Implementación de un sistema de monitorización en la red de un hospital

Juan Manuel Cañero Gómez

Redes de computadores

Nombre Tutor/a de TF
Amadeu Albós Raya
Profesor/a responsable de la asignatura
Joan Manuel Marquès Puig

Fecha Entrega
Enero 2024

Universitat Oberta
de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implementación de un sistema de monitorización en la red de un hospital*
Nombre del autor:	*Juan Manuel Cañero Gómez*
Nombre del consultor/a:	*Amadeu Albós Raya*
Nombre del PRA:	*Joan Manuel Marquès Puig*
Fecha de entrega (mm/aaaa):	09/01/2023
Titulación o programa:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Redes de computadores*
Idioma del trabajo:	*Castellano*
Palabras clave	*Monitorización, SNMP, checkMK*

Resumen del Trabajo

La infraestructura de red de los hospitales desempeña un papel fundamental para brindar atención sanitaria de calidad. Sin embargo, se enfrenta a desafíos constantes que pueden afectar todos los ámbitos: desde la pérdida de acceso a información crucial y el consecuente retraso en la atención médica, hasta riesgos en la seguridad de la información debido a posibles ataques informáticos que podrían comprometer la privacidad de los pacientes.

Por todo ello, en imprescindible una buena gestión de la infraestructura que minimice estos inconvenientes. Este proyecto trata de resolver esta problemática, para ello se ha realizado un análisis de la gestión de la red del centro hospitalario, lo que ha permitido descubrir sus puntos débiles. Con esta información, se han podido establecer una serie de requisitos que debe cumplir una solución que mejore la gestión de la infraestructura: la implementación de un sistema de monitorización de la infraestructura de red.

Se ha expuesto el funcionamiento de los sistemas de monitorización basados en SNMP, explicando algunos conceptos clave y comparando las distintas alternativas. Finalmente se ha implementado en un entorno real un sistema basado en CheckMK, realizando las configuraciones necesarias que han permitido cubrir los requisitos.

Esta implementación permitirá al equipo de soporte detectar incidencias de manera proactiva, conocer la capacidad de la infraestructura o realizar un seguimiento de los intentos de conexión no autorizados entre otras funcionalidades. Todo esto permitirá mejorar la gestión de la infraestructura de red, lo que se traducirá en un mejor servicio del centro en todos los niveles.

Abstract

Hospital network infrastructure plays a key role in providing quality healthcare. However, it faces constant challenges that can affect everything from loss of access to crucial information and the resulting delay in medical care, to information security risks due to potential cyber-attacks that could compromise patient privacy.

Therefore, a good management of the infrastructure is essential to minimise these inconveniences. This project aims to solve this problem by analysing the management of the hospital's network, which has allowed us to discover its weak points. With this information, it has been possible to establish a series of requirements to be met by a solution that improves the management of the infrastructure: the implementation of a monitoring system for the network infrastructure.

The operation of SNMP-based monitoring systems has been presented, explaining some key concepts and comparing the different alternatives. Finally, a system based on CheckMK has been implemented in a real environment, making the necessary configurations to cover the requirements.

This implementation will allow the support team to proactively detect incidents, know the capacity of the infrastructure or track unauthorised connection attempts, among other functionalities. All of this will improve the management of the network infrastructure, which will result in a better service at all levels of the centre.

Contenido

Lista de figuras

1. Introducción

Figura 1: sistema de monitorización

1.1 Contexto y justificación del Trabajo

Este proyecto se ubica en un complejo hospitalario donde se han detectado incidencias que afectan a la infraestructura de red y su gestión. En la actualidad, la infraestructura de red de los hospitales desempeña un papel fundamental para brindar atención sanitaria de calidad.

Sin embargo, enfrentan desafíos que van desde interrupciones en la red hasta problemas de seguridad, como la conexión no autorizada de dispositivos que plantea riesgos considerables para la integridad y privacidad de los datos sensibles [1]. Estas incidencias pueden afectar a todos los ámbitos: desde pérdida de acceso a información vital que generan retrasos en la atención médica hasta dificultades en la gestión del personal administrativo, que además se ve forzado a tener que perder tiempo reportando la incidencia al departamento de informática.

Para abordar estos desafíos y garantizar un funcionamiento óptimo de la red, se propone un control proactivo de la infraestructura de red del centro. La implementación de un sistema de monitorización de la red permitirá supervisar en tiempo real la infraestructura de red y obtener datos que, tras su análisis, permitirán identificar problemas de manera proactiva y tomar medidas correctivas de manera eficiente para garantizar el buen funcionamiento de los sistemas informáticos del centro.

Los sistemas de monitoreo de red incluyen herramientas de software y hardware que pueden hacer un seguimiento de diversos aspectos de la red y su funcionamiento, como el tráfico, el uso de ancho de banda y el tiempo de actividad. Estos sistemas pueden detectar dispositivos y otros elementos que componen la red, además de proporcionar actualizaciones de estado[2]. Se trata de un proceso crítico que se debería llevar a cabo en todas las infraestructuras, más aún en las que requieren alta disponibilidad como un centro hospitalario.

El sistema de monitorización permitirá detectar y solucionar problemas de red antes de que afecten a los usuarios, garantizando que los sistemas estén siempre disponibles, permitiendo que el personal sanitario y administrativo se enfoque en la atención al paciente en lugar de lidiar con problemas técnicos.

Por otro lado, el sistema puede supervisar en vivo los intentos de conexión no autorizados, lo que permite una detección temprana de cualquier actividad sospechosa o no permitida en la red, algo fundamental por la criticidad y confidencialidad de los datos manejados. En un futuro este sistema podría ampliarse para incluir servidores u otros tipos de dispositivos críticos.

La implementación de un servidor de monitorización de red encaja dentro del área Redes de computadores, concretamente como "Herramienta de análisis de rendimiento de una red" ya que permite evaluar el rendimiento de las redes de computadoras, proporcionando información valiosa para mantener y mejorar la eficiencia y la confiabilidad de la infraestructura.

En el ámbito personal, es un tema que me atrae bastante y espero que este proyecto se convierta en un punto de inflexión en mi ámbito profesional. Actualmente formo parte del equipo que da soporte TIC al hospital y considero que con la implementación de este sistema se conseguirá mejorar la calidad del servicio ofrecido.

1.2 Objetivos del Trabajo

El objetivo general de este trabajo de fin de grado es mejorar la gestión de la red en un entorno hospitalario, enfocándome en la disponibilidad y seguridad de los sistemas críticos mediante la implementación de un sistema de monitorización de la infraestructura de red.

Los objetivos específicos son:

- Explorar los componentes que forman una infraestructura de red crítica, como la de un centro hospitalario, identificando los switches y dispositivos de red críticos que deben ser monitorizados.

- Investigar e identificar el software de monitorización más adecuado, profundizando en el funcionamiento del protocolo simple de administración de red (SNMP) y su uso para monitorizar dispositivos.

- Desarrollar un sistema de alertas que permita al equipo de soporte TIC del hospital dar una respuesta rápida y proactiva a las incidencias.

- Investigar la detección de dispositivos no autorizados a través de los traps SNMP, analizando cómo los switches responden ante los intentos de intrusión.

1.3 Impacto en sostenibilidad, ético-social y de diversidad

La competencia de compromiso ético y global (CCEG) está definida a nivel de Grado como:

"Actuar de forma honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional" [3]

Por lo tanto, hay que considerar que aborda tres grandes dimensiones:

- Sostenibilidad

Consumo energético: el proyecto tiene un impacto negativo para la sostenibilidad del medioambiente, ya que su implementación aumenta el consumo energético del hospital debido a la necesidad de disponer de un servidor encendido continuamente para realizar la monitorización. Por lo tanto, el proyecto tiene un impacto negativo en el ODS 7 (energía asequible y no contaminante). Para reducir este impacto, se tratará de utilizar un servidor que requiera los menores recursos.

Reducción de papel: el sistema de monitorización de red es 100% digital y es capaz de enviar los informes por email, sin necesidad de imprimirlos, lo que contribuye a la reducción del consumo de papel. Esto es beneficioso desde el punto de vista de la sostenibilidad y se puede relacionar con el ODS 12 (producción y consumo responsables).

- Ético-social

Protección de datos de pacientes: el trabajo tiene un impacto positivo en el aspecto de que durante su desarrollo se cumplirá en todo momento con la legislación relacionada con la protección de datos. Por otro lado, el sistema ofrecerá herramientas que nos ayudan a proteger la privacidad y la seguridad de los datos de los pacientes, que lo que es positivo para el ODS 16 (Paz, justicia y fortaleza de las instituciones) [4]

- Diversidad

Este proyecto no tiene un impacto directo en la dimensión diversidad al tratarse de un proyecto técnico y no abordar cuestiones específicas relacionadas con la diversidad, el género o los derechos humanos.

1.4 Enfoque y método seguido

Dado que se trata de un proyecto individual, en el que yo seré el único recurso, se llevará a cabo siguiendo un enfoque waterfall [5]. Este proyecto es apropiado para usar este método de trabajo, ya que tanto los requisitos como el alcance están fijados desde un principio.

Siguiendo esta metodología, el trabajo se estructurará en distintas fases:

- Análisis y Requisitos: determinar qué aspectos de la red del hospital se deben supervisar, qué métricas son importantes, qué dispositivos deben incluirse y cualquier requisito regulatorio o de seguridad.

- Diseño: diseñar cómo se configurará y operará el sistema de monitorización de red en el hospital, selección de herramientas de monitoreo, la definición de umbrales de alerta y la elaboración de diagramas de flujo.

- Implementación: implementar el sistema de monitorización de red, añadir los clientes (switches), desarrollo de sistema de alertas, monitorización de traps y configuraciones personalizadas necesarias.

- Resultados: probar la capacidad del sistema para detectar problemas de red, generar alertas y registrar datos de manera precisa.

- Conclusiones: revisión final, conclusiones y validación por parte de expertos en redes.

Los hitos del proyecto están condicionados por las fechas de entrega de las pruebas de evaluación continua. De este modo, el logro de cada hito se programará de acuerdo con las fechas previstas para la finalización cada una de las cinco PECs:

Id	Hito	Fecha límite
1	Elaboración del Plan de Trabajo	10/10/23
2	Primera entrega parcial	07/11/23
3	Segunda entrega parcial	05/12/23
4	Entrega final	09/01/24

Figura 2: tabla de hitos

1.5 Planificación del Trabajo

Para la planificación del trabajo se han definido una serie de tareas que se deben completar en cada fase:

- Fase 0: plan de trabajo
  - Elaboración de un plan de trabajo en el que se incluyen los siguientes aspectos del proyecto: contexto, justificación.

- Fase I: análisis y requisitos
  - Análisis de la situación actual y requisitos
  - Inventariar los switches que forman parte del centro.

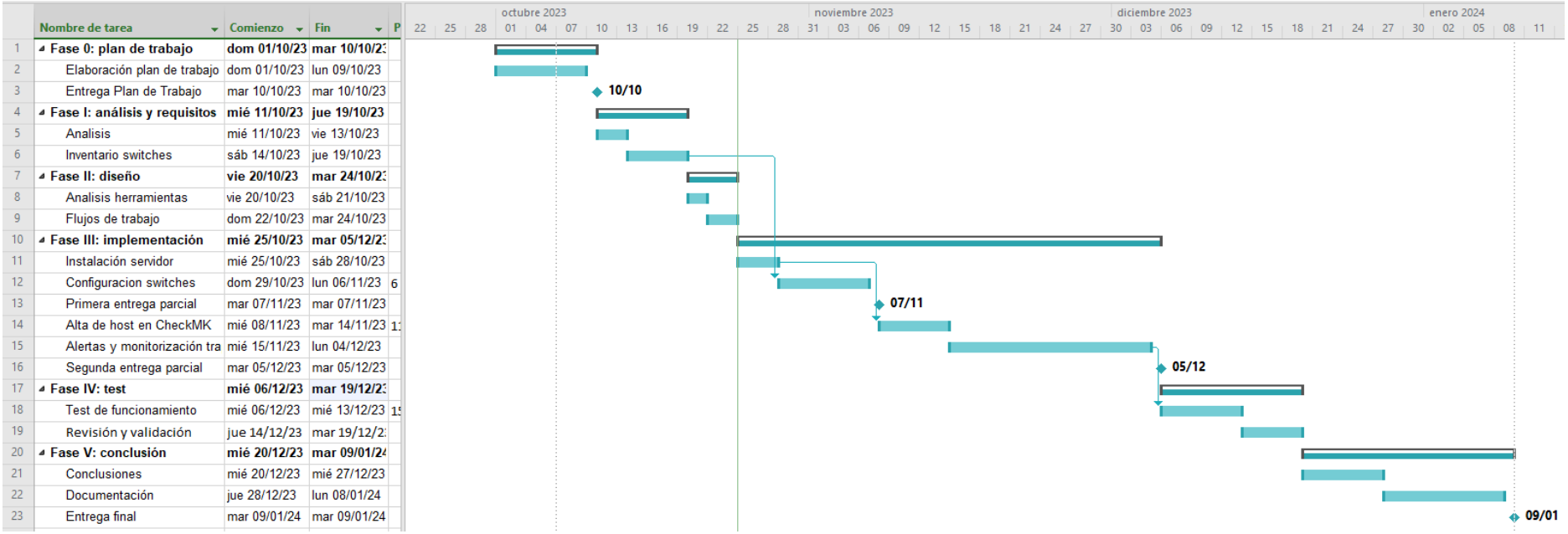
- Fase II: diseño
  - Analizar las herramientas existentes y determinar cuál es la que mejor se adapta a nuestras necesidades
  - Diseño de flujos de trabajo que determinen el comportamiento de la solución propuesta ante diversos escenarios.

- Fase III: implementación:
  - Instalación del servidor con su correspondiente sistema operativo, configuraciones y herramienta de monitorización.
  - Configuración de community en switches para que sean visibles desde nuestro sistema y activación de traps ante intentos de intrusión
  - Alta de host en el sistema de monitorización según inventario realizado en fase I.
  - Configuración de un sistema de alertas que permita a los operadores detectar y gestionar las incidencias sin necesidad de que el usuario tenga que generar un parte de avería.
  - Análisis de traps para visualizar los intentos de intrusión a través de la integración en el sistema de monitorización.

- Fase IV: resultados:
  - Probar la capacidad del sistema para detectar problemas de red, generar alertas y registrar datos de manera precisa.
  - Revisión y validación por parte de expertos en redes (consultor y dirección del centro).

- Fase V: conclusión:
  - Conclusiones sobre el proyecto

A continuación, se muestra un diagrama de Gantt, donde se especifican los plazos, hitos y dependencias de las tareas a realizar:



	Nombre de tarea	Comienzo	Fin	P
1	**Fase 0: plan de trabajo**	**dom 01/10/23**	**mar 10/10/23**	
2	Elaboración plan de trabajo	dom 01/10/23	lun 09/10/23	
3	Entrega Plan de Trabajo	mar 10/10/23	mar 10/10/23	
4	**Fase I: análisis y requisitos**	**mié 11/10/23**	**jue 19/10/23**	
5	Analisis	mié 11/10/23	vie 13/10/23	
6	Inventario switches	sáb 14/10/23	jue 19/10/23	
7	**Fase II: diseño**	**vie 20/10/23**	**mar 24/10/23**	
8	Analisis herramientas	vie 20/10/23	sáb 21/10/23	
9	Flujos de trabajo	dom 22/10/23	mar 24/10/23	
10	**Fase III: implementación**	**mié 25/10/23**	**mar 05/12/23**	
11	Instalación servidor	mié 25/10/23	sáb 28/10/23	
12	Configuracion switches	dom 29/10/23	lun 06/11/23	6
13	Primera entrega parcial	mar 07/11/23	mar 07/11/23	
14	Alta de host en CheckMK	mié 08/11/23	mar 14/11/23	1
15	Alertas y monitorización tra	mié 15/11/23	lun 04/12/23	
16	Segunda entrega parcial	mar 05/12/23	mar 05/12/23	
17	**Fase IV: test**	**mié 06/12/23**	**mar 19/12/23**	
18	Test de funcionamiento	mié 06/12/23	mié 13/12/23	1
19	Revisión y validación	jue 14/12/23	mar 19/12/2	
20	**Fase V: conclusión**	**mié 20/12/23**	**mar 09/01/24**	
21	Conclusiones	mié 20/12/23	mié 27/12/23	
22	Documentación	jue 28/12/23	lun 08/01/24	
23	Entrega final	mar 09/01/24	mar 09/01/24	

Figura 3: diagrama de Gantt

1.6 Breve sumario de productos obtenidos

Diseño e implementación del sistema de monitorización que permita analizar proactivamente los problemas de la red.

1.7 Breve descripción de los otros capítulos de la memoria

1. Introducción
   Se expone el contexto, la justificación y un plan de trabajo para poder desarrollar el proyecto

2 Análisis y requisitos: en este capítulo se realizará un estudio de la situación actual, detectando que problemas existen y que requisitos debe cumplir la solución propuesta para solucionarlos.

3 Diseño: análisis de las alternativas para implementar el sistema y diagramas de flujo de funcionamiento de la solución propuesta.

4 Implementación: en este apartado se detallan los pasos necesarios para poder implementar el sistema: instalación del servidor, configuraciones previas en switches, alta de host, sistema de alertas y monitorización de traps.

5 Resultados: en este capítulo se analiza el funcionamiento de la herramienta, evaluando la capacidad para detectar incidencias y generar alertas que hemos obtenido durante los test.

6 Conclusiones
   Informe de conclusiones donde se valora los objetivos logrados, las dificultades que han surgido y los trabajos futuros trabajos que se deberían realizar.

7 Glosario
   Definición de los términos y acrónimos más relevantes utilizados en la Memoria.

8 Bibliografía
   Lista numerada de las referencias bibliográficas utilizadas en la memoria.

2. Análisis y requisitos

El ámbito del proyecto se sitúa en un importante centro hospitalario, donde la robustez de la infraestructura de red no solo es vital, sino que es un elemento central para el funcionamiento eficiente de todas las operaciones. Con alrededor de 3000 puestos de usuario y 300 servidores, la infraestructura de red se revela como la columna vertebral que sostiene la conectividad y el intercambio de información esencial.

La infraestructura de red está formada por más de 100 switches, cuya interconexión eficiente se traduce directamente en la capacidad de brindar atención médica sin interrupciones, acceder a registros clínicos de manera instantánea y garantizar la fluidez de las operaciones administrativas. En este escenario, la infraestructura de red es un elemento crítico, que sostiene cada aspecto de la prestación de servicios del centro.

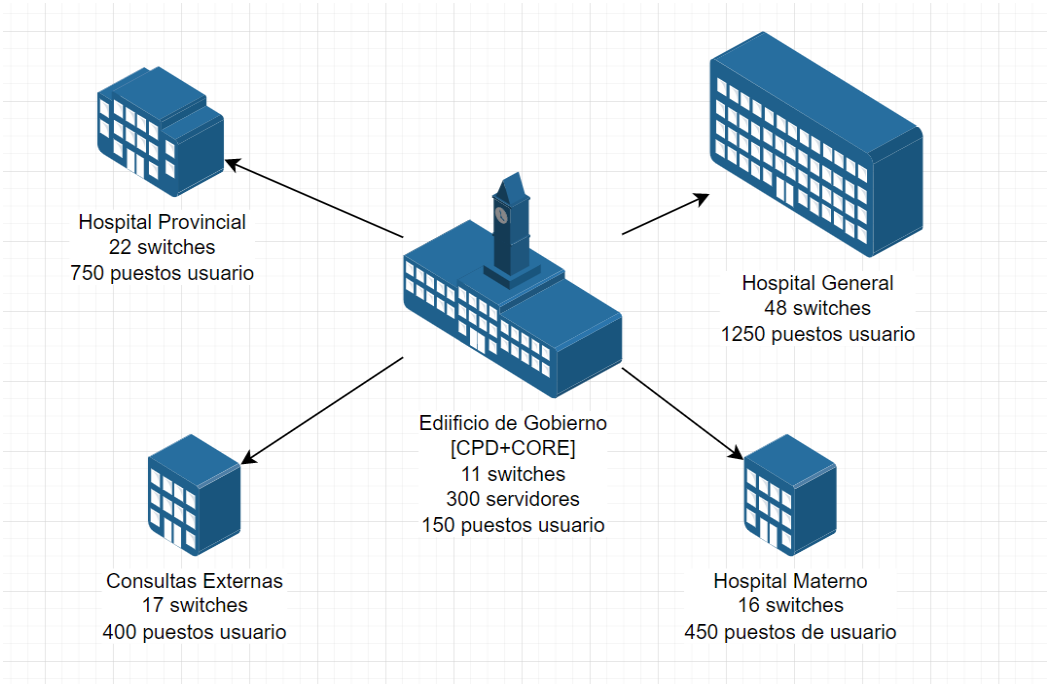


Figura 4: diagrama de infraestructura del complejo hospitalario

La gestión integral de esta infraestructura es llevada a cabo por el servicio de informática del hospital, cuya tarea no solo consiste en mantener la operatividad diaria, sino en asegurar la disponibilidad, seguridad y eficiencia continua de la red.

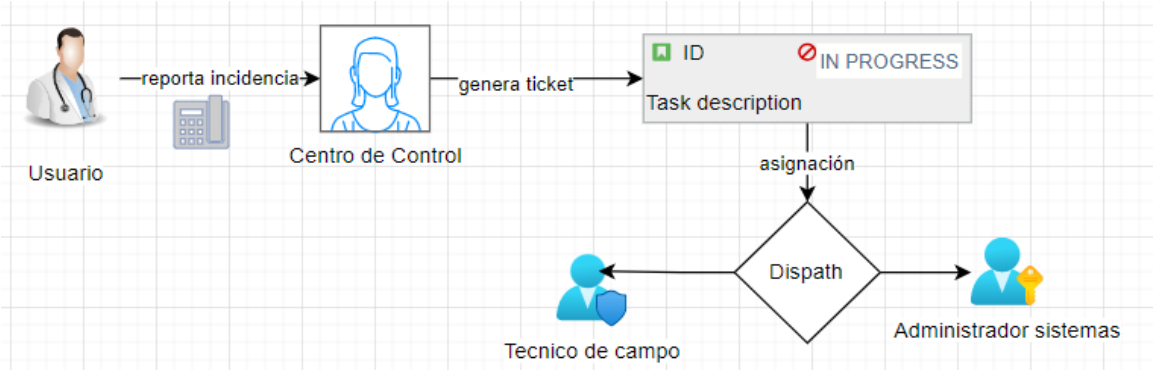


Figura 5: diagrama flujo de una incidencia

En este contexto, se realizará un análisis de los flujos de trabajo que afectan a la infraestructura de red existente, identificando sus puntos débiles y explorando cómo la implementación de un sistema de monitorización puede elevar la calidad del servicio ofrecido.

2.1 Problemáticas detectadas

2.1.1 Reporte incidencias de red

Actualmente, la gestión de incidencias se basa en un sistema que requiere la comunicación manual de los usuarios con el centro de atención al usuario vía teléfono cuando se produce un fallo en la red. Este sistema presenta algunos inconvenientes, como la falta de detección proactiva de las incidencias o el retraso en registrar las incidencias debido a la saturación de la centralita del centro de atención al usuario. Por ello, es necesario implementar una solución que permita la detección proactiva de problemas, asi como la generación de notificaciones automáticas, con el fin de evitar que el personal del centro tenga que perder tiempo en comunicar telefónicamente las incidencias.

El hecho de que la detección de problemas de red dependa en gran medida de que los propios usuarios notifiquen manualmente las incidencias al centro de atención al usuario, genera un retraso en la identificación y resolución de problemas, ya que la red puede verse afectada antes de que los usuarios informen de las dificultades.

Otro aspecto a considerar es la saturación en la centralita telefónica, ya que en ocasiones el centro de atención al usuario se encuentra con todos los operadores ocupados, por lo que los usuarios pueden experimentar dificultades para informar de incidencias. Esta situación tiene impacto significativo en la satisfacción del usuario, tanto por el tiempo dedicado a labores ajenas a sus funciones (comunicación de la incidencia), como por la demora que se produce en la resolución de su incidencia, al no poder avisar inmediatamente.

2.1.2 Desconocimiento capacidad de la infraestructura

Además, se ha detectado otra problemática a la hora de conocer la capacidad de la infraestructura, lo que ocasiona que no se tenga conocimiento en tiempo real de si existe una necesidad de ampliación de la misma. Como consecuencia de esto, en ocasiones los técnicos de campo se enfrentan a la falta de puertos disponibles en las electrónicas a la hora de instalar equipos o dispositivos críticos.

Para abordar esta problemática, es vital implementar un sistema que permita conocer y gestionar eficazmente la disponibilidad de puertos libres en los switches en tiempo real, con lo que se podrían planificar previamente las ampliaciones necesarias que eviten situaciones como la descrita anteriormente.

2.1.3 Shadow IT

En el Instituto Nacional de Ciberseguridad de se define shadow IT como “la práctica donde los empleados utilizan aplicaciones, dispositivos y servicios tecnológicos sin la aprobación de los departamentos TI de la empresa, ya sea por desconocimiento o de forma premeditada” [6].

Para afrontar este desafio, recientemente se ha implementado un sistema de control de acceso a la red (NAC) en el centro, que bloquea las conexiones MAC no autorizadas en los switches, ha sido un paso esencial para fortalecer la seguridad de la red. Esta medida garantiza que las interfaces se desactiven de manera automática cuando se detecta la presencia de dispositivos desconocidos [7], lo que contribuye en gran medida a mantener la integridad de nuestros sistemas y datos.

Sin embargo, esta mejora en la seguridad ha dado lugar a un desafío adicional. Los técnicos de campo a menudo se encuentran en situaciones en las que deben rastrear las conexiones físicas de cables a través de los racks y switches para localizar la roseta de red desactivada cuando se detecta un intento de intrusión, lo que supone una tarea compleja y consume una cantidad significativa de tiempo, ralentizando la respuesta a las posibles amenazas y ralentizando el tiempo que el puesto permanece inoperativo.

Como problema añadido, algunas rosetas carecen de etiquetas o nomenclatura que indique a qué rack corresponde, por lo que se complica aún más la tarea de identificar la ubicación exacta de la interfaz de la switch desactivada y, por tanto, el seguimiento de los intentos de intrusión se vuelve aún más difícil.

La falta de una solución eficiente para la localización de estos intentos de intrusión es un problema que debería de atajarse, tanto por el riesgo a la seguridad de los datos como por el tiempo que los equipos permanecen inoperativos hasta que el técnico restaura la conexión. Por lo tanto, considera imprescindible que se implemente un sistema que permita gestionar eficazmente estos eventos. Dicha solución debe proporcionar una forma más eficiente y

rápida a la hora de rastrear intentos de intrusión, recopilando todos los eventos y ayudando a la localización física de los mismos.

2.2 Requisitos

En este apartado se determina los requisitos funcionales que la aplicación debe cumplir, asi como los requisitos operativos y no funcionales.

2.2.1 Requisitos funcionales

- Detección proactiva de incidencias de red y envío automático de notificaciones al grupo de soporte.

- Detección de los intentos de intrusión en tiempo real y almacenado de histórico.

- Detección en tiempo real del estado de las interfaces de los switches, mostrando las interfaces libres que existen en cada dispositivo.

- Inventariado de todos los switches que forman parte de la infraestructura de red del centro.

2.2.2 Requisitos operativos

- Minimizar consumo de recursos: el sistema debe consumir pocos recursos, de manera que su implementación no repercuta sobre la infraestructura de red ni requiera la adquisición de hardware nuevo.

- Facilidad de implementación: la implementación debe llevarse a cabo antes de enero, por lo que el sistema no debe implicar una implementación demasiado compleja.

- Facilidad de operación: con el objetivo de facilitar la curva de aprendizaje, la solución debe ser intuitiva y fácil de operar.

2.2.3 Requisitos no funcionales:

- Dispositivos soportados: el sistema debe ser compatible con gran variedad de dispositivos, ya que la infraestructura del centro no es homogénea.

- Escalabilidad: el sistema debe proporcionar la base para incluir en futuros desarrollos la monitorización de otros dispositivos como servidores o bases de datos.

- Software libre: el sistema debe estar basado en software libre

- Soporte: el sistema debe estar basado en un software con soporte. Dada la criticidad de la infraestructura, es imprescindible el uso de software contrastado y con una comunidad de soporte ante posibles fallas.

Para afrontar estos desafíos y mejorar la calidad del servicio ofrecido se propone la implementación de un sistema de monitorización de la red, donde se consideren todos los switches presentes en la infraestructura del complejo hospitalario.

2.3 Análisis de herramientas

Dada la complejidad de los requisitos mencionados anteriormente, es crucial explorar y evaluar diferentes opciones de sistemas de monitorización.

En el proceso de análisis se han evaluado distintas soluciones para la monitorización de red, incluida la posibilidad de desarrollar una solución personalizada desde cero, con el objetivo de ver cual se adapta más a los requisitos propuestos durante el análisis. Sin embargo, se ha determinado utilizar una solución basada en CheckMK tras el siguiente análisis:

2.3.1 Desarrollo de una herramienta nueva

Esta opción aporta la ventaja de la personalización total, lo que significa que se podría diseñar una solución que se adapte exactamente a las necesidades específicas del hospital. Sin embargo, la ausencia de un soporte especializado o una comunidad la hacen inviable. Al tratarse de un entorno tan crítico no se puede asumirse este riesgo ante futuros problemas o necesidades que puedan surgir.

2.3.2 CheckmMK

CheckMK se trata de un software libre que cuenta con una comunidad de usuarios activa y un equipo de soporte, lo que garantiza alto nivel de repuesta y ayuda en caso de problemas. Además, ofrece una interfaz web intuitiva y amigable que reduce la curva de aprendizaje, facilitando la implementación y la operación. El software es capaz de monitorizar todo tipo de dispositivos: switches, servidores, bases de datos…

Por otro lado, brinda la capacidad de personalización y extensibilidad, lo que permite adaptar la solución a las necesidades específicas del hospital. La gestión eficiente de eventos y notificaciones, la monitorización en tiempo real y la implementación más rápida en comparación con el desarrollo desde cero son otras ventajas presentes. Se puede instalar sobre un sistema operativo Linux sin necesidad de muchos recursos.

La principal desventaja de CheckMK radica en la ausencia de un sistema especifico de monitorización de intentos de intrusión, sin embargo, es algo que se puede salvar mediante el desarrollo y adaptación de su consola de eventos.

2.3.3 Otras alternativas

Además, es importante destacar que otras herramientas de monitorización, como Nagios, Zabbix y Prometheus, ofrecen ventajas, como comunidades activas y flexibilidad, pero a menudo presentan una mayor complejidad demasiado elevada en la configuración inicial y menos opciones de personalización.

Figura 6: comparativa de software de monitorización

CheckMK [8] es la herramienta que mejor se adapta a las necesidades del proyecto. Cuenta con las características y funciones necesarias para cumplir con los requisitos técnicos, además de ser una solución robusta y escalable. La ausencia de un sistema específico de monitorización de intentos de intrusión se puede salvar mediante el desarrollo y adaptación de su consola de eventos.

Por otro, cumple con los requisitos establecidos anteriormente: es un software libre, proporciona monitorización en tiempo real, es compatible con una amplia variedad de dispositivos yes relativamente sencillo de implementar.

3. Diseño

En esta fase de diseño, se propone la implementación de un sistema de monitoreo de red integral que aborde los problemas identificados en el análisis y cumpla con los requisitos previamente establecidos.

Estos sistemas se basan en el protocolo SNMP. Este protocolo se desarrolla en la capa de aplicación y facilita el intercambio de información del estado de los dispositivos a un gestor SNMP (NMS), mediante el uso de dos puertos UDP (161 y 162). En este contexto, podemos dividir los dispositivos en dos tipos: servidor y agente:

1. Servidor (NMS): es el servidor donde se despliega el software de monitorización. Su función es recoger y guardar todos los datos de los agentes o dispositivos finales. Este dispositivo tiene capacidad tanto puede hacer un pool a los agentes, solicitándoles información de su estado y como para recibir las alarmas o traps de los agentes.

2. Un agente: es un servicio que se instala en los dispositivos finales y se encarga de atender las peticiones que realice el servidor o de enviar un trap cuando se produzca un evento. En este caso no es necesario instalar ningún agente, ya que los propios switches lo llevan integrado, por lo que tan solo habrá que activarlo y configurarlo correctamente

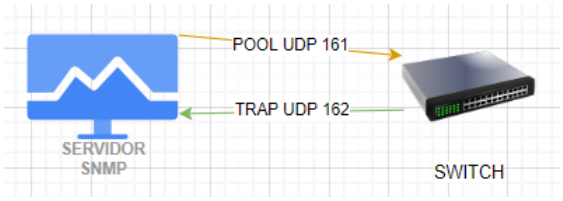


Figura 7: diagrama protocolo SNMP

SNMP es capaz de interpretar cualquier dato y hacerlo legible para los operadores, por ejemplo, una switch nos puede enviar un trap cuando se ha producido un intento de intrusión o cuando una interface tiene errores, el gestor SNMP tiene que ser capaz de interpretar ambos datos.

Para ello, el protocolo utiliza unas pequeñas bases de datos donde se describen y detalla cada información que se puede enviar o recibir llamadas managment information base (MIB), las cuales contienen la información organizada jerárquicamente mediante identificadores de objetos (OID), que definen qué valores e información pueden tener.

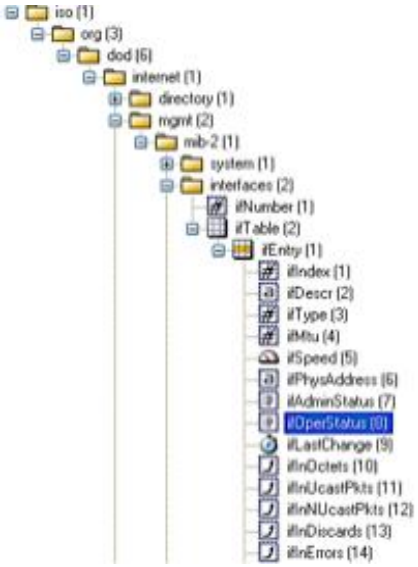


Figura 8: MIB

Como se observa en la imagen, un MIB se organiza en una estructura jerárquica donde dentro de cada "carpeta", tenemos una serie de directorios e identificadores. En esta MIB podemos ver qué datos vamos a obtener del equipo, por ejemplo, la velocidad de la interface o el estado. Cada dato que podemos obtener es un OID y generalmente, tienen una descripción de qué tipo de dato es (numérico, texto) o qué valores se pueden recibir.

De este modo, el servidor de monitorización y el agente SNMP del switch, pueden intercambiar información procesable que nos ayude a administrar una infraestructura de red tan compleja como la de un centro hospitalario.

3.1 Solución propuesta

La solución propuesta se centra en la implementación de un sistema de monitorización basado en CheckMK como solución para abordar las problemáticas identificadas durante el análisis. Se trata de un software libre que permite la monitorización de la red gracias al protocolo SNMP [9] y el análisis proactivo de la red.

Un sistema de monitorización realiza sondeos regulares a los switches mediante el protocolo SNMP, evaluando parámetros como el tráfico, la utilización de recursos y la tasa de errores, lo que permite una evaluación constante del estado operativo de la red. Al detectar anomalías, estos sistemas pueden enviar alertas automáticas, notificando a los administradores de red a través de canales definidos, proporcionando detalles específicos sobre la naturaleza de la incidencia, lo que permitirá una intervención rápida.

Por otro lado, se puede realizar un mapeo completo de las interfaces SNMP de todos los switches en la infraestructura, conociendo asi la disponibilidad de puertos, su estado operativo y cualquier cambio en la conectividad. Esto permitirá generar informes sobre la disponibilidad de puertos, proporcionando a

los administradores una visión detallada de la capacidad actual y permitiéndoles planificar expansiones según sea necesario.

La integración de la solución con el NAC permitirá la identificación de conexiones no autorizadas en tiempo real, mediante la supervisión de cambios en las direcciones MAC y el estado de las interfaces de los switches. Los eventos relacionados con intentos de intrusión se registrarán de manera detallada, proporcionando un historial que facilita la investigación y la implementación de medidas correctivas.

Un sistema de monitorización basado en CheckMK ofrece infinitas posibilidades y componentes, pero en este proyecto nos centraremos principalmente en tres de ellos, los cuales cumplimentarán los requisitos y darán solución a las problemáticas detectadas durante la fase de análisis.

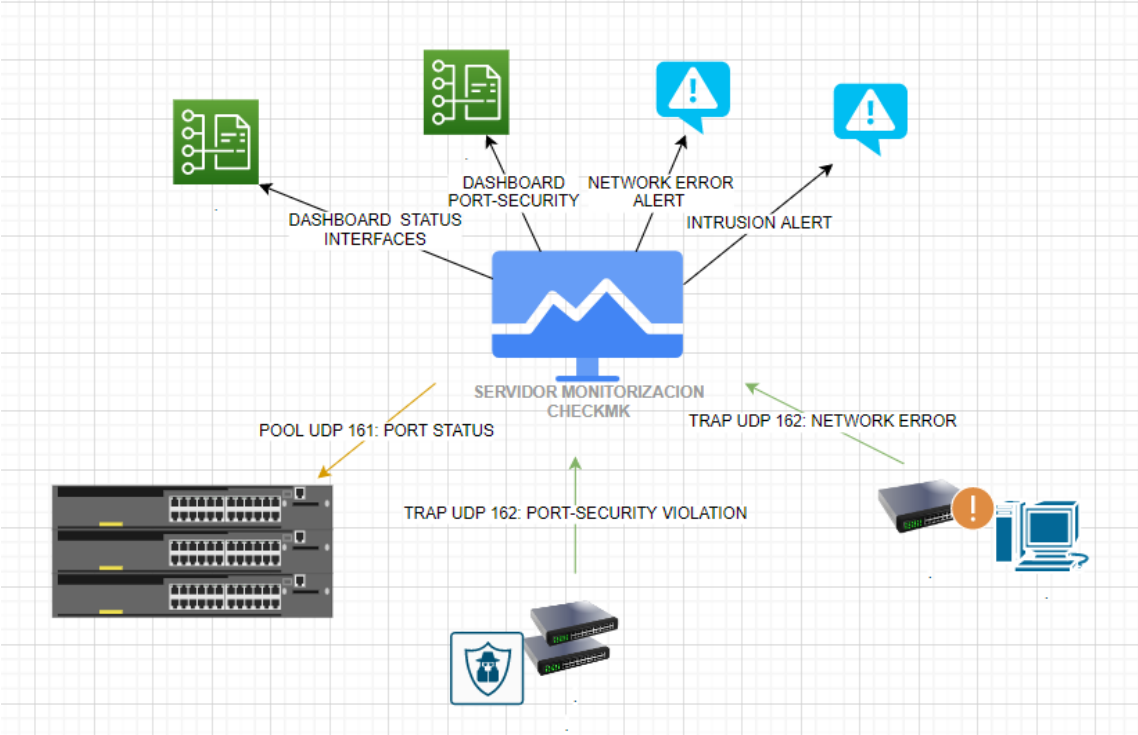


Figura 9: diagrama solución propuesta

En el siguiente apartado se detallará el papel de cada uno de estos componentes y los nuevos flujos de trabajo que lo solución implementará.

3.2 Componentes clave del sistema

A continuación, se muestran los componentes del sistema de monitorización y sus flujos de trabajo, con lo que se pretende cubrir los requisitos y dar respuesta a los problemas detectados en el análisis de la operativa actual.

3.2.1 Detección de incidencias de red

Con la implementación del sistema de monitorización se pretende monitorizar los switches de toda la infraestructura en tiempo real, gracias a la capacidad que le proporciona la tecnología SNMP para detectar las incidencias de red, generando alertas a los operadores y registrando la incidencia de manera automática en el sistema de ticketing.

De este modo, cuando un switch emite una trap SNMP debido a una anomalía, el sistema de monitorización recibe la notificación inmediatamente y activa los procedimientos de respuesta predefinidos, eliminando la necesidad de que los usuarios informen manualmente sobre incidencias. Asi se garantiza que el personal técnico sea alertado de inmediato ante cualquier problema en la red de manera que pueda empezar a trabajar en la solución de manera inmediata, en ocasiones incluso antes de que el usuario perciba el fallo.

Figura 10: flujo de trabajo incidencias de red

Con esta funcionalidad se pretende acabar con la problemática descrita por la dependencia de una comunicación manual de los usuarios con el centro de atención al usuario cuando se produce un fallo en la red, lo que conlleva algunos inconvenientes que aumentan el tiempo de respuesta como la falta de detección temprana de problemas o la saturación del centro de atención al usuario.

3.2.2 Inventariado y capacidad de la infraestructura

CheckMK se integra con los switches, mediante SNMP, lo que permite el monitoreo constante de la capacidad de puertos en tiempo real. El sistema recopila datos sobre el estado de los puertos, incluida su disponibilidad y ocupación, brindando a los técnicos de campo una visión actualizada de cuántos puertos están libres en cada switch y, por lo tanto, permite una planificación previa más eficaz a la hora de desplegar equipamiento nuevo.

El switch mantiene una tabla de puertos que almacena información sobre cada uno de sus puertos físicos. Checkmk utiliza SNMP para consultar esta tabla, conocida como la MIB ifTable (Management Information Base). En esta tabla, se almacenan detalles como el estado del puerto (activo, inactivo), la velocidad del enlace, el tipo de conexión, entre otros que servirán para determinar al sistema de monitorización si el puerto está libre o en uso.

El sistema de monitorización mostrará un dashboard con la información de todos los switches, por lo que los equipos de TIC pueden planificar de manera proactiva

las ampliaciones necesarias en la infraestructura de red, evitando situaciones en las que los técnicos de campo se enfrentan a la falta de puertos disponibles y garantizando que en todo momento la infraestructura disponga de suficiente capacidad para el despliegue de nuevos dispositivos.

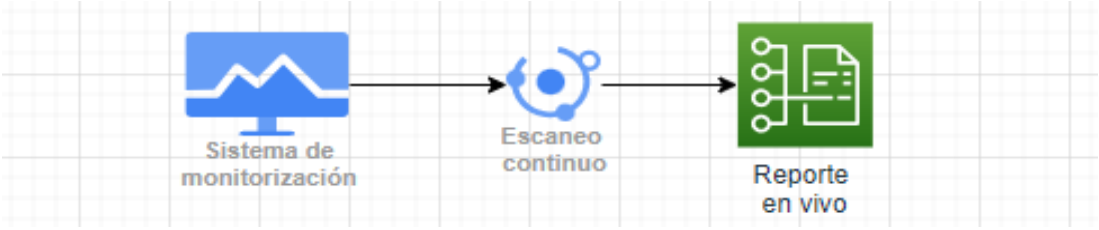


Figura 11: flujo de trabajo reporte capacidad

Esta capacidad de la solución propuesta aborda de manera efectiva la problemática identificada durante el análisis relacionada con la capacidad de la infraestructura y la falta de puertos disponibles en las electrónicas para instalar nuevos equipos o dispositivos críticos.

Por otro lado, con este componente tambien se cubre la necesidad de disponer de un inventario completo con todos los datos de los switches que forman parte de la infraestructura del centro.

3.2.3 Detección de intentos de intrusión

Debido a que CheckMK no dispone de un componente específico para este tipo de eventos, la solución propuesta para abordar este desafío implica la transformación de la consola de eventos en un dashboard personalizado que muestre todos los intentos de intrusión en tiempo real. Esta herramienta proporcionaría a los técnicos de campo una herramienta eficaz con datos claros sobre la ubicación exacta de la roseta afectada y el switch al que está conectada.

Para lograr esto, es necesario activar la funcionalidad SNMP traps en los switches de la infraestructura, la cual permite que estos dispositivos envíen notificaciones asincrónicas a nuestro servidor de monitorización. Una vez que los SNMP traps estén en funcionamiento y se reciban en el servidor de monitorización, se debe llevar a cabo un proceso de análisis para identificar aquellos que corresponden a intentos de intrusión, por ejemplo, identificándose los OID de los eventos que se reciben cuando se produce una conexión no autorizada.

Esta investigación llevará a la creación de filtros personalizados que permitirán separar los traps que correspondan con intentos de intrusión del resto, lo que permitirá convertir la consola de eventos de CheckMK en un visor de intentos de intrusión altamente eficaz. De este modo, los operadores de red y los técnicos de campo tendrán disponible la información de manera clara y ordenada. Además, existirá la posibilidad de generar una alarma de notificación si asi lo requiere el centro.

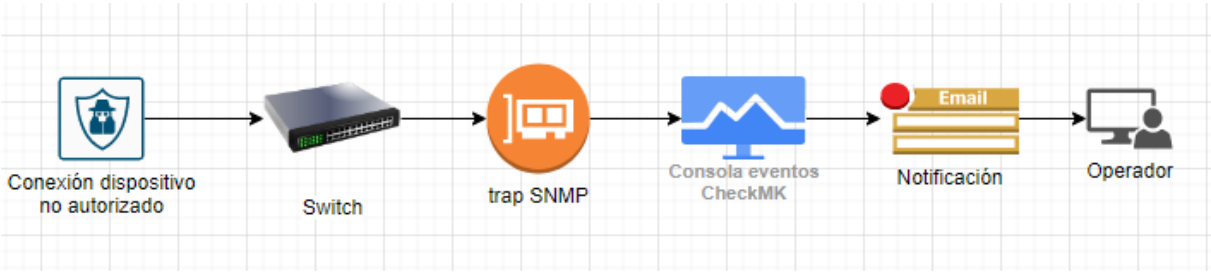


Figura 12: flujo de trabajo intento de intrusión

Con esta adaptación se pretende mitigar algunos de los inconvenientes causados por el shadow IT, responsable de una pérdida de tiempo significativa por parte de los técnicos de campo al intentar localizar las rosetas desactivadas debido a intentos de intrusión en la red del hospital y que en algunos casos ha llevado a que los operadores de sistemas a realizar una búsqueda exhaustiva en los registros de cada switch de forma manual, lo que resulta en una pérdida de recursos y una respuesta lenta ante posibles amenazas de seguridad.

3.2.4 Otras funcionalidades

El sistema de monitorización tiene un diseño abierto y está pensado para incorporar nuevas funcionalidades a medida que vaya evolucionando. Si bien estas utilidades no quedaran implementadas en el alcance de este proyecto, el sistema diseñado será fácilmente ampliable.

Una de las futuras ampliaciones que podrán llevarse a cabo es la monitorización de una interfaz concreta de un switch, con esto se puede garantizar la conectividad de un dispositivo crítico que siempre deba estar siempre encendido.

Por otro lado, tambien se podrían analizar las estadísticas de uso para comprobar si los usuarios siguen la política de ahorro energético del centro, según la cual, los puestos de trabajo deben quedar apagados una vez que ha finalizado su jornada laboral.

4. Implementación

Para llevar a cabo la implementación del sistema de monitorización se deben realizar las siguientes configuraciones:

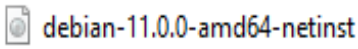
1. Instalación y configuración del sistema operativo base del servidor
2. Instalación y configuración del software de monitorización CheckMK en el servidor
3. Configuración SNMP de los switches
4. Alta de hosts a monitorizar en CheckMK
5. Configuración del sistema de alertas y notificaciones
6. Adaptación de la consola de eventos como registro de intentos de intrusión

4.1 Instalación del servidor

4.1.1 Instalación y configuración del sistema operativo

En el proceso de implementación del sistema de monitorización de red, se ha tomado la decisión de utilizar Debian [10] como sistema operativo para el servidor, ya que es la distribución utilizada como corporativa en el centro y es compatible Checkmk. Se usará el entorno de virtualización de desarrollo del centro basado en Proxmox.

El primer paso fue descargar la ISO de la web oficial de Debian:



Posteriormente se creó la maquina en el entorno de virtualización y se instaló la versión del sistema operativo sin entorno gráfico para consumir los mínimos recursos. Una vez instalado el sistema operativo, el siguiente paso fue configurar los parámetros de red, asignando una IP estática al servidor.

```
root@jcanero:~# nano /etc/network/interfaces
  GNU nano 5.4                        /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# Configuracion IP estatica
auto ens18
iface ens18 inet static
address 10.72.2.57
netmask 255.255.224.0
gateway 10.72.0.97
```

Figura 13: configuración IP del servidor

Al tratarse de una red corporativa, también fue necesario configurar los DNS y el proxy para el sistema y para los repositorios:

```
 GNU nano 5.4                                                    /etc/resolv.conf
nameserver 10.72.0.1
nameserver 10.72.0.71
```

Figura 14: configuración DNS y proxy del servidor

Ademas, se configuraron los siguientes repositorios:

```
 GNU nano 5.4                                                    /etc/apt/sources.list
#Contrib

deb http://deb.debian.org/debian/ bullseye main
deb-src http://deb.debian.org/debian/ bullseye main

deb http://security.debian.org/debian-security bullseye-security main contrib
deb-src http://security.debian.org/debian-security bullseye-security main contrib

deb http://debian.org/debian/ bullseye-updates main contrib
deb-src http://debian.org/debian/ bullseye-updates main contrib

#Non-free--i

deb http://deb.debian.org/debian bullseye main contrib non-free
deb-src http://deb.debian.org/debian bullseye main contrib non-free

deb http://deb.debian.org/debian-security bullseye/updates main contrib non-free
deb-src http://deb.debian.org/debian-security bullseye/updates main contrib non-free

deb http://deb.debian.org/debian bullseye-updates main contrib non-free
deb-src http://deb.debian.org/debian bullseye-updates main contrib non-free

#Backports

deb http://deb.debian.org/debian bullseye-backports main contrib non-free
deb-src http://deb.debian.org/debian bullseye-backports main contrib non-free
```

Figura 15: configuración repositorios del servidor

4.1.2 Instalación del sistema de monitorización

Una vez instalado y configurado el sistema operativo, el siguiente paso fue descargar e instalar el software CheckMK:

```
root@jcanero:~# apt install /home/jcanero/check-mk-raw-2.2.0p5_0.bullseye_amd64.deb
```

Figura 16: instalación de CheckMK

Antes del primer arranque, fue necesario crear un site nuevo, lo que generó un usuario y un grupo en el sistema operativo con el nombre indicado, asi como una configuración básica para el nuevo site

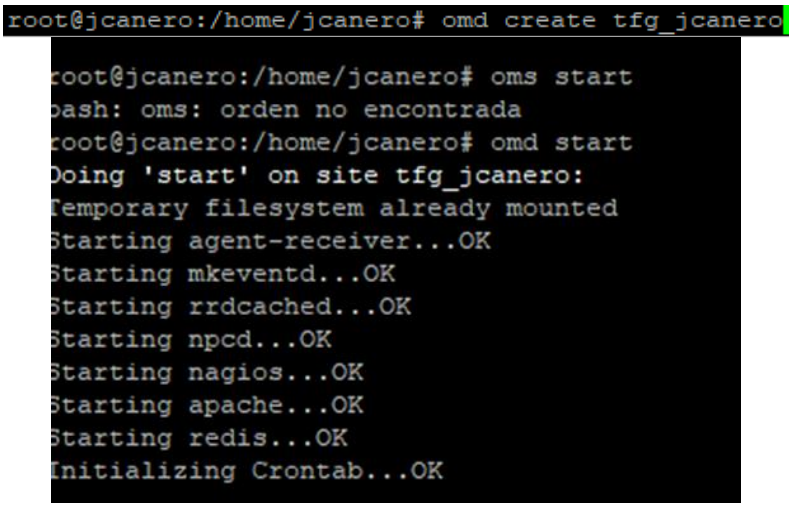


Figura 17: creación de site para CheckMK

Ahora ya se pudo ejecutar el sistema, comprobando que todos los servicios arrancan correctamente y es accesible acceder vía web.

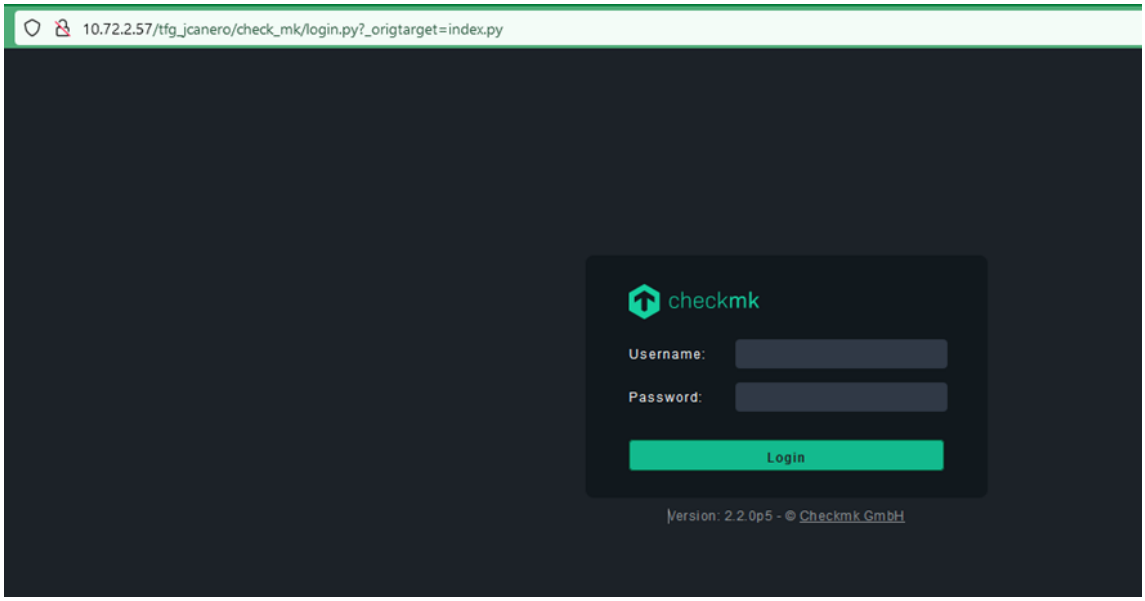


Figura 18: pantalla de login CheckMK

Para aumentar la seguridad del sistema, se cambió la password de acceso a la interfaz web

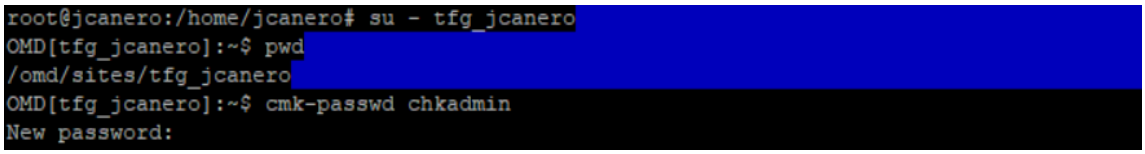


Figura 19: cambio de credenciales CheckMK

Y se verificó el correcto acceso al sistema con las nuevas credenciales. Para garantizar la seguridad del sistema, se añadirá al protocolo de cambio de contraseñas del centro, el cual determina la fecha en la que la contraseña debe renovarse.

4.2 Configuración de los switches

En esta fase de la implementación del sistema de monitorización de red se lleva a cabo la configuración de los switches para habilitar el protocolo SNMP y permitir el envío de SNMP traps.

La configuración SNMP permite que nuestro sistema de monitorización acceda a información crítica de los switches, lo que permitirá detectar caídas de red y saber la capacidad exacta de cada switch en tiempo real. Con la activación de los trap SNMP se pretende poder adaptar la consola de eventos de CheckMK, convirtiéndola en un dashboard que muestre los intentos de intrusión.

Además, es esencial destacar que, debido a la diversidad de switches de cuatro fabricantes distintos en nuestra infraestructura, se necesitó realizar cuatro tipos de configuraciones específicas.

A continuación, se detallan los comandos usados para cada uno de los switches que componen la infraestructura de red del centro según su fabricante [11] [12] [13] [14]

4.2.1 Configuración SNMP en HP

Se habilita el servicio snmp para poder monitorizar el switch:

snmp-server enable

Se configura la comunidad en modo solo lectura:

snmp-server community 1234 ro

Se habilita el envío de trap hacia el servidor de monitorización:

snmp-server host 10.72.2.57 community "1234" trap-level all

4.2.2 Configuración SNMP en Aruba

Se habilita el servicio snmp para poder monitorizar el switch:

snmp-server enable

Se configura la comunidad en modo solo lectura:

snmp-server community 1234 ro

Se habilita el envío de trap hacia el servidor de monitorización:

snmp-server host 10.72.2.57 trap version v2c community 1234

4.2.3 Configuración SNMP en Cisco

Se habilita el servicio snmp para poder monitorizar el switch:

snmp-server enable

Se configura la comunidad en modo solo lectura:

snmp-server community 123 RO

Se habilita el envío de trap relacionados con port-security:

snmp-server enable traps port-security

Se configura receptor de traps indicando la IP y comunidad:

snmp-server host 10.72.2.57 1234

4.2.4 Configuración SNMP en Huawei

Se habilita el servicio snmp para poder monitorizar el switch:

snmp-agent

Se configura la comunidad en modo solo lectura:

snmp-agent community read 1234 mib-view View_ALL

Se habilita el envío de trap:

snmp-agent trap enable

Se configura receptor de traps indicando la IP y comunidad:

snmp-agent target-host trap address udp-domain 10.72.2.57 params securityname 1234 v2c

4.3 Alta de hosts en CheckMK

El siguiente paso fue el alta de los hosts (switches) en el sistema de monitorización, para ello se usó de base el inventario generado previamente, en el que se disponía de IP, nombre y ubicación de cada dispositivo.

Para facilitar la organización y gestión de la herramienta, se crearon una serie de carpetas con los nombres de los distintos edificios que forman el complejo hospitalario. Estas carpetas servirán como contenedor lógico para los switches ubicados en ese edificio.

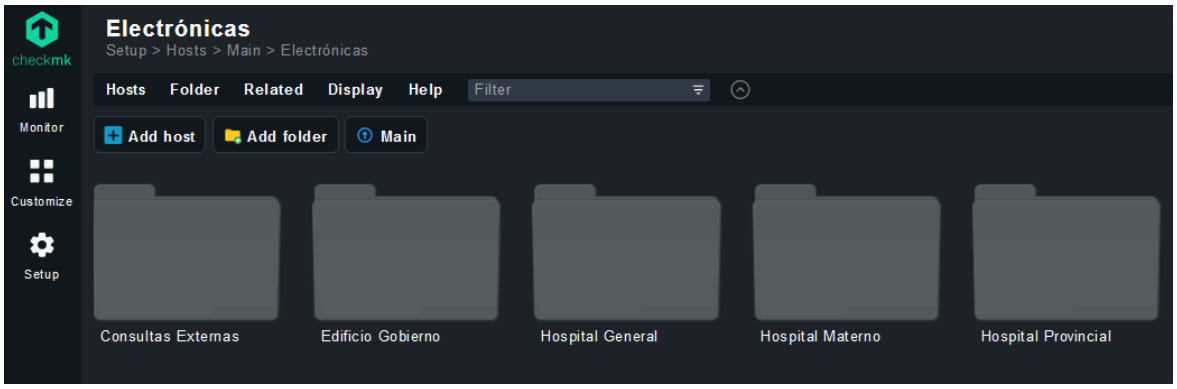


Figura 20: organización de hosts por carpetas

Esta organización por carpetas permite aplicar reglas comunes que aplicaran a todos los hosts que contienen, lo que facilita por ejemplo la configuración de la community usada en el protocolo SNMP. En la siguiente ilustración se muestra la configuración de la carpeta raíz, de donde colgaran el resto de las carpetas, heredando las reglas jerárquicamente.

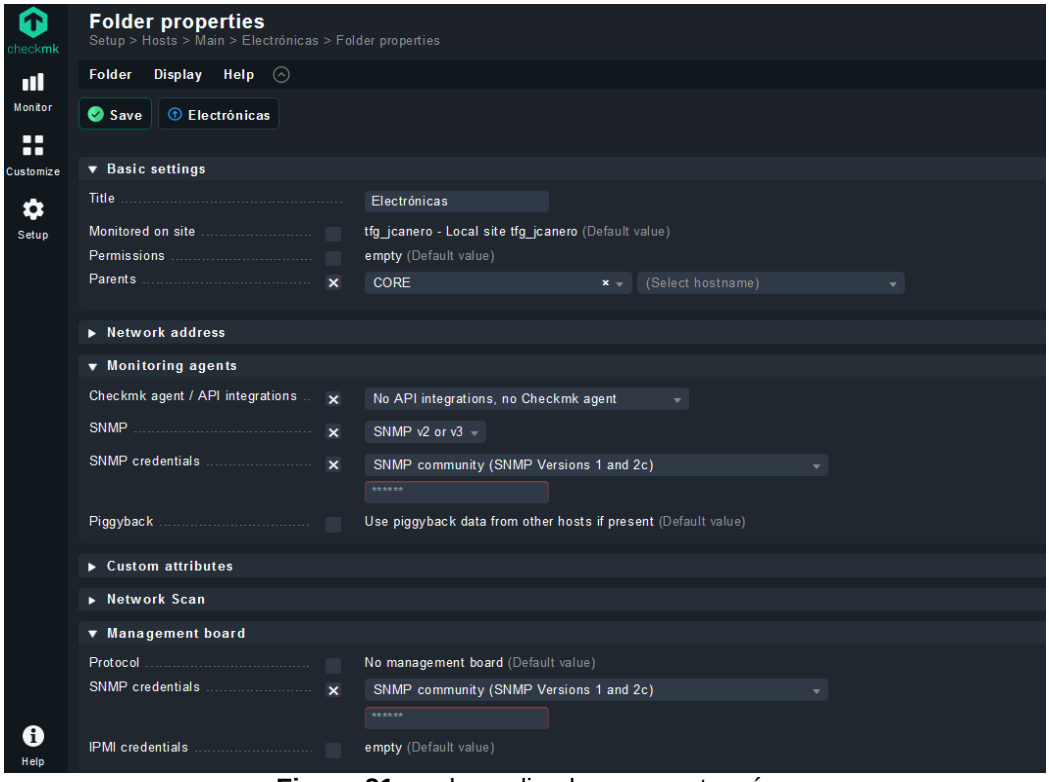


Figura 21: reglas aplicadas a carpeta raíz

Durante el proceso de alta de cada host, además de indicar la IP, se ha introducido como hostname la misma nomenclatura usada como hostname en los switches, lo que facilitará saber de qué switch se trata.

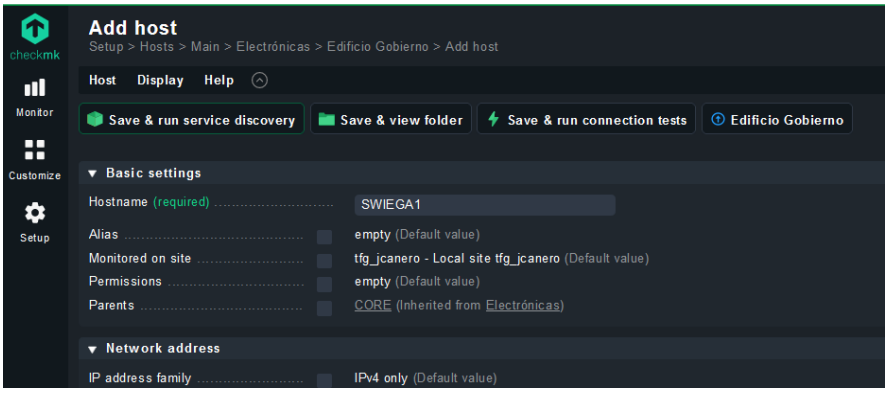


Figura 22: pantalla para añadir un host

Además, durante el alta de los switches, se ha indicado la dependencia de cada uno de ellos, lo que dará lugar a la generación de un mapa de red que permitirá a los operadores detectar los puntos críticos de la infraestructura y tomar algunas medidas proactivas como la configuración de LACPs que permitan la conectividad en caso de falla en alguna de las fibras.

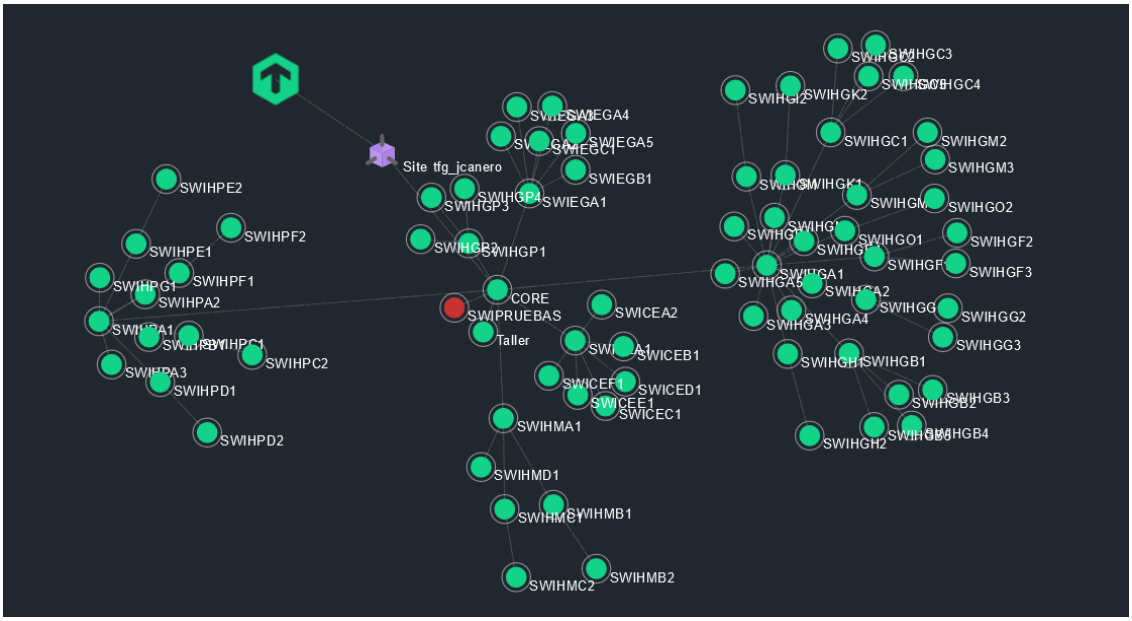


Figura 23: mapa de red

Los switches configurados como pilas, el sistema los detecta como un solo hosts, sin embargo, es capaz de detectar si se produce fallo en cualquiera de sus miembros. En total se han dado de alta 5 carpetas, que contienen un total de 75 hosts y 128 dispositivos físicos.

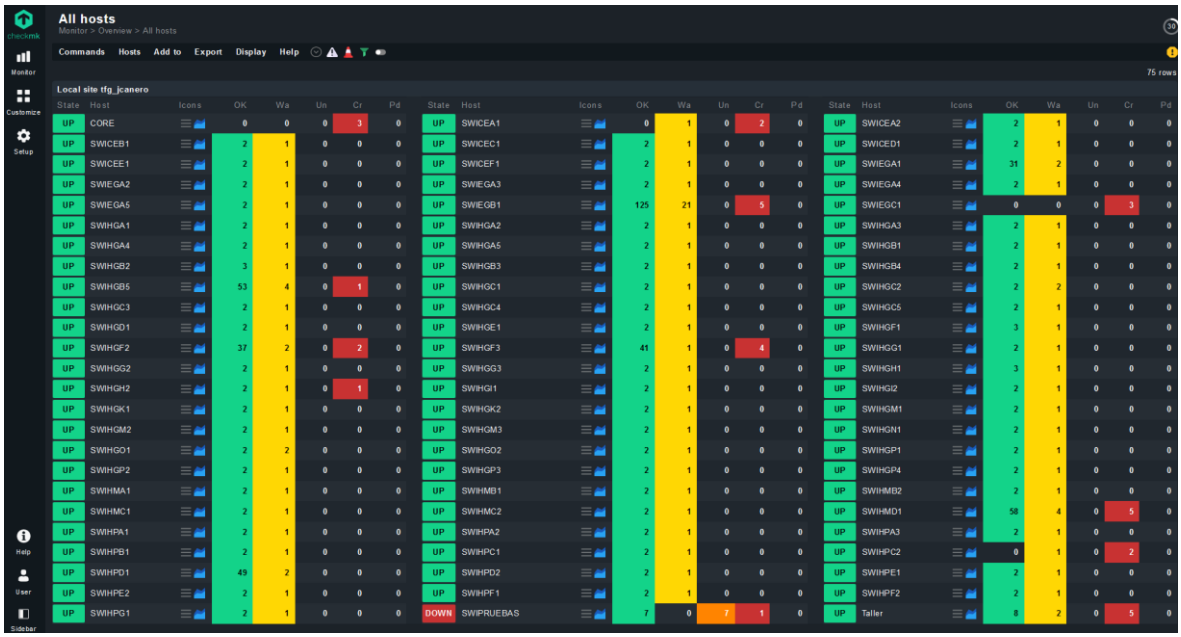


Figura 24: listado de hosts dados de alta

En cuanto a los servicios a monitorizar, desde la dirección del centro se ha solicitado que se incluyan todos los disponibles, entre los que se incluye conectividad, estado de la CPU, temperatura, estado de los ventiladores, fuente de alimentación o memoria entre otros. Para ello ha sido necesario entrar en la configuración de cada host y realizar un descubrimiento.

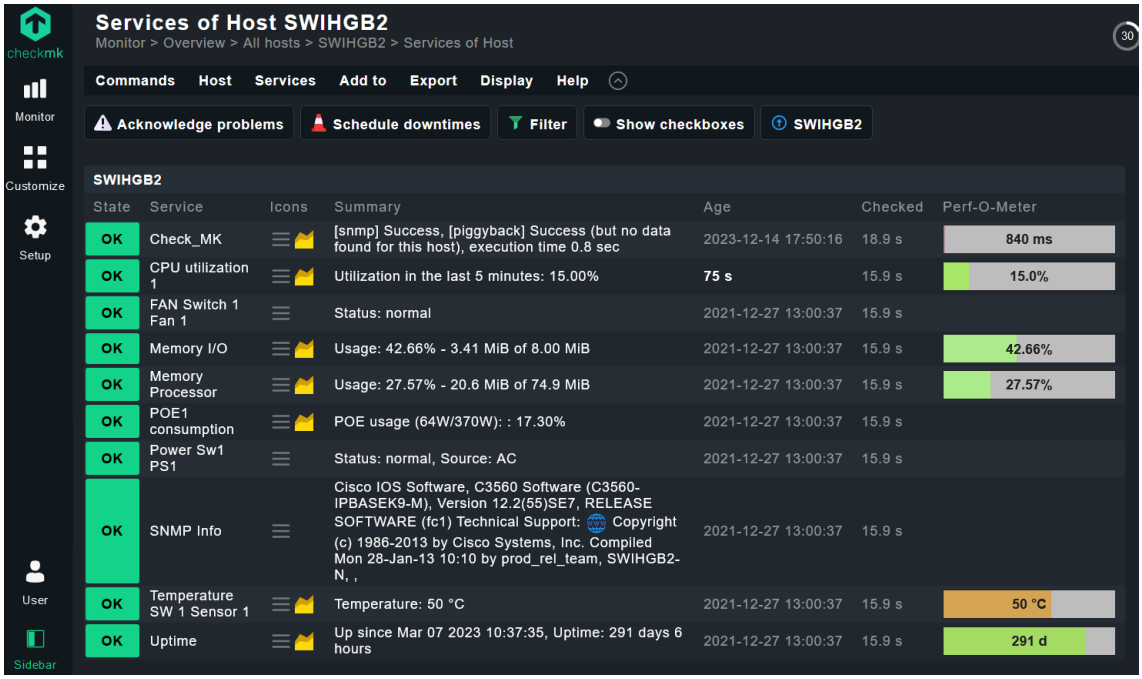


Figura 25: servicios descubiertos en un switch Cisco

Debido a la heterogeneidad de la infraestructura, nos encontramos con distintos servicios según el fabricante del dispositivo, sin embargo, se comprueba que todos permiten cubrir dos de los requisitos base del proyecto: detectar falta de conectividad en un dispositivo y conocer el estado de sus interfaces en tiempo real.

4.4 Configuración de alertas

La configuración de alertas y notificaciones en el sistema de monitorización es esencial para garantizar una respuesta efectiva a los problemas y amenazas que puedan surgir en los switches de la infraestructura de red del entorno hospitalario, lo que permite una acción rápida para minimizar el tiempo de inactividad.

Si en el apartado anterior se decidió monitorizar todos los servicios, en una primera fase de implementación se configuró el sistema para que solo envíe alertas cuando se produzca una falta de conectividad con el dispositivo, es decir, cuando un switch no responda a ping y cuando la recupere.

Esta decisión está motivada para evitar la saturación de notificaciones, ya que, en un primer momento, con las notificaciones habilitadas para todos los eventos se comprobó que la cantidad de avisos recibidos era imposible de gestionar y la

mayoría de ellas no aportaban mucho valor (up/down de puertos, warning de temperaturas…). En próximas revisiones se evaluará la posibilidad de ampliar los umbrales.

Se ha decidido que el canal de notificación será por correo electrónico durante el horario laboral y por SMS fuera de él, asegurando asi que el técnico de guardia recibirá alertas en su telefono sin tener que estar conectado a internet para revisar el email. Para ello se han configurado distintos grupos de notificación y se han aplicado las reglas a la carpeta raíz.

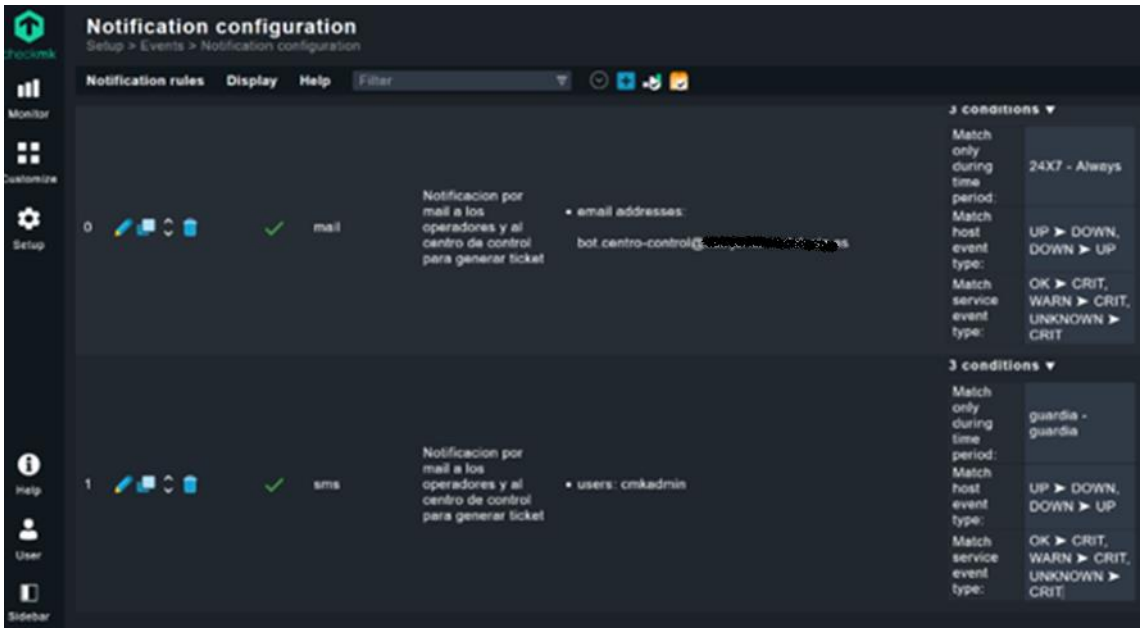


Figura 26: configuración de notificaciones

En la imagen anterior se muestra los dos tipos de notificaciones configurados en el sistema. En el primer caso, la notificación consistirá en el envió de un correo a los emails indicados durante ventana horaria, sin embargo, en el segundo caso, la notificación se realizará mediante el envío de un mensaje SMS y solo aplicará en el horario de guardia. En cuanto a los servicios que provocan el envío de la alerta en ambos casos son los mismos: cuando el servidor pierde comunicación con un host (UP → DOWN) y cuando la recupera (DOWN → UP), con el objetivo de que se detecte si se trata de un microcorte.

La notificación por email tambien será enviada a un buzón del centro de operaciones, el cual es procesado por un bot que es capaz de detectar y analizar los correos electrónicos entrantes con un formato determinado para crear una incidencia nueva en el sistema de tickets.

Con esta incorporación, los operadores recibirán los nuevos tickets creados automáticamente y pueden registrar las acciones realizadas para resolver cada incidencia. Esta automatización agiliza la gestión de las incidencias, eliminando la necesidad de que el usuario tenga que reportar el fallo de manera manual y mejorando la eficiencia operativa del equipo de TI.

4.5 Dashboard intentos de intrusión

Para implementar el dashboard que muestre los intentos de intrusión que se han producido se utilizará la consola de eventos de CheckMK, la cual recibe y muestra todos los traps que envían los switches cuando se produce un evento.

Para lograr el objetivo de que solo muestre los intentos de intrusión, se aplicaran filtros para que deseche todos los traps que no cumplan determinados criterios. Tras realizar un análisis de los traps que envían los distintos tipos de switches de la infraestructura cuando se produce un intento de intrusión, se han recopilado los distintos OIDs, los cuales nos servirán para la creación de los filtros.

Se han simulado intentos de intrusión mientras se capturaba el tráfico de la red con la herramienta Wireshark [15] para identificar los traps que generan los switches y poder realizar los filtros

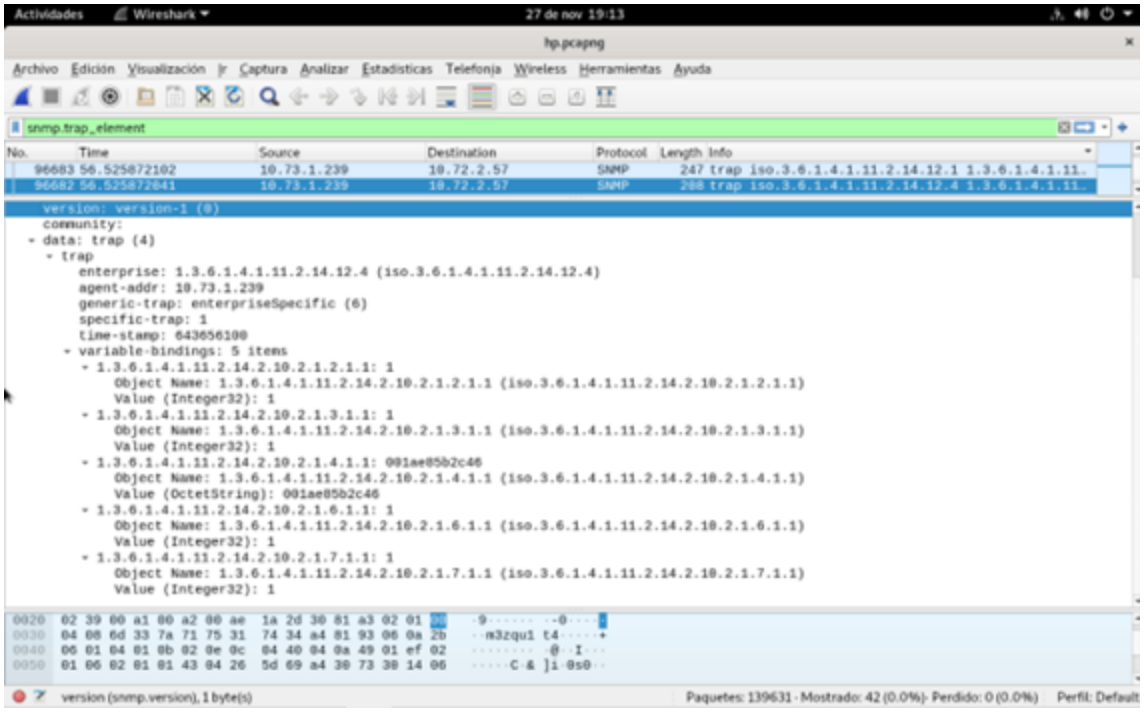


Figura 27: captura de trap port-security violation

En la captura de la imagen se ha capturado una trap de un intento de violación del port-security en un switch HP, se pueden identificar los siguientes OIDs y campos:

- Source: switch donde se ha detectado el intento de intrusión (10.73.1.239)

- Destination: destino del trap (servidor de monitorización 10.72.2.57)
    - Community: palabra de paso usada (****)

- 1.3.6.1.4.1.11.2.14.2.10.2.1.1: índice de esta entrada en el registro de intrusos.

- 1.3.6.1.4.1.11.2.14.2.10.3.1.1: identifica el puerto afectado (1)

- 1.3.6.1.4.1.11.2.14.2.10.4.1.1: contiene la dirección mac (001ae85b2c46)

Una vez aplicados los filtros para los distintos fabricantes, la consola de eventos se ha convertido en un registro de intentos de intrusión, permitiendo al operador ver los registros de toda la infraestructura en tiempo real y en una sola pantalla:

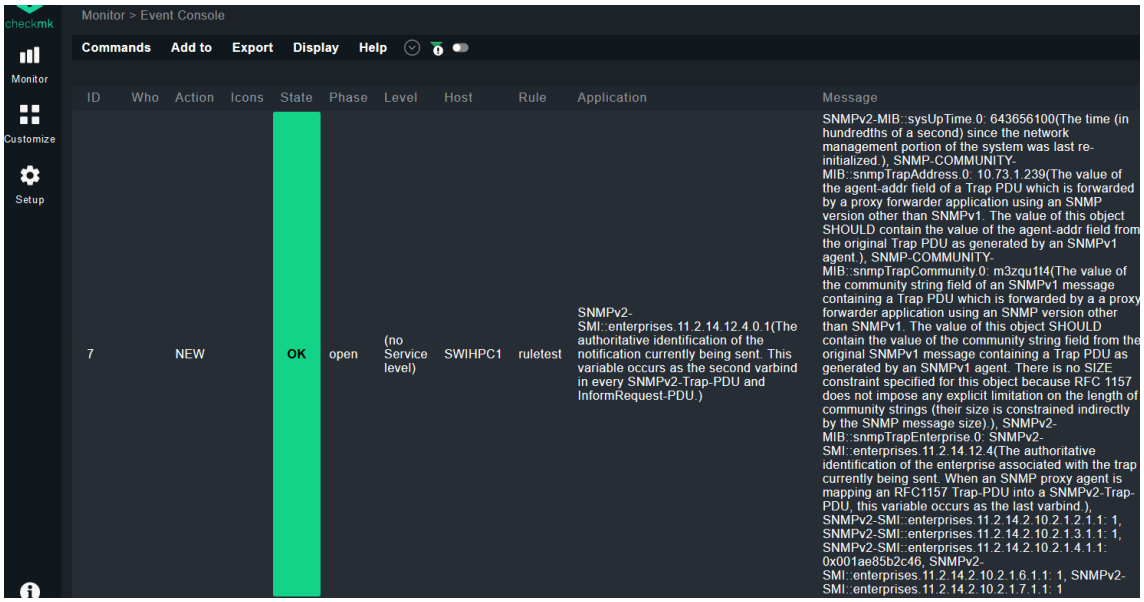


Figura 28: registro de intentos de intrusión

En la imagen se muestra el registro en la consola de eventos del servidor de monitorización, desechando el resto de traps que no corresponden a eventos relacionados con port-security. Si entramos en detalle se puede verificar que el evento ha sido generado por el mismo trap analizado anteriormente:

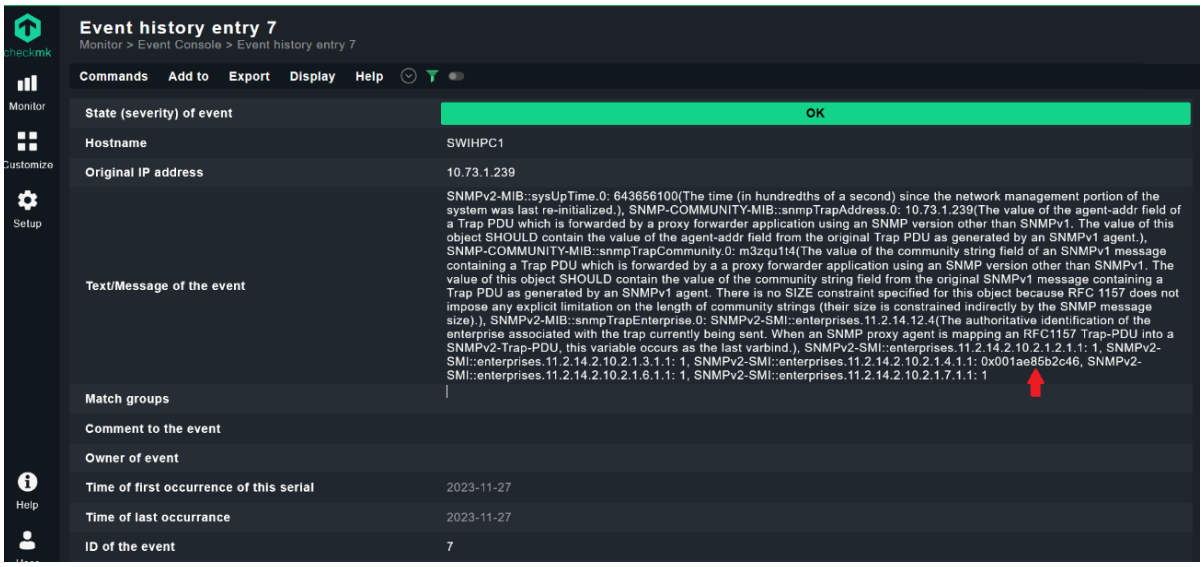


Figura 29: detalle de registro de intento de intrusión

Entre la información que se proporciona destaca el hostname y la IP del switch donde se ha producido el evento, asi como la MAC del infractor (001ae85b2c46) y el puerto del swicth (1).

En caso de incorporar switches de nuevos fabricantes, sería necesario volver a realizar el proceso de captura y análisis de paquetes para identificar los OIDs que usa dicho switch y poder crear el filtro correspondiente. En futuros desarrollos se implementará el uso de diccionarios MIBs personalizados para facilitar la lectura de esta información por parte de los operadores de red.

5. Resultados

Una vez implementado el sistema de monitorización se llevarán una serie de test que garanticen el correcto funcionamiento del sistema y el cumplimiento de los requisitos del proyecto:

- Detección proactiva de incidencias de red y envío automático de notificaciones: se debe probar que el sistema es capaz de detectar la caída de un switch y generar una alerta al equipo de soporte

- Detección en tiempo real del estado de las interfaces de los switches: se debe probar que el sistema proporciona en tiempo real el número de puertos disponibles en cada switch.

- Detección de los intentos de intrusión en tiempo real y almacenado de histórico: se debe probar la capacidad del sistema para detectar un intento de intrusión y generar un registro.

- Inventariado de todos los switches: se debe probar que el sistema aporta información sobre los dispositivos que forman parte de la infraestructura.

- Minimizar consumo de recursos mínimo: evaluar la capacidad del sistema para manejar un gran volumen de datos de monitoreo sin afectar su rendimiento general.

- Facilidad de implementación: el sistema debe quedar implementado de manera funcional antes durante el desarrollo del proyecto.

- Facilidad de operación: obtener retroalimentación del equipo de soporte TIC para evaluar la satisfacción con la herramienta y cualquier mejora que se pueda implementar.

- Dispositivos soportados y escalabilidad: probar la capacidad del sistema para expandirse y manejar la incorporación de nuevos dispositivos o crecimiento en la red sin pérdida de eficiencia o funcionalidad.

- Software libre: comprobar que todo el software usado durante la implementación es software libre

5.1 Detección proactiva de incidencias de red y envío automático de notificaciones

Para evaluar la capacidad de detectar una incidencia de red, se ha añadido a la red un switch nombrado como Taller. Se ha configurado el dispositivo como si de un switch más de producción se tratara y se ha conectado directamente al core.

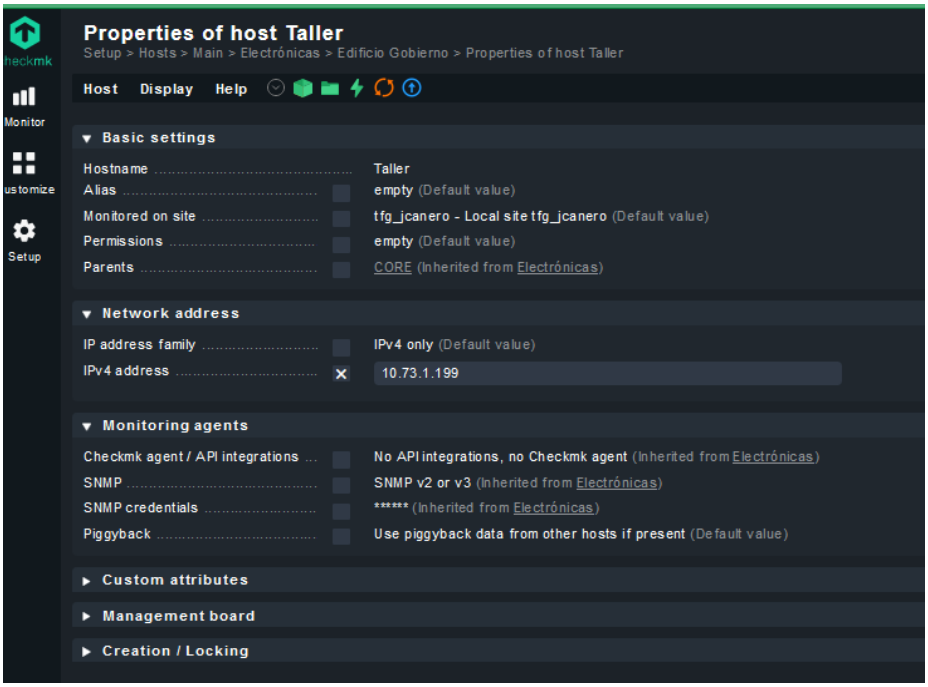


Figura 30: detalle de switch configurado en taller

Una vez comprobado que el dispositivo se está monitorizando correctamente, se ha procedido a desconecta el cable de fibra, dejando el dispositivo sin conectividad. De manera prácticamente instantánea, ha aparecido la alerta en el servidor de monitorización y se ha recibido la notificación por email y SMS.

Figura 31: notificación recibida por email y sms

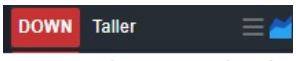


Figura 32: alerta en Check_MK

Se ha reconfigurado el sistema de notificaciones, añadiendo un retraso de cinco minutos para evitar falsas alertas por micro cortes y el reenvío al bot del centro de control para la generación del ticket. Tras ello, se ha vuelto a realizar la prueba con éxito, generándose la incidencia en el sistema de ticketing.

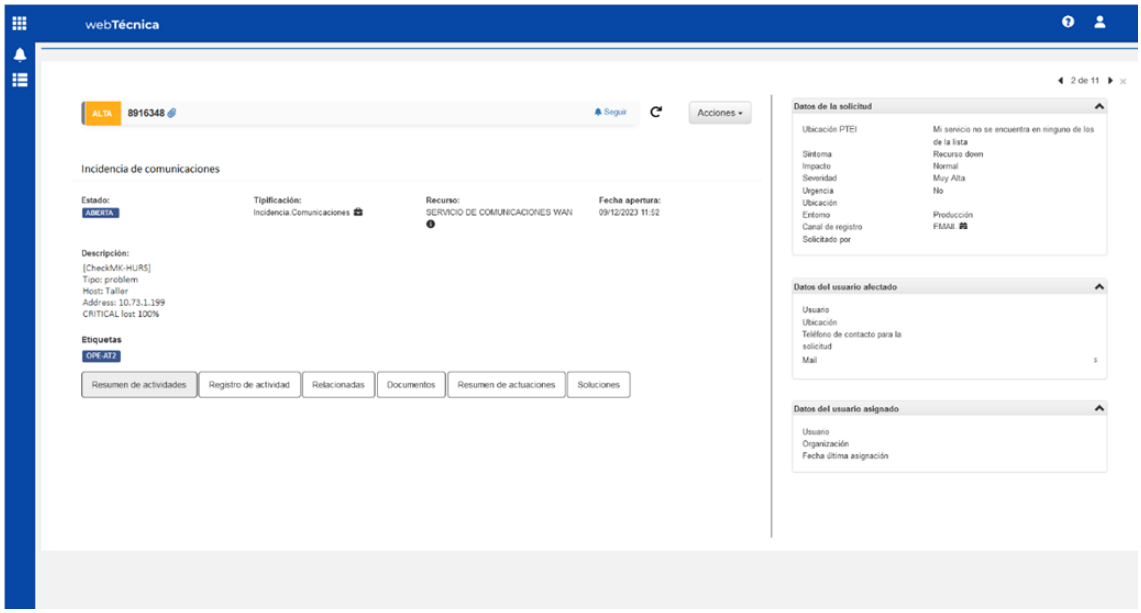


Figura 33: ticket generado por sistema monitorización

5.2 Detección en tiempo real del estado de las interfaces de los switches

El sistema de monitorización cuenta con un dashboard que muestra la disponibilidad de interfaces libres en cada switch que forma parte de la infraestructura

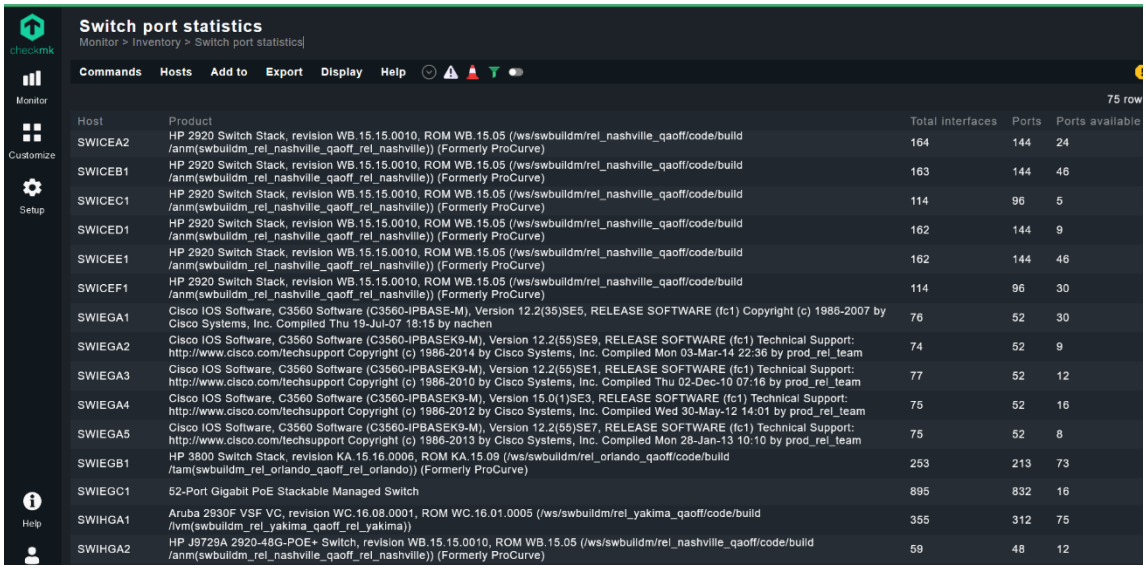
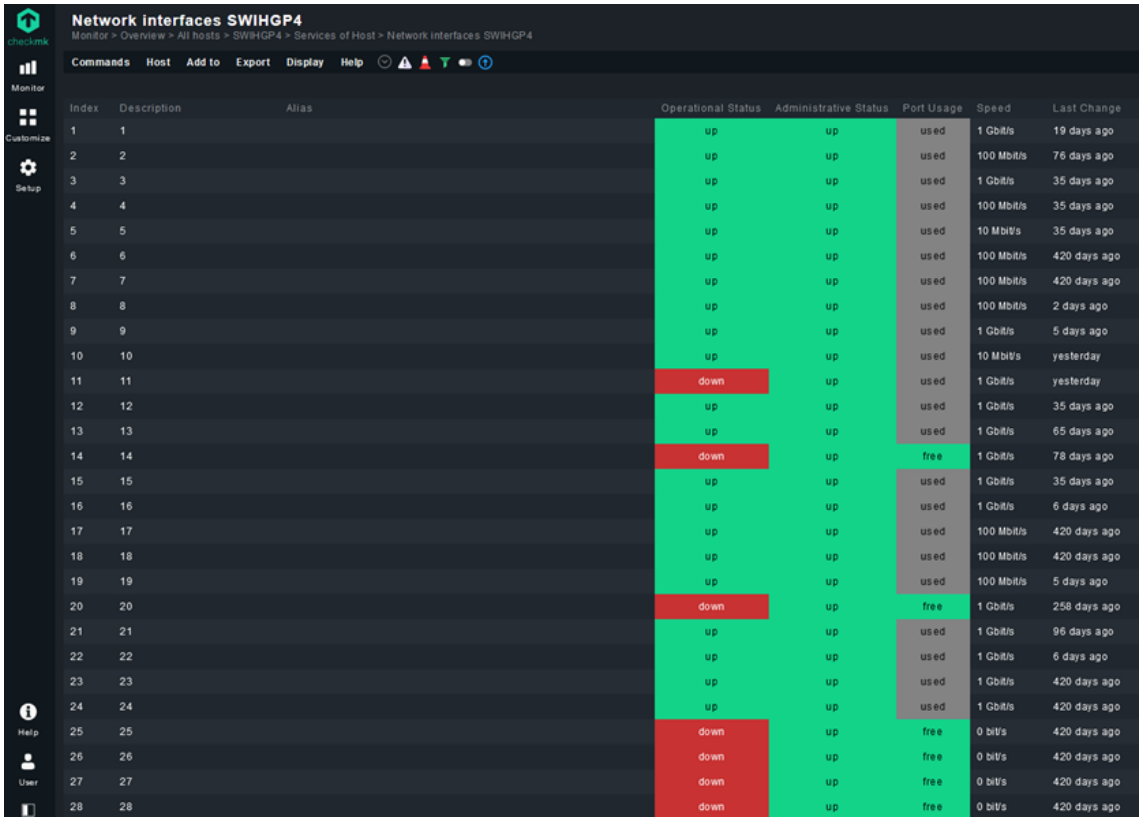


Figura 34: dashboard capacidad de la infraestructura

Para evaluar la fiabilidad de dicha información, se ha entrado en el detalle de uno de los dispositivos, concretamente el SWIHGP4 y se ha hecho una revisión visual del mismo.



Index	Description	Alias	Operational Status	Administrative Status	Port Usage	Speed	Last Change
1	1		up	up	used	1 Gbit/s	19 days ago
2	2		up	up	used	100 Mbit/s	76 days ago
3	3		up	up	used	1 Gbit/s	35 days ago
4	4		up	up	used	100 Mbit/s	35 days ago
5	5		up	up	used	10 Mbit/s	35 days ago
6	6		up	up	used	100 Mbit/s	420 days ago
7	7		up	up	used	100 Mbit/s	420 days ago
8	8		up	up	used	100 Mbit/s	2 days ago
9	9		up	up	used	1 Gbit/s	5 days ago
10	10		up	up	used	10 Mbit/s	yesterday
11	11		down	up	used	1 Gbit/s	yesterday
12	12		up	up	used	1 Gbit/s	35 days ago
13	13		up	up	used	1 Gbit/s	65 days ago
14	14		down	up	free	1 Gbit/s	78 days ago
15	15		up	up	used	1 Gbit/s	35 days ago
16	16		up	up	used	1 Gbit/s	6 days ago
17	17		up	up	used	100 Mbit/s	420 days ago
18	18		up	up	used	100 Mbit/s	420 days ago
19	19		up	up	used	100 Mbit/s	5 days ago
20	20		down	up	free	1 Gbit/s	258 days ago
21	21		up	up	used	1 Gbit/s	96 days ago
22	22		up	up	used	1 Gbit/s	6 days ago
23	23		up	up	used	1 Gbit/s	420 days ago
24	24		up	up	used	1 Gbit/s	420 days ago
25	25		down	up	free	0 bit/s	420 days ago
26	26		down	up	free	0 bit/s	420 days ago
27	27		down	up	free	0 bit/s	420 days ago
28	28		down	up	free	0 bit/s	420 days ago

Figura 35: detalle de ocupación de un switch

Como se muestra en la imagen, según el sistema de monitorización, el dispositivo cuenta con 6 interfaces libres. Sin embargo, durante la revisión se observa que realmente solo hay dos interfaces libres: la 14 y la 20.

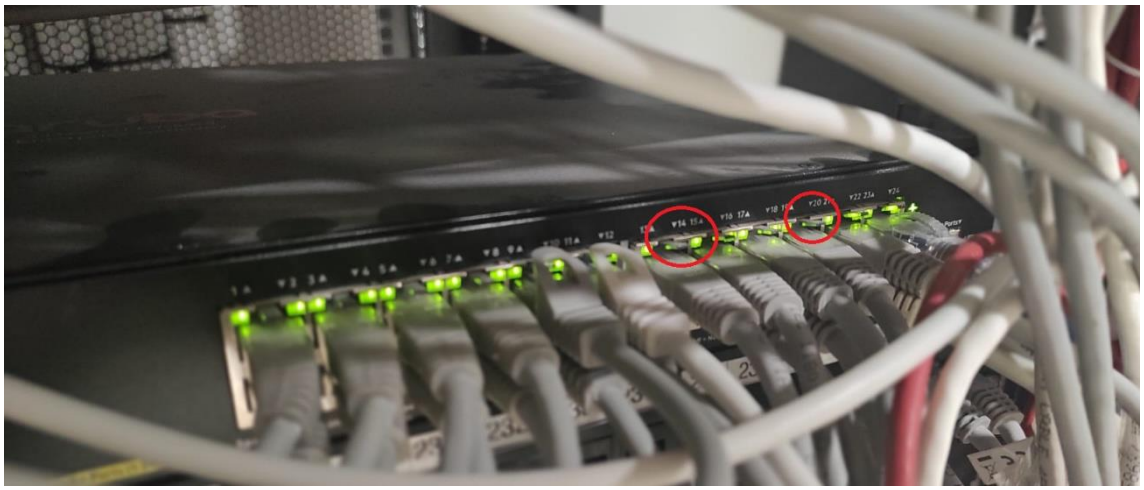


Figura 36: interfaces del dispositivo

Esta discrepancia se debe a que el sistema considera que el switch tiene 28 puertos usables, cuando realmente solo 24 de ellos están disponibles para conectar equipamiento, siendo el resto de uso administrativo, por lo que habrá que tener en cuenta esto a la hora de planificar el dimensionamiento de la infraestructura.

5.3 Detección de los intentos de intrusión en tiempo real y almacenado de histórico

Otro de los puntos clave del sistema de monitorización, es evaluar la capacidad de detectar shadow IT, concretamente la conexión de un dispositivo no autorizado a la red del centro. Se han seleccionado una interface libre de un switch y se ha configurado la seguridad siguiendo la política del centro: la interfaz admitirá la conexión de un solo dispositivo, de manera que, al conectar un segundo dispositivo, debe deshabilitarse y se debe generar un registro en el visor de eventos del sistema de monitorización.

```
SWITALLER(config)# port-security 1/6 learn-mode static address-limit 1 action send-disable
SWITALLER(config)# show running-config interface 1/6

Running configuration:

interface 1/6
   tagged vlan 21
   untagged vlan 2
   port-security learn-mode static action send-disable mac-address 387c76-4ad792
   exit
```

Figura 37: configuración port-security

Tras conectar el primer dispositivo, se observa que funciona correctamente y tiene conectividad

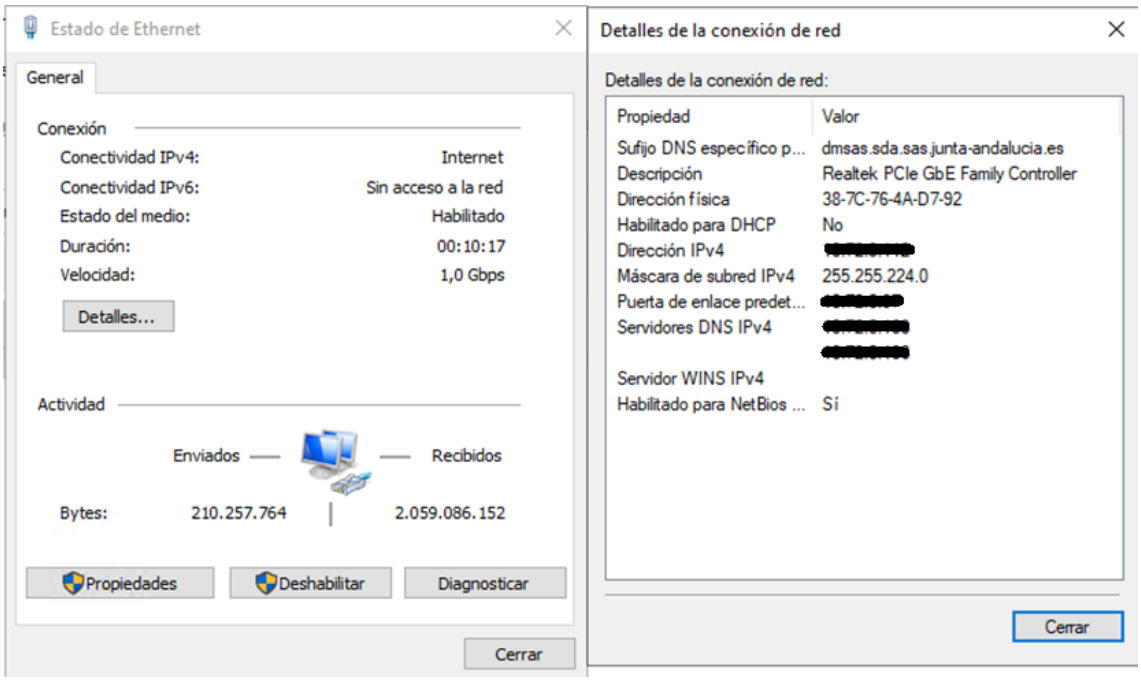


Figura 38: configuración de red del equipo

Se conecta un segundo dispositivo y se comprueba que no conecta, se puede ver en el log del switch que el puerto ha sido desactivado.

```
SWITALLER(config)# show port-security intrusion-log

 Status and Counters - Intrusion Log

  Port    MAC Address    Date / Time
  ------ ------------- ---------------------------
  1/6     001ae8-59a0b8 12/07/23 11:50:25
```

Figura 39: log en switch tras violación port-security

Se verifica que se ha generado una nueva entrada en el visor de eventos del sistema de monitorización, donde se puede apreciar que coincide el switch, puerto y la MAC que ha provocado el bloqueo

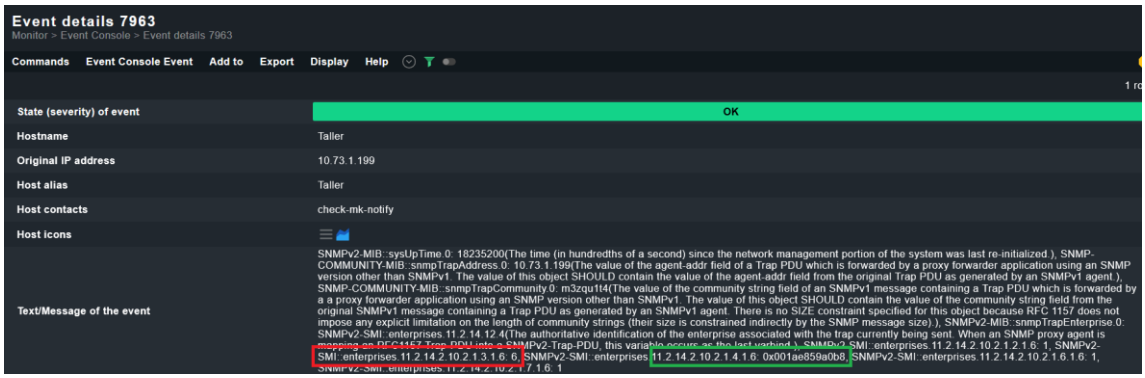


Figura 40: detalles del evento generado en checkmk

Se repite la misma prueba en otro switch y se comprueba que el registro se ha añadido al visor de eventos, con esto se verifica que el dashboard para visualizar los intentos de intrusión funciona correctamente

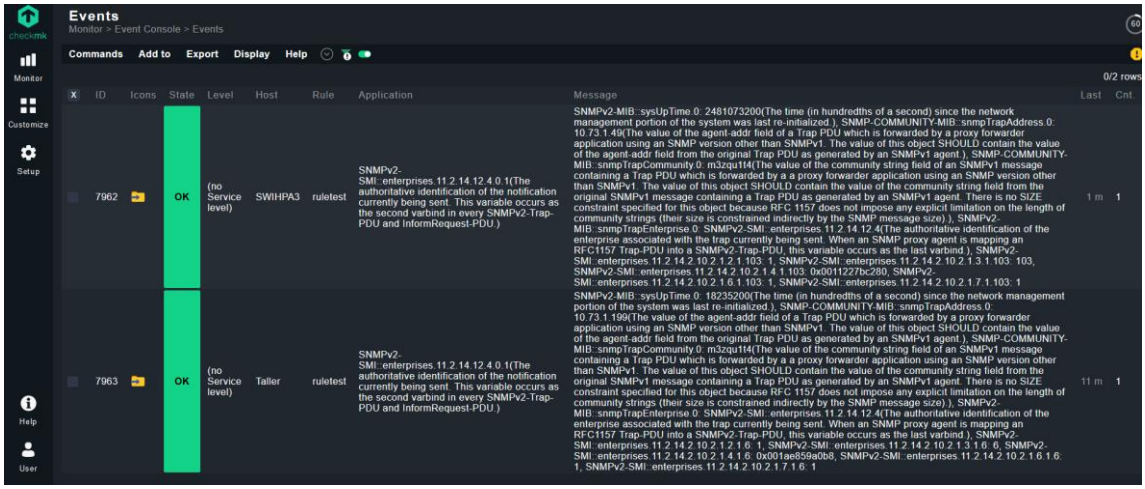


Figura 41: eventos generados por intentos de intrusión

5.4 Inventariado de todos los switches

Se accede al sistema de monitorización y se entra en el detalle de un dispositivo, concretamente el SWICEA2, comprobando que muestra información como el fabricante, modelo y número de serie de los miembros del stack.

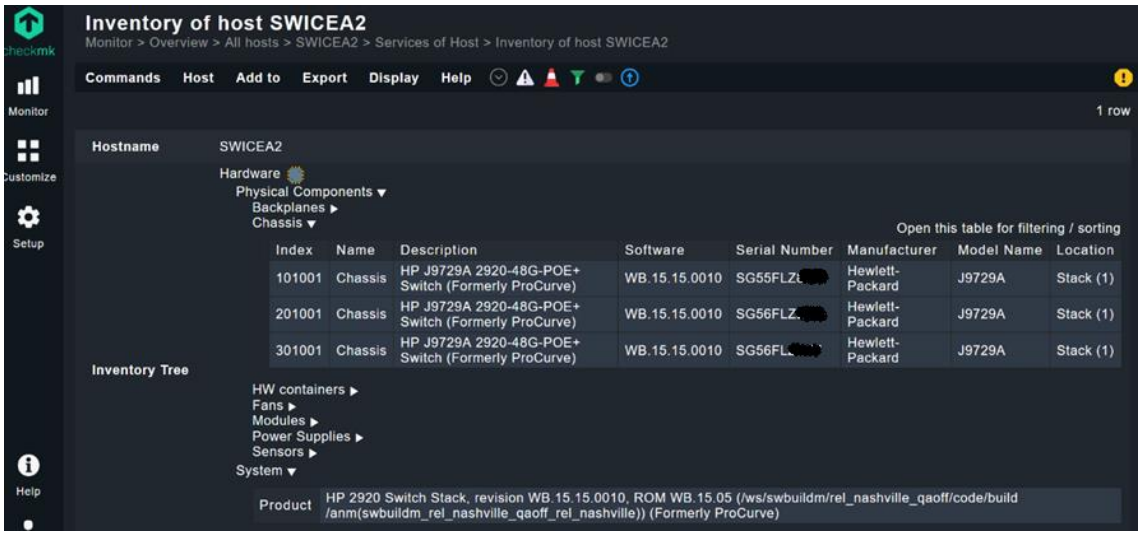


Figura 42: inventario facilitado por CheckMK

Se comprueba la información en el listado de switches anexo y se verifica que la información mostrada es correcta. Se trata de un stack de tres miembros, formado por switches HP J972A, cuyos números de serie corresponden con los proporcionados por el sistema de monitorización.

NOMBRE	S/N	FABRICANTE	MODELO
SWICEA1			
SWICEA2	SG55FLZ[redacted]	HP	J9729A
SWICEA2	SG56FLZ[redacted]	HP	J9729A
SWICEA2	SG56FLZ[redacted]	HP	J9729A
SWICEB1	SG55FLZ[redacted]	HP	J9729A

Figura 43: extracto de inventario realizado presencialmente

5.5 Minimizar consumo de recursos mínimo

El resultado de las pruebas de rendimiento del sistema ha sido altamente satisfactorio, evidenciando un desempeño excepcional del sistema de monitorización implementado. Una vez dados de alta todos los host y configurado el envío de traps hacia el servidor en todos los switches de la infraestructura de red, el sistema demostró una notable capacidad para gestionar un volumen considerable de datos de monitoreo sin comprometer su rendimiento general.

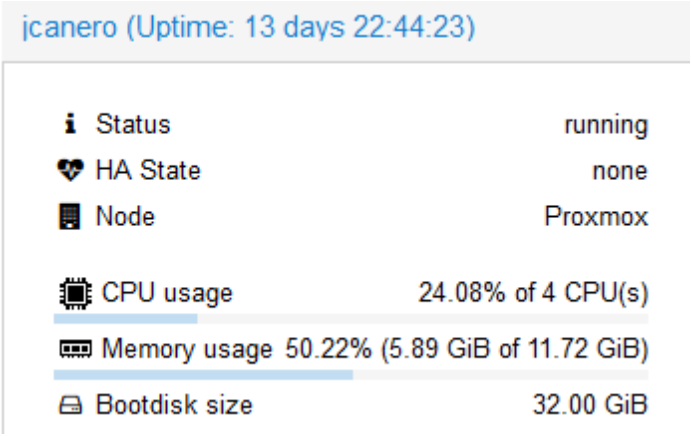


Figura 44: estado del servidor

En la imagen anterior se muestra el estado del servidor en producción, se puede observar que el uso de la CPU está a un cuarto de la capacidad y el uso de la memoria RAM apenas supera el 50% de los recursos asignados dentro del entorno de virtualización.

Si se consulta un histórico sobre el uso de CPU y memoria RAM del equipo, se puede comprobar que los valores se mantienen estables a los mostrados anteriormente.

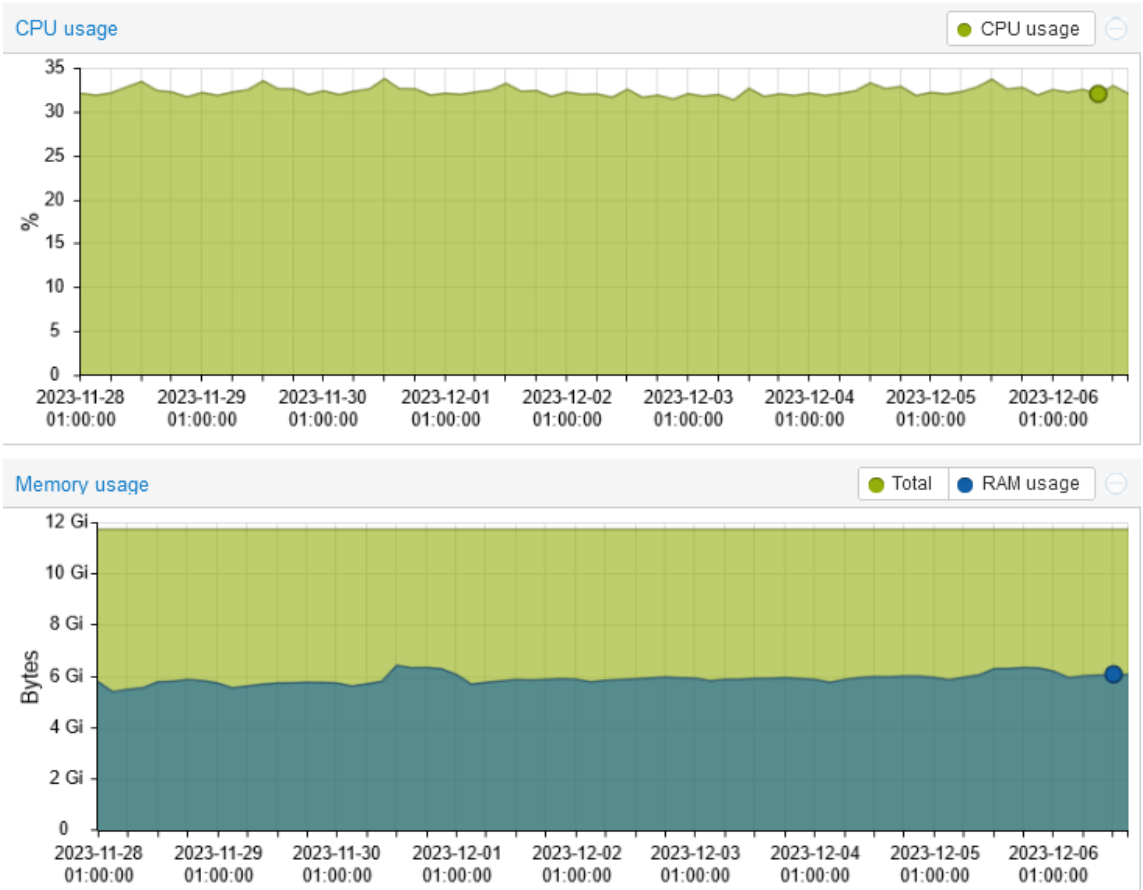


Figura 45: uso histórico de cpu y ram del servidor

Este rendimiento consistente y fiable valida la capacidad del sistema para mantener su eficiencia operativa en condiciones de alto estrés, lo que confirma su idoneidad para las demandas de monitoreo continuo en un entorno hospitalario crítico.

5.6 Facilidad de implementación

Durante el desarrollo del proyecto, el sistema de monitorización ha quedado implementado, con los switches reales de la infraestructura dados de alta y con las configuraciones de notificaciones y alertas correctamente definidas.

Con esto se verifica que la implementación del sistema de monitorización ha tenido una dificultad acorde a las circunstancias y ha sido posible realizarla en los 29 días laborables establecidos para esta fase. No se han producido intentos fallidos de configuración relevantes.

5.7 Facilidad de operación

El análisis de usabilidad y experiencia del usuario reveló resultados positivos tras las pruebas realizadas. El equipo de soporte TIC se involucró en la evaluación y manifestó un alto grado de satisfacción con la interfaz y funcionalidades del sistema de monitorización. Durante las pruebas, se destacó la facilidad de navegación y la claridad de la información presentada en la interfaz, lo que simplificó considerablemente la gestión y supervisión de la red.

La retroalimentación obtenida fue muy favorable, resaltando la intuición en la utilización de las herramientas y la accesibilidad de las funciones clave del sistema. Los usuarios destacaron especialmente la disposición lógica de los datos y la capacidad para acceder a información relevante de manera rápida y efectiva.

Figura 46: dashboard host configurados

Estos resultados indican que el sistema no solo cumple con sus objetivos técnicos, sino que también proporciona una experiencia de usuario satisfactoria y amigable. El entusiasmo expresado por el equipo de soporte TIC confirma la idoneidad del sistema para ser adoptado en el entorno hospitalario, facilitando su uso efectivo y contribuyendo a una gestión más eficiente de la red.

5.8 Escalabilidad y dispositivos soportados

El resultado de las pruebas de escalabilidad confirma la capacidad del sistema para adaptarse y expandirse eficientemente según las demandas cambiantes del entorno hospitalario. La base del sistema en Checkmk permitió demostrar su versatilidad al ofrecer la posibilidad de monitorizar una amplia variedad de dispositivos más allá de los switches, abriendo la puerta a una expansión integral de la supervisión dentro de la infraestructura hospitalaria en futuros desarrollos.

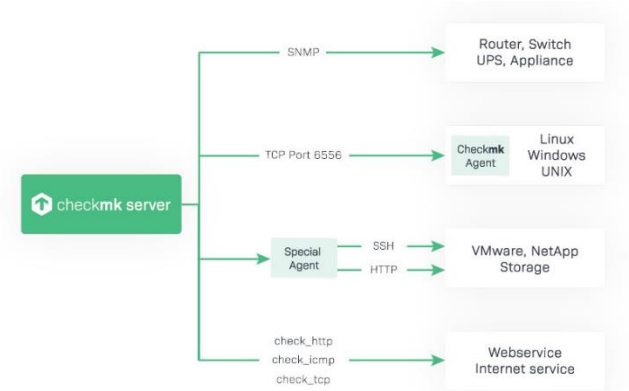


Figura 47: capacidad de monitorización de CheckMK

Además, al estar instalado sobre una máquina virtual, se evidenció la flexibilidad inherente del sistema para escalar recursos fácilmente en caso de requerimientos adicionales. Esta arquitectura adaptable garantiza la capacidad de asignar recursos adicionales según sea necesario (aumento de RAM, asignación de CPU, etc.), asegurando que el sistema mantenga su eficacia operativa incluso frente a un crecimiento significativo en la red o a un aumento en la carga de trabajo.

La capacidad comprobada del sistema para ampliar su alcance más allá de los switches y la flexibilidad para ajustar los recursos de manera dinámica constituyen evidencia sólida de su escalabilidad. Esto confirma su idoneidad para adaptarse a futuras expansiones o cambios en la infraestructura hospitalaria, garantizando que el sistema de monitorización continúe siendo una solución efectiva y adaptable a medida que evolucionen las necesidades del entorno, permitiendo por ejemplo la incorporación al sistema de monitorización de dispositivo hardware como servidores o aplicaciones como bases de datos.

5.9 Software libre

Se comprueba que todo el software sobre el que está basado el sistema de monitorización, asi como las herramientas utilizadas durante su desarrollo no requieren de licencia comercial para su uso:

- Proxmox (https://www.proxmox.com/en/): sistema de virtualización sobre el que se ha desplegado el servidor.

- Debian (https://www.debian.org): sistema operativo base instalado en el servidor

- Draw.io (https://www.drawio.com/): software utilizado para dibujar diagramas.

- Wireshark (https://www.wireshark.org/): herramienta utilizada para capturar y analizar tráfico de la red

- CheckMK (https://checkmk.com/): software base de monitorización instalado en el servidor

6. Conclusiones

6.1 Conclusiones del trabajo

El objetivo general de este trabajo de fin de grado era mejorar la gestión de la red en un entorno hospitalario, enfocándose en la disponibilidad y seguridad de los sistemas críticos. Para ello, se propuso la implementación de un sistema de monitorización de la infraestructura de red.

Los resultados de las pruebas realizadas son muy satisfactorios y confirman que el sistema de monitorización implementado cumple con todos los requisitos del proyecto.

En particular, el sistema ha demostrado una capacidad excepcional para:

- Detectar de forma proactiva las incidencias de red, incluyendo la caída de dispositivos, intentos de intrusión y problemas de conectividad.

- Proporcionar información en tiempo real sobre la disponibilidad de interfaces libres en los switches, lo que facilita la planificación del dimensionamiento de la infraestructura.

- Detectar la conexión de dispositivos no autorizados a la red, lo que ayuda a proteger la seguridad de la infraestructura.

- Generar inventario de los dispositivos que forman parte de la infraestructura, lo que proporciona una visión completa de la misma.

- Gestionar un volumen considerable de datos de monitoreo sin comprometer su rendimiento general.

- Adaptarse y expandirse eficientemente según las demandas cambiantes del entorno hospitalario.

- Proporcionar una experiencia de usuario satisfactoria y amigable.

En general, el sistema de monitorización implementado es una herramienta eficaz que ayudará a mejorar la gestión de la red del centro hospitalario. Los resultados obtenidos son en general los esperados, ya que se basaban en los requisitos funcionales y operativos del sistema de monitorización.

Sin embargo, hay algunos resultados que han sido sorprendentes. El sistema ha demostrado una buena capacidad de escalabilidad, concretamente ha sido capaz de monitorizar sin problemas una infraestructura de red con más de 100 switches. Esto es un resultado importante, ya que el centro hospitalario tiene previsto ampliar su infraestructura en el futuro.

6.2 Consecución de los objetivos

La implementación del sistema de monitorización de la infraestructura de red en un entorno hospitalario ha resultado exitosa en la consecución de los objetivos planteados:

- La exploración detallada de los componentes críticos de la red hospitalaria permitió identificar los dispositivos y switches esenciales que requerían monitorización constante para garantizar su disponibilidad y seguridad.

- La elección del software de monitorización, con un enfoque en el protocolo SNMP, demostró ser acertada, permitiendo una supervisión efectiva de los dispositivos.

- La implementación exitosa de un sistema de alertas ágil y eficiente ha fortalecido la capacidad del equipo de soporte TIC para responder proactivamente a las incidencias, asegurando la continuidad operativa de los sistemas críticos.

- La investigación detallada sobre la detección de dispositivos no autorizados a través de los traps SNMP proporcionó información valiosa sobre la respuesta de los switches ante intentos de intrusión, fortaleciendo así las medidas de seguridad de la red hospitalaria.

Los resultados obtenidos durante los test reflejan el cumplimiento de los objetivos técnicos establecidos inicialmente:

- Se logró la detección automática de incidencias de red, siendo capaz el sistema de generar una notificación y registrar la intendencia en el sistema de tickets.

- La visualización en tiempo real de la capacidad de puertos disponibles, si bien hay que tener en cuenta que no es del todo exacto, cumple la utilidad de ayudar a la planificación del dimensionamiento de la infraestructura.

- La adaptación de la consola de eventos nos ha permitido tener un registro de todos los intentos de intrusión que ocurren en el centro de manera centralizada.

- Se ha generado un inventario de dispositivos manual, que con la herramienta se puedo completar y mantener siempre actualizado.

Los resultados obtenidos a lo largo de la implementación del sistema de monitorización reflejaron una correspondencia directa con las expectativas y metas establecidas al inicio del proyecto.

6.3 Seguimiento de la planificación y metodología

La planificación se ha seguido de forma satisfactoria, ya que los plazos se fijaron de forma realista. El alcance completo de los objetivos establecidos en la etapa inicial del proyecto se ha logrado de manera exitosa y completa. Además, cada uno de los hitos propuestos se cumplió dentro de los parámetros previstos en tiempo y forma.

La elección de la metodología en cascada se mostró como la opción idónea para este proyecto, donde mi participación como único recurso era el principal hándicap. Esta metodología, con su enfoque secuencial y estructurado, facilitó una planificación detallada y su naturaleza progresiva me permitió comprender y abordar cada fase de forma individual, lo que resultó crucial dada la complejidad del entorno hospitalario.

Por otro lado, se ha mantenido comunicación continua con el consultor de la Universidad para revisar el progreso y abordar cualquier problema que pueda surgir. Además, se ha contado con el apoyo del departamento de informática del centro para revisar la solución propuesta y adaptarla a sus necesidades.

El conocimiento del entorno del centro hospitalario ha sido fundamental para el éxito del trabajo, ya que ha permitido hacer una estimación muy realista de los plazos que se requerían para ejecutar cada tarea, asi como conocer de primera mano las necesidades de la organización, lo que ha sido fundamental para definir los requisitos del sistema de monitorización.

No ha sido necesario realizar grandes cambios en la planificación, más allá de modificar la fecha de realización de alguna de las tareas, como el inventariado inicial, que requerían de mi presencia física en el complejo hospitalario, para hacerlas coincidir con mis visitas al centro por motivos laborales.

En base a la experiencia obtenida en este trabajo, se recomienda utilizar la metodología en cascada para proyectos de pequeño tamaño, en los que el equipo de trabajo es reducido y existe un conocimiento profundo del entorno.

6.4 Impactos ético-sociales, de sostenibilidad y de diversidad

En relación a los impactos ético-sociales, de sostenibilidad y de diversidad previstos, se han logrado mitigar algunos impactos negativos y se han potenciado los positivos, aunque no se han presentado impactos no previstos en las dimensiones ético-sociales, de sostenibilidad y diversidad.

Aunque la implementación del sistema de monitorización aumenta el consumo energético del hospital, se ha mitigado este impacto al utilizar de un servidor virtual ya existente. Además, todos informes se manejan digitalmente, siguiendo la política de no papel, lo que ha contribuido de manera positiva en este aspecto.

En el aspecto ético-social se ha logrado un impacto positivo al garantizar la protección de datos de los pacientes, cumpliendo rigurosamente con la legislación pertinente y fortaleciendo la seguridad y privacidad de la información, alineándose con el ODS 16.

Por otro lado, al tratarse de un proyecto de naturaleza técnica, no aborda directamente cuestiones relacionadas con la diversidad. Como se preveía, su implementación no ha generado impactos negativos en esta dimensión.

6.5 Líneas de trabajo futuras

En general, los resultados obtenidos son muy satisfactorios y confirman que el sistema de monitorización implementado es una herramienta eficaz que ayudará a mejorar la gestión de la red del centro hospitalario. Sin embargo, existen algunos aspectos que podrían mejorarse para que el sistema sea aún más completo y eficaz mediante líneas de trabajo futuro, que deberían abarcan dos áreas clave: mejorar la consola de eventos y ampliar el alcance de la monitorización

El enriquecimiento de la consola de eventos es esencial para una detección más precisa de intentos de intrusión. La creación de un diccionario MIB personalizado permitiría interpretar y presentar los datos de manera más contextualizada y comprensible. Con esta mejora, se podría identificar con mayor claridad la naturaleza y el origen de los intentos de intrusión, diferenciando entre distintos tipos de ataques o comportamientos sospechosos. Además, proporcionaría detalles adicionales sobre los eventos registrados, facilitando la adopción de medidas más específicas y rápidas para mitigar cualquier amenaza potencial.

La ampliación del alcance de la monitorización a otros dispositivos sería otra línea de trabajo muy a tener en cuenta, esto implica la incorporación de servidores físicos, entornos de virtualización, bases de datos y PCs críticos dentro del alcance de la monitorización. Al integrar estos dispositivos, se fortalecerá la capacidad de supervisión y detección de posibles problemas, permitiendo una gestión más integral y proactiva ya no solo de la red, sino de toda la infraestructura informática del complejo.

Estas líneas de trabajo futuro representan áreas esenciales para la evolución y mejora continua del sistema de monitorización, ampliando su funcionalidad y alcance para abarcar un espectro más amplio de dispositivos críticos en la infraestructura hospitalaria, así como para perfeccionar la capacidad del sistema ya implementado durante la ejecución de este proyecto.

7. Glosario

Bot: programa diseñado para simular la interacción humana en internet.

Community: clave de acceso, usada en SNMP, que permite autenticar y controlar la gestión de información.

CPU: unidad central de procesamiento que ejecuta instrucciones en una computadora.

CPD: centro de procesamiento de datos, lugar físico donde se concentran los recursos informáticos de una organización.

Debian: sistema operativo basado en Linux, conocido por su estabilidad y robustez.

Diagrama de Gantt: representación gráfica de la planificación y programación de actividades en un proyecto.

DNS: sistema de nombres de dominio que traduce los nombres de dominio a direcciones IP.

Dashboard: panel de control que muestra datos e indicadores clave de manera visual.

Hardware: componentes físicos de una computadora o dispositivo.

Host: dispositivo conectado a una red que puede recibir o enviar información.

Interfaz: punto de interacción entre dos componentes o sistemas.

IP: protocolo de internet, que identifica y localiza dispositivos en una red.

ISO: organización internacional de normalización, que establece estándares para varios campos.

MIB: base de información de gestión, que contiene parámetros y datos de dispositivos de red.

MAC: dirección de control de acceso de medios, identificador único de dispositivos de red.

NAC: control de acceso a la red, conjunto de tecnologías para gestionar el acceso a una red.

NMS: sistema de gestión de redes, utilizado para supervisar y gestionar dispositivos de red.
OID: identificador de objeto, cadena numérica que identifica un objeto en la jerarquía del MIB.

PECs: prueba de evaluación continua.

Proxy: servidor que actúa como intermediario entre los usuarios e internet.

Repositorio: almacenamiento centralizado de datos o software.

RAM: memoria de acceso aleatorio, donde se almacena temporalmente la información en una computadora.

Racks: estructuras para montar y organizar dispositivos informáticos.

Roseta: conector que permite la conexión de cables de red a una toma.

Shadow IT: uso no autorizado de hardware, software o servicios de TI en una organización.

SNMP: protocolo simple de gestión de red, utilizado para supervisar y gestionar dispositivos.

Stack: tecnología que conecta varios switches entre sí.

Switches: dispositivos de red que conectan diferentes segmentos de red para facilitar la comunicación.

TIC: tecnologías de la información y comunicación, conjunto de tecnologías para el manejo de información y comunicación.

Traps: mensajes de notificación enviados por dispositivos de red para alertar sobre eventos.

UDP: protocolo de datagramas de usuario, que permite la transmisión de datos sin establecer una conexión previa.

Waterfall: modelo de desarrollo de software secuencial y lineal, con fases bien definidas.

Wireshark: herramienta de análisis de redes utilizada para capturar y analizar paquetes de datos.

8. Bibliografía

1. SARDIÑA, Rafa. ¿Por qué los hospitales son el nuevo objetivo de los ciberdelincuentes? ¿Cómo afecta a los pacientes? En: *La Nueva España* [en línea]. 1 de octubre de 2022. [consulta: 4 de octubre de 2023. Disponible en: https://www.lne.es/salud/guia/2022/10/01/hospitales-son-nuevo-objetivo-ciberdelincuentes-76381568.html

2. *¿Qué es el monitoreo de red?* [en línea] [consulta: 3 de octubre de 2023]. Disponible en: https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

3. UOC, *Guía transversal sobre la CCEG para estudiantado de TFx-EIMT* [en línea]. Barcelona: UOC, 2022. [consulta: 5 de octubre de 2023]. Disponible en: https://aula.uoc.edu/courses/7771/files/664707?wrap=1

4. *Paz y justicia – Desarrollo sostenible* [en línea] [consulta: 5 de octubre de 2023]. Disponible en: https://www.un.org/sustainabledevelopment/es/peace-justice/

5. *¿Cuál es la metodología más adecuada para tu proyecto?* [en línea] [consulta: 7 de octubre de 2023]. Disponible en: https://www2.deloitte.com/es/es/pages/technology/articles/waterfall-vs-agile.html

6. *Shadow IT al descubierto: riesgos y buenas prácticas*. [en línea] [consulta: 19 de noviembre de 2023]. Disponible en: https://www.incibe.es/incibe-cert/blog/it-shadow-al-descubierto-riesgos-y-buenas-practicas

7. MC GUIRE, Cristian. Configurando Port-Security en los Switch para mejorar la seguridad [en línea]. *Backtrack Academy.* 27 de octubre de 2017. [consulta: 13 octubre 2023]. Disponible en: https://backtrackacademy.com/articulo/configurando-port-security-en-los-switch-para-mejorar-la-seguridad

8. *Infrastructure and Application monitoring with Checkmk* [en línea] [consulta: 16 de octubre de 2023]. Disponible en: https://checkmk.com/

9. *Protocolo simple de administración de red* [en línea] [consulta: 29 de octubre de 2023]. Disponible en: https://es.wikipedia.org/wiki/Protocolo_simple_de_administraci%C3%B3n_de_red

10. *Debian – El sistema operativo universal* [en línea] [consulta: 24 de octubre de 2023]. Disponible en: https://www.debian.org/index.es.html

11. *Configuring SNMP.* [en línea] [consulta: 29 de octubre de 2023]. Disponible en: https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/15-18/5998-8160_ssw_mcg/content/ch06s10.html

12. *Configuring SNMP.* [en línea] [consulta: 29 de octubre de 2023]. Disponible en: https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/Management_Utilities/Configuring_SNMP.htm

13. *Configurar trampas SNMP de IOS admitidas.* [en línea] [consulta: 29 de octubre de 2023]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/ip/simple-network-management-protocol-snmp/13506-snmp-traps.html

14. *Configuring the SNMP Trap Function.* [en línea] [consulta: 29 de octubre de 2023]. Disponible en: https://support.huawei.com/enterprise/es/doc/EDOC1000057410?section=j04l&topicName=configuring-the-snmp-trap-function

15. *How to Capture, Parse and Troubleshoot SNMP traps using Wireshark.* [consulta: 29 de octubre de 2023]. Disponible en: https://campus.barracuda.com/product/managedworkplace/doc/98217208/how-to-capture-parse-and-troubleshoot-snmp-traps-using-wireshark/