Monitorización de la red de comunicaciones de una Administración Pública

Ángel Monerris Aldeguer
Grado de Ingeniería Informática

Manuel Jesús Mendoza Flores

Enero 2020

A mi familia por su apoyo y comprensión
y, en especial, a María,
por disculpar el tiempo que su padre no ha pasado con ella,
y a Mayte, por compartir la vida,
por estar presente en los momentos difíciles
y por los instantes robados.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Monitorización de la red de comunicaciones de una Administración Pública
Nombre del autor:	Ángel Monerris Aldeguer
Nombre del consultor:	Manuel Jesús Mendoza Flores
Fecha de entrega:	01/2020
Área del Trabajo Final:	Administración de redes y sistemas operativos
Titulación:	*Grado de Ingeniería Informática*

Resumen del Trabajo:

Las redes de comunicaciones actuales no son sólo el canal por el que circulan los datos entre distintos artefactos electrónicos que comparten información, son una pieza fundamental que permite la hiperconectividad y la ubicuidad que la sociedad actual demanda. Las redes deben estar bien dimensionadas, ser flexibles y contar con mecanismos que les permitan recuperarse rápidamente de fallos. A medida que las redes de comunicaciones van creciendo y se hacen más complejas, es más difícil anticiparse a las posibles caídas que pudieran producirse o, si es inevitable, localizar rápidamente qué elemento no funciona adecuadamente.

Este TFG trata de resolver el problema descrito mediante el uso de sistemas de monitorización de redes. Un sistema de monitorización de redes consiste en un módulo central y una serie de sondas o agentes que se encargan de monitorizar los equipos conectados a la red. El módulo central analiza los datos recibidos y, mediante diferentes herramientas, es capaz de: lanzar alarmas por email, SMS u otros sistemas cuando hay un problema, de detectar tendencias que indiquen que algún equipo va a fallar, de proporcionar informes sobre el funcionamiento de la red, etc.

El trabajo consta de una parte teórica donde se estudiarán los fundamentos de los sistemas de monitorización y se compararán las características de varios de ellos; y de un caso práctico, donde se seleccionará, desplegará y pondrá en producción un sistema de monitorización en la red de la Agencia de Desarrollo Local de Santa Pola.

Abstract:

Nowadays, computer networks are more than a simple channel for sharing information among different electronic devices, they are the backbone that supports hyperconnectivity and ubiquity today's society demands. Networks must be well sized, flexible and have mechanisms that allow them to quickly recover from failures. As long as computer networks grow and become more complex, it is more difficult to anticipate possible failures that could happen or, if they are impossible to avoid, quickly locate what is not working properly.

This dissertation is about solving the problem described by using network monitoring systems. A network monitoring system consists of a central module that constantly keeps track of the equipment connected to the network by means of sensors or agents. The central module analyzes received data and, through different tools, is able to: send alarms by email, SMS or other channels when there is a trouble, detect trends that indicate that some equipment will be down, provide reports based on the network activities, and so on.

The first part of this work is theoretical, and deals with the study of the monitoring systems fundamentals and characteristics, also compares several of them. The second part is a practical case, where a network monitoring system for the network of the Local Development Agency of Santa Pola will be selected, deployed and finally gone live.

Palabras clave:

Monitorización, redes, scoring, SNMP, Zabbix, CentOS

Índice

1. Introducción 1
1.1 Contexto y justificación del Trabajo 1
1.2 Objetivos del Trabajo 3
1.3 Riesgos del Trabajo 4
1.4 Enfoque y método seguido 4
1.5 Planificación del Trabajo 6
1.6 Breve sumario de productos obtenidos 12
1.7 Breve descripción de los otros capítulos de la memoria 12
2. Estudio teórico de Sistemas de Monitorización 13
2.1 Fundamentos 13
2.1.1 Definición 13
2.1.2 Disponibilidad 16
2.1.3 SNMP 17
2.1.4 OID y MIB 20
2.1.5 WMI 22
2.1.6 Indicadores 24
2.2 Comparativa 25
2.2.1 Clasificación 25
2.2.2 Suites 28
3. Implantación 37
3.1 Selección 37
3.1.1 Definición del entorno a monitorizar 37
3.1.2 Criterios de selección 39
3.1.3 Selección 40
3.2 Estrategia de despliegue 42
3.3 Instalación y parametrización 43
3.3.1 Documentación 43
3.3.2 SNMP 45
3.3.3 Sistema Operativo 46
3.3.4 Instalación de requisitos 47
3.3.5 Zabbix 47
3.3.6 Monitorización SNMP 48
3.3.7 Monitorización mediante agentes 50
3.3.8 Monitorización del entorno de virtualización 52
3.3.9 Mapa de red 54
3.3.10 Alertas 56
3.4 Producción y estabilización 57
4. Cierre 61
4.1 Toma de datos y verificación 61
4.2 Análisis 65
5. Conclusiones 68
6. Glosario 71
7. Bibliografía 75
8. Tablas 79
9. Figuras 80
10. Anexos 85
10.1 Configuración SNMP 85
10.2 Instalación CentOS 7 87

10.3 Instalación requisitos adicionales 90
10.4 Instalación Zabbix..... 91
10.5 Instalación de plantillas 94
10.6 Instalación y configuración de agentes..... 98
10.7 Monitorización VMWare 100

Lista de tablas

Tabla 1. Fases del proyecto 9
Tabla 2. Disponibilidad 17
Tabla 3. Comandos SNMPv1 20
Tabla 4. Ampliación comandos SNMP v2 20
Tabla 5. Sistemas de monitorización centralizados vs distribuidos 25
Tabla 6. Scoring selección herramienta de monitorización 41
Tabla 7. Equipos monitorizados mediante SNMP 48
Tabla 8. Equipos monitorizados mediante agentes 51

Lista de figuras

Figura 1. Medidas de seguridad recogidas en el ENS 2
Figura 2. PMBOK: Ciclo de vida del proyecto 5
Figura 3. Planificación: Diagrama de Gantt 11
Figura 4. Capas del modelo OSI 14
Figura 5. Diagrama funcional de un sistema de monitorización 16
Figura 6. Mensajes SNMP 19
Figura 7. Árbol OID 21
Figura 8. Arquitectura WMI 22
Figura 9. Captura de pantalla Nagios 29
Figura 10. Captura de pantalla OPManager 30
Figura 11. Captura de pantalla OP5 Monitor 31
Figura 12. Captura de pantalla Pandora FMS 32
Figura 13. Captura de pantalla Network Performance Monitoring 33
Figura 14. Captura de pantalla Zabbix 34
Figura 15. Captura de pantalla Azure Monitor 35
Figura 16. Diagrama lógico red ADL 38
Figura 17. Estrategia de despliegue Zabbix 42
Figura 18. Comprobación SNMP mediante snmpwalk 46
Figura 19. Configuración hosts mediante SNMP – Network devices 49
Figura 20. Configuración hosts mediante SNMP – Firewalls 50
Figura 21. Configuración hosts mediante SNMP – UPS 50
Figura 22. Configuración hosts mediante SNMP – Printers 50
Figura 23. Configuración hosts mediante agentes – Linux servers 51
Figura 24. Configuración hosts mediante agentes – Windows servers 52
Figura 25. Virtualización – Descubrimiento de máquinas virtuales 53
Figura 26. Virtualización – Descubrimiento de hipervisores 54
Figura 27. Mapa de red Zabbix – red ADL 55
Figura 28. Alertas – Host sin respuesta ICMP 57
Figura 29. Estabilización – Disponibilidad agente Linux 58
Figura 30. Estabilización – Disponibilidad agente Windows 58
Figura 31. Estabilización – Disponibilidad dispositivos de red 58
Figura 32. Estabilización – Disponibilidad Cisco ASA 59
Figura 33. Estabilización – Utilización de la memoria del servidor Zabbix 59
Figura 34. Estabilización – Utilización de la CPU del servidor Zabbix 59
Figura 35. Estabilización – Utilización del disco del servidor Zabbix 60
Figura 36. Cierre – Sección problemas 62
Figura 37. Cierre – Sección vistazo general 62
Figura 38. Cierre – Tablero impresora 63
Figura 39. Cierre – Tablero servidor Windows 64
Figura 40. Cierre – High memory utilization 65
Figura 41. Cierre – Temperature too high 66
Figura 42. Cierre – Yellow toner level 66
Figura 43. Configuración SNMP - Impresoras HP 85
Figura 44. Configuración SNMP - Impresoras Nashuatec 85
Figura 45. Configuración SNMP - Impresoras Kyocera 86
Figura 46. Configuración SNMP - SAIs HP 86
Figura 47. Configuración CentOS – Máquina virtual 87

Figura 48. Configuración CentOS – Particionado 88
Figura 49. Configuración frontend – Inicio 93
Figura 50. Configuración frontend – Prerrequisitos 93
Figura 51. Configuración frontend – Base de datos 93
Figura 52. Configuración frontend – Conexión con el servidor 93
Figura 53. Configuración frontend – Sumario 93
Figura 54. Configuración frontend – Fichero configuración 93
Figura 55. Configuración frontend – Instalación 93
Figura 56. Instalación de plantillas – Macro SNMP 94
Figura 57. Agente Windows – Presentación 99
Figura 58. Agente Windows – Licencia 99
Figura 59. Agente Windows – Configuración 99
Figura 60. Agente Windows – Componentes 99
Figura 61. Agente Windows – Instalación 99
Figura 62. Monitorización VMWare – Macros 101
Figura 63. Monitorización VMWare – Definición hosts 101

1. Introducción

1.1 Contexto y justificación del Trabajo

La tendencia actual en el mundo de las tecnologías de la comunicación es la hiperconectividad, la ubicuidad y el uso intensivo de datos. Cada vez existen más dispositivos conectados a alguna red, desde cualquier sitio e intercambiando datos masivamente.

Las redes empresariales no son ajenas a estas tendencias y se vuelven cada día más y más complejas. A modo de ejemplo:

- Las redes actuales están jerarquizadas en varias capas (como mínimo una capa de acceso y otra de distribución y/o enrutamiento de tráfico) utilizando dispositivos especializados para gestionar cada una de ellas.
- El tráfico se segmenta, se clasifica y se prioriza para mejorar la seguridad y el rendimiento mediante tecnologías como VLAN (Virtual LAN) o QoS (Quality of Service).
- Se utilizan técnicas de virtualización para consolidar servidores en un mismo hardware, accediendo a dispositivos de almacenamiento en red.
- Existe una clara evolución de las clásicas soluciones on-premise a soluciones on-cloud.

A medida que se van incorporando estas y otras tecnologías a la empresa, aumenta la complejidad de las redes de comunicaciones, que son, al fin y al cabo, las que soportan todo el tráfico de datos. Esta complejidad hace que las redes sean más difíciles de gestionar, incrementándose la probabilidad de fallo. En este escenario la disponibilidad, entendida como la capacidad para acceder a la información cuando se necesita, se vuelve fundamental. Mantener operativa la red el mayor tiempo posible obliga a realizar mantenimientos preventivos regularmente para intentar anticiparse a los problemas y exige actuar rápidamente cuando se produce uno. Sin herramientas adecuadas, las tareas preventivas y reactivas de mantenimiento de las redes se vuelven laboriosas y complejas.

Si bien este planteamiento es adecuado para el mundo empresarial en general, en las administraciones públicas los requerimientos se ven incrementados, ya existe legislación específica sobre el funcionamiento de los sistemas de información que soportan los servicios que se prestan al ciudadano. Por ejemplo, la Ley 39/2015 [1] en el artículo 31.2 establece que los registros electrónicos permitirán la presentación de documentos todos los días del año durante las veinticuatro horas, es decir, si la red falla y el registro general de una administración deja de ser accesible se estarán vulnerando los derechos de los ciudadanos. Otro ejemplo es el Esquema Nacional de Seguridad [2], que "*está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos,*

informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias." (Artículo 1.2), es decir existe legislación específica para garantizar la protección de la información gestionada por los sistemas de proceso de datos de las Administraciones Públicas.

Figura 1. Medidas de seguridad recogidas en el ENS

En este contexto, la Agencia de Desarrollo Local de Santa Pola (ADL) es un Organismo Autónomo Administrativo dependiente del Ayuntamiento de Santa Pola, y por lo tanto Administración Pública. Para la consecución de sus fines dispone de diversos sistemas de información interconectados por una red de comunicaciones que ha ido creciendo a lo largo de los años. Las características básicas de esta red son:

- Red jerárquica y segmentada basada en TCP/IP
- Físicamente existe una sede principal y una delegación con conexión mediante VPN
- El acceso a Internet está protegido mediante Firewall
- Existe una zona DMZ donde se ubican los servidores que proporcionan servicios externos (sedes web, correo electrónico, etc.)
- La red interconecta unos 60 clientes, mayoritariamente PC con sistema operativo Windows y servidores hardware con máquinas Linux y Windows virtualizadas con VMware.

Actualmente, para asegurar el buen funcionamiento de la red y de los sistemas de información en la ADL, se realizan mantenimientos preventivos

regularmente y se actúa reactivamente en caso necesario cuando se produce un incidente. Sin embargo esta gestión presenta varios inconvenientes:

- No está totalmente automatizada, por lo que parte de la misma se realiza manualmente.
- Es imposible verificar todos los puntos susceptibles de fallo.
- Cuando se actúa reactivamente, no se dispone de herramientas que indiquen rápidamente qué elemento está fallando.
- No hay elementos que indiquen tendencias o que anticipen fallos.

Por este motivo, se considera necesario seleccionar e implantar un sistema de monitorización de redes que permita mejorar la detección de problemas, actuar tempranamente, establecer un sistema automático de alertas, etc. En definitiva, garantizar la disponibilidad e integridad de la información que circula por la red de la ADL.

En resumen, en este TFG se partirá de la situación actual de la red actual de la ADL, en la que no existen mecanismos automáticos de detección de fallos. Se compararán sistemas de monitorización de redes y se seleccionará más adecuado. Finalmente se implantará y se pondrá en producción el elegido con el objetivo final de disponer de una herramienta para automatizar la gestión de la red.

1.2 Objetivos del Trabajo

Aunque el objetivo general del proyecto es automatizar la gestión de la red de la ADL, podemos definir los siguientes objetivos específicos:

- Comprender el funcionamiento general de los sistemas de monitorización de redes: en qué se basan, cómo funcionan, qué son capaces de monitorizar.
- Ser capaz de seleccionar un sistema de monitorización que satisfaga las necesidades de la red de la ADL.
- Relacionar los puntos críticos que se deben monitorizar, y definir indicadores de control para cada uno de ellos.
- Desplegar un sistema de monitorización de redes en un entorno real.
- Recopilar datos y tendencias que proporcione el sistema una vez implantado.

Como se ha comentado anteriormente, el alcance del proyecto está circunscrito a la red de la ADL. En la ejecución de este proyecto no está prevista su extensión a otros dispositivos y redes más allá de los de la ADL, si bien es cierto que de las conclusiones que se extraigan del proyecto y dentro de un proceso de mejora continua, en el futuro podría extenderse a otros sistemas (por ejemplo los municipales) y/o ampliar funcionalidades no previstas en este estudio.

Si se cumplen los objetivos, se espera conseguir los siguientes beneficios:

- Disponer de un panel de control general del funcionamiento de la red de la ADL.
- Mejorar la detección temprana de incidentes mediante un sistema de alertas automatizado.
- Conocer cargas y tendencias de la red, con el fin de poder dimensionar adecuadamente los sistemas de información.

1.3 Riesgos del Trabajo

Como todo proyecto, existen riesgos que deben ser tenidos en cuenta con el objetivo de minimizarlos o, si es posible, eliminarlos:

- Establecer objetivos demasiado ambiciosos.
- Incorrecta planificación temporal.
- Incorrecta selección del sistema a implantar.
- Incapacidad para instalar y arrancar el sistema.
- Que los datos obtenidos una vez implantado el sistema no aporten valor.

Un factor de riesgo importante en casi todos los proyectos es la gestión del cambio. En este proyecto este factor no es determinante, ya que la implantación del software no afecta directamente al resto de usuarios de la red y no va a suponer ningún cambio de procedimientos o interfaces para ellos.

Sin embargo, sí que debe tenerse en cuenta como factor limitativo la inexistencia de financiación económica para el desarrollo del proyecto. Este factor restrictivo implica que la solución elegida para su implantación debe ser de fuentes abiertas, o versiones reducidas sin costo. Por otro lado, no podrán adquirirse dispositivos adicionales a los que ya están en funcionamiento en la red de la ADL para el proyecto.

1.4 Enfoque y método seguido

Una de las estrategias para conseguir el objetivo planteado en este proyecto podría ser el desarrollo de un producto ad hoc para la ADL. Teniendo en cuenta la gran variedad de sistemas de monitorización que existen y las prestaciones que ofrecen en general, no parece razonable desarrollar otro producto similar a los que ya existen en el mercado, que no aportaría nada nuevo. En este caso, se considera como mejor opción seleccionar uno de los existentes, parametrizarlo y, si es necesario, realizar algún desarrollo complementario en caso de que el producto adolezca de alguna funcionalidad requerida.

Por lo tanto, una parte de este TFG va a consistir en la implantación de un sistema de información. Esta implantación debe enfocarse desde el punto de vista de la gestión de proyectos, más que desde el ciclo de vida de un desarrollo a medida, que no es el caso.

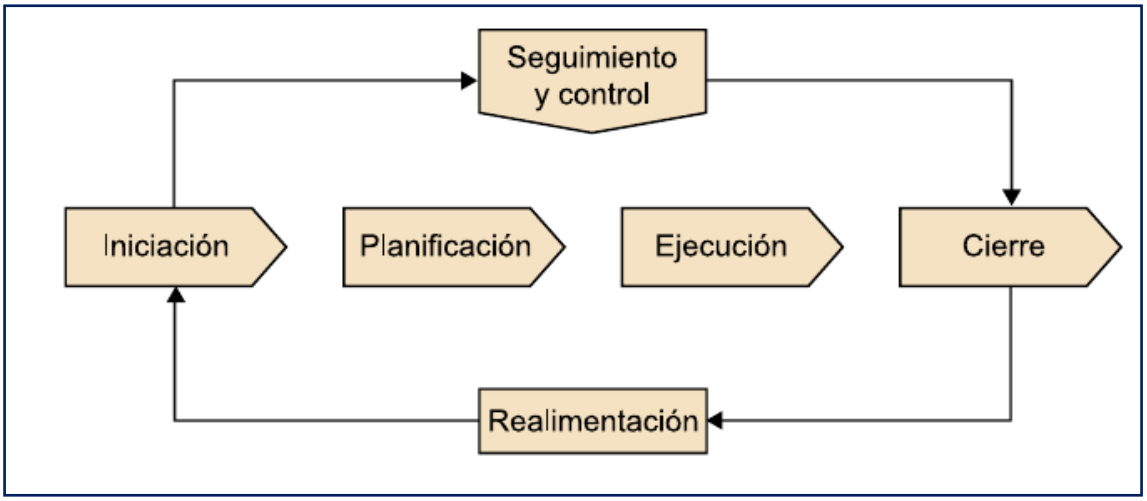


Figura 2. PMBOK: Ciclo de vida del proyecto

En este sentido, PMBOK es un estándar reconocido y utilizado habitualmente para la gestión de proyectos TIC [3]. PMBOK divide un proyecto en cinco grupos de procesos:

- **Iniciación:** Se evalúa un problema o necesidad y se toma la decisión de iniciar un proyecto que solvente el problema o satisfaga la necesidad. Normalmente se elabora un acta de inicio o constitución del proyecto.
- **Planificación:** Se definen objetivos y resultados a obtener y se planifican las actividades que van a ejecutarse.
- **Ejecución:** En esta fase se planifican detalladamente las actividades necesarias para la implantación propiamente dicha y se ejecuta esta implantación. Dentro de esta fase se produce el lanzamiento o puesta en marcha, y la estabilización posterior.
- **Cierre:** Una vez que el sistema está en funcionamiento o el producto está terminado se hace entrega al cliente y se produce la aceptación de éste (si es conforme) y se firma el acta de recepción.
- **Seguimiento y control:** Durante todo el ciclo de vida del proyecto se debe realizar un seguimiento del correcto cumplimiento de plazos, evaluar desviaciones, tomar decisiones ante problemas inesperados, etc. con el fin de conseguir los objetivos planteados.

En la versión 6.0 de PMBOK [4] se definen 49 procesos que es necesario realizar durante la dirección del proyecto y que se agrupan en las fases descritas anteriormente.

El objetivo es utilizar las fases que define PMBOK para la gestión de un proyecto como referencia para la planificación de este TFG. Esto no quiere decir que el trabajo se vaya a dividir en las mismas fases que se establecen en PMBOK, ya que el desarrollo de este trabajo no consiste sólo en la implantación de un sistema de monitorización.

En el apartado siguiente se describe la planificación del trabajo y su relación con las fases de PMBOK.

1.5 Planificación del Trabajo

El proyecto se ha dividido en 5 fases y cada una de ellas se ha subdividido en una serie de tareas. La descripción general de cada una de las fases se describe a continuación:

- **Fase 1 Definición del proyecto:** En esta etapa se realizarán las labores de definición de objetivos, alcance y planificación temporal del proyecto. Corresponde a las fases Iniciación y Planificación de PMBOK.
- **Fase 2 Estudio teórico de los sistemas de monitorización:** Una vez definido el proyecto, se pasará a realizar un estudio teórico de las metodologías utilizadas por los sistemas de monitorización de redes para realizar su cometido y se detectarán y compararán los principales sistemas existentes en el mercado. No tiene correspondencia con PMBOK, es propia de este trabajo y anexa a la implantación propiamente dicha.
- **Fase 3 Implantación:** Se definirán los criterios de selección y se elegirá el sistema más adecuado para la red de la ADL. Una vez seleccionado, se desplegará y se pondrá en producción. Esta fase es la que tiene una mayor duración temporal. Corresponde con la fase Ejecución de PMBOK.
- **Fase 4 Cierre:** En el momento en que el sistema esté operativo y estabilizado, se procederá a la toma de datos que proporcione el sistema, a su estudio y se extraerán conclusiones y propuestas de mejora. Corresponde con la fase Cierre de PMBOK.
- **Fase 5 Conclusiones:** En esta fase se procederá a elaborar las conclusiones definitivas del proyecto, a cerrar la memoria y realizar la memoria y el video final. No tiene correspondencia con PMBOK, ya que es propia de este trabajo.

A continuación se relaciona cada fase y su descomposición en tareas:

Fase 1 Definición del proyecto
Tarea 1.1 Propuesta de proyecto
Duración: 19/09 - 23/09 -> 5 días **Objetivo:** Definir el problema. **Actividades:** Describir el problema y las tecnologías utilizadas para su resolución. Contactar con el consultor para su validación.
Tarea 1.2 Definición – Planificación
Duración: 24/09 - 2/10 -> 9 días **Objetivo:** Confeccionar la planificación detallada del proyecto.

Actividades:

Contextualizar el trabajo.
Definir alcance, objetivos, metodología y riesgos.
Descomposición en fases y tareas.
Planificación temporal.

Fase 2 Estudio teórico de los sistemas de monitorización

Tarea 1.1 Fundamentos

Duración:

3/10 - 13/10 -> 11 días

Objetivo:

Conocer las metodologías utilizadas por los sistemas de monitorización.

Actividades:

Búsqueda de información.
Categorización y clasificación de la información.
Descripción de los protocolos utilizados.
Descripción de los algoritmos utilizados.

Tarea 1.2 Comparativa

Duración:

14/10 - 22/10 -> 9 días

Objetivo:

Comparar las funcionalidades de los principales sistemas de monitorización.

Actividades:

Búsqueda de información.
Categorización y tabulación de la información.
Descripción en las funcionalidades de cada sistema.

Fase 3 Implantación

Tarea 3.1 Selección

Duración:

23/10 - 27/10 -> 5 días

Objetivo:

Seleccionar el sistema de monitorización más adecuado para la red de la ADL.

Actividades:

Definir los criterios de selección.
Descartar los sistemas que no cumplen con los criterios excluyentes.
Ponderar el resto de sistemas.
Seleccionar el sistema más adecuado.

Tarea 3.2 Estrategia de despliegue

Duración:

28/10 - 30/10 -> 3 días

Objetivo:

Planificar el despliegue de la solución seleccionada.

Actividades:

Definir los requisitos previos para el sistema a desplegar.
Definir los sistemas y servicios se va a monitorizar.
Prever si será necesario algún desarrollo ad hoc.
Planificación temporal de la instalación.

Tarea 3.3 Instalación y parametrización

Duración:

31/10 - 17/11 -> 18 días

Objetivo:

Desplegar el sistema de monitorización en la red de la ADL.

Actividades:

Configurar el entorno necesario para el sistema.
Instalación y configuración básica.
Parametrización.
Monitorización de equipos de pruebas.
Incorporación de los posibles desarrollos ad hoc.
Verificación de funcionamiento en conjunto.

Tarea 3.4 Producción y estabilización

Duración:

18/11 - 24/11 -> 7 días

Objetivo:

Lanzamiento del sistema de monitorización.

Actividades:

Despliegue de sondas o agentes en los equipos de producción a monitorizar.
Puesta en producción.
Verificación del funcionamiento y estabilización.

Fase 4 Cierre

Tarea 4.1 Toma de datos y verificaciones

Duración:

25/11 - 1/12 -> 7 días

Objetivo:

Recopilar datos significativos del sistema.

Actividades:

Verificar que el sistema proporciona los datos necesarios para la monitorización.
Recopilar estadísticas, datos de uso y funcionamiento de la red.

Tarea 4.2 Análisis

Duración:

2/12 - 8/12 -> 7 días

Objetivo:

Analizar los datos obtenidos.

Actividades: Evaluar la información recopilada del sistema de monitorización. Identificar posibles mejoras u optimizaciones de la red.

Fase 5 Conclusiones
Tarea 5.1 Conclusiones finales
Duración: 9/12 - 22/12 -> 14 días **Objetivo:** Redacción de las conclusiones finales del proyecto. **Actividades:** Cierre del proyecto. Conclusiones globales. Redacción definitiva de la memoria.
Tarea 5.2 Presentación y video
Duración: 23/12 - 4/1 -> 11 días **Objetivo:** Elaboración del video y la presentación del proyecto. **Actividades:** Guión para la presentación y video. Elaboración de la presentación. Grabación de video. Entrega final.

Tabla 1. Fases del proyecto

Para el control del avance correcto del proyecto se han establecido tres hitos intermedios correspondientes a cada una de las PEC. Está previsto que en cada una de ellas hayan finalizado las siguientes partes del proyecto:

- **PEC 1 - (4/10):** Debe estar finalizado un 10% del total, se entregará la Fase 1 correspondiente a la definición y planificación del proyecto.
- **PEC 2 - (8/11):** Debe estar finalizado entre 40% y 60% del total, se entregará la Fase 2 y parte de la Fase 3 correspondiente al estudio teórico, la selección de la solución y la estrategia del despliegue.
- **PEC 3 - (13/12):** Debe estar finalizado un 90% del total, se entregará el resto de la Fase 3 y la Fase 4, correspondiente a la instalación y puesta en marcha del sistema y al análisis de los datos obtenidos
- **ENTREGA FINAL - (5/1):** Debe estar finalizado un 100% del total, se entregaría la memoria final, presentación y video.

Como se ha comentado anteriormente, este TFG carece de consignación económica, pero se puede hacer una estimación del coste en horas que supondrá el despliegue de la solución de monitorización y que se corresponde principalmente con las fases 3 y 4.

Teniendo en cuenta que el coste en horas del proyecto es de unas 300 y que se van a dedicar 106 días en ejecutarlo totalmente, se calcula que habrá que dedicar unas 3 horas diarias. Si los días planificados para las fases 3 y 4 son 67, el esfuerzo en horas de planificar, ejecutar y cerrar un proyecto de despliegue de una suite de monitorización será de unas 200 horas.

Finalmente se presenta un diagrama de Gantt a modo de resumen gráfico de la planificación expuesta:

Tarea	Inicio	Fin	Duración
1. Definición del proyecto			
1.1 Propuesta de proyecto	19/09	23/09	5
1.2 Definición-planificación	24/09	2/10	9
• PEC1	4/10		
2. Estudio teórico sistemas de monitorización			
2.1 Fundamentos	3/10	13/10	11
2.2 Comparativa	14/10	22/10	9
3. Implantación			
3.1 Selección	23/10	27/10	5
3.2 Estrategia despliegue	28/10	30/10	3
• PEC2	8/11		
3.3 Instalación y param.	31/10	17/11	18
3.4 Producción y estab.	18/11	24/11	7
4. Cierre			
4.1 Toma de datos y verif.	25/11	1/12	7
4.2 Análisis	2/12	8/12	7
• PEC3	13/12		
5 Conclusiones			
5.1 Conclusiones finales	9/12	22/12	14
5.2 Presentación y video	23/12	4/01	11
• ENTREGA FINAL	5/01		

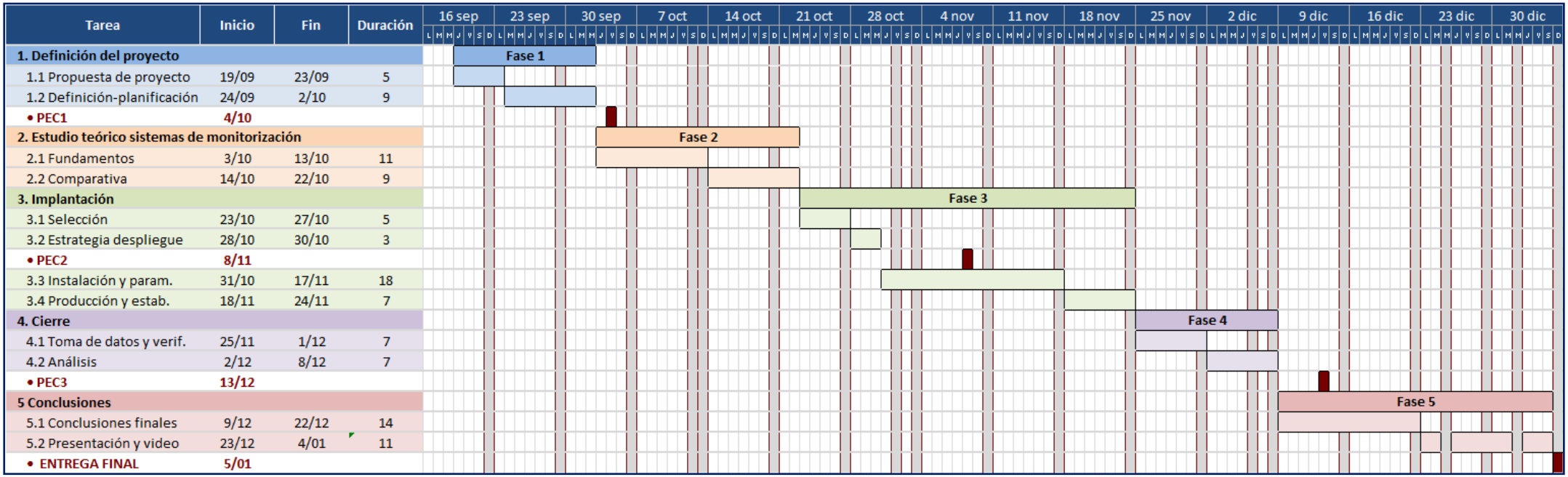


Figura 3. Planificación: Diagrama de Gantt

1.6 Breve sumario de productos obtenidos

Una vez finalizado el proyecto se obtendrán los siguientes productos:

- Memoria final
- Presentación resumen del proyecto
- Video defensa del proyecto
- Máquina virtual con el sistema desplegado

Además, se espera tener un sistema de monitorización operativo y que proporcione información para optimizar el funcionamiento, reducir el riesgo de fallos y minimizar el tiempo de recuperación en la red de la ADL.

1.7 Breve descripción de los otros capítulos de la memoria

Los capítulos del proyecto se han hecho coincidir con la planificación del trabajo. A continuación se describe someramente cada uno de ellos:

- **Capítulo 2:** Se estudiarán los fundamentos, el estado del arte y la tecnología existente relativa a los sistemas de información, con el fin de poder implantar el proyecto con garantías. En la primera parte de este capítulo se hará una revisión de las bases y protocolos que utilizan estos sistemas para su funcionamiento (SNMP, WMI, etc.). En la segunda parte se describirán las características de principales suites de monitorización disponibles en el mercado.
- **Capítulo 3:** Se realizará el despliegue de una suite de monitorización propiamente dicho. En primer lugar se deberá seleccionar una mediante un sistema objetivo, que permita elegir la que mejor se adecúe a las necesidades de la ADL. A continuación se realizará la instalación, puesta en marcha y estabilización de la solución elegida.
- **Capítulo 4:** Una vez que la suite elegida se haya puesto en producción, se deberá proceder el cierre del proyecto. El sistema instalado debe ser capaz de recopilar datos de los sistemas monitorizados. En este capítulo se analizarán y se comprobará si el sistema está correctamente implantado, y se procederá el cierre del proyecto de despliegue.
- **Capítulo 5:** Se describirán las conclusiones finales de todo el TFG, no solo del proyecto de implantación de una suite de monitorización y se confeccionarán la presentación y video final.

2. Estudio teórico de Sistemas de Monitorización

2.1 Fundamentos

2.1.1 Definición

La interconexión de los sistemas de información, tanto en el ámbito interno de las organizaciones como en el externo, es la base de la sociedad actual. En muchas ocasiones se considera a la red de comunicaciones que permite esta interconexión como un simple canal por el que circulan los datos; pero realmente, los elementos que la componen conforman el soporte vital para el resto de sistemas.

Se espera que la red esté operativa veinticuatro horas al día y que sea capaz de gestionar adecuadamente el flujo de datos que debe circular por ella. Sin embargo, garantizar la disponibilidad de las redes es cada día más complicado debido: al aumento de la heterogeneidad de las tecnologías involucradas, a la necesidad de conexión con sistemas externos que se escapan del control de las organizaciones, a la demanda de ubicuidad que incrementa el número de canales de conexión que se deben configurar y controlar (Ethernet, WiFi, 5G,…), al control de acceso a información sensible a través Internet, etc.

Es en este escenario donde se hace necesario contar con herramientas que permitan automatizar la gestión de la red, detectar fallos y puntos críticos y proporcionar estadísticas para poder dimensionarla adecuadamente. A estos sistemas se les conoce, en general, como Sistemas de Monitorización de Redes.

El concepto de monitorización de redes es muy amplio, pero en el ámbito de este trabajo podemos considerar que la monitorización de redes es la disciplina que proporciona las herramientas necesarias para poder gestionar una red con garantías. Ahora bien, ¿en qué aspectos debemos centrarnos para una gestión correcta?

Es bien conocido que el modelo OSI (Open Systems Interconnection) [5] de la ISO (International Organization for Standardization) es un marco conceptual que divide en siete capas las diferentes funciones necesarias para garantizar la comunicación entre dispositivos electrónicos. Cada una de ellas está especializada en realizar una función concreta y diferenciada del resto, de las que desconoce su funcionamiento. Las capas están apiladas y cada una se comunica únicamente con la capa inmediatamente inferior y con la capa inmediatamente superior de la pila. Como la forma y puntos de comunicación entre capas están estandarizados, permite que diferentes fabricantes puedan desarrollar dispositivos o software compatible con los de otros fabricantes, haciendo que este modelo sea abierto. La división de capas también permite mejorar la detección de fallos, ya que es posible verificar el funcionamiento capa a capa. Si la capa n de un sistema se comunica con la capa n de otro sistema quiere decir que esa capa y todas las inferiores funcionan correctamente, siendo necesario buscar el problema en capas superiores.

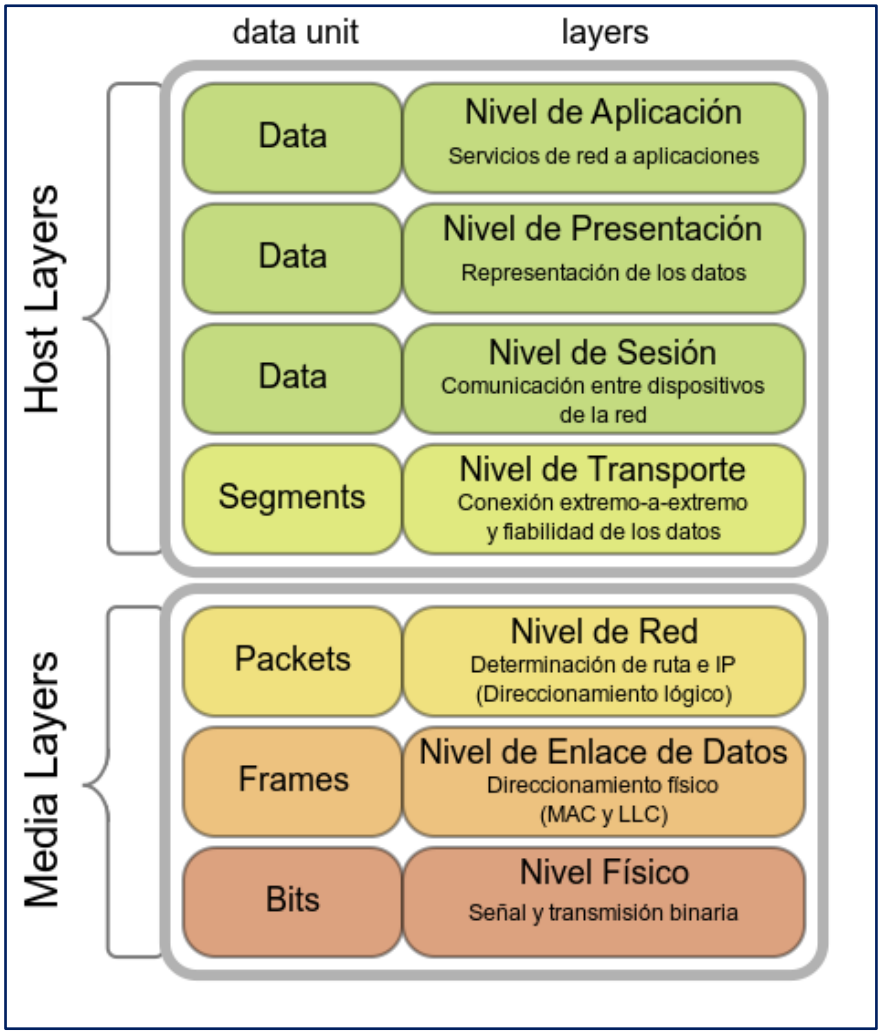


Figura 4. Capas del modelo OSI

El Modelo de Gestión de Red OSI (OSI Network Management Model – OSI NMM) es un subconjunto del marco global OSI explicado anteriormente. OSI NMM define cómo se deben gestionar las entidades que conforman una red para su correcto funcionamiento [6]. Según OSI NMM, las tareas de gestión de la red se dividen en cinco categorías funcionales. De acuerdo a Rao y Mohapatra (2010) [7], estas categorías son:

- **Gestión de fallos (Fault and Problem Management):** Detectar, aislar, notificar y corregir los problemas que surjan en la red con el fin de mantenerla operativa.
- **Gestión de la configuración (Configuration Management):** Monitorizar la configuración de los dispositivos de red para que las versiones y configuraciones de hardware y software de los distintos elementos sean interoperativas y no influyan en la disponibilidad de la red.
- **Gestión del rendimiento (Performance Management):** Medir diversos parámetros de la red con el fin de detectar cuellos de botella y mantener el flujo de datos en un nivel aceptable.

- **Gestión de la seguridad (Security Management):** Controlar el acceso a los recursos, del tal forma que se impida el acceso a datos o dispositivos por parte de usuarios no autorizados.
- **Gestión de inventario/cuentas (Inventory / Account Management):** Disponer de un inventario de usuarios y equipos para conocer los patrones de uso y poder optimizar la utilización de los recursos.

Por lo tanto, cada tarea necesaria para una correcta gestión y mantenimiento de una red estará enmarcada en alguna de estas cinco categorías funcionales. Realizar dichas tareas de forma manual en redes medianas o grandes es inasumible. Aquí es donde los sistemas de monitorización de redes devienen en fundamentales para automatizar estas tareas y dar soporte a los ingenieros de redes.

Como se ha comentado anteriormente, el ámbito que abarca la monitorización es muy amplio y las herramientas utilizadas para este menester también. El abanico de soluciones es tan amplio que puede ir desde un simple script que envíe un ping regularmente a un host para detectar si está activo, a una suite de monitorización con un cuadro de mando en el que se muestra gráficamente la salud de los sistemas y envía alertas a los administradores cuando se detecta un problema.

Este trabajo se va a centrar en el estudio de sistemas completos o suites de monitorización que puedan dar soporte a las cinco categorías de monitorización descritas, no en herramientas individuales que, si bien pueden ser utilizadas en un momento dado como complemento de estos sistemas, no son capaces por sí mismas de proporcionar una solución completa para la gestión de la red.

Generalmente las suites de monitorización están basadas en los siguientes bloques funcionales:

- **Sensores y/o agentes:** Son los encargados de recoger los datos relevantes de los sistemas que se están monitorizando. Pueden ser piezas de software instalables en los equipos o bien protocolos estándar para monitorización como SNMP. Una buena fuente de información son los ficheros log de los sistemas a monitorizar.
- **Sistema de recopilación de datos:** Es el encargado de recibir los datos que envían los sensores y/o agentes y almacenarlos en el sistema de base de datos para su posterior proceso.
- **Base de datos:** Sistema en el que se almacenan los datos, una vez recibido y normalizados por el sistema de recopilación de datos.
- **Inteligencia de negocio:** Es el sistema que se encarga de procesar los datos almacenados en la base de datos y convertirlos en información útil para los administradores de redes. Permite visualiza la información de forma gráfica y tabular, detectar tendencias, emitir alarmas cuando se detecta alguna anomalía, etc.

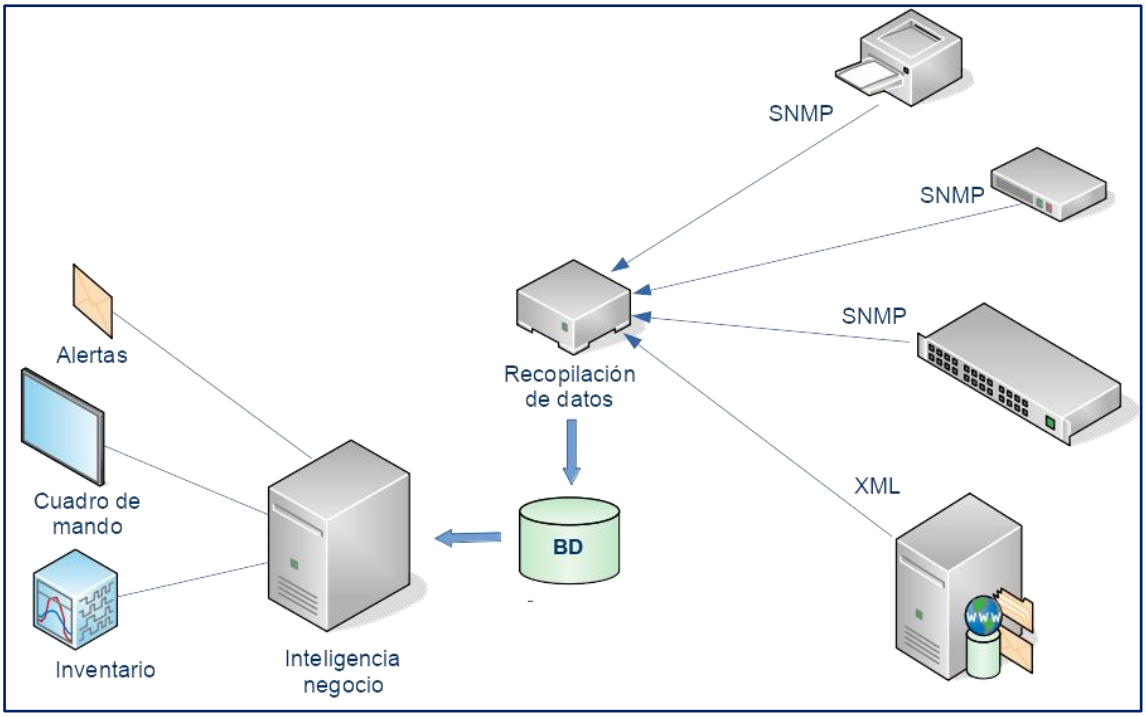


Figura 5. Diagrama funcional de un sistema de monitorización

En la figura 2 se muestra gráficamente el funcionamiento de un sistema de monitorización. En la parte derecha los sistemas a monitorizar envían datos al módulo de recopilación de datos. Estos datos pueden ser recopilados mediante protocolos específicos de monitorización de redes, por ejemplo SNMP en el caso de impresoras, routers o switches, o bien mediante agentes software instalados en un servidor (la comunicación en este último caso se hace utilizando algún lenguaje estándar como XML). El sistema de recopilación de datos normaliza los datos recibidos y los almacena en la base de datos. El módulo de inteligencia de negocio procesa los datos y los convierte en información útil.

2.1.2 Disponibilidad

Uno de los objetivos que se pretende conseguir es que los sistemas de información que se están monitorizando permanezcan operativos la mayor parte del tiempo. Para poder medir este tiempo, se deben introducir varios conceptos relacionados con él [8]:

- **Tiempo medio entre fallos** – Mean Time Between Failures (MTBF): Como su nombre indica es el tiempo medio que transcurre entre dos fallos consecutivos de un sistema.

- **Tiempo medio de reparación** – Mean Time To Repair (MTTR): Es la media del tiempo empleado en reparar un sistema defectuoso. Incluye todo el tiempo desde que el sistema deja de responder hasta que vuelve a estar operativo.

- **Confiabilidad** – Reliability: Indica la capacidad de un sistema para que funcione adecuadamente bajo los parámetros de funcionamiento establecidos. Por ejemplo, la probabilidad de que un servidor web pueda atender en tiempo y forma a las peticiones que le lleguen, siempre que el número de peticiones se mantenga por debajo del máximo para el que se ha diseñado.

- **Disponibilidad** – Availability: Es la probabilidad de que un sistema esté operativo durante un periodo de tiempo. Cuanto mayor sea la confiabilidad mayor será la disponibilidad de un sistema. La disponibilidad se puede calcular de la siguiente forma:

$$\textbf{Disponibilidad} = \frac{\textbf{MTBF}}{(\textbf{MTBF} + \textbf{MTTR})}$$

La disponibilidad se suele expresar como una notación de nueves en porcentaje, de acuerdo a la siguiente tabla [9]:

Disponibilidad	Tiempo de inactividad anual
90%	36,5 días
99%	3,65 días
99,9%	8,76 horas
99,99%	52 minutos
99,999 %	5 minutos
99,9999 %	31 segundos

Tabla 2. Disponibilidad

Los usuarios de sistemas de información esperan que estén operativos cuando los necesitan y que se garantice el poder acceder a ellos sin problemas la mayor parte del tiempo. El concepto de disponibilidad viene a medir cuanto podemos confiar en que un sistema permanecerá operativo y estará cumpliendo su función. Si se quiere garantizar una alta disponibilidad, es necesario prevenir los fallos o errores de los sistemas antes de que se produzcan y, si no es posible, resolverlos en el menor tiempo, es decir aumentar MTBF y reducir MTTR para que la disponibilidad tienda a un 100% (valor teórico que en los sistemas reales es inalcanzable). En este sentido, el uso de sistemas de monitorización debe permitir mejorar la disponibilidad de los sistemas de información.

2.1.3 SNMP

Como se ha comentado anteriormente los sistemas de monitorización de redes trabajan recopilando datos de los sistemas que están monitorizando y generando información útil a partir de estos. Una de las opciones para capturar datos es utilizar sondas o agentes que compartan un protocolo de comunicaciones común con la suite de monitorización, haciendo muy sencilla la captura de datos. Normalmente estos agentes suelen estar disponibles para

los sistemas operativos más comunes: Windows, Linux o UNIX, siendo necesario instalarlos en el sistema a monitorizar. El agente captura los datos de los servicios que se deseen monitorizar y los envía a intervalos regulares al módulo de recopilación de datos.

El problema viene cuando no existen agentes disponibles para el sistema a monitorizar o simplemente no se desea utilizar los agentes que proporciona la suite de monitorización. Supongamos que queremos monitorizar una impresora de red en la que no es posible instalar ningún agente software, en este caso podemos acudir a los protocolos estándar de gestión de red.

En este proyecto nos vamos a basar en el estudio del protocolo Simple Network Management Protocol (SNMP), integrante de la pila TCP/IP. Este protocolo pertenece a la capa de aplicación de la citada pila y proporciona la capacidad de gestionar y monitorizar los dispositivos conectados a la red que lo tengan habilitado.

El estudio de este protocolo se realiza porque forma parte del conjunto de protocolos TCP/IP, que es el estándar de facto en las redes actuales, la gran mayoría de los equipos conectados a una red lo tienen implementado, incluso se puede habilitar en los sistemas operativos más populares en entornos corporativos (Windows, Linux y UNIX) y está soportado por las principales suites de monitorización del mercado.

El protocolo SNMP [10] [11] funciona mediante un modelo agent/manager, en el cual los dispositivos a monitorizar ejecutan un agente (agent) y quedan a la espera de los comandos que reciban del manager (gestor). El gestor no es un ser humano sino una consola de gestión que se comunica con los agentes. SNMP utiliza los puertos UDP 161 y 162 para la comunicación entre agentes y gestores.

Actualmente existen tres versiones de SNMP, que pueden coexistir en un mismo dispositivo:

- **v1:** Especificación original. Aún está implementada en algunos dispositivos pero está desaconsejado su uso ya que dispone de un sistema muy rudimentario de seguridad basado en contraseña sin encriptación, que se denomina *comunidad*. En cada dispositivo se define el nombre de la comunidad que se desea utilizar, siendo el valor por defecto *public*. Todos los mensajes intercambiados entre el agente y el gestor contienen el nombre de la comunidad que se recupera de la configuración de cada dispositivo. Si el nombre de la comunidad del mensaje recibido coincide con el nombre de comunidad configurado en el dispositivo, se considera que la comunicación es legítima, en otro caso es descartada. El valor de la comunidad se transmite en texto plano sin ninguna seguridad a través de la red.
- **v2:** Esta versión permite utilizar UDP, pero también conexiones TCP orientadas a conexión. Además incluye un sistema de autentificación, contraseñas y encriptación más robusto que la versión 1. De esta versión existen tres variantes: v2c (que utiliza el mismo esquema de

autentificación que la v1 basado en comunidades y no el propuesto para la versión 2), v2u y v2*.

- **v3:** Es la última versión de SNMP. Añade requerimientos estrictos de seguridad: autentificación, encriptación y privacidad de la información.

El esquema de general de funcionamiento de SNMP es el siguiente:

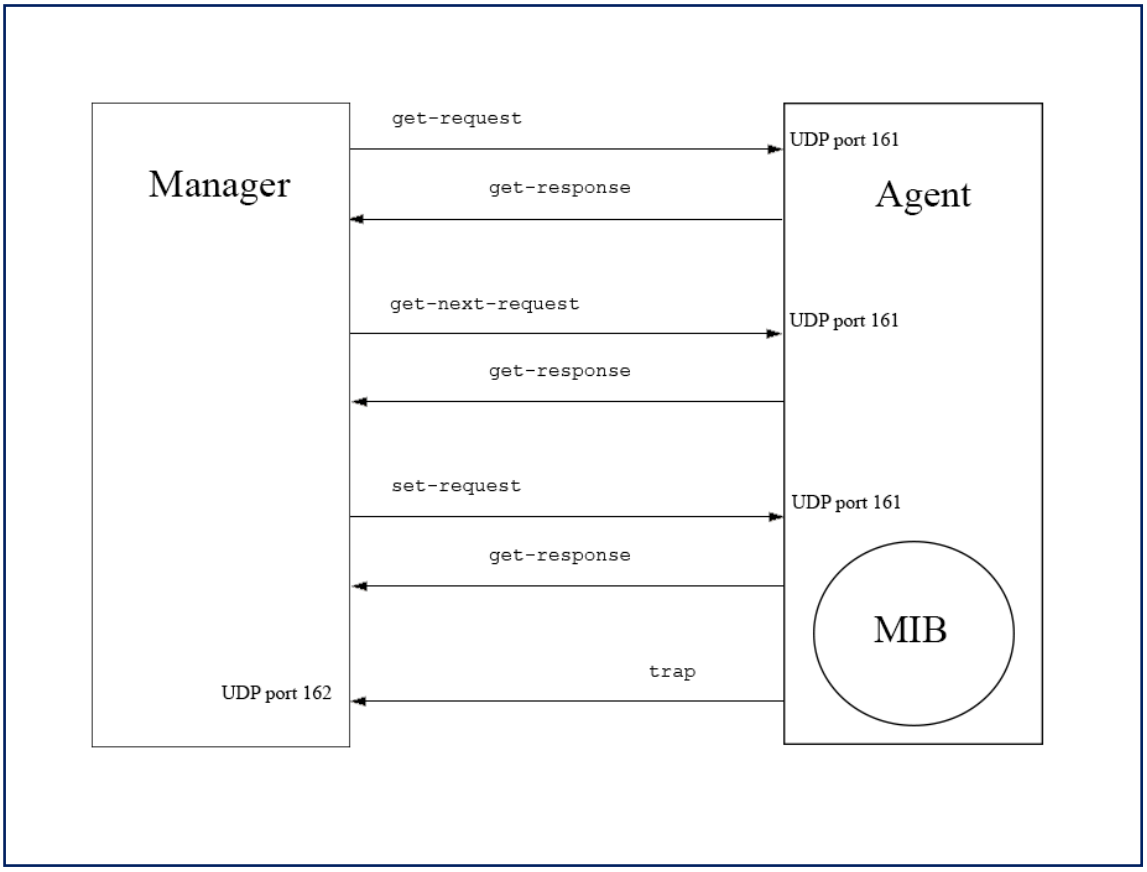


Figura 6. Mensajes SNMP

El protocolo SNMP es muy simple, la comunicación entre los agentes y los gestores se realiza mediante cinco mensajes diferentes. El funcionamiento de SNMP se basa en la lectura o escritura de objetos (variables) en el agente. La lectura de objetos se utilizar para recuperar el valor de un determinado parámetro del dispositivo, la escritura permite cambiar la configuración del mismo. Si el gestor desea monitorizar un determinado parámetro del dispositivo (por ejemplo el tiempo transcurrido desde el último encendido o reinicio), lanza un comando de lectura del objeto correspondiente al puerto UDP 161 del agente. Si lo que desea es cambiar la configuración del dispositivo, el gestor lanza un comando de escritura al puerto UDP 161 con el valor deseado. Además, en los agentes se pueden configurar eventos que disparan lo que se denomina un trap cuando se produce una determinada condición. Cuando se lanza un trap el agente lo comunica al puerto UDP 162 del gestor.

Los cinco comandos del protocolo SNMP son los siguientes:

Comando	Descripción
get-request	Recupera el valor de un objeto en el agente.
get-next-request	Se utiliza para valores almacenados en forma tabla. Recupera el siguiente valor.
set-request	Cambia el valor de un objeto en el agente.
get-response	Responde al manager con el valor solicitado.
trap	Notifica al manager que se ha producido un trap.

Tabla 3. Comandos SNMPv1

Estos cinco mensajes de la definición SNMP original, fueron ampliados a dos más en la versión 2. Los nuevos mensajes son:

Comando	Descripción
getbulk-request	El funcionamiento es similar al comando get-next-request, pero permite recuperar todos los valores en formato tabla de un objeto sin tener que ejecutar varios get-next-request.
inform-request	Es similar a trap con la diferencia de que el gestor envía un acuse de recibo cuando recibe el mensaje.

Tabla 4. Ampliación comandos SNMP v2

2.1.4 OID y MIB

El problema que nos encontramos con el protocolo SNMP es cómo definir de una manera estructurada los múltiples objetos que pueden ser controlados en la infinidad de dispositivos que pueden ser gestionados a través de este protocolo.

Cada objeto al que se puede acceder mediante SNMP en un dispositivo está identificado mediante un OID (Object Identifier) [10]. Los OID están clasificados en forma de árbol jerárquico, de tal forma que cada objeto tiene un valor único. Los OID se representan mediante números separados por puntos, por ejemplo, la variable sysName, que contiene el nombre del dispositivo, está identificada por el OID .1.3.6.1.2.1.1.5

Los OID no son exclusivos de SNMP sino que se utilizan para identificar objetos de manera unívoca y son utilizados por otros protocolos. Existen

organizaciones como la IANA que son las encargadas de gestionar y asignar estos OID.

Para el protocolo SNMP las ramas más importantes son la 1.3.6.1.2.1, que corresponde a los objetos estándares de SNMP y la 1.3.6.1.4.1, que corresponde a objetos específicos de cada vendedor y que no están incluidos entre los objetos estándar SNMP. En la siguiente figura se muestran estas ramas dentro de la estructura OID:

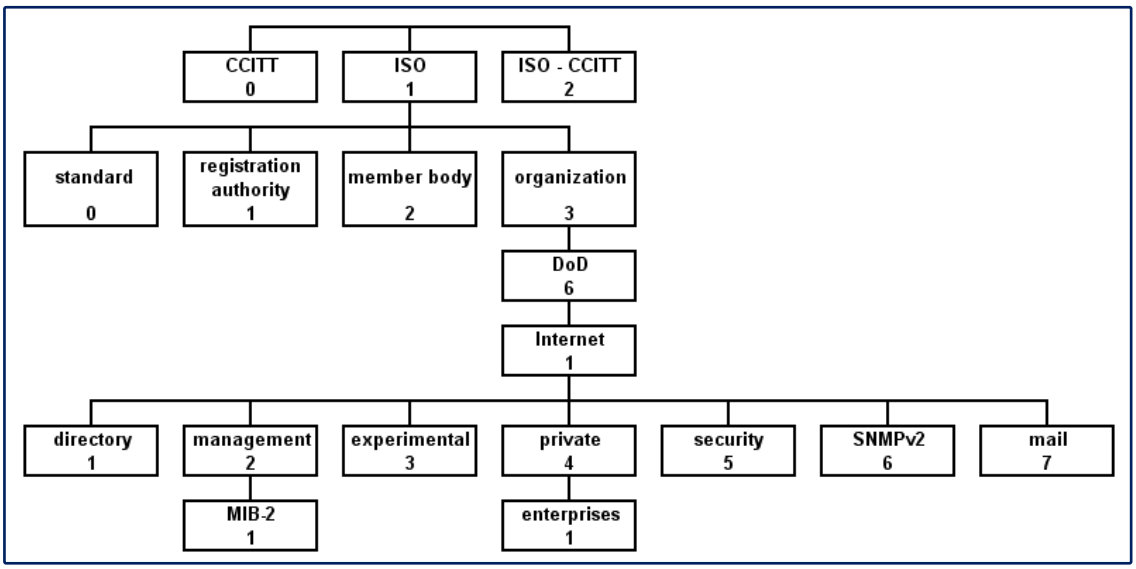


Figura 7. Árbol OID

Siguiendo con el ejemplo anterior, si queremos obtener el nombre del sistema que estamos monitorizando (variable sysName), enviaremos un comando get-request al agente SNMP con el OID .1.3.6.1.2.1.1.5, que dentro del árbol OID corresponde a .iso.org.dod.internet.mgmt.mib-2.system.sysName. El agente responderá con un mensaje get-response con el valor solicitado.

Una vez que tenemos referenciados cada uno de los objetos a los que se puede acceder mediante SNMP, nos queda por conocer las características de esos objetos (nombre, tipo, descripción, etc.). Para esto se utilizan los archivos MIB (Management Information Base) [10]. Un archivo MIB es una base de datos que contiene las descripciones de los objetos que pueden ser accedidos en el dispositivo mediante SNMP. Para generar estas descripciones se utiliza el lenguaje ASN.1. A modo de ejemplo la definición en ASN.1 del objeto sysUpTime es la siguiente:

```
OBJECT: sysUpTime { system 3 }
Syntax: TimeTicks
Definition: The time (in hundredths of a second) since the
network
management portion of the system was last reinitialized.
Access: read-only.
Status: mandatory.
```

Por lo tanto, los MIB nos proporcionan las características de los objetos a los que podemos acceder mediante SNMP y los OID la referencia unívoca de cada uno de ellos.

2.1.5 WMI

Si bien SNMP es un estándar para la gestión de sistemas conectados a una red, en los sistemas Microsoft Windows podemos utilizar WMI como complemento de SNMP. WMI (Windows Management Instrumentation) [12] es parte integral de los sistemas operativos modernos de Microsoft y se considera un estándar para la gestión de equipos Windows. Con WMI se pueden obtener parámetros de gestión y de rendimiento del sistema como: temperatura de la CPU, consumo de memoria, los servicios parados y activos, estadísticas de tráfico de red, etc. WMI es la implementación de Microsoft del estándar WBEM (Web-Based Enterprise Management).

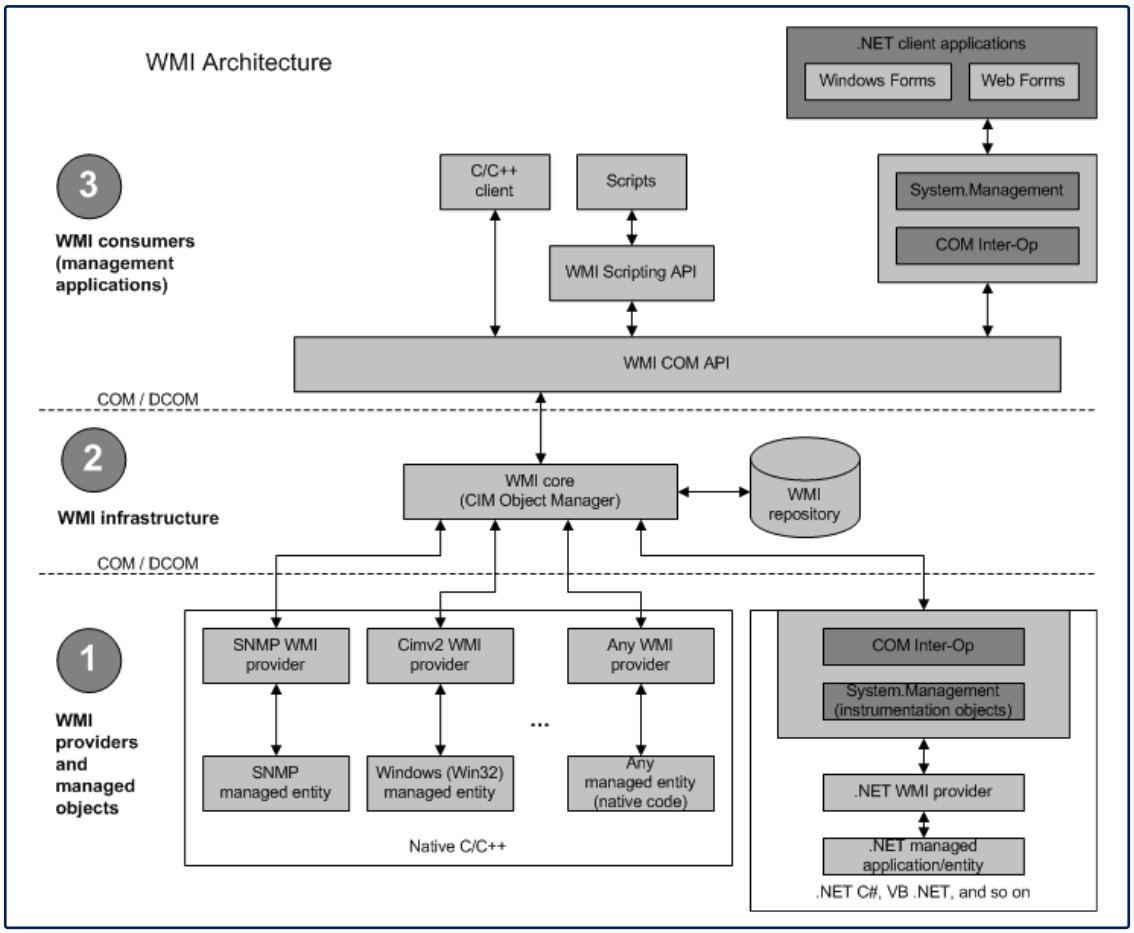


Figura 8. Arquitectura WMI

La arquitectura de WMI está basada en las siguientes capas:

- **Objetos y proveedores:** Un objeto gestionado (managed object) es un componente físico o lógico del sistema (disco duro, proceso, tarjeta de red, etc.) Un proveedor WMI (WMI provider) se encarga de monitorizar uno o más objetos y de gestionar las peticiones WMI dirigidas a los mismos. El proveedor puede tanto recuperar información de los objetos como realizar operaciones en ellos.

- **Infraestructura:** Está compuesto de dos elementos: WMI core y VMI repository. VMI repository contiene las descripciones de los proveedores WMI. WMI core se encarga de arbitrar las relaciones entre los proveedores, el repositorio y las peticiones de las aplicaciones de usuario. Está implementado como un servicio del sistema (winmgmt).

- **Consumidores:** Son aplicaciones de usuario o scripts que hacen llamadas a la API de la infraestructura, con el fin de obtener información o gestionar un objeto definido en el sistema WMI.

WMI define clases para acceder a los objetos administrados. La implementación de cada clase dispone de métodos y propiedades que permiten interactuar con los objetos del sistema. Además, se puede utilizar WMI Query Language (WQL) que permite ejecutar sentencias SQL sobre las clases WMI para recuperar instancias de objetos que cumplen unas determinadas características.

Por ejemplo, la clase Win32_LogicalDisk define el comportamiento de los objetos *disco lógico* de Windows. Con esta clase se puede acceder a las propiedades de las unidades de disco lógico de un sistema Windows y se pueden ejecutar órdenes contra estas unidades mediante los métodos definidos. En [13] se puede consultar la definición de esta clase. Alguna de las propiedades de esta clase son *FreeSpace* que indica el espacio libre o *DeviceID* que devuelve la letra de unidad asignada al disco. Un método de esta clase es *Chkdsk* que ejecuta un chequeo de la unidad.

El uso de esta clase se muestra en el siguiente script VBS, que utiliza una llamada a WMI para conocer el espacio libre de los discos lógicos del sistema. En este ejemplo, la consulta WQL *Select * from Win32_LogicalDisk* recupera todos los objetos *LogicalDisk*. Mediante la lectura de las propiedades *DeviceID* y *FreeSpace* se recuperan la letra de unidad y el espacio disponible.

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" &
"{impersonationLevel=impersonate}!\\" & strComputer &
"\root\cimv2")
Set colDisks = objWMIService.ExecQuery ("Select * from
Win32_LogicalDisk")
For Each objDisk in colDisks
    Wscript.Echo "DeviceID: " & objDisk.DeviceID
    Wscript.Echo "Free Disk Space: " & objDisk.FreeSpace
Next
```

2.1.6 Indicadores

Una vez que hemos definido los fundamentos de los sistemas de monitorización y sabemos qué existen millares de objetos de los que recopilar datos, debemos plantearnos cuáles monitorizar y cuáles no.

En este sentido, un aspecto capital en la monitorización de sistemas es definir claramente qué es lo que se quiere medir y para qué se quiere medir. De nada sirve implantar el mejor sistema de monitorización, si no somos capaces de definir adecuadamente los parámetros que se quieren monitorizar. Se deben elegir los que sean realmente representativos y que aporten información útil del funcionamiento de los sistemas.

En general a cada uno de los parámetros que monitoricemos de la red lo llamaremos indicador. Podemos dividir los indicadores en cualitativos o históricos y cuantitativos o de meta.

Los indicadores históricos registran los valores de un determinado parámetro con el objetivo de seguir la evolución de las magnitudes medidas. Por ejemplo, podríamos registrar cada intervalo de tiempo el tráfico de un puerto de un switch y ver cómo evoluciona para conocer en qué momentos del día hay una mayor densidad tráfico.

Los indicadores de meta tienen fijado un valor de referencia u objetivo. En este caso se realiza una medición continúa de la magnitud con el fin de alcanzar o no sobrepasar un determinado objetivo. Por ejemplo, podemos monitorizar el tiempo de respuesta de las consultas SQL del motor de base de datos y establecer que debe ser menor que un cierto valor. Generalmente este tipo de indicadores llevan aparejados un sistema de alarma que salta cuando no se cumple el objetivo deseado.

Podemos agrupar los indicadores de meta en las siguientes categorías:

- **Disponibilidad:** Nos indican si el sistema o servicio está operativo. Por ejemplo, podemos lanzar un ping a un servidor a intervalos regulares para comprobar si el equipo responde o no. Mediante este tipo de indicadores también se puede controlar si el equipo o sistema está inestable y está continuamente reiniciándose (flapping).
- **Rendimiento:** Nos indican si el sistema o servicio responde en el tiempo máximo que se haya definido. Es posible que el sistema esté operativo, pero que el tiempo de respuesta no sea el adecuado, debido a algún componente con fallos o a un incorrecto dimensionamiento.
- **Seguridad:** Nos indican si el acceso a los datos se está produciendo por usuarios autorizados. Lo que nos interesa conocer en este caso son los intentos de acceso no permitidos. Por ejemplo, se pueden monitorizar los ficheros log de un servidor apache para comprobar si hay intentos de acceso no permitido a una aplicación web y en caso afirmativo bloquear la dirección IP desde la que se realizan estos intentos.

2.2 Comparativa

2.2.1 Clasificación

Para poder elegir una suite de monitorización, es necesario clasificarlas previamente de acuerdo a los principales criterios que las discriminan. Por supuesto, pueden existir otros criterios distintos de los aquí expuestos, pero los que se describen a continuación se consideran los más importantes en el ámbito de este proyecto.

Centralizados vs distribuidos

Tradicionalmente los sistemas de monitorización consistían en un modo central que recibía información de los agentes instalados en los diversos sistemas a monitorizar. Con la tendencia actual que conlleva el uso masivo de sistemas distribuidos y la necesidad de ubicuidad y conexión permanente no siempre es posible ni recomendable el uso de sistemas centralizados de monitorización. Los sistemas distribuidos disponen de varios nodos de control, que permiten un reparto de las tareas de monitorización. Probablemente en instalaciones de tamaño medio con sistemas de información bastante homogéneos y poca dispersión geográfica, la solución más sencilla sea el uso de un sistema centralizado, pero cuando se necesita monitorizar una red dispersa geográficamente con un alto grado de heterogeneidad una solución distribuida sea la mejor solución.

De acuerdo a Somers (1996) [14], la gestión de red centralizada aporta simplicidad en la configuración y mantenimiento del sistema, pero sin embargo el punto de control se convierte en un cuello de botella, con el riesgo de que si falla deja de funcionar todo el sistema. Por el contrario, un sistema descentralizado es más complejo de instalar y mantener, ya que exige que los nodos están coordinados entre sí, pero por el contrario se distribuye mejor la carga de datos y se proporciona una redundancia que evita que la caída de un nodo haga fallar todo el sistema.

	Centralizado	Distribuido
Facilidad de integración del software	X	
Punto único de control y presentación	X	
Fácil aplicación de optimizaciones	X	
Baja sobrecarga de comunicación		X
Respuesta rápida de control		X
Alta escalabilidad		X
Alta resistencia a los fallos del sistema		X

Tabla 5. Sistemas de monitorización centralizados vs distribuidos

Suite estándar vs Best of breed

Otra interesante disyuntiva es si utilizamos una solución genérica estándar o por el contrario necesitamos soluciones de nicho para problemáticas específicas (Best of breed) [15].

Las suites de monitorización típicas proporcionan una solución llave en mano integrada que intenta cubrir la mayoría de las necesidades que surgen en el ámbito de la monitorización, pero por supuesto no pueden cubrir todas las casuísticas, ni entrar en profundidad en las especificidades de algunos sistemas. Al estar desarrolladas por un único fabricante, existe una alta integración entre sus componentes, tanto a nivel funcional como de presentación de la información.

Por el contrario, las soluciones de nicho están desarrolladas para monitorizar un sistema concreto pero necesitan integrarse con otras herramientas para proporcionar un sistema completo. Esto puede ser un problema, ya que integrar soluciones de distintos fabricantes no suele ser sencillo y en algunos casos imposible.

Deberemos sopesar, en base a nuestra red, si merece la pena implantar una suite estándar con el riesgo de no poder monitorizar en profundidad algún sistema, o bien adquirir varias soluciones de nicho y realizar su integración. La decisión dependerá de las necesidades de monitorización de dispositivos específicos que tengamos. Una alternativa, puede ser implantar una suite estándar que permita ampliar sus funcionalidades mediante un sistema de plugins o similar y desarrollar los módulos que proporcionen las funcionalidades de las que carezca el sistema y que sean necesarias.

On-premise vs On-cloud

La tendencia actual del Mercado es ir migrando hacia soluciones on-cloud, de hecho cada vez es más habitual encontrar oferta de soluciones en la nube de cualquier tipo. Hasta hace relativamente poco tiempo era impensable plantear que los proveedores ofertaran soluciones técnicas, como las de monitorización, on-cloud, pero hoy en día es una alternativa seria a valorar.

Por supuesto, las soluciones tradicionales on-premise siguen siendo válidas y se debe evaluar qué enfoque se ajusta mejor a nuestras necesidades. Las soluciones on-premise necesitan de una infraestructura en nuestras instalaciones para poderse instalar, consumen recursos y normalmente son mantenidas por el personal propio del servicio de sistemas de información. Las soluciones en la nube suelen funcionar como SaaS (Software as a Service) en el que se paga por uso, no necesitan instalación en las oficinas del cliente, el proveedor se encarga de que el software esté siempre actualizado, pero por el contrario se depende de un proveedor externo permanentemente.

Independientemente de si decidimos seleccionar una solución on-premise u on-cloud, debemos tener en cuenta también si nuestros sistemas están o van a

estar en un futuro próximo en la nube, en cualquier de los diferentes modelos que existen: SaaS, IaaS (Infrastructure as a Service), PaaS (Platform as a Service) o FaaS (Function as a Service). De nada sirve implantar una solución de monitorización on-premise si en breve vamos a alquilar equipos en la nube y mover allí nuestros sistemas de información. En este caso contrataremos un SLA (Service Level Agreement) en la que el proveedor se compromete a mantener la operatividad de los sistemas con sus propios medios.

Licencias

Un último aspecto a tener en cuenta en el momento de valorar los distintos sistemas de monitorización es su sistema de licenciamiento y, en su caso, el coste de la correspondiente licencia.

Normalmente la soluciones on-cloud tienen un pago por uso, con diferentes planes según la complejidad y número de sistemas a monitorizar. En este caso no se paga el precio inicial de una licencia, sino una cuota periódica durante el tiempo que se esté utilizando la solución.

Para las soluciones instalables en el cliente (on-premise) existe una más amplia variedad de licenciamientos. Podemos elegir desde el software propietario comercial con pago por el uso del producto (que puede incluir una suscripción periódica que de derecho a obtener todas las nuevas versiones sin coste adicional) hasta la solución de software libre que podremos descargar e instalar en nuestros sistemas sin limitaciones.

Estas no son las únicas opciones para las soluciones on-premise, ya que existen variaciones, mezcla de varios licenciamientos. Por ejemplo, están disponibles soluciones de software comercial gratuitas para entornos pequeños y con un número de sensores limitado (si se necesitan más sensores será necesario pagar por el producto completo), o soluciones con licencia dual en la que el núcleo y las funcionalidades básicas de la aplicación son software libre y las funcionalidades extendidas son versiones comerciales de pago.

En cualquier caso, será necesario tener claro qué tipo de licenciamiento se está buscando y cuál es el coste total del proyecto (no sólo de las licencias) que nos podemos permitir, ya que este será un elemento clave en la selección final de la solución elegida.

Además del licenciamiento del software, será necesario tener en cuenta la contratación de soporte, consultoría, instalación de software o adaptación que fueran necesarios y que pueden ir incluidos o no en los paquetes que ofrezca el fabricante.

2.2.2 Suites

Una vez que se han desarrollado los fundamentos de los sistemas de monitorización y los principales criterios de clasificación, vamos a proceder a estudiar los principales sistemas que ofrece el mercado. La cantidad de soluciones para monitorizar redes es amplísima. Es imposible realizar un estudio exhaustivo de todas ellas en este proyecto por las limitaciones de tiempo existentes, por lo que necesariamente hay que seleccionar algunas de ellas para la comparativa.

La selección de unas u otras no es sencilla. En general, se han buscado comparativas de este tipo de soluciones para detectar cuales de ellas son las que más frecuentemente aparecen en las búsquedas, por ejemplo:

- "26 Best Network Monitoring Tools and Software of 2019" en https://www.comparitech.com/net-admin/network-monitoring-tools
- "10 Best Network Monitoring Tools & Software of 2019", en https://www.pcwdld.com/best-network-monitoring-tools-and-software
- "Las 10 mejores herramientas de monitoreo de redes del 2017" en https://apen.es/2017/03/10/las-10-mejores-herramientas-de-monitoreo-de-redes-del-2017/
- "Los 7 Mejores softwares de Monitorización de Redes y Servidores de 2019"https://newesc.com/los-7-mejores-softwares-de-monitorizacion-de-redes-y-servidores-de-2019/
- "Herramientas para la Monitorización de redes de 2018", https://www.axarnet.es/blog/herramientas-monitorizacion-redes/

Las suites más representativas de las que aparecen en las comparativas son: Nagios XI, OPManager, OP5 Monitor, Pandora FMS, Solarwinds Network Performance Monitor y Zabbix. En general, estas comparativas están enfocadas a soluciones on-premise (aunque algunas como Zabbix también tienen versión on-cloud), por lo que se considera conveniente añadir a la comparativa alguna solución totalmente on-cloud como Microsoft Azure Monitor, para tener una visión más amplia.

Todos los fabricantes seleccionados se encuentran en la lista de proveedores más representativos de herramientas de monitorización IT elaborado por Prasad (2018) [16] para la consultora Gartner.

Nagios (https://www.nagios.org**)**

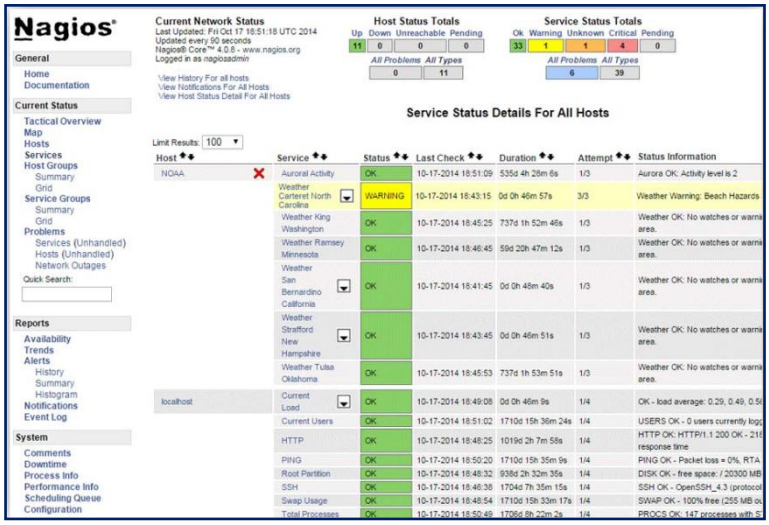


Figura 9. Captura de pantalla Nagios

Fabricante: Nagios Enterprises
Licenciamiento: Open Source / Comercial
Tipo: On-premise
Descripción: La base de Nagios es Nagios Core, que se distribuye con licencia GNU, por lo que puede ser descargado e instalado libremente. Sobre esta base se ha desarrollado Nagios XI, que se distribuye con licencia comercial y complementa las características básicas de Core. Nagios XI, a su vez se puede adquirir en dos versiones: Standar y Enterprise.
Requisitos mínimos (para Nagios XI): [17]

- Disco duro: 20 GB
- Memoria: 2 GB
- CPU: Dual core, 2.4 GHz
- Sistemas operativos: CentOS o Redhat Enterprise Linux (RHEL), Ubuntu or Debian
- Base de datos: MySQL/MariaDB, más PostgresQL para versiones inferiores a XI 5.

Principales funcionalidades versión Core: [18]

- Monitorización: Servidores, elementos de red, aplicaciones y servicios.
- Alertas: Email, móvil y otros (mediante plugins)
- Autodescubrimiento de la red: Mediante plugins
- Informes: Básicos
- Mapa de red: Básico
- Plugins: +4000 disponibles, pudiéndose desarrollar específicos si fuera necesario.
- Mobile app: Disponible
- Monitorización de servicios on-cloud: Amazon cloud (AWS, EC2, S3)

Principales funcionalidades versión XI Enterprise: [18]

- Monitorización: Igual que Core.
- Alertas: Las de Core más RSS, notificaciones por usuario, etc.
- Autodescubrimiento de la red: Automático

- Informes: Avanzados, SLA, rendimiento, personalizados, etc.
- Mapa de red: Avanzado, integración con Google Maps y Navgis, etc.
- Plugins: Igual que Core
- Mobile app: Igual que Core
- Monitorización de servicios on-cloud: Igual que Core

OPManager (https://www.manageengine.com/es/network-monitoring**)**

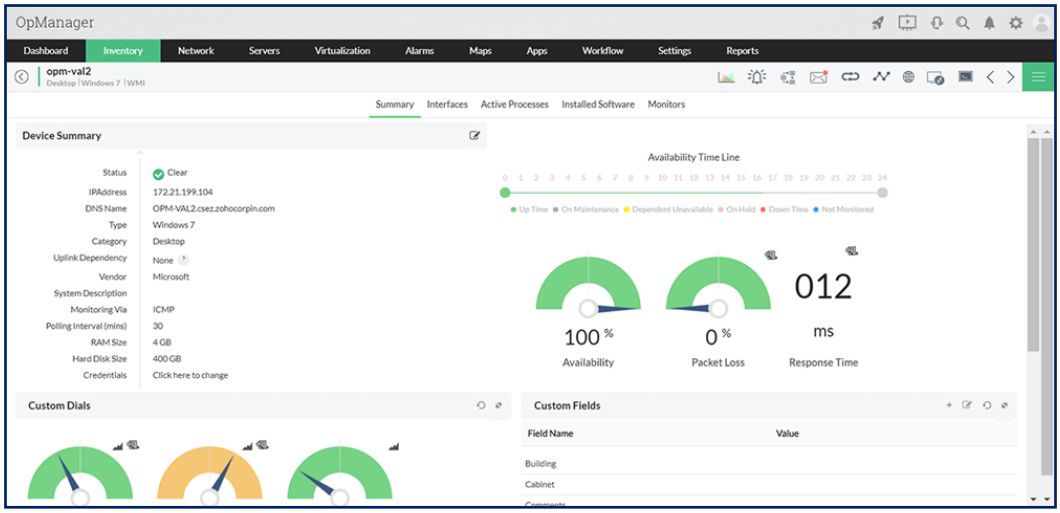


Figura 10. Captura de pantalla OPManager

Fabricante: Zoho Corporation
Licenciamiento: Comercial
Tipo: On-premise
Requisitos mínimos: [19]

- Disco duro: 20 GB
- Memoria: 4 GB
- CPU: Intel Xeon 2.0 Ghz 4 cores/ 4 threads
- Sistemas operativos: Windows Server 2008 o superior, Ubuntu, SUSE, Red Hat Enterprise Linux, Fedora o Mandriva
- Base de datos: Microsoft SQL o PostgresQL.

Descripción: OPManager se puede adquirir en tres versiones: Standard, Professional y Enterprise. Además se proporciona una versión gratuita (Free edition) que sólo permite monitorizar tres dispositivos.
Principales funcionalidades versión Standard: [20]

- Monitorización: Dispositivos SNMP, sistemas Windows mediante WMI, procesos, análisis de syslog, y eventlog para Windows.
- Alertas: Email, móvil y otros.
- Autodescubrimiento de la red: Automático.
- Mapa de red: Mapa de negocio.
- Mobile app: Disponible
- Monitorización de servicios on-cloud: AWS, Azure, Office 365, OpenStack

Principales funcionalidades versión Enterprise: [20]

- Monitorización: Las de la versión Standard más la posibilidad de monitorizar hipervisores (VMWare, Hyper-V, Xen), Active Directory, Exchange Server, Microsoft SQL y sensores hardware, entre otros.
- Alertas: Igual que la versión Standard.
- Autodescubrimiento de la red: Las de la versión Standard más descubrimiento planificado y capa 2, entre otros.
- Mapa de red: Los de la versión Standard más integración con GoogleMaps, 3D Datacenter, etc.
- Mobile app: Igual que la versión Standard.
- Monitorización de servicios on-cloud: Igual que la versión Standard.

OP5 Monitor (https://www.op5.com/op5-monitor)

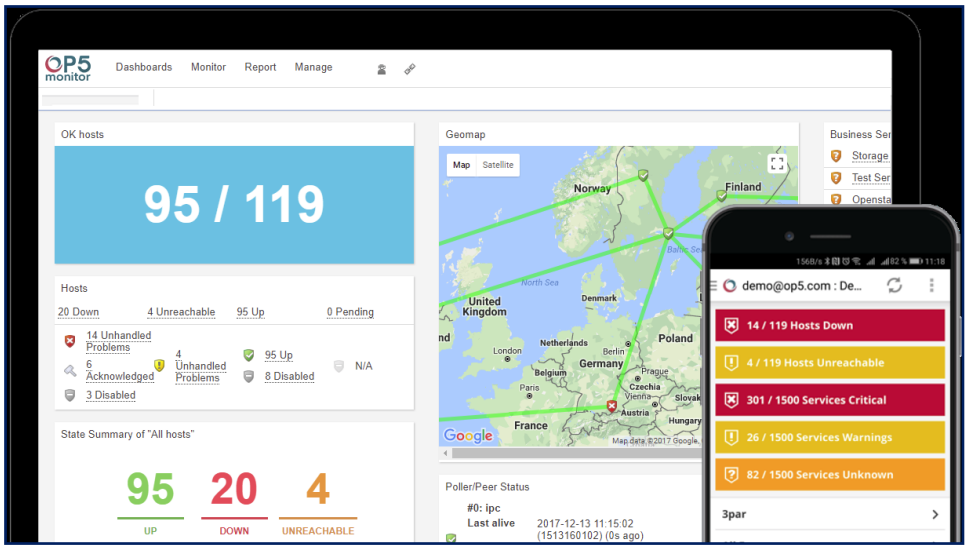


Figura 11. Captura de pantalla OP5 Monitor

Fabricante: OP5 AB
Licenciamiento: Comercial
Tipo: On-premise / Cloud
Requisitos mínimos: [21]

- Disco duro: 500 GB
- Memoria: 8 GB
- CPU: Xeon E3-1220v3
- Sistemas operativos: CentOS o Redhat Enterprise Linux (RHEL)
- Base de datos: MySQL/MariaDB.

Descripción: OP5 Monitor está basado en Nagios, complementado con desarrollos propios de OP5 AB. Además de las versiones de pago, existe una versión llamada OP5 Monitor Free 20, reducida y gratuita, dirigida a pequeñas empresas.

Principales funcionalidades: [22]

- Monitorización: Cualquier dispositivo con SNMP habilitado y recursos y servicios de servidores.
- Alertas: Email, móvil y otros.

- Autodescubrimiento de la red: Mediante un microservicio.
- Informes: Alertas, disponibilidad, SLA, rendimiento, etc. Configurables y exportables a PDF o CSV.
- Mapa de red: Mapas interactivos y geomapas.
- Mobile app: Disponible
- Monitorización de servicios on-cloud: No disponible

Pandora FMS (https://pandorafms.com)

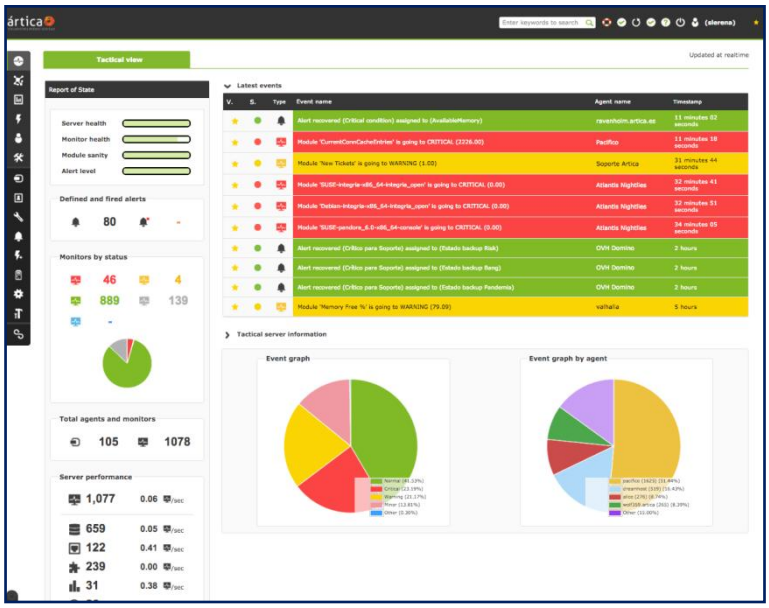


Figura 12. Captura de pantalla Pandora FMS

Fabricante: Ártica ST
Licenciamiento: Open Source / Comercial
Tipo: On-premise
Requisitos mínimos: [23]

- Disco duro: 20 GB
- Memoria: 4 GB
- CPU: 1 núcleo a 2 GHz
- Sistemas operativos: Windows Server 2003 o superior, Ubuntu 11 o superior, SUSE 11.X o superior, Red Hat Enterprise Linux 7.X, CentOS 7.X, SLES 11 SP1 o superior, Debian 5 o superior.
- Base de datos: MySQL/MariaDB, o Percona XTraDB.

Descripción: Pandora FMS es una suite de monitorización desarrollada por Artica ST que ofrece una versión open source con funcionalidades limitadas y versiones comerciales con funcionalidades extendidas y soporte técnico. Existen cuatro versiones comerciales: Trial (versión de prueba de 30 días), NMS, Enterprise y Corporate.
Principales funcionalidades de la versión Community (open source): [24]

- Monitorización: Dispositivos con SNMP habilitado, servidores Windows, HP-UX, Solaris, BSD, AIX y Linux y dispositivos Android y sistemas embebidos.

- Alertas: Email y SMS
- Autodescubrimiento de la red: No disponible.
- Informes: Básico
- Mapa de red: Básico
- Mobile app: Disponible
- Monitorización de servicios on-cloud: No disponible

Principales funcionalidades de la versión Enterprise: [24]

- Monitorización: Las de la versión Community más servidores de virtualización (VMWare, RHEV, XenServer, Hyper-V), servidores Oracle, Informix, SyBase, DB2, Weblogic, Jboss, Exchange, Citrix, WebSphere, etc.
- Alertas:
- Autodescubrimiento de la red: Sí y gestión descentralizada de agentes.
- Informes: Avanzados, cuadro de mando y niveles SLA
- Mapa de red: Mapas navegables dinámicos de red modificables por el usuario
- Mobile app: Igual que la versión Community
- Monitorización de servicios on-cloud: Amazon EC2

Solarwinds Network Performance Monitor

(https://www.solarwinds.com/es/network-performance-monitor**)**

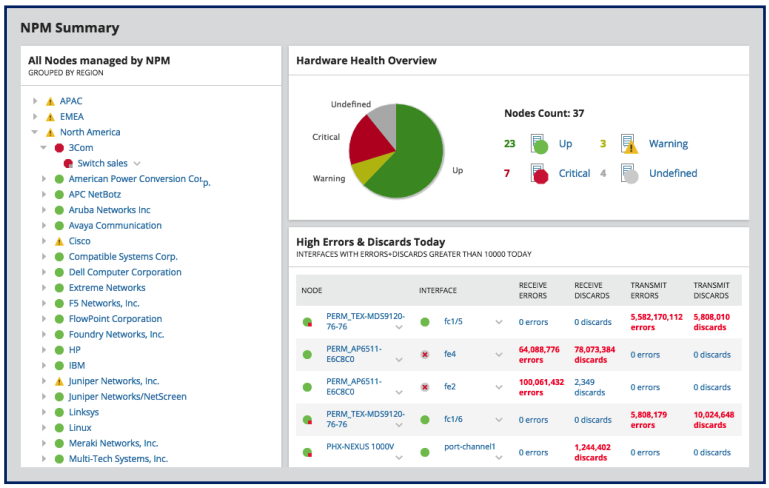


Figura 13. Captura de pantalla Network Performance Monitoring

Fabricante: SolarWinds Worldwide, LLC.
Licenciamiento: Comercial
Tipo: On-premise
Requisitos mínimos: [25]

- Disco duro: 10 GB
- Memoria: 6 GB
- CPU: Quad core processor
- Sistemas operativos: Windows Server 2016 o superior
- Base de datos: SQL Server 2014 o superior.

Descripción: Network Performance Monitor es una suite de monitorización comercial que funciona sobre servidores Windows. Dispone de una versión de prueba de 30 días. El coste de la licencia depende de los elementos a monitorizar, desde la versión SL100 (máximo 100 elementos) hasta la versión SLX con ilimitados elementos.
Principales funcionalidades: [25]

- Monitorización: Servidores, dispositivos de red, dispositivos de red avanzados (ASA, switches Nexus, …)
- Alertas: Alertas automáticas basadas en umbrales de pico y de niveles medios.
- Autodescubrimiento de la red: descubrimiento dinámico y mapeado.
- Informes: Plantillas de informes predefinidos y posibilidad de generar informes personalizados.
- Mapa de red: Mapas inteligentes
- Mobile app: No disponible.
- Monitorización de servicios on-cloud: Disponible.

Zabbix (https://www.zabbix.com)

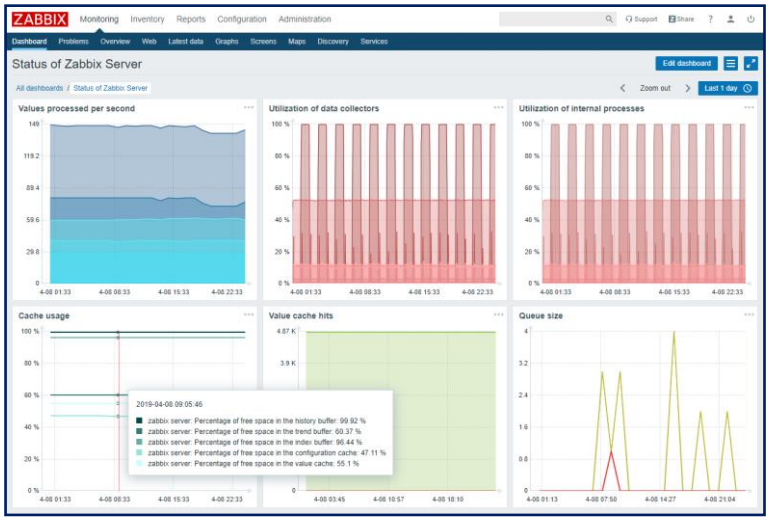


Figura 14. Captura de pantalla Zabbix

Fabricante: Zabbix LLC.
Licenciamiento: Open Source
Tipo: On-premise - Cloud
Requisitos mínimos: [26]

- Disco duro: 256 MB
- Memoria: 128 MB GB
- CPU: --
- Sistemas operativos: Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, HP-UX, Mac OS X y Solaris
- Base de datos: MySQL/MariaDB, Oracle, PostgreSQL, TimescaleDB, IBM DB2 y SQLite

Descripción: Zabbix es una solución open source, a diferencia de otras soluciones, sólo existe una única licencia sin limitaciones. Adicionalmente, se puede contratar servicios de consultoría, integración, implantación, etc.
Principales funcionalidades: [27]

- Monitorización: Servidores, dispositivos de red, servicios, aplicaciones, etc.
- Alertas: Mediante e-mail, SMS, Jabber, Ez texting, etc.
- Autodescubrimiento de la red: Descubrimiento dinámico, permite autoregistro de agentes en el servidor. Automáticamente crea ítems, disparadores y gráficos por cada dispositivo descubierto.
- Informes: Informes predefinidos y posibilidad de generar personalizados.
- Mapa de red: Sí, con la posibilidad de crear mapas públicos o privados según perfiles de usuario.
- Mobile app: Disponible
- Monitorización de servicios on-cloud: AWS, Google Cloud, Microsoft Azure, etc.

Azure Monitor (https://azure.microsoft.com/en-us/services/monitor)

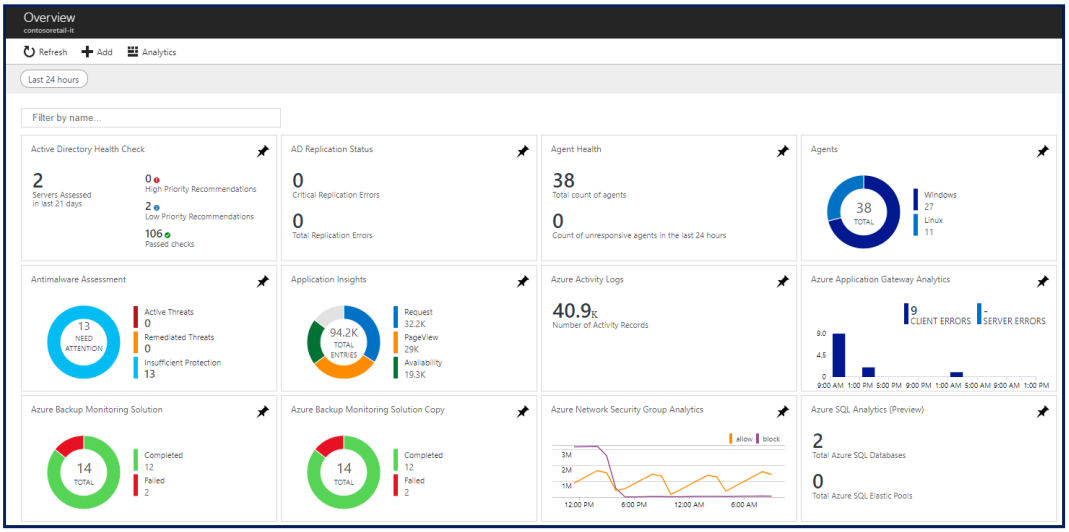


Figura 15. Captura de pantalla Azure Monitor

Fabricante: Microsoft
Licenciamiento: Comercial
Tipo: Cloud
Descripción: Azure Monitor es la solución en la nube de Microsoft para monitorizar tanto sistemas alojados on-cloud como locales.
Principales funcionalidades: [28]

- Monitorización: Aplicaciones, máquinas virtuales (Linux y Windows), dispositivos de red, etc. ubicados en la nube y locales.
- Alertas: Permite definir reglas basadas en métricas de diversas fuentes para enviar notificaciones. Las alertas se pueden integrar con otras herramientas de gestión de servicios IT (ITSM).
- Informes: Disponibles.

- Mapa de red: Disponible.
- Mobile app: --
- Monitorización de servicios on-cloud: Microsoft Azure.

En resumen, en este apartado se ha seleccionado una muestra de suites de monitorización, con el objetivo de tener una muestra representativa del mercado. Se han descrito soluciones open source, comerciales y mixtas, on-premise y on-cloud, funcionando sobre sistemas Linux y Windows.

3. Implantación

En esta fase se va a proceder a implantar una suite de monitorización en la red de la Agencia de Desarrollo Local, una vez definidos los fundamentos de estos sistemas y comparado un conjunto de suites representativas del mercado actual.

3.1 Selección

En primer lugar se deberá seleccionar una de las suites que se han descrito en la fase anterior, para lo cual debemos describir los sistemas de información a monitorizar, los criterios de selección y valorar cual es la más adecuada para las necesidades de la ADL.

3.1.1 Definición del entorno a monitorizar

La Agencia de Desarrollo Local desarrolla su actividad en el municipio de Santa Pola y dispone de tres sedes (ADL principal, ADL formación y Gran Alacant) ubicadas geográficamente en dicho municipio. En la figura 7 se muestra un diagrama lógico de la red de la ADL. Este diagrama se ha simplificado con el fin de preservar la privacidad de la configuración de los sistemas de información de la entidad.

La conexión entre ADL principal y Gran Alacant se realiza aprovechando la infraestructura municipal con un transporte capa 2, mientras que la conexión entre ADL principal y ADL formación se realiza mediante una VPN a través de Internet.

En las sedes más grandes (ADL principal y ADL formación) el tráfico está segmentado en varias VLAN. En cada una de ellas existe un firewall para controlar el acceso a Internet y en la ADL principal este firewall controla una zona DMZ donde se encuentran los servicios online que presta la ADL.

En estas dos sedes disponen de sendos CPD donde están ubicados los equipos de red y servidores. Tres de estos servidores (CPU0255, CPU0276 y CPU0228) funcionan con el hipervisor VMWare donde se virtualizan máquinas tanto Windows como Linux. Algunos de los servicios que proporcionan estas máquinas son: active directory, compartición de ficheros e impresoras, bases de datos, email, http, etc.

Los otros dos servidores CPU0215 y CPU0213 se utilizan como servidores de backup replicados.

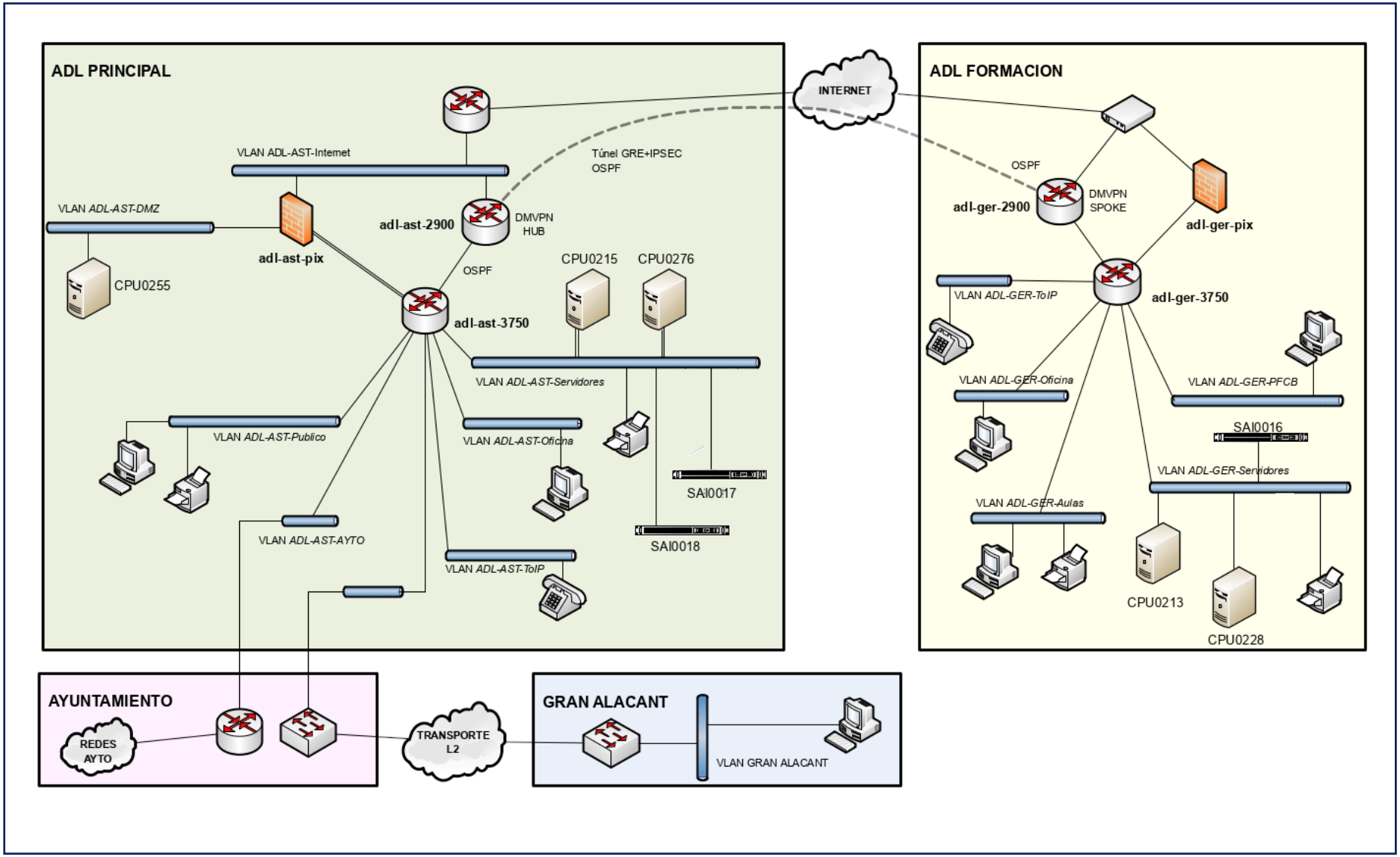


Figura 16. Diagrama lógico red ADL

En la misma red coexiste telefonía IP, aunque el Call Manager no se encuentra ubicado físicamente en la red de la ADL, sino en el CPD municipal.

Por último, cabe destacar que existen tres SAI conectados a la red con soporte para protocolo SNMP, varias impresoras también conectadas a la red y diversos equipos de cliente con sistema operativo Windows.

En resumen, los sistemas de información que se quieren monitorizar son los siguientes:

- 3 Servidores hardware con VMWare
- 2 Servidores hardware de backup (Linux)
- Máquinas virtualizadas Windows y Linux
- Servicios de compartición de ficheros e impresoras, base de datos, email, http, etc.
- 2 Firewalls Cisco
- Equipamiento de red Cisco (switches capa 2 y 3 y routers)
- 3 SAI HP
- 4 Impresoras de red

3.1.2 Criterios de selección

Para poder elegir la suite de monitorización que mejor se adapte a las necesidades de la ADL es necesario definir una serie de criterios que permitan discriminar entre las distintas soluciones existentes. La solución elegida será seleccionada de entre las que se han descrito en el capítulo 2.

Estos criterios se han clasificado en varias categorías. Los criterios de la categoría *limitantes* definen condiciones *sine qua non*, de tal forma que una solución que no cumpla con un criterio limitante quedará excluida del proceso de selección. Los criterios *no limitantes* son condicionantes deseados, pero que su ausencia no hará que se excluya a la suite del proceso de selección.

Limitantes:

- **Coste económico:** Debido a que este proyecto carece de consignación económica, no es posible seleccionar una solución por la que sea necesario pagar algún tipo de importe económico. En este sentido, será necesario seleccionar entre las open source o bien versiones gratuitas de software comercial. Por el mismo motivo no se podrá seleccionar una solución on-cloud, ya que las estudiadas en el capítulo 2 requieren el pago de una suscripción.
- **Sistema Operativo:** La solución elegida debe poder instalarse sobre CentOS 7, ya que los servidores Linux de la ADL funcionan con este sistema operativo. Este criterio se aplica porque se desea aprovechar el know-how de este entorno y reducir el tiempo necesario para la puesta en marcha, así como para mantener la homogeneidad del parque de sistemas operativos Linux. Tampoco se considera como opción instalar una suite que funcione sobre sistema operativo Windows, ya que sería necesario adquirir licencias adicionales a las que ya dispone la ADL.

No limitantes:

- **Funcionales:**
  - Autodescubrimiento de la red.
  - Monitorización de dispositivos a través de SNMP v2.
  - Agentes para CentOS, Windows VMI y VMWare.
  - Monitorización de servicios: Apache, Postfix, MySQL/MariaDB, IBM Domino y Symantec Endpoint Protection.
  - Monitorización de hardware.
  - Autentificación integrada con Active Directory
  - Cuadro de mandos parametrizable (Dashboard).
  - Disponibilidad de Mapa de red.
  - Informes parametrizables.
  - Alertas mediante email y SMS.
  - Mobile app.
- **Técnicos:**
  - Requisitos mínimos de instalación. Cuanto menores sean mayor puntuación.
  - Disponibilidad de API para desarrollar plugins/addons.
  - Documentación técnica para CentOS.
- **Empresariales:**
  - Lanzamiento de nuevas versiones. Tiempo transcurrido desde el lanzamiento de la última versión estable.
  - Disponibilidad de comunidad online de soporte.
  - Disponibilidad de versión on-cloud. Aunque en este proyecto se va a hacer una instalación on-premise, debido a la tendencia actual del mercado es posible que el futuro se tenga la necesidad de migrar a una solución on-cloud.

3.1.3 Selección

En primer lugar elegiremos las suites que satisfacen los criterios limitantes (aunque OPManager y OP5 ofrecen versiones gratuitas, la primera está limitada a tres dispositivos y la segunda a 20 y por eso no se incluyen en la comparativa):

- Nagios Core
- Pandora FMS Community
- Zabbix

En segundo lugar, es necesario establecer algún método cuantitativo para poder realizar la selección de las distintas soluciones en base a los criterios seleccionados anteriormente. Para ello, se va a utilizar un método de scoring [29].

En este método, a cada solución a comparar se le asigna una puntuación de 0 (si no cumple) a 9 (cumple totalmente) para cada uno de los criterios definidos. Como se considera que no todos los criterios tienen el mismo valor (por ejemplo no es lo mismo que no haya documentación específica para CentOS que no sea capaz de monitorizar un servidor Windows), a cada uno de los criterios se les asignará además un peso. Por cada criterio de cada suite

comparada se obtendrá un valor ponderado correspondiente al producto de la puntuación obtenida en ese criterio por el peso asignado. Finalmente los valores ponderados de cada una de las soluciones se sumarán y será seleccionada la que obtenga una mayor puntuación ponderada.

A continuación se muestra la tabla con las tres soluciones comparadas y su puntuación:

		INVIDUAL			PONDERADA		
	Peso	Nagios	Pandora	Zabbix	Nagios	Pandora	Zabbix
Funcionales							
Autodescubrimiento	5	0	0	9	0	0	45
SNMPv2	5	9	9	9	45	45	45
Agente CentOS	3	5	5	5	15	15	15
Agente Windows WMI	3	5	5	5	15	15	15
Agente VMWare	3	5	0	5	15	0	15
Monitor Apache	3	5	5	5	15	15	15
Monitor Postfix	3	5	5	5	15	15	15
Monitor MySQL	3	5	5	5	15	15	15
Monitor Domino	3	5	0	5	15	0	15
Monitor SEP	3	5	0	0	15	0	0
Monitor hardware	3	5	5	5	15	15	15
Autentificación AD	2	5	0	9	10	0	18
Dashboard	5	5	0	9	25	0	45
Mapa de red	5	5	0	9	25	0	45
Informes parametrizables	5	5	5	9	25	25	45
Alertas email	3	9	9	9	27	27	27
Alertas SMS	3	9	5	9	27	15	27
Mobile app	2	9	9	9	18	18	18
Técnicos							
Requisitos instalación	5	7	5	9	35	25	45
API	6	9	9	9	54	54	54
Plugins-addons	6	9	2	4	54	12	24
Documentación	8	9	9	9	72	72	72
Empresariales							
Nuevas versiones	8	7	9	9	56	72	72
Comunidad soporte	8	9	9	9	72	72	72
Version cloud	2	0	0	5	0	0	10
TOTALES	105	151	110	175	680	527	**784**

Tabla 6. Scoring selección herramienta de monitorización

Los pesos de cada uno de los criterios se han asignado de acuerdo a las necesidades actuales de monitorización de la red de la ADL. Por ejemplo, se considera más importante que la aplicación tenga autodescubrimiento, que reducirá el tiempo de implantación, que disponga de una versión on-cloud que es posible que se emplee en el futuro, pero no es una necesidad actual.

La puntuación de los aspectos funcionales se ha realizado asignando 0 si la funcionalidad no está disponible, 5 si lo está mediante plugins o módulos externos y 9 si es nativa del producto.

En cuanto a los aspectos técnicos, para los requisitos de la instalación se ha considerado que si se necesita 1 GByte o menos de memoria RAM se

asignarán 4 puntos y se irá restando 1 punto por cada GByte adicional, y si se necesita 10 GBytes de disco duro se asignarán 5 puntos y se irá restando 1 punto por cada 10 Gbytes adicionales. La existencia de API se ha valorado con 9 punto si existe y es fácilmente utilizable, 5 si existe y 0 si no existe. Los plugins se han valorado de acuerdo al número de extensiones disponibles: para Nagios hay alrededor de 4000, 800 para Pandora FMS y unos 1600 para Zabbix. Por último, la documentación se ha valorado si existe y está claramente explicada para CentOS 7.

Los aspectos empresariales se han valorado de la siguiente forma: para la disponibilidad de versiones se ha calculado el tiempo en años desde la última actualización que no sea de seguridad. Por cada año transcurrido se ha restado un punto del máximo de 9. La última versión de Nagios es la 4.4 de junio de 2018, Pandora FMS tiene una filosofía Rolling Release, lo que hace que sólo haya una versión estable cuya última actualización es de octubre de 2019 y la versión 4.4 de Zabbix es de octubre de 2019. En cuanto a la existencia de comunidad de soporte se ha valorado que existe y esté activa. Sobre la existencia de versión on-cloud, la única que dispone de ella es Zabbix y está en versión beta, por lo que se ha valorado con 5 puntos.

De la puntuación obtenida se considera que la herramienta más adecuada para las necesidades planteadas en este proyecto es Zabbix, que es la que se va a desplegar.

3.2 Estrategia de despliegue

Una vez seleccionada la suite que se va a implantar es necesario definir los pasos que se van a seguir en este despliegue.

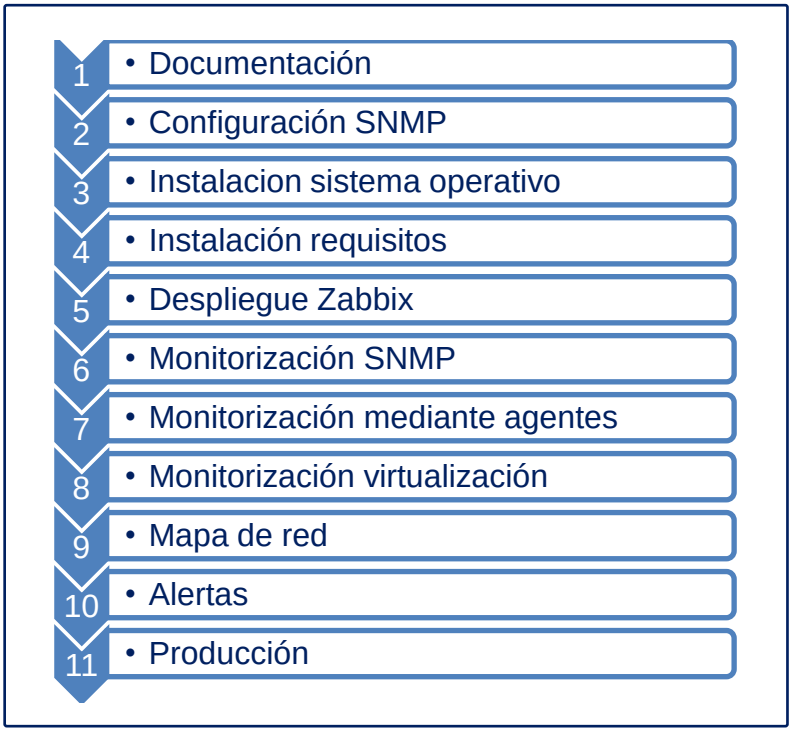


Figura 17. Estrategia de despliegue Zabbix

A continuación se describen cada una de los pasos:

1. **Documentación:** El primer paso es documentarse sobre la instalación y funcionamiento básico en la documentación oficial de Zabbix.
2. **SNMP:** Configurar los agentes SNMP en los dispositivos de la ADL que se van a monitorizar. Al menos un equipo de red Cisco y un SAI HP.
3. **Sistema Operativo:** Se creará una máquina virtual con sistema operativo CentOS 7 en el servidor CPU0276 de la sede principal.
4. **Instalación requisitos:** Se instalarán los requisitos de la suite de monitorización: base de datos, servidor http, herramientas SNMP, etc.
5. **Zabbix:** Despliegue de la versión 4.4 de la suite y configuración básica.
6. **Monitorización SNMP:** Configurar Zabbix para que monitorice dispositivos configurados en el paso 2 mediante SNMP.
7. **Monitorización mediante agentes:** Desplegar los agentes Zabbix en servidores Windows y Linux a monitorizar.
8. **Monitorización del entorno de virtualización:** Monitorización de los hipervisores VMWare.
9. **Mapa de red:** Generar un mapa de red con los dispositivos monitorizados.
10. **Configurar alertas:** Configurar alertas básicas con los equipos que se están monitorizando.
11. **Puesta en producción:** Una vez que se ha comprobado que Zabbix funciona correctamente y que se está monitorizando al menos dos equipos con SNMP y un servidor Windows y Linux, se iniciará el trabajo en real y se irán extendiendo los equipos monitorizados y ajustando Zabbix a las necesidades de la ADL.

Los pasos descritos en esta estrategia de despliegue se irán documentando en las siguientes secciones. El objetivo al finalizar la sección 3.4 es tener el sistema Zabbix operativo y monitorizando algunos de los equipos de la ADL.

3.3 Instalación y parametrización

3.3.1 Documentación

La fuente principal de información para el despliegue de la solución se ha obtenido del manual oficial de Zabbix [30]. La última versión estable es la 4.4, que es la que se va a utilizar en este proyecto. En este momento está en desarrollo la versión 5, pero aún no se ha liberado como versión estable.

Zabbix está constituido por varios componentes principales, cada uno de ellos encargado de realizar una función diferenciada:

- **Servidor:** Es el núcleo de Zabbix. Se encarga de recopilar datos de los equipos monitorizados. Gestiona todos los datos de configuración, estadísticos y operativos.
- **Base de datos:** Almacena permanentemente toda la configuración y los datos recopilados.

- **Interfaz Web:** Es el interfaz de comunicación entre Zabbix y las personas, basado los estándares web, por lo que sólo es necesario un navegador para comunicarse con Zabbix.
- **Proxy:** Se encarga de recopilar datos y remitírselos al servidor para su procesamiento. Su instalación es opcional, no siendo necesario para redes pequeñas. En instalaciones grandes, reduce la carga del servidor distribuyendo el proceso de captura de datos.
- **Agentes:** Se instalan en los equipos a monitorizar y envían datos al servidor. Zabbix puede monitorizar sin agentes con protocolos de gestión de red como SNMP.

Antes de comenzar la instalación y configuración de los equipos a monitorizar, es necesario definir algunos conceptos básicos en Zabbix:

- **Host:** Entidad, física o virtual, conectada a la red que se puede monitorizar, por ejemplo un switch o un servidor Windows.
- **Monitor:** Especifica qué es lo que se quiere monitorizar del host, es decir, qué métrica se va a medir, por ejemplo la carga de la CPU, o el tráfico de una interfaz ethernet.
- **Iniciador:** Evalúa los datos recuperados de un monitor y cambia el estado de *OK* a *PROBLEMA* cuando se cumplen unas determinadas condiciones, por ejemplo cuando la CPU esté por encima del 90% de uso durante 5 minutos, se cambia el estado a *PROBLEMA*. Si el estado es *PROBLEMA* se debe definir su gravedad, que se clasifica en los siguientes valores: No clasificada, Informativa, Advertencia, Promedio, Alta y Crítica.
- **Aplicaciones:** Las aplicaciones sirven para agrupar monitores relacionados entre sí. Por ejemplo la aplicación CPU agrupa los monitores: número de CPUs, carga media, número de interrupciones, etc.
- **Gráfico:** Los datos recuperados por los monitores pueden representarse gráficamente para una mejor visualización y detectar tendencias y errores de forma visual.
- **Regla de descubrimiento**: Permiten crear automáticamente monitores, iniciadores y gráficos para un host sin tener que definirlos manualmente. Esta funcionalidad es especialmente útil, ya que el sistema detecta entidades a monitorizar en el host y crea automáticamente los monitores necesarios en Zabbix. Por ejemplo, se puede configurar una regla de autodescubrimiento que busque todas las interfaces ethernet de un switch y que defina automáticamente y para cada una de ellas los monitores, iniciadores y gráficos necesarios.

Una vez que el sistema Zabbix esté operativo, se deben definir tantos hosts como dispositivos a monitorizar, y para cada host, a su vez, se debe configurar los monitores, iniciadores y gráficos necesarios.

La mejor forma de realizar esta configuración es utilizando plantillas, que pueden ser creadas por el usuario, utilizar alguna de la que están definidas en el sistema Zabbix o bien importarlas de alguno de los repositorios disponibles. Las plantillas permiten definir monitores, iniciadores, gráficos y reglas de descubrimiento para diversos tipos de host. Una vez creado el host se le

asigna una plantilla y automáticamente se definen todos los elementos de monitorización de este host sin tener que crearlos manualmente. Por ejemplo, la plantilla *Template OS Windows by Zabbix agent*, permite configurar un host Windows rápidamente ya que incorpora la definición de 31 monitores, 12 iniciadores, 5 gráficos y 3 reglas de descubrimiento.

3.3.2 SNMP

Antes de comenzar con la instalación propiamente dicha, es necesario preparar el entorno de monitorización.

En general, es preferible instalar los agentes nativos de Zabbix en los equipos que en los que sea posible, ya que son ligeros, flexibles y pueden recopilar una gran cantidad de información (por ejemplo en los equipos Windows puede interactuar con WMI para recuperar información de rendimiento). Los agentes están soportados en los siguientes entornos:

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac X
- Solaris: 9, 10, 11
- Windows

Para la monitorización de otro tipo de equipos, como por ejemplo: electrónica de red o impresoras es necesario recurrir a protocolos estándar como SNMP.

Por este motivo, el primer paso antes comenzar con la instalación de Zabbix es configurar y verificar el funcionamiento del protocolo SNMP en los equipos que no admiten la instalación de un agente.

En concreto, se ha configurado SNMP en los siguientes equipos de la red de la ADL:

- 2 Firewalls Cisco
- 2 Switches Cisco capa 3
- 3 Switches Cisco capa 2
- 2 Routers Cisco
- 3 SAI HP
- 4 Impresoras de red

La versión elegida de SNMP ha sido la 2c, o en su defecto la 1, ya que están soportadas por todos los equipos que se van a monitorizar y se desean unificar las configuraciones en la medida de lo posible. Con el fin de disminuir el riesgo que suponen las configuraciones por defecto, que pueden ser aprovechadas por malware, se ha configurado una comunidad de lectura distinta de *public* y se ha deshabilitado la comunidad de escritura en los dispositivos en los que estuviera configurada.

Figura 18. Comprobación SNMP mediante snmpwalk

Una vez configurados los equipos y para comprobar que la configuración es correcta, se ha utilizado el comando snmpwalk desde un servidor Linux que permite obtener datos de los agentes SNMP configurados. A este comando se le pasan como parámetros: la versión SNMP del agente (-v), el nombre de la comunidad (-c), la dirección IP del host y el OID consultado. En este caso se ha solicitado el OID 1.3.6.1.2.1.1.5 que recupera el nombre del host. En la figura 8 se muestra la consulta hecha varios dispositivos de la red de la ADL, una vez configurado el protocolo SNMP.

La configuración SNMP de los equipos se detalla en el Anexo 9.1.

3.3.3 Sistema Operativo

El primer paso para el despliegue de Zabbix es instalar y configurar el sistema operativo sobre el que se ejecutará. Los requisitos de Zabbix son los siguientes [30]:

- Sistema operativo: Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, HP-UX, Mac OS X, Solaris.
- Base de datos: MySQL/MariaDB, Oracle, PostgreSQL, TimescaleDB, IBM DB2 y SQLite
- Servidor web: Apache 1.3.12 o superior + PHP 5.4.0 o superior

Como se ha explicado anteriormente, el parque de instalaciones Linux de la ADL está basado en CentOS, por lo que esta será la distribución de Linux elegida. En el momento del despliegue de este proyecto está disponible CentOS 8. Sin embargo, se va a utilizar CentOS 7 por el know-how de esta versión que se tiene en la ADL, la estabilidad del mismo y que seguirá disponiendo de actualizaciones completas hasta el cuatro cuatrimestre de 2020 y de mantenimiento hasta el 30 de junio de 2024 [31].

Para el despliegue de Zabbix se creará una máquina virtual sobre VMWare en los servidores de la ADL.

La instalación de CentOS se detalla en el Anexo 9.2.

3.3.4 Instalación de requisitos

En cuanto a las versiones de base de datos, servidor web y PHP, CentOS 7 proporciona las siguientes, que cumplen los requerimientos mínimos de Zabbix:

- Apache 2.4.6
- MariaDB 5.5.x
- php 5.4

Sin embargo, y aunque el software proporcionado por defecto en la distribución de CentOS 7 cumple con los requisitos mínimos, se ha optado por utilizar repositorios de terceros para actualizar las versiones de php y MariaDB.

En cuanto a la versión de php, todas las ramas de la versión 5 han alcanzado el fin de vida, por lo que se utilizará la versión 7.2, que está soportada (a nivel de actualizaciones de seguridad) hasta el 30 de noviembre de 2020 [32]. No se utiliza una rama superior de la versión 7 de PHP (7.3 o 7.4), ya que se han realizado pruebas de instalación con la última versión estable de Zabbix y existen problemas de compatibilidad por la falta de dependencias. En concreto, los paquetes: php-mysql y php-mcrypt en la versión 7.2 de PHP son reemplazados por php-mysqlnd y php-pecl-mcrypt en la versión 7.4 que no son compatibles actualmente con Zabbix.

Sobre la instalación de MariaDB, la recomendación es utilizar la versión 10.x. El ciclo de vida de la versión 5.5 finalizó en 2017, aunque se ha decidido mantener el soporte para actualizaciones de seguridad hasta abril del 2020 por "*la extensión excepcional de su uso*" [33]. En el proyecto se va a utilizar MariaDB 10.4, que es la última versión estable y es la que se está utilizando actualmente en los servidores de la ADL, no habiéndose detectado ningún problema de funcionamiento.

La instalación de los requisitos adicionales se detalla en el Anexo 9.3.

3.3.5 Zabbix

El siguiente paso es desplegar Zabbix. Existen cuatro formas de instalar el producto:

- Utilizando paquetes precompilados (existen paquetes para Red Hat/CentOS, Debian/Ubuntu y SUSE)
- Desde las fuentes, descargando el código y compilándolo.
- Containes: se proporcionan imágenes Docker para cada componente de Zabbix.
- Virtual appliance: descargando una máquina preinstalada basada en Ubuntu (existen versiones para VMWare, Hyper-V, Qemu, etc.)

En este proyecto se ha optado por utilizar paquetes precompilados para Red Hat/CentOS, ya que el despliegue es rápido y sencillo, es fácil de mantener, permite elegir qué componentes adicionales se van a utilizar (en este caso Apache, MariaDB y PHP 7.2), y se aprovecha el know-how existente.

En la instalación se va a optar por no instalar ni configurar el componente proxy de Zabbix, ya que la instalación no es suficientemente grande como para necesitarlo y agregaríamos complejidad y una carga innecesaria al sistema.

Para la instalación es necesario agregar a la máquina virtual que se ha preparado en el punto 3.3.3 el repositorio para CentOS de Zabbix e instalar los siguientes módulos:

- Servidor: paquete zabbix-server-mysql
- Frontend web: paquete zabbix-web-mysql

La instalación de los requisitos adicionales se detalla en el Anexo 9.4. Una vez instalado, se puede acceder a través de la interfaz gráfica en la dirección http://zabbix.adl.local/zabbix con el usuario Admin y contraseña zabbix. El primer paso una vez conectado debe ser cambiar el alias del usuario y la contraseña. A partir de este momento, el sistema ya está operativo y procede configurar los equipos a monitorizar.

3.3.6 Monitorización SNMP

A continuación se definen en Zabbix los equipos que se van a monitorizar mediante SNMP. Como se ha comentado anteriormente la mejor opción es definir cada uno de los hosts y asignarles una o varias plantillas para comenzar la monitorización. En caso necesario, se puede modificar la configuración de host para ajustarlo a las necesidades de la ADL.

Los equipos monitorizados mediante SNMP son los siguientes:

Host	Descripción	Plantilla
Grupo Network devices		
adl-ast-2900	Router Cisco VPN	Net Cisco IOS SNMPv2
adl-ast-2960-1	Switch Cisco capa 2	
adl-ast-2960-2	Switch Cisco capa 2	
adl-ast-3750	Switch Cisco capa 3	
adl-ger-2900	Router Cisco VPN	
adl-ger-2960	Switch Cisco capa 2	
adl-ger-3750	Switch Cisco capa 3	
adl-ast-pix	Firewall Cisco ASA	ASA Discovery
adl-ger-pix	Firewall Cisco ASA	
Grupo UPS		
SAI0016	SAI HP	HP RT3000 SNMP
SAI0017	SAI HP	
SAI0018	SAI HP	
Grupo Printers		
IMP_HP5550	Impresora HP	Generic printers
IMP_KYOCERA	Multifunción Kyocera	Generic printers
IMP_MPC2500	Multifunción Nashuatec	SNMP Ricoh printers
IMP_MPC2000	Multifunción Nashuatec	

Tabla 7. Equipos monitorizados mediante SNMP

Para los equipos de red Cisco se ha utilizado la plantilla oficial Net Cisco IOS SNMPv2 sin ningún ajuste. En el caso de los dispositivos ASA, los sais y las impresoras se ha recurrido a plantillas no oficiales proporcionadas por la comunidad de Zabbix, en las que ha sido necesario realizar algunas modificaciones. En el anexo 9.5 se detalla la configuración de estas plantillas.

Todas las plantillas están definidas con rutinas de descubrimiento lo que facilita la configuración de los equipos monitorizados. Por ejemplo, en el caso de los switches no es necesario configurar manualmente cada una de las interfaces ethernet y los monitores asociados a ellas, o en el caso de las impresoras no es necesario definir todas las bandejas de papel disponibles.

En total se han definido más de 2.000 monitores, unos 1.000 iniciadores y más de 230 gráficos.

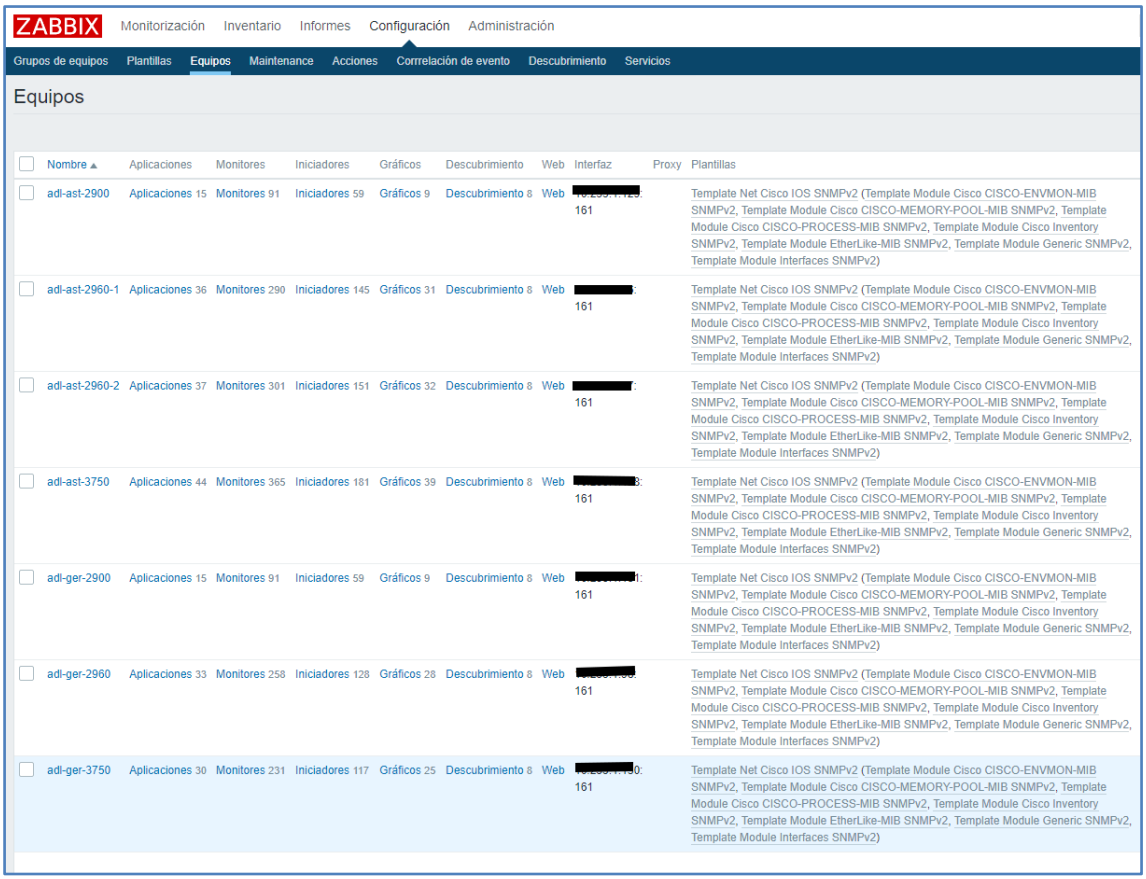


Figura 19. Configuración hosts mediante SNMP – Network devices

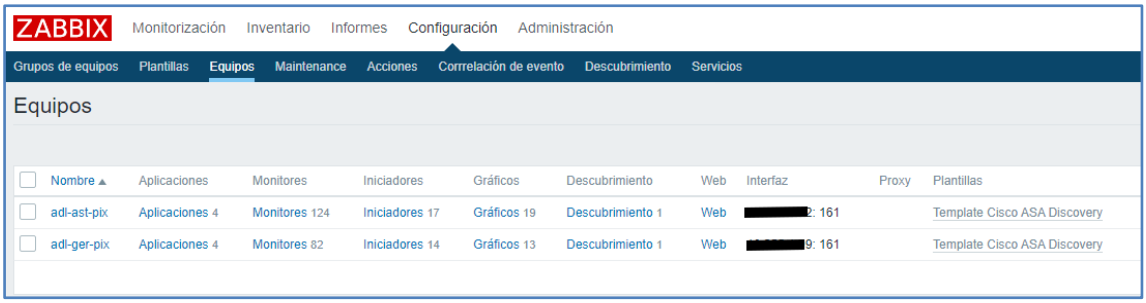


Figura 20. Configuración hosts mediante SNMP – Firewalls

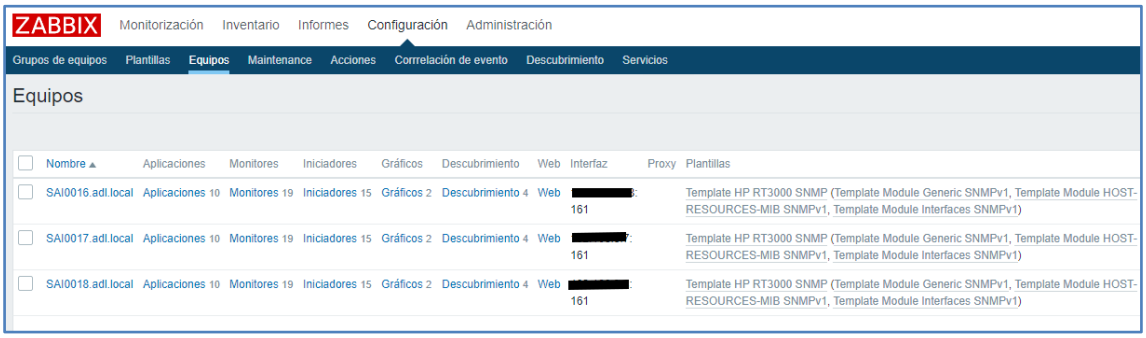


Figura 21. Configuración hosts mediante SNMP – UPS

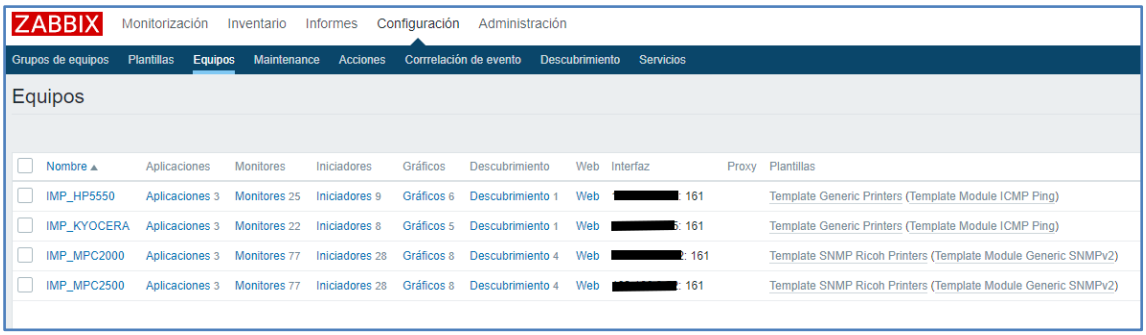


Figura 22. Configuración hosts mediante SNMP – Printers

3.3.7 Monitorización mediante agentes

La monitorización con agentes, a diferencia de la realizada mediante SNMP, se basa en la instalación de software en el host a monitorizar. El agente instalado se encarga de recopilar información de forma activa de los recursos y aplicaciones instalados en el sistema y de enviarlos al servidor Zabbix.

Existen dos formas de realizar la comunicación entre el agente y el servidor Zabbix: pasiva y activa. En la comunicación pasiva, el servidor interroga al agente y éste responde enviándole la información solicitada. En la comunicación activa, es el agente el que inicia a intervalos regulares la comunicación con el servidor sin que exista un requerimiento previo de éste. La comunicación activa se utiliza en entornos donde el agente se encuentra detrás de algún proxy, NAT o firewall que impide que el servidor pueda comunicarse directamente con el agente. El inconveniente que tiene este tipo de comunicación es que el servidor tiene que esperar a que el agente se

comunique con él, no pudiendo realizar ninguna petición fuera de los periodos programados de comunicación.

Existen agentes para entornos Linux y Windows, que se van a utilizar para la monitorización de los servidores de la Agencia, tanto virtuales como físicos. Los equipos monitorizados mediante agentes son los siguientes:

Host	Descripción	Plantilla
Grupo Linux servers		
backup-ast	Servidor backup principal	OS Linux by Zabbix Agent
backup-ger	Servidor backup formación	
castillo	Servidor desarrollo	
levante	Servidor producción	
lonja	Servidor acceso remoto	
www.adlsantapola.es	Servidor web – email	
Grupo Windows servers		
escaletes	Servidor ADL formación AD	OS Windows by Zabbix Agent
glorieta	Servidor Terminal Server	
puerto	Servidor ADL principal AD	
salinas	Servidor red pública	

Tabla 8. Equipos monitorizados mediante agentes

La instalación y configuración de estos agentes se detalla en el anexo 9.6.

En el caso de la monitorización con agentes se han definido unos 900 monitores, más de 250 iniciadores y más de 370 gráficos.

Figura 23. Configuración hosts mediante agentes – Linux servers

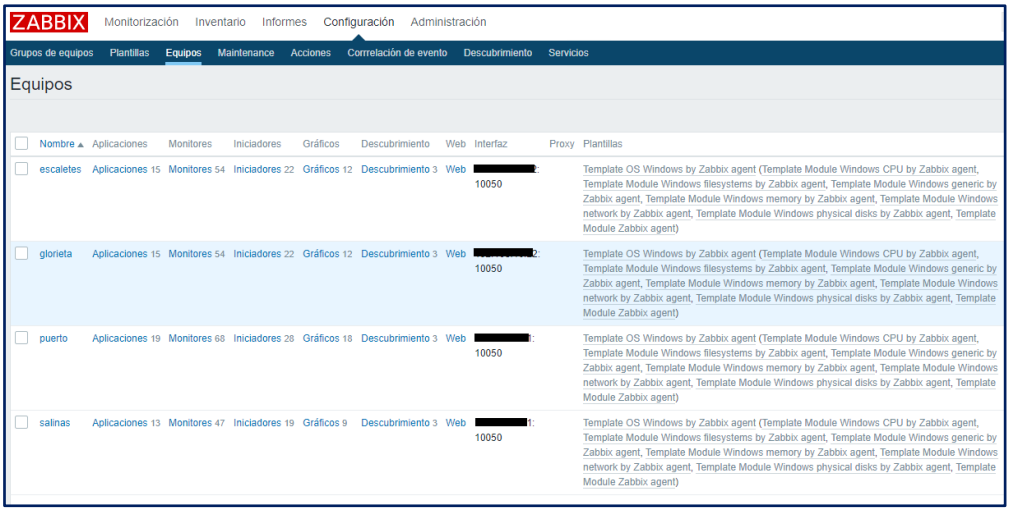


Figura 24. Configuración hosts mediante agentes – Windows servers

3.3.8 Monitorización del entorno de virtualización

Por último, se desea monitorizar los hipervisores VMWare instalados en la ADL. La monitorización del entorno de virtualización no se realiza de forma directa creando un host y asignándole una o varias plantillas como lo visto hasta el momento. Esta monitorización se realiza en dos pasos: en primer lugar es necesario configurar y activar en el servidor Zabbix el proceso vmware collector, que se encarga de obtener información de los hipervisores VMWare, y en segundo lugar, esta información se recupera por el servidor Zabbix para que pueda ser monitorizada.

La configuración de la monitorización del entorno de virtualización VMWare se describe en el anexo 9.7

Una vez habilitado el entorno de monitorización para VMWare es necesario crear un primer host en el servidor Zabbix, que corresponde al vcenter y a partir de ahí, Zabbix descubre la infraestructura y añade automáticamente los hipervisores y las máquinas virtuales.

En el caso de la ADL, al tener configurados los hipervisores como máquinas autónomas (no hay vcenter) ha sido necesario definir tres host distintos, uno para cada hipervisor y a partir de aquí, que el servidor Zabbix descubra la infraestructura y añada las máquinas virtuales encontradas.

Zabbix crea automáticamente varios grupos para almacenar la infraestructura de virtualización:

- (vm): Contiene todas las máquinas virtuales encontradas
- ha-datacenter: Contiene los hipervisores del datacenter
- ha-datacenter (vm): Contiene las máquinas virtuales del datacenter
- Hypervisor: Contiene los hipervisores detectados
- Virtual machines: Contiene las máquinas virtuales detectadas

Además crea un grupo por cada hipervisor con las máquinas virtuales alojadas en ese host. Al no dispone de datacenter, en los grupos (vm), ha-datacenter y ha-datacenter (vm) sólo se asignan los hosts del primer hipervisor que se haya definido, ya que el resto de hipervisores dan un error de grupo existente al intentar crear estos grupos.

A continuación se muestra la infraestructura de virtualización de la ADL descubierta por Zabbix. Como se puede comprobar, el número de máquinas virtuales descubiertas es mayor que el número de servidores monitorizados en el apartado 3.3.7, ya que no todas las máquinas virtuales son servidores de producción que se deseen monitorizar.

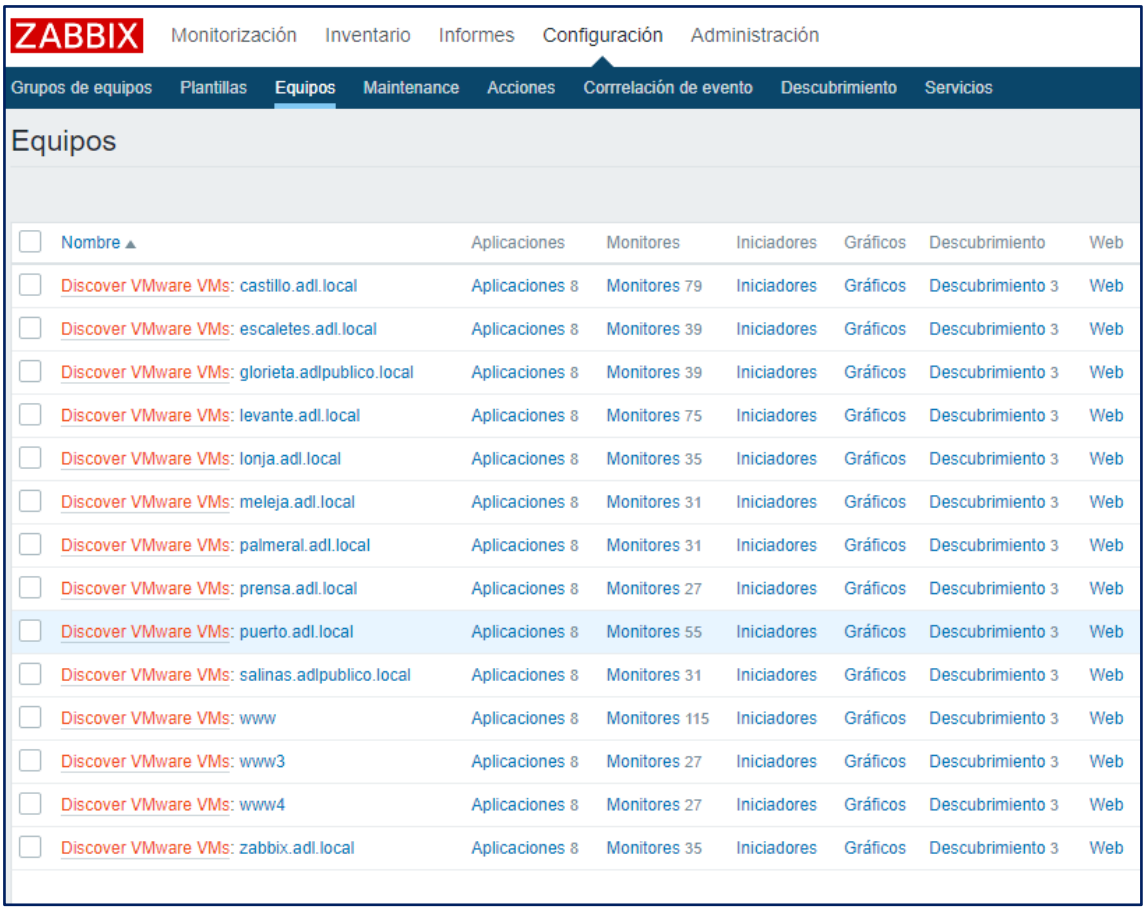


Figura 25. Virtualización – Descubrimiento de máquinas virtuales

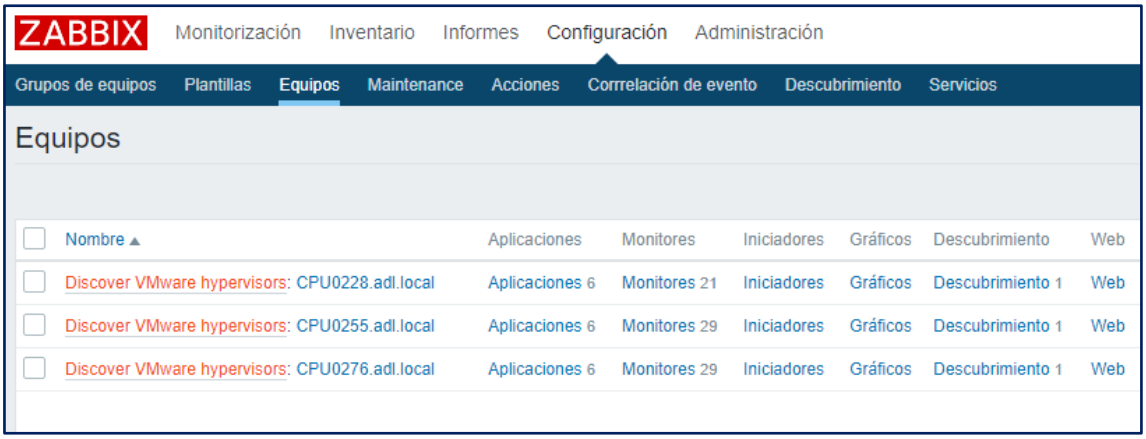


Figura 26. Virtualización – Descubrimiento de hipervisores

3.3.9 Mapa de red

Zabbix permite crear mapas de red, para inspeccionar rápidamente y de manera gráfica el funcionamiento de la infraestructura de red. Los mapas permiten crear enlaces entre hosts que representan las relaciones lógicas entre elementos de la red. A cada uno de estos enlaces se le puede asignar un color dependiendo del estado de la conexión. Por ejemplo, se puede configurar un enlace para que se muestre de color rojo si el host es inaccesible vía ICMP.

Los mapas también permiten ejecutar algunos comandos rápidos para detectar rápidamente la existencia de problemas. Para ello basta con hacer clic en un host y seleccionar una de las opciones del menú desplegable que se muestra:

- Scripts:
  - Detectar el sistema operativo
  - Ping
  - Traceroute
- Ir a:
  - Inventario de equipos
  - Última fecha
  - Problemas
  - Gráficos
  - Pantallas

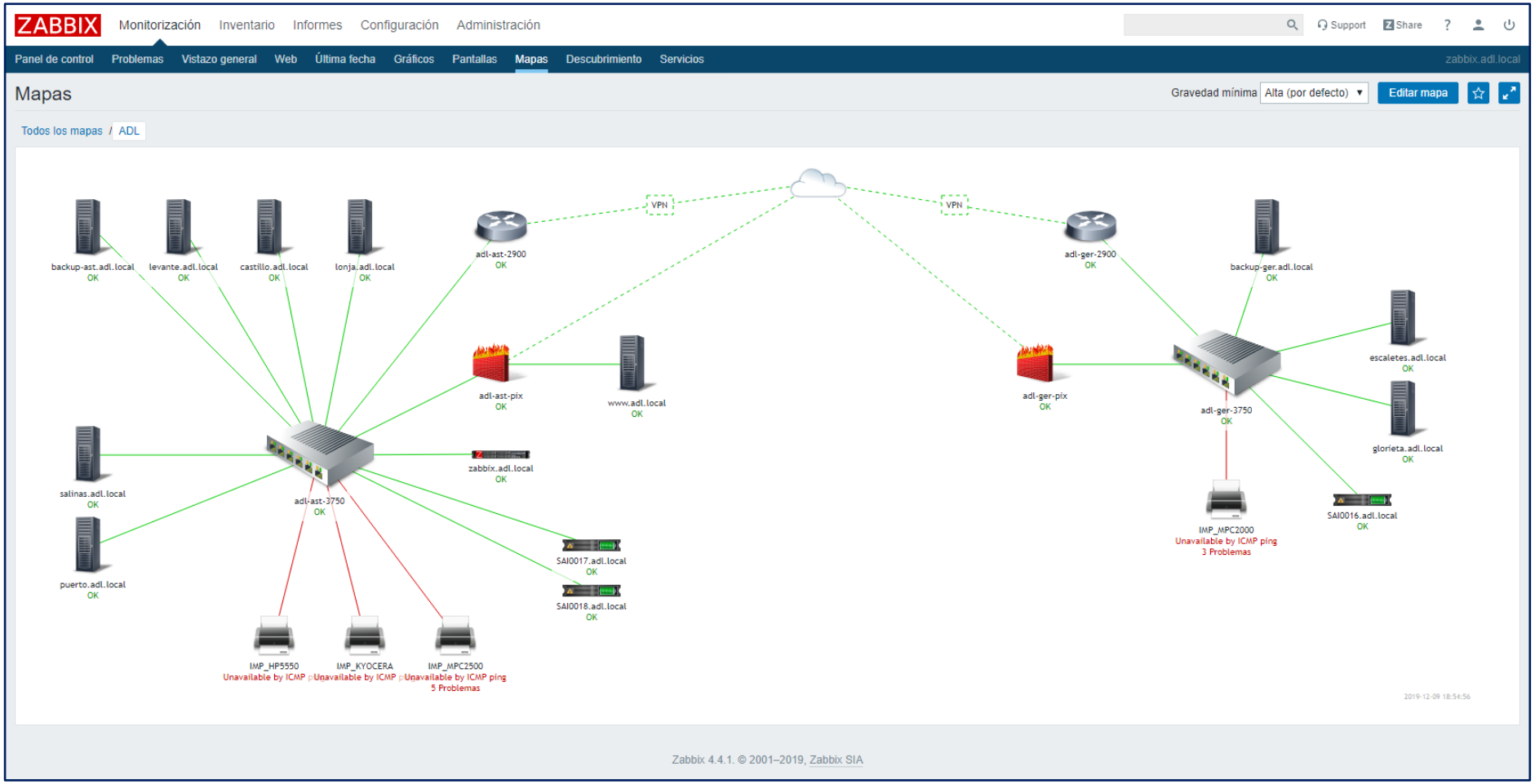


Figura 27. Mapa de red Zabbix – red ADL

En la instalación de este proyecto se ha creado un único mapa con la configuración lógica de la red de la ADL, en la que los enlaces de los hosts que no responden a ICMP se colorean en rojo. Así mismo, para cada host se muestra el número de problemas y se expande el más crítico con gravedad alta o superior.

En la figura 17 se muestra dicho mapa y se puede apreciar que en el momento de la captura el enlace de las impresoras es de color rojo (estaban apagadas las impresoras). También se muestran los errores de gravedad alta o superior en los host que presentan problemas.

3.3.10 Alertas

Finalmente se van a configurar alertas. De nada sirve monitorizar la red, si el sistema no es capaz de avisar a los administradores cuando sucede un evento grave.

La configuración del sistema de alertas consta de dos partes: en primer lugar es necesario configurar algún tipo de comunicación y en segundo lugar definir las acciones. Las acciones definen el contenido de la notificación, cuales son las condiciones para enviarla (por ejemplo que la gravedad del error sea alta o superior), etc.

Zabbix dispone de cuatro tipos de mecanismos de notificaciones:

- email: Envía un correo electrónico
- SMS: Envía una alerta mediante SMS
- scripts: Ejecuta un script
- Webhook: Hace llamadas HTTP utilizando JavaScript

En cuanto a los eventos que pueden desencadenar una acción son:

- Iniciadores: Cuando un iniciador cambia el estado de un host de *OK* a *PROBLEMA*
- Descubrimiento: Cuando el descubrimiento de la red se ejecuta
- Autoregistro: Cuando los agentes activos se registran automáticamente
- Eventos internos: Cuando un monitor se convierte en no soportado o un iniciador queda en un estado desconocido

En un primer momento se ha decidido utilizar el email como mecanismo de alerta, debido a su facilidad de configuración. Se ha definido una única alerta para poder monitorizar cualquier problema que se produzca en cualquier host. Seguramente el número de mensajes recibidos sea elevado pero, durante la fase de estabilización de la solución, se cree conveniente recibir todos los mensajes que genere el sistema. Posteriormente se ajustará la configuración para que el sistema sólo alerte de los problemas realmente graves.

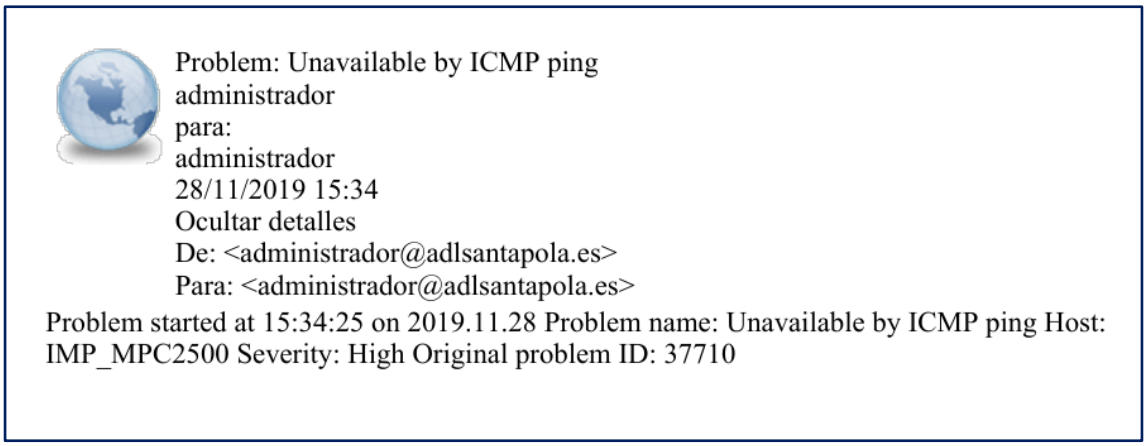

Problem: Unavailable by ICMP ping
administrador
para:
administrador
28/11/2019 15:34
Ocultar detalles
De: <administrador@adlsantapola.es>
Para: <administrador@adlsantapola.es>
Problem started at 15:34:25 on 2019.11.28 Problem name: Unavailable by ICMP ping Host: IMP_MPC2500 Severity: High Original problem ID: 37710

Figura 28. Alertas – Host sin respuesta ICMP

3.4 Producción y estabilización

Una vez que ha finalizado la configuración principal del sistema, procede avanzar en la siguiente fase que es la puesta en marcha. Es decir, pasamos de un sistema en desarrollo a un sistema en producción. Es en este momento cuando el sistema pasa a ser utilizado por los usuarios finales, en este caso por los compañeros del Servicio de Sistemas de Información de la ADL y/o del Ayuntamiento, y se comienza la explotación de datos reales.

En cualquier proyecto, aunque la implantación haya sido rigurosa y testeada, siempre es necesaria una primera subfase dentro de la fase de puesta en producción denominada *estabilización*. Es en esta subfase donde acaban de ajustarse y corregirse las pequeñas desviaciones que pudieran surgir al trabajar con un sistema en entorno real y no de pruebas.

En este sentido, durante varios días se ha ido comprobando que el sistema es estable y que se monitorizan adecuadamente los hosts que se han definido en la fase 3.3. Así mismo, se ha comprobado la carga del servidor Zabbix para comprobar si está correctamente dimensionado.

Para comprobar que la monitorización se está realizando correctamente se ha medido la disponibilidad del agente Zabbix o de la posibilidad de capturar datos mediante SNMP, dependiendo de si la monitorización se realiza mediante agente Zabbix o SNMP. A continuación se muestran valores de disponibilidad en el periodo del 25 de noviembre al 1 de diciembre de algunos de los hosts monitorizados.

Los únicos problemas detectados fueron en el servidor www y en los dispositivos Cisco ASA. En el primer caso se debió a un error en la configuración del firewall de Linux, que hizo que durante un 8,6 % del tiempo no estuviera disponible el agente Zabbix.

En cuanto a los dispositivos Cisco ASA, la monitorización se realizaba correctamente, pero sin embargo se recibía el error "*SNMP Failed*". Este error está debido a que la plantilla utilizada comprueba si se han recibido datos de la

utilización de la CPU en los últimos 5 segundos (monitor *cpmCPUTotal5secRev*). En caso negativo informa que no se han recibido datos de SNMP. En estos dispositivos este valor no está soportado, por lo que la activación del iniciador que indica que no se reciben datos SNMP no es correcta. Para solucionar el problema se ha reprogramado el iniciador *SNMP Failed* para que compruebe si se reciben datos del monitor *sysUpTime* en lugar del monitor *cpmCPUTotal5secRev*.

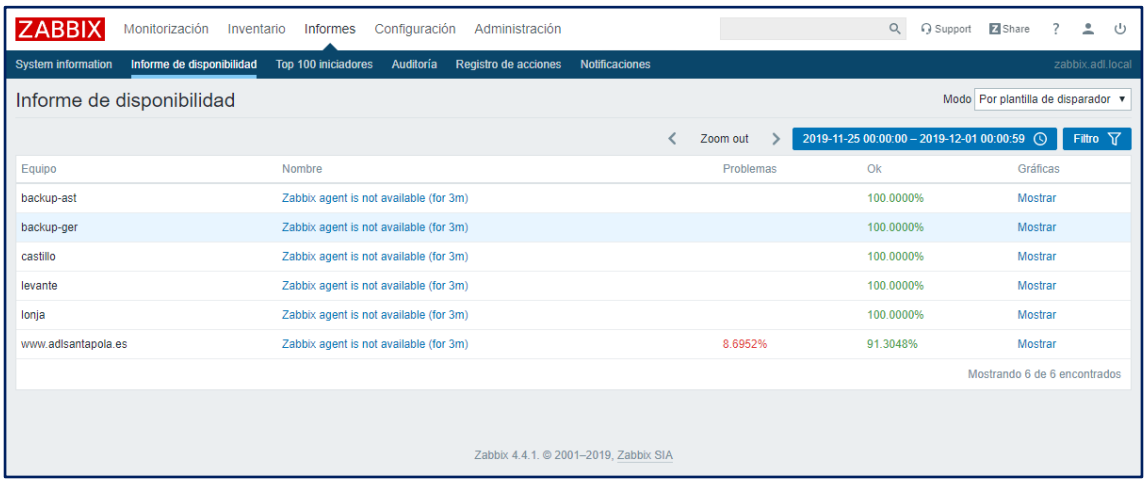


Figura 29. Estabilización – Disponibilidad agente Linux

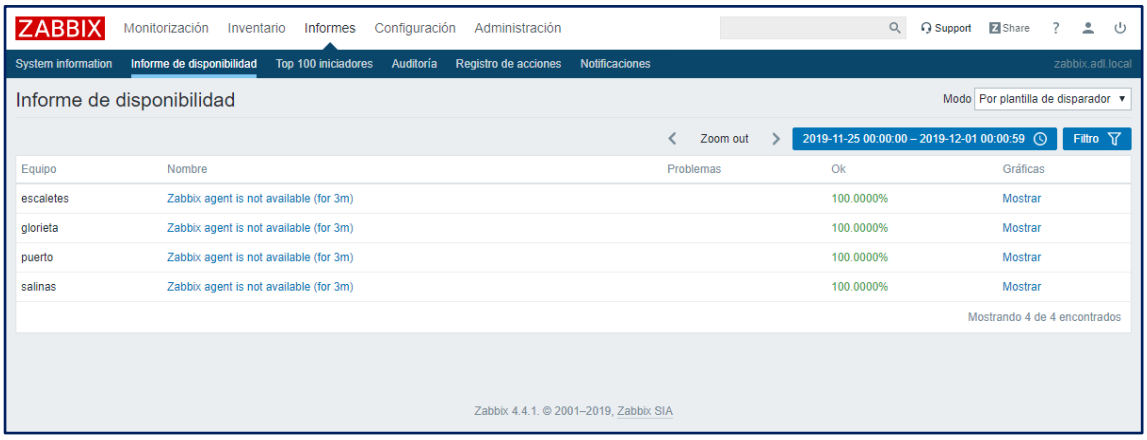


Figura 30. Estabilización – Disponibilidad agente Windows

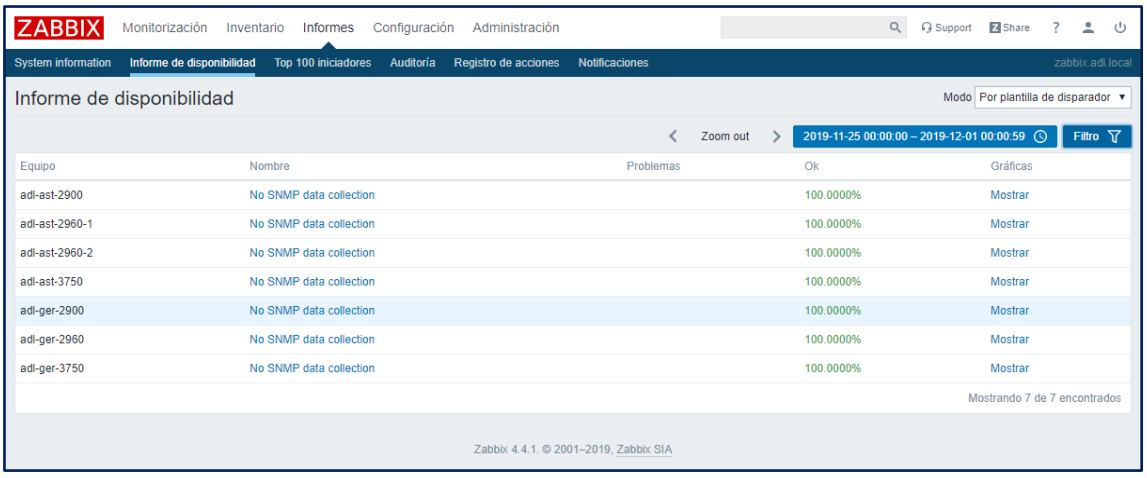


Figura 31. Estabilización – Disponibilidad dispositivos de red

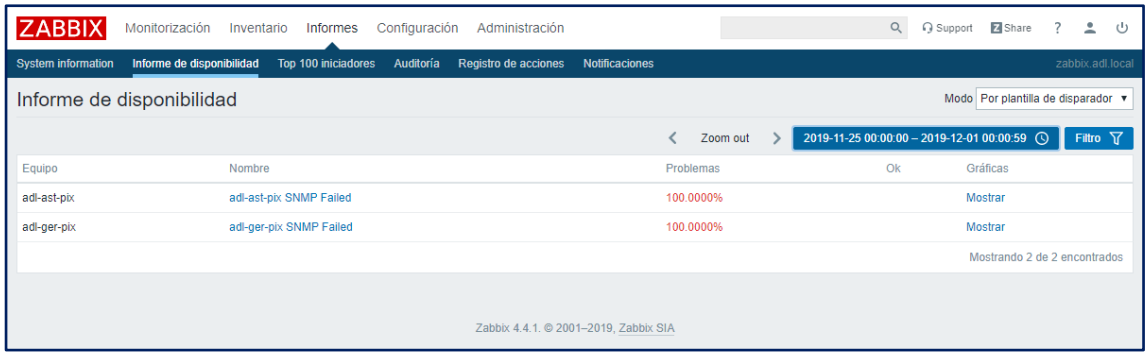


Figura 32. Estabilización – Disponibilidad Cisco ASA

Para la comprobación de la carga del servidor Zabbix se ha monitorizado el consumo de CPU, memoria y el espacio disponible en la partición /. A continuación se muestran valores de estos monitores para el servidor Zabbix en el periodo del 25 de noviembre al 1 de diciembre.

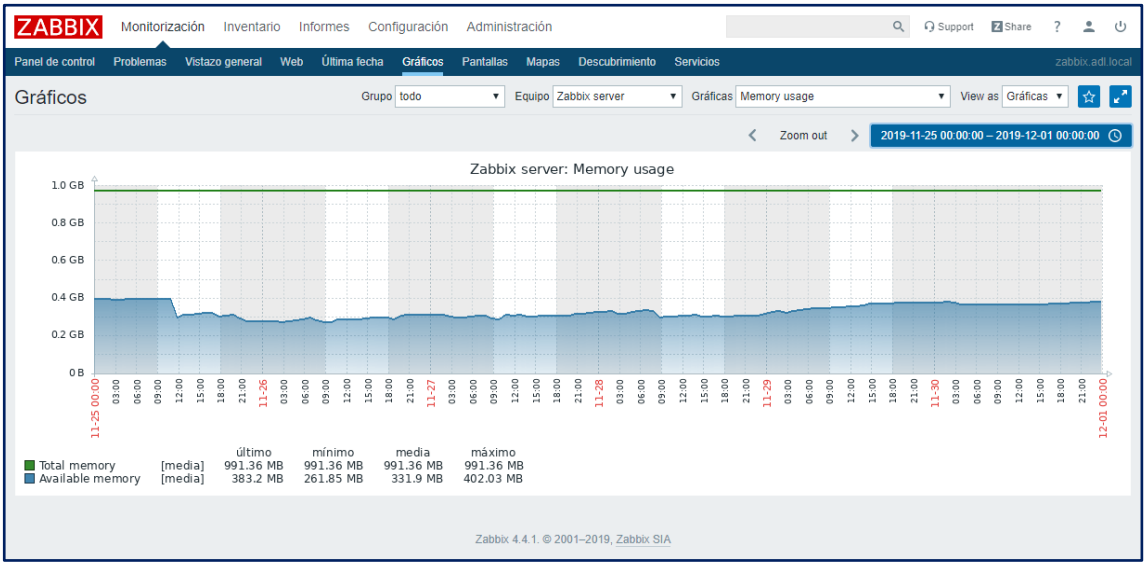


Figura 33. Estabilización – Utilización de la memoria del servidor Zabbix

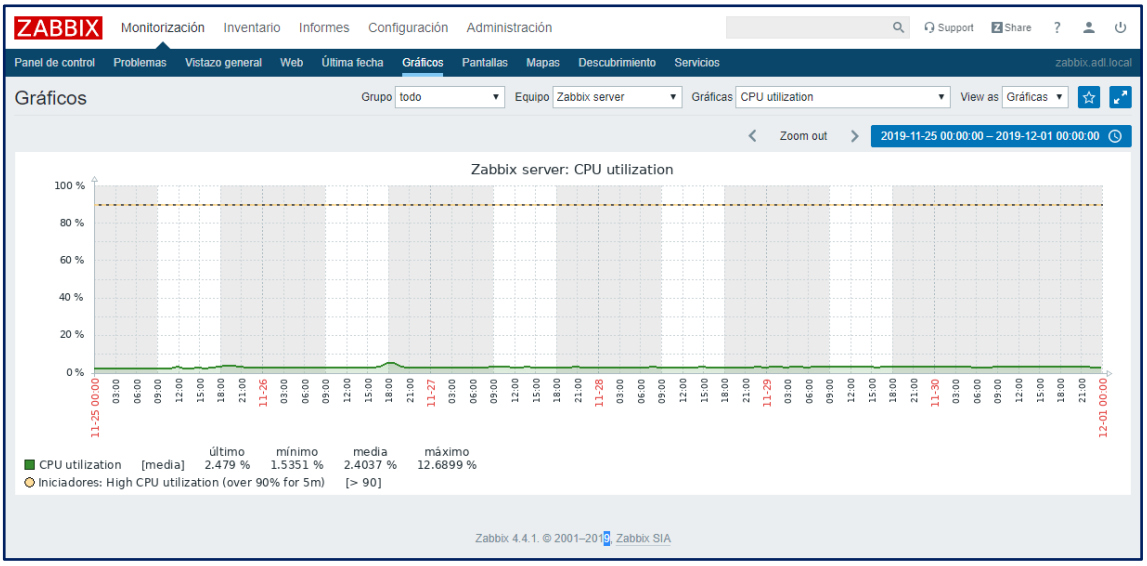


Figura 34. Estabilización – Utilización de la CPU del servidor Zabbix

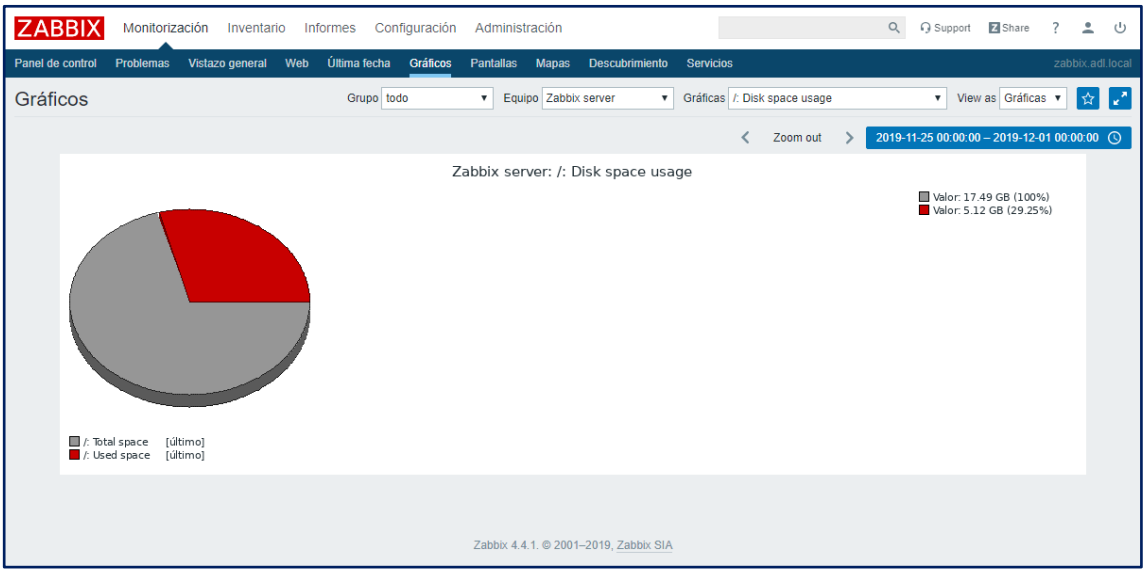


Figura 35. Estabilización – Utilización del disco del servidor Zabbix

En general, el servidor está funcionando correctamente y no se satura ni la CPU ni la memoria. Así mismo el espacio disponible en disco es suficiente.

Sí que ha sido necesario ajustar el envío de notificaciones por parte del sistema, ya que al activar que se envíe un email cada vez que un host cambie de estado de *OK* a *PROBLEMA*, hace que la cantidad de email informativos que se reciben sea abrumador, por ejemplo se avisa cada vez que se abre la puerta de una impresora o se queda sin papel. Por este motivo se ha ajustado el envío de mensajes a todos aquellos en los que la gravedad sea alta o superior, como ya se había anticipado en el punto 3.3.10.

4. Cierre

Una vez implantado el sistema correctamente y en el momento en que se encuentra estabilizado procede iniciar su explotación.

El objetivo de esta fase es utilizar las herramientas que proporciona el sistema para convertir los datos en información útil para extraer conclusiones y propuestas de mejora.

Debido a que el proyecto de implantación, y consecuentemente esta fase, es una parte del TFG completo, el tiempo de dedicado al cierre no puede ser muy extenso.

Durante unos días se procederá a explotar los datos que ofrezca el sistema y posteriormente a analizarlos.

Con esta fase daremos por concluida la implantación. Esto no quiere decir que no se siga obteniendo información del sistema y que no se siga analizando a lo largo de toda la vida útil del mismo.

4.1 Toma de datos y verificación

En primer lugar se trata de identificar en el sistema la información que sea valiosa para la ADL y aprovecharla. Con este motivo durante varios días se explora la información que es capaz de generar Zabbix. En este sentido son muy útiles las notificaciones mediante email, y las secciones *problemas* y *vistazo general* y los *tableros*.

La sección problemas muestra los iniciadores que han cambiado el estado del host de *OK* a *PROBLEMA*. Inicialmente nos hemos centrado en los problemas de gravedad alta o superior. A medida que se vayan corriendo se irán abordando los problemas de niveles inferiores con el fin de mejorar los sistemas de información de la ADL.

La sección vistazo general permite comparar el estado de los iniciadores de un grupo de host.

Los tableros permiten agrupar información gráfica para poder monitorizar rápidamente la información más importante de un host. A diferencia de las secciones problemas y vistazo general que están implementadas en Zabbix de manera nativa, los tableros es necesario generarlos y adecuarlos a nuestras necesidades. En este sentido se han generado algunos tableros para monitorizar algunos hosts que se han considerado interesantes.

En las figuras siguientes se muestran aspectos de las secciones problemas y vistazo general y un par de tableros generados con la información gráfica generada. Se puede comprobar que es fácil detectar posibles problemas o errores con estas herramientas gráficas.

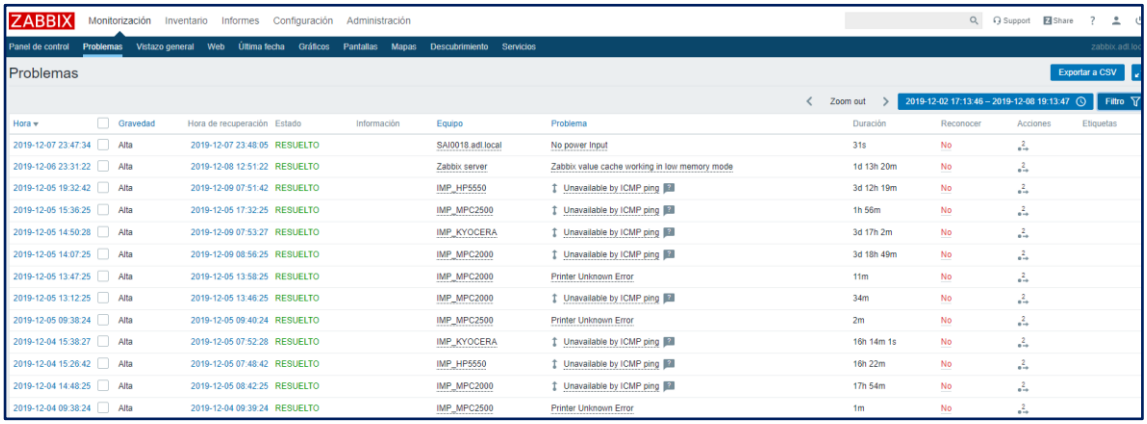


Figura 36. Cierre – Sección problemas

Figura 37. Cierre – Sección vistazo general

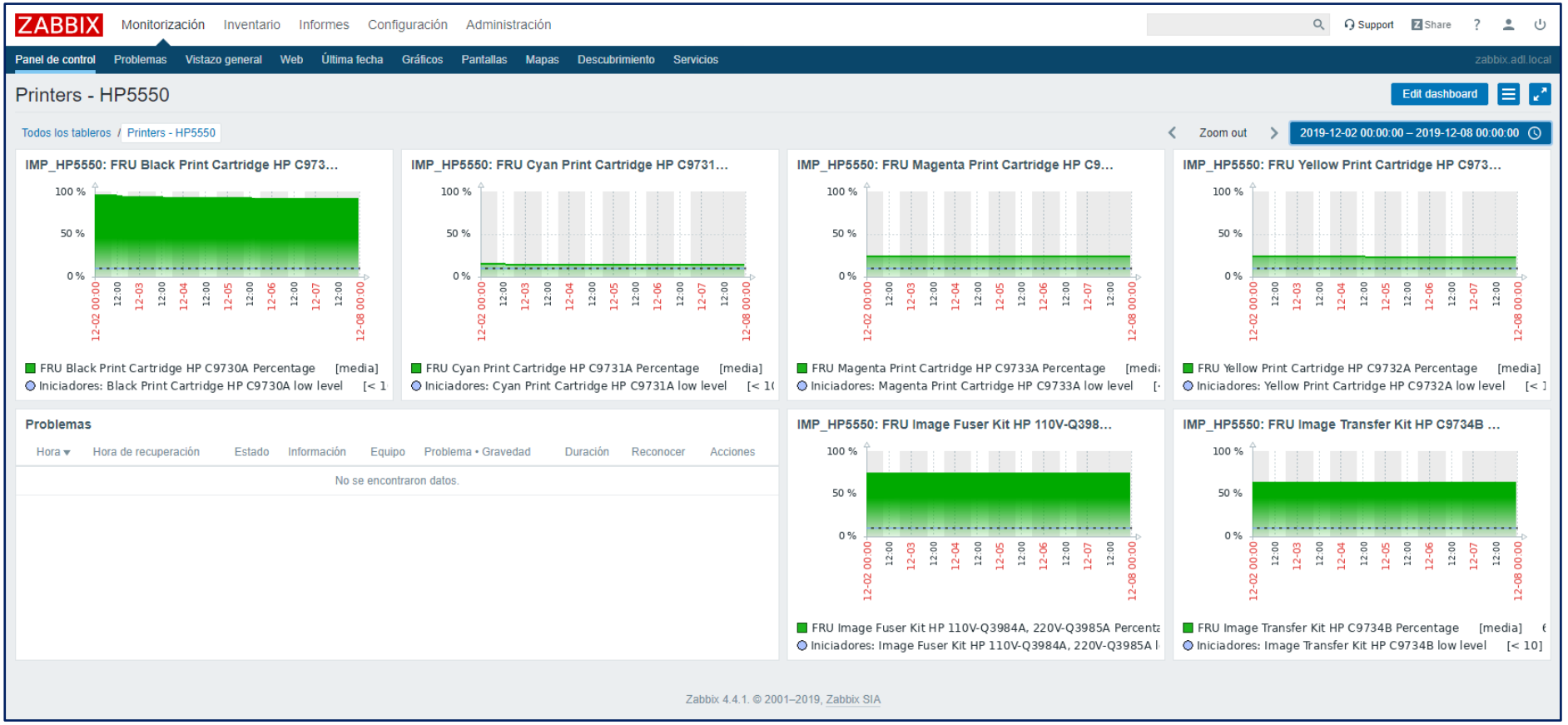


Figura 38. Cierre – Tablero impresora

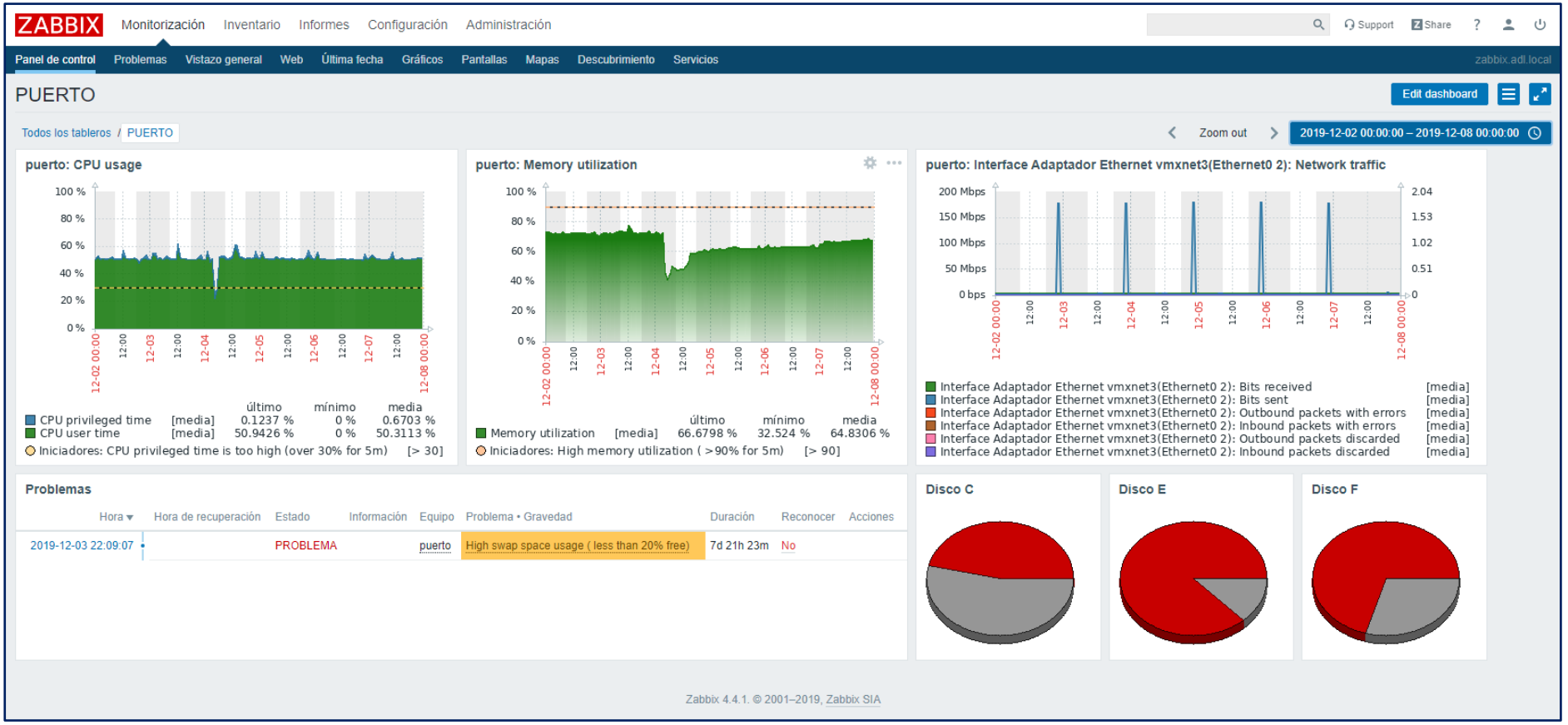


Figura 39. Cierre – Tablero servidor Windows

4.2 Análisis

La información que proporciona el sistema no sirve de nada si no se analiza y se actúa en consecuencia. Como se ha comentado anteriormente, el objetivo no es solucionar todos los problemas que se encuentren y olvidarse de la monitorización. Este debe ser un proceso continuo en el que el sistema implantado ayude a identificar posibles fallos y a mejorar el funcionamiento de la red de la ADL. Necesariamente por el tiempo limitado de duración de este TFG, es necesario centrarse en la resolución de algunos de los problemas que se detecten, abordando el resto progresivamente en el futuro inmediato.

En este ámbito, se exponen a continuación algunas de las deficiencias que se han detectado y que se han puesto de manifiesto gracias a la implantación del sistema de monitorización:

Alto nivel de utilización de la memoria

Se ha detectado que, durante periodos aleatorios de tiempo a lo largo del día, la utilización de la memoria del servidor que soporta los servicios externos de la ADL (sede web, correo, etc.) es superior al 90% durante más de 5 minutos seguidos, lo que provoca paginación del servidor y disminución del rendimiento.

Como el servidor que presenta estos problemas es una máquina virtual y existía memoria adicional en el hipervisor, se ha asignado más memoria a dicha máquina virtual, eliminándose el problema.

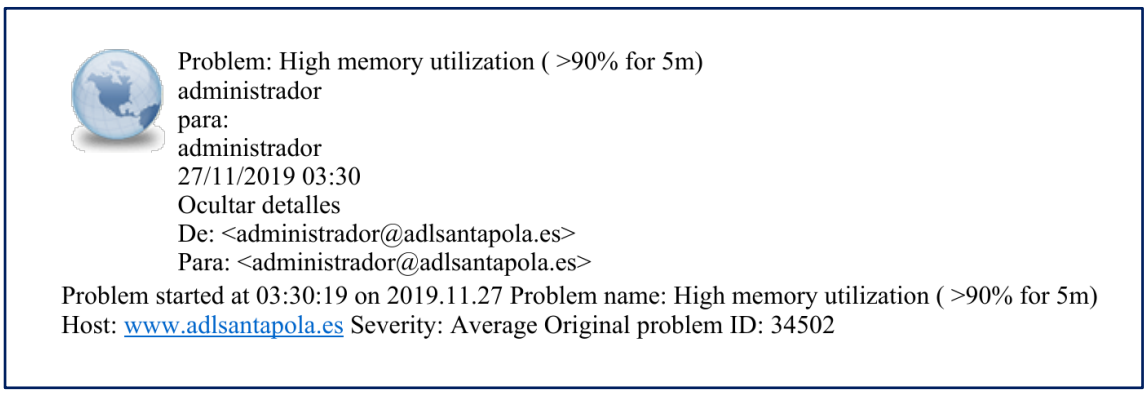
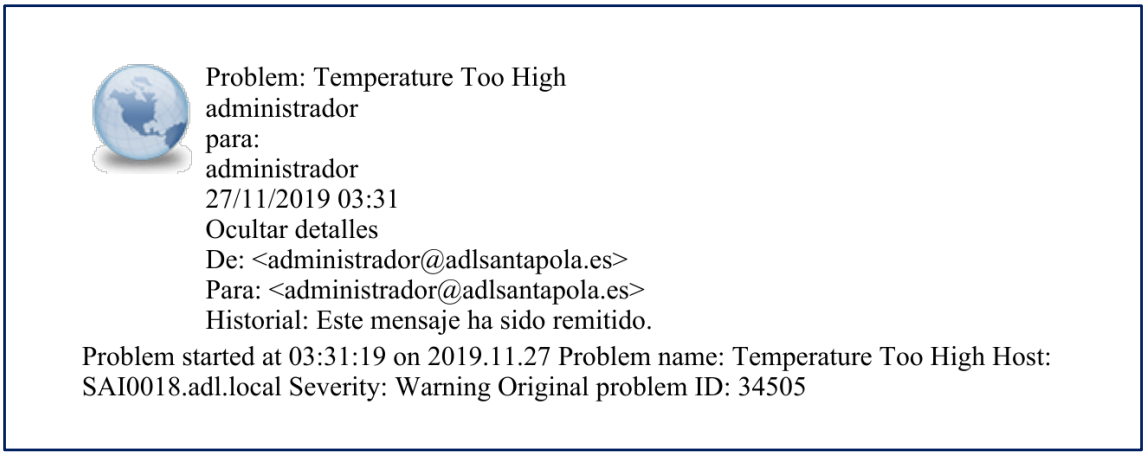


Figura 40. Cierre – High memory utilization

Alta temperatura del CPD

Algunos equipos del CPD de la sede principal reportan una temperatura alta durante algunos periodos del día. El hecho de que los equipos trabajen a una temperatura más alta de lo normal implica que sean más propensos a fallos de hardware y que se acorte su vida útil.

En este caso se ha optado por mejorar la ventilación del CPD eliminando un panel y se ha solicitado una revisión del sistema de refrigeración de la sala para que se compruebe el correcto funcionamiento del mismo.



Problem: Temperature Too High
administrador
para:
administrador
27/11/2019 03:31
Ocultar detalles
De: <administrador@adlsantapola.es>
Para: <administrador@adlsantapola.es>
Historial: Este mensaje ha sido remitido.

Problem started at 03:31:19 on 2019.11.27 Problem name: Temperature Too High Host: SAI0018.adl.local Severity: Warning Original problem ID: 34505

Figura 41. Cierre – Temperature too high

Fallo en sensor del tóner

Una de las impresoras generaba fallos aleatorios de impresión. Una vez que se ha podido monitorizar el equipo y se ha podido obtener gráficamente el estado de los consumibles se ha detectado que el error se debe a que no se mide correctamente el nivel de tinta amarilla. El nivel disminuye y aumenta aleatoriamente, aunque se reemplace el cartucho, lo que provoca los errores del equipo.

Con estos datos se ha podido demostrar que existe un problema con la medición del nivel de tinta y actuar en consecuencia, reportando el incidente al servicio técnico para su reparación.

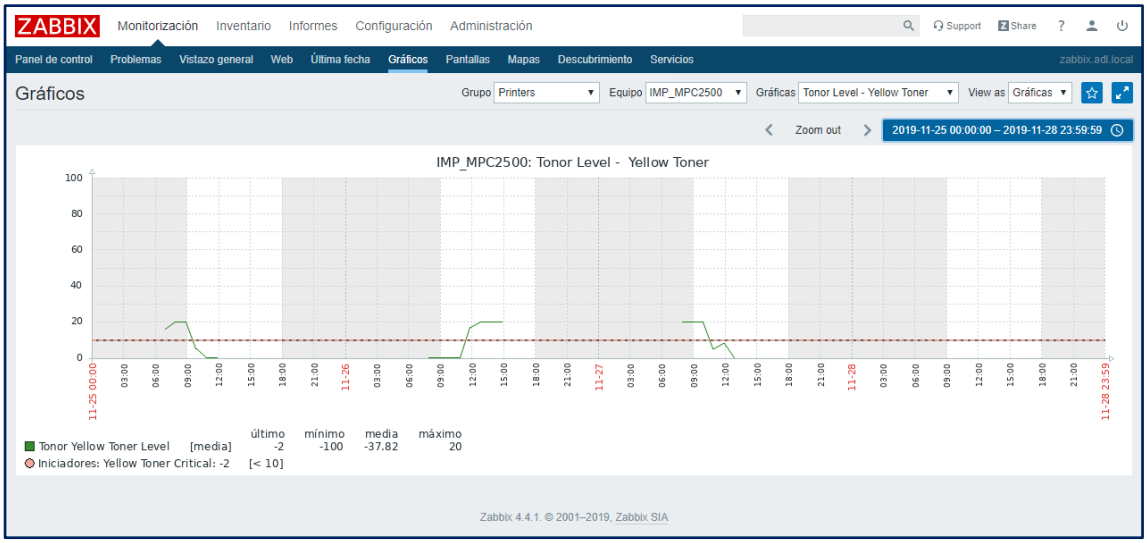


Figura 42. Cierre – Yellow toner level

Por otro lado, el análisis de la información proporcionada por el sistema también ha revelado que la monitorización de algunos aspectos de ciertos hosts no es correcta, dando falsos positivos o bien no obteniendo los datos que se desean. Generalmente esto es debido a la necesidad de ajustes en las plantillas utilizadas, o la que se ha deseado monitorizar una función no soportada.

Por ejemplo, ha sido necesario ajustar dos iniciadores de la plantilla HP RT3000 SNMP, que sirve de base para monitorizar los SAIs. Por defecto los iniciadores *InputVoltageLow* y *InputVoltageTooHigh* están definidos para que se activen si la tensión de entrada es <130V en el primer caso o >130V en el segundo, lo que provocaba falsos positivos continuamente. Se han ajustados estos valores a <210 y >240 respectivamente.

Un ejemplo de monitorización de funciones no soportadas sucede con los dispositivos Cisco ASA. La plantilla ASA Discovery hereda de la plantilla genérica SNMPv2 los monitores para la obtención de datos del funcionamiento de la CPU y la memoria, pero los OIDs definidos por la plantilla SNMPv2 no están implementados en los dispositivos Cisco ASA de la ADL y por lo tanto no pueden ser monitorizados.

También cabe destacar, que debido a las limitaciones de tiempo, no ha sido posible monitorizar aplicaciones que hubiera sido deseable como los servidores de base de datos MariaDB o los servidores Apache. Se han realizado algunas pruebas de configuración con las plantillas que proporciona Zabbix, pero no se ha obtenido ningún resultado, por lo que esta monitorización queda pendiente para realizarla una vez finalizado el TFG.

Así mismo sería deseable implantar algún canal adicional de envío de notificaciones como el envío de SMS para las notificaciones realmente graves y que no pueden esperar a ser atendidas.

Finalmente, queda pendiente la securización del entorno web Zabbix utilizando HTTPS mediante el uso del correspondiente certificado SSL y el puerto tcp/443.

En resumen, la fase de implantación de un sistema de monitorización en la ADL puede darse por concluida, habiendo conseguido un sistema estable y viable. En general, el sistema está funcionando adecuadamente y se está comenzando a obtener información valiosa tanto para corregir errores como para detectar tendencias. No obstante queda pendiente corregir algunos aspectos que no funcionan adecuadamente y ampliar las funcionalidades del sistema.

En este sentido el ciclo de vida del producto deberá seguir un proceso de mejora continua en el que el sistema se irá mejorando y ampliando de acuerdo a las necesidades de la ADL, con el fin de que siga proporcionando información útil.

5. Conclusiones

Este TFG nació con el objetivo de solucionar el problema que genera la creciente complejidad en las redes actuales, que hace que sean más difíciles de gestionar y se incremente la probabilidad de fallo. En la actualidad, las redes de comunicaciones son la columna vertebral sobre la que se construyen las relaciones entre los sistemas de información de las organizaciones. Cualquier problema, discontinuidad o disminución del rendimiento afecta al funcionamiento global de la organización, que se ve incapaz de cumplir sus objetivos y de atender a sus clientes (o a los ciudadanos en el caso de Administraciones Públicas). Por este motivo, detectar precozmente las tendencias que anticipen posibles problemas antes de que ocurran es crucial para poder prevenirlos y evitar la discontinuidad del negocio. Así mismo, se necesitan sistemas para reducir el tiempo de inactividad si, finalmente, el problema es inevitable y el sistema cae.

Con el fin de no realizar únicamente un estudio teórico sobre esta problemática, una parte de este TFG ha consistido en la gestión del proyecto de implantación de un sistema de monitorización para la gestión de la red de una Administración Pública. La metodología empleada para esta implantación está basada en la gestión de proyectos de PMBOK [4].

El trabajo ha quedado estructurado en cinco capítulos. En el primero de ellos se define y planifica tanto el TFG a nivel global como el proyecto de implantación, por lo que se puede hacer corresponder con las fases de Inicio y Planificación de PMBOK. En el capítulo 2 se realiza un estudio teórico de los fundamentos de los sistemas de monitorización. A lo largo del capítulo 3 se procede a la selección de la mejor suite de monitorización para las necesidades de la ADL y a su implantación. Este capítulo se entronca con la fase de Ejecución de PMBOOK. En el capítulo 4 se produce el cierre del proyecto de implantación, corresponde con la fase de cierre de PMBOOK y en ella el sistema de monitorización pasa a estado operativo. Finalmente, en este capítulo 5 se plasman las conclusiones del TFG a nivel global. Por lo tanto, parte del capítulo 1, el capítulo 3 y el 4 enteros tienen correspondencia con las distintas fases de la gestión de proyectos (la selección e implantación de un sistema de monitorización). Mientras que los capítulos 2 y 5 complementan esta implantación con el estudio teórico de los sistemas de monitorización y con las conclusiones finales, para conformar el TFG en su totalidad.

En general, se puede considerar que el objetivo principal del TFG se ha cumplido. Actualmente, la ADL de Santa Pola dispone de un sistema de monitorización operativo que está proporcionando información valiosa sobre el funcionamiento de la red. De hecho, tal y como se ha visto en el capítulo 4 ya se han comenzado a corregir algunos problemas que han sido detectados por el sistema.

Zabbix, la suite elegida como resultado el proceso de scoring, ha resultado sencilla de desplegar, no consume muchos recursos, incorpora plantillas que facilitan la monitorización de los dispositivos y proporciona herramientas

gráficas realmente útiles. Además, dispone de documentación suficiente y una comunidad activa que facilita su instalación y uso.

Sin embargo, hay que reconocer que no se ha podido monitorizar complemente todos los sistemas que se hubiera querido. Si bien, los equipos conectados a la red (servidores, electrónica de red, entorno de virtualización, etc.) se están monitorizando, no ha sido posible hacer lo mismo con las aplicaciones. Han quedado pendientes de monitorización, entre otros, los servidores de bases de datos (MariaDB) y los servidores HTTP (Apache). En el primero de los casos, ha sido imposible poner en marcha la monitorización. Zabbix dispone de plantillas para la monitorización de MySQL/MariaDB, pero aunque se ha seguido la documentación y se ha configurado el agente Zabbix en los servidores Linux y Windows donde residen los servidores de base de datos, no se ha logrado que dicho agente recopile los datos necesarios y los comunique al servidor Zabbix para su tratamiento. La monitorización de los servidores Apache ha quedado fuera por una cuestión temporal, ya que el desarrollo TFG debía finalizar y no ha quedado tiempo para configurarla.

Sobre el desarrollo temporal del proyecto, cabe decir que las primeras fases se han podido llevar a cabo de acuerdo a la planificación inicial. Sin embargo, la fase 3.1 (selección de la suite de monitorización) se ha alargado más de lo que se había previsto en un principio, obligando a deslizar las fases 3.2, 3.3 y 3.4 (instalación y puesta en marcha) y a reducir la fase 4 (cierre del proyecto de implantación) para poder encajar el desarrollo del proyecto.

El principal motivo de que la fase 3.1 se haya dilatado en el tiempo es que ha sido difícil, para algunas suites de monitorización, encontrar información útil y clara que permitiera conocer realmente sus características y funcionalidades. En algunos casos, en los sitios web oficiales se presentan las principales características del producto de forma general, pero no se profundiza.

Independientemente del proyecto de implantación, del que ya se ha hablado, el capítulo 2 se ha dedicado al estudio teórico de los fundamentos de los sistemas de monitorización. En general, este estudio ha servido personalmente para profundizar en los conocimientos que se tenían sobre protocolos como SNMP o frameworks como WMI, y que luego ha sido necesario utilizar en el despliegue de la solución. Por ejemplo, ha habido que configurar SNMP en varios dispositivos de red, decidir con qué versión se trabajaba o aprender a utilizar una herramienta como snmpwalk para comprobar si el protocolo estaba bien configurado y descubrir los OIDs que soporta cada dispositivo.

Cabe destacar que ha sorprendido que el mercado de herramientas de monitorización sea tan amplio y maduro, y que estas herramientas sean tan potentes y útiles. Como no puede ser de otra forma, las tradicionales versiones on-premise están dando paso a versiones on-cloud, lo que debe ser teniendo en cuenta para un futuro no muy lejano.

En este sentido, y de acuerdo a Prasad (2018) [16], algunas de las principales tendencias que están afectando al mercado de los sistemas de monitorización vienen marcadas por:

- Infraestructura dinámica: Los sistemas han dejado de ser estáticos, con pocas variaciones a lo largo del tiempo. Las redes actuales evolucionan mucho más rápido.
- Cloud: Existe una clara evolución a la computación en la nube, tanto por la necesidad de monitorizar sistemas de la organización que se han movido a la nube, como por la existencia de soluciones de monitorización SaaS.
- DevOps: La adopción de DevOps incrementa la necesidad de monitorizar la infraestructura de redes durante los ciclos de desarrollo y pruebas y no sólo en producción.
- IoT: La cantidad de dispositivos conectados a las redes de comunicaciones es cada vez es mayor y más diversa, lo que complica la monitorización.
- Heterogeneidad de los datos: Cada vez se mueven más datos y menos homogéneos por las redes de comunicaciones.

Estas tendencias marcan un incremento de la complejidad de la redes, lo que obliga a las organizaciones a utilizar varias herramientas para poder abarcar la mayor cantidad de dispositivos y datos a monitorizar. Una tendencia de los fabricantes de herramientas de monitorización es la de ofrecer más funcionalidades, como por ejemplo el análisis de logs, para reducir el número de herramientas de monitorización necesarias.

También es interesante observar que las tendencias citadas anteriormente están potenciando el uso de herramientas de Big Data. Estas herramientas son necesarias para el análisis e identificación de patrones en la gran cantidad de datos que se gestionan en las redes de comunicaciones actuales. Asimismo, también es más necesario el uso de herramientas basadas en IA para gestionar y adaptarse a la creciente complejidad de los entornos de comunicaciones y ser capaces de anticiparse rápidamente a los problemas antes de que sucedan.

En resumen, en este TFG se han estudiado los sistemas de monitorización de redes desde el punto de vista teórico y se ha llevado a cabo un proyecto de implantación de uno de ellos en la red física de la ADL de Santa Pola. Se ha sido capaz de conseguir que el sistema esté operativo, aunque ha quedado pendiente la monitorización de aplicaciones, ajustar los monitores que recopilan datos y diseñar un mayor número de gráficas y pantallas para mejorar la información obtenida del sistema.

Aunque el TFG termina aquí, se abren nuevas líneas de actuación. En primer lugar, el sistema de monitorización implantado se va a seguir explotando y mejorando siguiendo un ciclo PDCA (Plan – Do – Check – Act) [34]. Se debe estudiar la posibilidad de complementarlo con otros sistemas como, por ejemplo, herramientas de análisis de logs (Graylog [35]), de representación gráfica (Grafana [36]) o bien ampliar el sistema de alertas, entre otros. También, se debe seguir la evolución de estos sistemas hacia el entorno on-cloud y valorar si, en un momento dado, es necesario migrar de entorno.

6. Glosario

Best of breed

"*Lo mejor de cada casa*". Se aplica a la integración de soluciones de distintos fabricantes. Se elige la mejor aplicación para cada una de las funciones requeridas del sistema, en lugar de una aplicación estándar que las integre todas.

Big Data

Tecnología que permite el tratamiento masivo de datos provenientes de distintas fuentes, con el fin de descubrir patrones ocultos no apreciables con un tratamiento clásico e individualizado de los datos.

CPD

Centro de Proceso de Datos

Ciclo PDCA

Modelo de desarrollo de un producto o servicio basado en cuatro etapas (Planificar – Plan, Hacer – Do, Validar – Check, Actuar – Act). En la primera iteracción del proceso (Plan) se diseña el producto o se define el servicio, seguidamente se desarrollo o implementa (Do), a continuación se verifica que funciona adecuadamente (Check) y finalmente se evalúan los cambios necesarios para resolver las carencias o añadir nuevas funcionalidades (Act) y se vuelve al punto de inicio, generando un ciclo indefinido de mejora continua.

DevOps

Acrónimo de Development (Desarrollo) y Operations (Operaciones). Paradigma del desarrollo que propugna que los roles tradicionales en la ingeniería del software se coordinen para ofrecer mejores productos, en concreto entre los equipos de desarrollo y los de operaciones. El objetivo es conseguir desarrollar productos más rápidamente y con un alto nivel de calidad, siendo las demandas del mercado.

DMZ

Demilitarized Zone. Subred de una organización donde se ubican los servicios accesibles desde Internet.

FaaS

Function as a Service – Modelo de computación en la nube en el que se alquila un entorno que permite ejecutar funciones (no aplicaciones completas).

IA

Inteligencia Artificial.

IaaS

Infrastructure as a Service – Modelo de computación en la nube en el que se alquila hardware virtualizado o dedicado.

ICMP

Internet Control Message Protocol – Protocolo de la capa de red de la pila TCP/IP, utilizado para enviar mensajes de estado o error.

IoT

Internet of Things – Internet de las cosas. Se refiere a la gran cantidad de dispositivos, que no son ordenadores tradicionales, conectados a redes de comunicaciones (electrodomésticos, dispositivos de reconocimiento de voz, domótica, etc.)

ISO

International Organization for Standardization

MTBF

Mean Time Between Failunes – Tiempo medio entre fallos

MTTR

Mean Time To Repair – Tiempo medio para reparar

NAT

Network Address Translation – Protocolo de la pila TCP/IP utilizado para convertir las direcciones IP privadas de una organización en direcciones IP públicas.

OID

Object Identifier – Sistema se clasificación de objetos que asigna una referencia unívoca y jerárquica a cada uno.

On-cloud

Computación en la nube – Los sistemas de información no se ubican en las instalaciones del cliente, sino en DataCenters del proveedor, a los que se accede a través de redes de comunicaciones.

On-premise

Computación en local – Los sistemas de información están ubicados físicamente en las instalaciones del cliente.

OSI

Open System Interconnection – Estándar teórico que define la comunicación entre dispositivos de red, basándose en un sistema de capas.

PaaS

Platform as a Service – Modelo de computación en la nube en el que se alquila un entorno para desarrollar y publicar aplicaciones completas.

PHP

Lenguaje de programación, utilizado habitualmente para el desarrollo de sitios web dinámicos.

PMBOK

Estándar para la gestión de proyectos del PMI (Project Management Institute)

QoS

Quality of Service – Protocolo de la pila TCP/IP que permite discriminar el tráfico de una red, priorizando determinados tipos de comunicación.

SaaS

Software as a Service – Modelo de computación en la nube en el que se alquila el uso de una aplicación sin necesidad de tener que instalarla en las instalaciones del cliente.

SAI

Sistema de Alimentación Ininterrumpida

SLA

Service Level Agreement – Acuerdo de Nivel de Servicio

SNMP

Simple Network Management Protocol – Protocolo de la pila TCP/IP para la monitorización de equipos conectados a una red.

SQL

Structured Query Language

Switch capa 2

Dispositivo de red sin capacidad de enrutado, sólo es capaz de gestionar la capa de red (capa 2) de la pila TCP/IP.

Switch capa 3

Dispositivo de red con capacidad de enrutado, es capaz de gestionar la capa de red (capa 2) y la capa de transporte (capa 3) de la pila TCP/IP

TCP/IP

Modelo de protocolo para la comunicación de dispositivos en cuatro capas (física, red, transporte y aplicación). Es el estándar actual para interconectar dispositivos y es el protocolo base de Internet.

VLAN

Virtual LAN – Protocolo que permite realizar un marcado de tramas con el fin de conseguir que coexistan varias redes lógicas en la misma red física.

VPN

Virtual Private Network – Sistema que, en combinación con la criptografía, permite interconectar de forma segura redes privadas alejadas geográficamente a través de una red pública (por ejemplo Internet).

WMI

Windows Management Instrumentation - Estándar para la gestión de los sistemas Microsoft.

XML

eXtensible Markup Language – Formato textual basado en etiquetas para el intercambio de datos entre ordenadores.

7. Bibliografía

[1] “Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas”, en https://www.boe.es/eli/es/l/2015/10/01/39/con Última consulta: 28 de septiembre de 2019.

[2] “Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica”, en https://www.boe.es/eli/es/rd/2010/01/08/3/con Última consulta: 28 de septiembre de 2019.

[3] RODRIGUEZ, José Ramón (2014): *La gestión de proyectos. Conceptos básicos*, Barcelona: FUOC, pags. 20-24

[4] “PMBOK® Guide and Standards”, en https://www.pmi.org/pmbok-guide-standards Última consulta: 30 de octubre de 2019.

[5] “ISO 35,100 - Open Systems Interconnection (OSI)”, en https://www.iso.org/ics/35.100/x/ Última consulta: 6 de octubre de 2019.

[6] NUANGJAMNONG, C. MAJ, S.P. y VEAL, D. (2008): "The OSI network management model - capacity and performance management" en *4th IEEE International Conference on Management of Innovation and Technology, Bangkok*, págs. 1266-1270.

[7] RAO, Umesh Hodeghatta y MOHAPATRA, Sanjay (2010): "Deploying network management solutions in enterprises" en *INC2010: 6th International Conference on Networked Computing, Gyeongju*, págs. 1-2.

[8] TORREL, Wendy y AVELAR, Victor (2004): “Mean Time Between Failure: Explanation and Standards”, en https://www.researchgate.net/publication/251895269_Mean_Time_Between_Failure_Explanation_and_Standards Última consulta: 6 de octubre de 2019.

[9] ROHANI, Hoda y ROOSTA, Azad Kamali: “Calculating Total System Availability”, en https://www.delaat.net/rp/2013-2014/p17/report.pdf Última consulta 6 de octubre de 2019.

[10] GORALSKI, Walter (2008): “*The Illustrated Network: How TCP/IP Works in a Modern Network*”, Londres: Morgan, pags. 609-630.

[11] LOSHIN, Peter (2003): *“TCP/IP Clearly Explained”,* San Francisco: Morgan Kaufmann, pags. 643-655.

[12] “Windows Management Instrumentation“, en https://docs.microsoft.com/es-es/windows/win32/wmisdk/wmi-start-page Última consulta: 15 de octubre de 2019

[13] “Win32_LogicalDisk class“, en https://docs.microsoft.com/en-us/windows/win32/cimwin32prov/win32-logicaldisk Última consulta: 15 de octubre de 2019

[14] SOMERS, F. (1996): "Hybrid: unifying centralised and distributed network management using intelligent agents" en *NOMS '96 - IEEE Network Operations and Management Symposium,* Kyoto, Japón, págs. 34-43

[15] PRASAD, Pankaj (2017): “IT Infrastructure Monitoring Tools: Select a Suite Over Best of Breed”, en Gartner Research (www.gartner.com)

[16] PRASAD, Pankaj (2018): “Market Guide for IT Infrastructure Monitoring Tools”, en Gartner Research (www.gartner.com)

[17] “Nagios XI Enterprise Server and Network Monitoring Software”, en https://www.nagios.com/products/nagios-xi/#systemreqs Última consulta: 21 de octubre de 2019

[18] “Nagios XI // Core Feature Comparison”, en https://assets.nagios.com/handouts/nagiosxi/Nagios-XI-vs-Nagios-Core-Feature-Comparison.pdf Última consulta: 21 de octubre de 2019.

[19] “OpManager - System Requirements”, en https://www.manageengine.com/network-monitoring/help/hardware-and-software-requirements.html Última consulta: 21 de octubre de 2019.

[20] “OpManager - Editions and Pricing”, en https://www.manageengine.com/network-monitoring/opmanager-editions.html?btmMenu Última consulta: 21 de octubre de 2019.

[21] “System Requirements | OP5”, en https://www.op5.com/system-requirements Última consulta: 22 de octubre de 2019.

[22] “Features Archive | OP5”, en https://www.op5.com/features Última consulta: 22 de octubre de 2019.

[23] “Pandora: Documentation es: Instalacion”, en https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Instalacion Última consulta: 22 de octubre de 2019.

[24] “Análisis de Funcionalidades”, en https://pandorafms.com/downloads/PDF/funcionalidades_DEF_ES.pdf Última consulta: 22 de octubre de 2019.

[25] “NPM Datasheet”, en https://www.solarwinds.com/-/media/solarwinds/swdcv2/licensed-products/network-performance-monitor/resources/datasheets/npm-datasheet.ashx Última consulta: 22 de octubre de 2019.

[26] “2 Requirements [Zabbix Documentation 4.4]”, en https://www.zabbix.com/documentation/current/manual/installation/requirements Última consulta: 22 de octubre de 2019.

[27] “Zabbix features overview”, en https://www.zabbix.com/features Última consulta: 22 de octubre de 2019.

[28] “Azure Monitor overview | Microsoft Docs”, en https://docs.microsoft.com/en-us/azure/azure-monitor/overview Última consulta: 22 de octubre de 2019.

[29] RODRIGUEZ, José Ramón y JOANA, José María (2011): *Implantación de sistemas de información de empresas*, Barcelona: FUOC, pags. 25-32

[30] “Zabbix Documentation 4.4”, en https://www.zabbix.com/documentation/4.4/manual Última consulta: 27 de noviembre de 2019.

[31] “CentOS Product Specifications”, en https://wiki.centos.org/About/Product Última consulta: 29 de noviembre de 2019.

[32] “PHP: Supported Versions”, en https://www.php.net/supported-versions.php Última consulta: 29 de noviembre de 2019.

[33] “MariaDB: Maintenance Policy”, en https://mariadb.org/about/maintenance-policy Última consulta: 29 de noviembre de 2019.

[34] MOEN, Ronald y NORMAN, Clifford (2009): “Evolution of the PDCA cycle”, en http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.5465&rep=rep1&type=pdf Última consulta: 21 de diciembre de 2019.

[35] “Graylog”, en https://www.graylog.org Última consulta: 21 de diciembre de 2019.

[36] “Grafana”, en https://grafana.com Última consulta: 21 de diciembre de 2019.

[37] “Unix Toolbox”, en http://cb.vu/unixtoolbox.xhtml#shells Última consulta: 20 de noviembre de 2019.

[38] “Zabbix Share – Cisco ASA Discovery”, en https://share.zabbix.com/network_devices/cisco/cisco-asa-discovery Última consulta: 4 de diciembre de 2019.

[39] “Zabbix Share – HP UPS SNMP (R5000)”, en https://share.zabbix.com/power-ups/hp-ups-snmp-r5000 Última consulta: 4 de diciembre de 2019.

[40] “Zabbix Share – Template Ricoh SNMP Printers”, en https://share.zabbix.com/printers/ricoh/template-ricoh-snmp-printers Última consulta: 4 de diciembre de 2019.

[41] “Zabbix Share – HP Color Laserjet”, en https://share.zabbix.com/printers/hp/hp-color-laserjet Última consulta: 4 de diciembre de 2019.

[42] “Zabbix Share – Kyocera Devices (use snmp v2)”, en https://share.zabbix.com/printers/kyocera/kyocera-devices-use-snmp-v2 Última consulta: 5 de diciembre de 2019.

[43] “Zabbix Share – Generic printers monitoring template (Any brand), en ”https://share.zabbix.com/printers/generic-printers-monitoring-template-any-brand Ultima consulta: 5 de diciembre de 2019.

[44] “Download Zabbix agents”, en https://www.zabbix.com/download_agents Ultima consulta: 5 de diciembre de 2019.

[45] SUAREZ, Luis Carlos (2015): “Monitorizar vmware con Zabbix”, en http://wiki.intrusos.info/doku.php/seguridad:monitorizacion:zabbix2:vmware Última consulta: 7 de diciembre de 2019.

8. Tablas

[Tabla 1] Desglose temporal del TFG en fases y tareas. Elaboración propia.

[Tabla 2] Equivalencias entre disponibilidad y tiempo anual de inactividad. Elaboración propia.

[Tabla 3] Comandos SNMP versión 1. Elaboración propia.

[Tabla 4] Comandos SNMP versión 2, adicionales a los existentes en la versión 1. Elaboración propia.

[Tabla 5] Comparativa de las características de los sistemas de monitorización centralizados y distribuidos. Elaboración propia.

[Tabla 6] Procedimiento de scoring para la selección del sistema de monitorización más adecuado para la ADL. Elaboración propia.

[Tabla 7] Listado de equipos de la ADL que se monitorizan mediante SNMP. Elaboración propia.

[Tabla 8] Listado de equipos de la ADL que se monitorizan mediante agentes Zabbix. Elaboración propia.

9. Figuras

[Figura 1] “Medidas de seguridad recogidas en el ENS”, recuperado de https://www.ccn-cert.cni.es/ens.html. Última consulta: 18 de diciembre de 2019.

[Figura 2] RODRIGUEZ, José Ramón (2014): La gestión de proyectos. Conceptos básicos, Barcelona: FUOC, pag. 20.

[Figura 3] Diagrama de Gantt de la planificación del TFG. Elaboración propia.

[Figura 4] Offnfopt (2015): “Diagram of OSI model”, recuperado de https://commons.wikimedia.org/wiki/File:OSI_Model_v1.svg. Última consulta: 18 de diciembre de 2019.

[Figura 5] Diagrama funcional de un sistema de monitorización de redes. Elaboración propia.

[Figura 6] BELLIZI, An. (2017): “Snmp-interaction v1.1”, recuperado de https://commons.wikimedia.org/wiki/File:Snmp-interaction_v1.1.png Última consulta: 14 de octubre de 2019.

[Figura 7] MÜLLER, Stefan (2006): “Der Standard-SNMP-MIB-Baum”, recuperado de https://commons.wikimedia.org/wiki/File:SNMP.MIB-Tree.PNG Última consulta: 14 de octubre de 2019.

[Figura 8] “WMI Architecture”, recuperado de https://docs.microsoft.com/en-us/windows/win32/wmisdk/images/wmi-architecture.png Última consulta: 29 de octubre de 2019.

[Figura 9] “Nagios Core - Comprehensive Monitoring”, recuperado de https://www.nagios.com/wp-content/uploads/2016/02/xComprehensive_Monitoring_Drop2-255x170.jpg.pagespeed.ic.-a3qbhoYK4.jpg Última consulta: 18 de diciembre de 2019.

[Figura 10] “OPManager - Server monitoring”, recuperado de https://www.manageengine.com/network-monitoring/images/v1/opmanager-central-snapshot.png Última consulta: 18 de diciembre de 2019.

[Figura 11] “OP5 Monitor”, recuperado de https://cdn.op5.com/wp-content/themes/op5-theme/assets/images/op5-monitor-v1/op5-monitor-screens-4.png Última consulta: 18 de diciembre de 2019.

[Figura 12] “PandoraFMS - Tactical screen (Welcome)”, recuperado de https://pandorafms.org/wp-content/uploads/2016/06/pandora6.0sp3-tactical-view.png Última consulta: 18 de diciembre de 2019.

[Figura 13] “Network Performance Monitoring Summary”, recuperado de https://www.solarwinds.com/-/media/solarwinds/swdcv2/licensed-products/network-performance-monitor/images/product-screenshots/npm-network-summary.a

shx?rev=afa5cd679d8046238b8396b0752cf55e Última consulta: 18 de diciembre de 2019.

[Figura 14] “Zabbix - Monitoring Dashboard”, recuperado de https://assets.zabbix.com/img/screenshots/4.2/dashboard.png Última consulta: 18 de diciembre de 2019

[Figura 15] “Azure Monitor – Overview”, recuperado de https://docs.microsoft.com/en-us/azure/azure-monitor/media/overview/solutions-overview.png Última consulta: 18 de diciembre de 2019

[Figura 16] Diagrama lógico red ADL. Elaboración propia.

[Figura 17] Estrategia de despliegue Zabbix. Elaboración propia.

[Figura 18] Captura de pantalla comando snmpwalk. Elaboración propia.

[Figura 19] Captura de pantalla de la instalación Zabbix en la ADL. Grupo de hosts Network devices. Elaboración propia.

[Figura 20] Captura de pantalla de la instalación Zabbix en la ADL. Grupo de hosts Network devices. Elaboración propia.

[Figura 21] Captura de pantalla de la instalación Zabbix en la ADL. Grupo de hosts UPS. Elaboración propia.

[Figura 22] Captura de pantalla de la instalación Zabbix en la ADL. Grupo de hosts Printers. Elaboración propia.

[Figura 23] Captura de pantalla de la instalación Zabbix en la ADL. Grupo de hosts Linux servers. Elaboración propia.

[Figura 24] Captura de pantalla de la instalación Zabbix en la ADL. Grupo de hosts Windows servers. Elaboración propia.

[Figura 25] Captura de pantalla de la instalación Zabbix en la ADL. Descubrimiento de máquinas virtuales VMWare. Elaboración propia.

[Figura 26] Captura de pantalla de la instalación Zabbix en la ADL. Descubrimiento de hipervisores VMWare. Elaboración propia.

[Figura 27] Captura de pantalla de la instalación Zabbix en la ADL. Mapa de la red ADL en Zabbix. Elaboración propia.

[Figura 28] Captura de pantalla de la instalación Zabbix en la ADL. Ejemplo de alerta mediante email desencadenada por la falta de respuesta ICMP de un host. Elaboración propia.

[Figura 29] Captura de pantalla del informe de disponibilidad del agente Zabbix para servidores Linux durante la semana del 25 de noviembre al 1 de diciembre. Elaboración propia.

[Figura 30] Captura de pantalla del informe de disponibilidad del agente Zabbix para servidores Windows durante la semana del 25 de noviembre al 1 de diciembre. Elaboración propia.

[Figura 31] Captura de pantalla del informe de disponibilidad de los dispositivos de red durante la semana del 25 de noviembre al 1 de diciembre. Elaboración propia.

[Figura 32] Captura de pantalla del informe de disponibilidad de los dispositivos Cisco ASA durante la semana del 25 de noviembre al 1 de diciembre. Elaboración propia.

[Figura 33] Captura de pantalla del gráfico de la utilización de la memoria del servidor Zabbix durante la semana del 25 de noviembre al 1 de diciembre. Elaboración propia.

[Figura 34] Captura de pantalla del gráfico de la utilización de la CPU del servidor Zabbix durante la semana del 25 de noviembre al 1 de diciembre. Elaboración propia.

[Figura 35] Captura de pantalla del gráfico de la utilización del disco del servidor Zabbix durante la semana del 25 de noviembre al 1 de diciembre. Elaboración propia.

[Figura 36] Captura de pantalla de una parte de sección problemas durante la semana del 2 al 8 de diciembre. Elaboración propia.

[Figura 37] Captura de pantalla de una parte de la sección vistazo general para los servidores Windows durante la semana del 2 al 8 de diciembre. Elaboración propia.

[Figura 38] Captura de pantalla del tablero elaborado para la impresora HP5550 con datos de la semana del 2 al 8 de diciembre. Elaboración propia.

[Figura 39] Captura de pantalla del tablero elaborado para el servidor Windows puerto.adl.local con datos de la semana del 2 al 8 de diciembre. Elaboración propia.

[Figura 40] Email de error reportado por Zabbix para el host www.adlsantapola.es debido a una utilización de memoria superior al 90% durante más de 5 minutos. Elaboración propia.

[Figura 41] Email de error reportado por Zabbix para el host SAI0018.adl.local debido al aumento de la temperatura del equipo. Elaboración propia.

[Figura 42] Captura de pantalla de la gráfica del nivel de tinta amarilla de la impresora MPC2500 durante el periodo del 25 al 28 de noviembre. Elaboración propia.

[Figura 43] Captura de pantalla de la configuración SNMP en la impresora HP5550. Elaboración propia.

[Figura 44] Captura de pantalla de la configuración SNMP en la impresora Nashuatec MPC2500. Elaboración propia.

[Figura 45] Captura de pantalla de la configuración SNMP en la impresora Kyocera 2551. Elaboración propia.

[Figura 46] Captura de pantalla de la configuración SNMP en el SAI HP RT3000. Elaboración propia.

[Figura 47] Captura de pantalla de los parámetros de la máquina virtual creada en el hipervisor VMWare para albergar el servidor Zabbix. Elaboración propia.

[Figura 48] Captura de pantalla del esquema de particionado del servidor CentOS para albergar el servidor Zabbix. Elaboración propia.

[Figura 49] “Manual:installation:install_1.png”, recuperado de https://www.zabbix.com/documentation/4.4/_detail/manual/installation/install_1.png Última consulta: 22 de noviembre de 2019.

[Figura 50] “Manual:installation:install_2.png”, recuperado de https://www.zabbix.com/documentation/4.4/_detail/manual/installation/install_2.png Última consulta: 22 de noviembre de 2019.

[Figura 51] “Manual:installation:install_3.png”, recuperado de https://www.zabbix.com/documentation/4.4/_detail/manual/installation/install_3.png Última consulta: 22 de noviembre de 2019.

[Figura 52] “Manual:installation:install_4.png”, recuperado de https://www.zabbix.com/documentation/4.4/_detail/manual/installation/install_4.png Última consulta: 22 de noviembre de 2019.

[Figura 53] “Manual:installation:install_5.png”, recuperado de https://www.zabbix.com/documentation/4.4/_detail/manual/installation/install_5.png Última consulta: 22 de noviembre de 2019.

[Figura 54] “Manual:installation:install_6.png”, recuperado de https://www.zabbix.com/documentation/4.4/_detail/manual/installation/install_6.png Última consulta: 22 de noviembre de 2019.

[Figura 55] “Manual:installation:install_7.png”, recuperado de https://www.zabbix.com/documentation/4.4/_detail/manual/installation/install_7.png Última consulta: 22 de noviembre de 2019.

[Figura 56] Captura de pantalla de la configuración de la macro {$SNMP_COMMUNITY} de la plantilla Cisco ASA Discovery en el Frontend Zabbix. Elaboración propia.

[Figura 57] Captura de pantalla de la instalación del agente Zabbix para Windows 64 bits - Presentación. Elaboración propia.

[Figura 58] Captura de pantalla de la instalación del agente Zabbix para Windows 64 bits - Licencia. Elaboración propia.

[Figura 59] Captura de pantalla de la instalación del agente Zabbix para Windows 64 bits – Configuración del servicio. Elaboración propia.

[Figura 60] Captura de pantalla de la instalación del agente Zabbix para Windows 64 bits – Selección de componentes. Elaboración propia.

[Figura 61] Captura de pantalla de la instalación del agente Zabbix para Windows 64 bits – Instalación. Elaboración propia.

[Figura 62] Captura de pantalla de la configuración de las macros para el descubrimiento de la infraestructura de virtualización en el Frontend Zabbix. Elaboración propia.

[Figura 63] Captura de pantalla de los hipervisores definidos en el Frontend de Zabbix para el descubrimiento de la infraestructura de virtualización de la ADL. Elaboración propia.

10. Anexos

10.1 Configuración SNMP

La configuración de SNMP no es uniforme, en algunos equipos se realiza a través de una interfaz gráfica mediante un navegador, mientras que en otros se realiza mediante interfaz de comandos.

Impresoras HP

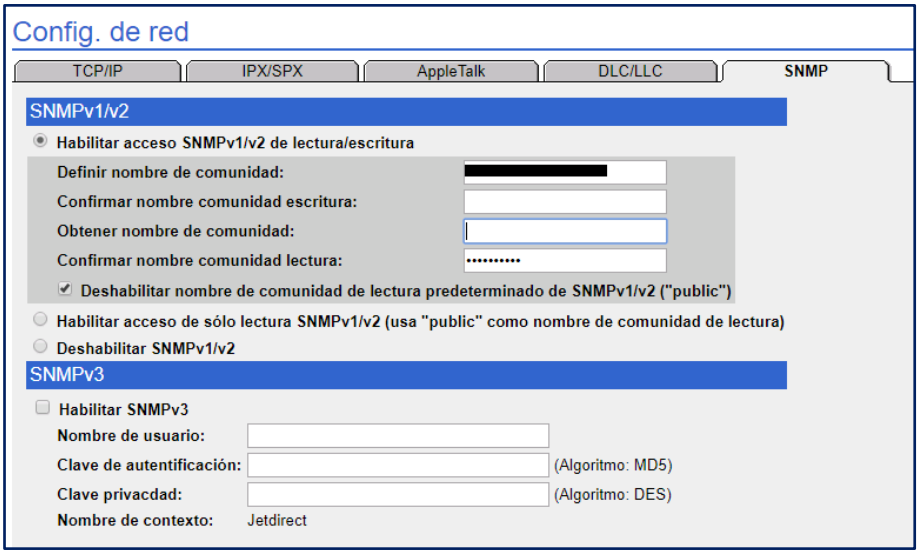


Figura 43. Configuración SNMP - Impresoras HP

Impresoras Nashuatec

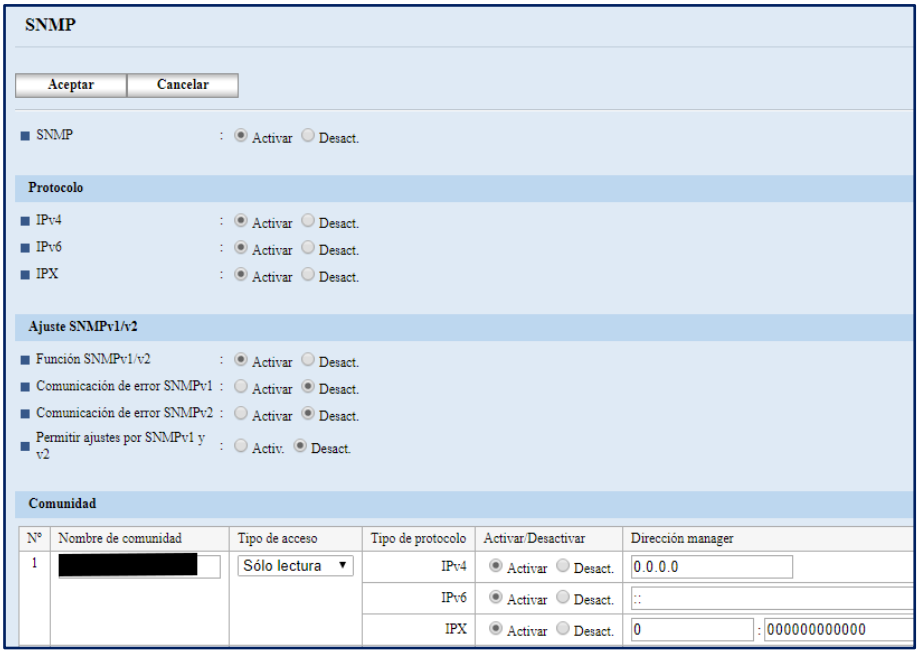


Figura 44. Configuración SNMP - Impresoras Nashuatec

Impresoras Kyocera

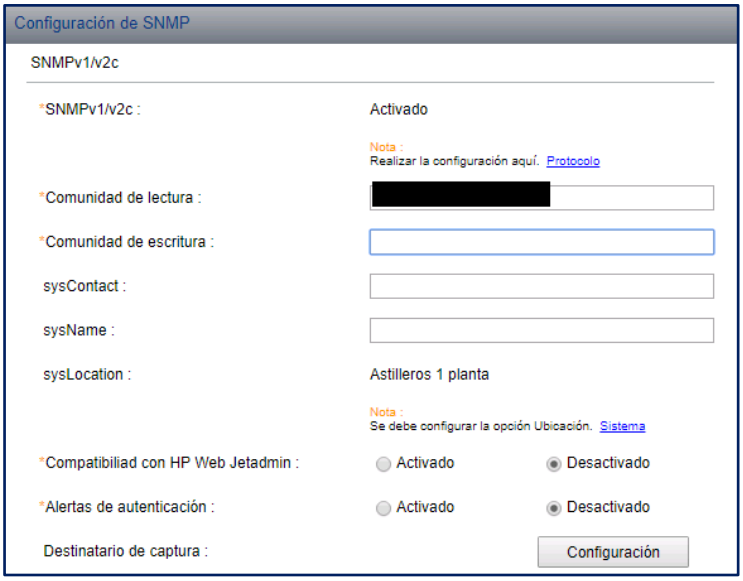


Figura 45. Configuración SNMP - Impresoras Kyocera

SAIs HP

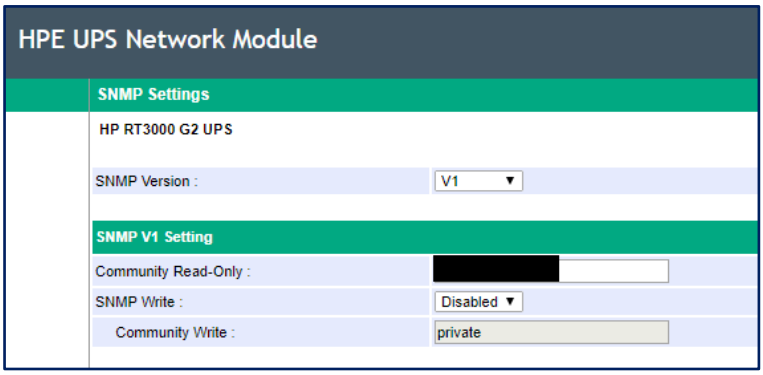


Figura 46. Configuración SNMP - SAIs HP

Switches y routers Cisco

En este caso es necesario realizar la configuración a través de consola. Los comandos necesarios para la configuración son los siguientes:

```
enable
configure terminal
snmp-server community <<comunidad>> RO
snmp-server location Astilleros
snmp-server contact ADL Santa Pola
```

Cisco ASA

La configuración se realiza mediante interfaz de comandos. En este caso, se ha restringido el acceso a las consultas SNMP a un único host (el servidor Zabbix):

```
enable
configure terminal
snmp-server host Management <<IP servidor Zabbix>> poll
community <<comunidad>> version 2c
snmp-server Astilleros
snmp-server ADL Santa Pola
snmp-server community <<comunidad>>
```

10.2 Instalación CentOS 7

En primer lugar se debe crear una máquina virtual en el hipervisor VMWare. Los parámetros de configuración son los siguientes:

- CPU: 1
- Memoria RAM: 1 Gbyte
- Disco duro: 20 Gbytes
- Adaptador de red: Único, conectado a la VLAN de servidores

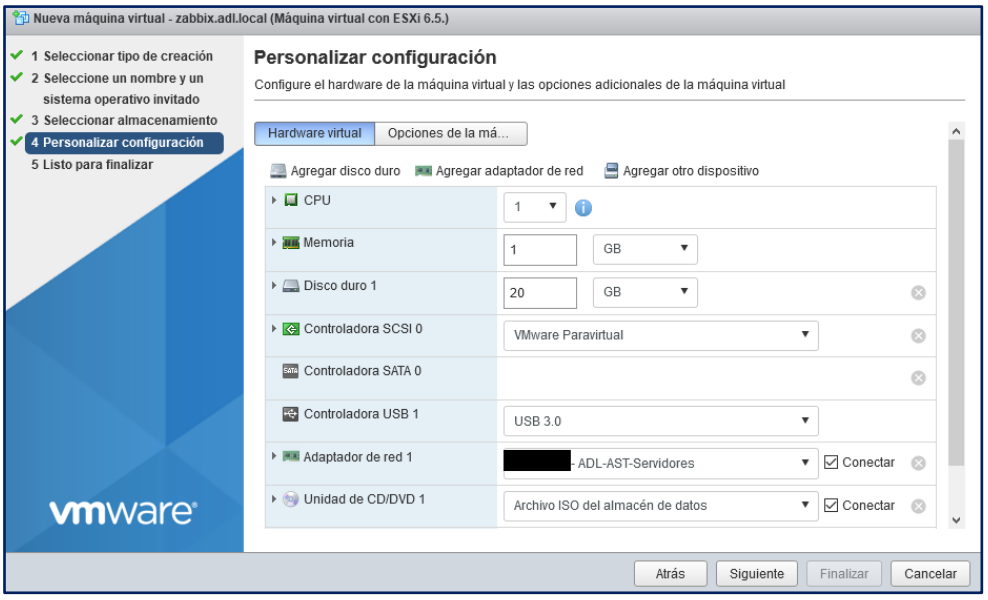


Figura 47. Configuración CentOS – Máquina virtual

Como nombre de la máquina se ha elegido zabbix.adl.local, y se ha creado un registro A en el servidor DNS interno de la ADL, de tal forma que zabbix.adl.local apunta a la IP elegida para el servidor Zabbix.

A continuación se instala CentOS en la máquina virtual creada, utilizando la imagen "*Minimal*" (CentOS-7-x86_64-Minimal-1908.iso) descargada desde uno de los servidores espejo (http://isoredirect.centos.org/centos/7/isos/x86_64/). El instalador de CentOS, Anaconda, proporciona un interfaz gráfico para la instalación básica.

El esquema de particionado elegido ha sido el siguiente:

- /boot : partición estándar xfs 512 Mbytes
- / : partición estándar xfs 17,5 Gbytes
- swap : 2 Gbytes

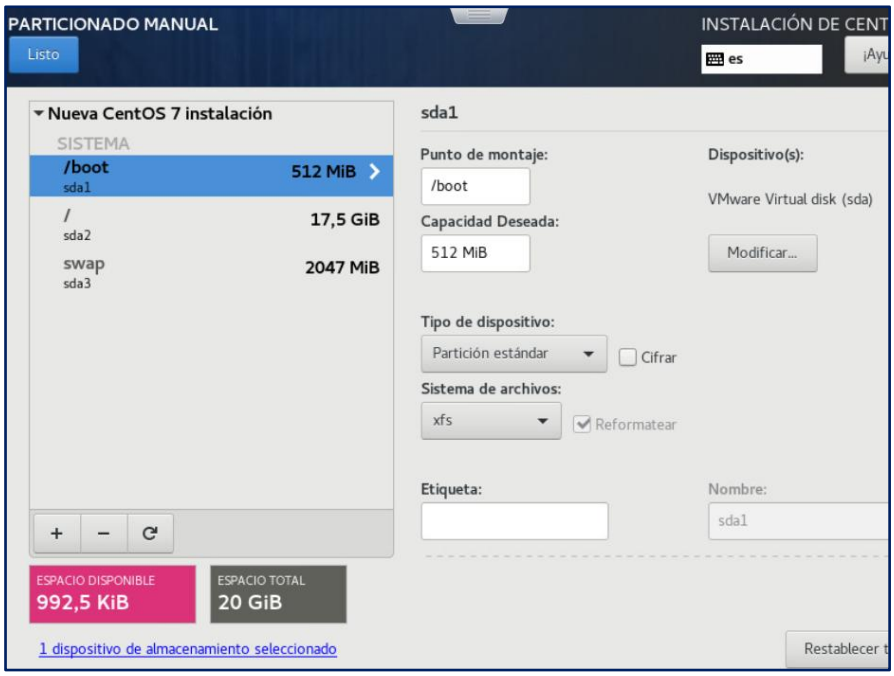


Figura 48. Configuración CentOS – Particionado

Una vez hecha la instalación mínima de CentOS, se comprueba desde la consola que la red esté operativa y se elimina el servicio NetworkManager:

```
yum remove NetworkManager
vi /etc/sysconfig/network-scripts/ifcfg-ens192
        Añadir el parámetro NM_CONTROLLED=no
        Configurar el parámetro ONBOOT=yes
systemctl restart network.service
```

Una vez configurada la red y comprobado que se puede acceder mediante SSH, se finaliza la configuración del sistema desde la línea de comandos. Se detalla a continuación:

Paquetes base

```
yum install wget vim net-tools deltarpm
```

Deshabilitar selinux

```
vim /etc/selinux/config
```

Cambiar `SELINUX=enforcing` por `SELINUX=disabled`

Deshabilitar tuned

```
systemctl disable tuned.service
```

Sincronización de tiempo

```
yum install ntp
systemctl enable ntpd
```

Repositorios EPEL

```
cd /tmp
wget
http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-
release-7-12.noarch.rpm
rpm –i epel-release-7-12.noarch.rpm
rm epel-release-7-12.noarch.rpm
```

Paquetes adicionales

```
yum install cmake gcc gcc-c++ unzip autoconf automake libtool
rpm-build cabextract ttmkfdir flex bison kernel-devel kernel-
headers yum-utils mlocate autofs rsync nail eject ntfs-3g gvfs
traceroute
```

VMWare tolos

```
yum install open-vm-tools open-vn-tools-desktop
systemctl enable vmtoolsd
systemctl start vmtoolsd
```

Personalizar el prompt [37]

```
touch /etc/profile.d/nice-prompt.sh
vim /etc/profile.d/nice-prompt.sh
```

Agregar las siguientes líneas

```
# Set a nice prompt like [user@host]/path/todir>
PS1="\[\033[1;30m\][\[\033[1;34m\]\u\[\033[1;30m\]"
PS1="$PS1@\[\033[0;33m\]\h\[\033[1;30m\]]\[\033[0;37m\]"
PS1="$PS1\w\[\033[1;30m\]>\[\033[0m\]"
```

Actualizar y reiniciar

```
yum update
reboot
```

10.3 Instalación requisitos adicionales

El siguiente paso es instalar Apache, php y mariaDB, requisitos indispensables para Zabbix. También se va a instalar y configurar nmap, ya que se utiliza en los mapas para descubrir el sistema operativo de un host.

En la instalación mínima de CentOS realizada en el Anexo 9.2 se instala MariaDB versión 5.5 por defecto. Para actualizarla a la versión 10.4 es necesario activar el repositorio que se puede obtener de la página https://downloads.mariadb.org/mariadb/repositories, seleccionando CentOS 7 como distribución y MariaDB 10.4 como versión elegida. La configuración del repositorio obtenida de esta página es la que se utilizará a continuación, en el paso *MariaDB 10.4*

Configuración firewall

```
firewall-cmd --zone=public --permanent --add-port=80/tcp
firewall-cmd --zone=public --permanent --add-port=443/tcp
firewall-cmd --reload
```

Apache y php 5.4

```
yum install httpd mod_ssl php php-mysql php-mbstring php php-gd
php-imap php-ldap php-mysql php-odbc php-pear php-xml php-xmlrpc
php-pecl-apc php-mbstring php-mcrypt php-mssql php-snmp php-soap
php-tidy  php-cli php-fpm
systemctl enable httpd.service
systemctl start httpd.service
```

php 7.2

Añadir repositorio REMI

```
cd /tmp
wget https://rpms.remirepo.net/enterprise/remi-release-7.rpm
rpm -Uvh remi-release-7.rpm
rm remi-release-7.rpm
```

Activar repositorio php 7.2 y actualizar

```
vim /etc/yum.repos.d/remi-php72.repo
```

Cambiar enable=1 en la sección [remi-php72]

```
yum update
```

Comprobar la versión de php

```
php -v
```

MariaDB 10.4

Añadir y activar repositorio:

```
vim /etc/yum.repos.d/MariaDB.repo
```

Agregamos el siguiente contenido (recuperado de https://downloads.mariadb.org/mariadb/repositories):

```
# MariaDB 10.4 CentOS repository list
# http://downloads.mariadb.org/mariadb/repositories/
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

Actualizar

```
systemctl stop mariadb.service
yum upgrade maria*
systemctl enable mariadb.service
systemctl start mariadb.service
mysql_upgrade -p
```

Securizar MariaDB

```
mysql_secure_installation
```

Comprobación de la versión

```
mysql -v -p
```

nmap

```
yum install nmap
```

Habilitar sudo para que el servidor zabbix pueda ejecutar nmap

```
visudo -f /etc/sudoers
```

Agregamos el siguiente contenido:

```
%zabbix ALL=(ALL)NOPASSWD:/usr/bin/nmap -O *
```

10.4 Instalación Zabbix

En primer lugar es necesario agregar el repositorio para CentOS de Zabbix, y a continuación instalar los paquetes zabbix-server-mysql y zabbix-web-mysql. A continuación se reproducen los pasos necesarios para dejar el sistema Zabbix instalado y operativo.

Agregar repositorio

```
cd /tmp
wget https://repo.zabbix.com/zabbix/4.4/rhel/7/x86_64/zabbix-release-4.4-1.el7.noarch.rpm
rpm -Uvh zabbix-release-4.4-1.el7.noarch.rpm
rm zabbix-release-4.4-1.el7.noarch.rpm
```

Instalar paquetes Zabbix

```
yum-config-manager --enable rhel-7-server-optional-rpms
yum install zabbix-server-mysql
yum install zabbix-web-mysql
```

Crear base de datos

Abrir sesión en MariaDB

```
mysql –u root –h localhost –p
```

Crear base de datos y usuario mediante sentencias SQL

```
create user zabbix@localhost identified by <<password>>;
create database zabbix character set utf8 collate utf8_bin;
grant all privileges on zabbix.* to zabbix@localhost;
quit;
```

Importar esquema inicial

```
zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -
u zabbix@localhost -p <<password>>
```

Configurar Zabbix

Servidor Zabbix

```
vim /etc/zabbix/zabbix_server.conf
```

Configuramos el acceso a la base de datos, modificante los parámetros siguientes:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=<<password>>
```

Frontend Zabbix

```
vim /etc/httpd/conf.d/zabbix.conf
```

El fichero ya está preconfigurado. En necesario ajustar la zona horaria y dejarla como sigue:

```
php_value date.timezone Europe/Madrid
```

Como la configuración está prepara para PHP 5.x y vamos a utilizar la versión 7.2 es necesario cambiar la sección mod_php dejándola como sigue:

```
<IfModule mod_php7.c>
```

En lugar de `<IfModule mod_php5.c>`

Arranque del servicio zabbix-server

```
systemctl enable zabbix-server.service
systemctl start zabbix-server.service
```

A partir de aquí, y una vez finalizada la configuración por línea de comandos, se continua la configuración del frontend mediante interfaz web.

- Acceder a la interfaz gráfica mediante un navegador (previamente se ha creado un registro A en el servidor DNS interno de la ADL para que zabbix.adl.local apunte a la IP del servidor Zabbix)

```
http://zabbix.adl.local/zabbix
```

- La configuración consta de 7 pasos: inicio, prerequisitos, base de datos, conexión con el servidor, sumario, generación del fichero configuración e instalación.

Figura 49. Configuración frontend – Inicio

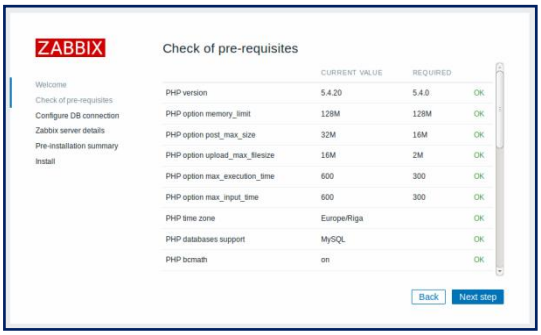


Figura 50. Configuración frontend – Prerrequisitos

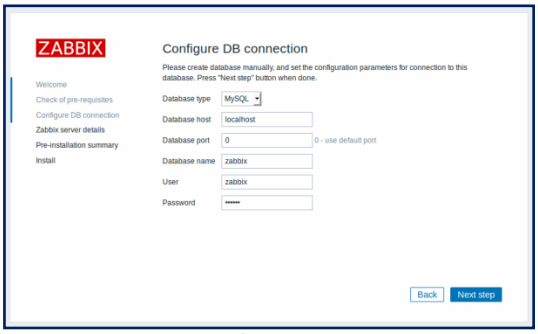


Figura 51. Configuración frontend – Base de datos

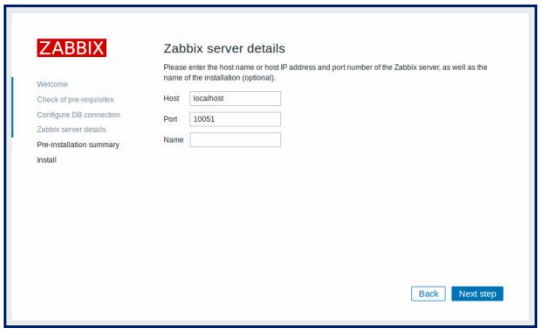


Figura 52. Configuración frontend – Conexión con el servidor

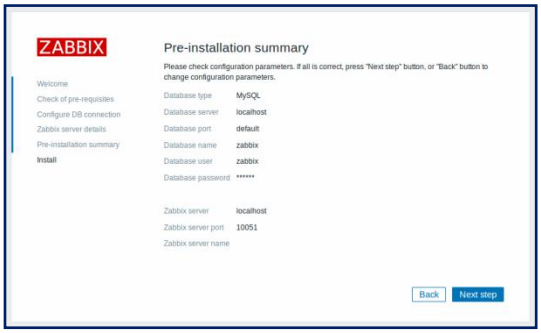


Figura 53. Configuración frontend – Sumario

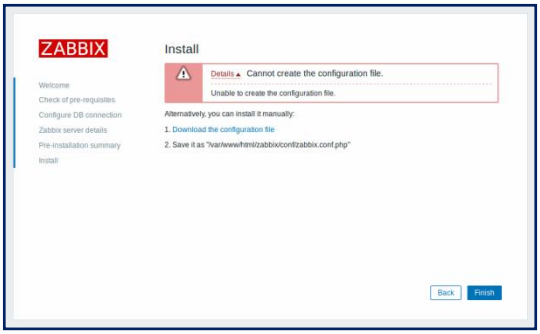


Figura 54. Configuración frontend – Fichero configuración

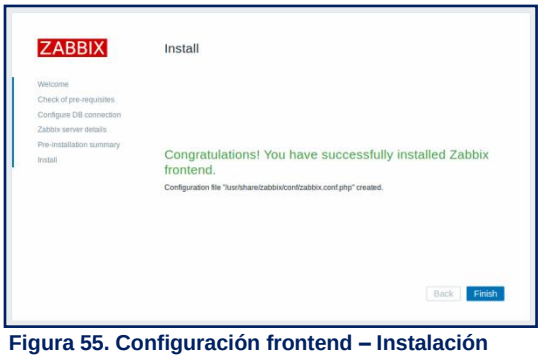


Figura 55. Configuración frontend – Instalación

10.5 Instalación de plantillas

Las plantillas en Zabbix proporcionan una forma fácil de configurar la monitorización de hosts similares, al definir una única vez las entidades de monitorización (monitores, iniciadores, gráficos, etc.) y aplicarlas masivamente a varios hosts.

Una vez definido un host a monitorizar, se le puede aplicar una plantilla. En el momento en que se le asigna, todas las entidades definidas en la plantilla se añaden al host.

Las plantillas facilitan el despliegue de Zabbix, ya que permiten definir una vez y reutilizar. Otra ventaja de las plantillas, es que las modificaciones realizadas se propagan a todos los hosts enlazados, facilitando el mantenimiento y la corrección de errores.

Zabbix incorpora un conjunto de plantillas oficiales que se pueden utilizar directamente, y un repositorio de plantillas creadas por la comunidad que pueden agregarse posteriormente. Las plantillas se pueden exportar e importar en otro sistema Zabbix de forma sencilla, ya que el formato utilizado para la exportación/importación es el estándar XML.

En la medida de lo posible se ha intentado utilizar plantillas oficiales, pero para algunos host ha sido necesario recurrir a las plantillas que ofrece la comunidad, y realizar modificaciones sobre ellas para que funcionen en el entorno de la ADL. A continuación se relacionarán las plantillas no oficiales que se han utilizado y las modificaciones que ha sido necesario realizar sobre ellas para que funcionen adecuadamente.

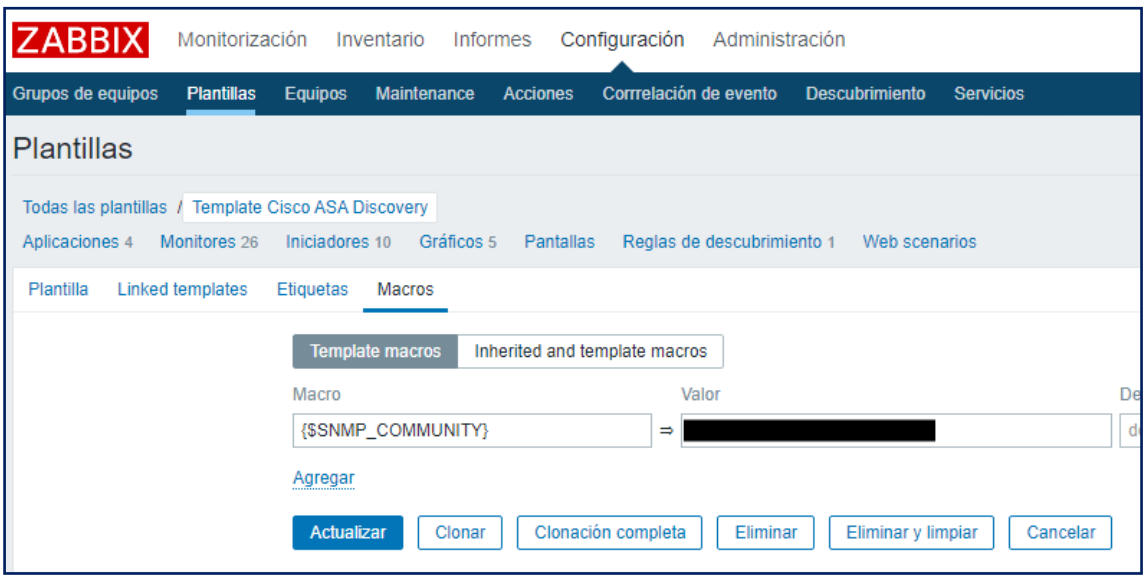


Figura 56. Instalación de plantillas – Macro SNMP

Es necesario recordar que en este proyecto se ha utilizado un nombre de comunidad SNMP distinto de *public*, por lo que para que la monitorización

funcione correctamente ha sido necesario asignar el valor de la comunidad SNMP definida a la macro

```
{$SNMP_COMMUNITY}
```

Esto se realiza desde el entorno gráfico, una vez importada la plantilla.

Plantilla Cisco ASA Discovery

Esta plantilla se ha utilizado para monitorizar los dos dispositivos de seguridad Cisco ASA [38]

La plantilla dispone de descubrimiento automático de interfaces, pero es necesario configurarlo antes de su importación a Zabbix. En concreto hay que modificar una expresión regular en el fichero XML de la plantilla que define los nombres de las interfaces.

El valor del elemento:

```
<value>@Firewalls network interfaces for discovery</value>
```

de la única regla de descubrimiento definida y que se localiza mediante la siguiente secuencia XPath:

```
/zabbix_export/templates/template/discovery_rules/discovery_rule
/filter/conditions/condition/value
```

se ha modificado con los nombres de las interfaces de los dos dispositivos ASA instalados en la ADL, quedando así:

```
<value>Ethernet0/1|Ethernet0/2|Ethernet0/3|Ethernet0/4|inside|ou
tside|dmz|management|Management|Virtual254</value>
```

Independientemente de esta modificación que está descrita en la página web de la plantilla, el autodescubrimiento no funcionaba correctamente. El problema residía en que la plantilla está definida para comparar las descripciones de los interfaces de red con los valores definidos anteriormente y en nuestro caso las interfaces no tienen descripción. Para corregir esto, se modificó la plantilla para que se utilizaran los nombres de las interfaces en lugar de su descripción. En concreto, se modificaron los valores de los siguientes elementos:

```
<snmp_oid>discovery[{#SNMPVALUE},IF-MIB::ifDescr]</snmp_oid>
<key>ifDescr</key>
```

por

```
<snmp_oid>discovery[{#SNMPVALUE},IF-MIB::ifName]</snmp_oid>
<key>ifName</key>
```

que se localizan mediante el siguiente XPath:

```
/zabbix_export/templates/template/discovery_rules/discovery_rule
```

De esta forma, en lugar de recuperar el OID IF-MIB::ifDescr, se obtiene el OID IF-MIB::ifName con el nombre de la interfaz. Con este cambio el autodescubrimiento funcionó correctamente y se pudieron monitorizar los dos dispositivos Cisco ASA.

Plantilla HP RT3000 SNMP

Para la monitorización de los SAIs HP RT3000 se utilizó como base la plantilla HP UPS SNMP (R5000) [39], en la que se realizaron algunas modificaciones para ajustarla a las necesidades de la ADL.

La última versión de esta plantilla está diseñada para funcionar con Zabbix 3.2 y al intentar importarla en Zabbix 4.4 se lanza el error: "*XML declaration allowed only at the start of the document*". Para solventarlo ha sido necesario eliminar la primera línea, que consiste en un comentario en el que se indica el autor de la plantilla

```
<!-- Made By Tom Adolfs -->
```

También se ha ampliado la capacidad de monitorización de esta plantilla al enlazarla con las siguientes plantillas genéricas para SNMPv1:

```
Template Module Generic SNMPv1
Template Module HOST-RESOURCES-MIB SNMPv1
Template Module Interfaces SNMPv1
```

De esta forma se consigue, por ejemplo, descubrir y monitorizar parámetros como el tiempo encendido (*uptime)* o el nombre del equipo (*System name*) que no están definidos en la plantilla original.

Plantilla SNMP Ricoh printers

La monitorización de las impresoras multifunción Nashuatec se ha realizado utilizando la plantilla Ricoh SNMP Printers [40] como base.

Al igual que sucede con la plantilla para la monitorización de SAIs, no existe una versión de esta plantilla para Zabbix 4.4 por lo que no se puede utilizar directamente. Al intentar importarla se obtiene el siguiente error: "*No pudo importar la plantilla porque la plantilla enlazada Template SNMP Generic no existe.*". Esto se produce porque la plantilla *SNMP Generic* ha sido sustituida por *Module Generic SNMPv2*. La solución es sencilla, basta con sustitutir el valor del elemento definido por el siguiente XPath:

```
/zabbix_export/templates/template/templates/name
```

de

```
Template SNMP Generic
```

a

```
Template Module Generic SNMPv2
```

Plantilla Generic printers

Con el fin de monitorizar las impresoras HP y Nashuatec se ha intentado utilizar varias plantillas de la comunidad específicas para estos fabricantes, como: *HP Color Laserjet* [41] o *Kyocera Devices (use snmp v2*) [42], pero no se consiguió que funcionaran correctamente, por lo que se optó por utilizar una plantilla genérica para impresoras SNMP, que es la que finalmente se está utilizando.

No obstante, ha sido necesario realizar algunas modificaciones en la plantilla original (*Generic printers monitoring template*), tal y como se describe en la su sitio web [43]. Las modificaciones se deben a que está enlazada con la plantilla *Template ICMP Ping* que ha sido sustituida por *Template Module ICMP Ping*. Es necesario realizar dos cambios en la plantilla original. En primer lugar modificar el nombre de la plantilla dependiente, para ello cambiar el valor del elemento definido por el siguiente XPath:

```
/zabbix_export/templates/template/templates/name
```

de

```
Template ICMP Ping
```

a

```
Template Module ICMP Ping
```

Y en segundo lugar, la definición de un iniciador generado por la regla de descubrimiento Printer FRU, para ello es necesario cambiar el valor del elemento definido por el siguiente XPath:

```
zabbix_export\templates\template\discovery_rules\discovery_rule\
item_prototypes\item_prototype\trigger_prototypes\trigger_protot
ype\dependencies\dependecy\expression
```

de

```
{Printers Generic Template:icmpping.max(#3)}=0
```

a

```
{Template ICMP Ping:icmpping.max(#3)}=0
```

Una vez realizadas estas modificaciones, la plantilla se importa perfectamente y descubre los componentes de la impresora (consumibles, bandejas, etc.) a monitorizar.

10.6 Instalación y configuración de agentes

Zabbix proporciona agentes para entornos Linux y Windows. En este anexo se describe el procedimiento seguido para la instalación de los agentes en los servidores Linux de la ADL basados en CentOS 7 y en los servidores Windows basados en Windows 2016.

Linux CentOS 7

Agregar repositorio

```
cd /tmp
wget https://repo.zabbix.com/zabbix/4.4/rhel/7/x86_64/zabbix-release-4.4-1.el7.noarch.rpm
rpm -Uvh zabbix-release-4.4-1.el7.noarch.rpm
rm zabbix-release-4.4-1.el7.noarch.rpm
```

Instalar agente Zabbix

```
yum install zabbix-agent
```

Configurar agente en modo pasivo

```
vim /etc/zabbix/zabbix_agentd.conf
```

Definir el nombre del servidor Zabbix que se va a conectar al agente. Cambiar el parámetro Server y comentar el parámetro ServerActive.

```
Server=zabbix.adl.local
…
# ServerActive=
```

Configuración firewall

```
firewall-cmd --zone=public --permanent --add-port=10050/tcp
firewall-cmd –reload
```

Arranque del servicio zabbix-agent

```
systemctl enable zabbix-agent.service
systemctl start zabbix-agent.service
```

Una vez que el agente esté instalado y funcionando, es necesario crear el host en el servidor Zabbix y asignarle la plantilla *OS Linux by Zabbix agent* para que comience la monitorización.

Windows Server 2016

En este caso, la instalación se realiza en entorno gráfico. Zabbix proporciona un paquete en formato .msi directamente instalable en el servidor [44].

La instalación y configuración del agente Windows se muestra en las siguientes capturas de pantalla:

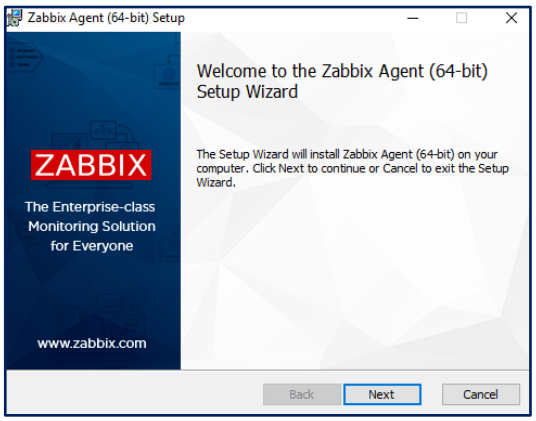


Figura 57. Agente Windows – Presentación

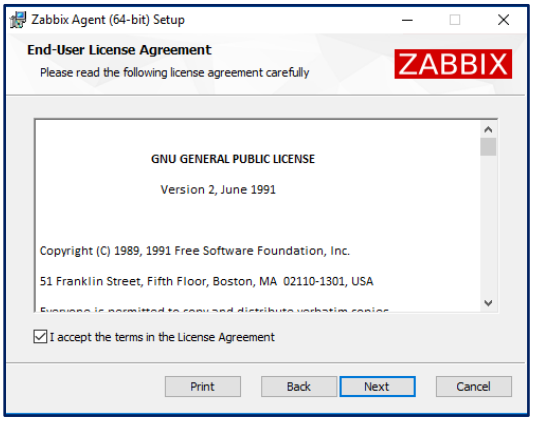


Figura 58. Agente Windows – Licencia

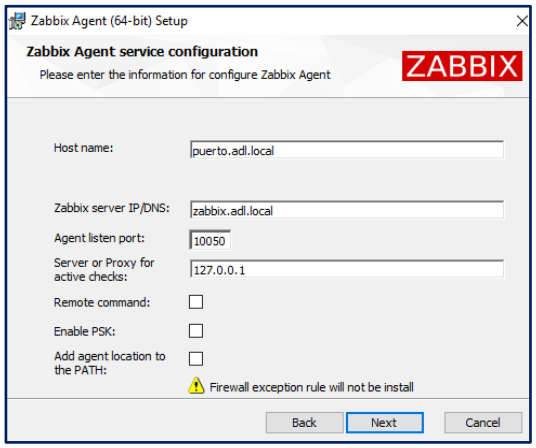


Figura 59. Agente Windows – Configuración

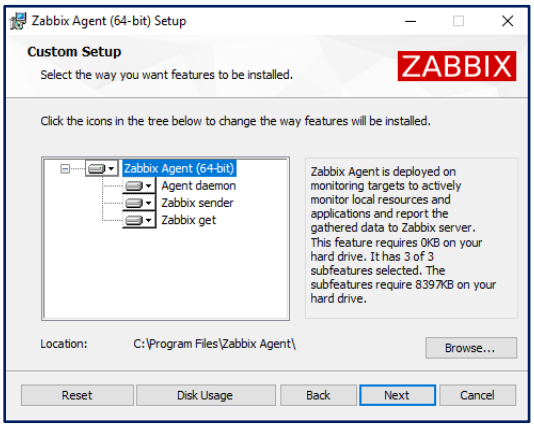


Figura 60. Agente Windows – Componentes

Figura 61. Agente Windows – Instalación

Para que el servidor Zabbix se puede comunicar con el agente, es necesario abrir el puerto tcp/10050 en el firewall del servidor Windows.

Una vez que el agente esté instalado y se haya comprobado que el servicio *Zabbix Agent* esté operativo, es necesario crear el host en el servidor Zabbix y asignarle la plantilla *OS Windows by Zabbix agent* para que comience la monitorización.

10.7 Monitorización VMWare

La monitorización de la infraestructura de virtualización VMWare se realiza en dos pasos: en primer lugar es necesario activar el proceso vmware collector y en segundo lugar es necesario definir el host que alberga el vcenter (en el caso de que dispongamos de él) y asignarle la plantilla *VM VMWare*. Si no disponemos de vcenter será necesario crear un host por cada hipervisor que se quiere monitorizar [45].

Durante el proceso de descubrimiento, Zabbix creará un host nuevo por cada hipervisor que descubra y le asignará la plantilla *VM VMware Hypervisor*, y un host nuevo por cada máquina virtual que descubra y le asignará la plantilla *VM VMware Guest*. Asimismo, creará automáticamente varios grupos para clasificar los hipervisores y máquinas virtuales descubiertas. En otros, creará un grupo por cada hipervisor descubierto y asignará a cada una de las máquinas virtuales que residan en ese hipervisor dicho grupo.

VMWare collector

Por defecto, este proceso está deshabilitado. Para habilitarlo es necesario configurar los siguientes parámetros en el fichero de configuración del servidor Zabbix:

- StartVMwareCollectors: Número de instancias del proceso vmware collector.
- VMwareCacheSize: Tamaño de la memoria caché
- VMwareFrequency: Frecuencia de muestreo
- VMwarePerfFrequency: Frecuencia de muestreo para datos de rendimiento.
- VMwareTimeout: Tiempo máximo de espera de respuesta.

En nuestro caso, se ha configurado únicamente el parámetro StartVMWareCollectors, dejando el resto de parámetros con su valor por defecto.

Configurar proceso vmware collector

vim /etc/zabbix/zabbix_server.conf

Cambiar el valor del parámetro StartVMwareCollectors.

```
StartVMwareCollectors=1
```

Reiniciar el servidor Zabbix

```
systemctl restart zabbix-server.service
```

Comprobar que se ha activado el proceso

```
systemctl status zabbix-server.service | grep collector
```

Creación servidor VMWare y descubrimiento

- Crear un host en Zabbix dejando como IP la que viene por defecto (127.0.0.1). La dirección IP del servidor real se configura posteriormente, a través de macros.
- Asignarle la plantilla *VM VMware*
- Crear las siguientes macros en la pestaña correspondiente:

```
{$PASSWORD} – Contraseña para conectarse al servidor VMWare
{$URL} – Dirección ip del servidor VMWware, en el siguiente
formato: https://xxx.xxx.xxx.xxx/sdk
{$USERNAME} – Usuario para conectarse al servidor VMWare
```

- A partir de aquí Zabbix, irá descubriendo la infraestructura VMWare.

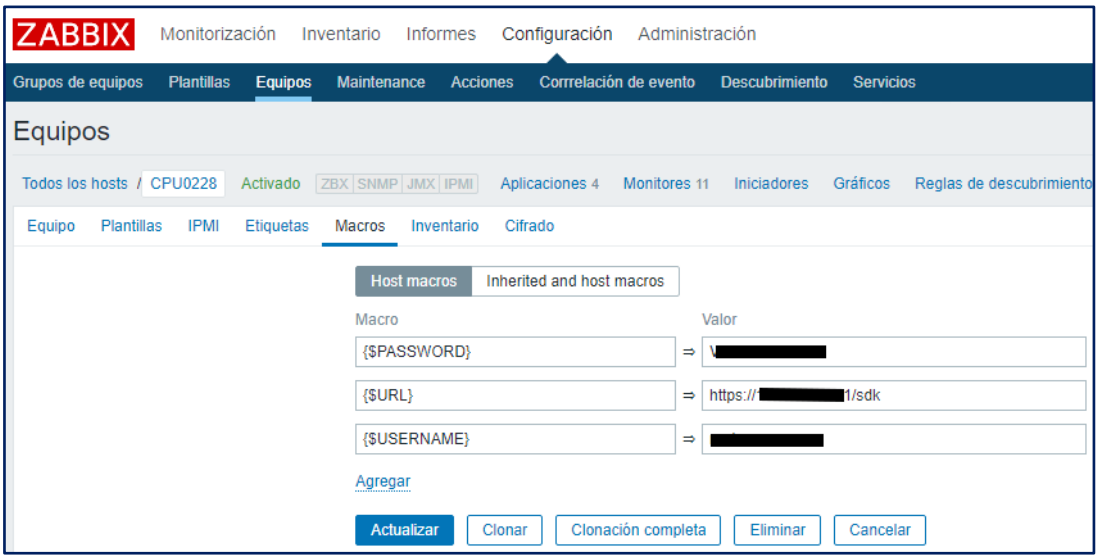


Figura 62. Monitorización VMWare – Macros

Figura 63. Monitorización VMWare – Definición hosts