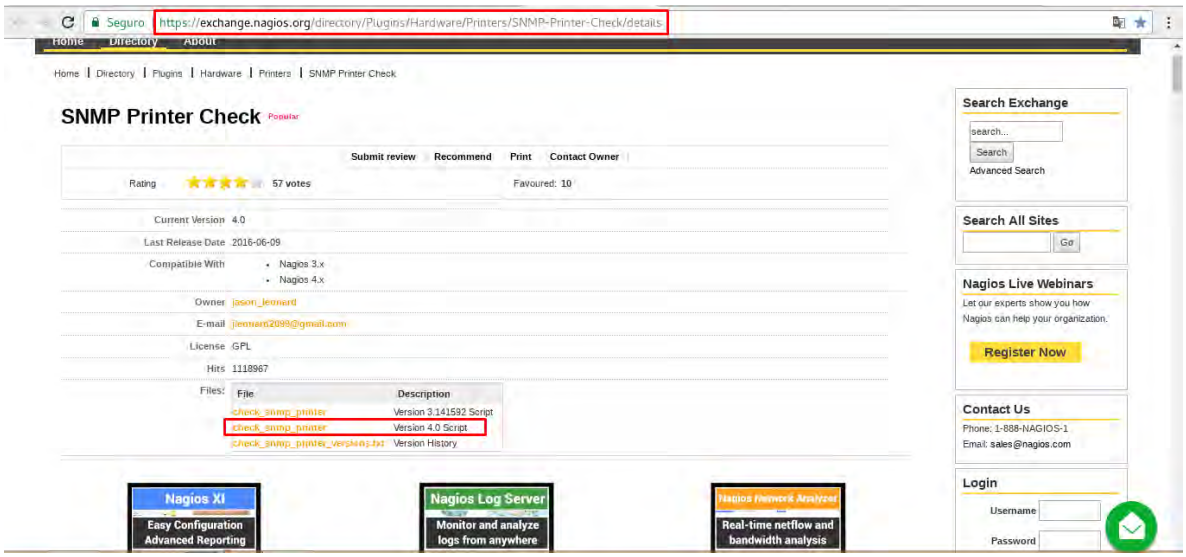


A continuación, se descarga el plugin para el monitoreo de la impresora de red, esto se debe hacer ya que el plugin que viene por defecto en Nagios no sirve para la impresora Kyosera que se va a monitorizar.

Para la descarga se debe dirigir a la página, con la siguiente dirección.

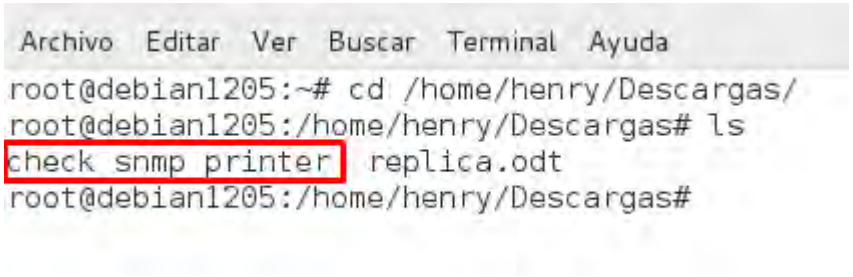
https://exchange.nagios.org/directory/Plugins/Hardware/Printers/SNMP-Printer-Check/details

Una vez se ingresa a la página, se descarga el plugin dando clic sobre ***check_snmp_printer Version 4.0 Script.***



El archivo es guardado en la carpeta Descargas, que para este caso queda en a la siguiente ruta:

```
cd /home/henry/Descargas/
```



Enseguida se mueve el plugin check_snmp_printer a la carpeta libexec que se encuentra en la ruta /usr/local/nagios/libexec

```
cp check_snmp_printer /usr/local/nagios/libexec/
```

Para mirar que el archivo se copió, se debe dirigir a la carpeta libexec.

```
cd /usr/local/nagios/libexec/
```

Se lista el contenido de la carpeta

```
ls
```

Mostrará algo como lo siguiente:



Se debe dar al plugin permisos de lectura y ejecución.

```
chmod 755 check_snmp_printer
```

Es de mucha utilidad saber que parámetros son los que el plugin maneja para su definición, para esto se coloca el siguiente comando donde lista los parámetros y los describe. La “-h” es una abreviación de la palabra en inglés help (ayuda).

```
./chec_snmp_printer -h
```

Una vez hecho lo anterior se procede a realizar la definición de los servicios que se van a monitorear a la impresora, para esto se define el servicio de la impresora en el archivo commands.cfg ubicado en la ruta cd /usr/local/nagios/etc/objects/

```
cd /usr/local/nagios/etc/objects/
nano commands.cfg
```

Una vez dentro del archivo se define el servicio, de la siguiente manera:

```
define command{
   command_name check_printer
   command_line $USER1$/check_snmp_printer -H 192.168.0.25 -C public -t $ARG1$ -w $ARG2$ -c $ARG3$
   }
```

Una vez definido en el archivo commands, se debe dirigir hacia el archivo nagios.cfg que queda en la ruta /usr/local/nagios/etc/objects y descomentar la línea *#cfg_file=/usr/local/nagios/etc/objects/printer.cfg*

```
nano /usr/local/nagios/etc/nagios.cfg
```

La cual debe quedar así:

```
cfg_file=/usr/local/nagios/etc/objects/printer.cfg
```

Luego, se edita el archivo printer.cfg que se encuentra en la ruta /usr/local/nagios/etc/objects/

```
nano /usr/local/nagios/etc/objects/printer.cfg
```

Se configura la definición de la impresora de la siguiente manera.

```
define host{
        use             generic-printer  ; Inherit default values from a template
        host_name       kyocera          ; The name we're giving to this printer
        alias           kioseraH         ; A longer name associated with the printer
        address         192.168.0.25     ; IP address of the printer
        hostgroups      network-printers      ; Host groups this printer is associated
with
        }
```

Dentro del mismo archivo printer.cfg se realiza la definición de los servicios a supervisar.

A continuación, se define el ping hacia la impresora.

```
define service{
        use                     generic-service
        host_name               kyocera
        service_description     PING
        check_command                   check_ping!3000.0,80%!5000.0,100%
        check_interval          10
        retry_interval 1
      }
```

A continuación, se define cómo saber el modelo de la impresora.

```
define service{
        use generic-service
```

```
        host_name kyocera
        service_description Printer_Model
        check_command check_printer!"MODEL"
        }
```

En seguida, se define el servicio de conteo de páginas de la impresora.

```
define service{
        use generic-service
        host_name kyocera
        service_description Contador_paginas
        check_command check_printer!'PAGECOUNT'
        }
```

Luego, se define el servicio del estado de la impresora.

```
define service{
        use generic-service
        host_name kyocera
        service_description Estado_impresora
        check_command check_printer!"STATUS"
        }
```

Seguidamente, se define el servicio del estado de la primera bandeja.

```
define service{
        use generic-service
        host_name kyocera
        service_description Bandeja1
        check_command check_printer!'TRAY 1'
        }
```

Posteriormente, se define el servicio del estado de la segunda bandeja.

```
define service{
        use generic-service
        host_name kyocera
        service_description Bandeja2
        check_command check_printer!"TRAY 2"
        }
```

A continuación, se define el estado del Display de la impresora.

```
define service{
        use generic-service
        host_name kyocera
        service_description Display
        check_command check_printer!"DISPLAY"
        }
```

Despues de esto, verificamos que no haya errores en las definiciones con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

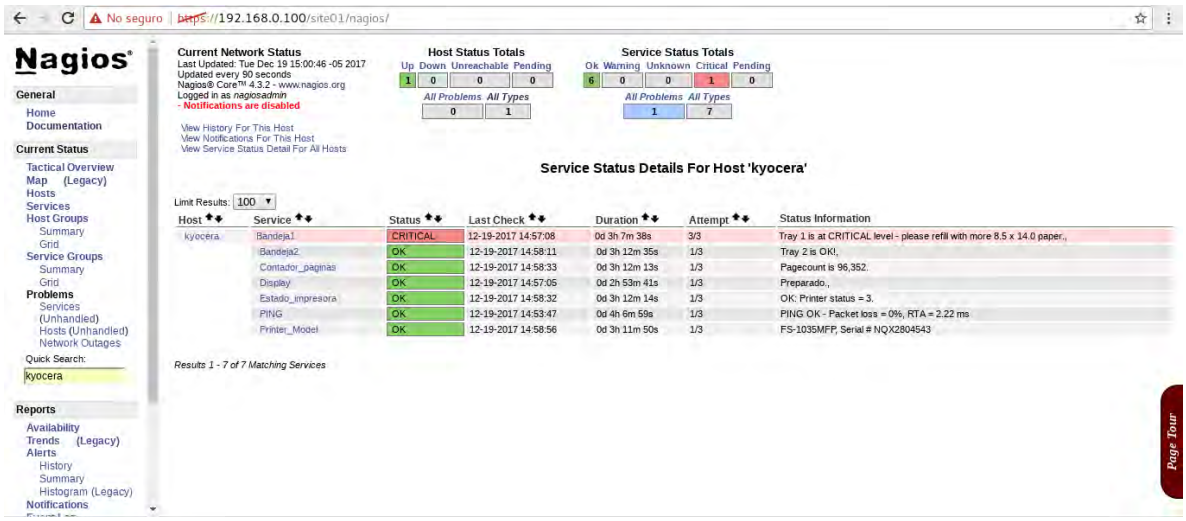
```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

Al ingresar a la página de monitorio de Nagios mostrará algo como lo siguiente.

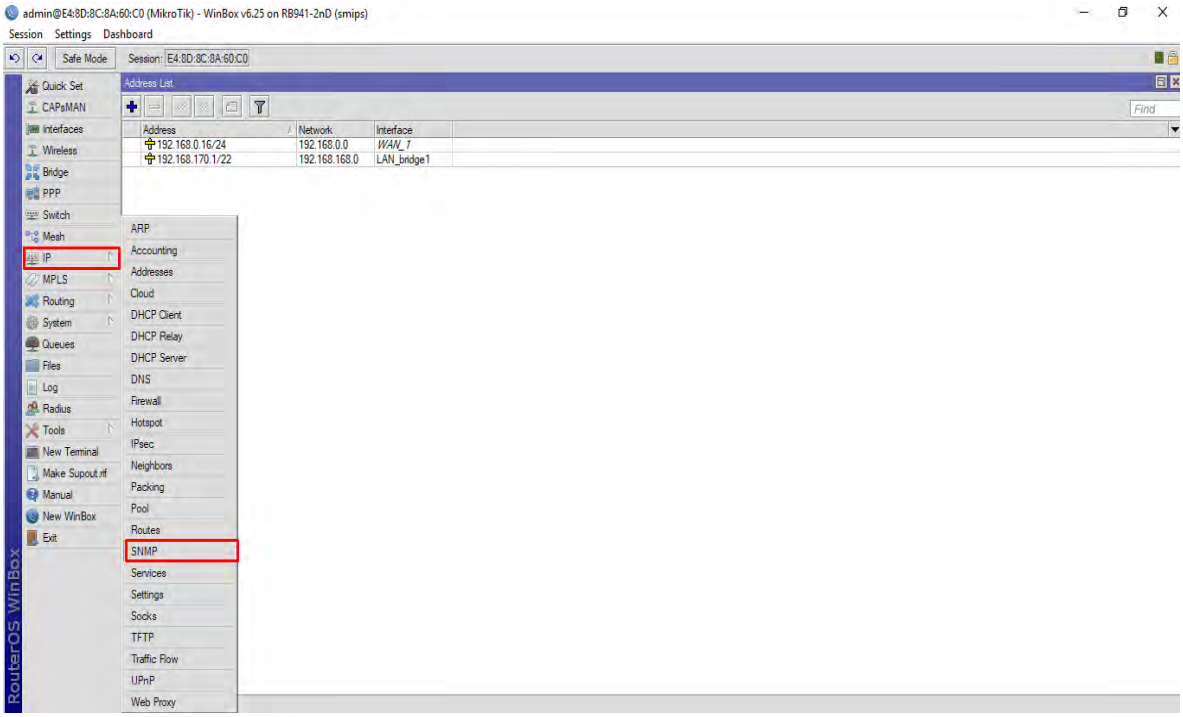


1.4 Switch

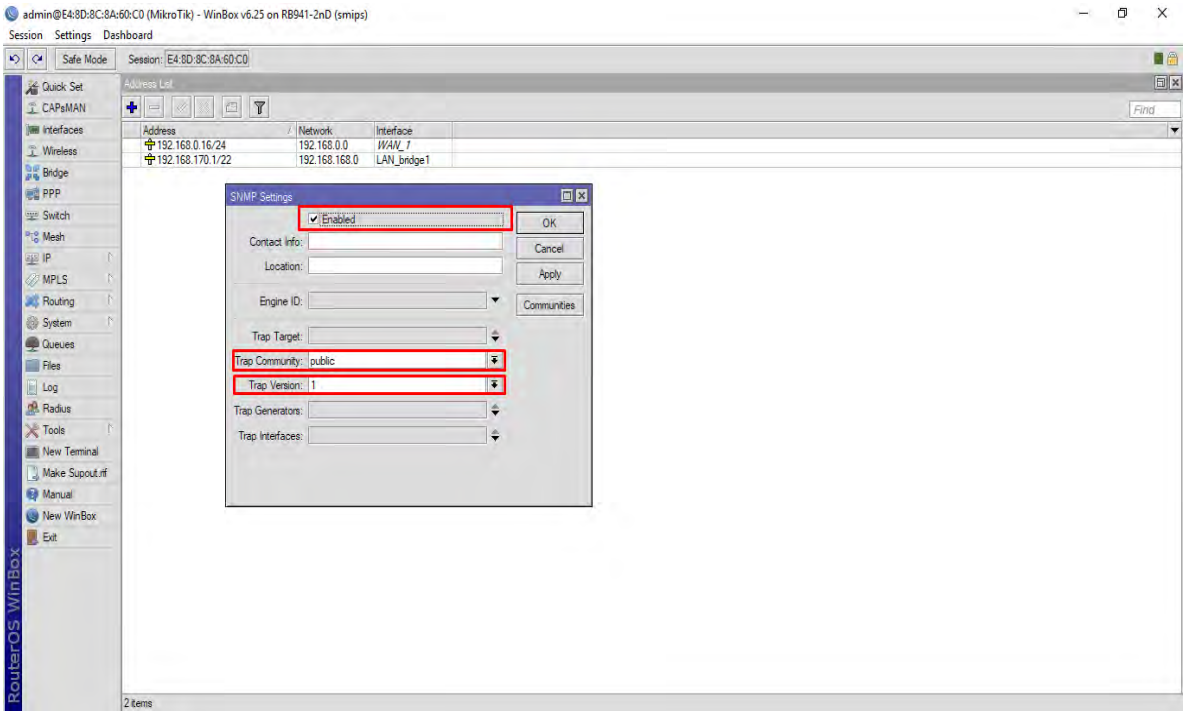
Al igual que para la impresora para poder llevar un monitoreo de un switch es necesario habilitar el protocolo snmp. En este caso se realiza el monitoreo de un switch RouterOS V6.25 Mikrotik.

Como primer paso se activa SNMP en la consola de administración.

Para activarlo se elige la opción SNMP



Se habilita SNMP y se elige el **Trap de Community** como **PUBLIC**.



Luego de activar el protocolo SNMP en el Router, se procede a configurar el servidor NAGIOS.

Se crea el archivo switch.cfg en el directorio */objets*

```
touch switch.cfg /usr/local/nagios/etc/objects/ switch.cfg
```

Creado se edita el archivo para definir el Router a monitorear. Este archivo se encuentra en la ruta: /usr/local/nagios/etc/objects.

Se edita con el comando:

```
nano switch.cfg
```

Dentro de este archivo se define el nombre y la IP del Router a monitorear.

```
define host{
        use             generic-switch         ; Inherit default values from a template
        host_name       Mikrotik               ; The name we're giving to this switch
        alias           Linksys SRW224P Switch  ; A longer name associated with the
switch
        address         192.168.170.1          ; IP address of the switch
```

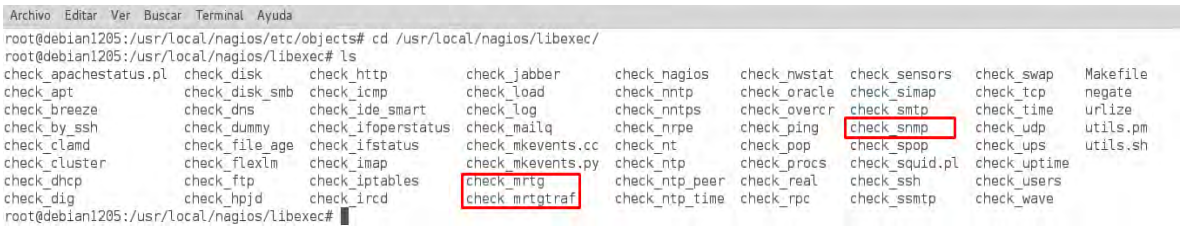
```
        hostgroups      switches                ; Host groups this switch is associated with
        }
```

Para el monitoreo de Routers o switch administrables se utilizan los plugins check_ping, check_snmp y check_ mrtgtraf que están incorporados en Nagios.

Los plugins instalados por defecto en nagios se pueden encontrar en la siguiente ruta:

```
cd /usr/local/nagios/libexec/
```

Se mostrará lo siguiente:



Es de mucha utilidad saber que parámetros son los que el plugins manejan para su definición, para esto se coloca el siguiente comando donde lista los parámetros y los describe.

La “-h” es una abreviación de la palabra en inglés help (ayuda).

```
./check_ping -h
./check_snmp -h
./check_ mrtgtraf -h
```

En el mismo archivo switch.cfg se definen los servicios a monitorear con los parámetros dados por el plugin.

A continuación, se define el servicio del ping para el switch.

```
define service{
        use                     generic-service         ; Inherit values from a template
        host_name               Mikrotik        ; The name of the host the service is associated with
        service_description     PING            ; The service description
        check_command           check_ping!200.0,20%!600.0,60%          ; The command used to monitor the service
        check_interval          5               ; Check the service every 5 minutes
```

```
under normal conditions
        retry_interval 1                ; Re-check the service every minute until its
final/hard state is determined
        }
```

A continuación, se define el tiempo de actividad a través de SNMP.

```
define service{
        use                     generic-service         ; Inherit values from a template
        host_name               Mikrotik
        service_description     Uptime
        check_command                   check_snmp!1.3.6.1.2.1.1.3.0
        }
```

Seguidamente, se define el control del estado del puerto 1 a través de SNMP.

```
define service{
        use                     generic-service         ; Inherit values from a template
        host_name               Mikrotik
        service_description     Port 1 Link Status
        check_command                   check_snmp!1.3.6.1.2.1.1.3.0 -r 1 -m RFC1213-
MIB
        }
```

Los parámetros de los plugins snmp y mrtg están definidos en la ruta:

```
/usr/local/nagios/etc/objects
```

En el archivo commands.cfg

```
nano commands.cfg
```

Se definen parámetros y argumentos según el plugin a utilizar.

Para el plugin check_snmp se define de la siguiente manera.

```
# 'check_snmp' command definition
define command{
       command_name    check_snmp
       command_line    $USER1$/check_snmp -H 192.168.170.1 -P 1 -L authPriv -a
MD5 -C public -U nagios -A start123 -X start123 -o $ARG1$
```

```
}
```

Para el plugin check_local_mrtgtraf se define de la siguiente manera.

```
# 'check_local_mrtgtraf' command definition
define command{
	command_name	check_local_mrtgtraf
	command_line	$USER1$/check_mrtgtraf -F $ARG1$ -a $ARG2$ -w $ARG3$ -c $ARG4$ -e $ARG5$
	}
```

La definición del plugin check_ping ya se encuentra por defecto dentro del archivo commands.cfg, se deja la misma.

Después de esto se procede a descomentar la siguiente línea: "cfg_file=/usr/local/nagios/etc/objects/switch.cfg" que está en el archivo nagios.cfg en la ruta: /usr/local/nagios/etc.

```
nano /usr/local/nagios/etc/nagios.cfg
```

Quedando lo siguiente:

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

NOTA: Para poder monitorear el ancho de banda es necesario instalar MRTG Y SNMP en el servidor Nagios.

Instalación de SNMP

```
apt-get install snmp snmpd
```

Se reinicia el servicio

```
/etc/init.d/snmpd restart
```

Instalacion de MRTG

```
apt-get install mrtg
```

En el servicio donde se monitorea el ancho de banda se coloca la ruta donde se encuentra MRTG en este caso está en: /usr/bin/mrtg

Quedando así:

```
# Monitor bandwidth via MRTG logs

define service{
        use                     generic-service ; Inherit values from a template
        host_name               Mikrotik
        service_description     Port 1 Bandwidth Usage
        check_command
check_local_mrtgtraf!/usr/bin/mrtg!AVG!1000000,1000000!5000000,5000000!10
}
```

Despues de esto verificamos que no haya errores en las definiciones con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

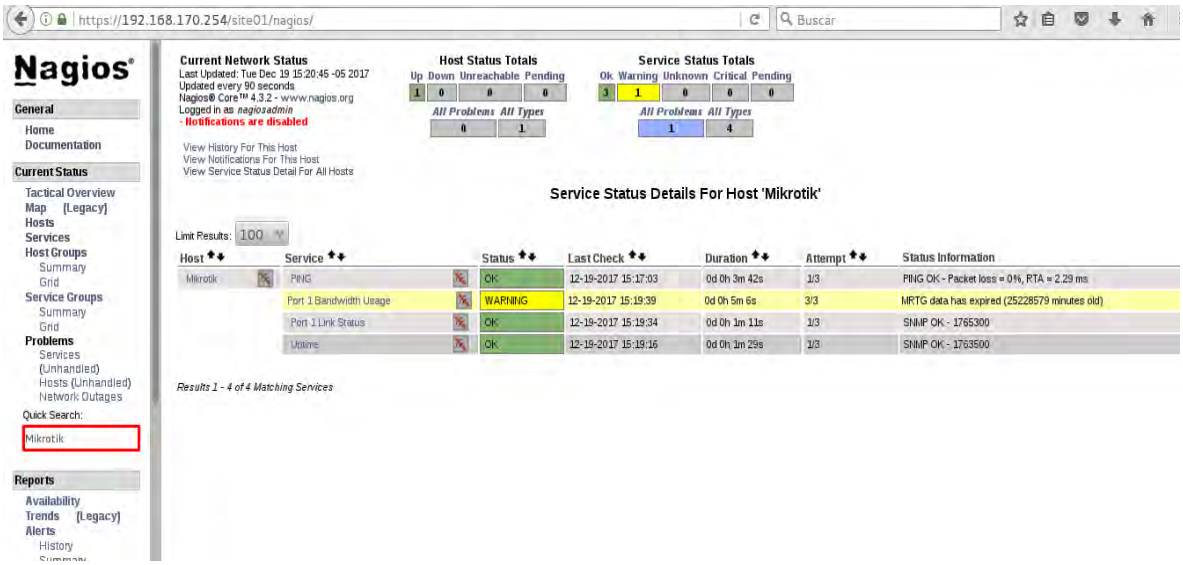
```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

Por último, se verifica el estado del monitoreo en Nagios.



2. SERVICIOS PUBLICOS

Dentro de la empresa algunos servicios públicos se encuentran instalados en un mismo servidor, los servidores físicos de nombre Azkaban y Voldemort (nombres asignados en la red de datos). La siguiente tabla muestra los servicios instalados en los servidores que van a ser monitoreados.

SERVIDOR AZKABAN	SERVIDOR VOLDEMORT
Servicio ssh	Servicio ssh
Servicio ftp	Servicio web (apache)
Servicio chat (openfire)	Servicio proxy (squid)
	Servicio dns (bind9)

Se debe tener en cuenta que los servidores azkaban y voldemort fueron previamente creados en check_mk, es decir que no es necesario hacer la definición de estos servidores en Nagios, por lo tanto, a continuación, se mostrará la configuración y definición de comandos y servicios para la supervisión de los servicios públicos descritos en la tabla anterior.

2.1 SERVICIO SSH EN SERVIDOR AZKABAN Y VOLDEMORT

Nagios cuenta con el plugin check_ssh, el cual viene con el paquete de plugin de Nagios al momento de realizar la instalación, dicho plugin cumple con la función de supervisar el servicio ssh.

El paquete de plugin de Nagios, se encuentra en directorio libexec. Para poder mirar los plugins que vienen con Nagios y posteriormente los plugins que se instalarán, verificamos el contenido del directorio. Se debe tener en cuenta que los puglins pueden ser modificados en su código a conveniencia.

```
ls /usr/local/nagios/libexec
```

Una ayuda muy útil al momento de querer realizar la configuración de un servicio es poder mirar que argumentos son los que acepta el plugin al momento de definirlo, para esto basta con escribir un camando: (./nombre_plugin -h), donde la “h” hace referencia a “help”, ayuda.

Se debe estar ubicado en el directorio libexec donde se encuentran los plugins.

```
cd /usr/local/nagios/libexec
```

En el caso del plugin check_ssh se coloca.

```
./check_ssh -h
```

Como es un plugin que viene por defecto, el archivo commands.cfg contiene la definición del comando para poder utilizarlo.

Se ingresa al archivo.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez dentro del archivo el plugin debe estar definido de la siguiente manera.

```
define command{
        command_name    check_ssh
        command_line    $USER1$/check_ssh $ARG1$ $HOSTADDRESS$
        }
```

Una vez definido el comando, se realiza la definición del servicio, para esto se crea un archivo en donde se van a definir todos los servicios a monitorear.

En primer lugar se debe crear la ruta donde va a existir el archivo, la ruta se la define dentro del archivo nagios.cfg.

Nota: existen rutas preestablecidas que se pueden descomentar para dar uso en cualquier momento.

```
nano /usr/local/nagios/etc/nagios.cfg
```

Una vez dentro del archivo, en el apartado (OBJECTS CONFIGURATIONS FILE(S)), se define la ruta del archivo servicios.cfg. Se debe tener en cuenta que en este apartado se pueden crear rutas tanto como para archivos (cfg_file) y directorios (cfg_dir).

```
cfg_file=/usr/local/nagios/etc/objects/servicios.cfg
```

Una vez creada la ruta, se crea el archivo servicios.cfg dentro del directorio objects.

```
touch /usr/local/nagios/etc/objects/servicios.cfg
```

Ahora, en el archivo creado se procede a definir el servicio ssh del servidor azkaban.

A continuación se muestra una configuración en donde se verifica el funcionamiento del servidor ssh, genera una alerta si el servidor no responde dentro de cinco (5) segundos o si la cadena de la versión del servidor no coincide con el argumento.

```
define service {
   use             generic-service     ; Inherit default values from a template
   host_name       azkaban
   service_description SSH-verifica Puerto Tiempo en 5s y Vers.
   check_command       check_ssh!-p 5707!-t 5!-r "OpenSSH_6.6.1p1"
   }
```

La misma definición es utilizada para el servicio ssh instalado en el servidor voldemort, dentro del archivo servicios.cfg, se diferencia en el nombre del host (host_name) donde debe ir el nombre de este.

```
define service {
   use             generic-service     ; Inherit default values from a template
   host_name       voldemort
   service_description SSH-verifica Puerto Tiempo en 5s y Vers.
   check_command       check_ssh!-p 5706!-t 5!-r "OpenSSH_6.6.1p1"
   }
```

Despues de esto verificamos que no haya errores en las definiciones con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

2.2 SERVICIO FTP EN SERVIDOR AZKABAN

Nagios cuenta con el plugin check_ftp, el cual viene con el paquete de plugin de Nagios. Con este es posible supervisar el servicio ftp que se encuentra instalado en el servidor azkaban.

Para mirar que el plugin se encuentra, listamos el directorio libexec.

```
ls /usr/local/nagios/libexec
```

A continuación, observamos que argumentos son los que acepta el plugin, para esto se debe estar ubicado en el directorio libexec donde se encuentran los plugins.

```
cd /usr/local/nagios/libexec
```

Se coloca.

```
./check_ftp -h
```

Como es un plugin que viene por defecto, el archivo commands.cfg contiene la definición del comando para poder utilizarlo.

Se ingresa al archivo.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez dentro del archivo el plugin debe estar definido de la siguiente manera.

```
define command{
```

```
    command_name    check_ftp
    command_line    $USER1$/check_ftp -H $HOSTADDRESS$ $ARG1$
    }
```

Definido el comando, se realiza la definición del servicio ftp instalado en el servidor azkaban dentro del archivo servicios.cfg

A continuación, se muestra una configuración en donde se verificará que el servidor FTP se ejecuta en el puerto 1023 en el host remoto. Generará una alerta si el servidor no responde dentro de 5 segundos o si la respuesta del servidor no contiene la cadena "vsFTPd 3.0.2".

```
define service {
   use              generic-service     ; Inherit default values from a template
   host_name        azkaban
   service_description Special FTP
   check_command       check_ftp!-p 21!-t 5!-e "vsFTPd 3.0.2"
   }
```

Despues de esto, verificamos que no haya errores en las definiciones con el siguiente comando.

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

Si todo esta correcto se mostrará algo como lo siguiente.

```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

2.3 SERVICIO DE MENSAJERIA INSTANTANEA (OPENFIRE) EN SERVIDOR AZKABAN

Al tener instalado el servicio de mensajería instantánea OPENFIRE, en el servidor azkaban, y este hacer uso del protocolo jabber conocido formalmente como XMPP (**Extensible Messaging and Presence Protocol**), es posible supervisarlo mediante

el plugin check_jabber que viene previamente instalado en el paquete de plugin de Nagios.

Para mirar que el plugin se encuentra, listamos el directorio libexec.

```
ls /usr/local/nagios/libexec
```

A continuación, observamos que argumentos acepta el plugin, para esto se debe estar ubicado en el directorio libexec donde se encuentran los plugins.

```
cd /usr/local/nagios/libexec
```

Se coloca.

```
./check_jabber -h
```

Aunque el plugin viene por defecto no está definido en el archivo commands.cfg, por lo que es necesario definirlo

Se ingresa al archivo.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez dentro del archivo se debe definir el comando de la siguiente manera.

```
define command{
      command_name check_jabber
      command_line $USER1$/check_jabber -H 192.168.170.7
}
```

Definido el comando, se realiza la definición del servicio dentro del archivo servicios.cfg.
La primera y más básica producirá alertas si el servidor web no responde dentro de 10 segundos.

```
define service{
      use                     generic-service
      host_name                azkaban
      service_description        Estado OpenFire
      check_command              check_jabber
      }
```

Despúes de esto, verificamos que no haya errores en las definiciones con el

siguiente comando.

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

Si todo esta correcto se mostrará algo como lo siguiente.

```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

2.4 SERVICIO WEB (APACHE) SERVIDOR VOLDEMORT

Anteriormente solo se utilizaron los puglin que vienen en el paquete de Nagios. Para el monitoreo del servicio web apache se hará uso de dos plugin, check_http y check_apachestatus.pl, el primero pertenece al paquete de monitoreo que viene por defecto con Nagios, y el segundo a un plugin desarrollado por la comunidad nagiosexchenge para el monitoreo especifico de apache.

Se comenzará describiendo la forma de utilización y configuración de check_http.

Para mirar que el plugin se encuentra, listamos el directorio libexec.

```
ls /usr/local/nagios/libexec
```

A continuación, observamos que argumentos son los que acepta el plugin, para esto se debe estar ubicado en el directorio libexec donde se encuentran los plugins.

```
cd /usr/local/nagios/libexec
```

Se coloca.

```
./check_http -h
```

Como es un plugin que viene por defecto, el archivo commands.cfg contiene la definición del comando para poder utilizarlo.

Se ingresa al archivo.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez dentro del archivo el plugin debe estar definido de la siguiente manera.

```
define command{
        command_name    check_http
        command_line    $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
        }
```

Definido el comando, se realiza la definición del servicio dentro del archivo servicios.cfg, para este caso se realizan varias verificaciones.

La primera y más básica producirá alertas si el servidor web no responde dentro de 10 segundos o si devuelve códigos de error HTTP (403, 404, etc.). Eso es lo que se necesita para un control básico.

```
define service{
        use                     generic-service
        host_name               voldemort
        service_description     Estado de apache2
        check_command           check_http
        }
```

A continuación, se muestra una configuración en donde se verificará la dirección y el puerto por donde está corriendo el servicio de web de apache.

```
define service{
        use                     generic-service
        host_name               localhost
        service_description     Estado de apache2
        check_command           check_http!192.168.170.100!8080
        }
```

En la siguiente definición de servicio se verifica la disponibilidad de una pagina https://192.168.170.100/site01/nagios.

```
define service{
        use                     generic-service
        host_name               localhost
        service_description     pagina disponible
```

```
    check_command                    check_http!192.168.170.100!-u
https://192.168.170.100/site01/nagios
    }
```

Como se dijo anteriormente también se hizo uso de un plugin que al igual que el plugin check_http permite monitorear el servicio web de apache.

El plugin es check_apachestatus.pl el cual puede ser descargado de la siguiente manera.

Colocando en la url la siguiente dirección.

```
https://exchange.nagios.org/components/com_mtree/attachment.php?link_id=137
6&cf_id=24
```

Una vez descargado, el archivo se encuentra en el directorio Descargas, se debe ubicar en esta ruta y copiar el archivo al directorio libexec.

Nota: el directorio /henry se debe cambiar por el directorio personal se tenga por defecto.

```
cd /home/henry/Descargas/
cp check_apachestatus.pl /usr/local/nagios/libexec
```

Y damos permisos.

```
cd /usr/local/nagios/libexec
chmod 755 check_apachestatus.pl
```

A continuación, observamos que argumentos son los que acepta el plugin, para esto se debe estar ubicado en el directorio libexec en donde se copió el plugin.

Se coloca.

```
./check_apachestatus.pl -h
```

Para su definición, al contrario de los anteriores, por ser un plugin descargado no viene definido el comando en el archivo commands.cfg, por lo que se debe definirlo.

Se ingresa al archivo.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez dentro del archivo, el plugin se lo debe definir de la siguiente manera.

```
define command{
        command_name    check_apachestatus
        command_line    $USER1$/check_apachestatus.pl -H $HOSTADDRESS$ -p
$ARG1$
        }
```

Definido el comando, se realiza la definición del servicio dentro del archivo servicios.cfg

A continuación, se muestra una configuración en donde se verificará que el servicio web apache está escuchando por el puerto 80.

```
define service{
        use                     generic-service
        host_name               voldemort
        service_description     Estado de apache
        check_command           check_apachestatus!-p 80
        }
```

Despues de esto verificamos que no haya errores en las definiciones con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

2.5 SERVICIO PROXY (SQUID) SERVIDOR VOLDEMORT

Para la supervisión del servicio proxy se hará uso del plugin check_squid.pl, este plugin no pertenece al paquete de plugin de Nagios, por lo que es necesario

descargarlo.

Antes de realizar la instalación y configuración del puglin se descarga dos librerías para su funcionamiento.

```
sudo apt-get install libwww-perl libnagios-plugin-perl
```

Luego, se coloca en la url la siguiente dirección.

```
https://exchange.nagios.org/components/com_mtree/attachment.php?link_id=1402&cf_id=24
```

Una vez descargado, el archivo se encuentra en el directorio Descargas, se debe ubicar en esta ruta y copiar el archivo al directorio libexec.

Nota: el directorio /henry se debe cambiar por el directorio personal se tenga por defecto.

```
cd /home/henry/Descargas/
cp check_squid.pl /usr/local/nagios/libexec
```

Y damos permisos.

```
cd /usr/local/nagios/libexec
chmod 755 check_squid.pl
```

Enseguida ingresamos al archivo check_squid.pl, y se modifica la línea donde se define la ruta en donde se va a instalar en plugin, por defecto viene con la siguiente ruta:
(use lib "/usr/lib/nagios/plugins";) se la debe modificar por la siguientes.

```
use lib "/usr/local/nagios/libexec"
```

A continuación, verificamos que argumentos son los que acepta el plugin.

Se coloca.

```
./check_apachestatus.pl -h
```

Por ser un plugin nuevo no viene definido el comando en el archivo commands.cfg, por lo que se debe definirlo.

Se ingresa al archivo.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez dentro del archivo, el plugin se lo debe definir de la siguiente manera.

```
define command{
	command_name	check-squid
	command_line	$USER1$/check_squid.pl -u $ARG1$ -p $ARG2$ -l $ARG3$ -
e $ARG4$
	}
```

Definido el comando, se realiza la definición del servicio dentro del archivo servicios.cfg

A continuación, se muestra una configuración en donde se verificará que el servicio proxy squid tenga acceso a internet, en este caso la url no debe estar denegada en el proxy, si la url estuviese denegada mostraría un mensaje de denegación de acceso. También se verifica la dirección ip y puerto donde está corriendo el servicio.

Por último, se coloca un valor entero el cual pertenece a un ccódigo http que debe ser devuelto.

```
define service{
	use			generic-service
	host_name		voldemort
	service_description	Squid Proxy
	check_command		check-
squid!https://www.google.com!192.168.170.6!3128!200
	}
```

Despues de esto verificamos que no haya errores en las definiciones con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

2.6 SERVICIO DNS (BIND9) SERVIDOR VOLDEMORT

Para la supervisión del servicio dns se hace uso del plugin check_dns el cual viene el paquete de plugins de Nagios.

Para mirar que el plugin se encuentra, listamos el directorio libexec.

```
ls /usr/local/nagios/libexec
```

A continuación, observamos que argumentos acepta el plugin, para esto se debe estar ubicado en el directorio libexec donde se encuentran los plugins.

```
cd /usr/local/nagios/libexec
```

Se coloca.

```
./check_dns -h
```

Aunque el plugin viene por defecto no está definido en el archivo commands.cfg, por lo que es necesario definirlo

Se ingresa al archivo.

```
nano /usr/local/nagios/etc/objects/commands.cfg
```

Una vez dentro del archivo se debe definir el comando de la siguiente manera.

```
define command {
        command_name    check_dns
        command_line    $USER1$/check_dns -H $ARG1$ -w $ARG2$ -c $ARG3$
}
```

Definido el comando, se realiza la definición del servicio dentro del archivo servicios.cfg.

En la definición del servicio se supervisa mediante el nombre de dominio que se desea consultar, en este caso electro.com donde se encuentra alojado el servicio dns, el tiempo de respuesta, poniendo unos límites donde si supera los diez segundos pasaría a un estado warning (advertencia) y si supera los quince

segundos a un estado de critical (critico).

```
define service{
        use                     generic-service         ; Name of service template to use
        host_name               voldemort
        service_description     tiempo de respuesta dns
        check_command           check_dns!electro.com!10!15
        }
```

Despues de esto verificamos que no haya errores en las definiciones con el siguiente comando.

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

Si todo esta correcto se mostrara algo como lo siguiente.

```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Al comprobar que todo está correcto, entonces se reinicia el servicio de Nagios.

```
service nagios restart
```

Anexo M. Funcionamiento de suite de monitoreo.

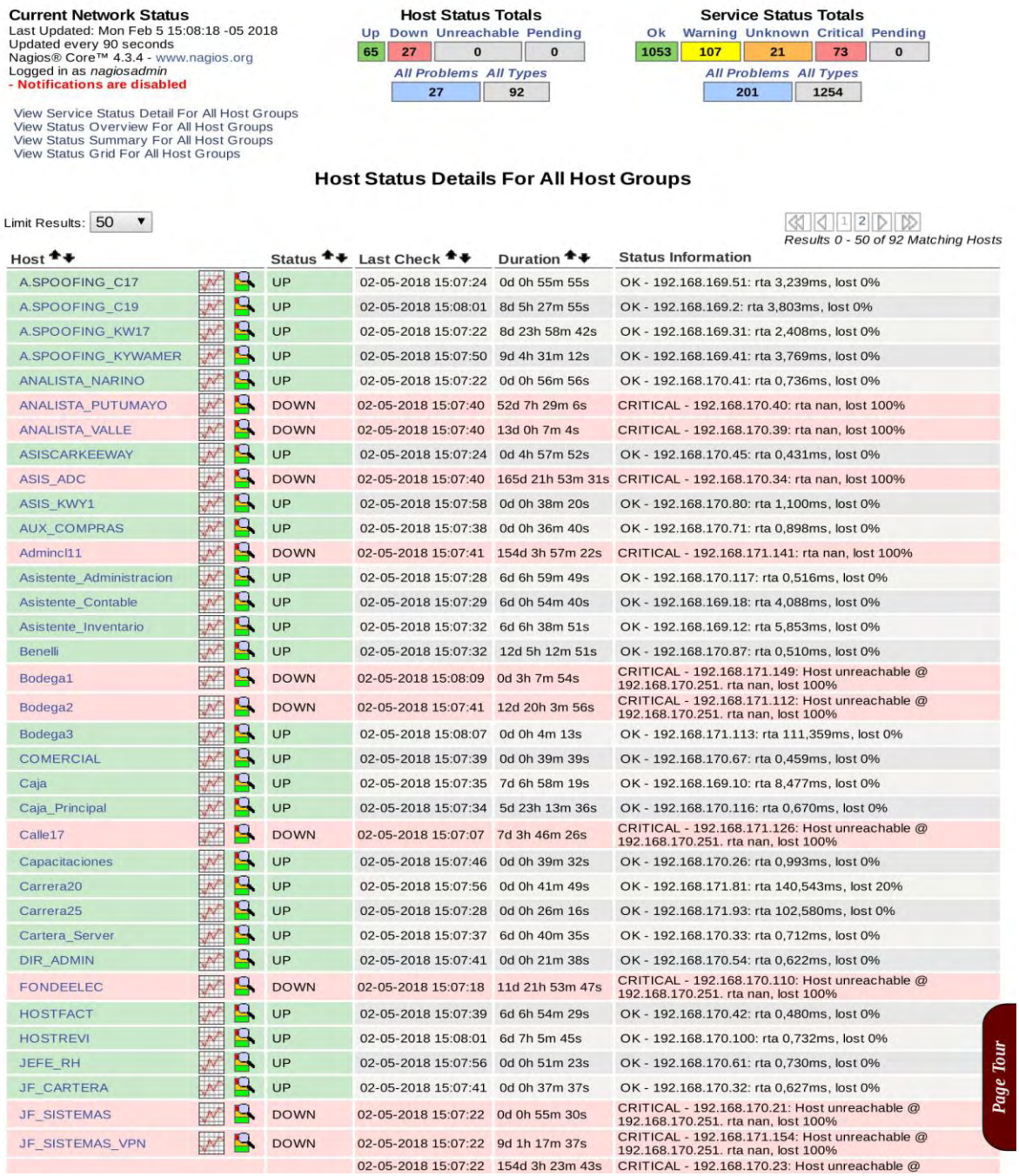
ÍNIDICE

Pág.

1. FUNCIONAMIENTO CON NAGIOS.....573
2. FUNCIONAMIENTO CON CHECK_MK.....576
3. FUNCIONAMIENTO CON MAPEO CON NAGVIS 581
4. FUNCIONAMIENTO CON PNP4.....600
5. FUNCIONAMIENTO ENVÍO DE NOTIFICACIONES 603

1. FUNCIONAMIENTO CON NAGIOS

Con Nagios se observa el estado de todos los host.



Current Network Status
Last Updated: Mon Feb 5 15:08:18 -05 2018
Updated every 90 seconds
Nagios® Core™ 4.3.4 - www.nagios.org
Logged in as *nagiosadmin*
- Notifications are disabled

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
65	27	0	0

All Problems	All Types
27	92

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
1053	107	21	73	0

All Problems	All Types
201	1254

Host Status Details For All Host Groups

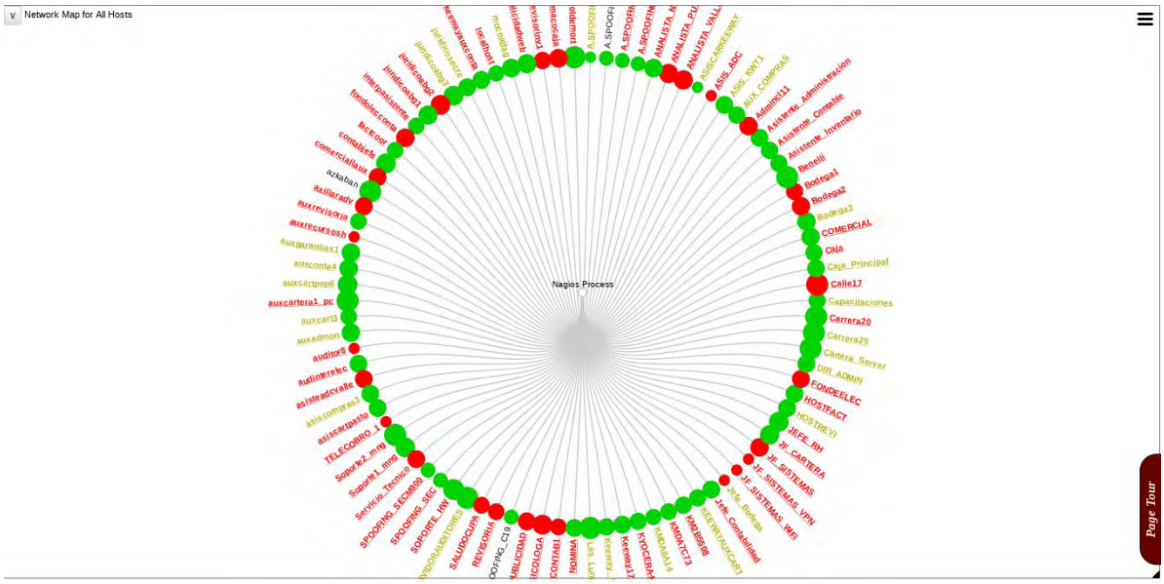
Limit Results: 50

Results 0 - 50 of 92 Matching Hosts

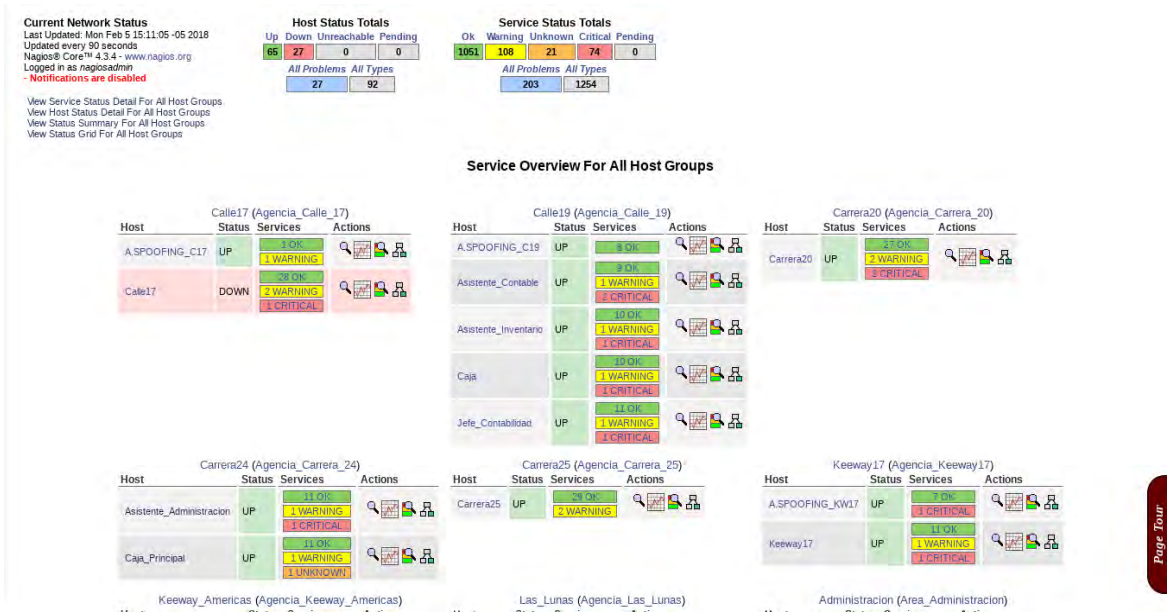
Host	Status	Last Check	Duration	Status Information
A.SPOOFING_C17	UP	02-05-2018 15:07:24	0d 0h 55m 55s	OK - 192.168.169.51: rta 3,239ms, lost 0%
A.SPOOFING_C19	UP	02-05-2018 15:08:01	8d 5h 27m 55s	OK - 192.168.169.2: rta 3,803ms, lost 0%
A.SPOOFING_KW17	UP	02-05-2018 15:07:22	8d 23h 58m 42s	OK - 192.168.169.31: rta 2,408ms, lost 0%
A.SPOOFING_KYWAMER	UP	02-05-2018 15:07:50	9d 4h 31m 12s	OK - 192.168.169.41: rta 3,769ms, lost 0%
ANALISTA_NARINO	UP	02-05-2018 15:07:22	0d 0h 56m 56s	OK - 192.168.170.41: rta 0,736ms, lost 0%
ANALISTA_PUTUMAYO	DOWN	02-05-2018 15:07:40	52d 7h 29m 6s	CRITICAL - 192.168.170.40: rta nan, lost 100%
ANALISTA_VALLE	DOWN	02-05-2018 15:07:40	13d 0h 7m 4s	CRITICAL - 192.168.170.39: rta nan, lost 100%
ASISCARKEEWAY	UP	02-05-2018 15:07:24	0d 4h 57m 52s	OK - 192.168.170.45: rta 0,431ms, lost 0%
ASIS_ADC	DOWN	02-05-2018 15:07:40	165d 21h 53m 31s	CRITICAL - 192.168.170.34: rta nan, lost 100%
ASIS_KWY1	UP	02-05-2018 15:07:58	0d 0h 38m 20s	OK - 192.168.170.80: rta 1,100ms, lost 0%
AUX_COMPRAS	UP	02-05-2018 15:07:38	0d 0h 36m 40s	OK - 192.168.170.71: rta 0,898ms, lost 0%
Admincl11	DOWN	02-05-2018 15:07:41	154d 3h 57m 22s	CRITICAL - 192.168.171.141: rta nan, lost 100%
Asistente_Administracion	UP	02-05-2018 15:07:28	6d 6h 59m 49s	OK - 192.168.170.117: rta 0,516ms, lost 0%
Asistente_Contable	UP	02-05-2018 15:07:29	6d 0h 54m 40s	OK - 192.168.169.18: rta 4,088ms, lost 0%
Asistente_Inventario	UP	02-05-2018 15:07:32	6d 6h 38m 51s	OK - 192.168.169.12: rta 5,853ms, lost 0%
Benelli	UP	02-05-2018 15:07:32	12d 5h 12m 51s	OK - 192.168.170.87: rta 0,510ms, lost 0%
Bodega1	DOWN	02-05-2018 15:08:09	0d 3h 7m 54s	CRITICAL - 192.168.171.149: Host unreachable @ 192.168.170.251. rta nan, lost 100%
Bodega2	DOWN	02-05-2018 15:07:41	12d 20h 3m 56s	CRITICAL - 192.168.171.112: Host unreachable @ 192.168.170.251. rta nan, lost 100%
Bodega3	UP	02-05-2018 15:08:07	0d 0h 4m 13s	OK - 192.168.171.113: rta 111,359ms, lost 0%
COMERCIAL	UP	02-05-2018 15:07:39	0d 0h 39m 39s	OK - 192.168.170.67: rta 0,459ms, lost 0%
Caja	UP	02-05-2018 15:07:35	7d 6h 58m 19s	OK - 192.168.169.10: rta 8,477ms, lost 0%
Caja_Principal	UP	02-05-2018 15:07:34	5d 23h 13m 36s	OK - 192.168.170.116: rta 0,670ms, lost 0%
Calle17	DOWN	02-05-2018 15:07:07	7d 3h 46m 26s	CRITICAL - 192.168.171.126: Host unreachable @ 192.168.170.251. rta nan, lost 100%
Capacitaciones	UP	02-05-2018 15:07:46	0d 0h 39m 32s	OK - 192.168.170.26: rta 0,993ms, lost 0%
Carrera20	UP	02-05-2018 15:07:56	0d 0h 41m 49s	OK - 192.168.171.81: rta 140,543ms, lost 20%
Carrera25	UP	02-05-2018 15:07:28	0d 0h 26m 16s	OK - 192.168.171.93: rta 102,580ms, lost 0%
Cartera_Server	UP	02-05-2018 15:07:37	6d 0h 40m 35s	OK - 192.168.170.33: rta 0,712ms, lost 0%
DIR_ADMIN	UP	02-05-2018 15:07:41	0d 0h 21m 38s	OK - 192.168.170.54: rta 0,622ms, lost 0%
FONDEELEC	DOWN	02-05-2018 15:07:18	11d 21h 53m 47s	CRITICAL - 192.168.170.110: Host unreachable @ 192.168.170.251. rta nan, lost 100%
HOSTFACT	UP	02-05-2018 15:07:39	6d 6h 54m 29s	OK - 192.168.170.42: rta 0,480ms, lost 0%
HOSTREVI	UP	02-05-2018 15:08:01	6d 7h 5m 45s	OK - 192.168.170.100: rta 0,732ms, lost 0%
JEFE_RH	UP	02-05-2018 15:07:56	0d 0h 51m 23s	OK - 192.168.170.61: rta 0,730ms, lost 0%
JF_CARTERA	UP	02-05-2018 15:07:41	0d 0h 37m 37s	OK - 192.168.170.32: rta 0,627ms, lost 0%
JF_SISTEMAS	DOWN	02-05-2018 15:07:22	0d 0h 55m 30s	CRITICAL - 192.168.170.21: Host unreachable @ 192.168.170.251. rta nan, lost 100%
JF_SISTEMAS_VPN	DOWN	02-05-2018 15:07:22	9d 1h 17m 37s	CRITICAL - 192.168.171.154: Host unreachable @ 192.168.170.251. rta nan, lost 100%
		02-05-2018 15:07:22	154d 3h 23m 43s	CRITICAL - 192.168.170.23: Host unreachable @

Page Tour

Se observa el mapa de los host.



Con Nagios se pueden observar los grupos de host de la siguiente manera:





Keeway_Americas (Agencia_Keeway_Americas)

Host	Status	Services	Actions
A.SPOOFING_KYWAMER	UP	7 OK 1 CRITICAL	
Keeway_Americas	UP	10 OK 2 WARNING	

Las_Lunas (Agencia_Las_Lunas)

Host	Status	Services	Actions
Las_Lunas	UP	43 OK 2 WARNING	

Administracion (Area_Administracion)

Host	Status	Services	Actions
DIR_ADMIN	UP	11 OK 2 WARNING	
JEFE_RH	UP	13 OK 2 WARNING 1 CRITICAL	
NOMINA	UP	11 OK 1 WARNING 1 CRITICAL	
PSICOLOGA	DOWN	13 OK 1 WARNING 2 CRITICAL	
SALUDOCUPA	DOWN	9 OK 1 WARNING 1 CRITICAL	
auxrecursosh	DOWN	1 WARNING 1 CRITICAL	

Analista (Area_Analista)

Host	Status	Services	Actions
ANALISTA_NARINO	UP	12 OK 1 WARNING 1 CRITICAL	
ANALISTA_PUTUMAYO	DOWN	13 OK 1 WARNING 1 CRITICAL	
ANALISTA_VALLE	DOWN	11 OK 2 WARNING 1 UNKNOWN 1 CRITICAL	

Cartera (Area_Cartera)

Host	Status	Services	Actions
ASISCARKEEWAY	UP	1 OK 1 WARNING	
ASIS_ADC	DOWN	1 WARNING 1 CRITICAL	
Cartera_Server	UP	26 OK 3 WARNING	
JF_CARTERA	UP	11 OK 2 WARNING 1 UNKNOWN 1 CRITICAL	
KEEWAYAUXCART	UP	11 OK 1 WARNING	
TELECOBRO_1	DOWN	1 WARNING 1 CRITICAL	
asiscartpasto	UP	11 OK 1 WARNING 1 CRITICAL	

Comercial (Area_Comercial)

Host	Status	Services	Actions
AUX_COMPRAS	UP	11 OK 1 WARNING	
COMERCIAL	UP	12 OK 1 WARNING 1 CRITICAL	
comercialaux	DOWN	10 OK 2 WARNING 1 CRITICAL	

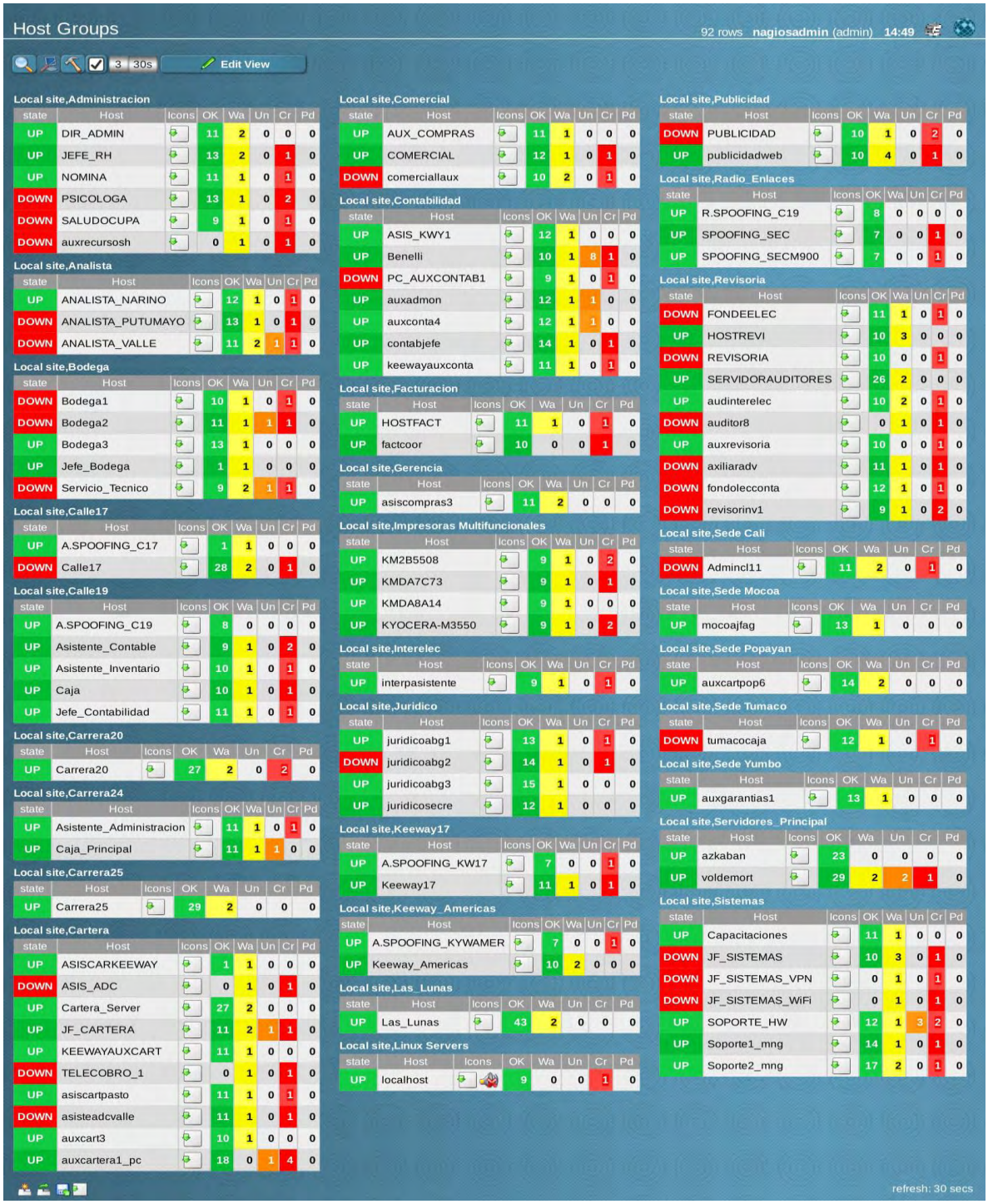
Page Tour

2. FUNCIONAMIENTO CON CHECK_MK

Se visualizan los estados de los servicios de cada host por grupos con check_mk.



Mediante check_mk se visualizan los grupos de host así:



Se muestra el monitoreo del servidor Azkaban con sus servicios de red SSH, FTP y OPENFIRE.



State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Check_MK		OK - Agent version 1.2.6p12, execution time 0.2 sec	2018-01-15 09:43:01	59 sec	178 ms
OK	Check_MK Discovery		OK - no unmonitored services found, no vanished services found	2017-08-10 11:04:02	19 min	
OK	CPU load		OK - 15 min load 0.06 at 2 Cores (0.03 per Core)	2017-08-10 10:43:27	59 sec	0.170
OK	CPU utilization		OK - user: 1.0%, system: 0.6%, wait: 1.5%, steal: 0.0%, guest: 0.0%, total: 3.0%	2017-08-10 10:43:27	59 sec	3.05%
OK	Disk IO SUMMARY		OK - Utilization: 0.1%, Read: 0.00 B/s, Write: 7.02 kB/s, Average Wait: 0.90 ms, Average Read Wait: 0.00 ms, Average Write Wait: 0.90 ms, Latency: 0.90 ms	2017-08-10 10:43:27	59 sec	0 B/s / 7.02 kB/s
OK	Estado OpenFire		JABBER OK - 0,005 second response time on 192.168.170.7 port 5222	2018-01-25 17:36:03	102 sec	
OK	Filesystem /		OK - 9.8% used (4.50 of 45.71 GB), trend: +52.85 kB / 24 hours	2017-08-10 10:43:27	59 sec	9.8%
OK	Filesystem /home		OK - 7.0% used (6.40 of 91.54 GB), trend: +682.49 B / 24 hours	2017-08-10 10:43:27	59 sec	7%
OK	Filesystem /var		OK - 7.7% used (11.42 of 148.38 GB), trend: -74.61 kB / 24 hours	2017-08-10 10:43:27	59 sec	7.7%
OK	Interface 2		OK - [eth0] (up) MAC: E8:94:F6:02:B9:A5, 1 Gbit/s, in: 18.62 kB/s(0.0%), out: 15.68 kB/s(0.0%)	2017-08-10 10:43:27	59 sec	18.62 kB/s / 15.68 kB/s
OK	Kernel Context Switches		OK - 321/s	2017-08-10 10:44:27	59 sec	321.1/s
OK	Kernel Major Page Faults		OK - 0/s	2017-08-10 10:44:27	59 sec	0/s
OK	Kernel Process Creations		OK - 2/s	2017-08-10 10:44:27	59 sec	1.75/s
OK	Memory		OK - RAM used: 1.32 GB of 3.74 GB, Swap used: 9.26 MB of 7.52 GB, Total virtual memory used: 1.33 GB of 11.25 GB (11.8%),	2017-08-10 10:43:27	59 sec	1.32 GB
OK	Mount options of /		OK - Mount options exactly as expected	2017-08-10 10:43:27	59 sec	
OK	Mount options of /home		OK - Mount options exactly as expected	2017-08-10 10:43:27	59 sec	
OK	Mount options of /var		OK - Mount options exactly as expected	2017-08-10 10:43:27	59 sec	
OK	Number of threads		OK - 287 threads	2017-08-10 10:43:27	59 sec	287
OK	SSH-verifica Puerto Tiempo en 5s y Vers.		SSH OK - OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.6 (protocol 2.0)	2018-01-15 09:43:14	18 sec	
OK	Special FTP		FTP OK - 0,007 second response time on 192.168.170.7 port 21 [220 ********** BIENVENIDOS AL SERVIDOR FTP ELECTRO **********]	2018-01-15 09:43:16	3 min	
OK	TCP Connections		OK - ESTABLISHED: 135, TIME_WAIT: 1, LISTEN: 25	2017-08-10 10:43:27	59 sec	
OK	Temperature Zone 0		OK - 40.0 °C	2017-08-10 10:43:27	59 sec	40 °C
OK	Uptime		OK - Up since Fri Jan 12 18:45:08 2018 (23d 20:12:29)	2017-08-10 10:43:27	60 sec	24 d

Se muestra el monitoreo del servidor Voldemort con sus servicios de red SSH, HTTP, DNS, PROXY.



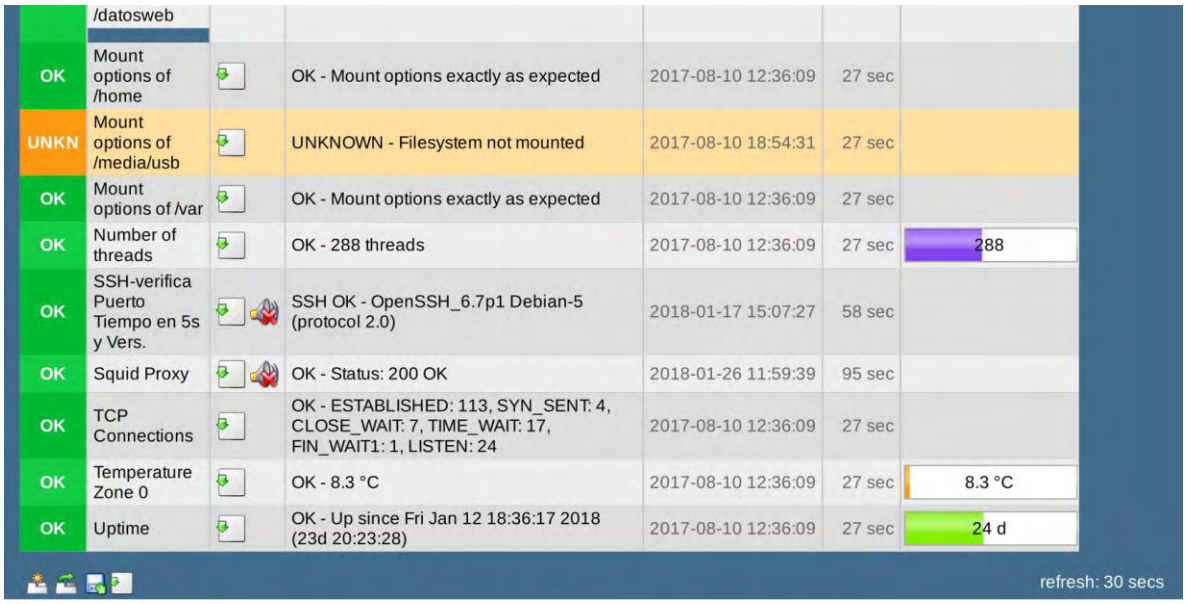
Services of Host voldemort

34 rows **nagiosadmin** (admin) **15:00**

3 30s | Host notifications | Edit View | Availability | ...

voldemort

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Check_MK		OK - Agent version 1.2.6p12, execution time 0.1 sec	2018-01-15 09:43:00	27 sec	97.0 ms
OK	Check_MK Discovery		OK - no unmonitored services found, 2 vanished services (df:1, mounts:1)	2017-08-10 13:06:09	9 min	
OK	CPU load		OK - 15 min load 0.11 at 8 Cores (0.01 per Core)	2017-08-10 12:36:09	27 sec	0.170
OK	CPU utilization		OK - user: 0.3%, system: 0.3%, wait: 0.1%, steal: 0.0%, guest: 0.0%, total: 0.7%	2017-08-10 12:36:09	27 sec	0.72%
OK	DNS electro.com		DNS OK: 0,126 seconds response time. electro.com returns 185.53.178.6	4 hrs	25 sec	
OK	Disk IO SUMMARY		OK - Utilization: 0.8%, Read: 763.66 B/s, Write: 19.32 kB/s, Average Wait: 11.89 ms, Average Read Wait: 6.29 ms, Average Write Wait: 12.27 ms, Latency: 4.22 ms	2017-08-10 12:36:09	27 sec	764 B/s / 19.32 kB/s
WARN	Estado de apache2		HTTP WARNING: HTTP/1.1 403 Forbidden - 3505 bytes in 0,001 second response time	4 hrs	11 sec	3505000.0 ms
CRIT	Estado de apache		CRITICAL 403 Forbidden	4 hrs	3 min	
OK	Filesystem /		OK - 13.3% used (6.08 of 45.71 GB), trend: -0.09 B / 24 hours	2017-08-10 12:36:09	27 sec	13.3%
OK	Filesystem /cache		OK - 5.1% used (12.93 of 253.07 GB), trend: 0.00 B / 24 hours	2017-08-10 12:36:09	27 sec	5.1%
WARN	Filesystem /datosbd		WARN - 86.8% used (79.46 of 91.54 GB), (warn/crit at 80.00/90.00%), trend: +65.99 MB / 24 hours	2018-01-15 09:43:01	27 sec	86.8%
OK	Filesystem /datosweb		OK - 5.2% used (14.37 of 274.89 GB), trend: +30.97 kB / 24 hours	2017-08-10 12:36:09	27 sec	5.2%
OK	Filesystem /home		OK - 5.4% used (2.48 of 45.71 GB), trend: +0.00 B / 24 hours	2017-08-10 12:36:09	27 sec	5.4%
UNKN	Filesystem /media/usb		UNKNOWN - filesystem not found	2017-08-10 18:54:31	27 sec	
OK	Filesystem /var		OK - 6.0% used (22.10 of 366.56 GB), trend: +4.16 MB / 24 hours	2017-08-10 12:36:09	27 sec	6%
OK	Interface 2		OK - [eth1] (up) speed unknown, in: 75.98 kB/s, out: 1.17 MB/s	2017-08-10 12:36:09	27 sec	75.98 kB/s / 1.17 MB/s
OK	Interface 3		OK - [eth0] (up) speed unknown, in: 1.15 MB/s, out: 54.50 kB/s	2017-08-10 12:36:09	27 sec	1.15 MB/s / 54.50 kB/s
OK	Kernel Context Switches		OK - 567/s	2017-08-10 12:37:36	27 sec	567.12/s
OK	Kernel Major Page Faults		OK - 0/s	2017-08-10 12:37:36	27 sec	0/s
OK	Kernel Process Creations		OK - 2/s	2017-08-10 12:37:36	27 sec	1.53/s
OK	Memory		OK - RAM used: 1.25 GB of 11.76 GB, Swap used: 185.10 MB of 22.34 GB, Total virtual memory used: 1.43 GB of 34.10 GB (4.2%),	2017-08-10 12:36:09	27 sec	1.25 GB
OK	Mount options of /		OK - Mount options exactly as expected	2017-08-10 12:36:09	27 sec	
OK	Mount options of /cache		OK - Mount options exactly as expected	2017-08-10 12:36:09	27 sec	
OK	Mount options of /datosbd		OK - Mount options exactly as expected	2017-08-10 12:36:09	27 sec	
OK	Mount options of		OK - Mount options exactly as expected	2017-08-10 12:36:09	27 sec	

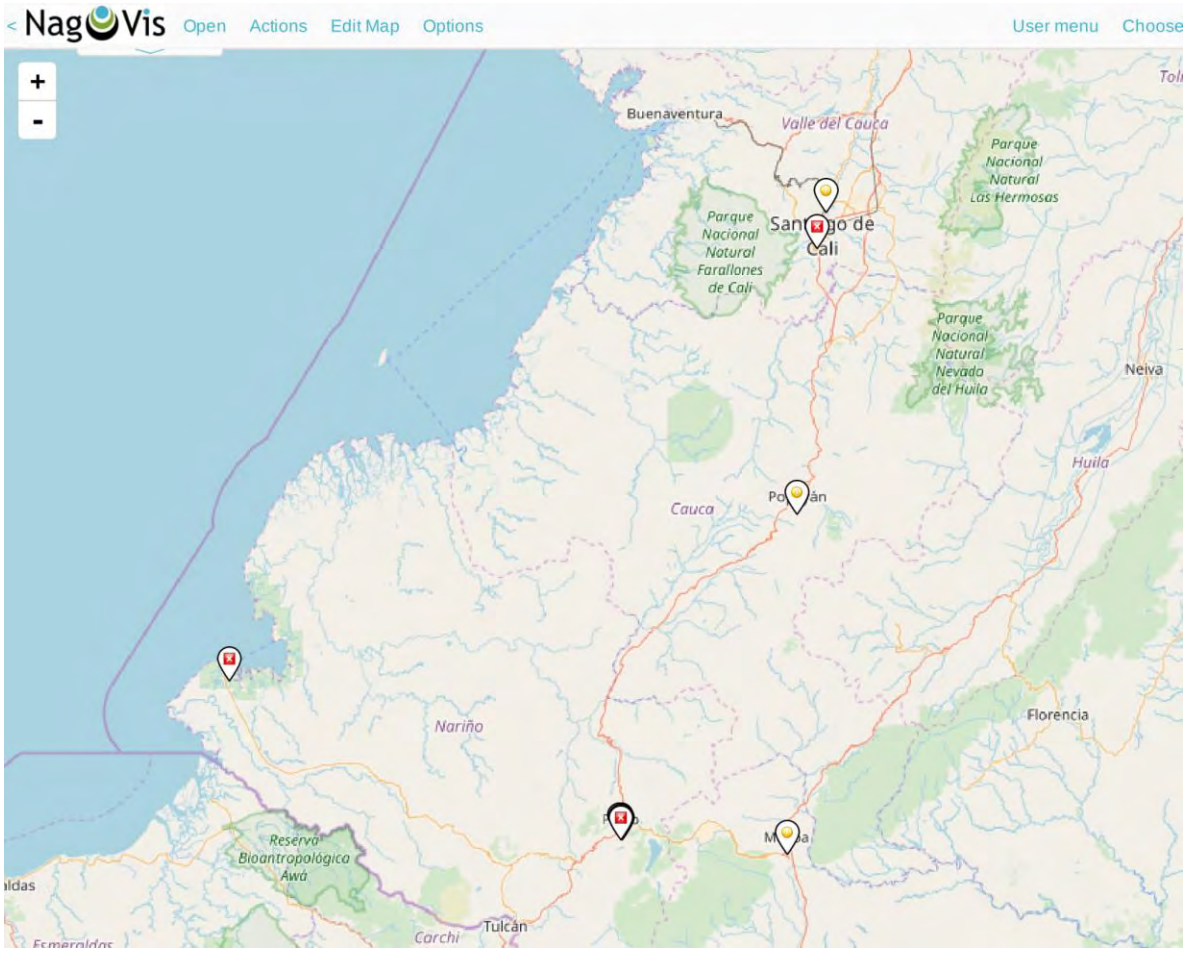


	/datosweb					
OK	Mount options of /home		OK - Mount options exactly as expected	2017-08-10 12:36:09	27 sec	
UNKN	Mount options of /media/usb		UNKNOWN - Filesystem not mounted	2017-08-10 18:54:31	27 sec	
OK	Mount options of /var		OK - Mount options exactly as expected	2017-08-10 12:36:09	27 sec	
OK	Number of threads		OK - 288 threads	2017-08-10 12:36:09	27 sec	288
OK	SSH-verifica Puerto Tiempo en 5s y Vers.		SSH OK - OpenSSH_6.7p1 Debian-5 (protocol 2.0)	2018-01-17 15:07:27	58 sec	
OK	Squid Proxy		OK - Status: 200 OK	2018-01-26 11:59:39	95 sec	
OK	TCP Connections		OK - ESTABLISHED: 113, SYN_SENT: 4, CLOSE_WAIT: 7, TIME_WAIT: 17, FIN_WAIT1: 1, LISTEN: 24	2017-08-10 12:36:09	27 sec	
OK	Temperature Zone 0		OK - 8.3 °C	2017-08-10 12:36:09	27 sec	8.3 °C
OK	Uptime		OK - Up since Fri Jan 12 18:36:17 2018 (23d 20:23:28)	2017-08-10 12:36:09	27 sec	24 d

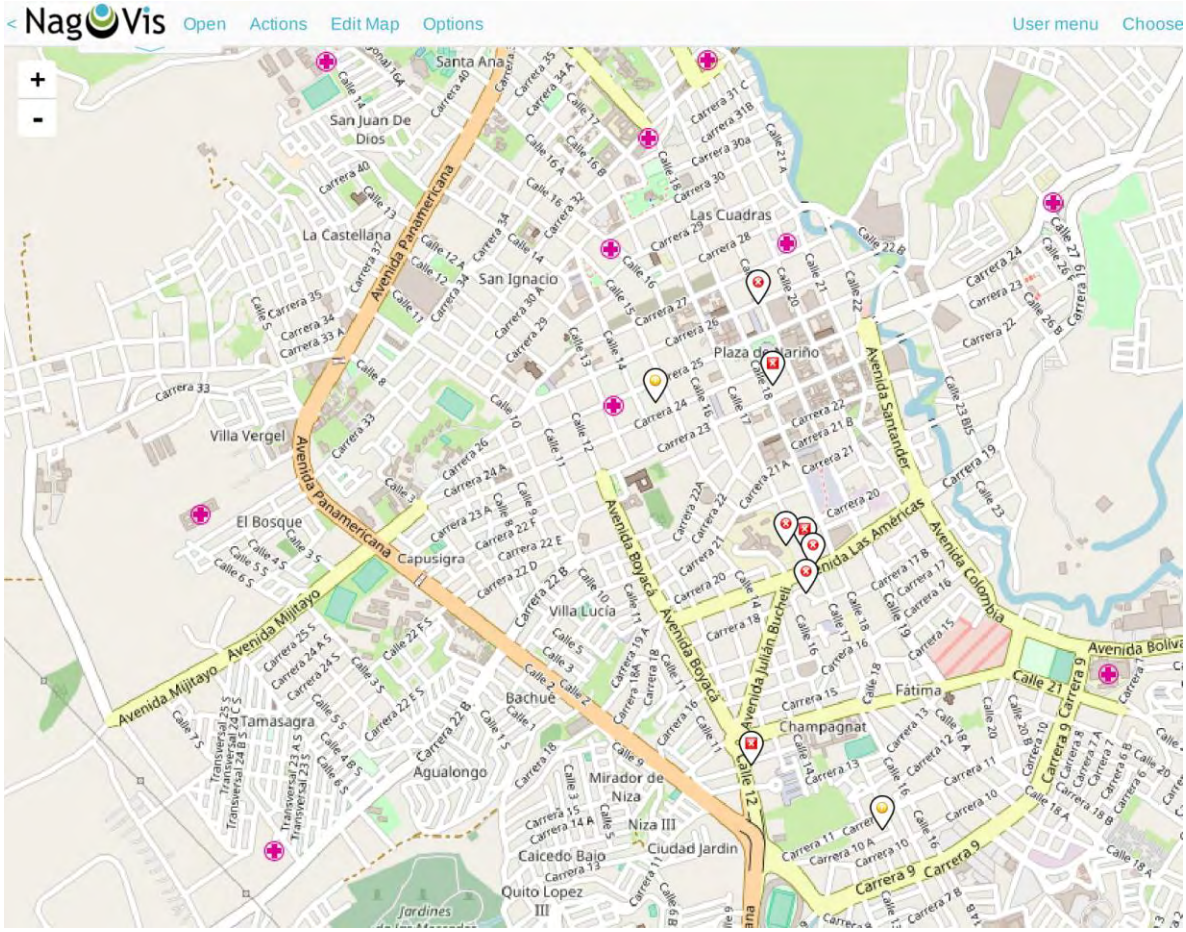
refresh: 30 secs

3. FUNCIONAMIENTO CON MAPEO CON NAGVIS

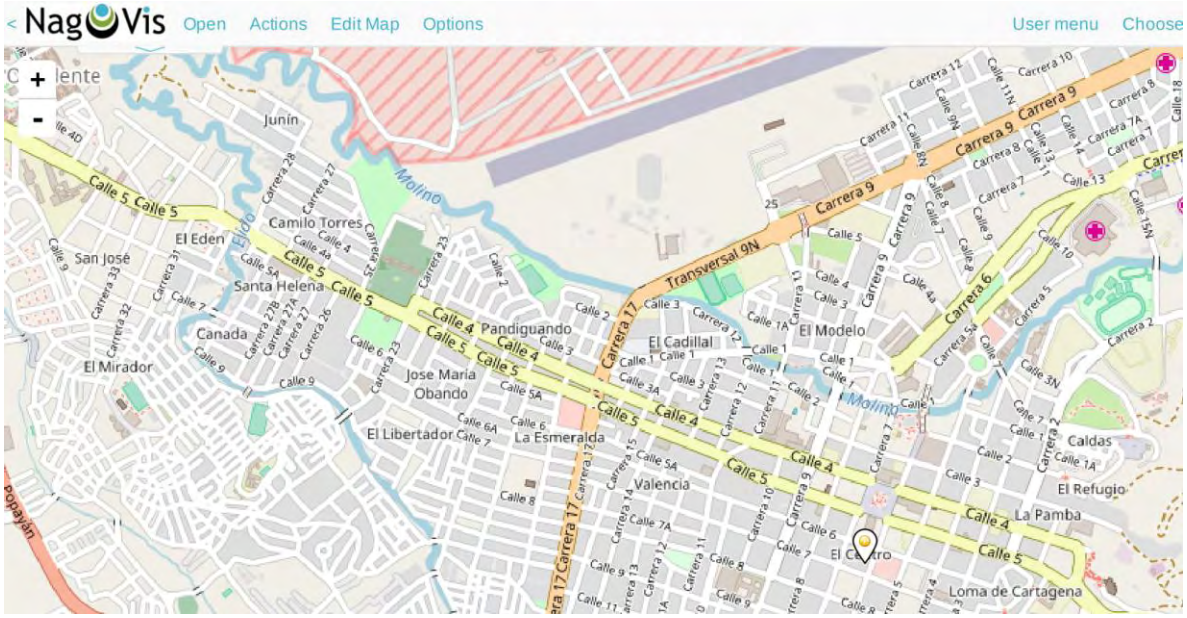
Se muestra con Nagvis el Geomapa Regional de los Departamentos donde se encuentran agencias monitoreadas.



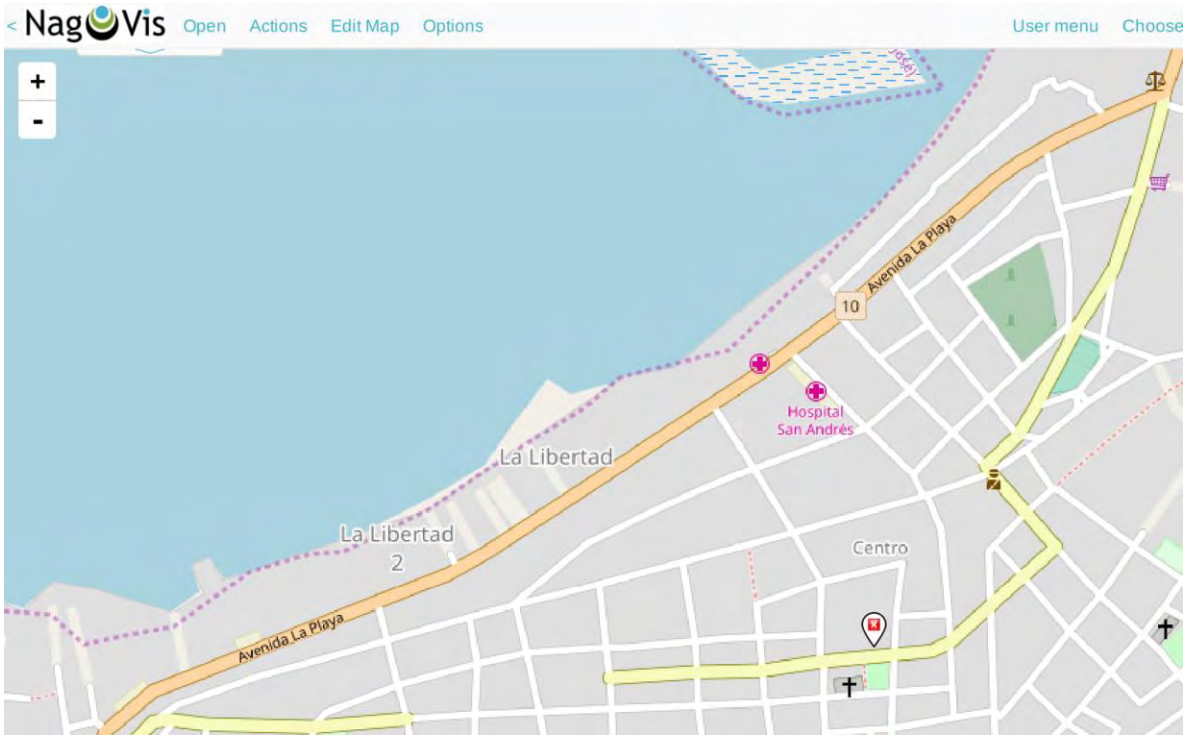
Geomapa agencias de Pasto.



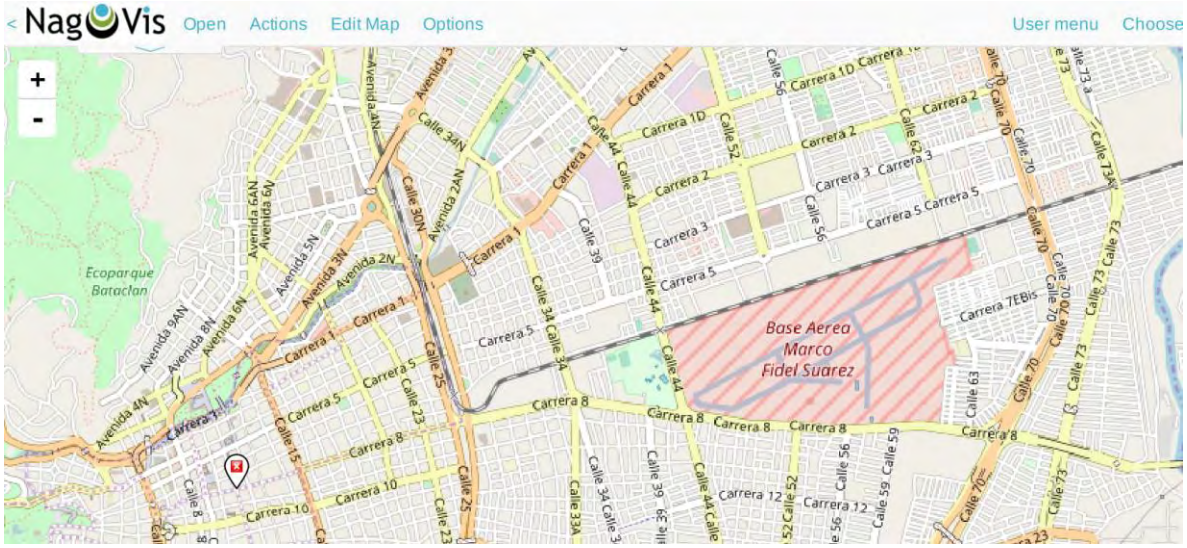
Geomapa agencia de Popayan.



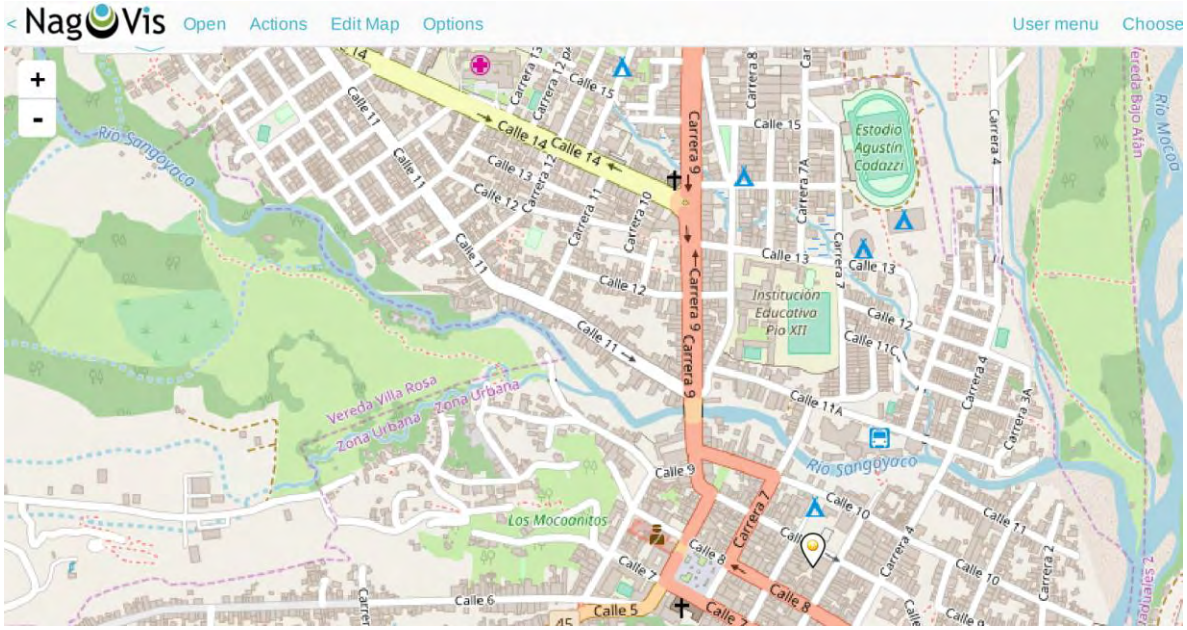
Geomapa agencia de Tumaco.



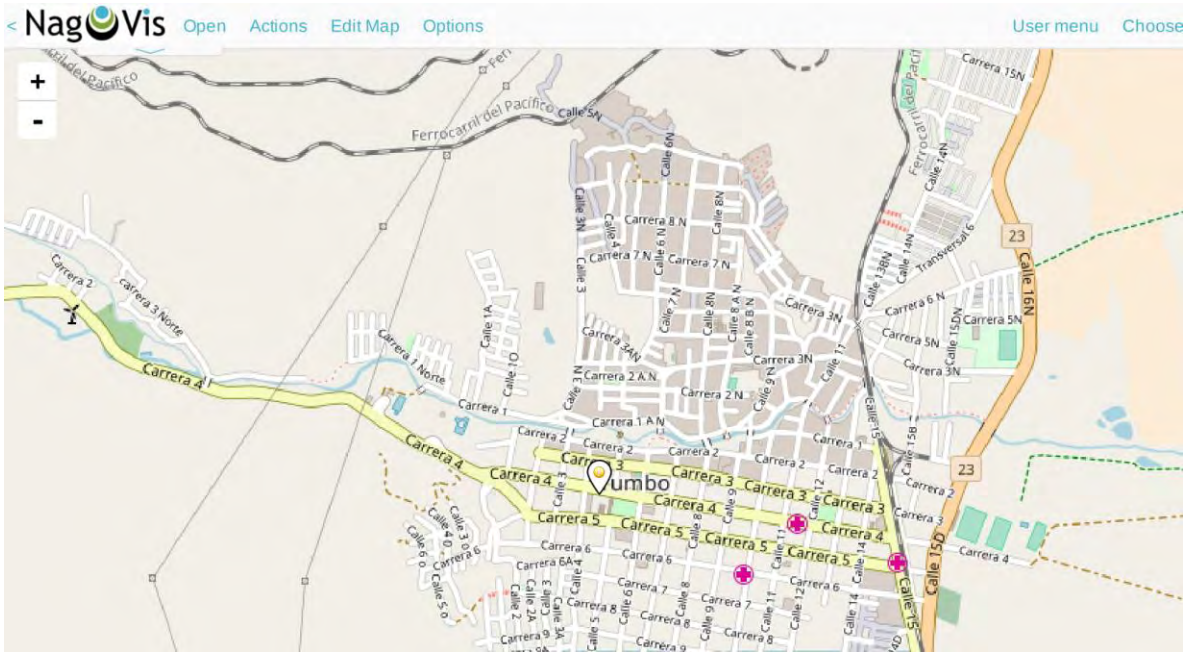
Geomapa agencia de Cali.



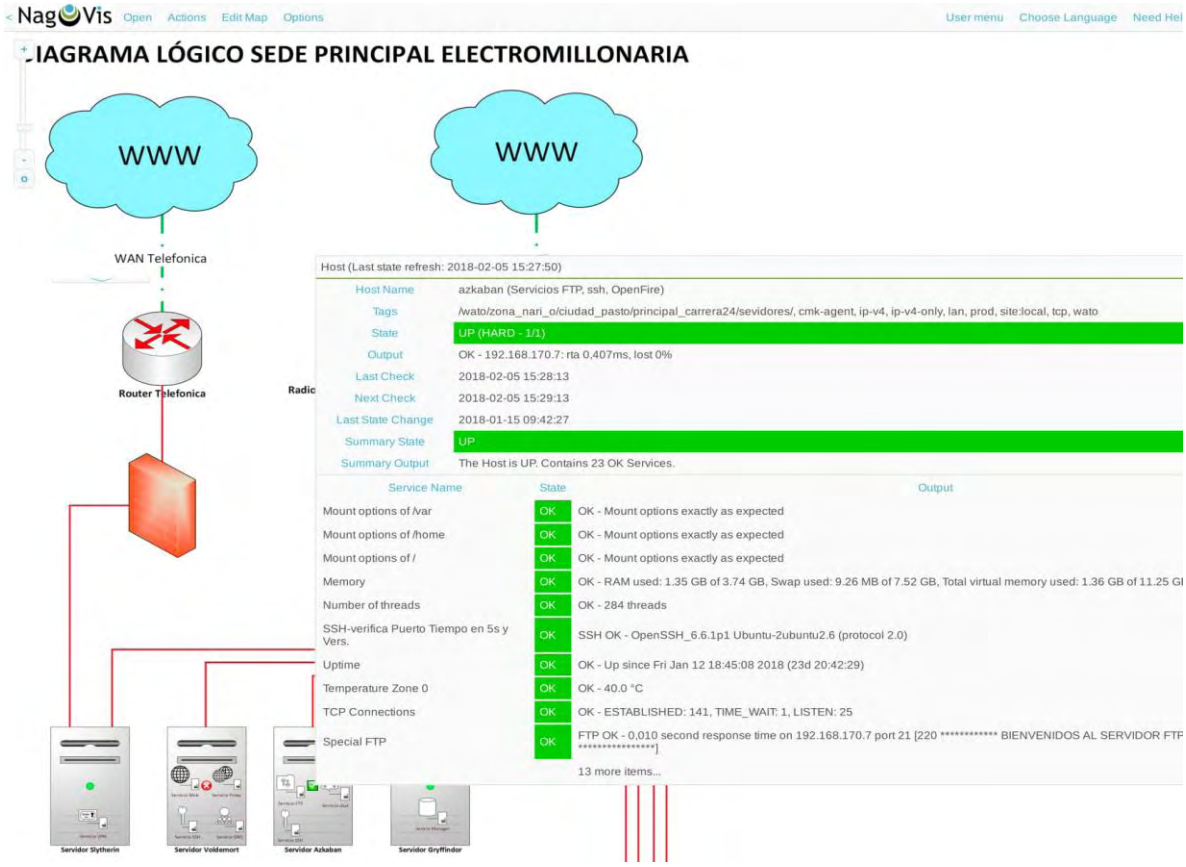
Geomapa agencia de Mocoa.



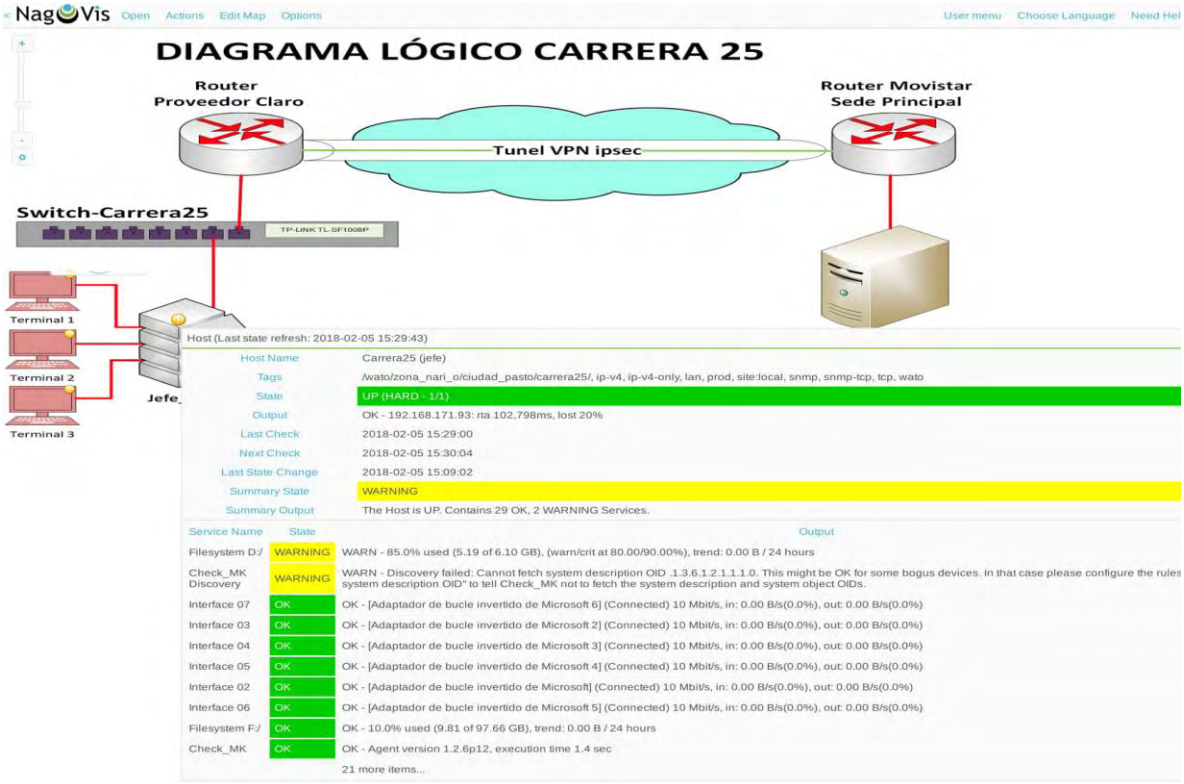
Geomapa agencia de Yumbo.



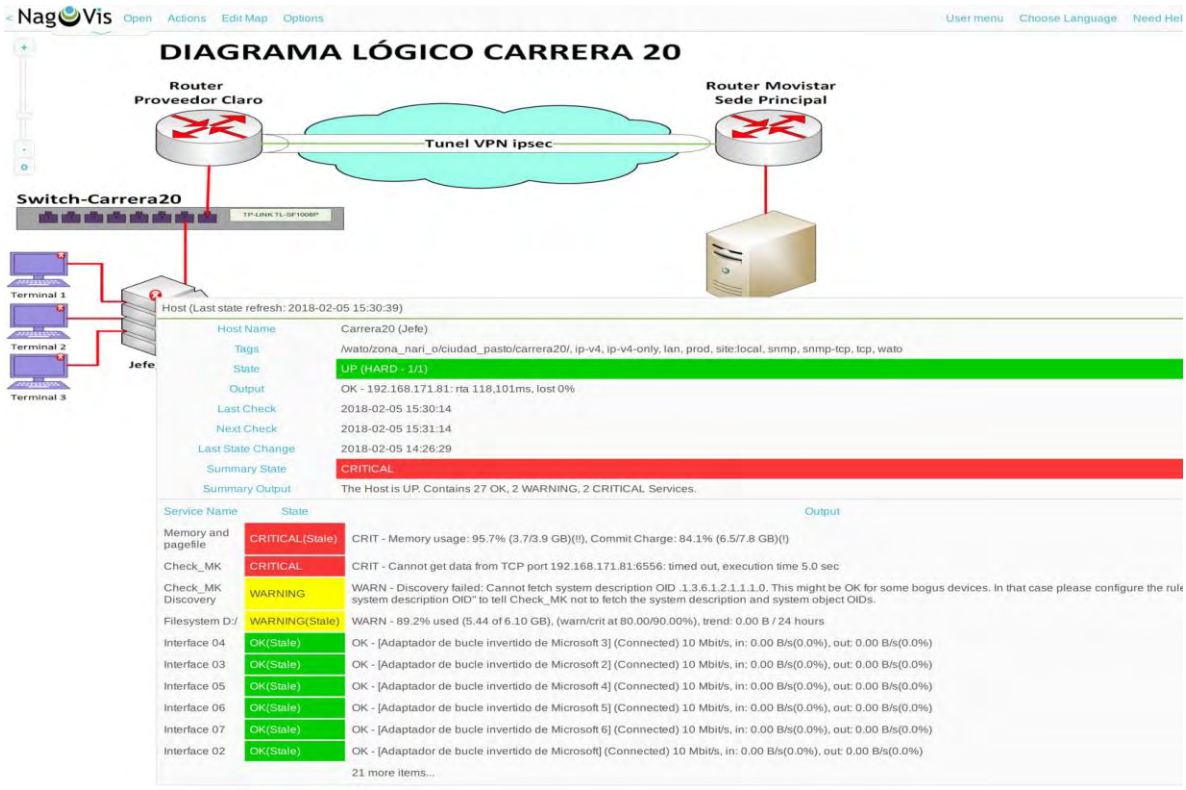
Se visualiza el monitoreo del Servidor Azkaban colocando el puntero en la imagen del servidor.



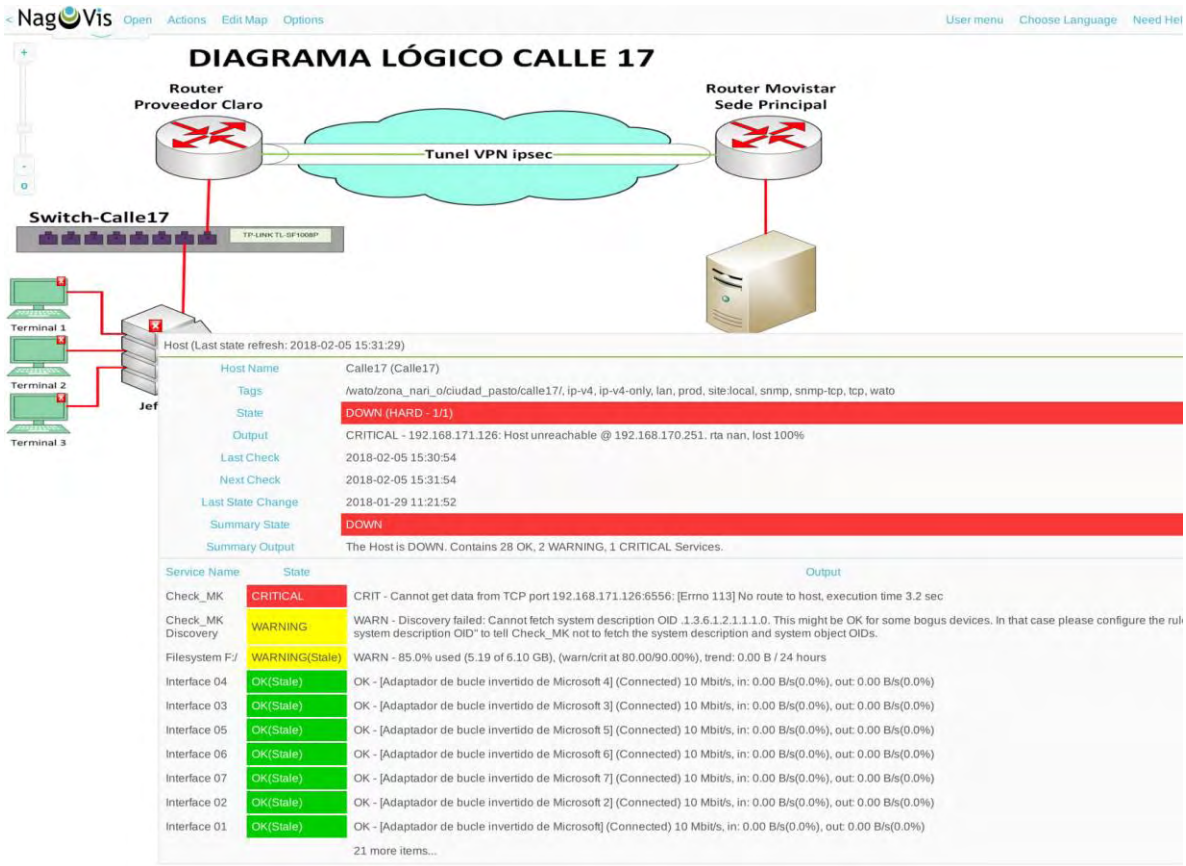
Se visualiza el monitoreo del equipo principal.



Se visualiza el monitoreo del equipo principal.



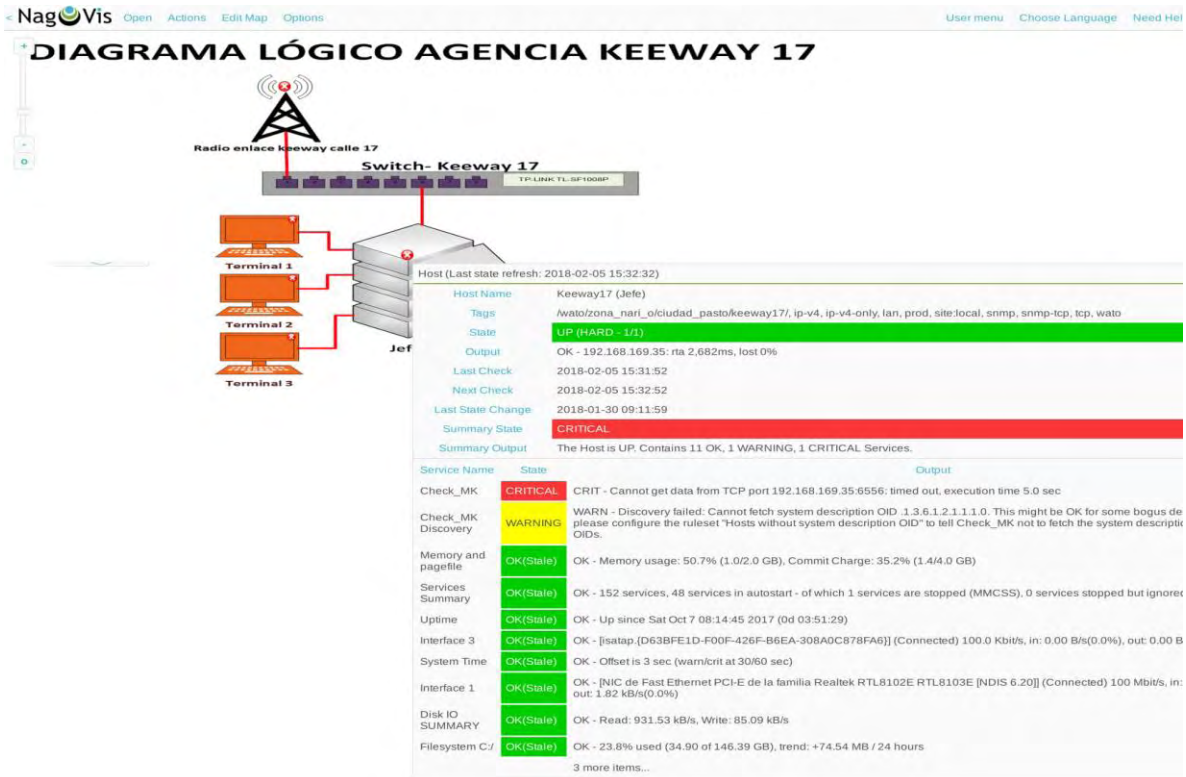
Se visualiza el monitoreo del equipo principal.



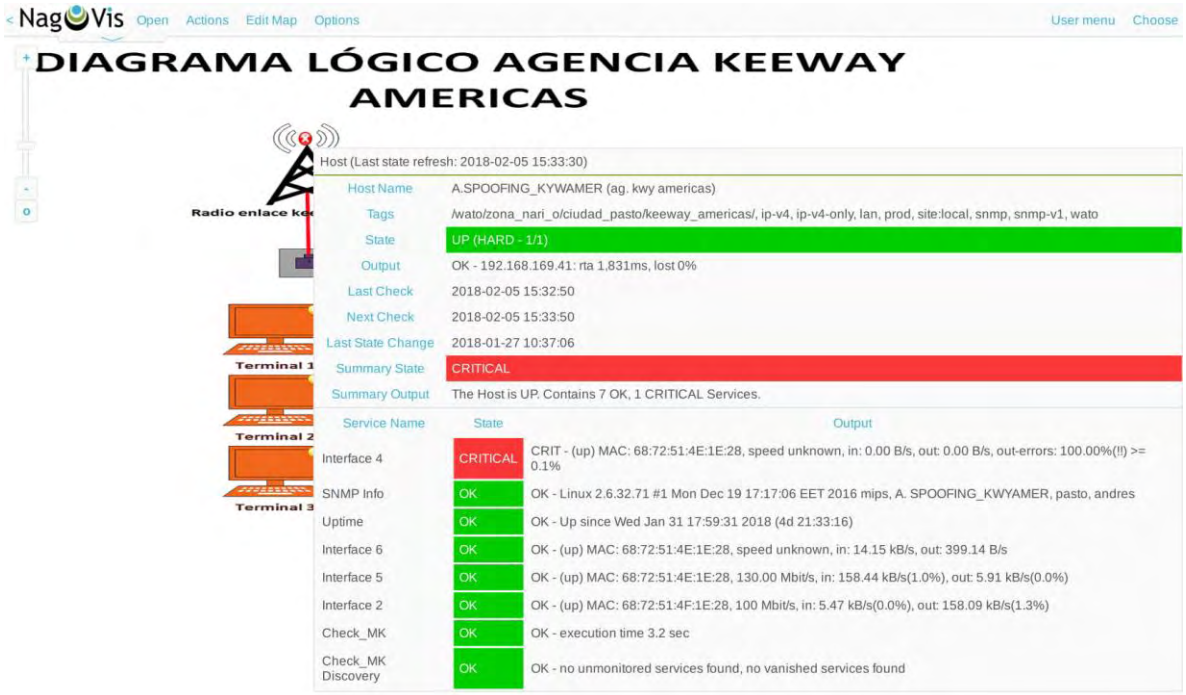
Se visualiza el monitoreo del Radio enlace.



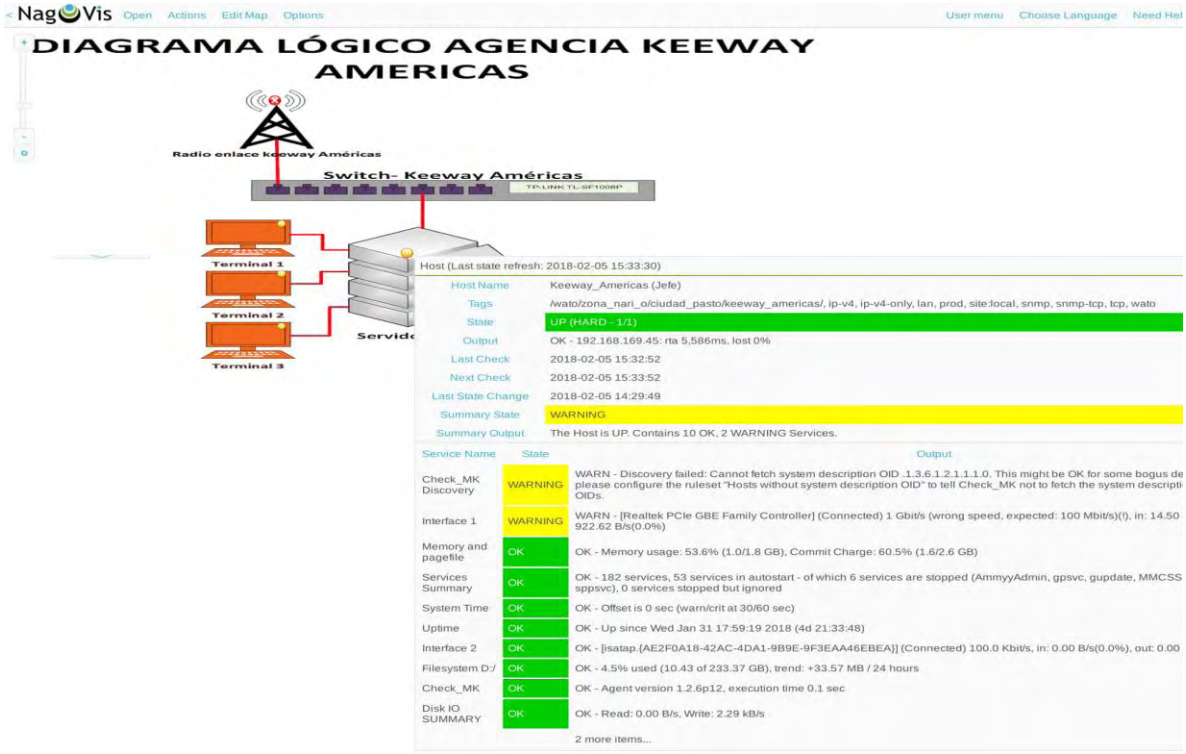
Se visualiza el monitoreo del equipo principal.



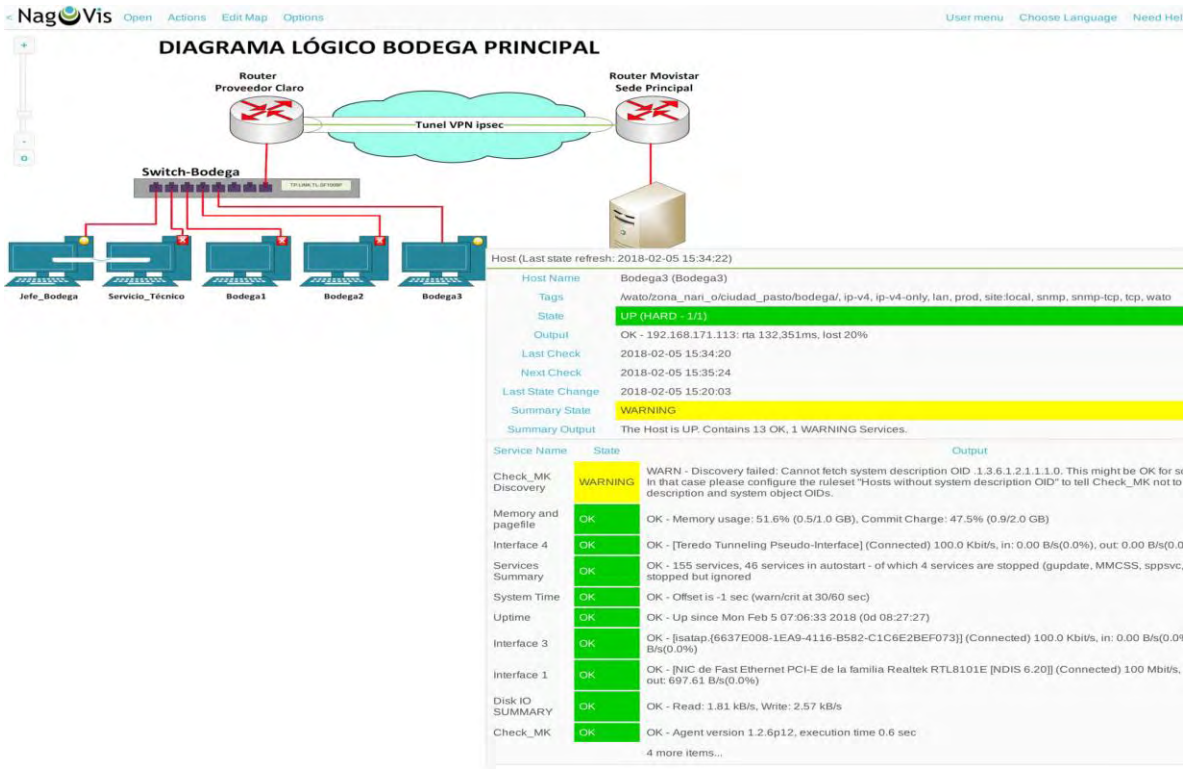
Se visualiza el monitoreo del Radio enlace.



Se visualiza el monitoreo del equipo principal.



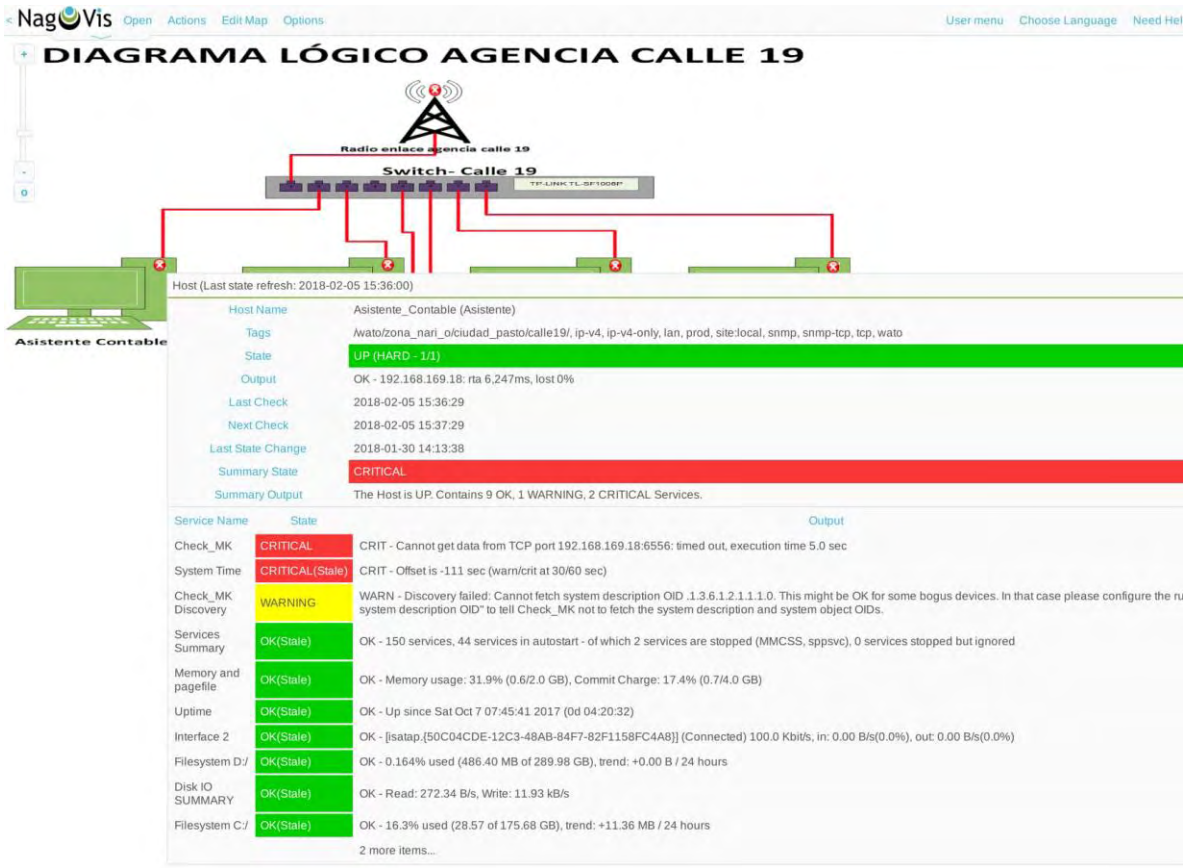
Se visualiza el monitoreo del equipo principal.



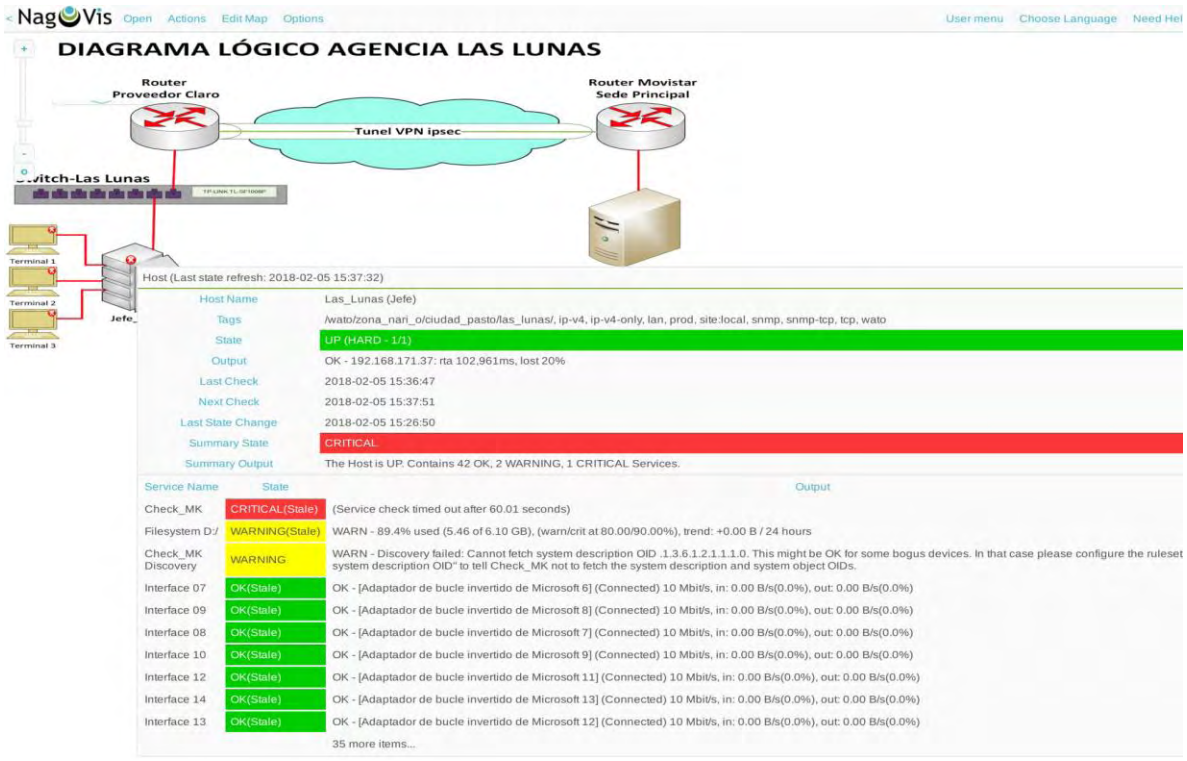
Se visualiza el monitoreo del Radio enlace.



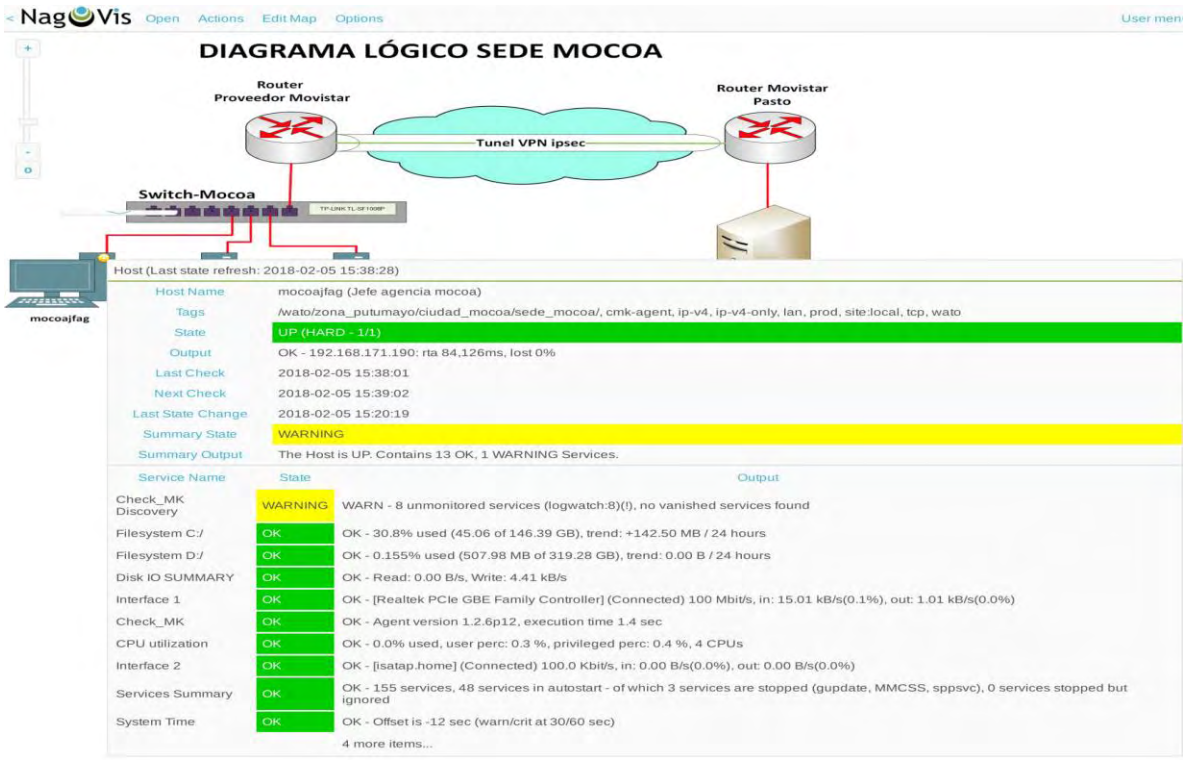
Se visualiza el monitoreo del equipo principal.



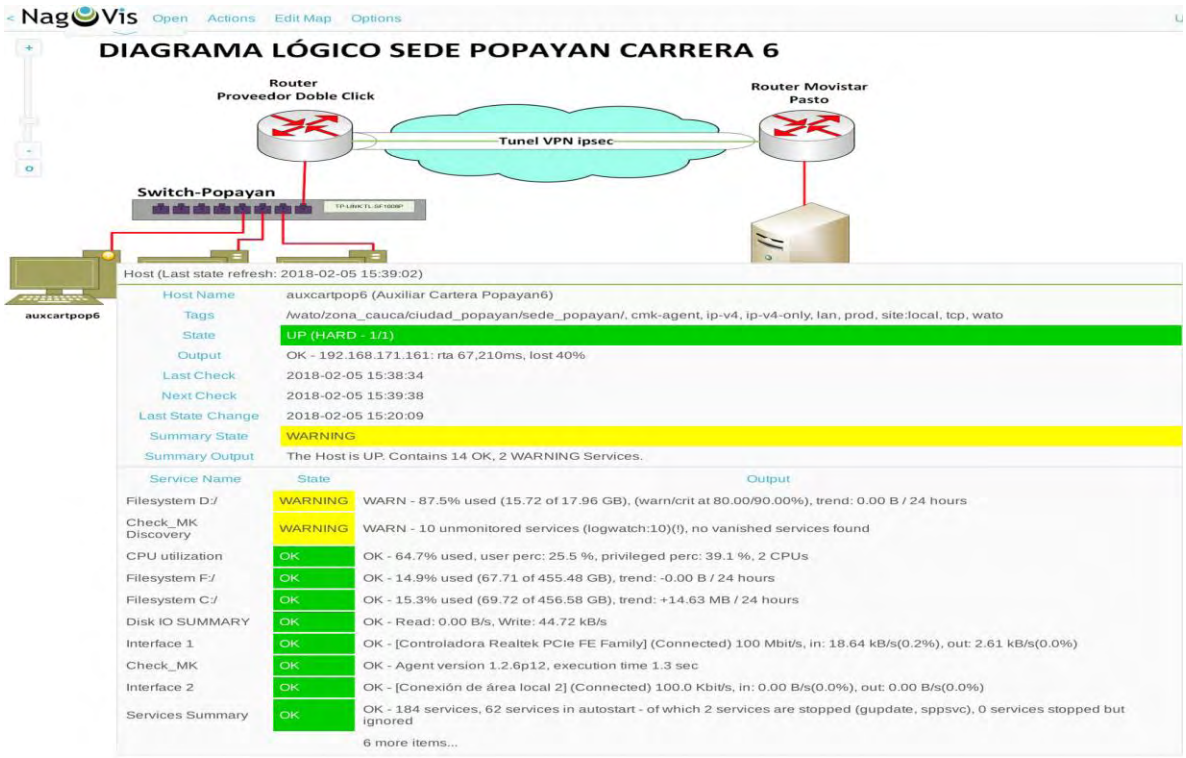
Se visualiza el monitoreo del equipo principal.



Se visualiza el monitoreo del equipo principal.



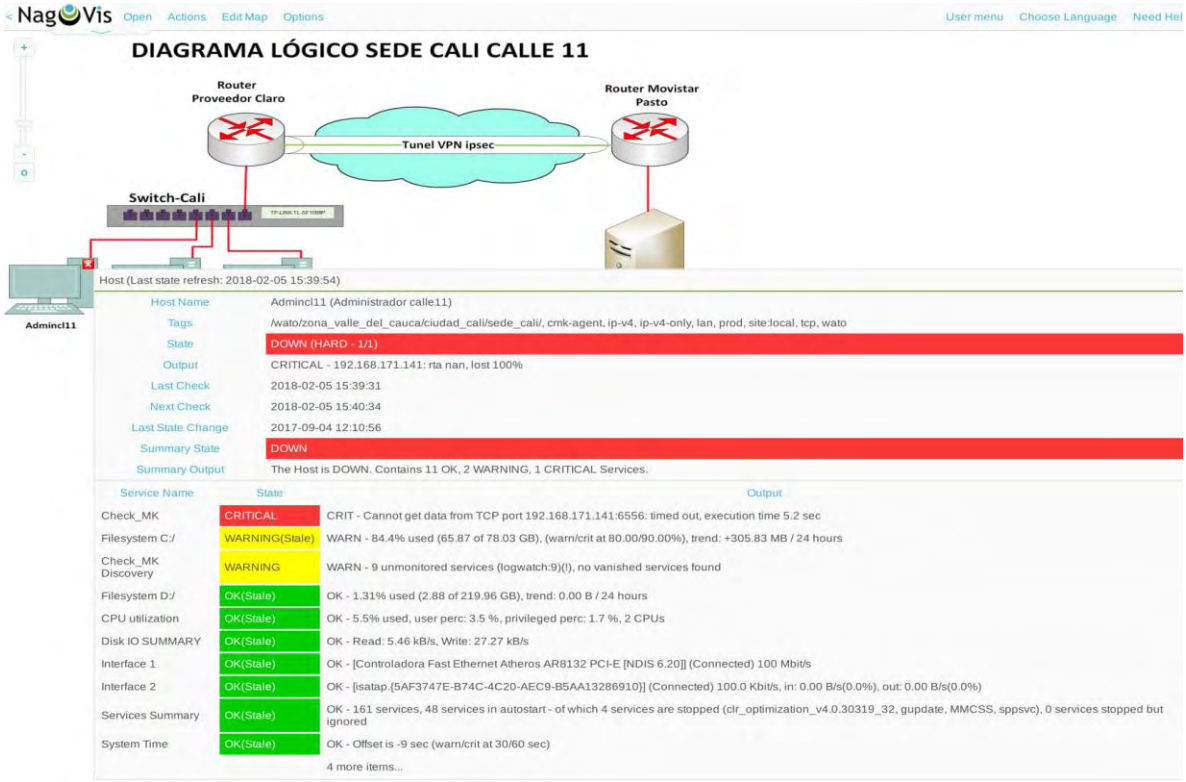
Se visualiza el monitoreo del equipo principal.



Se visualiza el monitoreo del equipo principal.



Se visualiza el monitoreo del equipo principal.

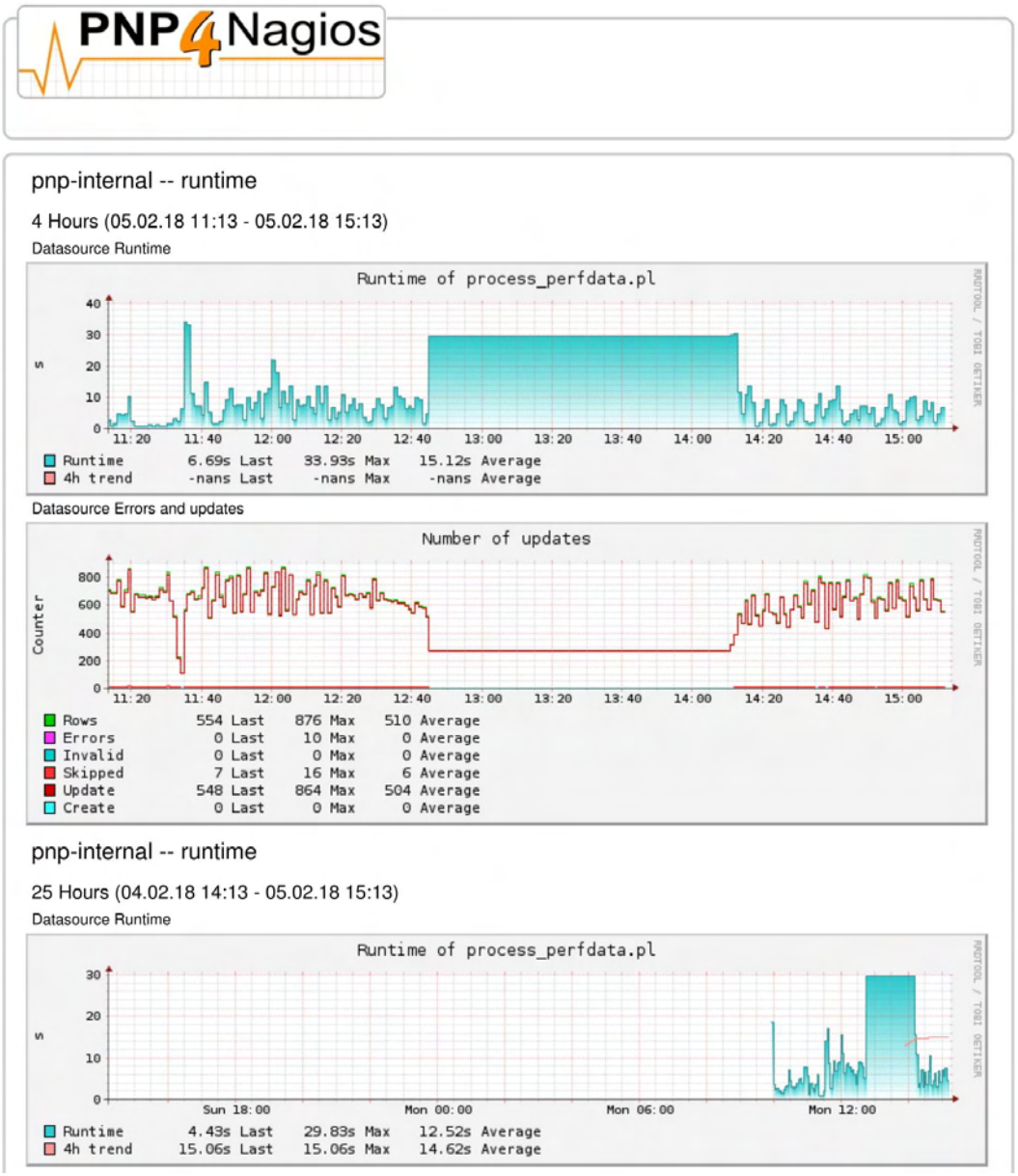


Se visualiza el monitoreo del equipo principal.



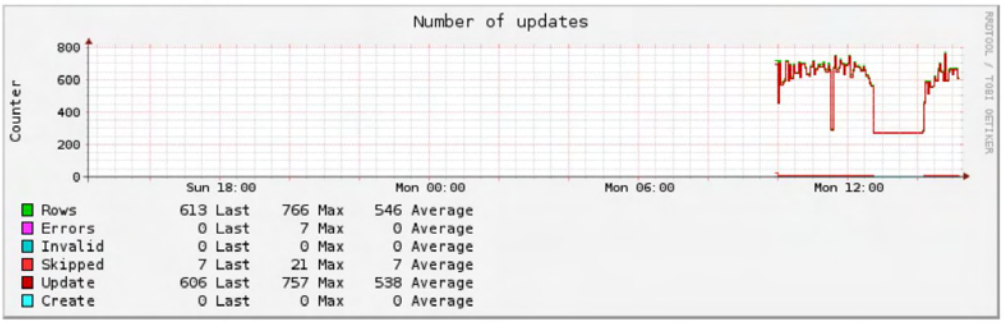
4. FUNCIONAMIENTO CON PNP4

Mediante PNP4Nagios se puede observar un resumen grafico del ultimo mes de monitoreo.



PNP4Nagios

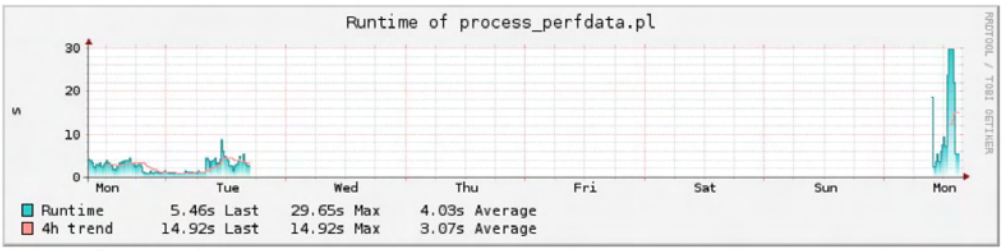
Datasource Errors and updates



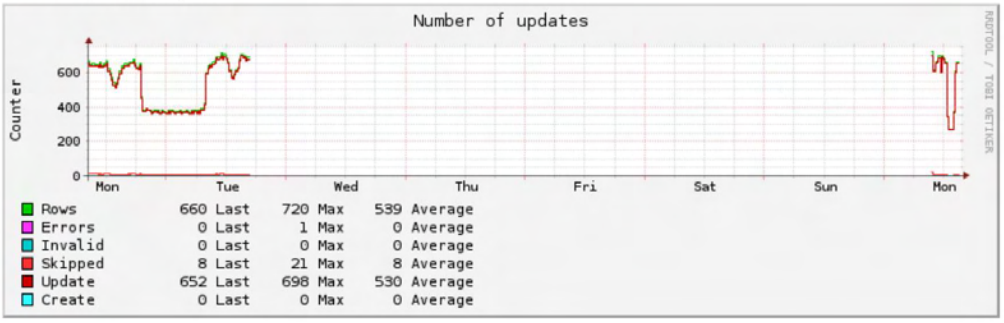
pnp-internal -- runtime

One Week (29.01.18 8:13 - 05.02.18 15:13)

Datasource Runtime



Datasource Errors and updates

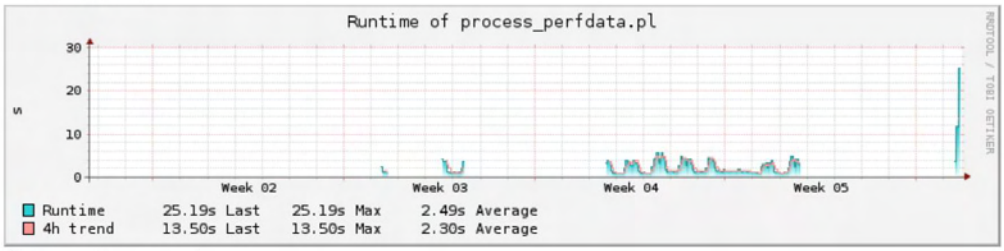


PNP4Nagios

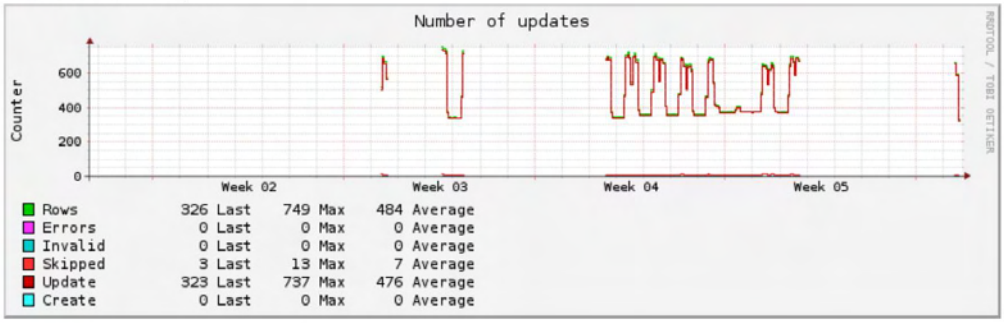
pnp-internal -- runtime

One Month (04.01.18 15:13 - 05.02.18 15:13)

Datasource Runtime



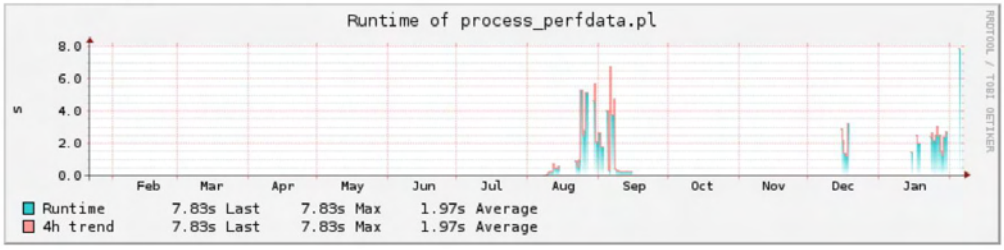
Datasource Errors and updates

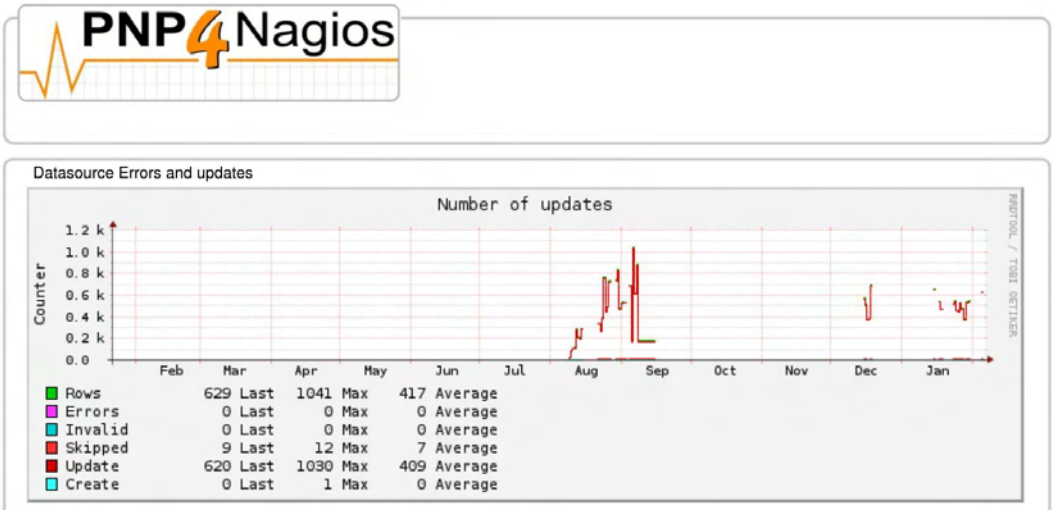


pnp-internal -- runtime

One Year (21.01.17 15:13 - 05.02.18 15:13)

Datasource Runtime





5. FUNCIONAMIENTO ENVÍO DE NOTIFICACIONES

A continuación, se muestran los diferentes estados de las notificaciones enviadas por email. Como ejemplo se tomó el host *Soporte2_mng*.



Check_MK: Soporte2_mng/Check_MK OK -> CRIT Papelera x

nagioselectromillonaria@gmail.com 5 feb. (Hace 1 día.)
para mí

Host	Soporte2_mng (Equipo_Esteban)
Service	Check_MK
Event	OK → CRITICAL
Address	192.168.170.24
Date / Time	Mon Feb 5 13:03:20 -05 2018
Plugin Output	CRIT - Cannot get data from TCP port 192.168.170.24:6556: timed out, execution time 5.0 sec
Additional Output	
Host Performance Data	rta=0,000ms;200,000;500,000;0; pl=100%;80;100;; rtmax=0,000ms;;;; rtmin=0,000ms;;;;
Performance Data	execution_time=5.012 user_time=0.030 system_time=0.000 children_user_time=0.000 children_system_time=0.000

Haz clic aquí para Responder o Reenviar el mensaje

0 GB (0%) de 15 GB utilizados
Administrar
Condiciones - Privacidad
Última actividad de la cuenta: Hace 6 minutos.
Detalles

Check_MK: Soporte2_mng/CPU utilization OK -> CRIT Papelera x

nagioselectromillonaria@gmail.com 5 feb. (Hace 1 día.)
para mí

Host	Soporte2_mng (Equipo_Esteban)
Service	CPU utilization
Event	OK → CRITICAL
Address	192.168.170.24
Date / Time	Mon Feb 5 14:02:17 -05 2018
Plugin Output	CRIT - 98.8% used, 15min average: 93.2%, (warn/crit at 85.00/90.00)(!!), user perc: 0.1 %, privileged perc: 0.1 %, 4 CPUs
Additional Output	
Host Performance Data	rta=0,281ms;200,000;500,000;0; pl=0%;80;100;; rtmax=0,333ms;;;; rtmin=0,249ms;;;;
Performance Data	util=98.818874;85;90;0;4 avg=93.230443;85;90;0;100 cpu_core_util_0=98.874789;;;; cpu_core_util_1=98.790593;;;; cpu_core_util_2=98.863131;;;; cpu_core_util_3=98.746983;;;; user=0.053756;;;;

Haz clic aquí para Responder o Reenviar el mensaje

0 GB (0%) de 15 GB utilizados
Administrar
Condiciones - Privacidad
Última actividad de la cuenta: Hace 8 minutos.
Detalles

Check_MK: Soporte2_mng/CPU utilization CRIT -> WARN Papelera x

nagioselectromillonaria@gmail.com 5 feb. (Hace 1 día.)
para mí

Host	Soporte2_mng (Equipo_Esteban)
Service	CPU utilization
Event	CRITICAL → WARNING
Address	192.168.170.24
Date / Time	Mon Feb 5 14:03:17 -05 2018
Plugin Output	WARN - 13.0% used, 15min average: 89.7%, (warn/crit at 85.00/90.00)(!), user perc: 9.4 %, privileged perc: 3.8 %, 4 CPUs
Additional Output	
Host Performance Data	rta=0,334ms;200,000;500,000;0; pl=0%;80;100;; rtmax=0,368ms;;;; rtmin=0,281ms;;;;
Performance Data	util=12.996391;85;90;0;4 avg=89.666228;85;90;0;100 cpu_core_util_0=17.00218;;;; cpu_core_util_1=11.449602;;;; cpu_core_util_2=17.240147;;;; cpu_core_util_3=6.293637;;;; user=9.432772;;;;

Haz clic aquí para Responder o Reenviar el mensaje

0 GB (0%) de 15 GB utilizados
Administrar
Condiciones - Privacidad
Última actividad de la cuenta: Hace 9 minutos.
Detalles

Check_MK: Soporte2_mng/CPU utilization WARN -> OK Papelera x

nagioselectromillonaria@gmail.com 5 feb. (Hace 1 día.)

para mí

Host	Soporte2_mng (Equipo_Esteban)
Service	CPU utilization
Event	WARNING → OK
Address	192.168.170.24
Date / Time	Mon Feb 5 14:05:17 -05 2018
Plugin Output	OK - 15.0% used, 15min average: 83.1%, user perc: 12.0 %, privileged perc: 3.1 %, 4 CPUs
Additional Output	
Host Performance Data	rta=0,322ms;200,000;500,000;0; pl=0%;80;100;; rtmax=0,417ms;;;; rtmin=0,258ms;;;;
Performance Data	util=14.972955;85;90;0;4 avg=83.148946;85;90;0;100 cpu_core_util_0=20.36149;;;; cpu_core_util_1=10.533426;;;; cpu_core_util_2=25.09352;;;; cpu_core_util_3=3.903384;;;; user=12.038077;;;;

Haz clic aquí para Responder o Reenviar el mensaje

0 GB (0%) de 15 GB utilizados
Administrar

Condiciones - Privacidad

Última actividad de la cuenta: Hace 10 minutos.
Detalles

Anexo N. Resultados de reporte Nagios Availability Host Groups.

Hostgroup 'Agencia_Calle_17' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_C17	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
Calle17	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Average	49.996% (49.996%)	50.004% (50.004%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Calle_19' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_C19	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
Asistente_Contable	90.952% (90.952%)	9.048% (9.048%)	0.000% (0.000%)	0.000%
Asistente_Inventario	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Caja	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Jefe_Contabilidad	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	98.185% (98.185%)	1.815% (1.815%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Carrera_20' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Carrera20	99.916% (99.916%)	0.084% (0.084%)	0.000% (0.000%)	0.000%
Average	99.916% (99.916%)	0.084% (0.084%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Carrera_24' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Asistente_Administracion	91.302% (91.302%)	8.698% (8.698%)	0.000% (0.000%)	0.000%
Caja_Principal	19.227% (19.227%)	80.773% (80.773%)	0.000% (0.000%)	0.000%
Average	55.264% (55.264%)	44.736% (44.736%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Carrera_25' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Carrera25	98.483% (98.483%)	1.517% (1.517%)	0.000% (0.000%)	0.000%
Average	98.483% (98.483%)	1.517% (1.517%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Keeway17' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_KW17	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Keeway17	91.665% (91.665%)	8.335% (8.335%)	0.000% (0.000%)	0.000%
Average	95.833% (95.833%)	4.167% (4.167%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Keeway_Americas' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_KYWAMER	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
Keeway_Americas	91.494% (91.494%)	8.506% (8.506%)	0.000% (0.000%)	0.000%
Average	95.743% (95.743%)	4.257% (4.257%)	0.000% (0.000%)	0.000%

Hostgroup 'Agencia_Las_Lunas' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Las_Lunas	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Administracion' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
DIR_ADMIN	89.263% (89.263%)	10.737% (10.737%)	0.000% (0.000%)	0.000%
JEFE_RH	1.068% (1.068%)	98.932% (98.932%)	0.000% (0.000%)	0.000%
NOMINA	92.319% (92.319%)	7.681% (7.681%)	0.000% (0.000%)	0.000%
PSICOLOGA	2.958% (2.958%)	97.042% (97.042%)	0.000% (0.000%)	0.000%
SALUDO CUPA	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
auxrecursosh	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Average	30.935% (30.935%)	69.065% (69.065%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Analista' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
ANALISTA_NARINO	90.475% (90.475%)	9.525% (9.525%)	0.000% (0.000%)	0.000%
ANALISTA_PUTUMAYO	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
ANALISTA_VALLE	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Average	30.158% (30.158%)	69.842% (69.842%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Cartera' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
ASISCARKEEWAY	1.062% (1.062%)	98.938% (98.938%)	0.000% (0.000%)	0.000%
ASIS_ADC	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Cartera_Server	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
JF_CARTERA	87.829% (87.829%)	12.171% (12.171%)	0.000% (0.000%)	0.000%
KEEWAYAUXCART	92.342% (92.342%)	7.658% (7.658%)	0.000% (0.000%)	0.000%
TELECOBRO_1	1.079% (1.079%)	98.921% (98.921%)	0.000% (0.000%)	0.000%
asiscartpasto	92.299% (92.299%)	7.701% (7.701%)	0.000% (0.000%)	0.000%
asisteadcvalle	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
auxcart3	88.000% (88.000%)	12.000% (12.000%)	0.000% (0.000%)	0.000%
auxcartera1_pc	91.464% (91.464%)	8.536% (8.536%)	0.000% (0.000%)	0.000%
Average	55.408% (55.408%)	44.592% (44.592%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Comercial' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
AUX_COMPRAS	91.157% (91.157%)	8.843% (8.843%)	0.000% (0.000%)	0.000%
COMERCIAL	0.398% (0.398%)	99.602% (99.602%)	0.000% (0.000%)	0.000%
comerciallaux	86.544% (86.544%)	13.456% (13.456%)	0.000% (0.000%)	0.000%
Average	59.366% (59.366%)	40.634% (40.634%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Contabilidad' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
ASIS_KWY1	19.170% (19.170%)	80.830% (80.830%)	0.000% (0.000%)	0.000%
Benelli	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
PC_AUXCONTAB1	85.038% (85.038%)	14.962% (14.962%)	0.000% (0.000%)	0.000%
auxadmon	90.035% (90.035%)	9.965% (9.965%)	0.000% (0.000%)	0.000%
auxconta4	91.690% (91.690%)	8.310% (8.310%)	0.000% (0.000%)	0.000%
contabjefe	91.322% (91.322%)	8.678% (8.678%)	0.000% (0.000%)	0.000%
keewayauxconta	89.861% (89.861%)	10.139% (10.139%)	0.000% (0.000%)	0.000%
Average	81.015% (81.015%)	18.985% (18.985%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Facturacion' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
HOSTFACT	92.392% (92.392%)	7.608% (7.608%)	0.000% (0.000%)	0.000%
factcoor	92.224% (92.224%)	7.776% (7.776%)	0.000% (0.000%)	0.000%
Average	92.308% (92.308%)	7.692% (7.692%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Gerencia' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
asiscompras3	90.052% (90.052%)	9.948% (9.948%)	0.000% (0.000%)	0.000%
Average	90.052% (90.052%)	9.948% (9.948%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Interelec' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
interpasistente	4.086% (4.086%)	95.914% (95.914%)	0.000% (0.000%)	0.000%
Average	4.086% (4.086%)	95.914% (95.914%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Juridico' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
juridicoabg1	1.061% (1.061%)	98.939% (98.939%)	0.000% (0.000%)	0.000%
juridicoabg2	91.157% (91.157%)	8.843% (8.843%)	0.000% (0.000%)	0.000%
juridicoabg3	92.297% (92.297%)	7.703% (7.703%)	0.000% (0.000%)	0.000%
juridicosecre	92.243% (92.243%)	7.757% (7.757%)	0.000% (0.000%)	0.000%
Average	69.189% (69.189%)	30.811% (30.811%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Publicidad' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
PUBLICIDAD	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
publicidadweb	91.746% (91.746%)	8.254% (8.254%)	0.000% (0.000%)	0.000%
Average	45.873% (45.873%)	54.127% (54.127%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Revisoria' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
FONDEELEC	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
HOSTREVI	92.313% (92.313%)	7.687% (7.687%)	0.000% (0.000%)	0.000%
REVISORIA	86.863% (86.863%)	13.137% (13.137%)	0.000% (0.000%)	0.000%
SERVIDORAUDITORES	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
audinterelec	91.205% (91.205%)	8.795% (8.795%)	0.000% (0.000%)	0.000%
auditor8	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
auxrevisoria	92.402% (92.402%)	7.598% (7.598%)	0.000% (0.000%)	0.000%
axiliaradv	90.229% (90.229%)	9.771% (9.771%)	0.000% (0.000%)	0.000%
fondolecconta	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
revisorinv1	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Average	55.301% (55.301%)	44.699% (44.699%)	0.000% (0.000%)	0.000%

Hostgroup 'Area_Sistemas' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Capacitaciones	89.746% (89.746%)	10.254% (10.254%)	0.000% (0.000%)	0.000%
JF_SISTEMAS	90.803% (90.803%)	9.197% (9.197%)	0.000% (0.000%)	0.000%
JF_SISTEMAS_VPN	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
JF_SISTEMAS_WiFi	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
SOPORTE_HW	98.825% (98.825%)	1.175% (1.175%)	0.000% (0.000%)	0.000%
Soporte1_mng	87.865% (87.865%)	12.135% (12.135%)	0.000% (0.000%)	0.000%
Soporte2_mng	90.702% (90.702%)	9.298% (9.298%)	0.000% (0.000%)	0.000%
Average	65.420% (65.420%)	34.580% (34.580%)	0.000% (0.000%)	0.000%

Hostgroup 'Bodega' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Bodega1	85.856% (85.856%)	14.144% (14.144%)	0.000% (0.000%)	0.000%

Bodega2	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Bodega3	89.189% (89.189%)	10.811% (10.811%)	0.000% (0.000%)	0.000%
Jefe_Bodega	5.338% (5.338%)	94.662% (94.662%)	0.000% (0.000%)	0.000%
Servicio_Tecnico	78.464% (78.464%)	21.536% (21.536%)	0.000% (0.000%)	0.000%
Average	51.770% (51.770%)	48.230% (48.230%)	0.000% (0.000%)	0.000%

Hostgroup 'Enlaces_Ubiquity' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
R.SPOOFING_C19	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
SPOOFING_SEC	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SPOOFING_SECM900	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
Average	99.995% (99.995%)	0.005% (0.005%)	0.000% (0.000%)	0.000%

Hostgroup 'Impresoras' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
KM2B5508	92.174% (92.174%)	7.826% (7.826%)	0.000% (0.000%)	0.000%
KMDA7C73	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
KMDA8A14	90.838% (90.838%)	9.162% (9.162%)	0.000% (0.000%)	0.000%
KYOCERA-M3550	92.024% (92.024%)	7.976% (7.976%)	0.000% (0.000%)	0.000%
Average	93.757% (93.757%)	6.243% (6.243%)	0.000% (0.000%)	0.000%

Hostgroup 'Sede_Cali' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Admincl11	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Average	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%

Hostgroup 'Sede_Mocoa' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
moc oajfag	93.138% (93.138%)	6.862% (6.862%)	0.000% (0.000%)	0.000%
Average	93.138% (93.138%)	6.862% (6.862%)	0.000% (0.000%)	0.000%

Hostgroup 'Sede_Popayan' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
auxcartpop6	92.363% (92.363%)	7.637% (7.637%)	0.000% (0.000%)	0.000%
Average	92.363% (92.363%)	7.637% (7.637%)	0.000% (0.000%)	0.000%

Hostgroup 'Sede_Tumaco' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
tumacocaja	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Average	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%

Hostgroup 'Sede_Yumbo' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
auxgarantias1	91.592% (91.592%)	8.408% (8.408%)	0.000% (0.000%)	0.000%
Average	91.592% (91.592%)	8.408% (8.408%)	0.000% (0.000%)	0.000%

Hostgroup 'Servidores' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
azkaban	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
voldemort	99.985% (99.985%)	0.015% (0.015%)	0.000% (0.000%)	0.000%
Average	99.988% (99.988%)	0.012% (0.012%)	0.000% (0.000%)	0.000%

Hostgroup 'linux-servers' Host State Breakdowns:

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

Anexo O. Resultados de reporte Nagios Availability Individual Host.

All Hosts

Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A.SPOOFING_C17	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
A.SPOOFING_C19	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
A.SPOOFING_KW17	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

A.SPOOFING_KYWAMER	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
ANALISTA_NARINO	90.382% (90.382%)	9.618% (9.618%)	0.000% (0.000%)	0.000%
ANALISTA_PUTUMAYO	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
ANALISTA_VALLE	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
ASISCARKEEWAY	1.532% (1.532%)	98.468% (98.468%)	0.000% (0.000%)	0.000%
ASIS_ADC	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
ASIS_KWY1	19.170% (19.170%)	80.830% (80.830%)	0.000% (0.000%)	0.000%
AUX_COMPRAS	91.157% (91.157%)	8.843% (8.843%)	0.000% (0.000%)	0.000%
Admincl11	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Asistente_Administracion	91.571% (91.571%)	8.429% (8.429%)	0.000% (0.000%)	0.000%
Asistente_Contable	90.952% (90.952%)	9.048% (9.048%)	0.000% (0.000%)	0.000%
Asistente_Inventario	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Benelli	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Bodega1	86.018% (86.018%)	13.982% (13.982%)	0.000% (0.000%)	0.000%
Bodega2	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Bodega3	89.189% (89.189%)	10.811% (10.811%)	0.000% (0.000%)	0.000%
COMERCIAL	0.785% (0.785%)	99.215% (99.215%)	0.000% (0.000%)	0.000%
Caja	99.990% (99.990%)	0.010% (0.010%)	0.000% (0.000%)	0.000%
Caja_Principal	19.227% (19.227%)	80.773% (80.773%)	0.000% (0.000%)	0.000%
Calle17	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Capacitaciones	89.746% (89.746%)	10.254% (10.254%)	0.000% (0.000%)	0.000%
Carrera20	99.916% (99.916%)	0.084% (0.084%)	0.000% (0.000%)	0.000%
Carrera25	98.483% (98.483%)	1.517% (1.517%)	0.000% (0.000%)	0.000%
Cartera_Server	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
DIR_ADMIN	89.270% (89.270%)	10.730% (10.730%)	0.000% (0.000%)	0.000%
FONDEELEC	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
HOSTFACT	92.392% (92.392%)	7.608% (7.608%)	0.000% (0.000%)	0.000%
HOSTREVI	92.313% (92.313%)	7.687% (7.687%)	0.000% (0.000%)	0.000%
JEFE_RH	1.537% (1.537%)	98.463% (98.463%)	0.000% (0.000%)	0.000%
JF_CARTERA	87.829% (87.829%)	12.171% (12.171%)	0.000% (0.000%)	0.000%
JF_SISTEMAS	90.803% (90.803%)	9.197% (9.197%)	0.000% (0.000%)	0.000%
JF_SISTEMAS_VPN	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
JF_SISTEMAS_WiFi	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
Jefe_Bodega	5.338% (5.338%)	94.662% (94.662%)	0.000% (0.000%)	0.000%
Jefe_Contabilidad	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
KEEWAYAUXCART	92.342% (92.342%)	7.658% (7.658%)	0.000% (0.000%)	0.000%
KM2B5508	92.174% (92.174%)	7.826% (7.826%)	0.000% (0.000%)	0.000%
KMDA7C73	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
KMDA8A14	90.838% (90.838%)	9.162% (9.162%)	0.000% (0.000%)	0.000%
KYOCERA-M3550	92.024% (92.024%)	7.976% (7.976%)	0.000% (0.000%)	0.000%
Keeway17	91.665% (91.665%)	8.335% (8.335%)	0.000% (0.000%)	0.000%
Keeway_Americas	91.494% (91.494%)	8.506% (8.506%)	0.000% (0.000%)	0.000%
Las_Lunas	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
NOMINA	92.319% (92.319%)	7.681% (7.681%)	0.000% (0.000%)	0.000%
PC_AUXCONTAB1	84.569% (84.569%)	15.431% (15.431%)	0.000% (0.000%)	0.000%
PSICOLOGA	3.427% (3.427%)	96.573% (96.573%)	0.000% (0.000%)	0.000%
PUBLICIDAD	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
R.SPOOFING_C19	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
REVISORIA	86.863% (86.863%)	13.137% (13.137%)	0.000% (0.000%)	0.000%
SALUDO CUPA	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
SERVIDORAUDITORES	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SOPORTE_HW	98.825% (98.825%)	1.175% (1.175%)	0.000% (0.000%)	0.000%
SPOOFING_SEC	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
SPOOFING_SECM900	99.992% (99.992%)	0.008% (0.008%)	0.000% (0.000%)	0.000%
Servicio_Tecnico	78.735% (78.735%)	21.265% (21.265%)	0.000% (0.000%)	0.000%
Soporte1_mng	88.334% (88.334%)	11.666% (11.666%)	0.000% (0.000%)	0.000%
Soporte2_mng	90.702% (90.702%)	9.298% (9.298%)	0.000% (0.000%)	0.000%
TELECOBRO_1	1.079% (1.079%)	98.921% (98.921%)	0.000% (0.000%)	0.000%
asisc artpasto	92.299% (92.299%)	7.701% (7.701%)	0.000% (0.000%)	0.000%
asisc ompras 3	90.052% (90.052%)	9.948% (9.948%)	0.000% (0.000%)	0.000%
asisteadc valle	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%

audinterelec	91.205% (91.205%)	8.795% (8.795%)	0.000% (0.000%)	0.000%
auditor8	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
aux admon	90.035% (90.035%)	9.965% (9.965%)	0.000% (0.000%)	0.000%
aux c art3	88.470% (88.470%)	11.530% (11.530%)	0.000% (0.000%)	0.000%
aux c artera1_pc	91.464% (91.464%)	8.536% (8.536%)	0.000% (0.000%)	0.000%
aux c artpop6	92.363% (92.363%)	7.637% (7.637%)	0.000% (0.000%)	0.000%
aux c onta4	91.690% (91.690%)	8.310% (8.310%)	0.000% (0.000%)	0.000%
aux garantias 1	91.592% (91.592%)	8.408% (8.408%)	0.000% (0.000%)	0.000%
aux rec urs os h	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
aux rev is oria	92.402% (92.402%)	7.598% (7.598%)	0.000% (0.000%)	0.000%
ax iliaradv	90.229% (90.229%)	9.771% (9.771%)	0.000% (0.000%)	0.000%
az k aban	99.991% (99.991%)	0.009% (0.009%)	0.000% (0.000%)	0.000%
c omerc iallaux	86.661% (86.661%)	13.339% (13.339%)	0.000% (0.000%)	0.000%
c ontabjefe	91.322% (91.322%)	8.678% (8.678%)	0.000% (0.000%)	0.000%
fac tc oor	92.224% (92.224%)	7.776% (7.776%)	0.000% (0.000%)	0.000%
fondolec c onta	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
interpas is tente	4.143% (4.143%)	95.857% (95.857%)	0.000% (0.000%)	0.000%
juridic oabg1	1.530% (1.530%)	98.470% (98.470%)	0.000% (0.000%)	0.000%
juridic oabg2	90.687% (90.687%)	9.313% (9.313%)	0.000% (0.000%)	0.000%
juridic oabg3	92.297% (92.297%)	7.703% (7.703%)	0.000% (0.000%)	0.000%
juridic os ec re	92.243% (92.243%)	7.757% (7.757%)	0.000% (0.000%)	0.000%
k eeway aux c onta	89.861% (89.861%)	10.139% (10.139%)	0.000% (0.000%)	0.000%
loc alhos t	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
moc oajfag	93.138% (93.138%)	6.862% (6.862%)	0.000% (0.000%)	0.000%
public idadweb	91.746% (91.746%)	8.254% (8.254%)	0.000% (0.000%)	0.000%
rev is orinv 1	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
tumac oc aja	0.000% (0.000%)	100.000% (100.000%)	0.000% (0.000%)	0.000%
v oldemort	99.985% (99.985%)	0.015% (0.015%)	0.000% (0.000%)	0.000%
Av erage	66.636% (66.636%)	33.364% (33.364%)	0.000% (0.000%)	0.000%

Anexo P. Resultados de reporte en archivo .cvs avail individual all hots.

```
HOST_NAME, TIME_UP_SCHEDULED, PERCENT_TIME_UP_SCHEDULED,
PERCENT_KNOWN_TIME_UP_SCHEDULED, TIME_UP_UNSCHEDULED,
PERCENT_TIME_UP_UNSCHEDULED, PERCENT_KNOWN_TIME_UP_UNSCHEDULED,
TOTAL_TIME_UP, PERCENT_TOTAL_TIME_UP, PERCENT_KNOWN_TIME_UP,
TIME_DOWN_SCHEDULED, PERCENT_TIME_DOWN_SCHEDULED,
PERCENT_KNOWN_TIME_DOWN_SCHEDULED, TIME_DOWN_UNSCHEDULED,
```

PERCENT_TIME_DOWN_UNSCHEDULED, PERCENT_KNOWN_TIME_DOWN_UNSCHEDULED,
TOTAL_TIME_DOWN, PERCENT_TOTAL_TIME_DOWN, PERCENT_KNOWN_TIME_DOWN,
TIME_UNREACHABLE_SCHEDULED, PERCENT_TIME_UNREACHABLE_SCHEDULED,
PERCENT_KNOWN_TIME_UNREACHABLE_SCHEDULED,
TIME_UNREACHABLE_UNSCHEDULED, PERCENT_TIME_UNREACHABLE_UNSCHEDULED,
PERCENT_KNOWN_TIME_UNREACHABLE_UNSCHEDULED, TOTAL_TIME_UNREACHABLE,
PERCENT_TOTAL_TIME_UNREACHABLE, PERCENT_KNOWN_TIME_UNREACHABLE,
TIME_UNDETERMINED_NOT_RUNNING, PERCENT_TIME_UNDETERMINED_NOT_RUNNING,
TIME_UNDETERMINED_NO_DATA, PERCENT_TIME_UNDETERMINED_NO_DATA,
TOTAL_TIME_UNDETERMINED, PERCENT_TOTAL_TIME_UNDETERMINED
"A.SPOOFING_C17", 0, 0.000%, 0.000%, 2632133, 98.273%, 98.273%,
2632133, 98.273%, 98.273%, 0, 0.000%, 0.000%, 46267, 1.727%, 1.727%,
46267, 1.727%, 1.727%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"A.SPOOFING_C19", 0, 0.000%, 0.000%, 2677381, 99.962%, 99.962%,
2677381, 99.962%, 99.962%, 0, 0.000%, 0.000%, 1019, 0.038%, 0.038%,
1019, 0.038%, 0.038%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"A.SPOOFING_KW17", 0, 0.000%, 0.000%, 2677792, 99.977%, 99.977%,
2677792, 99.977%, 99.977%, 0, 0.000%, 0.000%, 608, 0.023%, 0.023%,
608, 0.023%, 0.023%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"A.SPOOFING_KYWAMER", 0, 0.000%, 0.000%, 2677800, 99.978%, 99.978%,
2677800, 99.978%, 99.978%, 0, 0.000%, 0.000%, 600, 0.022%, 0.022%,
600, 0.022%, 0.022%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"ANALISTA_NARINO", 0, 0.000%, 0.000%, 1982507, 74.018%, 74.018%,
1982507, 74.018%, 74.018%, 0, 0.000%, 0.000%, 695893, 25.982%,
25.982%, 695893, 25.982%, 25.982%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"ANALISTA_PUTUMAYO", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"ANALISTA_VALLE", 0, 0.000%, 0.000%, 1907421, 71.215%, 71.215%,
1907421, 71.215%, 71.215%, 0, 0.000%, 0.000%, 770979, 28.785%,
28.785%, 770979, 28.785%, 28.785%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"ASISCARKEEWAY", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"ASIS_ADC", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%,
0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400, 100.000%,
100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"ASIS_KWY1", 0, 0.000%, 0.000%, 2082521, 77.752%, 77.752%, 2082521,
77.752%, 77.752%, 0, 0.000%, 0.000%, 595879, 22.248%, 22.248%, 595879,
22.248%, 22.248%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"AUX_COMPRAS", 0, 0.000%, 0.000%, 2088721, 77.984%, 77.984%, 2088721,
77.984%, 77.984%, 0, 0.000%, 0.000%, 589679, 22.016%, 22.016%, 589679,

22.016%, 22.016%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Admincl11", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%,
0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400, 100.000%,
100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"Asistente_Administracion", 0, 0.000%, 0.000%, 2232509, 83.352%,
83.352%, 2232509, 83.352%, 83.352%, 0, 0.000%, 0.000%, 445891,
16.648%, 16.648%, 445891, 16.648%, 16.648%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Asistente_Contable", 0, 0.000%, 0.000%, 2089434, 78.011%, 78.011%,
2089434, 78.011%, 78.011%, 0, 0.000%, 0.000%, 588966, 21.989%,
21.989%, 588966, 21.989%, 21.989%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Asistente_Inventario", 0, 0.000%, 0.000%, 2631281, 98.241%, 98.241%,
2631281, 98.241%, 98.241%, 0, 0.000%, 0.000%, 47119, 1.759%, 1.759%,
47119, 1.759%, 1.759%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Benelli", 0, 0.000%, 0.000%, 2677485, 99.966%, 99.966%, 2677485,
99.966%, 99.966%, 0, 0.000%, 0.000%, 915, 0.034%, 0.034%, 915, 0.034%,
0.034%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"Bodega1", 0, 0.000%, 0.000%, 484615, 18.093%, 18.093%, 484615,
18.093%, 18.093%, 0, 0.000%, 0.000%, 2193785, 81.907%, 81.907%,
2193785, 81.907%, 81.907%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Bodega2", 0, 0.000%, 0.000%, 1258571, 46.990%, 46.990%, 1258571,
46.990%, 46.990%, 0, 0.000%, 0.000%, 1419829, 53.010%, 53.010%,
1419829, 53.010%, 53.010%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Bodega3", 0, 0.000%, 0.000%, 2005910, 74.892%, 74.892%, 2005910,
74.892%, 74.892%, 0, 0.000%, 0.000%, 672490, 25.108%, 25.108%, 672490,
25.108%, 25.108%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"COMERCIAL", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%,
0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400, 100.000%,
100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"Caja", 0, 0.000%, 0.000%, 2594412, 96.864%, 96.864%, 2594412,
96.864%, 96.864%, 0, 0.000%, 0.000%, 83988, 3.136%, 3.136%, 83988,
3.136%, 3.136%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Caja_Principal", 0, 0.000%, 0.000%, 2109738, 78.769%, 78.769%,
2109738, 78.769%, 78.769%, 0, 0.000%, 0.000%, 568662, 21.231%,
21.231%, 568662, 21.231%, 21.231%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Calle17", 0, 0.000%, 0.000%, 6558, 0.245%, 0.245%, 6558, 0.245%,
0.245%, 0, 0.000%, 0.000%, 2671842, 99.755%, 99.755%, 2671842,
99.755%, 99.755%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Capacitaciones", 0, 0.000%, 0.000%, 2085438, 77.861%, 77.861%,
2085438, 77.861%, 77.861%, 0, 0.000%, 0.000%, 592962, 22.139%,

22.139%, 592962, 22.139%, 22.139%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Carrera20", 0, 0.000%, 0.000%, 2677095, 99.951%, 99.951%, 2677095,
99.951%, 99.951%, 0, 0.000%, 0.000%, 1305, 0.049%, 0.049%, 1305,
0.049%, 0.049%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Carrera25", 0, 0.000%, 0.000%, 2406170, 89.836%, 89.836%, 2406170,
89.836%, 89.836%, 0, 0.000%, 0.000%, 272230, 10.164%, 10.164%, 272230,
10.164%, 10.164%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Cartera_Server", 0, 0.000%, 0.000%, 2677745, 99.976%, 99.976%,
2677745, 99.976%, 99.976%, 0, 0.000%, 0.000%, 655, 0.024%, 0.024%,
655, 0.024%, 0.024%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"DIR_ADMIN", 0, 0.000%, 0.000%, 1978459, 73.867%, 73.867%, 1978459,
73.867%, 73.867%, 0, 0.000%, 0.000%, 699941, 26.133%, 26.133%, 699941,
26.133%, 26.133%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"FONDEELEC", 0, 0.000%, 0.000%, 1941772, 72.497%, 72.497%, 1941772,
72.497%, 72.497%, 0, 0.000%, 0.000%, 736628, 27.503%, 27.503%, 736628,
27.503%, 27.503%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"HOSTFACT", 0, 0.000%, 0.000%, 2103413, 78.532%, 78.532%, 2103413,
78.532%, 78.532%, 0, 0.000%, 0.000%, 574987, 21.468%, 21.468%, 574987,
21.468%, 21.468%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"HOSTREVI", 0, 0.000%, 0.000%, 2105132, 78.597%, 78.597%, 2105132,
78.597%, 78.597%, 0, 0.000%, 0.000%, 573268, 21.403%, 21.403%, 573268,
21.403%, 21.403%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"JEFE_RH", 0, 0.000%, 0.000%, 733313, 27.379%, 27.379%, 733313,
27.379%, 27.379%, 0, 0.000%, 0.000%, 1945087, 72.621%, 72.621%,
1945087, 72.621%, 72.621%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"JF_CARTERA", 0, 0.000%, 0.000%, 1924875, 71.867%, 71.867%, 1924875,
71.867%, 71.867%, 0, 0.000%, 0.000%, 753525, 28.133%, 28.133%, 753525,
28.133%, 28.133%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"JF_SISTEMAS", 0, 0.000%, 0.000%, 1671895, 62.421%, 62.421%, 1671895,
62.421%, 62.421%, 0, 0.000%, 0.000%, 1006505, 37.579%, 37.579%,
1006505, 37.579%, 37.579%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"JF_SISTEMAS_VPN", 0, 0.000%, 0.000%, 23232, 0.867%, 0.867%, 23232,
0.867%, 0.867%, 0, 0.000%, 0.000%, 2655168, 99.133%, 99.133%, 2655168,
99.133%, 99.133%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"JF_SISTEMAS_WiFi", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Jefe_Bodega", 0, 0.000%, 0.000%, 37941, 1.417%, 1.417%, 37941,
1.417%, 1.417%, 0, 0.000%, 0.000%, 2640459, 98.583%, 98.583%, 2640459,

98.583%, 98.583%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Jefe_Contabilidad", 0, 0.000%, 0.000%, 2525646, 94.297%, 94.297%,
2525646, 94.297%, 94.297%, 0, 0.000%, 0.000%, 152754, 5.703%, 5.703%,
152754, 5.703%, 5.703%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"KEEWAYAUXCART", 0, 0.000%, 0.000%, 2113591, 78.912%, 78.912%,
2113591, 78.912%, 78.912%, 0, 0.000%, 0.000%, 564809, 21.088%,
21.088%, 564809, 21.088%, 21.088%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"KM2B5508", 0, 0.000%, 0.000%, 2393928, 89.379%, 89.379%, 2393928,
89.379%, 89.379%, 0, 0.000%, 0.000%, 284472, 10.621%, 10.621%, 284472,
10.621%, 10.621%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"KMDA7C73", 0, 0.000%, 0.000%, 2342591, 87.462%, 87.462%, 2342591,
87.462%, 87.462%, 0, 0.000%, 0.000%, 335809, 12.538%, 12.538%, 335809,
12.538%, 12.538%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"KMDA8A14", 0, 0.000%, 0.000%, 2098891, 78.364%, 78.364%, 2098891,
78.364%, 78.364%, 0, 0.000%, 0.000%, 579509, 21.636%, 21.636%, 579509,
21.636%, 21.636%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"KYOCERA-M3550", 0, 0.000%, 0.000%, 2329127, 86.960%, 86.960%,
2329127, 86.960%, 86.960%, 0, 0.000%, 0.000%, 349273, 13.040%,
13.040%, 349273, 13.040%, 13.040%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Keeway17", 0, 0.000%, 0.000%, 2152616, 80.369%, 80.369%, 2152616,
80.369%, 80.369%, 0, 0.000%, 0.000%, 525784, 19.631%, 19.631%, 525784,
19.631%, 19.631%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Keeway_Americas", 0, 0.000%, 0.000%, 2080829, 77.689%, 77.689%,
2080829, 77.689%, 77.689%, 0, 0.000%, 0.000%, 597571, 22.311%,
22.311%, 597571, 22.311%, 22.311%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Las_Lunas", 0, 0.000%, 0.000%, 2677786, 99.977%, 99.977%, 2677786,
99.977%, 99.977%, 0, 0.000%, 0.000%, 614, 0.023%, 0.023%, 614, 0.023%,
0.023%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"NOMINA", 0, 0.000%, 0.000%, 835486, 31.193%, 31.193%, 835486,
31.193%, 31.193%, 0, 0.000%, 0.000%, 1842914, 68.807%, 68.807%,
1842914, 68.807%, 68.807%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"PC_AUXCONTAB1", 0, 0.000%, 0.000%, 2030422, 75.807%, 75.807%,
2030422, 75.807%, 75.807%, 0, 0.000%, 0.000%, 647978, 24.193%,
24.193%, 647978, 24.193%, 24.193%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"PSICOLOGA", 0, 0.000%, 0.000%, 1800802, 67.234%, 67.234%, 1800802,
67.234%, 67.234%, 0, 0.000%, 0.000%, 877598, 32.766%, 32.766%, 877598,
32.766%, 32.766%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"PUBLICIDAD", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%,
0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400, 100.000%,

100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"R.SPOOFING_C19", 0, 0.000%, 0.000%, 2677853, 99.980%, 99.980%,
2677853, 99.980%, 99.980%, 0, 0.000%, 0.000%, 547, 0.020%, 0.020%,
547, 0.020%, 0.020%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"REVISORIA", 0, 0.000%, 0.000%, 14897, 0.556%, 0.556%, 14897, 0.556%,
0.556%, 0, 0.000%, 0.000%, 2663503, 99.444%, 99.444%, 2663503,
99.444%, 99.444%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"SALUDOCUPA", 0, 0.000%, 0.000%, 2084766, 77.836%, 77.836%, 2084766,
77.836%, 77.836%, 0, 0.000%, 0.000%, 593634, 22.164%, 22.164%, 593634,
22.164%, 22.164%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"SERVIDORAUDITORES", 0, 0.000%, 0.000%, 2677836, 99.979%, 99.979%,
2677836, 99.979%, 99.979%, 0, 0.000%, 0.000%, 564, 0.021%, 0.021%,
564, 0.021%, 0.021%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"SOPORTE_HW", 0, 0.000%, 0.000%, 2662055, 99.390%, 99.390%, 2662055,
99.390%, 99.390%, 0, 0.000%, 0.000%, 16345, 0.610%, 0.610%, 16345,
0.610%, 0.610%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"SPOOFING_SEC", 0, 0.000%, 0.000%, 2677844, 99.979%, 99.979%, 2677844,
99.979%, 99.979%, 0, 0.000%, 0.000%, 556, 0.021%, 0.021%, 556, 0.021%,
0.021%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"SPOOFING_SECM900", 0, 0.000%, 0.000%, 2677841, 99.979%, 99.979%,
2677841, 99.979%, 99.979%, 0, 0.000%, 0.000%, 559, 0.021%, 0.021%,
559, 0.021%, 0.021%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Servicio_Tecnico", 0, 0.000%, 0.000%, 1841700, 68.761%, 68.761%,
1841700, 68.761%, 68.761%, 0, 0.000%, 0.000%, 836700, 31.239%,
31.239%, 836700, 31.239%, 31.239%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Soporte1_mng", 0, 0.000%, 0.000%, 2051012, 76.576%, 76.576%, 2051012,
76.576%, 76.576%, 0, 0.000%, 0.000%, 627388, 23.424%, 23.424%, 627388,
23.424%, 23.424%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"Soporte2_mng", 0, 0.000%, 0.000%, 2061132, 76.954%, 76.954%, 2061132,
76.954%, 76.954%, 0, 0.000%, 0.000%, 617268, 23.046%, 23.046%, 617268,
23.046%, 23.046%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"TELECOBRO_1", 0, 0.000%, 0.000%, 237037, 8.850%, 8.850%, 237037,
8.850%, 8.850%, 0, 0.000%, 0.000%, 2441363, 91.150%, 91.150%, 2441363,
91.150%, 91.150%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"asiscartpasto", 0, 0.000%, 0.000%, 1861677, 69.507%, 69.507%,
1861677, 69.507%, 69.507%, 0, 0.000%, 0.000%, 816723, 30.493%,
30.493%, 816723, 30.493%, 30.493%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"asiscompras3", 0, 0.000%, 0.000%, 2055063, 76.727%, 76.727%, 2055063,
76.727%, 76.727%, 0, 0.000%, 0.000%, 623337, 23.273%, 23.273%, 623337,

23.273%, 23.273%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"asisteadcvalle", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"audinterelec", 0, 0.000%, 0.000%, 1882859, 70.298%, 70.298%, 1882859,
70.298%, 70.298%, 0, 0.000%, 0.000%, 795541, 29.702%, 29.702%, 795541,
29.702%, 29.702%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auditor8", 0, 0.000%, 0.000%, 42609, 1.591%, 1.591%, 42609, 1.591%,
1.591%, 0, 0.000%, 0.000%, 2635791, 98.409%, 98.409%, 2635791,
98.409%, 98.409%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxadmon", 0, 0.000%, 0.000%, 2070675, 77.310%, 77.310%, 2070675,
77.310%, 77.310%, 0, 0.000%, 0.000%, 607725, 22.690%, 22.690%, 607725,
22.690%, 22.690%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxcart3", 0, 0.000%, 0.000%, 2066059, 77.138%, 77.138%, 2066059,
77.138%, 77.138%, 0, 0.000%, 0.000%, 612341, 22.862%, 22.862%, 612341,
22.862%, 22.862%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxcartera1_pc", 0, 0.000%, 0.000%, 867631, 32.394%, 32.394%, 867631,
32.394%, 32.394%, 0, 0.000%, 0.000%, 1810769, 67.606%, 67.606%,
1810769, 67.606%, 67.606%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxcartpop6", 0, 0.000%, 0.000%, 2109374, 78.755%, 78.755%, 2109374,
78.755%, 78.755%, 0, 0.000%, 0.000%, 569026, 21.245%, 21.245%, 569026,
21.245%, 21.245%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxconta4", 0, 0.000%, 0.000%, 825169, 30.808%, 30.808%, 825169,
30.808%, 30.808%, 0, 0.000%, 0.000%, 1853231, 69.192%, 69.192%,
1853231, 69.192%, 69.192%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxgarantias1", 0, 0.000%, 0.000%, 2062764, 77.015%, 77.015%,
2062764, 77.015%, 77.015%, 0, 0.000%, 0.000%, 615636, 22.985%,
22.985%, 615636, 22.985%, 22.985%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxrecursosh", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"auxrevisoria", 0, 0.000%, 0.000%, 907419, 33.879%, 33.879%, 907419,
33.879%, 33.879%, 0, 0.000%, 0.000%, 1770981, 66.121%, 66.121%,
1770981, 66.121%, 66.121%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"axiliaradv", 0, 0.000%, 0.000%, 2069569, 77.269%, 77.269%, 2069569,
77.269%, 77.269%, 0, 0.000%, 0.000%, 608831, 22.731%, 22.731%, 608831,
22.731%, 22.731%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", 0, 0.000%, 0.000%, 2677869, 99.980%, 99.980%, 2677869,
99.980%, 99.980%, 0, 0.000%, 0.000%, 531, 0.020%, 0.020%, 531, 0.020%,

0.020%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"comerciallaux", 0, 0.000%, 0.000%, 35977, 1.343%, 1.343%, 35977,
1.343%, 1.343%, 0, 0.000%, 0.000%, 2642423, 98.657%, 98.657%, 2642423,
98.657%, 98.657%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"contabjefe", 0, 0.000%, 0.000%, 2104854, 78.586%, 78.586%, 2104854,
78.586%, 78.586%, 0, 0.000%, 0.000%, 573546, 21.414%, 21.414%, 573546,
21.414%, 21.414%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"factcoor", 0, 0.000%, 0.000%, 2093812, 78.174%, 78.174%, 2093812,
78.174%, 78.174%, 0, 0.000%, 0.000%, 584588, 21.826%, 21.826%, 584588,
21.826%, 21.826%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"fondolecconta", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"interpasistente", 0, 0.000%, 0.000%, 557635, 20.820%, 20.820%,
557635, 20.820%, 20.820%, 0, 0.000%, 0.000%, 2120765, 79.180%,
79.180%, 2120765, 79.180%, 79.180%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"juridicoabg1", 0, 0.000%, 0.000%, 1919194, 71.654%, 71.654%, 1919194,
71.654%, 71.654%, 0, 0.000%, 0.000%, 759206, 28.346%, 28.346%, 759206,
28.346%, 28.346%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"juridicoabg2", 0, 0.000%, 0.000%, 1620216, 60.492%, 60.492%, 1620216,
60.492%, 60.492%, 0, 0.000%, 0.000%, 1058184, 39.508%, 39.508%,
1058184, 39.508%, 39.508%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"juridicoabg3", 0, 0.000%, 0.000%, 813841, 30.385%, 30.385%, 813841,
30.385%, 30.385%, 0, 0.000%, 0.000%, 1864559, 69.615%, 69.615%,
1864559, 69.615%, 69.615%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"juridicosecre", 0, 0.000%, 0.000%, 2102035, 78.481%, 78.481%,
2102035, 78.481%, 78.481%, 0, 0.000%, 0.000%, 576365, 21.519%,
21.519%, 576365, 21.519%, 21.519%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"keewayauxconta", 0, 0.000%, 0.000%, 2064986, 77.098%, 77.098%,
2064986, 77.098%, 77.098%, 0, 0.000%, 0.000%, 613414, 22.902%,
22.902%, 613414, 22.902%, 22.902%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"localhost", 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"mocoajfag", 0, 0.000%, 0.000%, 876100, 32.710%, 32.710%, 876100,
32.710%, 32.710%, 0, 0.000%, 0.000%, 1802300, 67.290%, 67.290%,
1802300, 67.290%, 67.290%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"publicidadweb", 0, 0.000%, 0.000%, 1894866, 70.746%, 70.746%,
1894866, 70.746%, 70.746%, 0, 0.000%, 0.000%, 783534, 29.254%,

```
29.254%, 783534, 29.254%, 29.254%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"revisorinv1", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400,
100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"tumacocaja", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%,
0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%, 2678400, 100.000%,
100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"voldemort", 0, 0.000%, 0.000%, 2677807, 99.978%, 99.978%, 2677807,
99.978%, 99.978%, 0, 0.000%, 0.000%, 593, 0.022%, 0.022%, 593, 0.022%,
0.022%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
```

Anexo Q. Resultados de reporte en archivo .cvs avail all service servidores Azkaban y Voldemort.

```
HOST_NAME, SERVICE_DESCRIPTION, TIME_OK_SCHEDULED,
PERCENT_TIME_OK_SCHEDULED, PERCENT_KNOWN_TIME_OK_SCHEDULED,
```

```
TIME_OK_UNSCHEDULED, PERCENT_TIME_OK_UNSCHEDULED,
PERCENT_KNOWN_TIME_OK_UNSCHEDULED, TOTAL_TIME_OK,
PERCENT_TOTAL_TIME_OK, PERCENT_KNOWN_TIME_OK, TIME_WARNING_SCHEDULED,
PERCENT_TIME_WARNING_SCHEDULED, PERCENT_KNOWN_TIME_WARNING_SCHEDULED,
TIME_WARNING_UNSCHEDULED, PERCENT_TIME_WARNING_UNSCHEDULED,
PERCENT_KNOWN_TIME_WARNING_UNSCHEDULED, TOTAL_TIME_WARNING,
PERCENT_TOTAL_TIME_WARNING, PERCENT_KNOWN_TIME_WARNING,
TIME_UNKNOWN_SCHEDULED, PERCENT_TIME_UNKNOWN_SCHEDULED,
PERCENT_KNOWN_TIME_UNKNOWN_SCHEDULED, TIME_UNKNOWN_UNSCHEDULED,
PERCENT_TIME_UNKNOWN_UNSCHEDULED,
PERCENT_KNOWN_TIME_UNKNOWN_UNSCHEDULED, TOTAL_TIME_UNKNOWN,
PERCENT_TOTAL_TIME_UNKNOWN, PERCENT_KNOWN_TIME_UNKNOWN,
TIME_CRITICAL_SCHEDULED, PERCENT_TIME_CRITICAL_SCHEDULED,
PERCENT_KNOWN_TIME_CRITICAL_SCHEDULED, TIME_CRITICAL_UNSCHEDULED,
PERCENT_TIME_CRITICAL_UNSCHEDULED,
PERCENT_KNOWN_TIME_CRITICAL_UNSCHEDULED, TOTAL_TIME_CRITICAL,
PERCENT_TOTAL_TIME_CRITICAL, PERCENT_KNOWN_TIME_CRITICAL,
TIME_UNDETERMINED_NOT_RUNNING, PERCENT_TIME_UNDETERMINED_NOT_RUNNING,
TIME_UNDETERMINED_NO_DATA, PERCENT_TIME_UNDETERMINED_NO_DATA,
TOTAL_TIME_UNDETERMINED, PERCENT_TOTAL_TIME_UNDETERMINED
"azkaban", "CPU load", 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%,
2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "CPU utilization", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Check_MK", 0, 0.000%, 0.000%, 2677742, 99.975%, 99.975%,
2677742, 99.975%, 99.975%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 658, 0.025%, 0.025%, 658, 0.025%, 0.025%,
0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Check_MK Discovery", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Disk IO SUMMARY", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Estado OpenFire", 0, 0.000%, 0.000%, 2677923, 99.982%,
99.982%, 2677923, 99.982%, 99.982%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 477, 0.018%, 0.018%, 477, 0.018%,
0.018%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Filesystem /", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
```

0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Filesystem /home", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Filesystem /var", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Interface 2", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Kernel Context Switches", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Kernel Major Page Faults", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Kernel Process Creations", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Memory", 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%,
2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Mount options of /", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Mount options of /home", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Mount options of /var", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,

0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Number of threads", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "SSH-verifica Puerto Tiempo en 5s y Vers.", 0, 0.000%,
0.000%, 2677863, 99.980%, 99.980%, 2677863, 99.980%, 99.980%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 537,
0.020%, 0.020%, 537, 0.020%, 0.020%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Special FTP", 0, 0.000%, 0.000%, 2677861, 99.980%,
99.980%, 2677861, 99.980%, 99.980%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 539, 0.020%, 0.020%, 539, 0.020%,
0.020%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "TCP Connections", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Temperature Zone 0", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"azkaban", "Uptime", 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%,
2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "CPU load", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "CPU utilization", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Check_MK", 0, 0.000%, 0.000%, 2677740, 99.975%, 99.975%,
2677740, 99.975%, 99.975%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 660, 0.025%, 0.025%, 660, 0.025%, 0.025%,
0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Check_MK Discovery", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%

"voldemort", "DNS electro.com", 0, 0.000%, 0.000%, 0, 0.000%, 0.000%,
0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 2677751, 99.976%, 99.976%,
2677751, 99.976%, 99.976%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 649, 0.024%, 0.024%, 649, 0.024%,
0.024%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Disk IO SUMMARY", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Estado de apache", 0, 0.000%, 0.000%, 2677862, 99.980%,
99.980%, 2677862, 99.980%, 99.980%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 538, 0.020%, 0.020%, 538, 0.020%,
0.020%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Estado de apache2", 0, 0.000%, 0.000%, 2677863, 99.980%,
99.980%, 2677863, 99.980%, 99.980%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 537, 0.020%, 0.020%, 537, 0.020%,
0.020%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Filesystem /", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Filesystem /cache", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Filesystem /datosbd", 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 1433810, 53.532%,
53.532%, 1433810, 53.532%, 53.532%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 1244590, 46.468%,
46.468%, 1244590, 46.468%, 46.468%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Filesystem /datosweb", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Filesystem /home", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Filesystem /media/usb", 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%,
2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Filesystem /var", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,

0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Interface 2", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Interface 3", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Kernel Context Switches", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Kernel Major Page Faults", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Kernel Process Creations", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Memory", 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%,
2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Mount options of /", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Mount options of /cache", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Mount options of /datosbd", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Mount options of /datosweb", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,

```
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Mount options of /home", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Mount options of /media/usb", 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Mount options of /var", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Number of threads", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "SSH-verifica Puerto Tiempo en 5s y Vers.", 0, 0.000%,
0.000%, 2677862, 99.980%, 99.980%, 2677862, 99.980%, 99.980%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 538,
0.020%, 0.020%, 538, 0.020%, 0.020%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Squid Proxy", 0, 0.000%, 0.000%, 2677818, 99.978%,
99.978%, 2677818, 99.978%, 99.978%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 582, 0.022%, 0.022%, 582, 0.022%,
0.022%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "TCP Connections", 0, 0.000%, 0.000%, 2678400, 100.000%,
100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Temperature Zone 0", 0, 0.000%, 0.000%, 2678400,
100.000%, 100.000%, 2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0, 0.000%, 0, 0.000%
"voldemort", "Uptime", 0, 0.000%, 0.000%, 2678400, 100.000%, 100.000%,
2678400, 100.000%, 100.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%,
0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0, 0.000%, 0.000%, 0,
0.000%, 0, 0.000%, 0, 0.000%
```

Anexo R. Manual Check_MK.

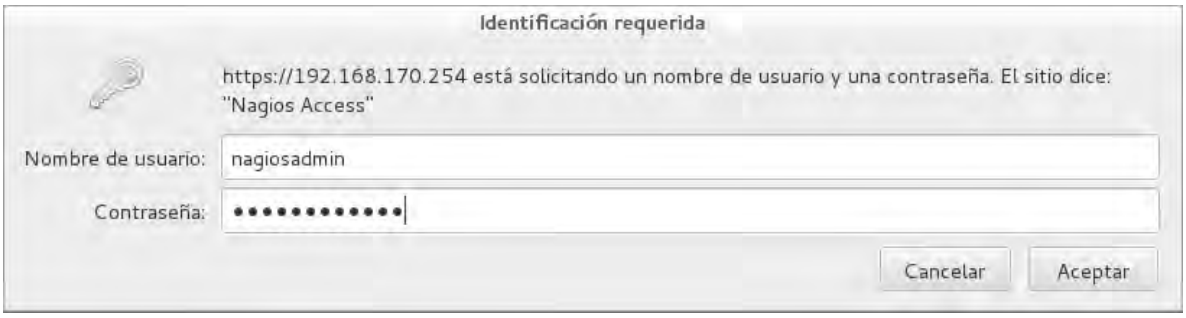
ÍNDICE

Pág.

1. INICIO A LA APLICACIÓN 628
2. ENTORNO DE LA APLICACIÓN 628
3. DESCRIPCIÓN PANTALLA PRINCIPAL 629
3.1 VISIÓN POR CONJUNTO 629
3.2 BÚSQUEDA RÁPIDA 629
3.3 BARRA DE VISTAS 630
3.4 BARRA DE CONFIGURACIONES 636
3.4 BARRA DE CONTROL 656
3.5 BARRA DE ENLACES PERSONALIZADOS 656
3.6 BARRA DE OPCIONES DE PROGRAMA 662
3.7 ÁREA DE VISIÓN GENERAL 664

1. INICIO A LA APLICACIÓN

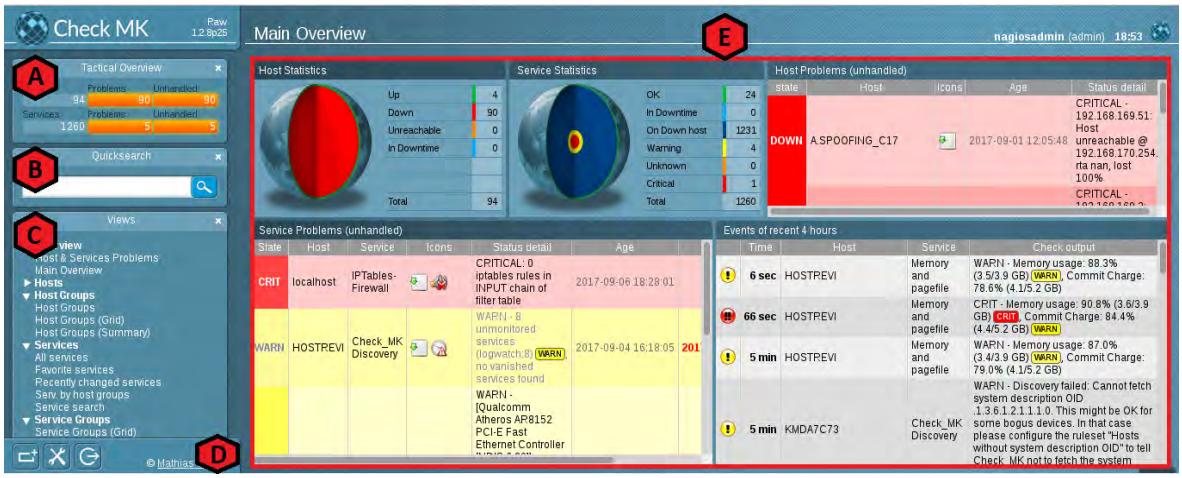
Al momento de ingresar a la aplicación será necesario ingresar el nombre de usuario y la contraseña.



2. ENTORNO DE LA APLICACIÓN

Lo que encontramos es una pantalla con 5 áreas:

- A – Visión por conjunto,
- B – Búsqueda rápida,
- C –Barra de vistas, configuraciones, de control y enlaces personalizados,
- D – Barra de opciones de programa,
- E – Área de Visión General.



3. DESCRIPCIÓN PANTALLA PRINCIPAL

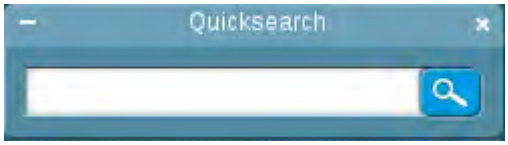
3.1 VISIÓN POR CONJUNTO

En visión por conjunto se puede observar el resumen del número de hosts y servicios con su respectiva información.



3.2 BÚSQUEDA RÁPIDA

Esta opción se muestra al inicio de la carga de la aplicación para realizar una búsqueda rápida por host o servicio.



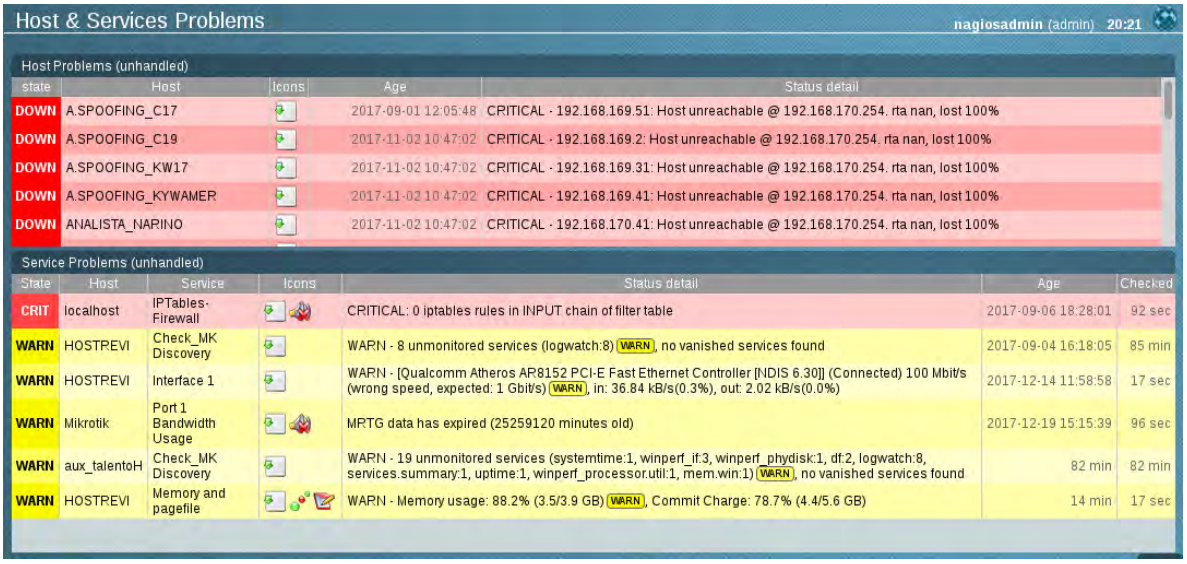
3.3 BARRA DE VISTAS

Mediante la barra de vistas se puede observar el resultado del monitoreo de diferentes perspectivas según se lo desee.

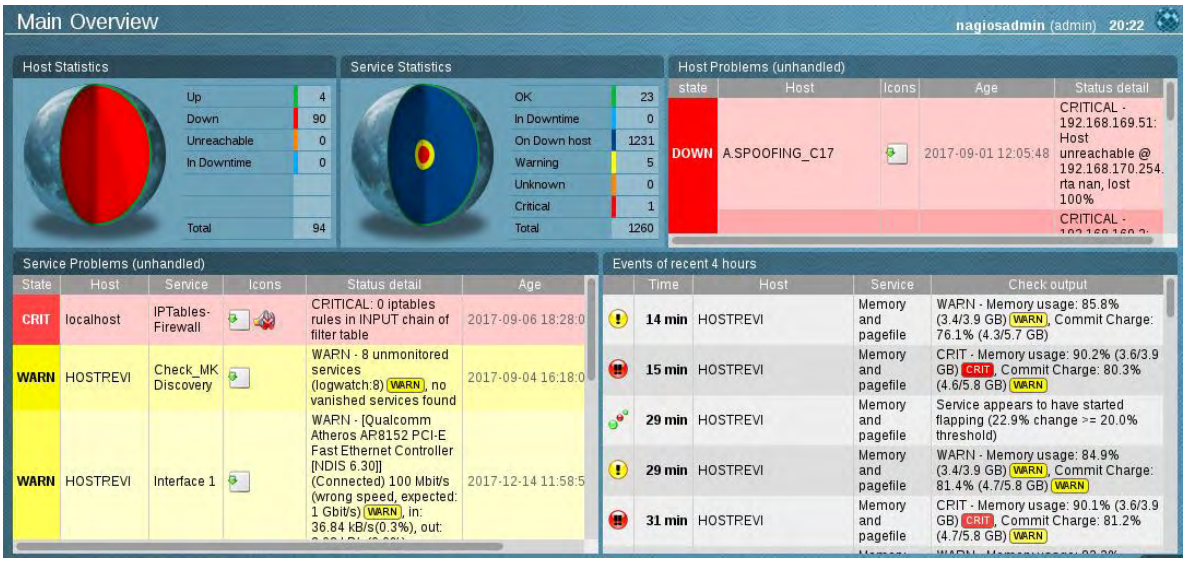


A continuación, se da a conocer lo que muestra cada opción.

Host & Services Problems: Muestra los host y servicios que tienen algún problema aquellos que están en estado Warning o critical, esta información se presenta independiente para hosts y servicios.



Main Overview: Muestra una visión general del monitoreo de hosts y servicios con totales, además de mostrar las últimas actividades del monitoreo en el área de Events.



All host: En esta opción se muestran todos los hosts en tres columnas, se observa información numérica completa del monitoreo de los hosts.



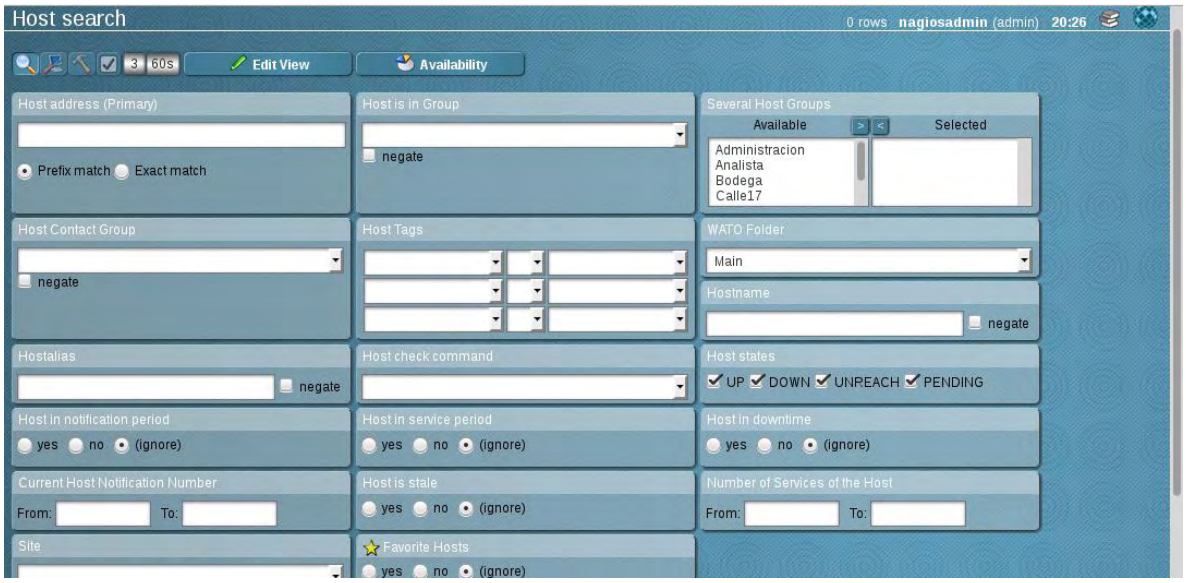
All hosts (Mini): Indica el número de problemas por cada host juntamente con su estado.



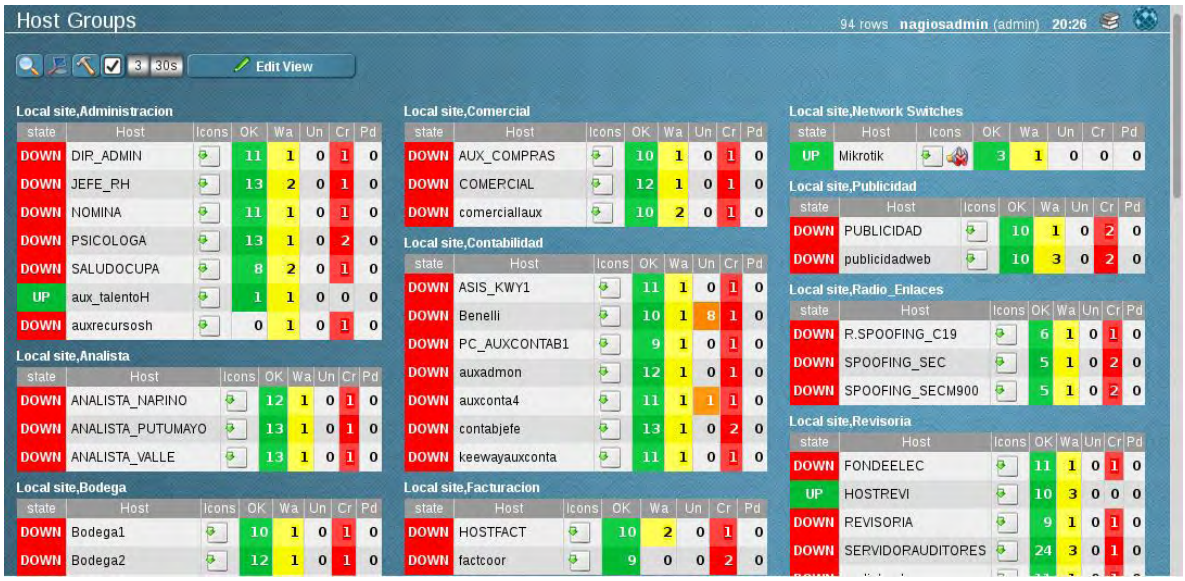
All hosts (tiled): Esta opción muestra una vista más agradable con información como: Ip, nombre del host, estado y numero de problemas.



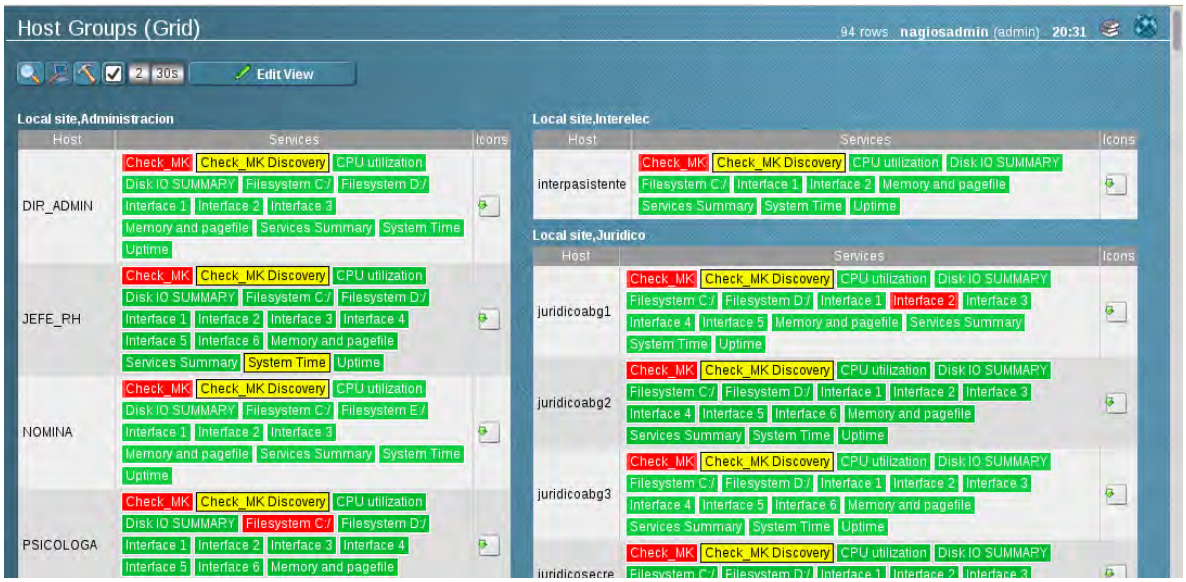
Host search: Con esta opción se puede hacer una búsqueda personalizada de los hosts, para obtener una información más detallada del resultado del monitoreo.



Host Groups: Se puede visualizar de una forma ordenada el monitoreo de los hosts, debido a que se pueden detallar mediante grupos.



Host Groups (Grid): con esta opción se muestra el estado de los servicios de cada host.



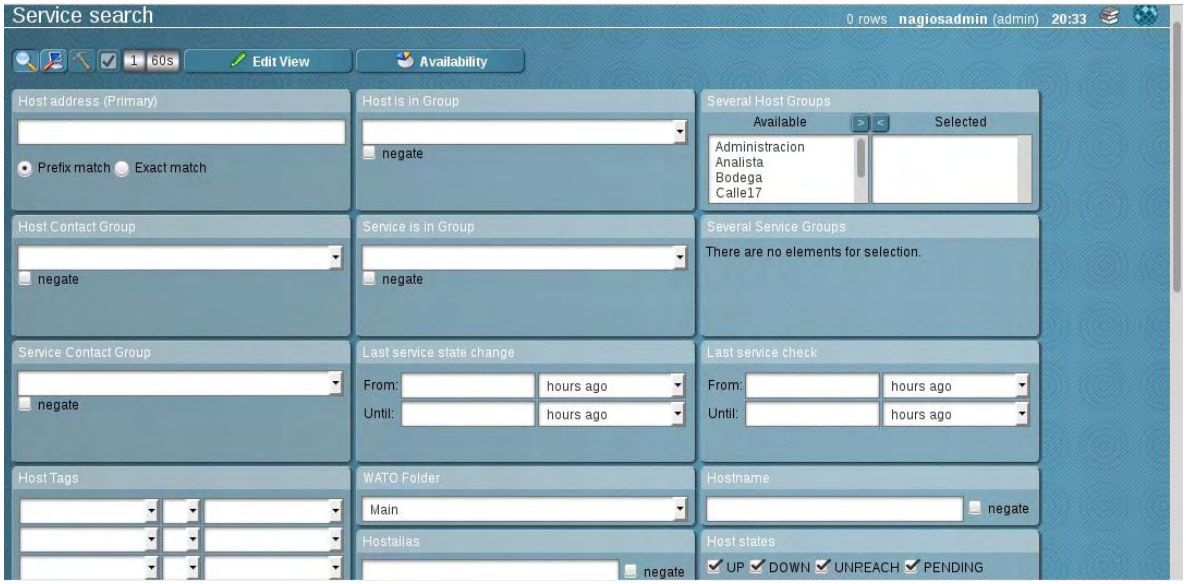
Host Groups (Summary): Se muestra información general de cada grupo.



All services: Con esta opción se puede observar detalladamente el estado de todos los servicios.

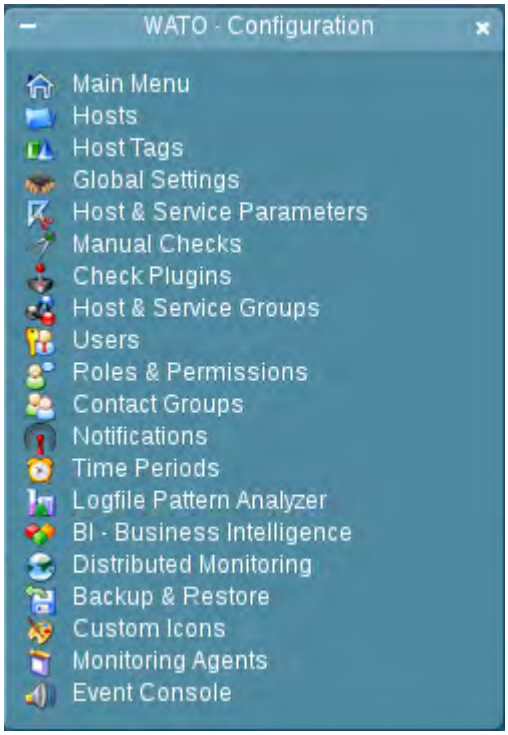


Service search: Con esta opción se puede hacer una búsqueda personalizada de los servicios, para obtener una información más detallada del resultado del monitoreo.



3.4 BARRA DE CONFIGURACIONES

En esta barra se realiza toda la configuración de la aplicación. El buen manejo de las opciones permitirá realizar un monitoreo completo y organizado.

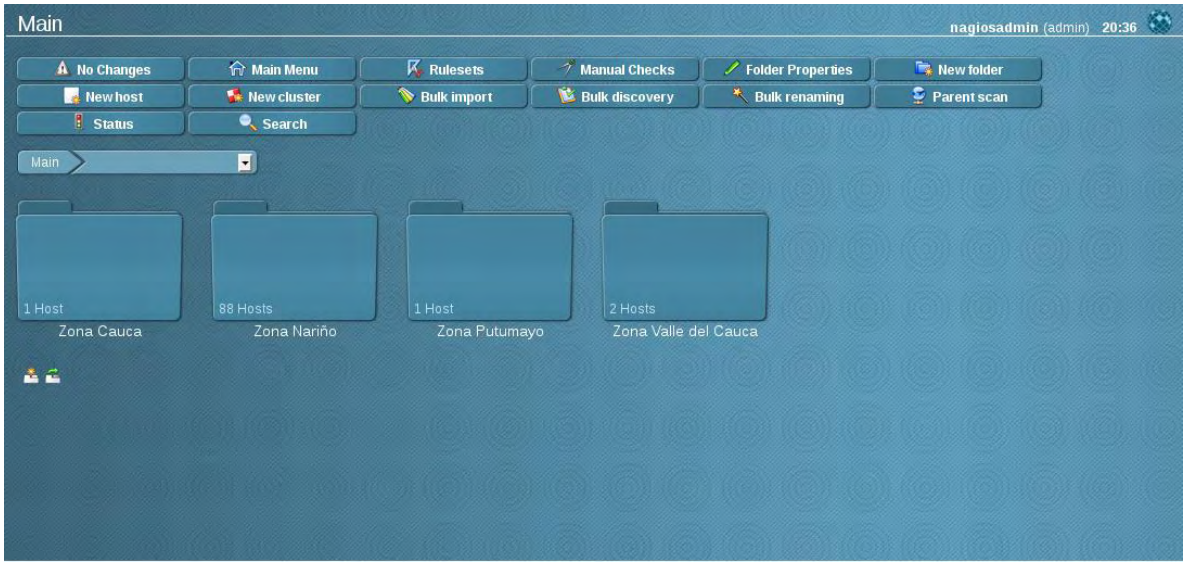


A continuación, se da a conocer lo que muestra cada opción.

Main Menu: Muestra las opciones de la barra de configuración en el entorno de trabajo con su respectiva descripción.



Hosts: En esta opción se pueden crear, organizar y visualizar todos los hosts. Dentro de las principales opciones encontramos: crear nuevo host (New host), crear nuevas carpetas (New folder) y aplicar reglas (Rulesets) ya sea a host o grupos de host mediante las carpetas.



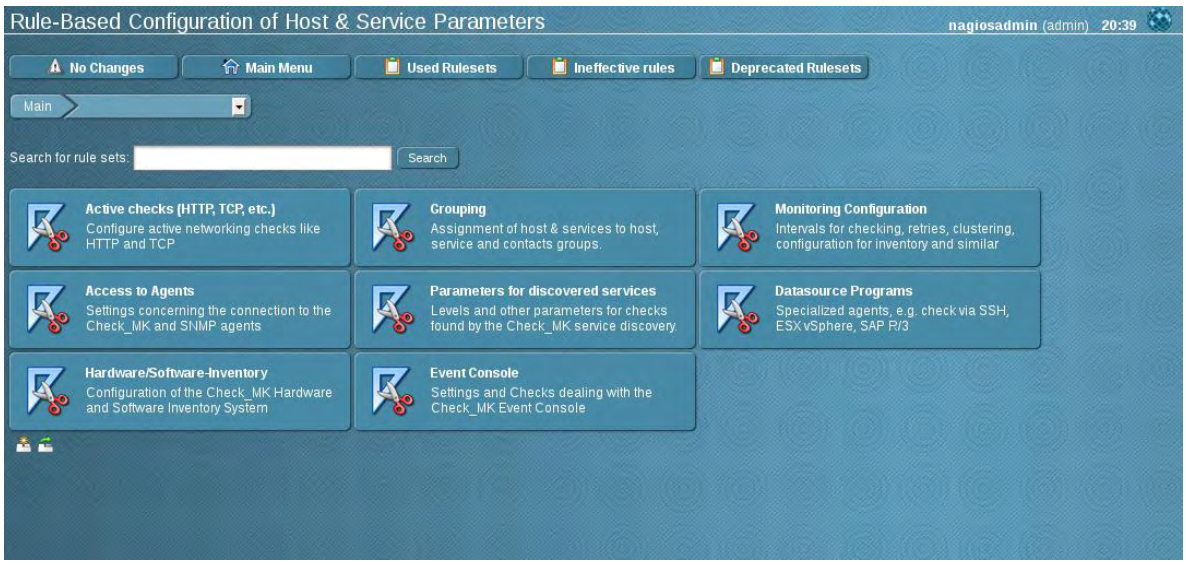
Esta es la forma como se presenta la información de cada host creado.

Las acciones que se pueden realizar a un host son:

- A - Editar las propiedades del host.
- B - Vista de los parámetros de las reglas del host.
- C - Editar los servicios del host.
- D - Mover el host a otra carpeta.
- E - Crear un clon del host.
- F - Eliminar el host.



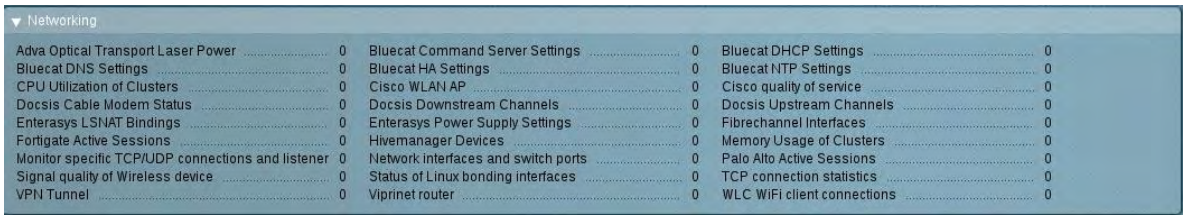
Host & Service Parameters: En esta opción se encuentran agrupadas todas las reglas configurables a los host, dependiendo de la acción que se desee realizar; ya sea a los host o a los servicios.



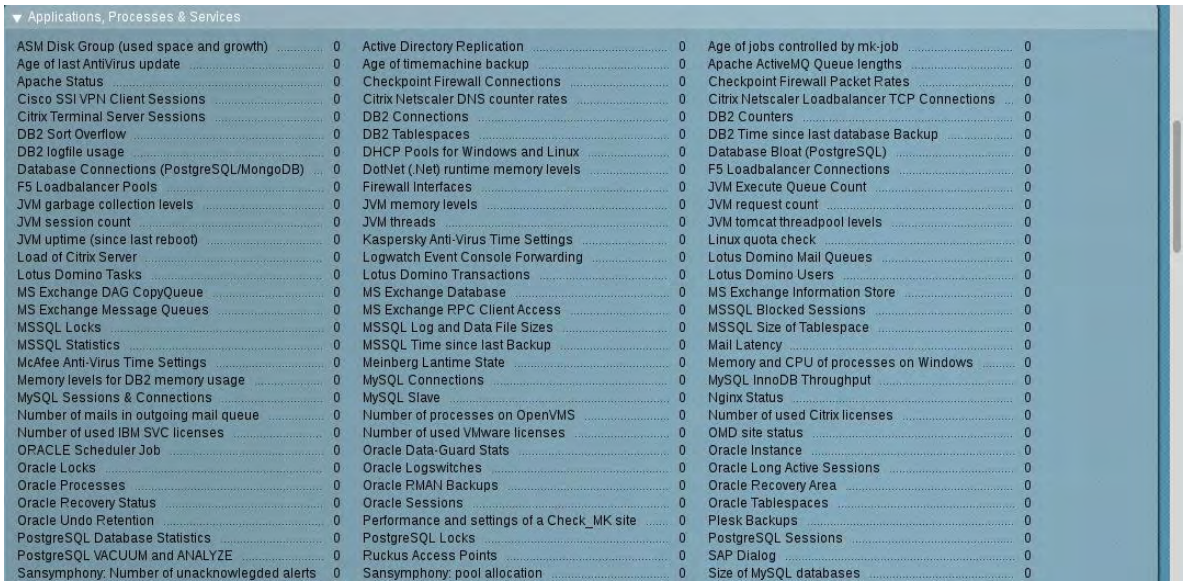
Se pueden configurar reglas para comprobar el estado de los servicios que se monitorean.

Estas comprobaciones se encuentran clasificadas por áreas. De la siguiente manera:

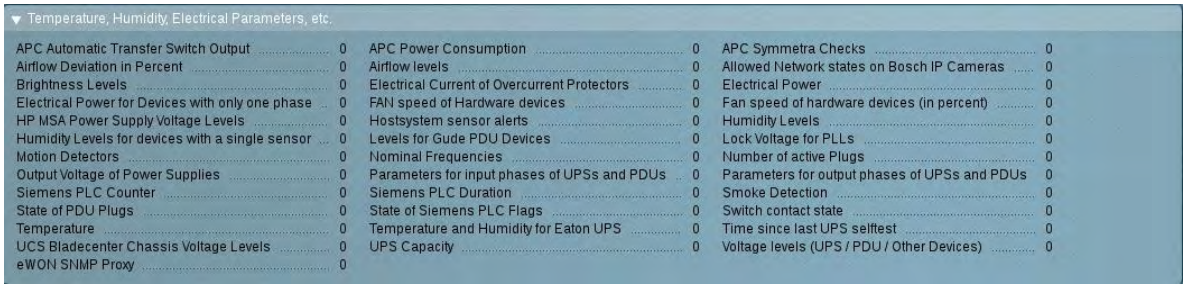
Área de Redes.



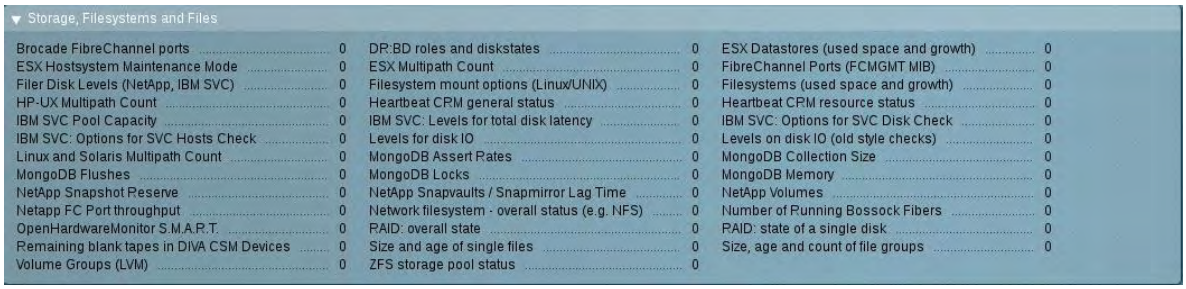
Área de Aplicaciones, Procesos y Servicios.



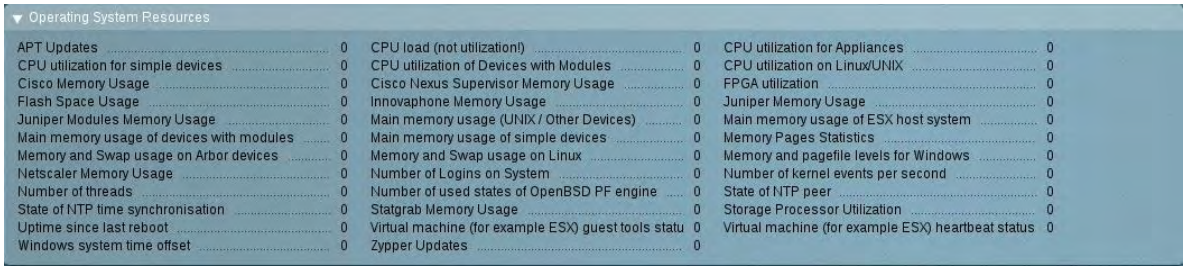
Área de Temperatura, Humedad, Parámetros eléctricos, etc.



Área de Almacenamiento, Sistemas de archivos y Archivos.



Área de Recursos del sistema operativo.



Área de impresoras.



Área de Virtualización.



Área de Hardware y BIOS.

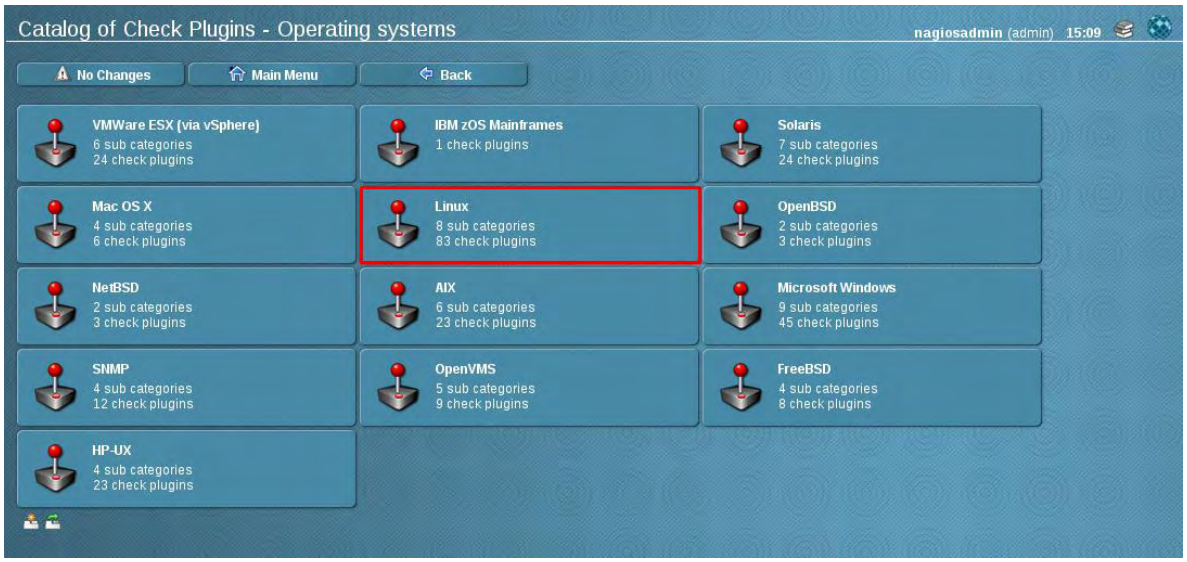


Check plugins: Se encuentra un catálogo agrupado de los plugins de monitoreo con los que cuenta la herramienta Check_mk.

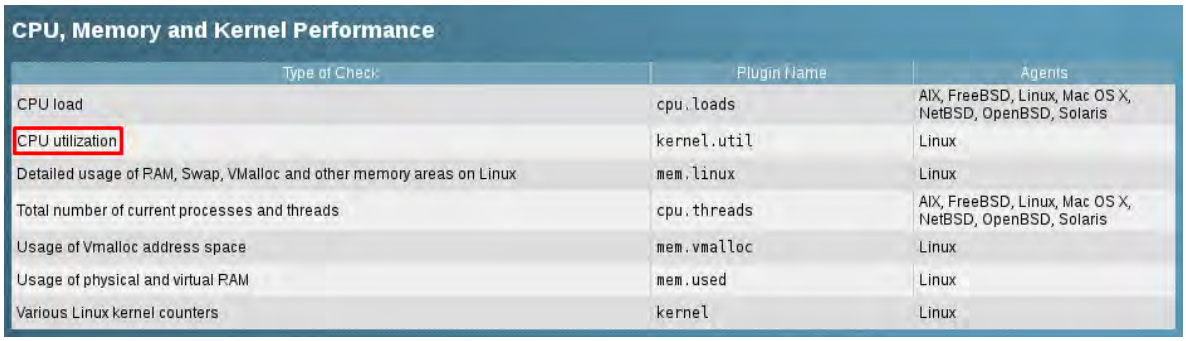
A continuación, vamos a realizar un ejemplo de cómo utilizar uno de ellos en un área específica, en este caso plugins clasificados por sistemas operativos.



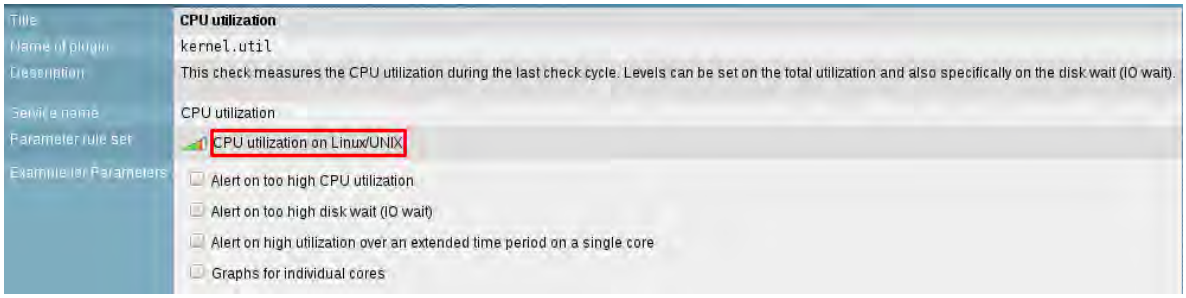
Se selecciona la opción de plugins para LINUX.



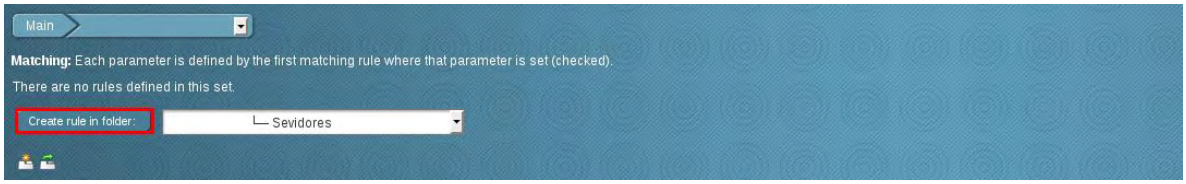
Se elige el plugin a utilizar, en este caso un plugin que monitoree la utilización de la CPU.



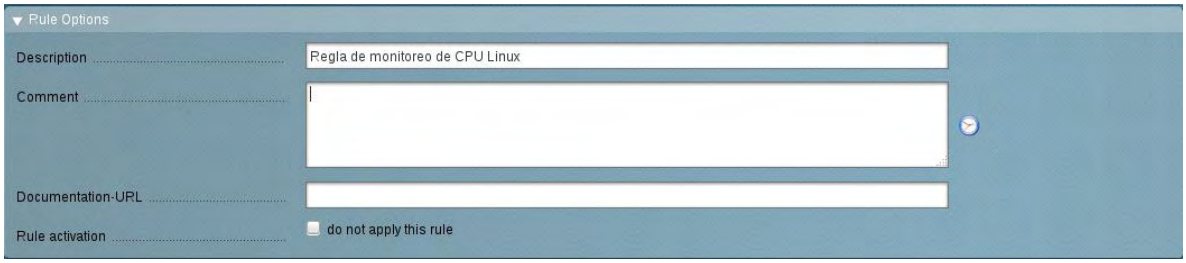
Se ingresa a la configuración de los parámetros del plugin para monitorear.



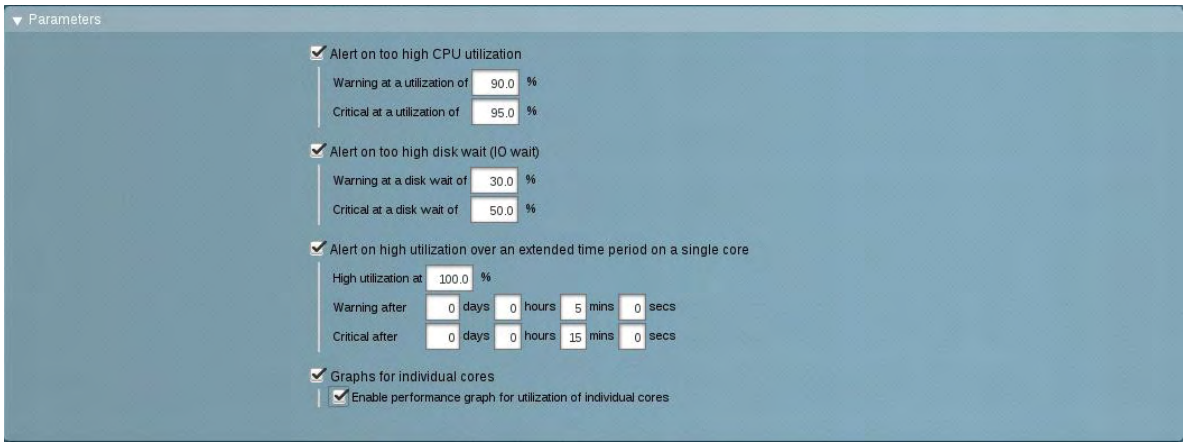
En este caso se monitoreará el servicio de CPU a los servidores.



Se hace una pequeña descripción de lo que se va a monitorear.

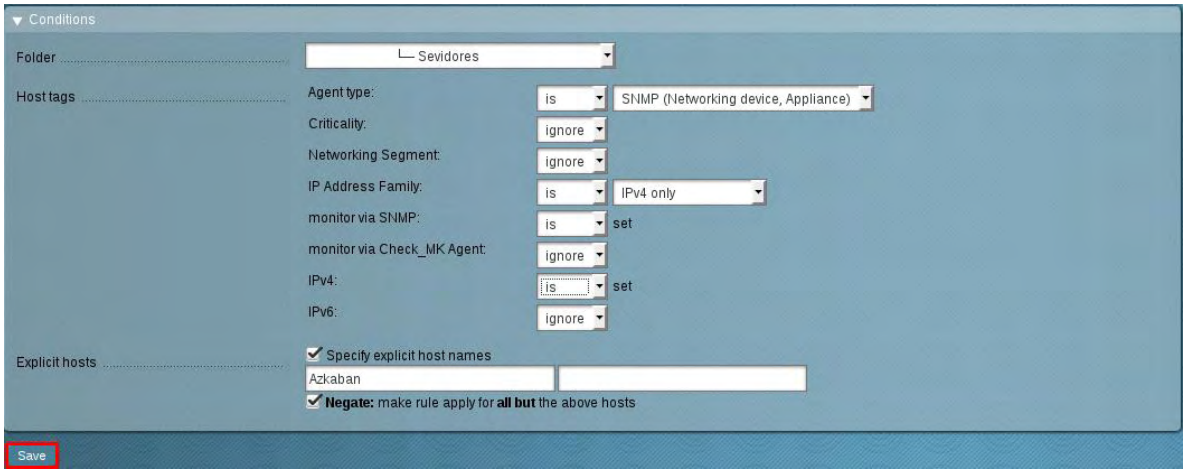


Se configuran los parámetros a evaluar con sus respectivos datos, según lo deseado.



Se especifica al grupo que se va a efectuar el monitoreo, el monitoreo se realizará mediante el agente SNMP y se hará solamente con IPv4.

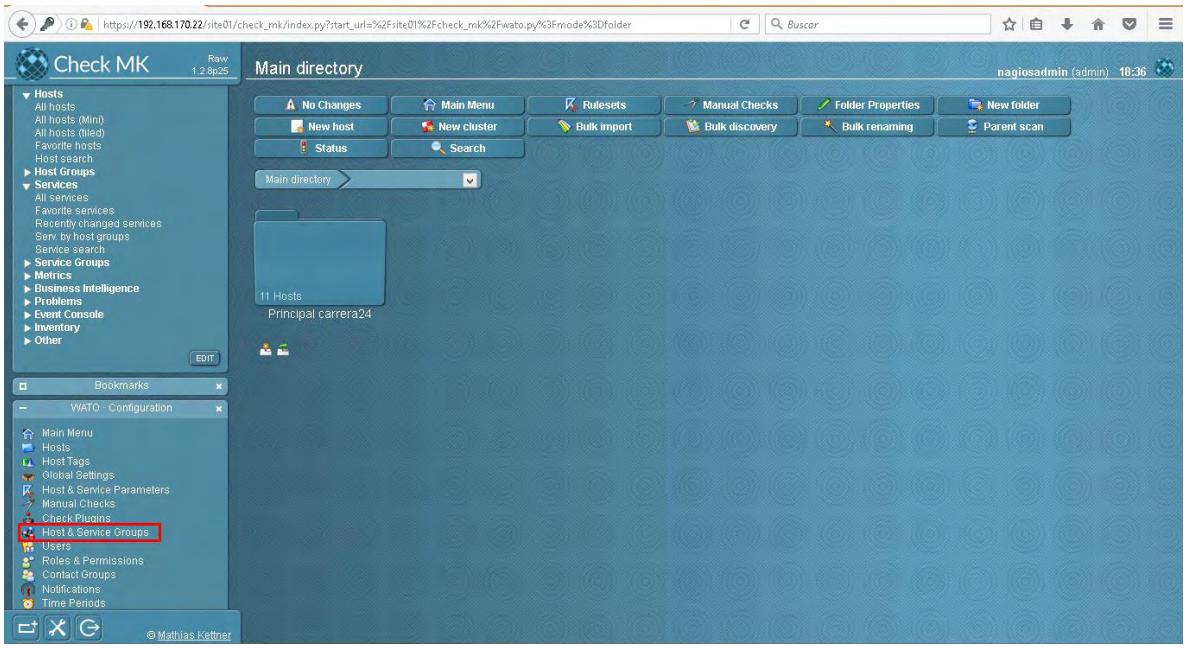
Encontramos la opción Explicit host, esta opción permite ingresar el nombre de un host o varios hosts que se desean excluir de este monitoreo.



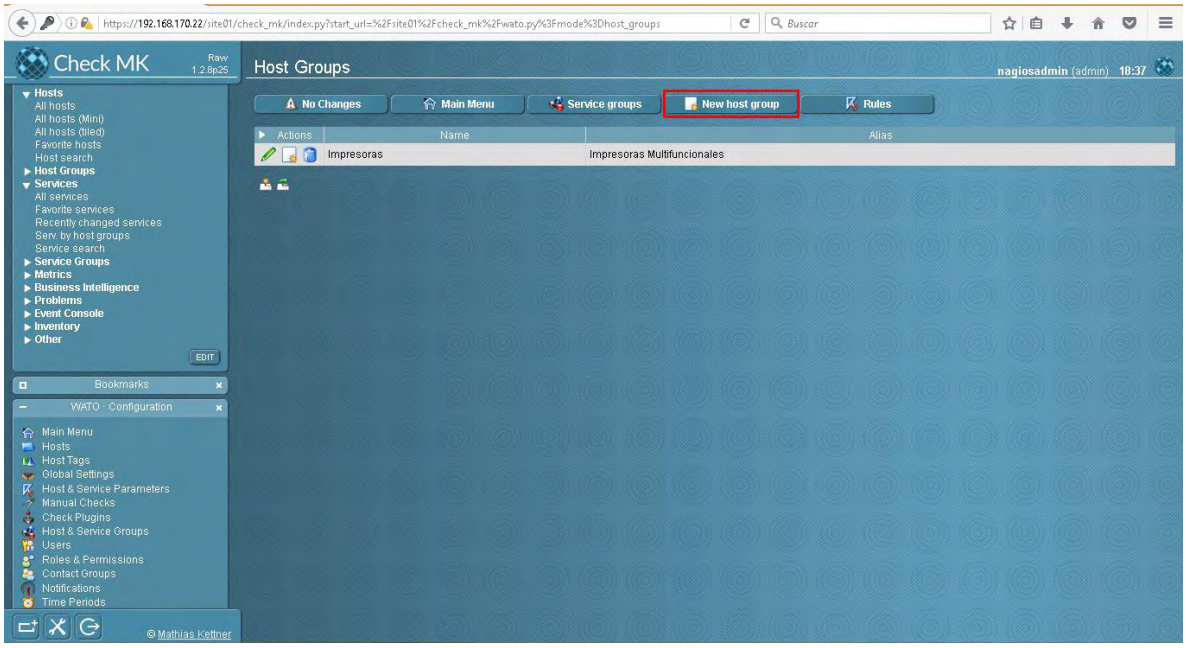
Host & Service groups: Permite crear grupos de hosts y grupos de servicios.

A continuación, se hace un ejemplo de cómo crear un grupo de hosts.

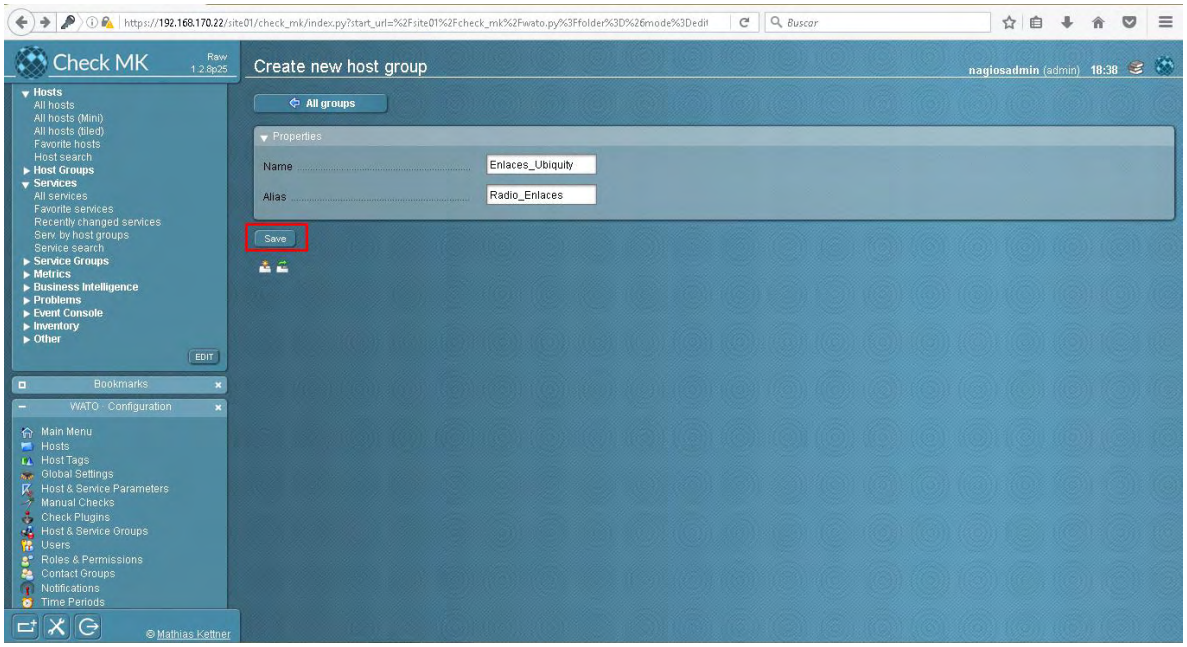
Se elige la opción “Host & Service groups”.



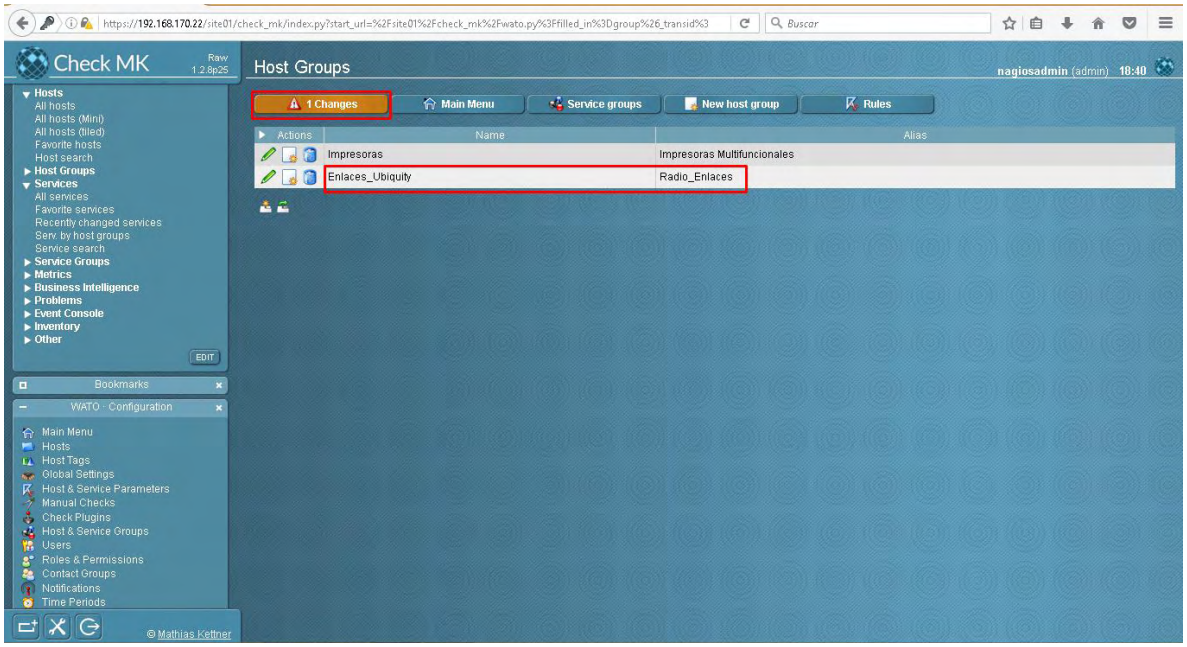
Se crea un nuevo grupo.



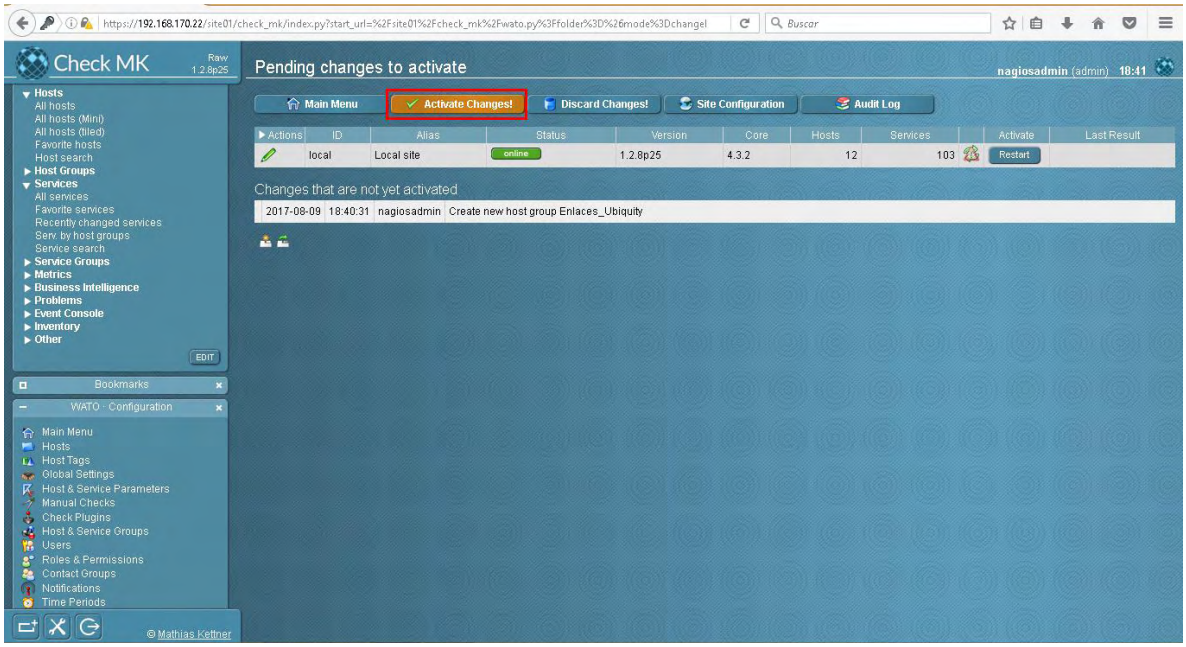
Se completa la información del grupo y se guarda.



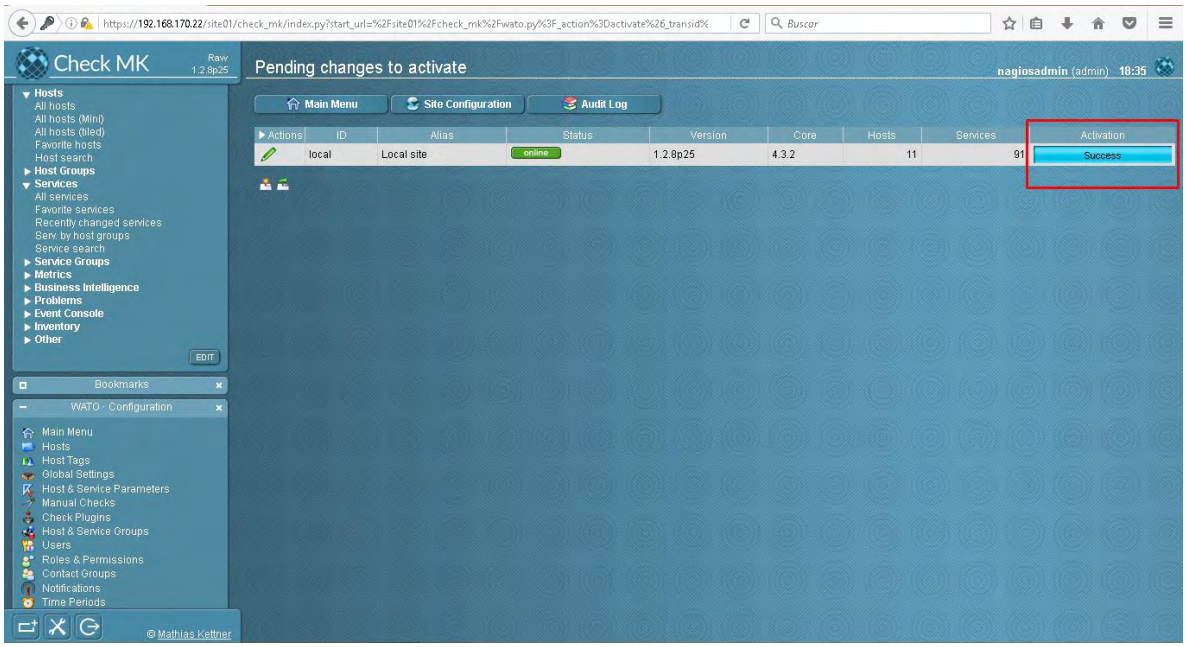
Se guardan los cambios, se observa el nuevo grupo creado.



Se activan los cambios realizados.

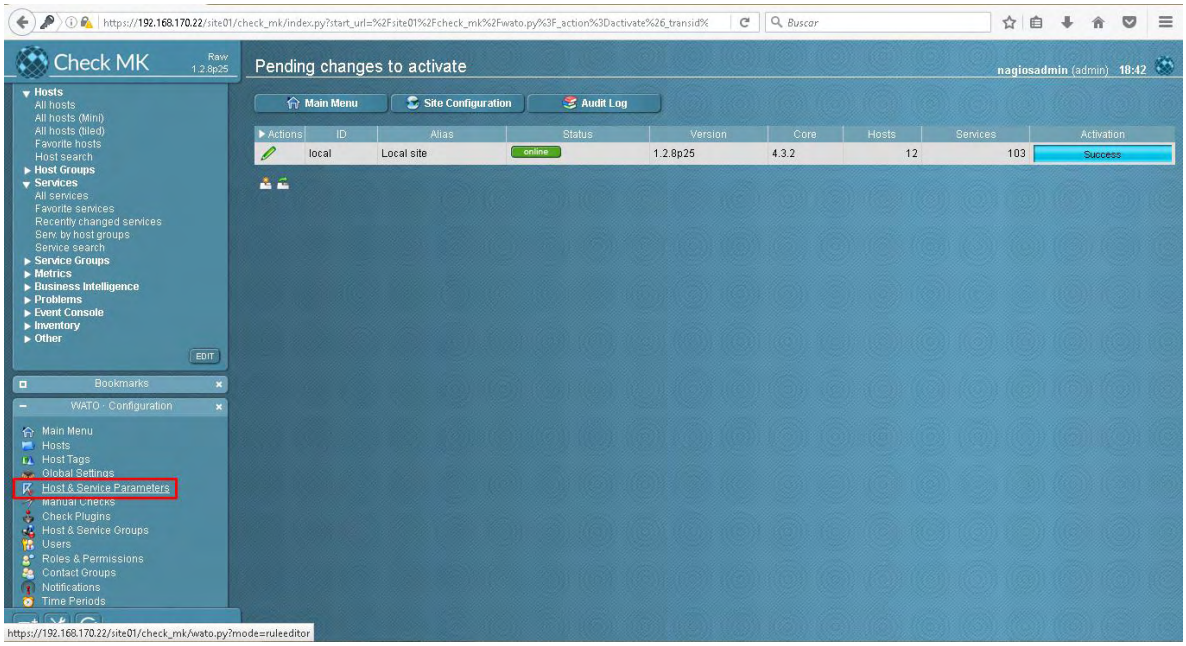


Se verifica que se guarde con éxito la configuración.

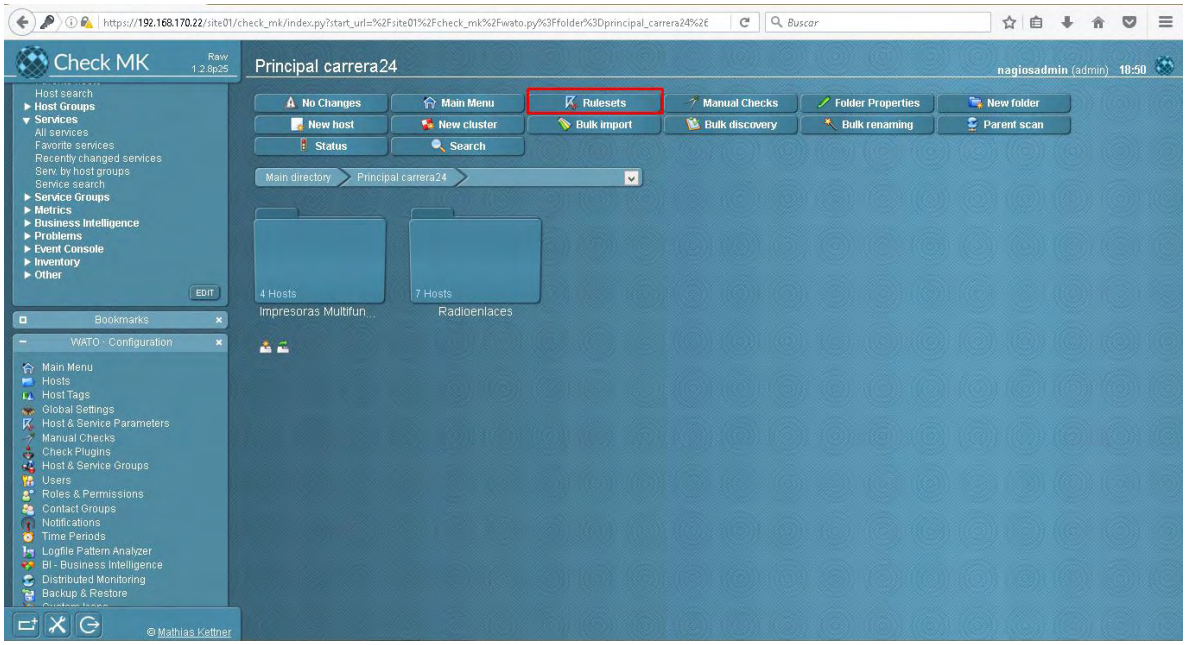


Para poder ingresar equipos a los grupos es necesario crear reglas.

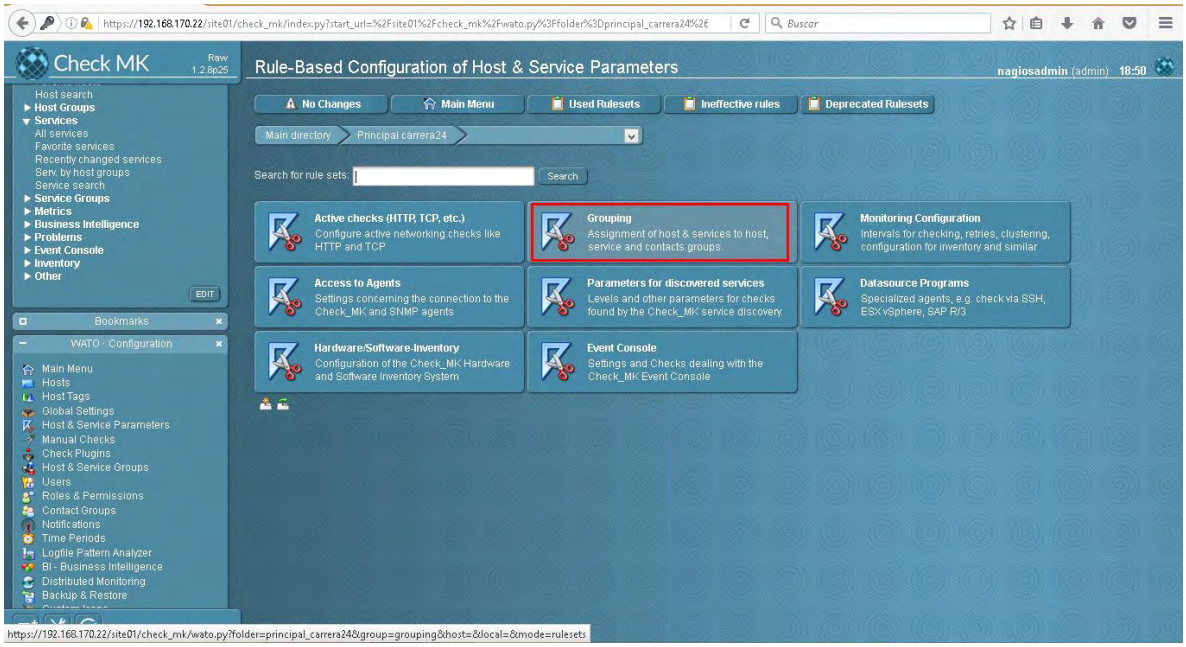
Se selecciona la opción “Host & Service Parameters”.



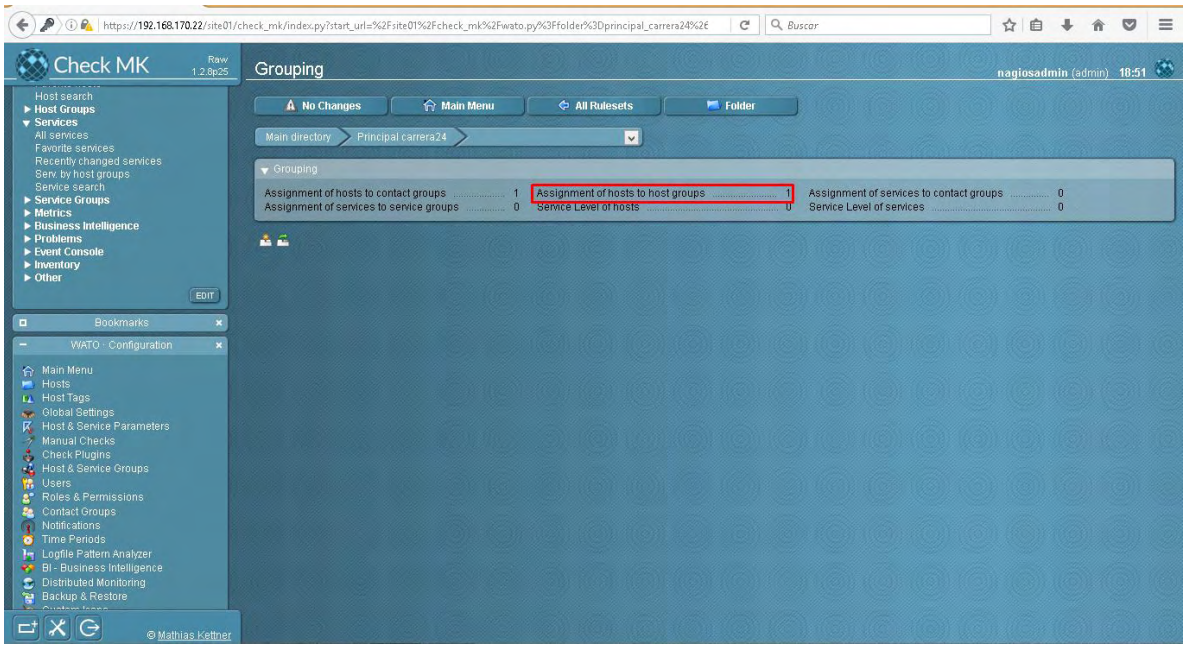
Dentro de la configuración de check_mk existen reglas ya definidas. Se utilizará una de ellas dando en la opción “Rulesets”.



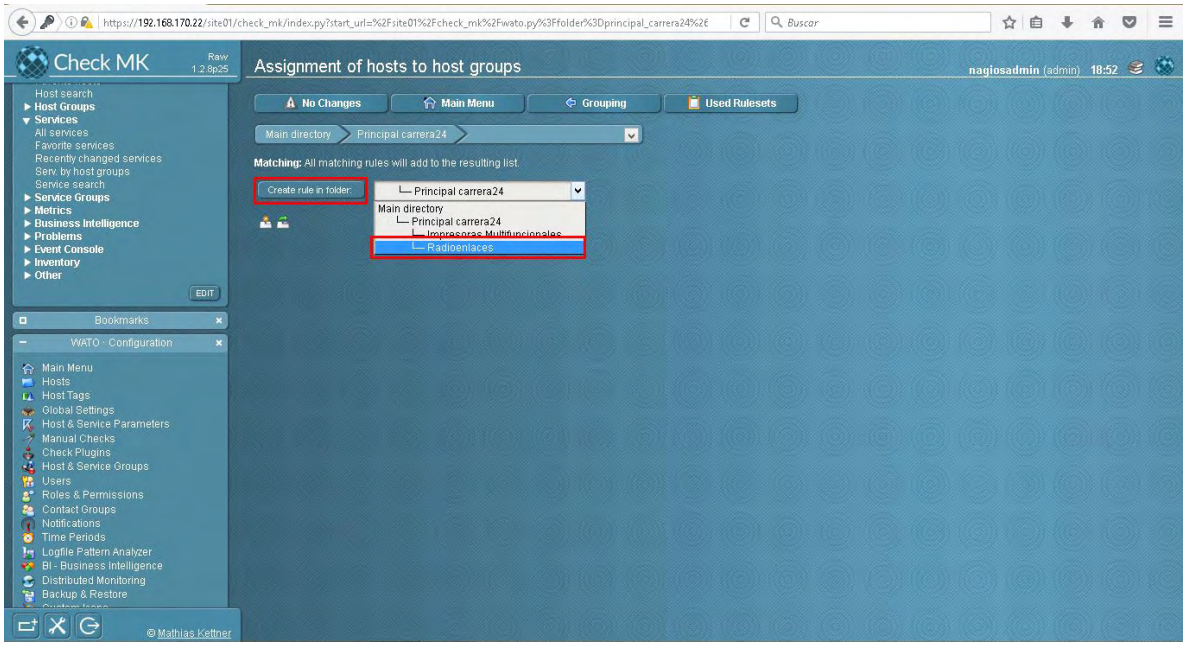
Una regla es la asignación de host a grupos, lo que permite tener más ordenada la información del monitoreo.



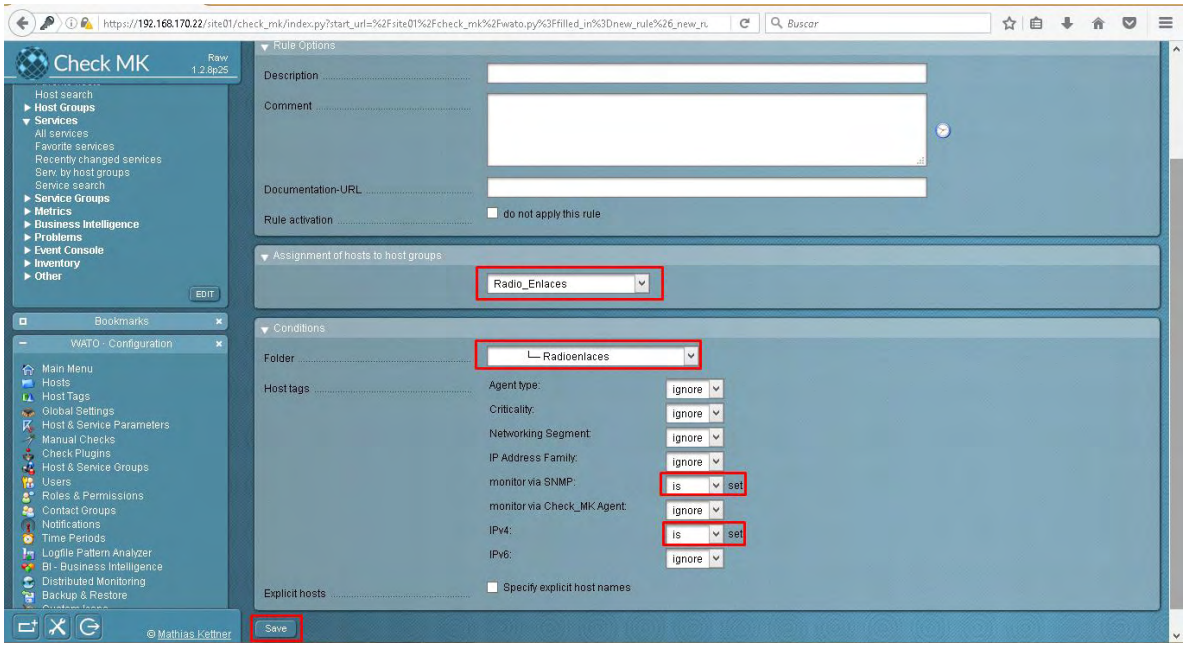
Se selecciona la opción asignar hosts a grupos de host.



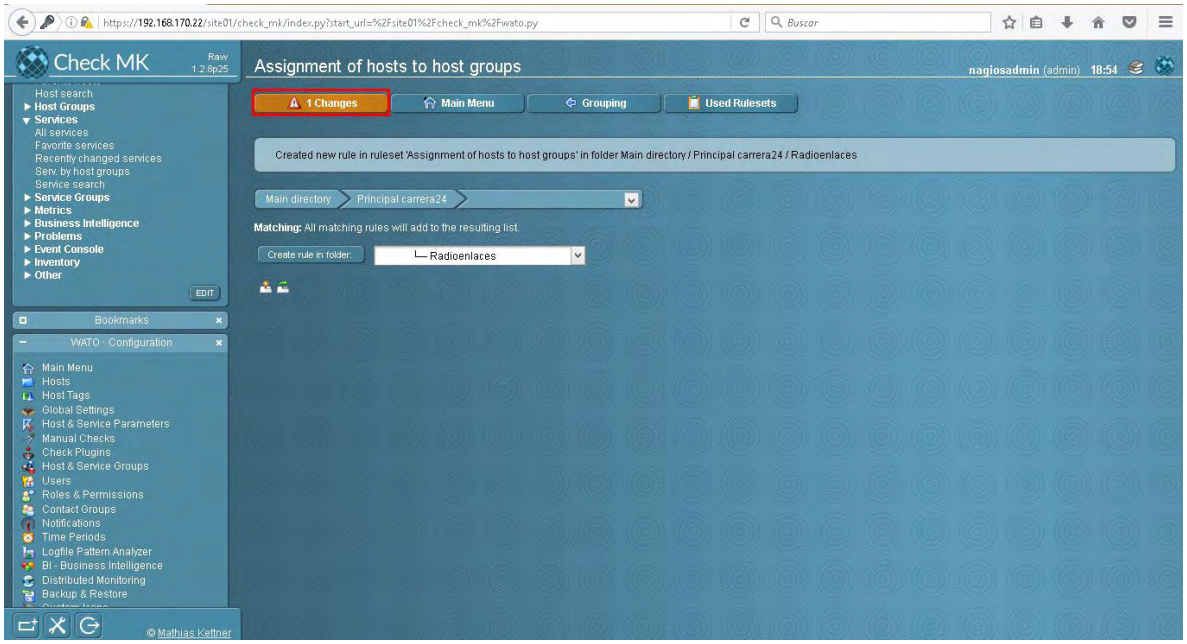
La regla se crea con los equipos que se encuentran en el folder de radioenlaces. Debido a que el grupo radioenlaces va a contener todos los hosts de este tipo.



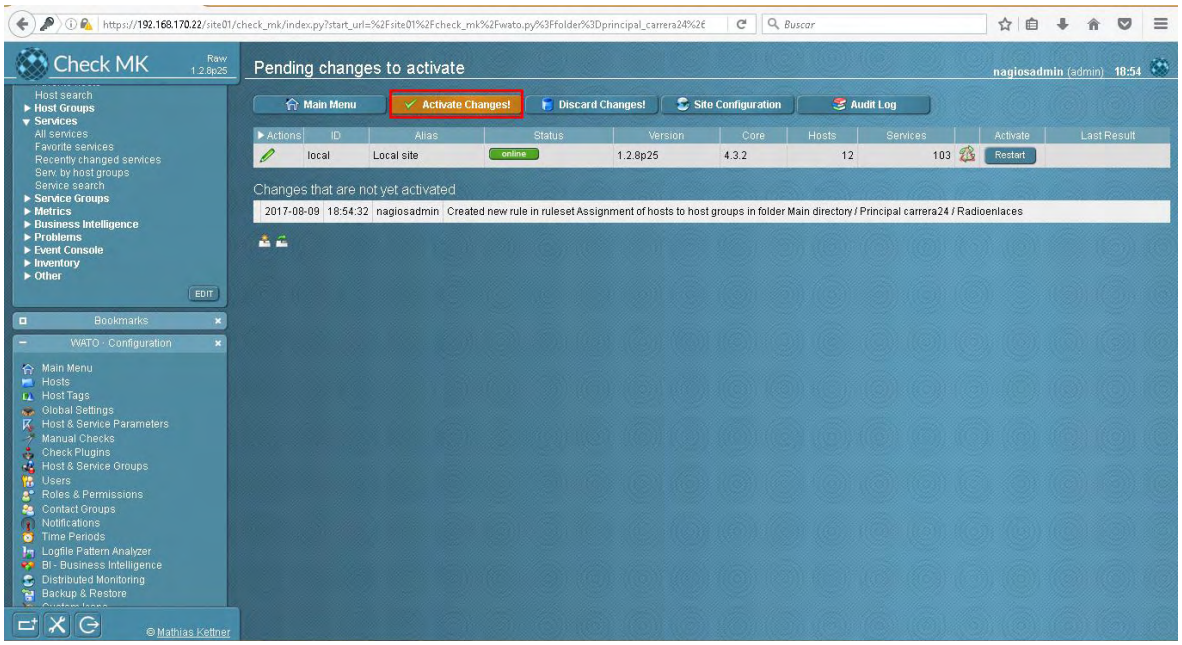
Se realiza la configuración de la regla, se tiene en cuenta que estos dispositivos se monitorean a través del agente SNMP. Se procede a guardar la configuración.



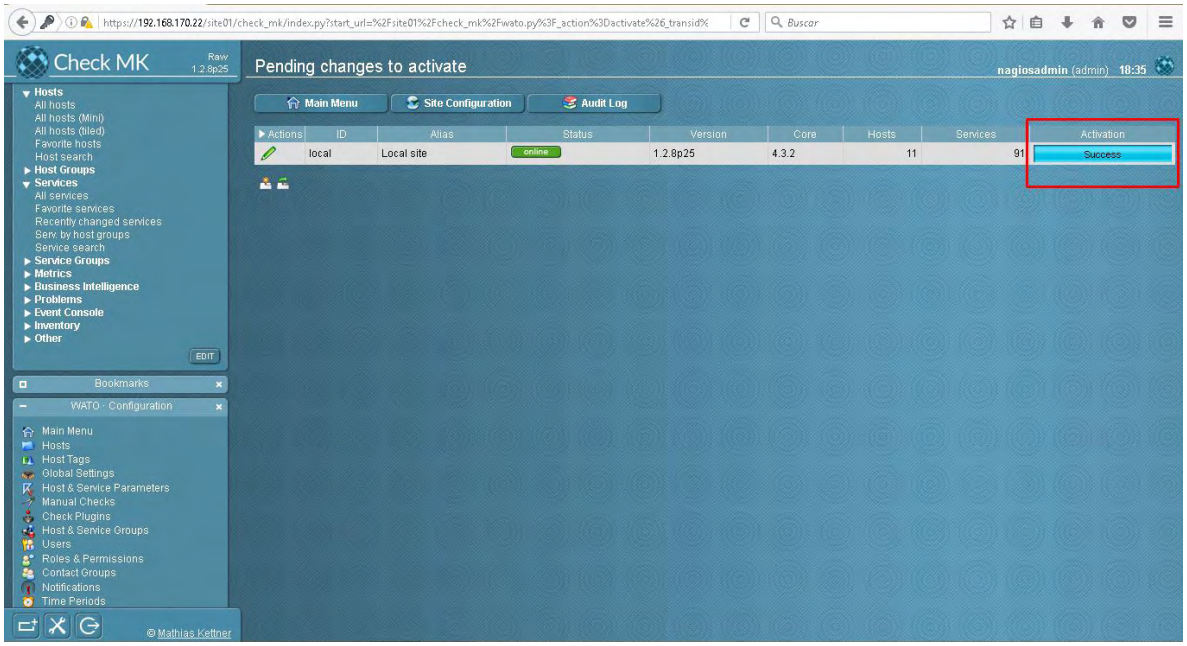
Se guardan los cambios realizados.



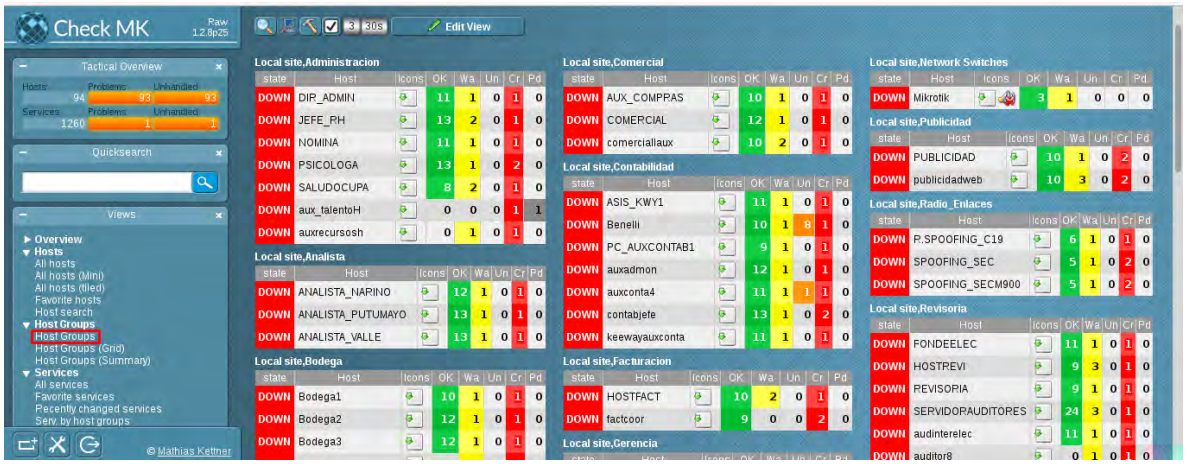
Se activan los cambios.



Se verifica que la nueva configuración se realice con éxito.



En la barra de vistas se da la opción Host Groups y mostrara lo siguiente:



Users: En esta opción se crean usuarios, los cuales van a tener acceso a la suite de monitoreo. Además, a estos se les podrá enviar notificaciones mediante email.

A continuación, se creara un usuario.

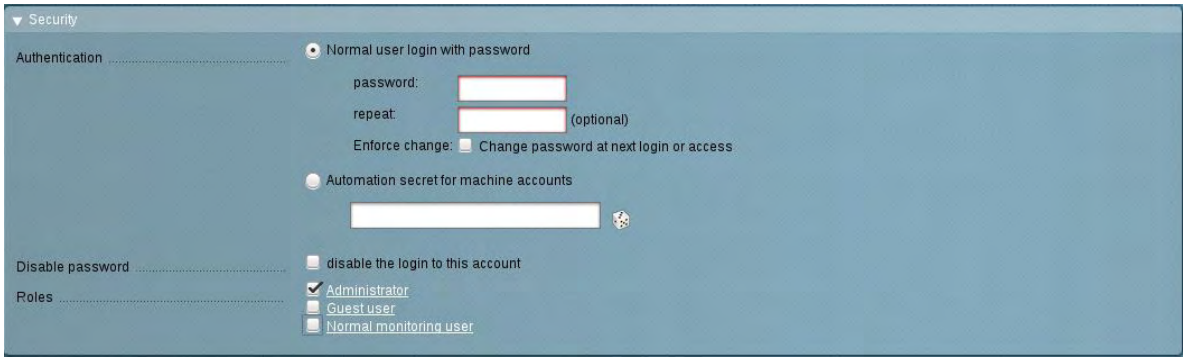
Se elige la opción New User.



Se llena la información del usuario, muy importante la dirección de correo electrónico. Si se desea enviar notificaciones a este usuario el email debe ser del servidor de correos GMAIL debido a configuraciones previas.

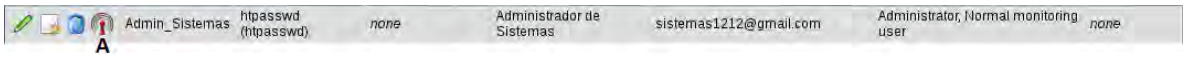


Se crea la contraseña de usuario y se selecciona el rol.



Luego de guardar cambios, se mostrará el usuario creado de la siguiente manera:

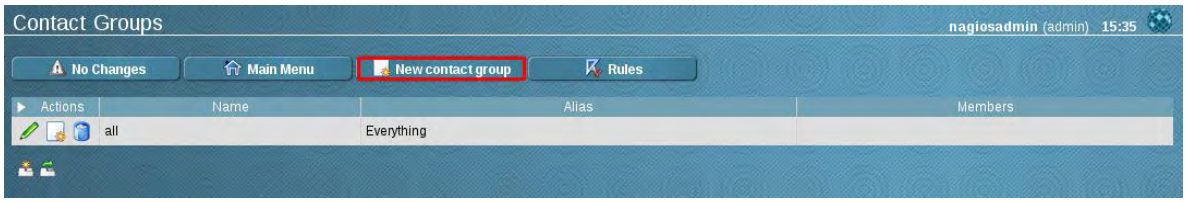
Seleccionando la opción A se podrá configurar el envío de notificaciones para este usuario.



Roles & Permissions: En esta opción se pueden editar los permisos que tendrá cada rol.



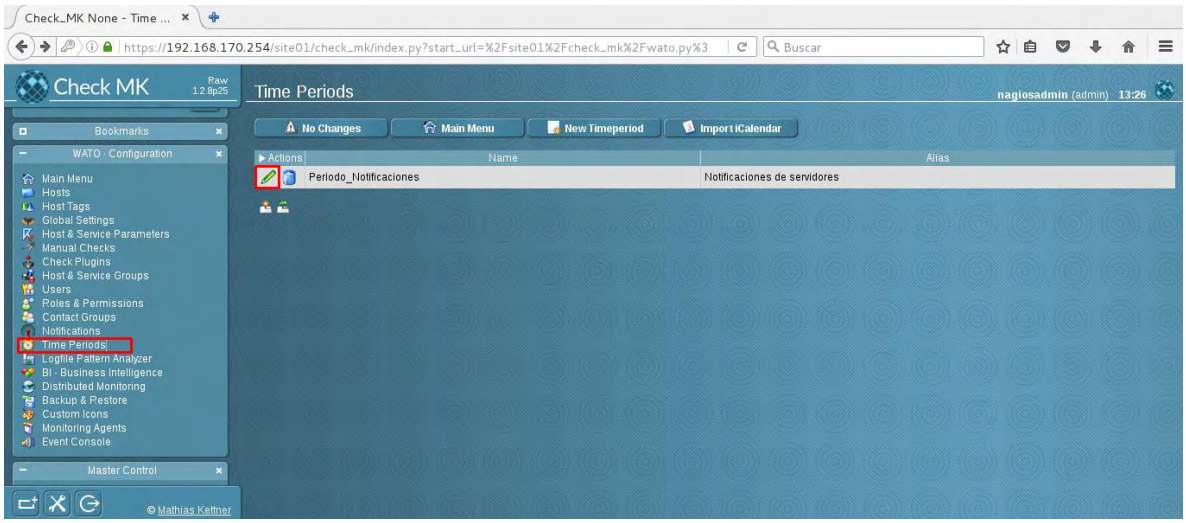
Contact Groups: Se crean grupos de contacto. Esto es útil si se desea repartir tareas de la administración del monitoreo, por ejemplo, el monitoreo por áreas. Si solo hay un administrador de la red de datos no es conveniente crear grupos de contacto.



Time Periods: En esta opción se crean periodos para las notificaciones.

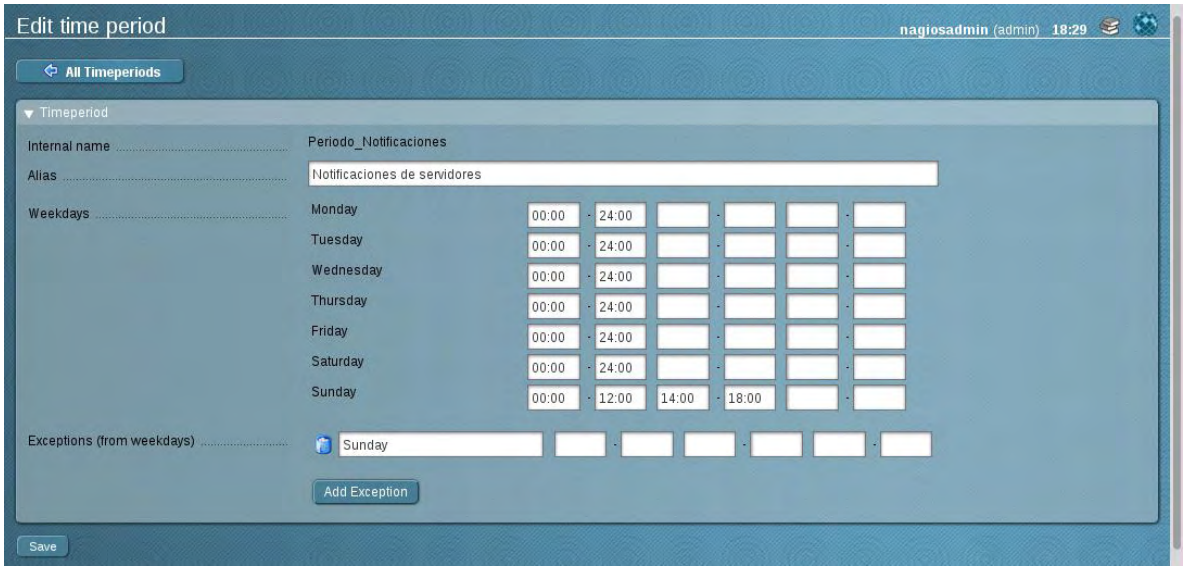
A continuación, se hará un ejemplo de cómo crear o editar un Time Periods.

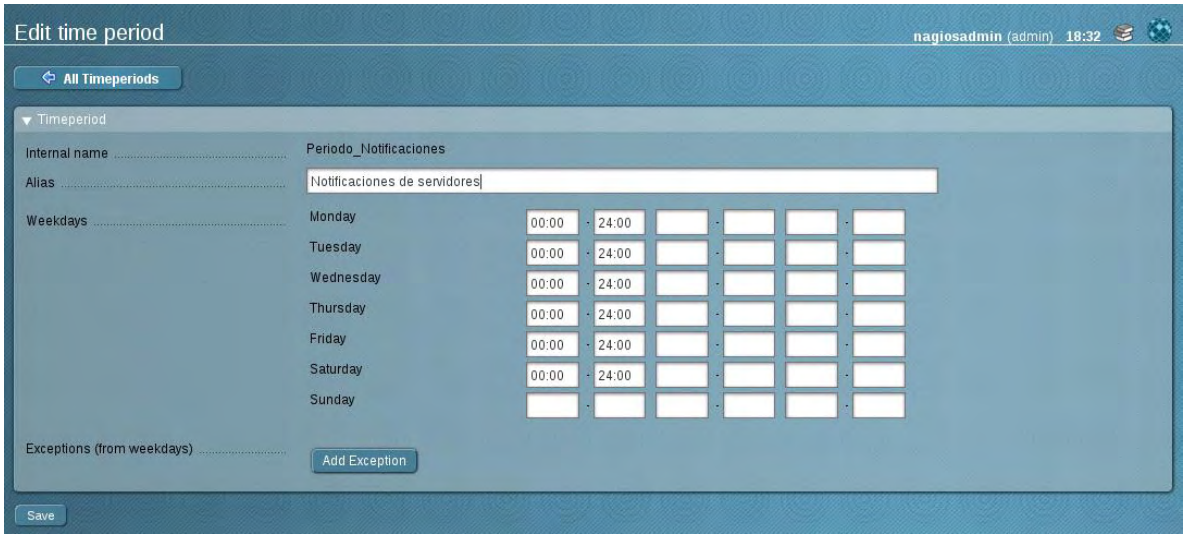
Se elige la opción Time Periods y en este caso se edita el Time Periods creado anteriormente.

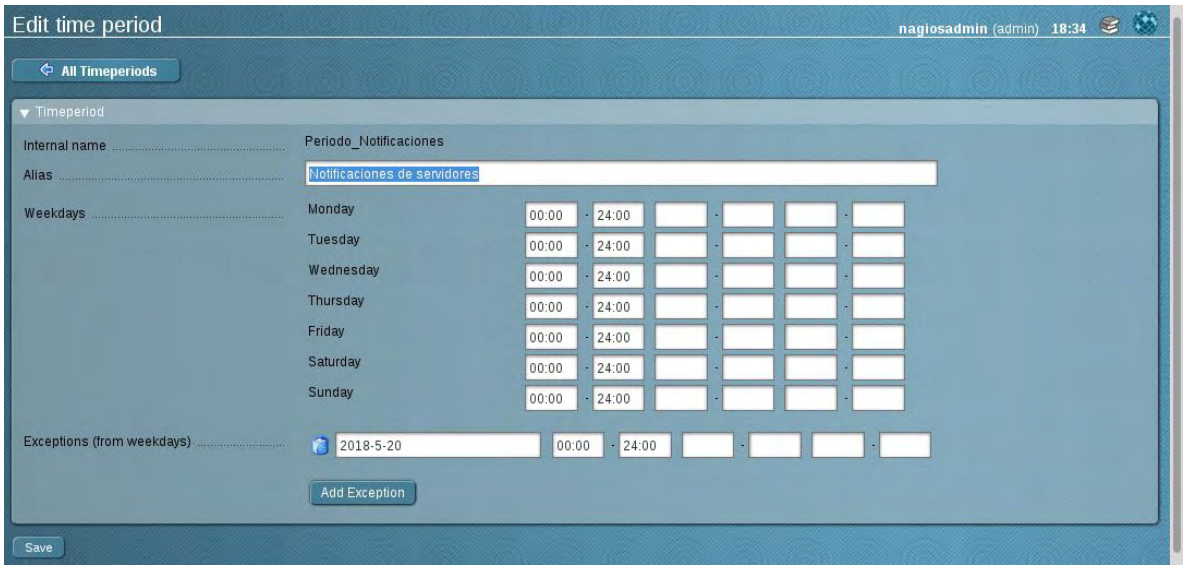


A continuación, se muestran unos ejemplos de cómo hacer un Time period.

Luego, se guardan los cambios. Y el Time Period se lo utiliza al momento de configurar notificaciones a los usuarios.







- Backup & Restore

El backup es recomendable hacerlo desde la terminal. Se lo hace de la siguiente manera:

Para crear la copia de seguridad se elige un nombre de archivo, por ejemplo, backup-1.tar.gz y se usa la opción --backup.

Se usa la opción -v para salida detallada.

```
check_mk -v -- backup backup-1.tar.gz
```

Mostrará lo siguiente:

```
root@debian1205:/home/henry/Descargas# check_mk -v --backup backup-1.tar.gz
Creating backup file 'backup-1.tar.gz'...
  Adding Main configuration file (/usr/local/check_mk/main.mk) (73 bytes)...
  Adding Final configuration file final.mk (/usr/local/check_mk/final.mk) (0 bytes)...
  Adding Configuration sub files (/usr/local/check_mk/conf.d) (163840 bytes)...
  Adding Automatically inventorized checks (/var/lib/check_mk/autochecks) (122880 bytes)...
  Adding Performance counters (/var/lib/check_mk/counters) (430080 bytes)...
  Adding Agent cache (/var/lib/check_mk/cache) (1740800 bytes)...
  Adding Logwatch (/var/lib/check_mk/logwatch) (1884160 bytes)...
Successfully created backup.
root@debian1205:/home/henry/Descargas#
```

Antes de restaurar el backup es necesario dar permisos de forma recursiva al directorio “conf.d”.

```
chmod -R 777 /usr/local/check_mk/conf.d/
```

Para restaurar la copia se hace lo mismo pero con la opción --restore :

```
check_mk -v --restore backup-17.tar.gz
```

Mostrará lo siguiente:

```
root@debian1205:/home/henry/Descargas# check_mk -v --restore backup-1.tar.gz
Restoring from 'backup-1.tar.gz'...
  Deleting old version of '/usr/local/check_mk/main.mk'
  Extracting Main configuration file (/usr/local/check_mk/main.mk)
  Changing ownership to root:root
  Deleting old version of '/usr/local/check_mk/final.mk'
  Extracting Final configuration file final.mk (/usr/local/check_mk/final.mk)
  Changing ownership to root:root
  Deleting old contents of '/usr/local/check_mk/conf.d'
  Extracting Configuration sub files (/usr/local/check_mk/conf.d)
  Changing ownership to root:root
  Deleting old contents of '/var/lib/check_mk/autochecks'
  Extracting Automatically inventorized checks (/var/lib/check_mk/autochecks)
  Changing ownership to root:root
  Deleting old contents of '/var/lib/check_mk/counters'
  Extracting Performance counters (/var/lib/check_mk/counters)
  Changing ownership to nagios:root
  Deleting old contents of '/var/lib/check_mk/cache'
  Extracting Agent cache (/var/lib/check_mk/cache)
  Changing ownership to nagios:root
  Deleting old contents of '/var/lib/check_mk/logwatch'
  Extracting Logwatch (/var/lib/check_mk/logwatch)
  Adding group write permissions
  Changing ownership to nagios:nagios
Successfully restored backup.
root@debian1205:/home/henry/Descargas#
```

Se reinicia el servicio de check_mk “mkeventd”.

```
/etc/init.d/mkeventd restart
```

3.4 BARRA DE CONTROL

Esta Barra permite activar o desactivar de forma general las acciones que están contenidas en esta barra. Por ejemplo, si no se desean enviar notificaciones se desactiva la opción como lo muestra la imagen.

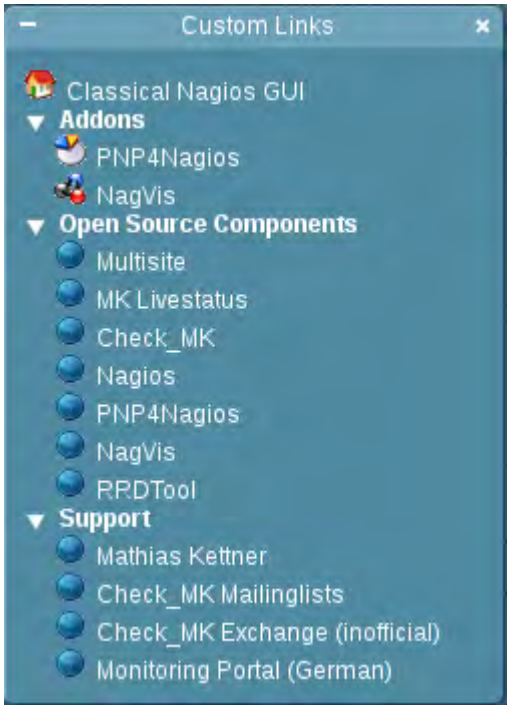


3.5 BARRA DE ENLACES PERSONALIZADOS

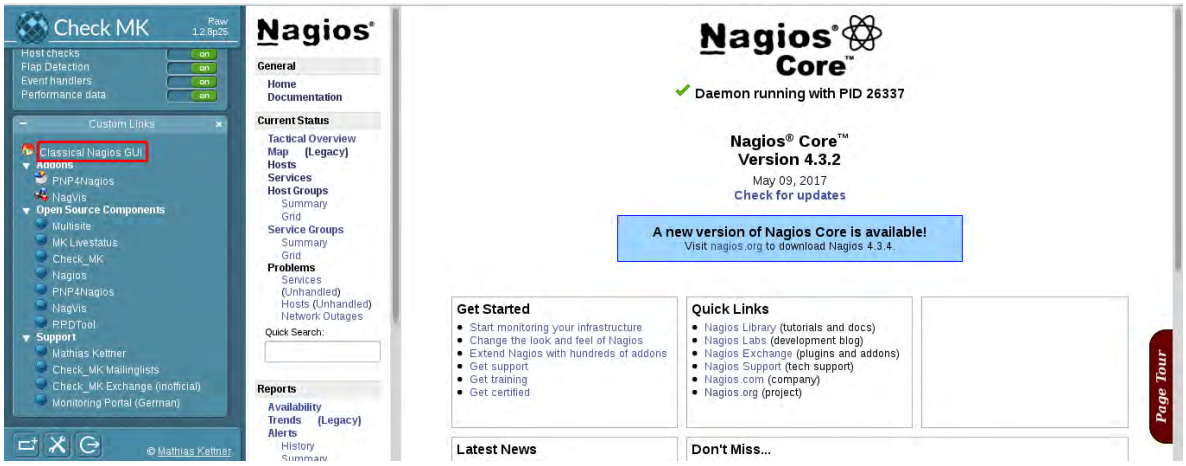
En la primera parte de la barra se tienen los enlaces para ingresar a las herramientas que componen la suite de monitoreo como son: Nagios, PNP4Nagios y Nagvis en donde se pueden obtener muchas opciones de visualizar y configurar el monitoreo de la red de datos.

En la segunda parte de la barra se tienen los enlaces de las paginas donde se encuentra toda la información de las herramientas que componen la suite de monitoreo. En estas páginas se encuentra todo lo referente a los manuales de instalación y configuración, descargas, información adicional, ayuda, etc.

En la tercera parte de la barra están los enlaces de soporte de la aplicación Check_mk.



Classical Nagios GUI: Muestra el entorno de trabajo de la herramienta Nagios.



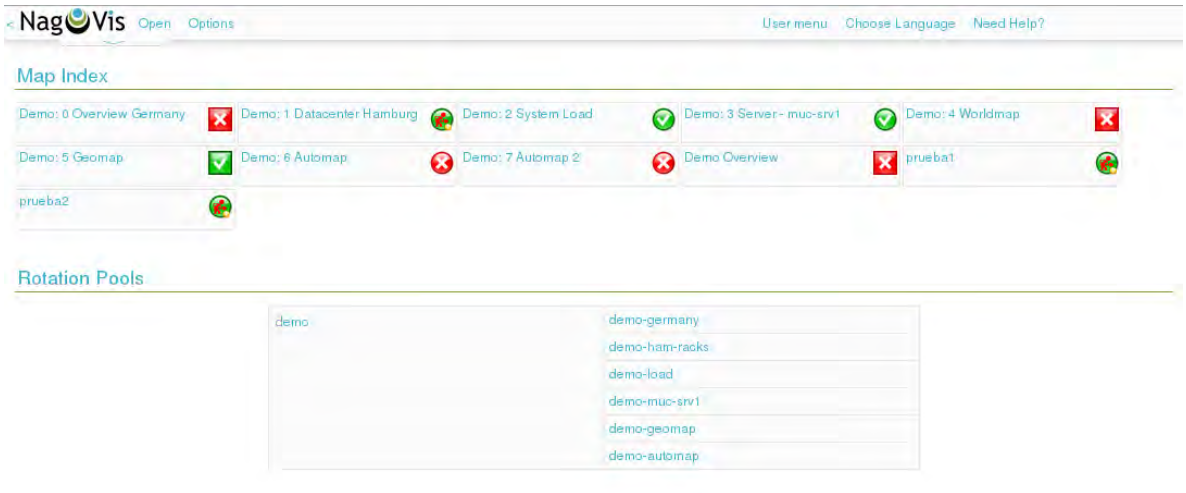
PNP4Nagios: Muestra el entorno de trabajo de la herramienta PNP4Nagios.



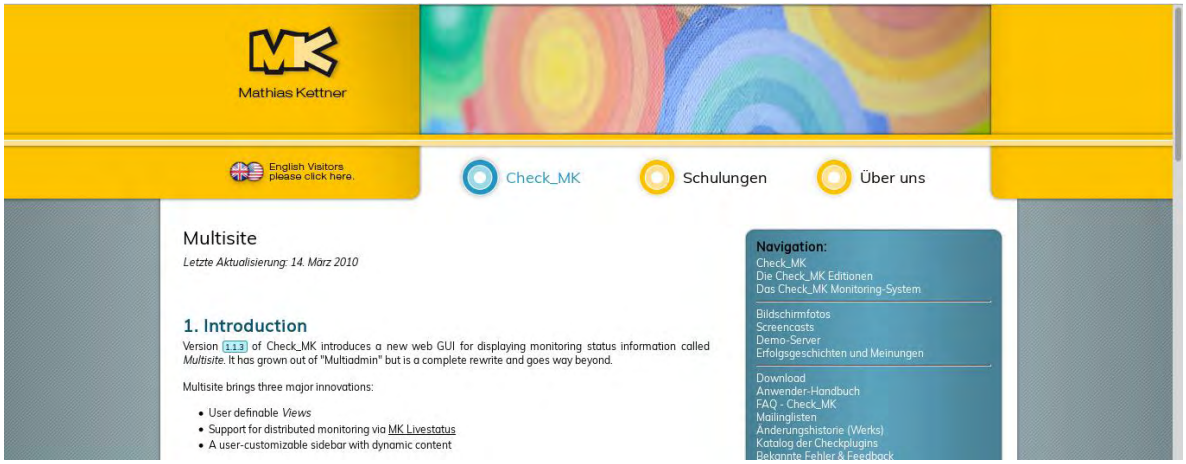
NagVis: Muestra el entorno de trabajo de la herramienta Nagvis.


Check MK
Raw
1.2.8p25
Host checks
Flap Detection
Event handlers
Performance data
Custom Links
Classical Nagios GUI
Addons
PNP4Nagios
NagVis
Open Source Components
Multisite
MK Livestatus
Check_MK
Nagios
PNP4Nagios
NagVis
PPDTool
Support
Mathias Kettner
Check_MK Mailinglists
Check_MK Exchange (inofficial)
Monitoring Portal (German)
© Mathias Kettner
NagVis
Name
Password
Login

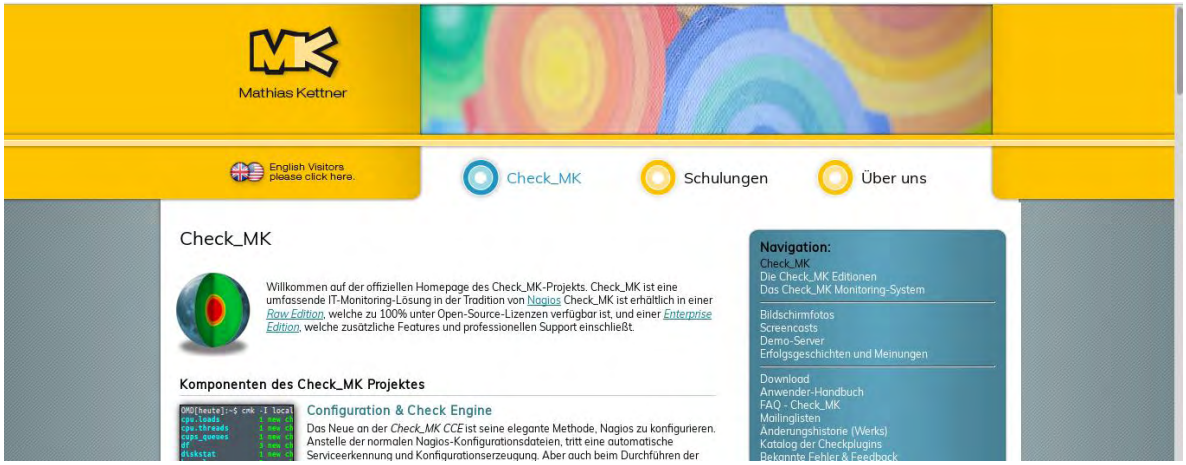

NagVis
Name
admin
Password
Login


NagVis
Open
Options
User menu
Choose Language
Need Help?
Map Index
Demo: 0 Overview Germany
Demo: 1 Datacenter Hamburg
Demo: 2 System Load
Demo: 3 Server - muc-srv1
Demo: 4 Worldmap
Demo: 5 Geomap
Demo: 6 Automap
Demo: 7 Automap 2
Demo Overview
prueba1
prueba2
Rotation Pools
demo
demo-germany
demo-ham-racks
demo-load
demo-muc-srv1
demo-geomap
demo-automap

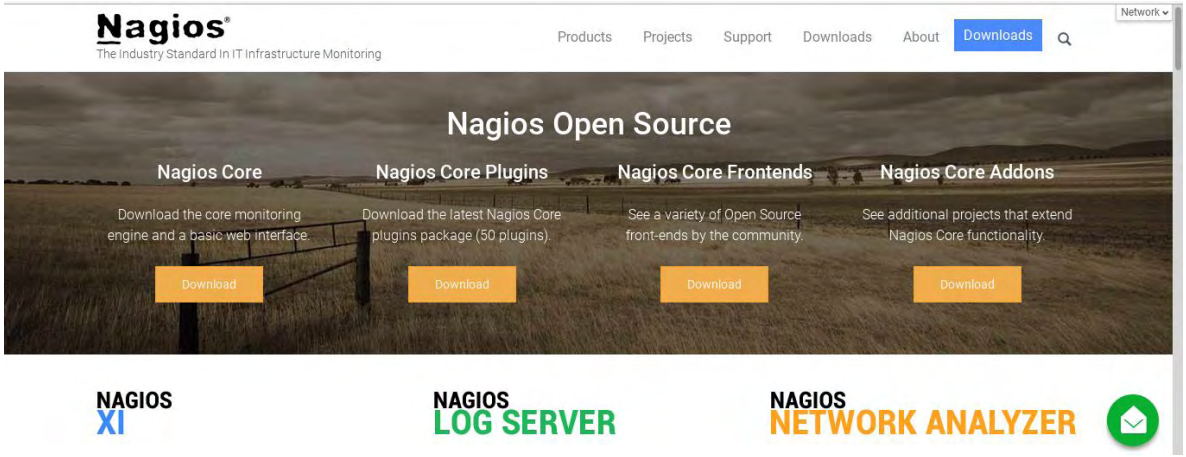
Multisite: Muestra información general de la herramienta Check_mk



Check_mk: Muestra la configuración de la herramienta check_mk con su panel de navegación.



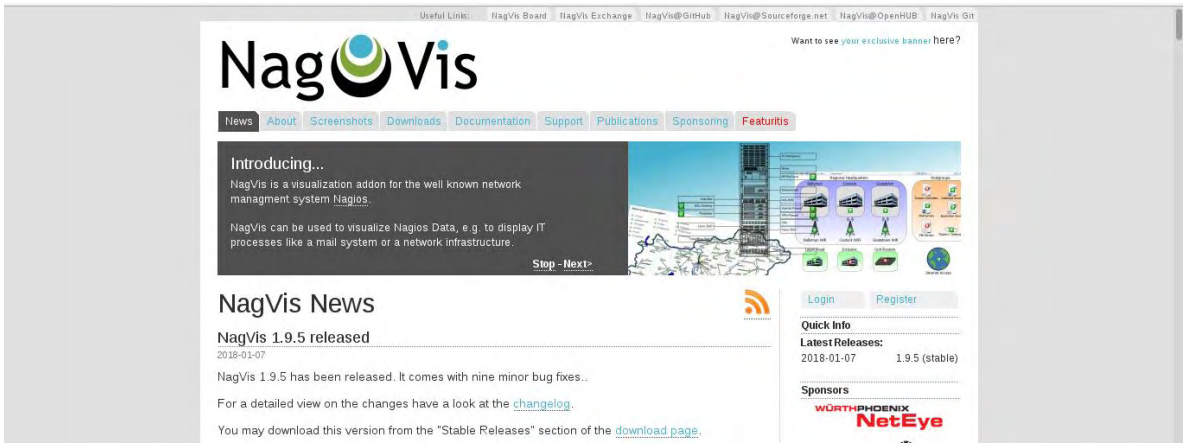
Nagios: Muestra la página principal de Nagios con sus opciones de navegación, para obtener la información completa de esta herramienta.



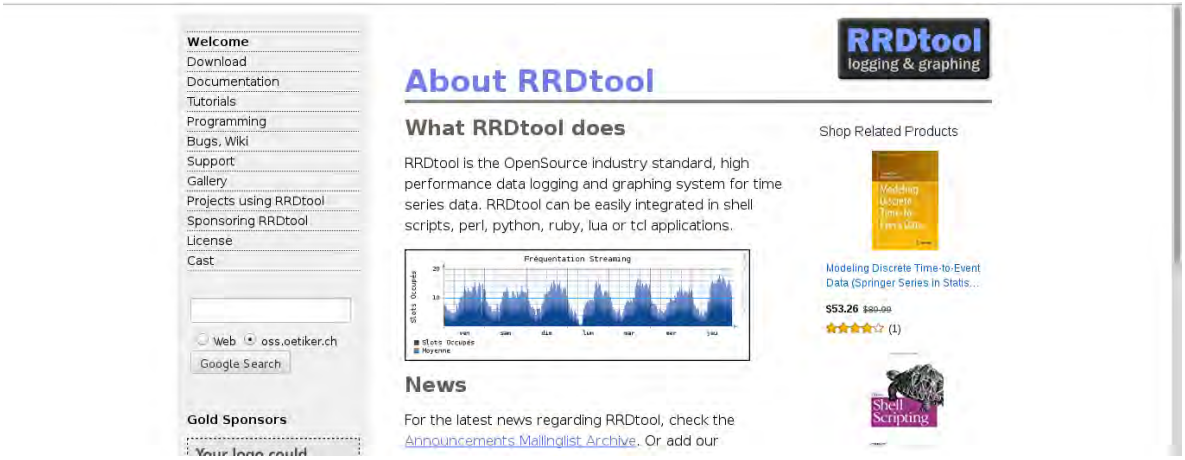
PNP4Nagios: Muestra la página principal de PNP4Nagios.



NagVis: Muestra la página principal de Nagvis.



RRDTool: Muestra la página principal de RRDtool, herramienta que le da un manejo a las gráficas del monitoreo.



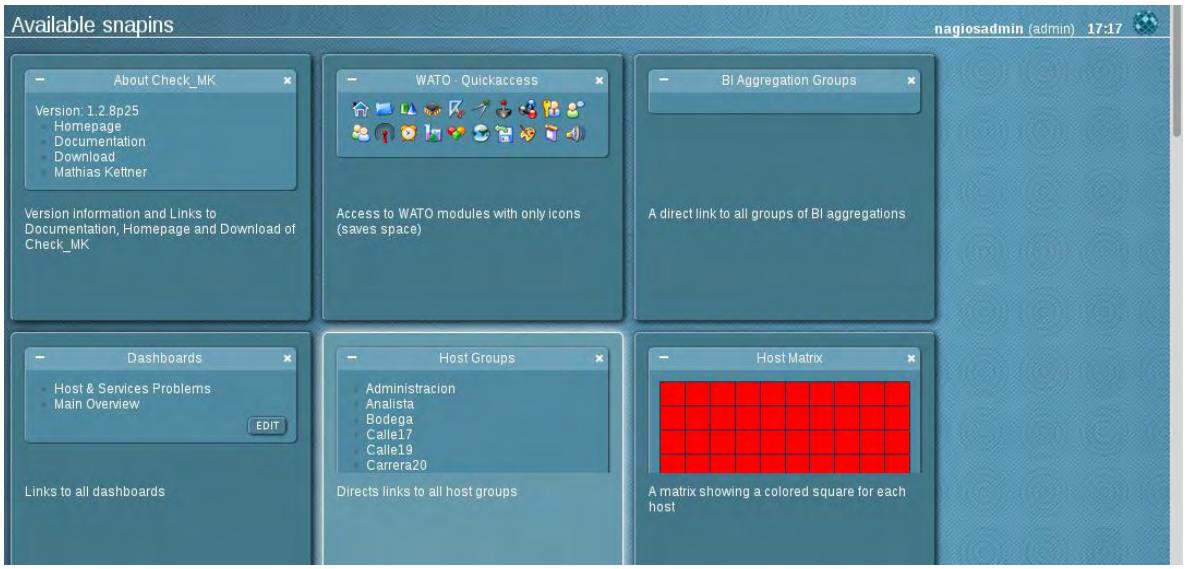
3.6 BARRA DE OPCIONES DE PROGRAMA

En esta se encuentran acciones que se pueden hacer en la herramienta. Las cuales son:

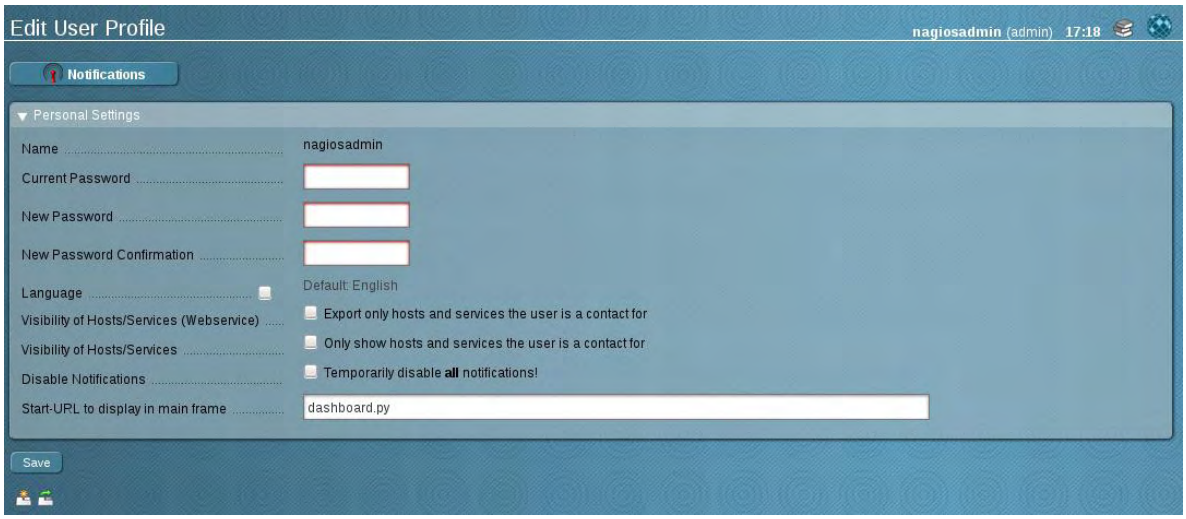


- 1 - Nuevo Proyecto
- 2 - Abrir Proyecto existente
- 3 - Guardar Proyecto

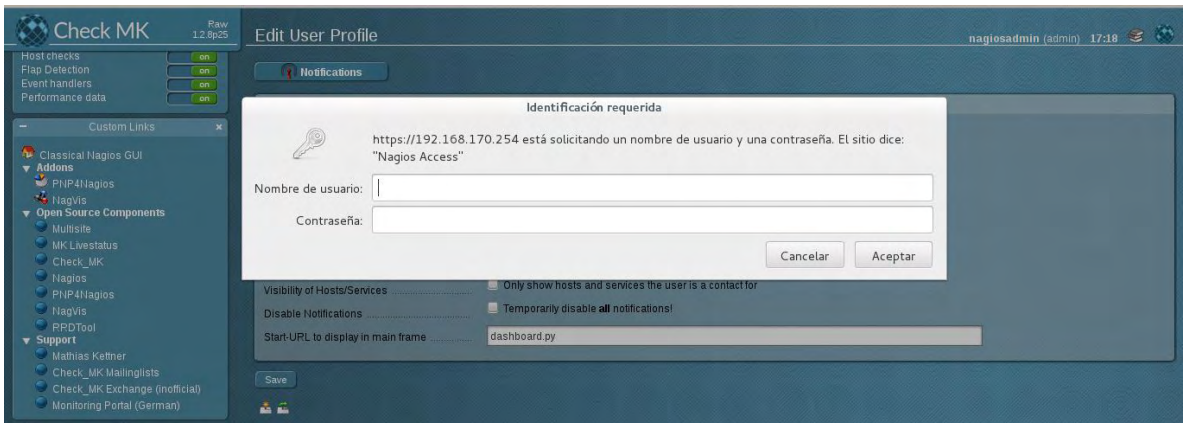
Con esta opción se logra observar diferentes paneles de navegación los cuales pueden ser arrastrados a la barra de herramientas y así poder tener accesos directos según la necesidad del usuario.



Con esta opción se puede editar la contraseña de un usuario para su posterior ingreso a la suite de monitoreo.

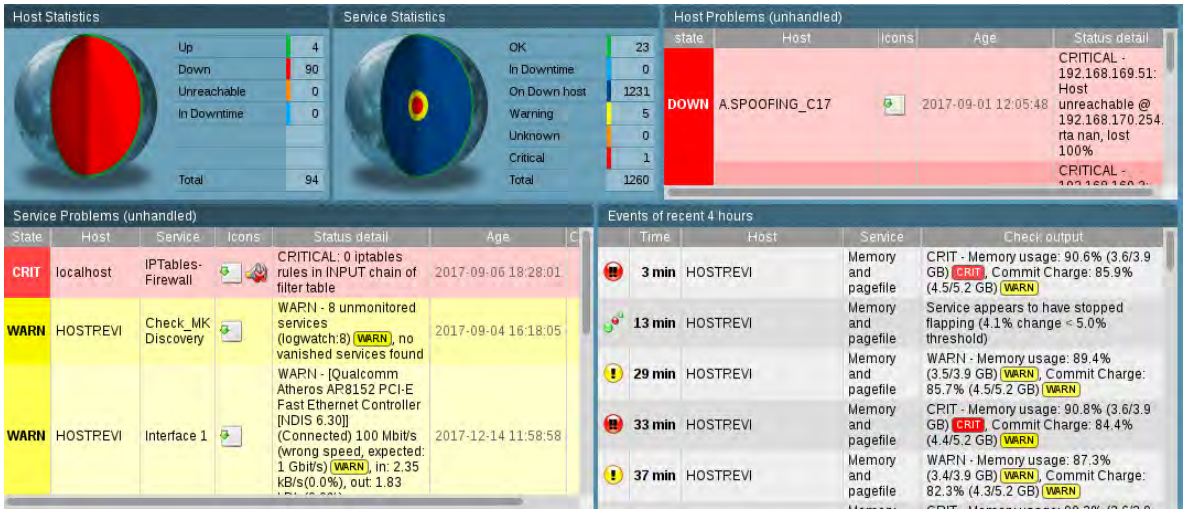


Con esta opción se cierra sesión de la suite de monitoreo, ya sea para finalizar la sesión o para hacer cambio de usuario para el ingreso.



3.7 ÁREA DE VISIÓN GENERAL

En esta área se puede visualizar los contenidos de todo el proceso de monitoreo desde la configuración hasta los resultados, dependiendo de la navegación donde se encuentre el usuario.



NOTA: Cabe resaltar que la interfaz de la herramienta es muy intuitiva y fácil de manejar, tiene textos de ayuda en la mayoría de las opciones colocando el puntero en cada opción; lo que ayuda al administrador a ser más práctico. Además, cuenta con cajas de texto donde se define información de los servicios y cuenta con ejemplos de configuración para entender mejor los procesos de monitoreo.

Anexo S. Acta de capacitación personal área de sistemas.

	UNIVERSIDAD DE NARIÑO		
	FORMATO ACTA DE CAPACITACIÓN	REVISION 00	ENERO 2018

PROGRAMA DE INGENIERIA DE SISTEMAS

ACTA DE CAPACITACIÓN

ACTA No 01

En la ciudad de Pasto a los 25 días del mes de Enero de 2018, se reunieron los encargados del área de sistemas de la empresa JL Y RB SAS Electromillonaria con previa convocatoria realizada por Henry Gaviria Cerón y Julian Portilla Lagos, egresados del programa de ingeniería de sistemas de la universidad de Nariño.

A continuación se presenta el objetivo y los temas a tratar de la capacitación.

Objetivo:	Temas:
Capacitar al personal del área de sistemas en la configuración y manejo de la suite de monitoreo.	• Alcance y delimitaciones del proyecto. • Planteamiento del problema. • Objetivo del Proyecto. • Componentes de la suite de monitoreo. • ¿Qué es Nagios? • ¿Qué es Check_mk? • ¿Qué es PNP4Nagios? • ¿Qué es Nagvis? • ¿Cómo se complementan? • ¿Qué se monitorea? • Ventajas de la suite de monitoreo. • Resultados esperados. • Capacitación de configuración y manejo de la suite de monitoreo.

	UNIVERSIDAD DE NARIÑO		
	FORMATO ACTA DE CAPACITACIÓN	REVISION 00	ENERO 2018

Observaciones:

Se entregó el tutorial de instalación, configuración y manejo de la suite de monitoreo y se acordó realizar otra capacitación para aclarar dudas luego de ser revisado el tutorial por parte del personal del área de sistemas.

En constancia y satisfacción firman:

No	Nombre	Cargo	Cedula	Teléfono	Firma
1	Estaban Delgado	Admin. y desarrollador	1085278208	3184637998	
2	Edgar Moreno	Aux. Sistemas	98392182	3007836365	
3	Andrés Benavides	Ing. Telecc	87067551	3207881160	
4	Gustavo Pérez	Jefe Sistemas	8706 1509	3207881161	

CAPACITADORES:

Julian Camilo Portilla Lagos

C.C 1.085.257.155

Henry Cauvia C.

C.C 1'088.973.024

JEFE DE SISTEMAS:

C.C

Anexo T. Carta de satisfacción por realización del trabajo.

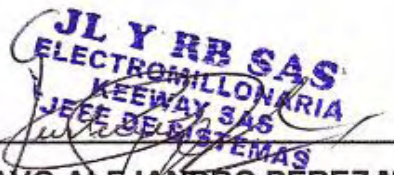
San Juan de Pasto, 06 de abril de 2018

Señores:

Departamento de Ingeniería de Sistemas

Cordial saludo.

La presente es con el fin de dar a conocer nuestro alto grado de satisfacción con el proyecto ANALISIS, DISEÑO E IMPLEMENTACION DE UNA SUITE DE MONITOREO A LA RED DE DATOS DE LA EMPRESA JL Y RB S.A.S – ELECTROMILLONARIA, implementado por los estudiantes HENRY GAVIRIA CERÓN y JULIÁN PORTILLA del Programa de Ingeniera de Sistemas de la Universidad de Nariño. Actualmente, el proyecto está en funcionamiento y lo seguirá estando debido a la gran contribución en la gestión de la red de datos de nuestra empresa.



Ing. GUSTAVO ALEJANDRO PEREZ M.
JEFE DE SISTEMAS JL Y RB S.A.S
ELECTROMILLONARIA.
Dirección: Carrera 24 No. 28-40 Centro
Email: jfsistemas@electromillonaria.co
Celular: 320 788 11 61