Pontificia Universidad Católica del Ecuador

Sede Ibarra

ESCUELA DE INGENIERÍA

INFORME FINAL DEL PROYECTO

TEMA:

"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y MODELO DE GESTIÓN DE LA RED DE DATOS DE LA PUCE – SI BASADO EN HERRAMIENTAS OPEN SOURCE"

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERA EN SISTEMAS

LÍNEAS DE INVESTIGACIÓN:

DOMÓTICA Y COMUNICACIONES

AUTORA: MARÍA FERNANDA PINTO CAÑIZARES

ASESOR: Mgs. DARWIN PILLO

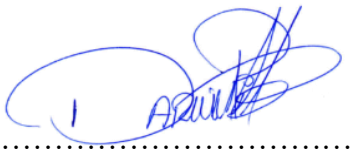
IBARRA, JUNIO de 2021

Ibarra, 15 de junio de 2021

Mgs.
Darwin Marcelo Pillo Guanoluisa
ASESOR

CERTIFICA:

Haber revisado el presente informe final de investigación, el mismo que se ajusta a las normas vigentes en la Escuela de Ingeniería de Sistemas, de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI); en consecuencia, autorizo su presentación para los fines legales pertinentes.



(f.)……
Mgs. Darwin Marcelo Pillo Guanoluisa
C.C.: 1003319660

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El jurado examinador, aprueba el presente informe de investigación en nombre de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI):

(f): ……

Mgs. Darwin Marcelo Pillo Guanoluisa

C.C.: 1003319660

(f): ……

Mgs. Luis David Narváez Erazo

C.C.: 1002868378

(f): ……..

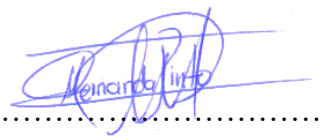
Mgs. Juan Carlos Armas Cárdenas

C.C.: 1001685732

ACTA DE CESIÓN DE DERECHOS

Yo, Pinto Cañizares María Fernanda, declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: “Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones, a título gratuito u oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia”.

Ibarra, 15 de junio de 2021



f): …….

María Fernanda Pinto Cañizares

C.C.: 1004660849

AUTORÍA

Yo Pinto Cañizares María Fernanda, portador de la cédula de ciudadanía N°1004660849, declaro que la presente investigación es de total responsabilidad del autor, y eximo expresamente a la Pontificia Universidad Católica del Ecuador Sede Ibarra de posibles reclamos o acciones legales.

f): ……

María Fernanda Pinto Cañizares

C.C. 1004660849

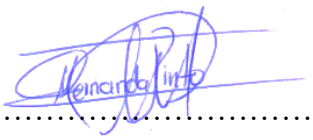
DECLARACIÓN Y AUTORIZACIÓN

Yo Pinto Cañizares María Fernanda con CC: 1004660849, autora del trabajo de grado intitulado: IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y MODELO DE GESTIÓN DE LA RED DE DATOS DE LA PUCE-SI BASADA EN HERRAMIENTAS OPEN SOURCE, previo a la obtención del título profesional de INGENIERA EN SISTEMAS, en la Escuela de Ingeniería.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador Sede- Ibarra, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador Sede Ibarra a difundir a través de sitio web de la Biblioteca de la PUCESI el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ibarra, 15 de junio de 2021



(f.)……

María Fernanda Pinto Cañizares

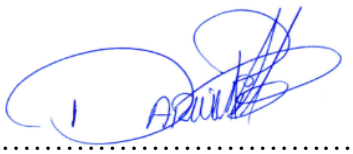
C.C. 1004660849

CERTIFICACIÓN ANTIPLAGIO

Yo Mgs. Darwin Marcelo Pillo Guanoluisa, declaro que luego del proceso de revisión en el sistema anti plagio TURNITIN el porcentaje de similitud del trabajo de titulación denominado: "Implementación de un sistema de monitoreo y modelo de gestión de la red de datos de la PUCE – SI basado en herramientas open source", es del 5%, de acuerdo al documento 1606448501.

En base a lo anterior, considero que el trabajo de titulación NO [ ] SÍ [X] cumple los requisitos de originalidad y autenticidad, de acuerdo con los requisitos establecidos por la ley.

Ibarra, 15 de junio de 2021



(f.)……

Mgs. Darwin Marcelo Pillo Guanoluisa

C.C.: 1003319660

DEDICATORIA

Dedicado con mucho amor para mi querida madre Yolanda Cañizares por ser mi ejemplo a seguir, este trabajo y todo lo que he logrado ha sido gracias a su fortaleza, virtudes y valores inculcados en mí.

Con mucho cariño a mi hermana Jahaira Fernanda, logro que se lo dedico como como impulso para que alcance sus propias metas.

A mi amada hija Rafaela Valentina quien con su existencia ha sido mi motivo y motor para seguir adelante ante cualquier adversidad.

AGRADECIMIENTO

A mis padres Juan Fernando Pinto y Yolanda Cañizares, mis tíos Fernando y Martha Cañizares, mis abuelos Amilcar Cañizares y Teresa Monteros quienes han estado presentes en cada etapa de mi vida brindándome su confianza, amor y apoyo incondicional.

A la Pontificia Universidad Católica del Ecuador Sede Ibarra, a la escuela de Ingeniería de manera particular a mi asesor Mgs. Darwin Pillo por su supervisión durante la realización de este proyecto.

Al personal administrativo de la Unidad de Sistemas de la PUCE-SI en especial al Mgs. Franklin Sánchez por haberme permitido llevar a cabo con éxito este proyecto.

Finalmente, quiero expresar mi más grande y sincero agradecimiento al Mgs. Paúl Enríquez, principal colaborador durante todo este proceso, quien supo brindarme su apoyo, confianza y tiempo. Gracias a su dirección, conocimiento y enseñanza que permitió el desarrollo de este trabajo.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La Pontificia Universidad Católica del Ecuador (PUCE-SI) es una institución de educación superior que contribuye a la formación de profesionales en el norte del país, la cual cuenta con una infraestructura tecnológica amplia. Es de gran importancia que los servicios de TI que brinda dicha institución se encuentren disponibles las 24 horas durante los 7 días de la semana.

En este proyecto se plantea la implementación de un sistema de monitoreo y modelo de gestión de red para la red de datos local basado en herramientas open source, con la finalidad de administrar los dispositivos que conforman la red, así el administrador de la red puede solventar cualquier fallo ocurrido de forma oportuna.

En cuanto a la investigación dentro sus etapas se encuentra en primer momento la investigación documental, en la cual se reúne información de diferentes fuentes bibliográficas, las mismas que sustentan la puesta en marcha del proyecto que ocurre dentro de la investigación aplicada, ya que ésta se enfoca a la aplicación del conocimiento obtenido para la implementación tanto del modelo de gestión como del software de monitoreo y herramientas complementarias.

El modelo de gestión a implementar para la red de datos de la PUCE -SI se denomina FCAPS o modelo funcional, el cual está basado en el estándar ISO y ha sido elegido después de un análisis registrado dentro de este documento, de la misma forma que el software de monitoreo Nagios, el cual cuenta con el análisis de requerimientos descrito a través del estándar IEEE 830.

El presente trabajo delimitará su alcance al desarrollo de las fases más relevantes para cubrir las necesidades institucionales y requerimientos técnicos de la Unidad de Sistemas de la PUCE -SI bajo sus normas y políticas. Estas fases son: Gestión de la configuración, fallos y contabilidad. El modelo implementado fue sometido a pruebas llevadas junto a personal técnico del área de redes, obteniendo resultados satisfactorios y cubriendo las necesidades por las cuales se implementó.

Finalmente, se establece una guía de procedimientos para facilitar el cumplimiento del modelo de gestión implementado, así como también la configuración de nuevos dispositivos dentro de la herramienta de monitoreo.

PALABRAS CLAVE

Modelo de gestión de red, FCAPS, Monitoreo de redes, Nagios, PNP4Nagios, NSClient++, NRPE, SNMP.

ABSTRACT

Pontificia Universidad Católica del Ecuador (PUCE-SI) is a higher education institution that contributes to the training of professionals in the north of the country, which has a wide technology infrastructure. It is of great importance that the IT services provided by this institution are available 24 hours a day, 7 days a week.

This project proposes the implementation of a monitoring system and network management model for the local data network, based on open source tools in order to manage the devices that make up the network, so the network administrator can solve any fault occurred in a timely manner.

Within the stages of the investigation, the documentary research is found at first, in which information from different bibliographic sources is gathered, which supports the implementation of the project that occurs within the applied research, since it focuses on the application of the knowledge gained for the implementation of the management model as well as the monitoring software and complementary tools.

The management model to be implemented for the PUCE-SI data network is called FCAPS or functional model. It is based on the ISO standard and has been chosen after an analysis recorded in this document, like the Nagios monitoring software, which has the requirements analysis described through the IEEE 830 standard.

This work will develop the most relevant phases to cover the institutional needs and technical requirements of Unidad de Sistemas of PUCE-SI under its rules and policies. These phases are: Configuration, Fault and Accounting management.

The implemented model was tested together with the technical staff from the IT department. Satisfactory results were obtained and the needs, which is why it was implemented, were met.

Finally, a procedure guide was established to facilitate compliance with the implemented management model, as well as the configuration of new devices in the monitoring tool.

KEYWORDS

Network management model, FCAPS, Network monitoring, Nagios, PNP4Nagios, NSClient++, NRPE, SNMP.

INTRODUCCIÓN

La gestión de seguridad de la información se fundamenta en tres principios básicos: disponibilidad, integridad y confidencialidad. Integridad se refiere a que la información debe mantenerse inalterada previniendo modificaciones no autorizadas, el principio de confidencialidad hace referencia a que el acceso a la información debe ser mediante autorización y de forma controlada.

La disponibilidad se refiere a la capacidad de garantizar el acceso a servicios y datos mediante la integración de mecanismos o estrategias necesarios. Precisamente este trabajo pretende mejorar este último pilar de la seguridad que es la disponibilidad de los servicios de TI de la PUCE-SI. La evolución constante provoca que los centros de datos estén en una incesante operatividad para lograr cumplir con los requisitos de un funcionamiento eficiente y sin interrupciones para los usuarios.

El elemento básico a garantizar es la continuidad operativa para que los servicios de TI sean accesibles en todo momento. Bajo este principio la Pontificia Universidad Católica del Ecuador Sede Ibarra cuenta con un Data Center el cual conserva y resguarda datos e información de los estudiantes, del personal docente y administrativo de la sede, por lo que la conservación adecuada del centro de datos es primordial.

Mejorar la disponibilidad del Centro de Datos se logra a través de un monitoreo permanente del estado de los dispositivos, por lo que es necesaria la implementación de un sistema de alerta inmediata en caso de presentar alguna incidencia con los dispositivos y esto pueda ocasionar la suspensión de cualquier servicio crítico para la PUCESI.

Esta propuesta está enfocada en la implementación de la herramienta de monitoreo permanente de los dispositivos de red dentro del Data Center de la Pontificia Universidad Católica del Ecuador Sede Ibarra las 24 horas del día durante los 7 días de la semana, así permitir que el administrador de la red tenga conocimiento de manera oportuna de los incidentes que se presenten.

Es de suma importancia conocer el estado de los recursos que conforman la red con el objetivo de preservar los servicios que brindan a los usuarios. El personal autorizado será notificado de forma oportuna vía correo electrónico para que de esta forma se pueda actuar y tomar las medidas necesarias corrigiendo los problemas que se detecten de manera eficaz.

Como complemento esencial del monitoreo de los recursos de red es indispensable la implementación de un modelo de gestión de red que ayudará a prestar un mejor servicio, garantizar la disponibilidad y hacer que la administración de la red sea más eficiente y ordenada. La gestión de red tiene como finalidad proveer organización y supervisión para evaluar los recursos de red garantizando un nivel óptimo de servicio a los usuarios.

Monitorear la infraestructura de TI ha sido una tarea difícil. Hay algunas soluciones comerciales comunes; sin embargo, este tipo de soluciones tienen un costo elevado y no siempre se ajustan a las necesidades institucionales, por lo que es primordial el uso de herramientas de código abierto que permiten libre uso y distribución.

Los objetivos específicos para este trabajo de titulación son:

- Recopilar información que fundamente las técnicas y herramientas que serán utilizadas para la investigación, creación del modelo y desarrollo del proyecto.
- Obtener una valoración de la situación inicial de la infraestructura actual de la red de datos mediante historiales, informes, logs así poder implementar las fases del modelo de gestión escogido.
- Desarrollar el modelo de gestión de red FCAPS con la finalidad de administrar los dispositivos que conforman la red mediante el software de monitoreo Nagios y sus herramientas complementarias.
- Elaborar la documentación necesaria con los parámetros elegidos del modelo de gestión aplicado.
- Validar el sistema de monitoreo mediante el análisis y evaluación, de los resultados obtenidos.

El desarrollo de este proyecto de titulación ha sido organizado por capítulos los cuales se detallan de forma rápida a continuación.

Dentro del primer capítulo denominado Estado del Arte se fundamenta los conceptos, antecedentes de proyectos anteriormente realizados y sustentos bibliográficos que validen la puesta en marcha de este trabajo.

En el segundo capítulo llamado Materiales y Métodos se presenta la puesta en marcha de la metodología aplicada detallando cada una de las fases aplicadas dentro del proyecto.

Seguidamente, el tercer capítulo titulado Resultados y Discusión se presenta el análisis de datos obtenidos con la implementación de la herramienta de monitoreo y modelo de gestión.

En el cuarto capítulo Conclusiones y Recomendaciones se efectúa un resumen general de la implementación del modelo de gestión y software de monitoreo. Y sugerencias realizadas en base a los resultados obtenidos.

Finalmente, en la sección de Anexos se puede observar los manuales de configuración del software implementado, manual de las fases del modelo de gestión FCAPS y política de monitoreo.

CAPÍTULO I

ESTADO DEL ARTE

Cumpliendo con la primera etapa de la investigación, el presente capítulo recopila información de investigaciones realizadas, conceptos que fundamentan el desarrollo del proyecto de implementación de un sistema de monitoreo y modelo de gestión de la red de datos de la PUCE-SI basada en herramientas open source.

1.1. Gestión de redes

Es un proceso de planificación, supervisión y control de la información compleja que circula por la red, dirigido o encaminado a mejorar el rendimiento de la misma, es decir de sus actividades con la finalidad de mejorar la disponibilidad, reducir riesgos y garantizar un adecuado nivel de servicio en todo momento.

La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable (Saydam & Magedanz, 1996)

Según la Organización Internacional de normalización que se encarga de la elaboración de normas técnicas internacionales, la gestión de red es el conjunto de actividades necesarias para el control y supervisión de los recursos que ayudan al intercambio de información que circula por la red de datos, aumentando su funcionalidad y rendimiento (ISO/IEC, 1989)

La administración es un complemento indispensable para la construcción y la implementación de un sistema de gestión de la red.

1.1.1. Elementos de un sistema de gestión de red

Se refieren a los equipos que se comunican con la red.

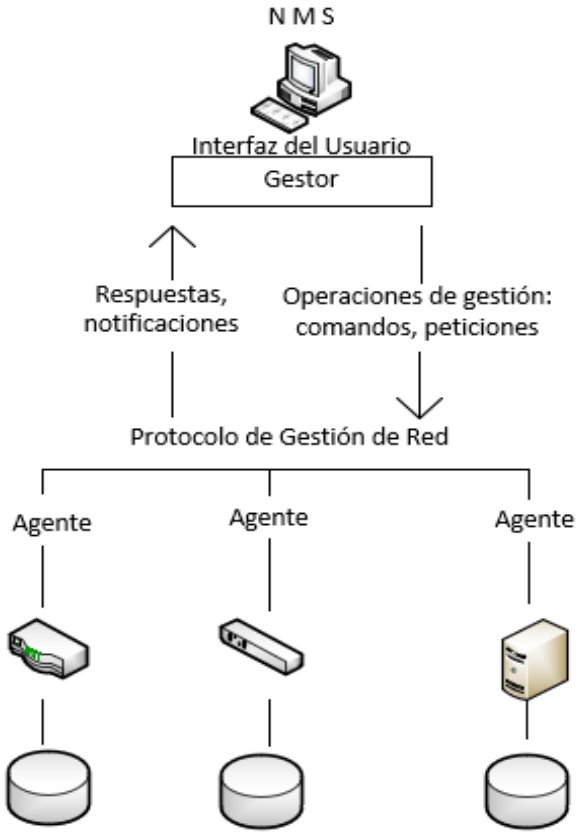


Figura 1. Elementos de un sistema de Gestión de Red
Fuente: María Fernanda Pinto

1.1.1.1. Administrador

Es el encargado de generar comandos y recibir notificaciones de los agentes.

1.1.1.2. Dispositivos gestionados

Son dispositivos de red como switches, routers, servidores que están controlados por el centro de administración o gestor que los monitorea. Estos recolectan información

1.1.1.3. Gestor

Están encargados de ejecutar aplicaciones para controlar, recibir notificaciones y respuestas permanentemente todos los dispositivos gestionados.

1.1.1.4. Agentes

Son entidades que interactúan con el dispositivo gestionado cumple la función de contestar las directivas enviadas por el gestor, puede utilizar el protocolo de administración para informar a la estación de red de un evento inesperado.

1.1.1.5. Estación de red

También llamada por sus siglas en ingles NMS (Network Management Station). Son dispositivos autónomos como servidores que ejecutan aplicaciones de gestión para el monitoreo de los dispositivos de la red y almacenan información de los mismos por esta razón deben poseer una memoria sustancial y espacio suficiente en el disco. Por lo general existe al menos una estación de red.

1.1.1.6. Protocolo de gestión de red

Un protocolo es el conjunto de delimitaciones y acuerdos que gobiernan la transmisión de información de procesos dentro de un sistema de Gestión de Red.

1.1.1.7. Base de información de gestión

Es un tipo de base de datos utilizada para la gestión de equipos dentro de una red de comunicaciones, se encarga del almacenamiento de datos entregados por los dispositivos gestionados de la red. (Ding, 2010)

1.1.2. Componentes de la gestión de red

1.1.2.1. Componente técnico

Establece las herramientas que se utilizaran para la gestión de Red, se basa en el intercambio de información entre agentes y gestor a través de un protocolo de gestión.
Y en dos procedimientos básicos:

Monitorización: Se refiere todas las actividades para la obtención de datos correspondientes a los dispositivos gestionados.

Control: Toma la información recolectada por la monitorización y actúa sobre los dispositivos de la red.

1.1.2.2. Componente funcional

Precisa las funciones que el componente organizacional ejecuta utilizando la herramienta de gestión.

1.1.2.3. Componente organizacional

Determina la estructura para el proceso de gestión y la estrategia adecuada para ejecutar de acuerdo con las necesidades.
Dentro de este componente se encuentran cuatro aspectos principales que son:

Control operacional: que son actividades con responsabilidades en un plazo de horas como por ejemplo el soporte a usuarios. Todas estas actividades deben registrarse para un posterior análisis.

Administración: son actividades con responsabilidad de duración en días orientadas al seguimiento de tareas de control operacional como la evaluación de calidad de los servicios o detección de fallos.

Análisis: son actividades de responsabilidad medida en meses que garantizan la calidad del servicio o define indicadores de desempeño para poder evaluar la calidad de servicio.

Planificación: que son actividades a largo plazo es decir en años, es la encargada de determinar las características principales que debe tener la red. (Orozco, 2010)

1.2. Estándar de gestión de red

Es una política entre el centro de administración y los dispositivos administrados que permite saber el estado de los dispositivos gestionados.

1.2.1. Protocolo simple de gestión de red

El protocolo SNMP (Simple Network Management Protocol) es un protocolo estándar de internet, su especificación se encuentra en el RFC 1157 (Force, 1990). Siendo RFC (Request for Comments) publicaciones pertenecientes al IETF (Internet Engineering Task Force) realizadas por un grupo de ingenieros o expertos que describen diversos aspectos del funcionamiento de redes, internet, procedimientos y protocolos.

SNMP es un protocolo de la capa de aplicación, se ha convertido en un estándar de gestión en donde su función principal es proporcionar monitorización y control centralizado de todos los dispositivos de una red determinando la estructura de paquetes y la secuencia de comunicación con la estación central. Los mensajes SNMP son recibidos en el puerto 161/UDP , 162/UDP (Trap).

Se basa en la flexibilidad y la facilidad de implementación gracias a este protocolo se puede administrar la red de forma remota mediante sondeo. Define el formato y el significado de los mensajes que intercambian un administrador con el agente, tiene la posibilidad de integrarse con productos sin importar su fabricante ya que la mayoría de equipos ofrecen agentes SNMP para ser gestionados. El protocolo SNMP cuenta con varias versiones, tales como SNMPv1, SNMPv2, SNMPv3, las mismas que tienen características en común que contribuyen al desarrollo del protocolo.

1.3. Modelos de gestión de red

Los modelos de gestión de red se ocupan de normalizar la información gestionada, es decir demuestra el modo en el que deben llevar a cabo las comunicaciones en cuanto a protocolos y servicios de gestión.

1.3.1. Modelo TMN (Telecomunications Management Network)

El modelo de Telecomunications Management Network (TMN), creado por la Unión Internacional de Telecomunicaciones con su comisión de normalización de las telecomunicaciones (UIT -T), su objetivo es brindar funciones de comunicación y gestión para la operación y mantenimiento de la red con los servicios de la misma. (Vicente Altamirano, 2003)

1.3.2. Modelo SNMP (Simple Network Management Protocol)

Este modelo presenta dos componentes estandarizados como son: la estructura de la información y los protocolos de gestión (RFC 1157, SNMP). Este modelo fue desarrollado por IETF (Internet Engineering Task Force) y generalmente se lo describe como un modelo sencillo pero limitado. (Sáiz Diez, Marticorena Sánchez, & López Nozal, 2009)

1.3.3. Modelo FCAPS o funcional

Este modelo describe previamente los objetos gestionados en una red para poder ser administrados. La norma ISO/IEC 10165-1 (1993) ISO/IEC 7498 (1989) definen al modelo y finalmente se introduce por recomendación de la ISO y la UIT-T como estándar de gestión de redes. Establece cinco áreas funcionales que son: (Martí, 1999)

1.3.3.1. Gestión de la configuración

Es registrar la configuración y el estado actual de la red identificando los elementos de la red, para finalmente realizar la configuración de una herramienta que cumpla con las necesidades del administrador, es importante mencionar que esta fase es la más importante ya que una configuración incorrecta puede hacer que la red no funcione correctamente. Cumple con la tarea de facilitar la creación de controles para supervisar las normas básicas, conservar datos de configuración y mantenimiento. (Ding, 2010)

1.3.3.2. Gestión de las prestaciones

Esta fase se basa en el registro del uso de servicios y recursos prestados por la red. Las principales tareas dentro de esta fase es la recolección de datos de recursos, registro de cuentas de usuarios. Dentro de los recursos gestionados se encuentran los recursos de comunicación, hardware, software y servicios. (Guerrero Pantoja , 2011)

1.3.3.3. Gestión de la contabilidad

Se refiere a evaluar el comportamiento de los dispositivos gestionados para medir la efectividad de medidas implementadas ya sea orientadas a servicios como la disponibilidad, tiempo de respuesta y fiabilidad u orientadas a eficiencia como: prestaciones y utilización. Para esta evaluación se define varios parámetros de monitoreo, estado y chequeo.

Las principales funciones son la captura de datos que indiquen el rendimiento ya sea: tasa de datos, tiempos de respuesta a los usuarios, recursos como CPU, memoria, puertos. (Tlv, 2010)

1.3.3.4. Gestión de fallos

Conjunto de tareas que posibilitan la detección, aislamiento y corrección de fallos, mediante una jerarquía de alertas dependiendo de la prioridad de los equipos y umbrales previamente establecidos por el administrador. Se realizará el envío de notificaciones oportunas si se registra un fallo en los dispositivos.

Dentro de esta fase se realiza la gestión de fallos de forma pasiva, esto se realiza a través de SNMP, si el dispositivo falla completamente no producirá una alarma para detectar el problema. La gestión de fallos activa se realiza a través de utilidades de diagnóstico como PING de esta forma si el dispositivo deja de responder se genera una alarma y la notificación oportuna del mismo.

Las funciones de esta fase es evitar que suceda el fallo a esto se lo conoce como gestión proactiva y se puede lograr mediante la definición de parámetros de alerta previa los mismos que cuando sean superados emitirán una notificación, también a través de pruebas preventivas como conectividad, integridad de protocolos, saturación de datos, saturación de conexiones y tiempo de respuesta.

La función si el fallo sucede se lo conoce como gestión reactiva y dentro de la misma está la detección de fallos que determina la causa del problema y lo localiza mediante alarmas ya sea de la herramienta de monitoreo o de usuarios.

Una vez detectado, se procede al aislamiento del componente de la falla con la herramienta de monitoreo según las opciones q presente esta. Finalmente, dentro de la gestión reactiva se realiza el diagnostico de fallos por intermedio de la experiencia del administrados, registros previos de fallos y la verificación o descarte de diferentes hipótesis. (Orozco, 2010)

1.3.3.5. Gestión de la seguridad

Dentro de esta fase están actividades para asegurar la red de comportamientos inapropiados de usuarios o accesos no autorizados, mediante el acceso, autorización y confidencialidad exclusiva del administrador de la red al sistema de gestión de los equipos y a la información.

Los ataques más probables que puede recibir el hardware o software dentro de esta gestión son la interrupción de un recurso mediante como puede ser un servidor o un equipo mediante técnicas de Haking. La intercepción de un usuario no autorizado para violar la integridad de la red y sus datos. (Tlv, 2010)

1.4. Software gestión de redes

Actualmente existen varias herramientas libres para realizar la monitorización de elementos de la red de datos. Dentro de la investigación realizada se han tomado en cuenta varias opciones de software como Pandora FMS, Cacti, Zenoss, Zabbix, Centreon y Nagios.

Es necesario realizar un análisis comparativo de cada una de las herramientas como se detalla a continuación.

	PANDORA FMS	**CACTI**	**Zenoss**	**Zabbix**
Monitorización de rendimiento y disponibilidad	X	X	X	
Gestión en eventos	X		X	
Geolocalización	X			
Administración por línea de comando	X		X	
Virtualización	X		X	X
Alta disponibilidad	X		X	X
Agentes multiplataformas	X			
Agentes para Android	X			
Entorno WEB	X		X	X
Consola WEB	X	X	X	
Métricas ITIL v3	X			
Consola SSH	X		X	
Consola Telnet	X		X	
Inventarios remotos	X		X	
Monitorización SNMP v1	X	X	X	X
Monitorización SNMO v2	X	X	X	X
Monitorización SNMP v3	X	X	X	X
Soporte IPv6	X			
Gestión de cambio de configuraciones	X			X
Gestión centralizada de recursos				
Monitorización de servicios				X
Monitorización remota descentralizada		X		X

Gestión remota de agentes				X
Escalabilidad				
Inventarios remotos				X
Personalización de informes	X		X	X
Manejo avanzado de plantillas		X		
Generación de gráficos		X	X	
Reportes vía email y SMS		X		X
Monitoreo en tiempo real		X	X	X
Código abierto	X	X	X	X

Tabla 1. Software de gestión de red
Fuente: María Fernanda Pinto

1.4.1. Pandora FMS (Flexible Monitoring System)

Es una herramienta de código abierto cuya función es encargarse del análisis de gestión de red desarrollado en el año 2003. Cuenta con la funcionalidad de monitorización de rendimiento y disponibilidad, geolocalización, agentes para Android, un nivel de control basado en role (Pandora FMS Enterprise, 2014).

Es importante mencionar que esta herramienta no es aconsejable utilizarla en entornos virtualizados ya que, si se desea utilizarla de esta manera los recursos como el disco, la memoria y CPU se los debe asignar de forma independiente. (Artica Soluciones Tecnológicas, 2014).

Es un software de monitorización generalizada ya que no cuenta con módulos de monitoreo en tiempo real.

1.4.2. Cacti

Cacti es una solución de gráficos de red el cual ayuda a controlar casi en tiempo real los dispositivos que soporten el protocolo SNMP, cuenta con el almacenamiento de datos y una

funcionalidad de gráficos llamada RRDtool. Funciona bajo entornos Apache, Php, Mysql es decir permite la visualización y gestión de forma WEB. (The Cacti Group, s.f.).

Cuenta con una base de datos relacional más sin embargo solo es utilizada para guardar información sobre las gráficas, informes y otros detalles, pero no para procesar o almacenar la información que se visualiza en las gráficas.

Esta herramienta no dispone de capacidad suficiente para saber si se ha caído un enlace de red, o para explorar la red, no se nos es posible visualizar la topología de la red. Otra de las desventajas de utilizar Cacti es la configuración tediosa de las interfaces y su complejidad para realizar las actualizaciones. Sobre todo, Cacti no monitorea el uso de memoria, disco o CPU de un servidor.

1.4.3. Zenoss

Es una herramienta de código abierto que fue creada en el año 2002 cuenta con dos versiones una de código de abierto y otra comercial. Posee varias características en una interfaz complicada por lo que se sugiere contar con una guía. Zenoss Core proporciona una solución de monitoreo de disponibilidad que incorpora la gestión de dispositivos, gráficos e informes de rendimiento, gestión de usuarios y alertas para controlar los activos en la infraestructura de la red. No se podría llamar un sistema escalar al momento de agregar manualmente los dispositivos que tengan activado el protocolo SNMP al sistema. (Badger, 2011)

1.4.4. Zabbix

Es una solución de monitoreo para varios parámetros de una red en código abierto, fue creado por Alexei Vladishev y actualmente respaldado por Zabbix SIA. Posee monitoreo en tiempo real de varios parámetros de la red y de la infraestructura de TI, utiliza mecanismos de notificaciones por correo electrónico que permite que permite a los usuarios una reacción rápida a problemas de los dispositivos, permite acceder a los informes, estadísticas y parámetros de configuración a través de una interfaz web. (Zabbix Company).

Zabbix tiene una configuración compleja sin una guía adecuada en cuanto a esto la documentación tiende a ser irregular y no cuenta con una comunidad de soporte actualizada.

1.4.5. Centreon

Es un software de monitoreo de aplicaciones y redes de código abierto, cuenta con una interfaz más amigable con el usuario puede ser utilizada también como una interfaz gráfica para otro software con más servicios como es Nagios. Cuenta con una cartografía de red personalizable como vistas por grupos, estos gráficos son similares a los de Cacti. Proporciona capacidad para obtener informes de host, servicios, grupos y porcentajes de accesibilidad y notificaciones. (Centreon, 2018).

Al realizar el análisis en cuanto al software se establece una diferencia principal entre el software con licencia y sin licencia. Siendo el software libre la mejor opción ya que su versión empresarial se basa en la versión core y se diferencian principalmente en brindar soporte técnico, consultas y mantenimiento. Este beneficio adicional de la versión paga se puede obtener mediante foros de comunidades en software libre.

En cuanto al nivel de detalle de la información mostrada, la facilidad para usar módulos, la flexibilidad para ampliar funcionalidades, además cumple con los aspectos requeridos por el modelo de gestión FCAPS se ha optado por Nagios.

1.4.6. Nagios

Es una herramienta de monitorización de redes, de código abierto que vela el rendimiento del hardware y los servicios que brinden los mismos. Dentro de las características importantes que tiene están: la monitorización de los servicios de red, la monitorización de recursos del hardware, autonomía de sistemas operativos.

Anteriormente llamado Netsaint y que se debió cambiar por similitud con otra marca, fue creado por Ethan Galstad con un conjunto de desarrolladores de software, originalmente fue diseñado para ser ejecutado en Linux y algunas variantes de Unix. (Wolfgang, 2008)

Nagios dentro de su estructura cuenta con un núcleo el cual controla y contiene el software para la realizar la monitorización de los dispositivos gestionados y servicios de la red, además hace uso de diversos componentes que están dentro de su paquete de instalación, así como también se puede hacer uso de extensiones o componentes realizados por terceros.

Nagios cumple con la supervisión del estado que es la tarea de realizar un seguimiento del estado actual de los dispositivos de red. Los estados de un dispositivo de red pueden estar disponibles o no ser accesibles. Nagios necesita constantemente saber el estado de un host o servicio, el proceso se llama “check”. Existen dos tipos de controles:

El control activo se usa cuando Nagios ejecuta un complemento para que verifique un host o servicio dependiendo de la forma de respuesta del complemento Nagios actualiza la información del estado del host o de los servicios. Nagios necesita poder comunicarse directamente con el dispositivo de destino. Por lo tanto, deben existir reglas de firewall para permitir esta comunicación.

El control pasivo se usa cuando una fuente externa se comunica con Nagios para dictar nueva información de estado para sus servicios al demonio NCSA, que a su vez notifica a Nagios. (Dondich, 2006). Los datos del monitoreo de la red son guardados en una base de datos y son mostrados en una interfaz web a través de un conjunto de páginas HTML que están incorporadas y CGI’s (Interfaz de Entrada Común).

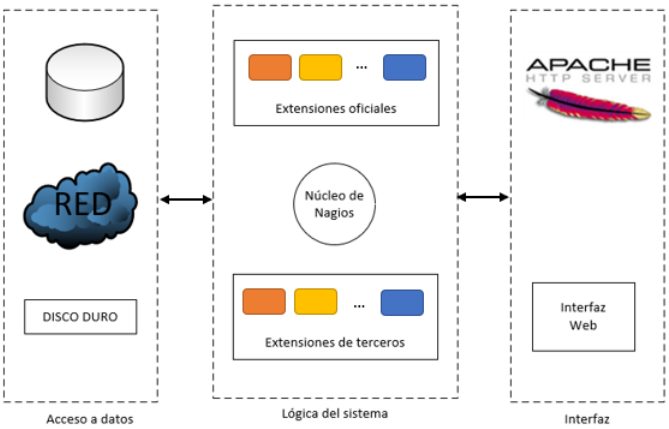


Figura 2. Estructura de Nagios
Fuente: (Guerrero Pantoja , 2011)

La herramienta como requisito de software para este proyecto está basada en la IEESTD-830-1998: Especificaciones de los Requerimientos del Software.

1.4.6.1. Requerimientos para Nagios

Los requerimientos necesarios para el funcionamiento de Nagios basados en el estándar IEEE 830 se detallan a continuación:

Recursos	Requerimientos Mínimos	Requerimientos Virtuales
Memoria RAM	1 GB	4 GB
Disco Duro	40 GB	80 GB
Procesador	Intel® Core ™ 1.80 GHz	Intel® Xeon ® E55600@ 2.8 GHz
Sistema Operativo	Linux	

Tabla 2. Requerimientos para Nagios
Fuente: María Fernanda Pinto

1.4.6.2. Directorios de Nagios

El software de gestión Nagios guarda su configuración, funcionamiento y ejecución en un directorio ubicado en **/usr/local/nagios**, el mismo que posee subdirectorios que se detallan a continuación:

bin: Aquí se encuentra el ejecutable de Nagios. Está en la ruta /usr/local/nagios/bin

etc: En este directorio está la configuración donde se especifica los host y servicios a monitorear con todas sus especificaciones, se encuentra en la ruta /usr/local/nagios/etc

libexec: Este directorio almacena los plugins que serán utilizados para ejecutar los servicios, está ubicado en la ruta /usr/local/nagios/libexec

sbin: Aquí se encuentra los archivos ejecutables que permiten la visualización de la interfaz web de Nagios, se encuentra en la ruta /usr/local/nagios/sbin.

var: Este directorio guarda un registro de la monitorización y se encuentra en la ruta /usr/local/nagios/var

share: Aquí se almacena la información que será mostrada en la interfaz web y se encuentra en la ruta/usr/local/nagios/share

1.4.6.3. Archivos de Nagios

Archivo de configuración principal: Es "nagios.cfg", está situado en la ruta /usr/local/nagios/etc/ cuenta con una serie de disposiciones que afectan la forma de funcionamiento del demonio de Nagios. Este archivo es leído por los CGIs y el demonio de Nagios.

Archivo de recursos: Su nombre es "resource.cfg", aquí se encuentra la información de configuración confidencial como usuarios y contraseñas que usan los comandos que ejecuta Nagios.

Archivos de definición de objetos: Aquí se define como se desea monitorear cada uno de los dispositivos gestionados. Nagios tiene por defecto archivos para tenerlos como ejemplos sobre diferentes tipos de objetos:

Host: Son dispositivos físicos de la red, estos archivos no son un modelo estricto a seguir, se puede crear nuevos archivos con la tipología que se desee.

Comandos: Sirven para indicar que plugins se deben ejecutar y el archivo toma el nombre de "commands.cfg"

Contactos: Son los usuarios que tienen acceso al Software y a los cuales se notificará cuando exista alertas, el archivo se llama "contacts.cfg"

Periodos de tiempo: Donde se configura los tiempos de ejecución de comandos y envío de notificaciones, el archivo se nombra "timeperiods.cfg"

Plantillas: Son archivos que tiene Nagios por defecto los cuales son utilizados de ayuda para la configuración de dispositivos y servicios. Toman el nombre de "templates.cfg"

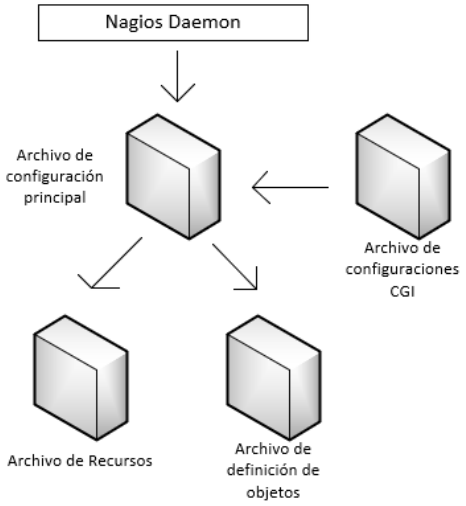


Figura 3. Estructura de Archivos de Nagios
Fuente: (Barth, 2008)

1.4.6.4. Complementos para Nagios

Para el software de gestión Nagios existen varios complementos que pueden ser instalados tanto en el gestor como en los dispositivos gestionados para alcanzar un mejor desempeño dentro de la obtención y análisis de los datos de cada ente gestionado.

1.4.6.4.1. PNP4 Nagios

Es un módulo el cual analiza los datos de rendimiento de los recursos de red a monitorear obtenidos por los plugins. Mediante este complemento se generan estadísticas gráficas personalizadas de equipos y servicios para intervalos de tiempo predefinidos las mismas que pueden ser exportadas. (Ortega Acosta & Sinche Cruz , 2011)

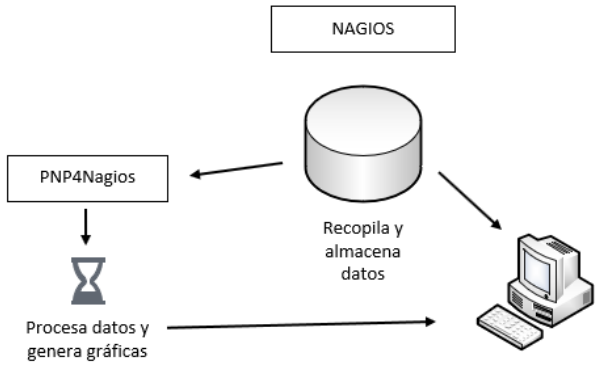


Figura 4. Comunicaciones de Nagios con el agente PNP4Nagios
Fuente: María Fernanda Pinto

1.4.6.4.2. Agente NSClient++

Este agente se encarga de obtener datos de servidores con sistema operativo Windows Server. Esto se obtiene mediante la instalación y configuración de dicho agente en cada uno de los equipos a monitorear y mediante el componente o plugin "check_nt". (Álvarez García)

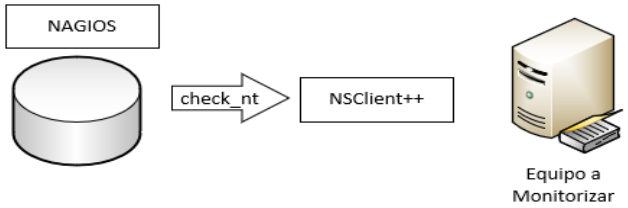


Figura 5. Comunicación de Nagios con el agente NSClient++
Fuente: María Fernanda Pinto

1.5. Análisis de temas relacionados

1.5.1. "Administración y Gestión de la red inalámbrica del Gobierno Autónomo Descentralizado (GADIP) del cantón Cayambe basada en el modelo funcional FCAPS de la ISO"

El tema "Administración y Gestión de la red inalámbrica del Gobierno Autónomo Descentralizado (GADIP) del cantón Cayambe basada en el modelo funcional FCAPS de la ISO" realizado por Edgar. D Jaramillo, Linda. E Torres. Este proyecto muestra los beneficios del monitoreo de la red inalámbrica mostrando la notable reducción de tiempo para resolver los fallos ocasionados con el establecimiento alarmas y notificaciones mediante correo electrónico al administrador o personal encargado de la administración y mantenimiento de la red. (Torres Chicaiza, 2015)

1.5.2. "Administración y gestión de la red de área local del GADIP Municipio de Cayambe, basado en el modelo funcional de gestión de red ISO/OSI con el protocolo SNMP y uso de herramientas de software libre"

El proyecto creado por Inuca Gonza, Cyntia Maribel focaliza el uso de herramientas con software libre para la gestión de redes siendo esta la mejor opción y además la importancia

del análisis de la situación inicial de la red siendo parte de esta el inventario de los equipos y sus características.

Como beneficio importante se tiene la facilidad que proporciona al administrador de tener un control de la información y funcionamiento de la red, para los usuarios una red más estable, disponible y segura. (Inuca Gonza, 2015)

1.5.3. "Análisis e implementación de un sistema integrado de gestión, para la red de datos de la Universidad Estatal de Bolívar matriz, en software libre"

En el presente trabajo investigativo realizado por Jairo Lozano Ramos, puntualiza la importancia y beneficios del modelo de gestión de redes FCAPS con sus diferentes fases, proporcionando a la institución superior el beneficio de un mejor servicio por parte del soporte técnico y facilitando la toma de decisiones a nivel administrativo para implementar nuevas políticas de acuerdo a los fallos que hayan ocurrido y los informes que proporciona la herramienta. (Ramos Gaibor, 2016)

1.5.4. "Diseño e implementación de un modelo de gestión de red para la red de área local del edificio central de la Universidad Técnica del Norte en base al modelo de la gestión con el protocolo SNMP"

El presente proyecto enfoca la importancia del levantamiento de la información para la generación de alertas y reportes para la implementación de un modelo de gestión. Menciona también la significación de los manuales de procedimientos para cada una de las áreas. Con este proyecto se comprueba el sistema de gestión de la red basada en modelo ISO permitiendo que la red se monitoree continuamente. (Báez Cheza, 2017)

1.5.5. Comparativa de temas relacionados.

Los trabajos antes mencionados se focalizan en la importancia del uso de modelo funcional y sus etapas dentro de la gestión de la red para su correcta monitorización y mantenimiento.

Además, en base a las conclusiones de temas relacionados, la herramienta escogida para poner en función el modelo de gestión es la óptima ya que cubre las necesidades que se tiene dentro de este trabajo de titulación. Cada una de las investigaciones anteriormente realizadas han servido de base para la propuesta y puesta en marcha de este trabajo de titulación ya que cada uno aporta individualmente con la metodología empleada, el protocolo a utilizar y el software de monitoreo. Para en el caso de este trabajo de titulación juntar esos aportes y realizar esta propuesta sustentada en las investigaciones.

CAPÍTULO II
MATERIALES Y MÉTODOS

Dentro de este capítulo se obtiene una valoración de la situación inicial de la infraestructura actual de la red de datos, se indican procesos para el desarrollo del modelo de gestión dentro de cada una de las fases del mismo esto incluye la configuración detallada del software de gestión y monitoreo.

2.1. Tipo de investigación

El presente proyecto se basa en primer lugar en la investigación documental en diferentes fuentes bibliográficas que sustenten el desarrollo del modelo de gestión de redes y la configuración necesaria de la herramienta de monitoreo. Como primer momento dentro de la investigación se realiza el análisis de las actividades que se realizan dentro del área de redes, lugar donde se implementa el sistema propuesto, lo cual permite una mejor comprensión de la importancia del trabajo que ahí se realiza para posteriormente proceder con la solución tecnológica que permita resolver los inconvenientes que se presentan dentro de la misma.

Basados en esta investigación previa y sustentada en el capítulo anterior se emplea el Modelo de gestión funcional el cual al ser una norma ya suple el uso de un marco de referencia ya que dicho modelo de gestión está en base a la norma FCAPS lo cual faculta que este modelo esté en base a dichas normativas y buenas prácticas en cada una de sus fases las cuales serán desarrolladas en este capítulo.

2.2. Modelo de gestión FCAPS

Basado en el modelo definido anteriormente, el presente trabajo delimitará su alcance al desarrollo de las fases más relevantes para cubrir las necesidades institucionales y requerimientos técnicos de la Unidad de Sistemas de la PUCE-SI.

2.2.1. Gestión de la configuración

Dentro de esta fase se realiza un análisis de la situación actual de la red de datos, de esto se obtiene la topología de red, diagramas físicos y lógicos de la LAN, y el inventario actualizado de los componentes activos de la red. Con esta información se determina los recursos que debe tener el servidor virtual donde se realizará la implementación de la herramienta de monitoreo. También se determina las configuraciones necesarias en los dispositivos de red y finalmente la configuración de la herramienta de gestión.

2.2.1.1. Situación actual de la infraestructura tecnológica

Es importante conocer la situación actual en la que se encuentra la infraestructura tecnológica de la PUCE-SI para de esta manera poder determinar que equipos soportan los protocolos necesarios para poner en marcha la configuración de monitoreo.
Cabe recalcar que el direccionamiento y segmentación no se especifican por la razón de ser información confidencial.

Inventario de la red de datos

No.	Descripción / Modelo		Marca	Ubicación
1	FIREWALL	FIREWALL/VPN Cisco ASA 5510	Cisco	#3 Rack Principal
2		compaq dc6300	HP	#3 Rack Principal
3		compaq DC5850_Backup	HP	#3 Rack Principal
4		Fortigate	Fortinet	#3 Rack Principal
5	ENRUTADOR	switch catalyst 4500	Cisco	EDIF#3 Data center
6	SWITCHES	Switch Catalyst 3560G Series	Cisco	EDIF#3 Data center
7		Switch Baseline 2024	3com	#3 Rack Secundario Lab

8		Switch Baseline 2024	3com	#3 Rack Secundario Lab
9		Switch Baseline 2024	3com	#3 Rack Secundario Lab
10		Switch Baseline SuperStack 3	3com	#3 Rack Secundario Lab
11		Switch Catalyst 2960G Series	Cisco	#3 Rack Principal
12		Switch Catalyst 2960G Series	Cisco	#1 secundario ENCI
13		Switch Catalyst 2960G Series	Cisco	#2 Rack secundario
14		Switch Catalyst 2960G Series	Cisco	#2 Rack secundario
15		Switch Catalyst 3560G Series	Cisco	#3 Rack Principal
16		Switch LinkSys SRW2024P	Cisco	#2 Rack secundario planta baja
17		Switch LinkSys SRW2024	Cisco	#2 UCI
18		Switch LinkSys SRW2024	Cisco	#3 ECAA
19		Switch LinkSys SRW2024	Cisco	#2 Rack secundario planta baja
20		Switch LinSys SRW2024P	Cisco	#1 Rack secundario Biblioteca
21		Switch LinSys SRW2024P	Cisco	#3 rack Secundario Sala 9
22		Switch LinSys SRW2024P	Cisco	#1 secundario ENCI
23		Switch ProCurve HP 4000M	HP	#3 Rack Principal

24		Switch ProCurve HP 4104GL	HP	#3 Rack Principal
25		Switch Catalyst 2960G Series	Cisco	#2 Rack secundario
26		Switch LinkSys SRW2024P	Cisco	#3 Rack secundario ECAA
27		Switch LinkSys SRW2024P	Cisco	#3 Rack Secundario Lab
28		Switch LinkSys SRW2024P	Cisco	Centro interactivo ECAA
29		switch small business SG300 28P	Cisco	#2 rack secundario Aula Magna
30		Access Point Small Business Pro	Cisco	#1 rack secundario Docentes T. Completo
31		switch small business SG300 28P	Cisco	#2 rack sala docentes general
32		switch small business SG300 28P	Cisco	#2 rack Oficina adquisiciones
33		switch small business SF300 48P	Cisco	#3 Rack Secundario Lab
34		switch small business SG300 28P	Cisco	#1 rack secundario ENCI
35		switch small business SG300 28P	Cisco	#2 rack secundario
36		switch small business SG300 28P	Cisco	#2 rack secundario UCI
37		switch small business SG300 28P	Cisco	#1 rack secundario Biblioteca
38		switch cisco catalys 2960S	Cisco	#1 rack secundario ENCI

39		switch cisco catalys 2960S	Cisco	#2 rack secundario
40		switch cisco catalys 2960S	Cisco	#3 rack principal
41		wireless cisco 2500 AIR-CT2504-K9	Cisco	#3 rack principal
42		switch small business SG300 28P	Cisco	#2 rack Sala DTCFrente adquisiciones
43		switch small business SG300 28P	Cisco	Sala DTC Edif#1 piso1.2.1
44		switch small business SG300 28P	Cisco	EDIF #1 rack principal
45		switch small business SG300 28P	Cisco	EDIF #1 Sala DTC 1.2.x
46		switch small business SG300 28P	Cisco	SALA12 EDIF3 PISO1
47		Wireless LAN controller 5508	Cisco	data center
48		switch cisco catalys 2960S	Cisco	EDIF#4 Piso1 Rack Principal SW1
49		switch small business SG300 52P	Cisco	EDIF#4 Piso1 Rack Principal SW2
50		switch small business SG300 28P	Cisco	EDIF#4 Piso1 Rack Principal SW3
51		switch small business SG300 52P	Cisco	EDIF#4 Piso2 Rack secundario SW1
52		switch small business SG300 28P	Cisco	EDIF#4 Piso2 Rack secundario SW2
53		switch small business SG300 28P	Cisco	EDIF#3 Sala 13 piso3

54		switch small business SG300 28P	Cisco	EDIF#3 Sala 14 piso3
55		switch small business SG300 28P	Cisco	Nueva Capilla sala de reuniones
56		small business sg200 8p	Cisco	garita seguridad
57		switch small business SG300 28P	Cisco	Sala de audiencias 2.1.14
58		switch cisco catalys 2960S	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW1
59		switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW2
60		switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW3
61		switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW4
62		switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso2 Rack secundario SW5
63		switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso2 Rack secundario SW6
64		catalyst 2960S	Cisco	SW1 EDIF 4 ET3
65		switch small business 28PP	Cisco	SW3 EDIF 4 ET2
66		switch small business 28PP	Cisco	SW4 EDIF 4 ET3
67		switch small business 28PP	Cisco	SW5 EDIF 4 ET3
68		switch small business 28PP	Cisco	SW6 EDIF 4 ET3
69		switch small business 28PP	Cisco	SW2 EDIF 4 ET3

70		switch small business 28PP	Cisco	EDIF#3 SALA 6
71		switch small business 28PP	Cisco	EDIF#3 SALA 5
72		switch small business 28PP	Cisco	EDIF#3 SALA 9
73		switch small business 28PP	Cisco	BODEGA SISTEMAS PARA REDES TEMPORALES
74		switch cisco sg200-10fp	Cisco	OFICINA INFORMACION
75		switch small business 28PP	Cisco	BANCO DE GERMOPLASMA
76		switch small business 28PP	Cisco	ARCHIVO INACTIVO DIR ESTUADINTES
77		switch small business 28PP	Cisco	EDIF #3 RACK ASO INGENIERIA
78		switch small business 28PP	Cisco	EDIF #2 SALA 2.3.18
79		switch small business 28PP	Cisco	BODEGA SISTEMAS STOCK
80		switch small business 28PP	Cisco	BODEGA SISTEMAS STOCK
81	ACCES POINT	AIR-LAP1041N-A-K9	Cisco	Edif #1_piso6_ biblioteca
82		AIR-LAP1041N-A-K9	Cisco	Edif #1 piso4_Arquitectura
83		AIR-LAP1041N-A-K9	Cisco	Edif #1 piso2_AEPUCESI
84		AIR-LAP1041N-A-K9	Cisco	Edif #1 piso5_aula1.5.3
85		AIR-LAP1041N-A-K9	Cisco	Edif #1 piso3_aula 1.3
86		AIR-LAP1041N-A-K9	Cisco	Edif #1 piso1_aula1.1
87		AIR-LAP1041N-A-K9	Cisco	Edif #2 piso2_Maestrias
88		AIR-LAP1041N-A-K9	Cisco	Edif #2 piso2_Ecoms

89		externo AIR-LAP1310G-A-K9R	Cisco	Edif #1 piso4_parte exterior frontal
90		AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 1 _aula2.2.2
91		AIR-LAP1041N-A-K9	Cisco	Edif #2 Planta baja SALA DTC
92		AIR-LAP1041N-A-K9	Cisco	Edif #2 Piso1 planta física
93		AIR-LAP1041N-A-K9	Cisco	Edif #2 planta baja PLANIFICACION
94		AIR-LAP1041N-A-K9	Cisco	Edif #2 parte posterior ADQUISICIONES
95		AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 2 SALA DE GRADOS
96		AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 2 SALA CONFERENCIAS
97		AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 1 PRORECTORADO
98		AIR-LAP1041N-A-K9	Cisco	Edif #2 planta baja HALL PRINCIPAL
99		AIR-LAP1041N-A-K9	Cisco	Edif #2 planta baja AULA MAGNA
100		AIR-LAP1041N-A-K9	Cisco	Edif #3 piso 2 ECAA
101		AIR-LAP1041N-A-K9	Cisco	Edif #3 piso1
102		AIR-LAP1041N-A-K9	Cisco	Edif #3 planta baja (laboratorios sistemas)
103		AIR-LAP1041N-A-K9	Cisco	Edif #3 Piso 1 sala IMac
104		AIR-LAP1041N-A-K9	Cisco	Edif #3 piso1 pasillo
105		AIR-LAP1041N-A-K9	Cisco	Edif #3 planta baja pasillo
106		AIR-CAP1602I-A-K9	Cisco	EDIF#4 Planta baja fin pasillo 4.1.5
107		AIR-CAP1602I-A-K9	Cisco	EDIF#4 Planta baja inicio pasillo

108		AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 1 fin pasillo
109		AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 1 inicio pasillo
110		AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 2 fin pasillo
111		AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 2 inicio pasillo
112		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 1
113		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 2
114		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 3
115		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 4
116		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 PISO2 PASILLO JUNTO SSHH
117		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 PISO2 PASILLO MITAD
118		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 PISO2 PASILLO INICIO
119		AIR-CAP2702I-A-K9	Cisco	EDIF#3_P3_PASILLO IDIOMAS
120		AIR-CAP2702I-A-K9	Cisco	TALLERES GESTHUR AULA 2.1.26
121		AIR-CAP2702I-A-K9	Cisco	EDIF#1 PISO1 AULA 1.3.1
122		AIR-CAP2702I-A-K9	Cisco	EDIF#1 PISO2 SALA DTC 1.1.2
123		AIR-CAP2702I-A-K9	Cisco	EDIF #1 PISO 5 DERECHA AULA 1.5.2
124		AIR-CAP2702I-A-K9	Cisco	EDIF #1 PISO 3 DERECHA AULA 1.3.6
125		AIR-CAP2702I-A-K9	Cisco	EDIF #1 PISO 5 IZQUIERDA AULA 1.5.4

126		AIR-CAP2702I-A-K9	Cisco	REDES TEMPORALES EN AREAS ESPECIFICAS
127		AIR-CAP2702I-A-K9	Cisco	REDES TEMPORALES EN AREAS ESPECIFICAS
128		AIR-CAP2702I-A-K9	Cisco	REDES TEMPORALES EN AREAS ESPECIFICAS
129		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO1 F
130		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO1 P
131		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO2 F
132		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO2 P
133		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO3 F
134		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO3 P
135		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 PLANTA BAJA NUEVA SALA DE GRADOS
136		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 SECRETARIA PASILLO JARDINERA
137		AIR-CAP2702I-A-K9	Cisco	EDIF#4 COUNTER INFORMACION
138		AIR-CAP2702I-A-K9	Cisco	CASA EVENTOS ECAA
139		AIR-CAP2702I-A-K9	Cisco	EDIF#2 USE OFICINAS
140		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 GALERIA ARQUEOLOGICA
141		AIR-CAP2702I-A-K9	Cisco	HERBARIO

142		AIR-CAP2702I-A-K9	Cisco	EDIF#3 PISO2 SALA IMAC
143		AIR-CAP2702I-A-K9	Cisco	EDIF#2 SALA 2.3.16
144		AIR-CAP2702I-A-K9	Cisco	EDIF#2 SALA 2.3.17
145		AIR-CAP2702I-A-K9	Cisco	EDIF#4 OFICINAS CONTABILIDAD
146		AIR-CAP2702I-A-K9	Cisco	EDIF#4 HALL ENTRADA PRINCIPAL
147		AIR-CAP2702I-A-K9	Cisco	EDIF#4 PB BIBLIOTECA CERCA AL COUNTER
148		AIR-CAP2702I-A-K9	Cisco	EDIF#4 PB BIBLIOTECA CERCA A CUBICULOS
149		AIR-CAP2702I-A-K9	Cisco	EDIF4_P1_MITAD PASILLO
150		AIR-CAP2702I-A-K9	Cisco	EDIF4_PISO3_AULA4_3_17
151		AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3
152	ANTENAS	Nanobridgem5	Ubiquiti	BANCO DE GERMOPLASMA
153		Nanobridgem5	Ubiquiti	SALA INTERACTIVA ECAA
154		antena rocket	Ubiquiti	TERRAZA EDIFICIO 4
155		Nanobridgem5	Ubiquiti	BODEGA ECAA

Tabla 3. Listado de componentes de la red de datos PUCE-SI
Fuente: Msc. Paúl Enríquez, Jefe Área de Redes

Infraestructura de servidores

nro	UBICACIÓN	tipo			NOMBRE EN EL RACK	Estado	aplicaciones y servicios
1	data center RACK 1	BLADE	cuchilla 1	virtual	ECOMS	Producción	radio PUCESI on line /bdd sitio web/ showcast
2	data center RACK 1			virtual		Producción	Sitios web revistas digitales
3	data center RACK 1			virtual		Producción	pruebas uci
4	data center RACK 1		cuchilla 2	virtual	Svracademico	Producción	Syllabus
5	data center RACK 1			virtual		Producción	Nuevo sistema Académico
6	data center RACK 1		cuchilla 3	virtual	campus virtual	Producción	Moodle campus virtual
7	data center RACK 1			virtual	Capacitación virtual	Producción	Moodle capacitación virtual
8	data center RACK 1		cuchilla 4	virtual	Sistemas	Producción	Respaldos/Iperius/Drive
9	data center RACK 1					Producción	replicador directorio activo / Sincronización Google Apps/DHCP
10	data center RACK 1		cuchilla 5	virtual	DSPACE	Producción	dspace/repositorio digital
11	data center RACK 1			virtual		Producción	freeradius/eduroam
12	data center RACK 1			virtual		Producción	freeradius para autenticación en Wireless
13	data center RACK 1		cuchilla 6	físico	WEBPUCESI_antiguo	Inactivo	web site pucesi / SAML2.0
14	data center RACK 1		cuchilla 7	virtual	PRODUCCION	Producción	Aplicaciones web para producción
15	data center RACK 1			virtual		Producción	BDD oracle y MySQL para producción

16	data center RACK 1		cuchilla 8	virtual	PRUEBAS	Producción	Aplicaciones web en ambiente de pruebas
17	data center RACK 1			virtual		Producción	BDD oracle y MySQL en ambiente de pruebas
18	data center RACK 1	BLADE	cuchilla 1	físico	PUCESI.EDU.EC	Producción	Controlador de dominio / DNS
19	data center RACK 1		cuchilla 2	físico	SVRPROXY	Producción	Squid / DHCP
20	data center RACK 1		cuchilla 3	físico	SVRTINI	Producción	TINI /BDD
21	data center RACK 1		cuchilla 4	físico	fuera de servicio	Inactivo	fuera de servicio
22	data center RACK 1		cuchilla 6	virtual	Ingeniería	Producción	BDD oracle uso prácticas estudiantes
23	data center RACK 1			virtual		Producción	BDD SQL uso prácticas estudiantes
24	data center RACK 1			virtual		Producción	aplicaciones web escuela ingeniería
25	data center RACK 1		cuchilla 7	virtual	INGENIERIA BDD	Producción	prácticas de bdd estudiantes ingeniería
26	data center RACK 1			virtual		Producción	sitio web escuela de ingeniería
27	data center RACK 1			virtual		Producción	aplicaciones web escuela de ingeniería
28	data center RACK 1			virtual		Producción	proyecto hydroVlab
29	data center RACK 1		cuchilla 8	físico	APLILAB	Producción	Aplicaciones Laboratorio /Antivirus Eset
30	data center RACK 3	SYNERGY	BAY1	virtual	svrtelefonia	Producción	Telefonía IP
31	data center RACK 3			virtual	svrnagios	Pruebas	En pruebas de Nagios, Monitoreo de red y servidores.
32	data center RACK 3			virtual	svrSSO	Producción	SAML /SSO Login WIFI, login mail.
33	data center RACK 3		BAY7	virtual	webpucesi	Producción	sitio web pucesi
34	data center RACK 3			virtual	BddPUCESI	Producción	bdd sitio web

35	data center RACK 3			virtual	RadioPUCESI	Producción	radio PUCESI on line
36	data center RACK2		rack	físico	svrbdd_desarrollo	Producción	Bases de datos para pruebas de desarrollo / SUBVERSION
37	data center RACK2		rack	físico	svrreportes	Producción	Reporting server
38	data center RACK2		rack	físico	bdd_desarrollo_acad	Producción	BDD Oracle / BDD MySQL
39	data center RACK2		rack	físico	svruse	Producción	MOODLE / educación continua
40	data center RACK2		rack	físico	srvbddsql	Producción	BDD SQL / Data Protector Manager / SAB
41	data center RACK2		torre	físico	svrfirewall	Producción	IPTABLES
42	data center RACK2		torre	físico	svrfirewall_bk	Inactivo	IPTABLES
43	data center		torre	físico	pucesitelefonia	Producción	Elastix/ telefonía IP
44	data center RACK 1		rack	virtual	svrescuelaing	Producción	aplicaciones web escuela de ingeniería
45	data center		torre	físico	cámaras	Producción	DviewCam / cámaras de seguridad laboratorios de sistemas

Tabla 4. Listado de servidores PUCE-SI
Fuente: Msc. Paúl Enríquez, Área de Redes

Topología de la red

En este apartado se detallan los diagramas físicos y lógicos de la red.

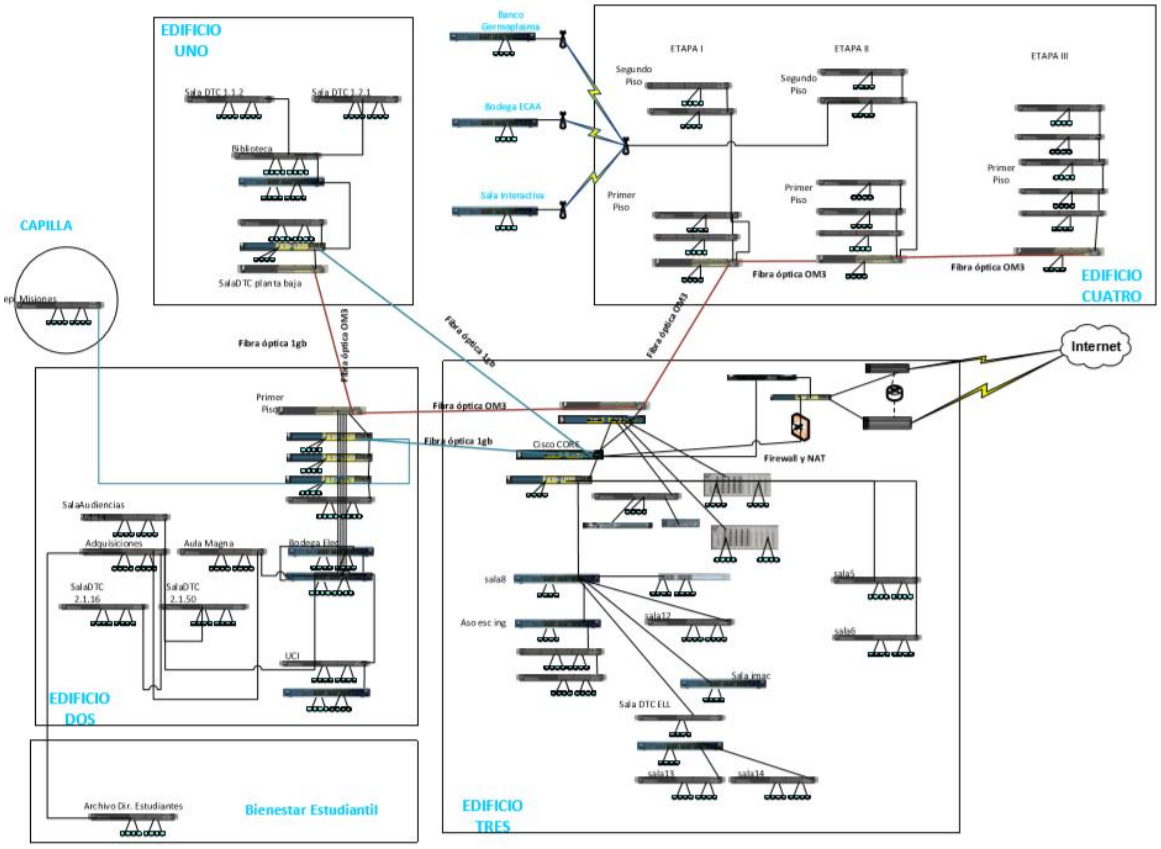


Figura 6. Diagrama físico de la red de datos de la PUCE-SI
Fuente: MSc. Paúl Enríquez, jefe del Área de Redes

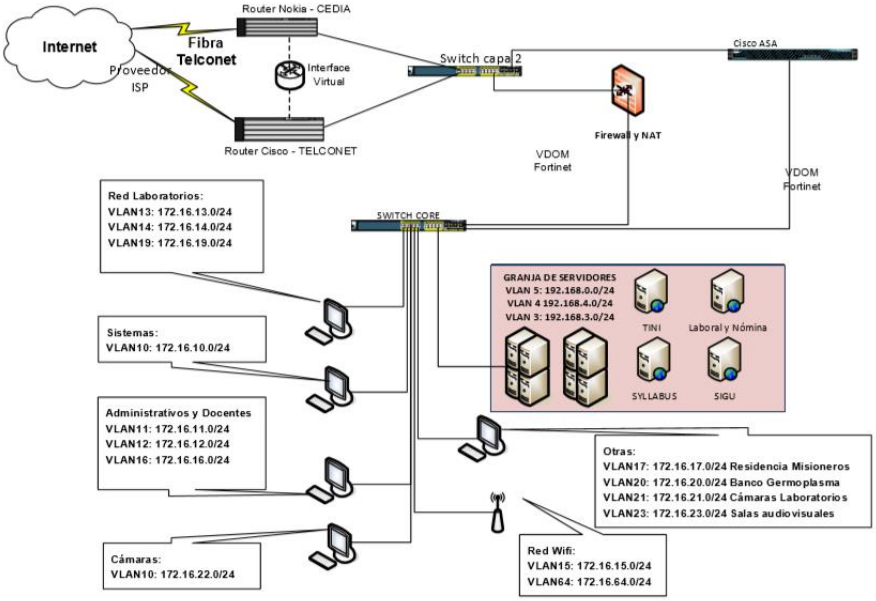


Figura 7. Diagrama lógico de la red de datos de la PUCE-SI
Fuente: MSc. Paúl Enríquez, Área de Redes

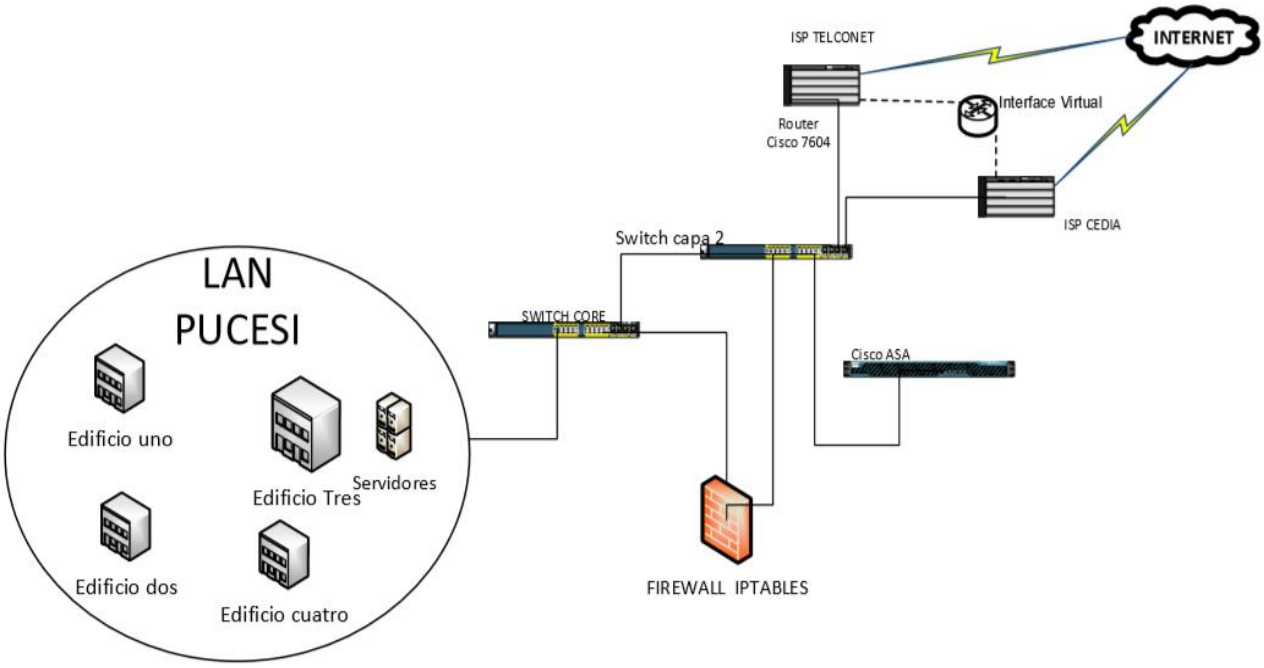


Figura 8. Diagrama lógico 2 de la red PUCE -SI
Fuente: MSc. Paúl Enríquez, Área de Redes

2.2.1.2. Especificación de Requisitos

Basada en el formato de especificación de requisitos (ERS), según la última versión del estándar IEEE 830.

Introducción

En esta sección se detallará los requisitos de software para la herramienta de monitoreo que se implementará para el desarrollo del presente trabajo de titulación.

Propósito

La especificación de requisitos tiene como finalidad precisar los requerimientos, restricciones y funcionalidades del software de gestión.

Ámbito del sistema

El sistema de monitoreo y gestión de red cumplirá la función de permitir una administración centralizada de los dispositivos de red anclados al mismo con envío de notificación vía correo electrónico al administrador de la red si ocurre un evento fuera de lo normal.

Definiciones, Acrónimos, Abreviaturas

ERS: Especificación de Requisitos de Software

IEEE: Instituto de Ingenieros Electrónicos y Eléctricos

STD: Estándar.

SNMP: Simple Network Management Protocol

Referencias

(IEEE-STD-830, 1998)

Descripción general

Perspectiva del Producto

El software de gestión debe ser estable y sobre todo estar basado en software libre.

Funciones del Producto

La función principal es monitorear constantemente los dispositivos gestionados.

Características de los Usuarios

Los usuarios destinados a usar este software de gestión y monitoreo son personal técnico con conocimiento de redes.

Restricciones

- La herramienta de gestión y los complementos de la misma deben ser open source.
- Debe ser compatible con un sistema de virtualización
- Soportar el envío de información mediante SNMP

Requisitos Específicos

Id:	1F	**Nombre:**	Ingresar host
Prioridad:	Alta		
Descripción:	El Administrador ingresa al sistema y genera el archivo de configuración del host y sus servicios a monitorear		

- El usuario ingresa vía CLI al servidor - Ingresa a la ruta donde se declaran los objetos monitoreados. - Se edita el archivo con el nombre del host y con IP - Se reinicia el servicio

Tabla 5. Requisito funcional - Ingresar host
Fuente: María Fernanda Pinto

Id:	2F	**Nombre:**	Modificar del host
Prioridad:	Alta		
Descripción:	El Administrador ingresa al sistema para realizar la modificación de un parámetro del host		
- El usuario ingresa vía CLI al servidor - Ingresa a la ruta donde está el archivo a modificar - Edita el archivo con el parámetro a cambiar. - Reinicia el servicio.			

Tabla 6. Requisito funcional - Modificar host
Fuente: María Fernanda Pinto

Id:	3 F	**Nombre:**	Eliminar de host
Prioridad:	Alta		
Descripción:	El Administrador ingresa al sistema y elimina el archivo de configuración del host a eliminar.		
- El usuario ingresa vía CLI al servidor. - Ingresa a la ruta donde está el archivo a eliminar. - Elimina el archivo. - Reinicia el servicio.			

Tabla 7. Requisito funcional - Eliminar host
Fuente: María Fernanda Pinto

Id:	4F	**Nombre:**	Alertas
Prioridad:	Alta		
Descripción:	El Administrador ingresa al sistema y en el apartado de alertas revisa los eventos que ha tenido un host.		
- El usuario ingresa vía GUI al software.			

- Elige el host a monitorear - Selecciona la opción de ver alertas del host.

Tabla 8. Requisito funcional – Alertas
Fuente: María Fernanda Pinto

Id:	5F	**Nombre:**	Generar reporte
Prioridad:	Media		
Descripción:	El Administrador ingresa al sistema y elige el dispositivo del cual desea generar un reporte		
- El usuario ingresa vía GUI al software. - Selecciona la opción “disponibilidad” - Elige el host o grupo de host a generar reporte de disponibilidad. - Selecciona el tiempo del reporte - Genera el reporte.			

Tabla 9. Requisito funcional - Generar reporte
Fuente: María Fernanda Pinto

Id:	1NF	**Nombre:**	Seguridad
Prioridad:	Alta		
Descripción:	Los permisos de acceso solo pueden ser cambiados por el administrador		
- El administrador ingresar vía CLI al servidor - Ingresa a la ruta donde se encuentran los contactos - Ejecuta el comando htpasswd sobre el fichero. - Añade o cambia los permisos para los usuarios.			

Tabla 10. Requisito no funcional – Seguridad
Fuente: María Fernanda Pinto

Id:	2NF	**Nombre:**	Usabilidad
Prioridad:	Alta		
Descripción:	El sistema debe contar con manuales estructurados		
- El administrador contará con los manuales de la herramienta de monitoreo			

Tabla 11. Requisito no funcional – Usabilidad
Fuente: María Fernanda Pinto

2.2.1.3. Diseño para la implementación del modelo de gestión

La herramienta a implementar es Nagios, un software líder que cumple con los aspectos requeridos para el modelo de gestión FCAPS, el cual en puntos anteriores fue escogida después de una selección de entre otras con el respaldo bibliográfico correspondiente.

Habiendo escogido la herramienta y cumplido los requerimientos de hardware se procede a realizar el diseño del sistema de gestión. Para ello se ha determinado el alojamiento de un servidor virtualizado dentro de la arquitectura de servidores Synergy que posee la PUCESI.

Modelo	HP Synergy 12000
Servidor	HP SY480 Gen10
Procesador	Intel Xeon Silver 4114
Memoria	128GB
Disco duro	1TB
Conectividad LAN	HPE VC SE 10Gb F8 Module Redundante
Gestión de Infraestructura	HPE Synergy Composer desarrollado por HPE OneView.

Tabla 12. Características y especificaciones - Arquitectura Synergy
Fuente: María Fernanda Pinto

Memoria	4 GB
Espacio en disco	100 GB
CPU	1vCPU

Tabla 13. Características Servidor Virtual
Fuente: María Fernanda Pinto

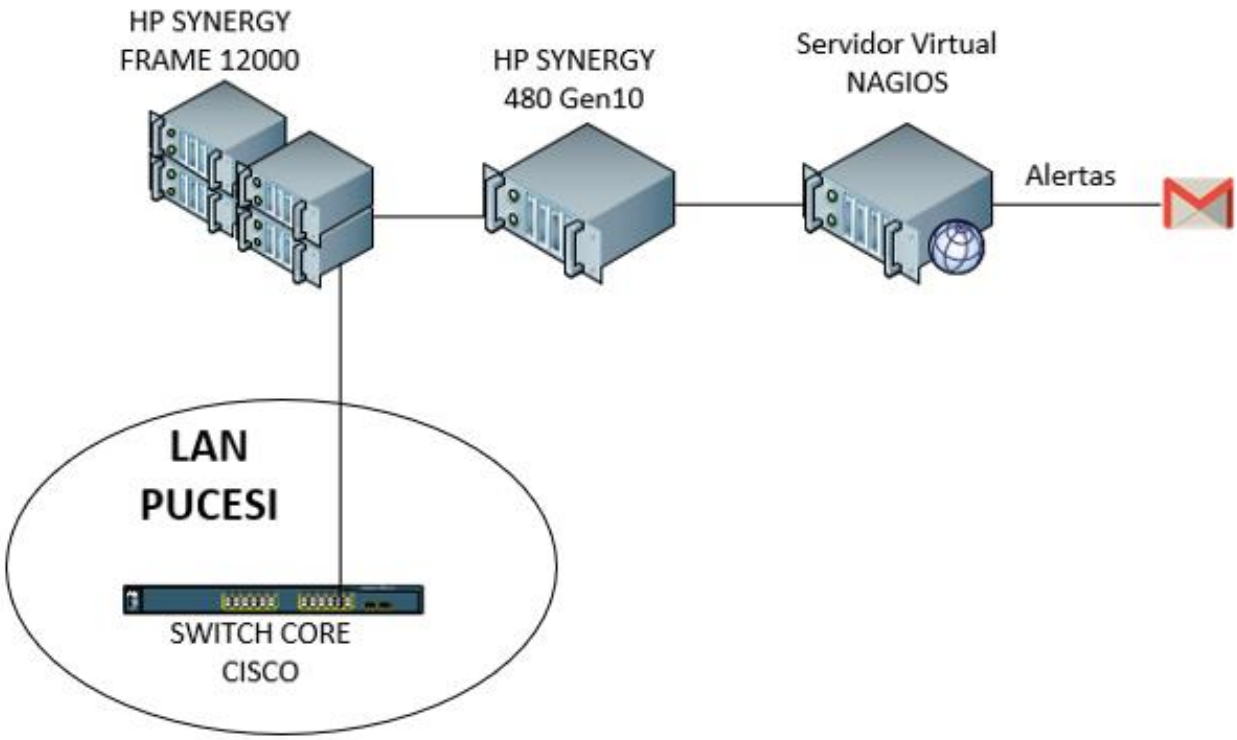


Figura 9. Diseño para la implementación del modelo de gestión
Fuente: María Fernanda Pinto

2.2.1.4. Configuración del Gestor

Instalación y configuración de Nagios.

Para la instalación de Nagios se necesitan ciertos requisitos previos los cuales se detallan a continuación, cada uno con la versión instalada:

Requerimiento	Versión
Centos	7
Apache	2.4.6
PHP	7.2

Tabla 14. Requisitos previos para instalar Nagios
Fuente: María Fernanda Pinto

Para la instalación de Nagios y sus dependencias se debe seguir una serie de pasos ejecutando los comandos que se encuentran debidamente enlistados dentro del Manual de Instalación y Configuración de Nagios 4.4.3 (ver anexo I). Una vez instalado Nagios se podrá visualizar la interfaz web de la herramienta de monitoreo como se muestra a continuación.

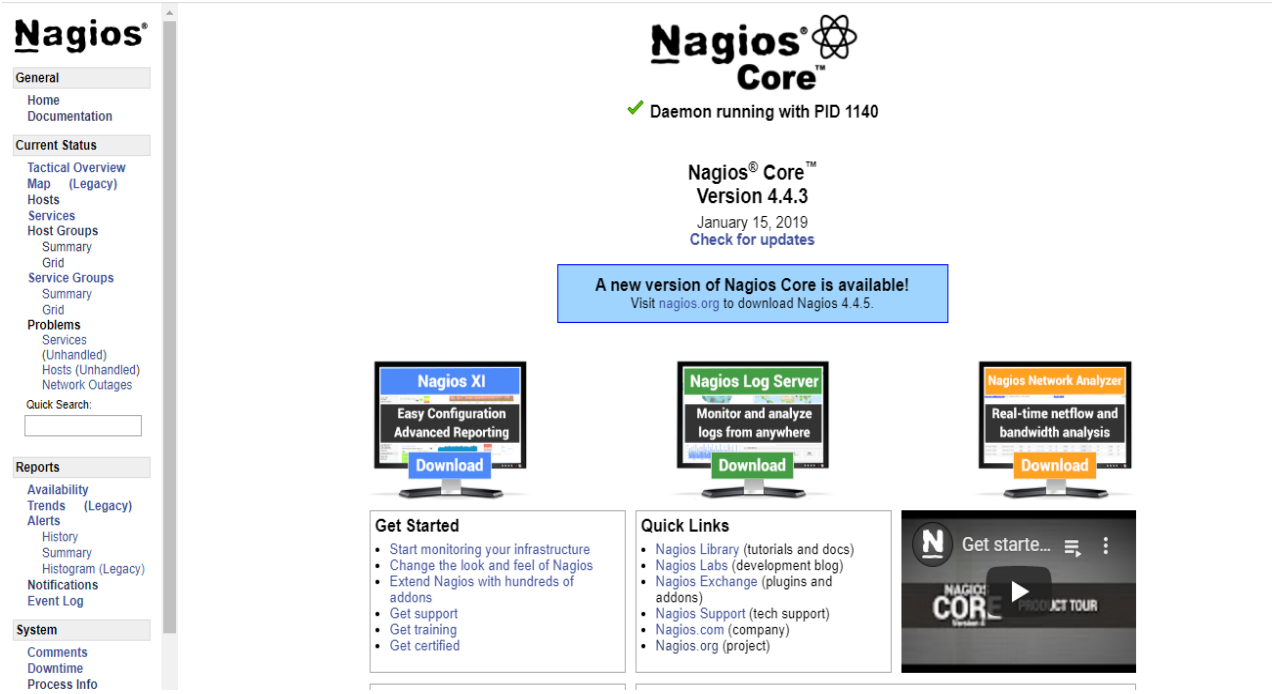


Figura 10. Interfaz web de Nagios
Fuente: Software de gestión Nagios

Instalación de SNMP

Se lleva a cabo la instalación del agente SNMP el cual se encarga de que se pueda realizar la comunicación entre el gestor y los dispositivos gestionados en los cuales posteriormente será instalado.

Dentro del gestor se debe instalar el demonio snmp y snmpd, posteriormente modificar cada uno de esos archivos, finalmente levantar el servicio SNMP en el gestor.

Para los comandos de configuración véase anexo I

Instalación de PNP4Nagios

El componente permitirá realizar gráficas las cuales permitirán realizar un análisis más acertado del monitoreo de los dispositivos gestionados. Se debe descargar el paquete del componente y modificar los archivos de configuración principal, comandos y plantillas. Una vez realizado esto iniciar el servicio de PNP4Nagios.
El proceso detallado de instalación con los respectivos comandos se detalla en el anexo I

Instalación para envío de correos

Para el envío de notificaciones por correo electrónico se ha escogido utilizar el agente de transporte de correo (MTA) postfix por las características antes mencionadas, es necesario seguir una serie de pasos y comandos como se detallan en el anexo I.

Configuración de dispositivos gestionados

Dentro de los dispositivos gestionados es necesario instalar agentes los cuales permitan la comunicación con el gestor para ser monitorizados.

Instalación de SNMP en switches

Se realiza la activación del agente dentro de los switches de dos maneras posibles la primera utilizando comandos que se enlistan dentro del apartado de anexos y la segunda dentro de la interfaz gráfica del switch (Cisco, 2008) siguiendo estos pasos:

a) En la interfaz web del Switch buscar SNMP
b) Seguir al ítem Communities.

c) Ingresar el nombre de la comunidad y dirección IP del servidor Nagios

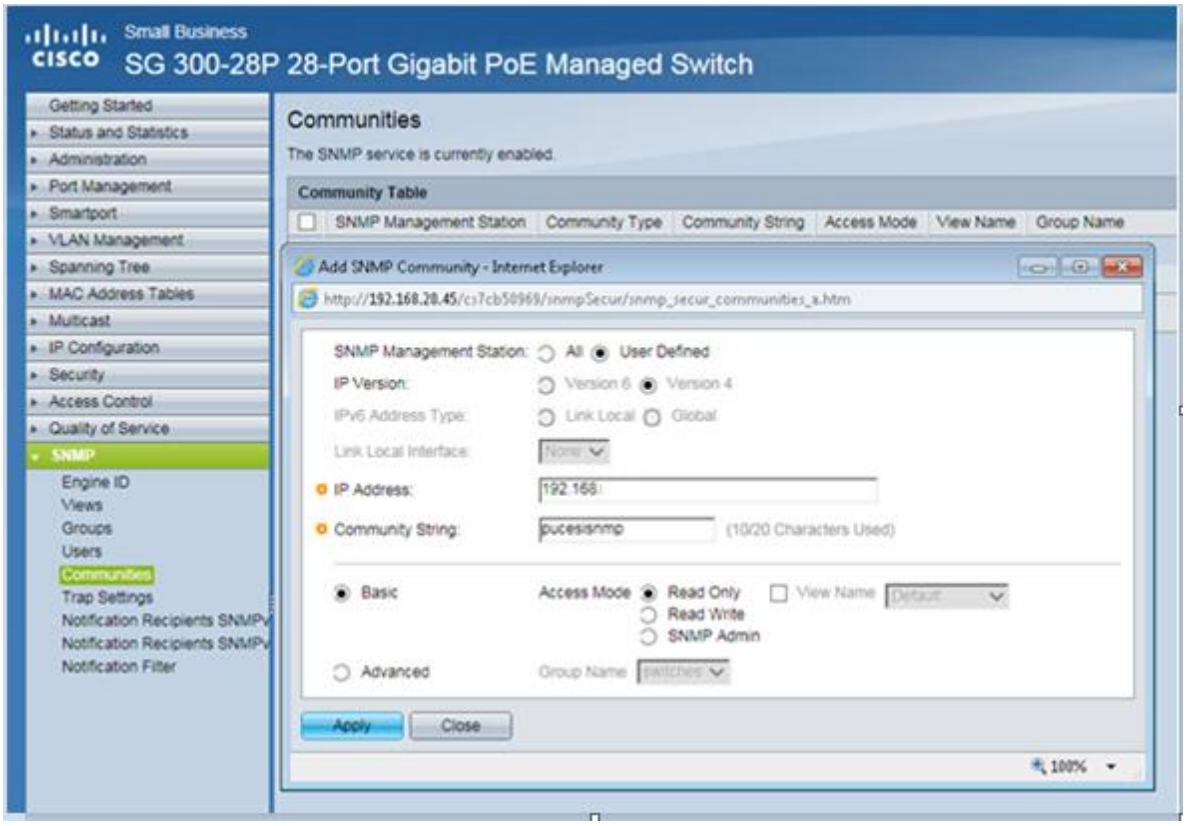


Figura 11. Configuración del agente SNMP en un switch CISCO
Fuente: Interfaz switch Small Business

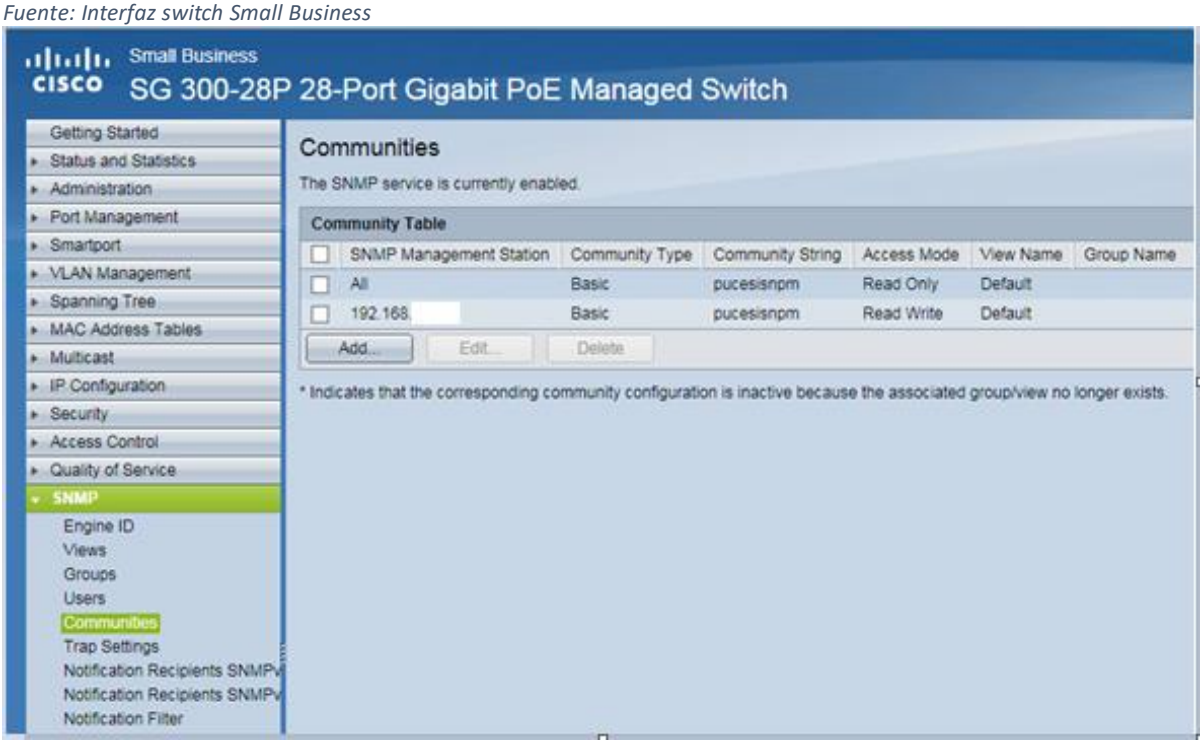


Figura 12. Agente SNMP habilitado en un switch CISCO
Fuente: Interfaz switch Small Business

Instalación de SNMP en Wireless LAN Controller

Los pasos para instalar el agente SNMP dentro de las controladoras es muy similar a los switch los pasos se detallan a continuación:

a) Entrar a la interfaz web de la controladora.

b) Dirigirse al menú SNMP Communities.

c) Cambiar el nombre de la comunidad y a IP del gestor.

d) Activar el agente.

(Cisco, 2008)

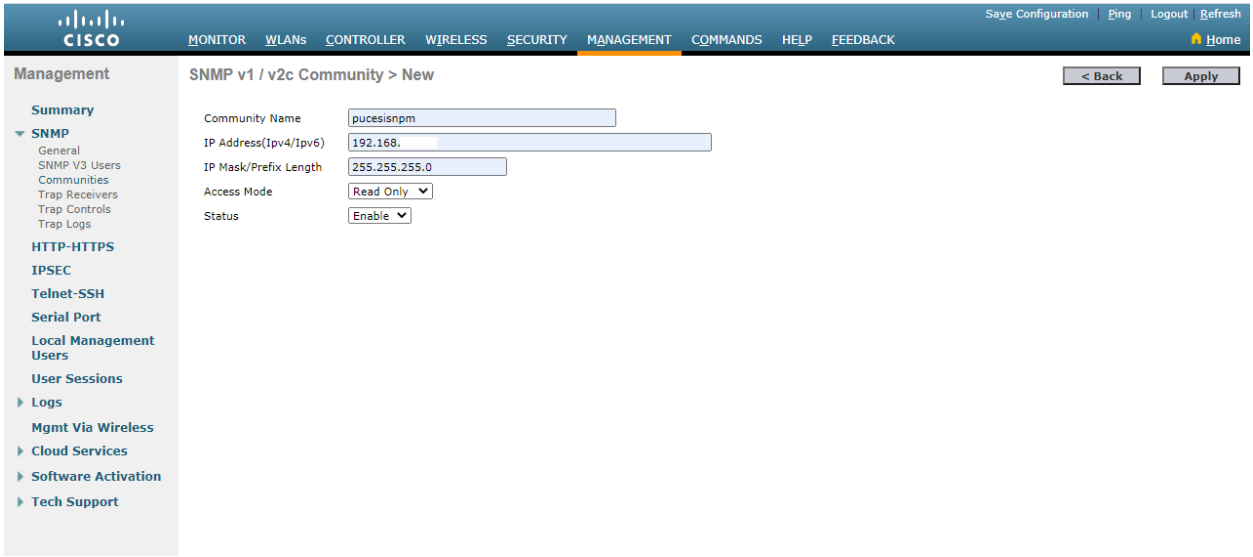


Figura 13. Configuración del agente SNMP en WLC
Fuente: Interfaz WLC Cisco

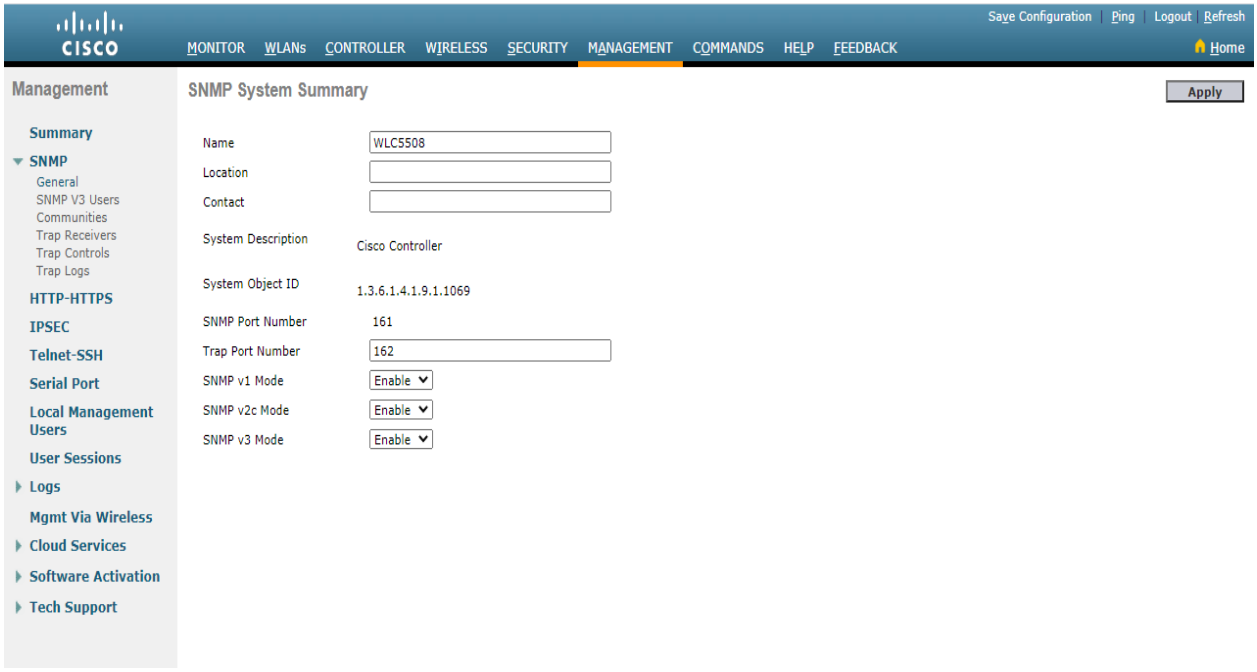


Figura 14. Activación del agente SNMP en WLC
Fuente: Interfaz WLC Cisco

Instalación de NSClient ++ en servidores Windows

Para realizar la instalación de este componente se procede descargar la última versión NSClient ++ para este proyecto se instaló la versión 0.5.2.35, dentro del servidor el cual va a ser monitoreado se instala siguiendo los pasos detallados en el anexo I.

En donde es primordial la colocación de la dirección IP del gestor en este caso la dirección del servidor Nagios, también es importante modificar el archivo "nsclient.ini", el cual se encuentra en la carpeta donde está instalado el agente, la información a modificar se muestra en el anexo I en el apartado de nominado Configuración NSClient++

2.2.1.5. Configuración de dispositivos dentro del gestor.

Con los dispositivos configurados se inicia la configuración dentro del servidor Nagios de cada uno de los mismos.

Configuración de switches dentro de Nagios

Para declarar un nuevo dispositivo en este caso de switches de la capa core, distribución y acceso de la red local de la PUCE-SI se debe ingresar al archivo de configuración se llama "switch.cfg" que se encuentra en la ruta /usr/local/nagios/etc/objects/switch.cfg.
Dentro del cual se seguirá la plantilla que se encuentran en el archivo "templates.cfg" y tiene la siguiente estructura.

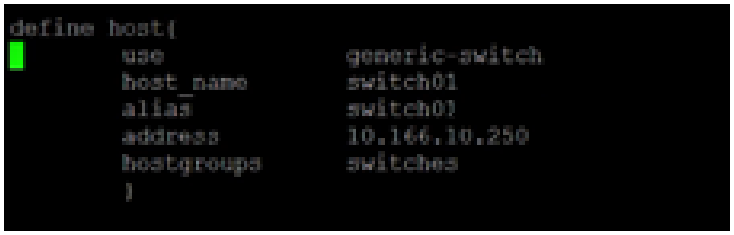


Figura 15. Estructura para declarar un switch dentro de Nagios
Fuente: Software de gestión Nagios

La misma que se detalla a continuación:

use	Indica el tipo de host
host_name	Es el nombre del host que sirve como identificador
alias o display_name	Define el nombre que aparece en la interfaz web
address	Es la dirección IP del host
hostgroups	Nombre del grupo al que pertenece

Tabla 15. Plantilla para la declaración de un host
Fuente: María Fernanda Pinto

Si se desea realizar una especificación de propiedades más detalladas existen opciones que se pueden agregar, tales como:

check_period	Es el periodo en el que está activo el host (Nagios, Assets Nagios, s.f.)
check_interval	Es el intervalo en el que se monitorea al host
retry_interval	Es el intervalo de re comprobación cuando una consulta falla

max_check_attempts	Indica el máximo de intentos que el host realiza después de pasar a estado DOWN

Tabla 16. Propiedades adicionales para la declaración de un switch en Nagios
Fuente: Software de gestión Nagios

Una buena práctica y para una rápida configuración se recomienda crear grupos por el tipo de dispositivo gestionado monitorizado, de esta manera tener una configuración para todo el grupo. Para la creación del grupo de switches utilizamos la siguiente plantilla.

```
define hostgroup {
        hostgroup_name  servidores-weblinux
        alias   Servidores Web Linux
        members SRVweb01
}
```

Figura 16. Estructura para declarar un grupo en Nagios
Fuente: Software de gestión Nagios

hostgroup_name	Define el nombre del grupo
alias	Es el nombre descriptivo que aparece en la interfaz web

Figura 17. Plantilla para la declaración de un grupo en Nagios
Fuente: Software de gestión Nagios

Se procede a definir los servicios que ser van a monitorizar, para este paso se debe seguir igualmente una plantilla con la siguiente información:

```
define service {
        use     generic-service
        hostgroup_name  servicedores-weblinux
        service_description     PING
        check_command   check_ping!100.0,0,20%!500.0,60%
}
```

Figura 18. Estructura para declarar un servicio en Nagios
Fuente: Software de gestión Nagios

use	Indica el tipo de servicio
host_name	Es el nombre de los host o grupo a los que afectará este servicio
service_description	Descripción de la funcionalidad del servicio
check_command	Este es el comando que se ejecutará para el host
check_interval	Es el intervalo entre la ejecución de cada comando
retry_check_interval	Periodo de tiempo entere la ejecución fallida y el siguiente intento.

Tabla 17. Plantilla para la declaración de un servicio en Nagios
Fuente: Software de gestión Nagios

En la figura 18 se puede observar el servicio ping, el cual monitorea la pérdida de paquetes en donde el servicio será CRITICO si es mayor a 500ms o la pérdida es 60%, será PRECAUCIÓN si es mayor a 100ms o la pérdida es de 20%.

Dentro de los servicios que se pueden monitorear para switches se tiene:

check_ping	Monitoreo de pérdida de paquetes.
check_snmp	Monitoreo de la temperatura
check_ifftraffic	Monitoreo de tráfico que cursa por interfaces físicas y virtuales
check_local_disk	Monitoreo de la capacidad del disco
check_load	Monitoreo de la carga del procesador.
check_mem	Monitoreo del uso de memoria RAM
check_http	Monitoreo del estado del servidor web.
check_flash	Monitoreo del uso de memoria Flash
check_fans	Monitoreo de uso de ventiladores

Tabla 18. Servicios a monitorizar de un switch
Fuente: Software de gestión Nagios

Una vez ingresado el nuevo host es importante revisar dentro de la ruta /etc/nagios3/nagios.cfg que el fichero "switch.cfg" no esté comentado, para que de esta manera Nagios pueda leer el mismo al iniciar el servicio. Finalmente, para que los cambios se reflejen es necesario reiniciar el servicio Nagios.

Configuración de servidores dentro de Nagios

Para ingresar un servidor Linux a Nagios es necesario modificar el archivo "servers.cfg" el cual se encuentra en la ruta /usr/local/nagios/etc/objects/servers.cfg.
En el caso si se tratara de un servidor Windows se modifica el archivo "serversWindows,cfg" en la ruta /usr/local/nagios/etc/objects/serversWindows.cfg
Dentro de estos en cualquiera que fuera el caso, se procede a llenar la declaración del servidor como se muestra a continuación especificando cada uno de las propiedades.

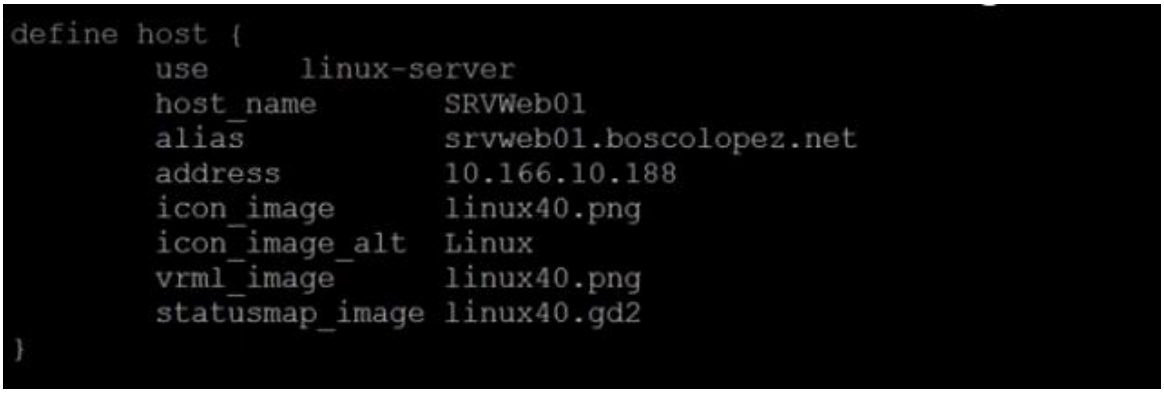


Figura 19. Estructura para declarar un servidor en Nagios
Fuente: Software de gestión Nagios

name	Es el nombre asignado al servidor
use	Indica el tipo de servidor
check_period	Es el periodo de tiempo en el cual se va a monitorear el servidor
check_interval	Es el intervalo de tiempo en cada chequeo
notification_interval	Es el intervalo de tiempo de cada notificación

Tabla 19. Plantilla para declarar un servidor en Nagios
Fuente: Software de gestión Nagios

A continuación, se define los servicios que se desean monitorear. Es importante mencionar que los servicios pueden ser públicos, es decir, servicios ofrecidos por el servidor sin necesidad de acreditarse, como por ejemplo HTTP, FTP, IMAP.

Los servicios privados son de uso interno del equipo como por ejemplo los procesos, el uso de memoria carga de CPU, espacio en disco. Para poder monitorizar estos servicios en Windows es necesario instalar el agente NSClient++ como se indicó en el apartado correspondiente.

check_ping	Monitorea el estado del servidor
check_mem	Monitorea el uso de memoria RAM
check_load	Monitorea el uso de CPU
check_disk	Monitorea el espacio en disco

Tabla 20. Servicios a monitorear para servidores Linux
Fuente: Software de gestión Nagios

check_ping	Monitorea el estado del servidor
check_nt!MEMUSE	Monitorea el uso de memoria RAM
check_nt!CPULOAD	Monitorea el uso de CPU
check_nt!USEDDISKSPACE	Monitorea el espacio en disco

Tabla 21. Servicios a monitorear para servidores Windows
Fuente: Software de gestión Nagios

Finalmente, comprobamos si los archivos de configuración no están comentados en el archivo de configuración principal el cual se encuentra en la ruta /etc/nagios3/nagios.cfg y se reinicia el servicio de Nagios.

2.2.2. Gestión de fallos

La principal meta de la gestión de fallos es buscar la mejor solución en el menor tiempo posible, frente a cualquier incidente. Las fallas dentro de dispositivos gestionados son

detectadas y alertadas por medio de correo electrónico, existen dos situaciones de las cuales se encarga la gestión proactiva o reactiva como se explica a continuación.

2.2.2.1. Gestión proactiva

Establece un fallo antes que suceda para que se efectúe esta gestión es fundamental establecer umbrales para que el administrador pueda visualizarlos en el software, tomar las medidas necesarias antes de que ocurra un fallo y mantener dinámicamente el nivel de servicio de la red.

Esto evitará pasar por alto notificaciones importantes, de esta manera asegurarse de que tipo es la alerta y para que el administrador pueda solucionar de una forma rápida antes que el dispositivo gestionado entre en estado crítico.

Un servidor tiene áreas como CPU, proceso y memoria en las que se puede observar su rendimiento, si se hace excesivo el uso de estos recursos el servidor o aplicación puede ralentizarse. Dichos parámetros poseen un valor límite determinado dentro del cual el dispositivo trabaja sin problemas.

Con respecto al uso del procesador se considera importante no sobrepasar el 75%, ya que esta forma se considera que este mecanismo es un cuello de botella y no permite el funcionamiento correcto de los servidores. (Vega Mateo).

La memoria si se encuentra siendo utilizada en su totalidad ralentizará el tiempo en que se ejecuta las aplicaciones solicitadas, para este caso el umbral que se sugiere sostener es no sobre pasar el 70% de memoria dentro del servidor. Para el caso de la capacidad del disco el 25% libre es lo ideal. (Microsoft, s.f.)

Los porcentajes de umbrales han sido definidos de acuerdo a la experiencia del administrador de la red de la PUCE – SI.

Dispositivos	Métrica	Umbrales de Advertencia	Umbrales de Criticidad
Switches	Carga de CPU	70%	80%
	Memoria	30% libre	20% libre
Servidores	Carga de CPU	60%	75%
	Memoria	30% libre	20% libre
	Disco	25% libre	15% libre

Tabla 22. Umbrales según el dispositivo
Fuente: María Fernanda Pinto

Dentro de los servicios a monitorear se organizó dentro de la jerarquía.

Servicios	Criticidad
Ping	Alta
DHCP	Alta
DNS	Alta
Uso de memoria	Media
Uso de CPU	Alta
Espacio en disco	Baja

Tabla 23. Jerarquía de criticidad según el servicio
Fuente: María Fernanda Pinto

Dentro de los dispositivos gestionados se midió la criticidad de cada uno.

Dispositivo	Criticidad
Switch en capa CORE	Alta
Switch en capa de distribución	Media
Switch en capa de acceso	Baja
Servidores físicos	Alta
Servidores virtuales	Alta

Tabla 24. Jerarquía de criticidad según los dispositivos
Fuente: María Fernanda Pinto

2.2.2.2. Gestión de pruebas preventivas

En primera instancia se realiza pruebas de conectividad física las cuales comprueban el funcionamiento de cada dispositivo como cables de red, tarjetas, fuentes de poder.

Es importante también realizar pruebas de conectividad lógica con los comandos “ping” y “traceroute” en los servidores y switches.

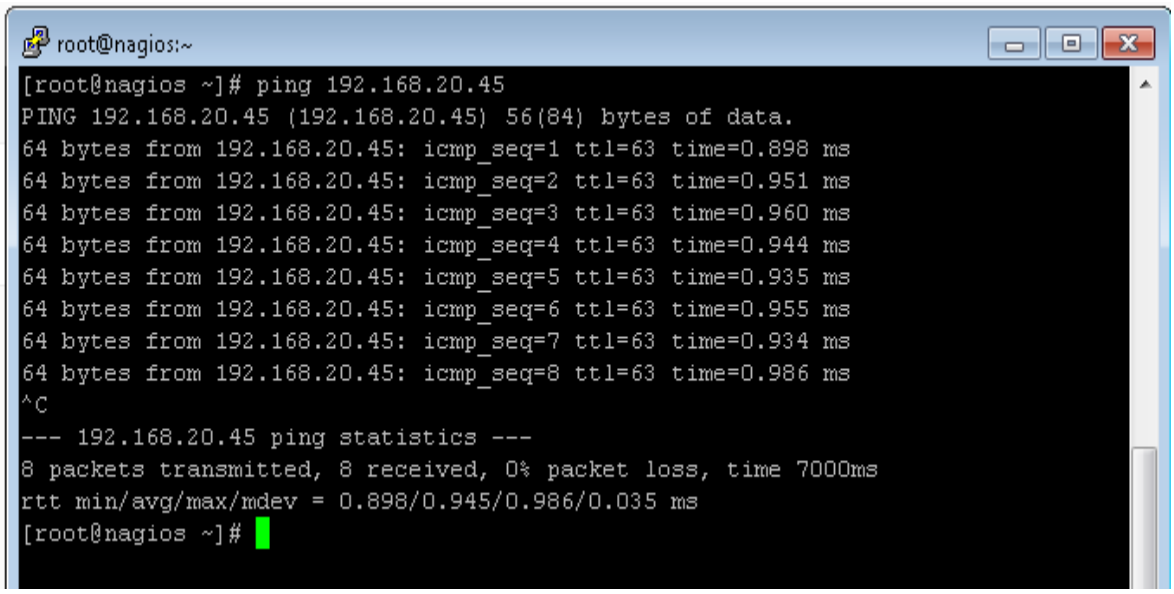


Figura 20. Ejecución del comando “ping” en un switch de acceso
Fuente: Servidor Nagios

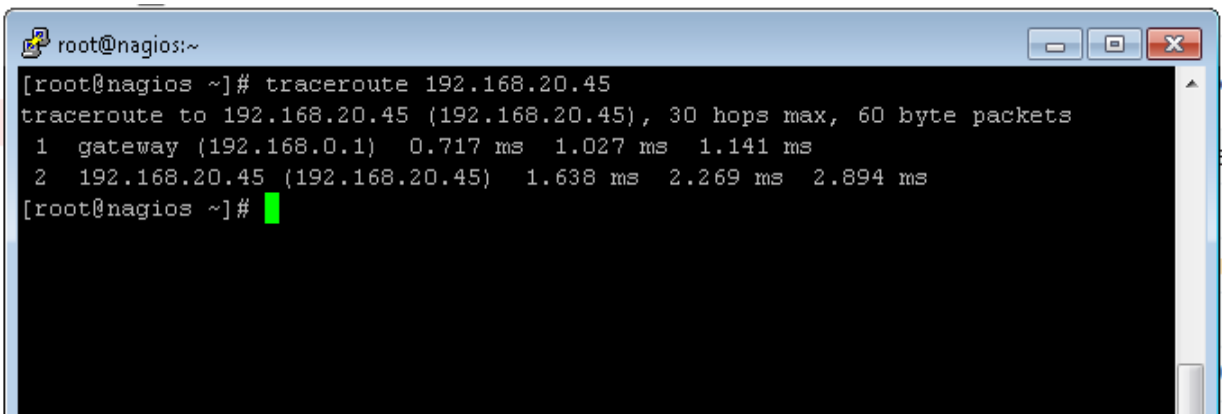


Figura 21. Ejecución del comando “traceroute” en un switch de acceso
Fuente: Servidor Nagios

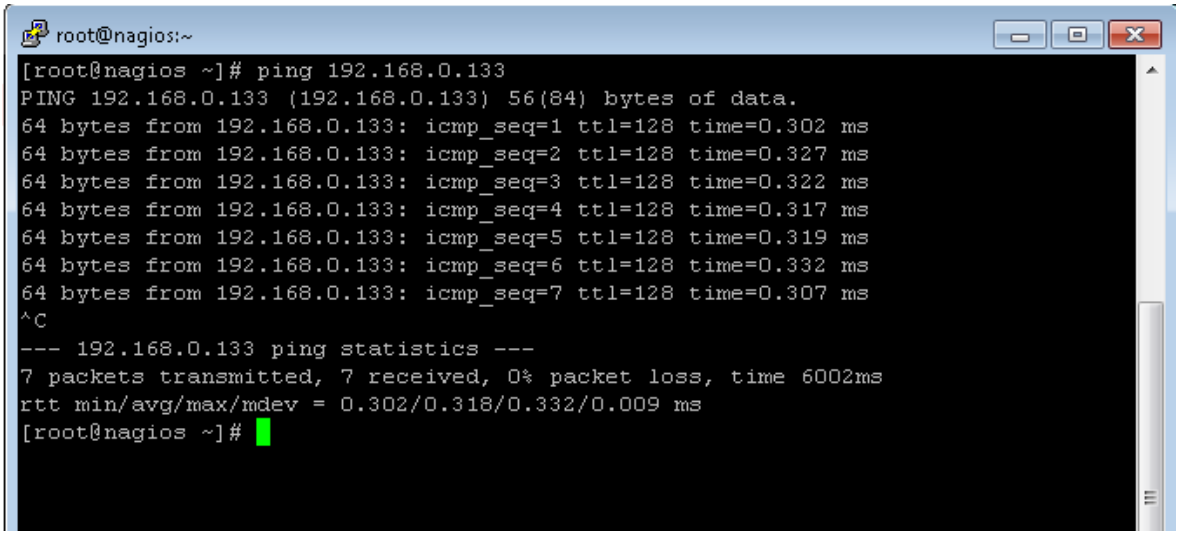


Figura 22. Ejecución del comando "ping" en un servidor
Fuente: Servidor Nagios

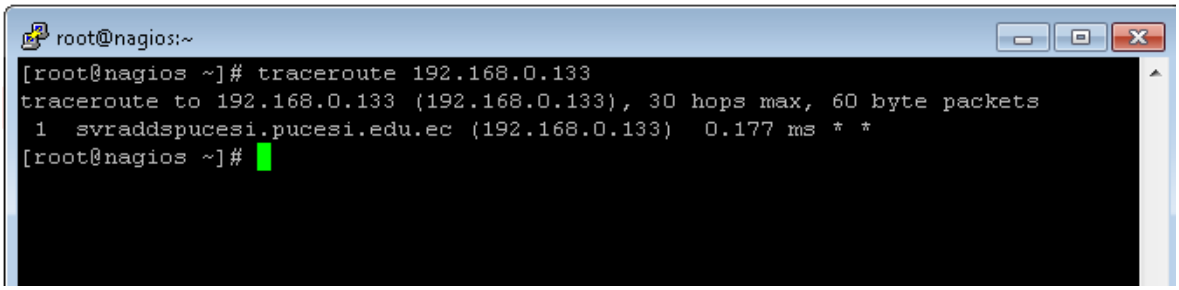


Figura 23. Ejecución del comando "traceroute" en un servidor
Fuente: Servidor Nagios

2.2.2.3. Gestión Reactiva.

Esta gestión se aplica inmediatamente haya ocurrido el fallo en los dispositivos. Para resolver el inconveniente se recure a un proceso en el cual se detecta el fallo con el objetivo de diagnosticar y resolver el problema ocurrido.

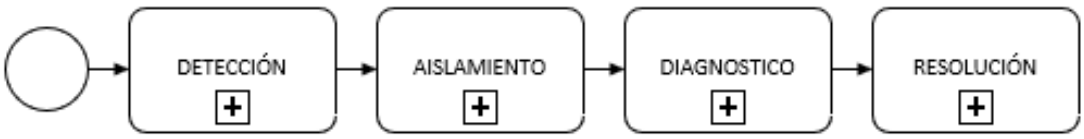


Figura 24. Ciclo de vida de incidencias
Fuente: Modelo de gestión FCAPS

Detección

Las notificaciones enviadas desde el software de gestión Nagios al contacto especificado es decir el administrador de la red sirven para detectar el problema, el lugar en el que sucedió, en el servicio o dispositivo. Así también dentro de la interfaz web el administrador puede observar cambios en los dispositivos mediante el mapa que se refleja en la misma.

En la figura 25 se muestra una notificación enviada desde Nagios a la cuenta del administrador donde se informa un problema de falta de espacio para el Servidor de aplicaciones del área de laboratorio de la PUCE -SI.

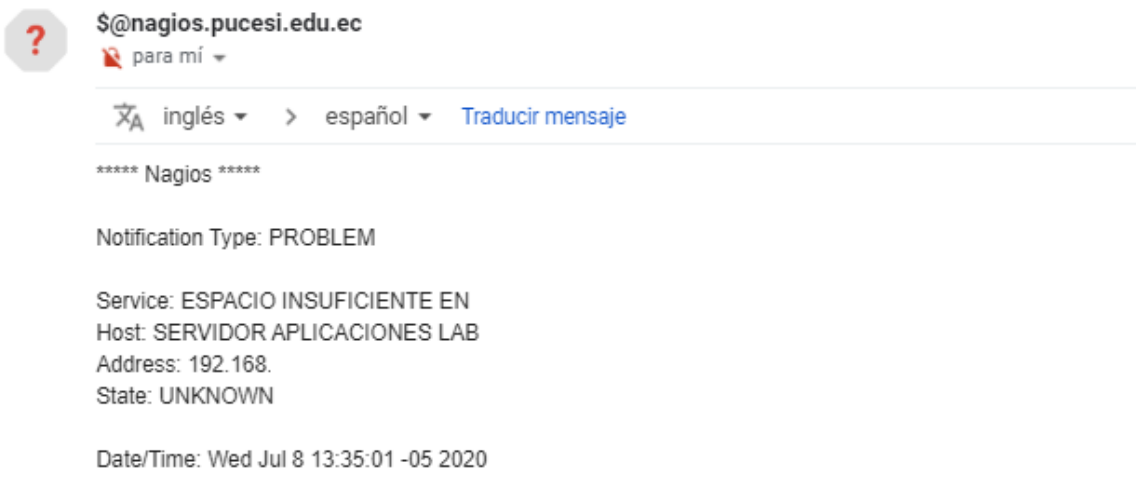


Figura 25. Correo electrónico informando un fallo
Fuente: Extraída de la cuenta de correo del Administrador

Aislar

El software de gestión posibilita el aislamiento de una falla mediante la jerarquía de alertas en base a los elementos de la red (equipos y servicios), con el fin de evitar alertas innecesarias y poder agrupar las mismas.

RECUPERADO	ADVERTENCIA	CRÍTICO	DESCONOCIDO	PENDIENTE

Tabla 25. Jerarquía de alertas de Nagios
Fuente: Software de gestión Nagios

Cuando un dispositivo gestionado o un servicio está en el estado recuperado (recovery) en la comprobación realizada después de un tiempo determinado dentro de la configuración.

Figura 26. Representación del estado recuperado
Fuente: Software de gestión Nagios

Si se detectó problemas en la última comprobación del dispositivo gestionado o de un servicio, se interpreta que el mismo se encuentra en advertencia (warning) que es un paso antes de volverse crítico.

Figura 27. Representación del estado advertencia
Fuente: Software de gestión Nagios

Si un dispositivo o servicio se encuentra abajo (down) o inalcanzable (unreacheable) y si sobrepasa los umbrales establecidos para su funcionamiento normal en la última comprobación de estado, dicho dispositivo o servicio se ubica en estado crítico (critical).

Figura 28. Representación del estado crítico
Fuente: Software de gestión Nagios

Cuando un servicio o dispositivo no está bien definido presenta un estado desconocido (unknown)

Figura 29. Representación del estado desconocido
Fuente: Software de gestión de Nagios

Si una nueva configuración está siendo reconocida por Nagios el estado es pendiente (pending)

Figura 30. Representación del estado pendiente
Fuente: Software de gestión Nagios

Diagnosticar

Una vez detectado y aislado el origen del fallo se procede a realizar un diagnóstico las posibles y más comunes causas son:

- Se ha perdido la conectividad lógica, es decir no existe comunicación entre el gestor y dispositivos gestionados.
- Se ha perdido la conectividad física, es decir existen cables rotos o tarjetas de red dañadas.
- No existe respuesta SNMP de los dispositivos gestionados.
- Problemas con el tráfico de la red.

Nagios provee una ventaja en esta etapa de la gestión reactiva, si se da click en el dispositivo detectado el software diagnostica un fallo crítico si se extralimita los umbrales normales.

Resolución

En base a la experiencia los mecanismos por los que se opta para la resolución de fallos son:

- Verificación de la configuración
- Reinicio de dispositivos o servicios.
- Cambios de versión de software.
- Sustituir los recursos dañados en casos extremo de daños.

2.2.3. Gestión de la Contabilidad

Dentro de esta fase se establece parámetros con los cuales se va a realizar la evaluación.

2.2.3.1. Parámetros de monitoreo

A continuación, se define los parámetros de monitoreo según el dispositivo.

Dispositivos	Parámetros	
Switch Cisco	Estado	Si se encuentra encendido
	Tiempo de encendido	El tiempo q ha estado encendido
3 Com	Estado	Si se encuentra encendido
	Tiempo de encendido	El tiempo q ha estado encendido
HP	Estado	Si se encuentra encendido
	Tiempo de encendido	El tiempo q ha estado encendido
Servidores Físicos	Estado	Si se encuentra encendido
	Procesador	Uso de CPU
	Memoria	Cantidad de memoria
	Espacio en Disco	Capacidad utilizada

Tabla 26. Parámetros de monitoreo
Fuente: Basado en el inventario de dispositivos de la PUCE -SI

2.2.3.2. Parámetros de estado.

Para los dispositivos los parámetros son los siguientes:

Estado	Letra	Descripción
down	d	El dispositivo esta abajo
unreachable	u	El dispositivo no es visible
recobery	r	El dispositivo se recuperó
flapping	f	Estado indeterminado
none	n	No se envían notificaciones

Tabla 27. Parámetros de estado para dispositivos
Fuente: Software de gestión Nagios

Mientras que para los servicios:

Estado	Letra	Descripción
warning	w	Sobre paso de umbrales de advertencia
critical	c	Sobre paso de umbrales de normalidad
recobery	r	Servicio recuperado

flapping	f	Servicio en estado indeterminado
none	n	No enviar notificaciones

Tabla 28. Parámetros de estado para servicios
Fuente: Software de gestión Nagios

2.2.3.3. Parámetros de chequeo

Dentro de Nagios es posible limitar un tiempo para el chequeo definido por días y horas específicas. Para el desarrollo de este proyecto se ha decidido tener el parámetro 24 x 7 esto significa que los dispositivos y servicios serán monitoreados durante las 24 horas los 7 días de la semana.

CAPÍTULO III
RESULTADOS Y DISCUSIÓN

En este apartado se realiza un análisis de los resultados obtenidos durante la puesta en marcha del modelo de gestión FCAPS. La información recolectada es analizada con herramientas propias del software de gestión Nagios el cual arroja reportes y se ha decidido agruparlo de acuerdo al modelo jerárquico de la red es decir por capas.

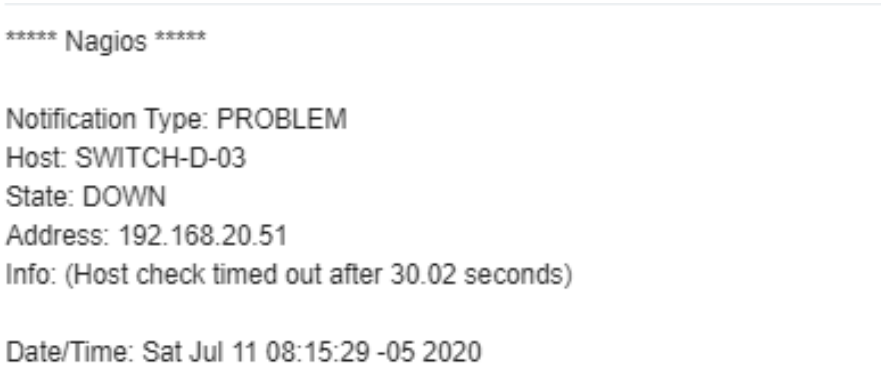
Una vez realizado el análisis y de acuerdo al mismo se ha concluido con la última fase del modelo de gestión el cual implica crear nuevas políticas para el manejo de incidentes dentro del área de redes de la PUCE-SI. Finalmente, se procede a realizar manuales de procedimiento para cada área funcional como guía de uso técnico para el administrador.

1.1. Pruebas de funcionamiento

Estas prueban realizan la verificación del funcionamiento de cada una de las áreas del modelo de gestión FCAPS.

1.1.1. Prueba para el área de Gestión de Fallos.

Para que esta área se encuentre funcionando de forma adecuada la manera de comprobarlo es el envío de notificaciones a través de correo electrónico indicando en que dispositivo gestionado a ocurrido el fallo, como se muestra en la figura 37


***** Nagios *****

Notification Type: PROBLEM
Host: SWITCH-D-03
State: DOWN
Address: 192.168.20.51
Info: (Host check timed out after 30.02 seconds)

Date/Time: Sat Jul 11 08:15:29 -05 2020

Figura 31.Correo electrónico de alerta por la caída de un switch
Fuente: Extraída de la cuenta electrónica del administrador

Figura 32. Correo electrónico indicando el cambio de estado de un switch
Fuente: Extraída de la cuenta de correo del Administrador

1.1.2. Prueba para el área de gestión de la contabilidad

Para realizar estas pruebas de rendimiento se ha tomado los reportes que se muestran en la sección 3.4 referente a los reportes los cuales se muestran el historial de dispositivos y servicios monitoreados por el software de gestión Nagios con los parámetros de monitoreo anteriormente configurados.

1.1.3. Pruebas para el área de gestión de la configuración

Para comprobar la funcionalidad correcta de esta área, no es necesario aplicar una prueba específica ya que estuvo presente en las pruebas de cada gestión anteriormente explicadas y proporciona la base que para que funcionen correctamente, es decir que sin una configuración correcta las demás áreas no habrían pasado dichas pruebas de manera satisfactoria.

1.2. Políticas de Monitoreo

Una vez implementado el modelo de gestión para la red de datos de la PUCE sede Ibarra se determina las políticas de monitoreo que velen el cumplimiento de cada una de las áreas funcionales del modelo FCAPS. Estas políticas son elaboradas en base al formato establecido por la Unidad de Sistemas que se encuentra en detalle en el anexo II.

1.3. Manuales de Procedimientos

Los manuales de procedimiento para las áreas de gestión son una guía que posibilita al administrador reaccionar ante los fallos que pueden ocasionarse en dispositivos gestionados o servicios de la red de la PUCE -SI los cuales fueron elaborados y estructurados bajo el formato que provee la Unidad de Sistemas.

Dentro de los cuales se describen los procesos que se siguen dentro de cada área del modelo de gestión FCAPS detallando la configuración de equipos, prevención de fallos, gestión de fallos ya suscitados. De esta manera garantizar el cumplimiento correcto del modelo de gestión implementado. Los manuales de los que se hablan en esta sección se encuentran en el anexo III.

1.4. Reportes

Nagios posee un módulo dedicado a generar reportes históricos de un dispositivo gestionado y servicios. A continuación, se los describen.

1.4.1. Disponibilidad

En esta sección "Availability" se muestran las fallas y estado de los dispositivos gestionados y de cada servicio monitoreado, como se muestra en la siguiente figura

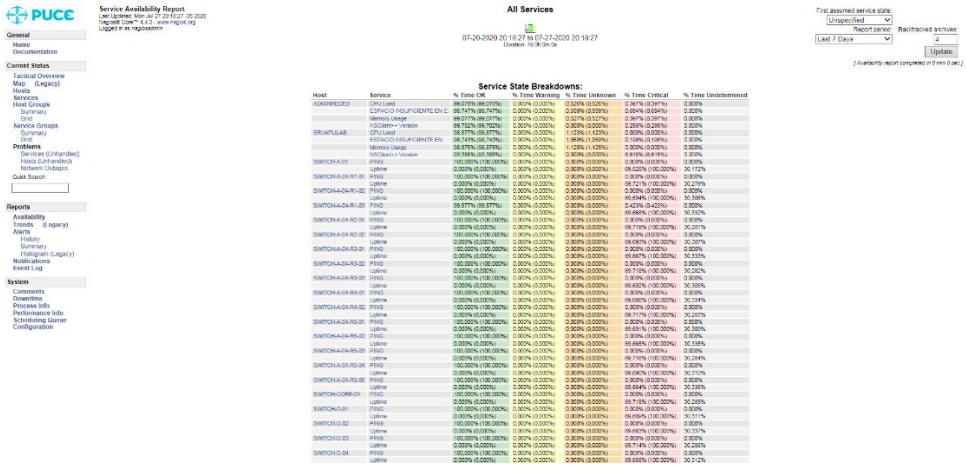


Figura 33. Reporte de disponibilidad por servicio
Fuente: Software de gestión Nagios

La figura 33 muestra el reporte de disponibilidad por servicio durante los últimos 7 días, es decir los porcentajes de tiempo que los servicios se han mantenido en un estado específico.

Ejemplo el switch A-04-R1-03 se encontró en un estado “OK” en el 99.577% de estos 7 días mientras que en un 0.423% del tiempo se encontró en estado crítico “CRITICAL” ya que en esos días hubo una caída de energía en el edificio 4 de la PUCE -SI.

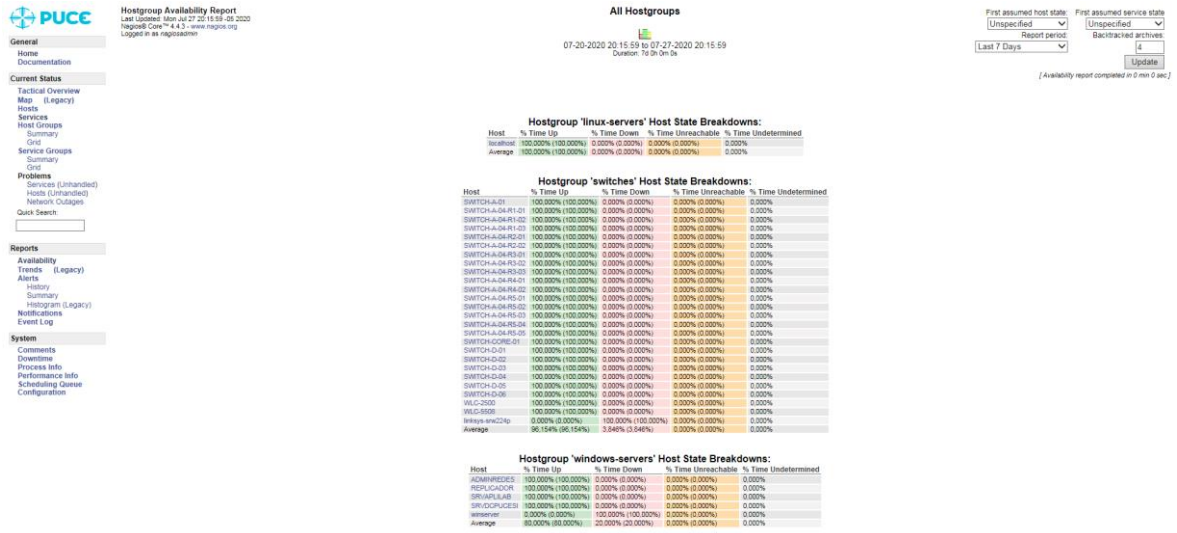


Figura 34. Reporte de disponibilidad por host
Fuente: Software de gestión Nagios

La figura anterior muestra el reporte de disponibilidad de acuerdo a los grupos de host, aquí se puede observar que cada grupo se ha mantenido disponible durante los 7 días de parámetro para este reporte.

1.4.2. Tendencia

Dentro de este reporte en inglés llamado “Trends” se muestra el estado del dispositivo gestionado a medida que ha transcurrido el tiempo, pudiendo ver en qué momento ha cambiado de estado.

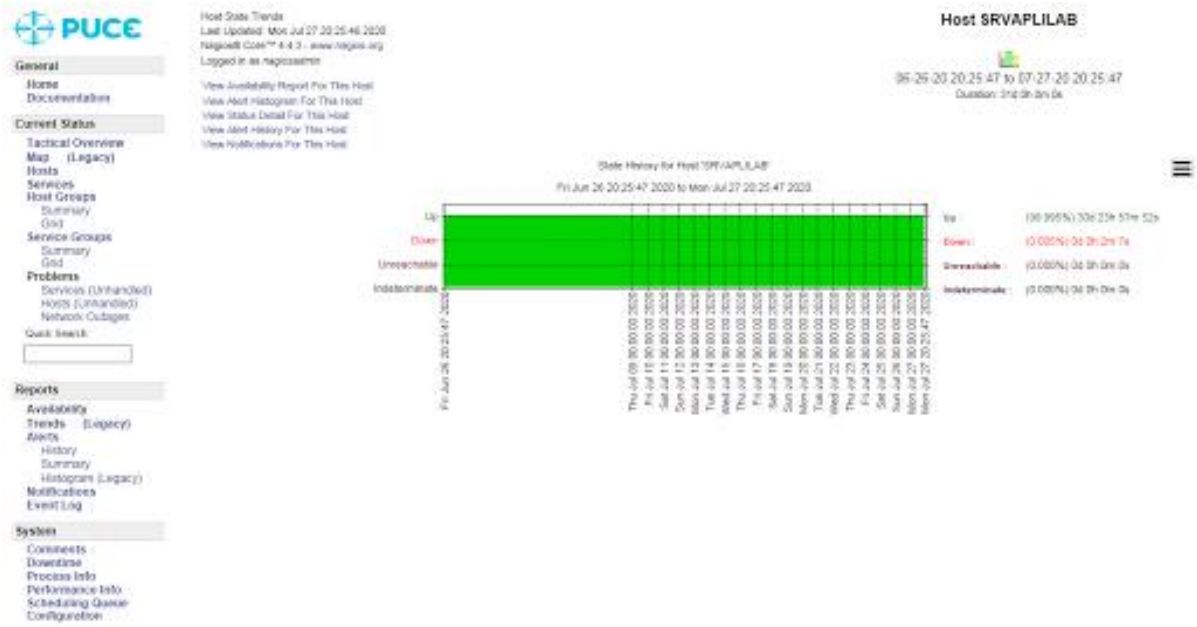


Figura 35. Reporte de Tendencia de un host
Fuente: Software de gestión Nagios

El reporte de tendencia mostrado en la figura 35 indica que el host llamado SRVAPLILAB se encontró disponible durante los últimos 31 días sin haber ninguna falla en la conectividad del gestor con dicho host.

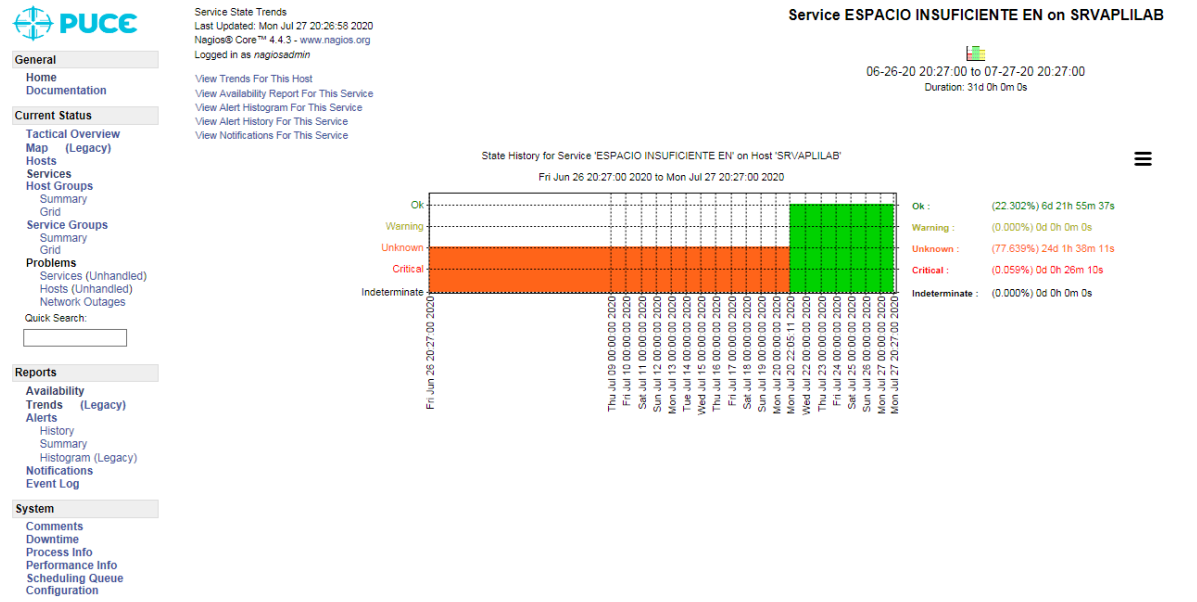


Figura 36. Reporte de tendencia de un servicio
Fuente: Software de gestión Nagios

En la figura 36 se muestra el reporte de tendencia de un servidor Windows destinado a las aplicaciones que se manejan dentro del Laboratorio de la Unidad de Sistemas, en el cual se puede observar que durante 24 días el estado del servicio de espacio en disco envió alertas, mientras que después de haber reparado la falla el estado cambió a "Ok", lo cual significa que el estado del espacio en disco volvió a estar dentro de los umbrales establecidos para un buen funcionamiento.

1.4.3. Alertas

Son creadas cuando un dispositivo o servicio cambia de estado. Dentro de este apartado llamado en inglés "Alerts" se puede observar el reporte de alertas de un día determinado.

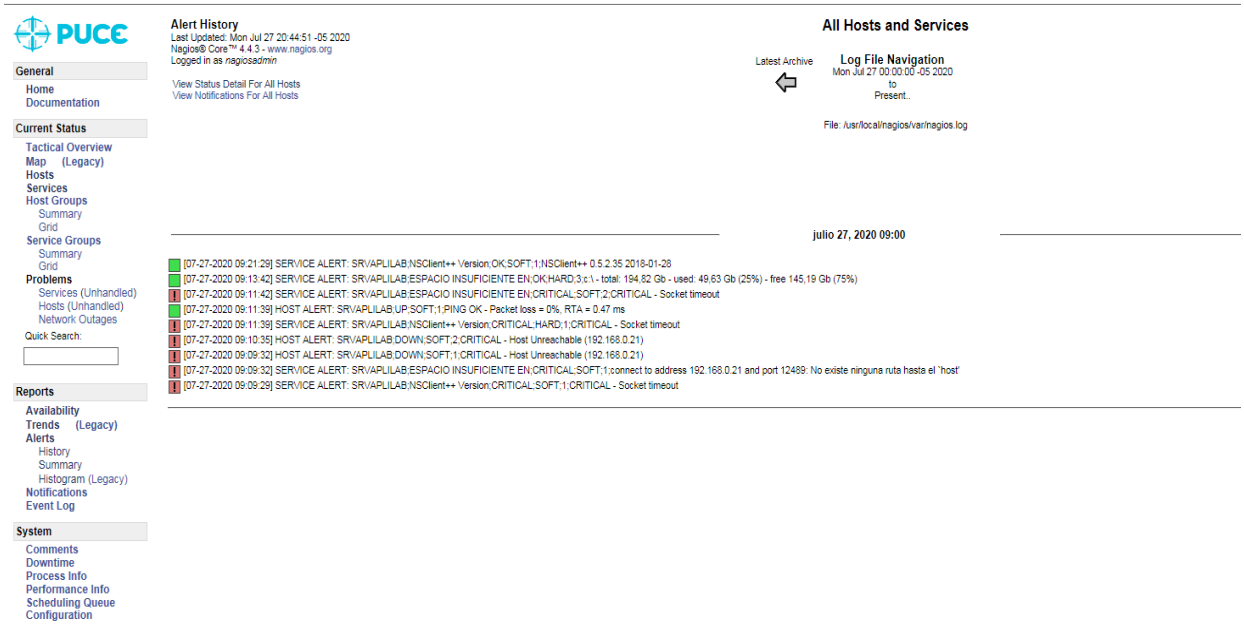


Figura 37. Reporte de alertas
Fuente: Software de Gestión Nagios

1.4.3.1. Historial

Genera una lista con todas las alertas generadas por dispositivos y servicios en intervalos de horas.

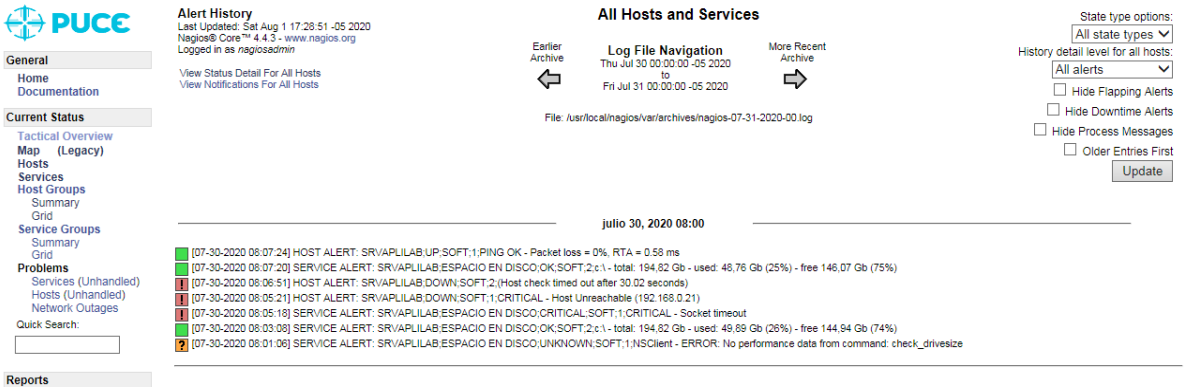


Figura 38. Historial de alertas
Fuente. Software de gestión Nagios

1.4.3.2. Resumen

Crea resultados en forma de tabla con criterios previamente ingresados en un formulario como se muestra a continuación:

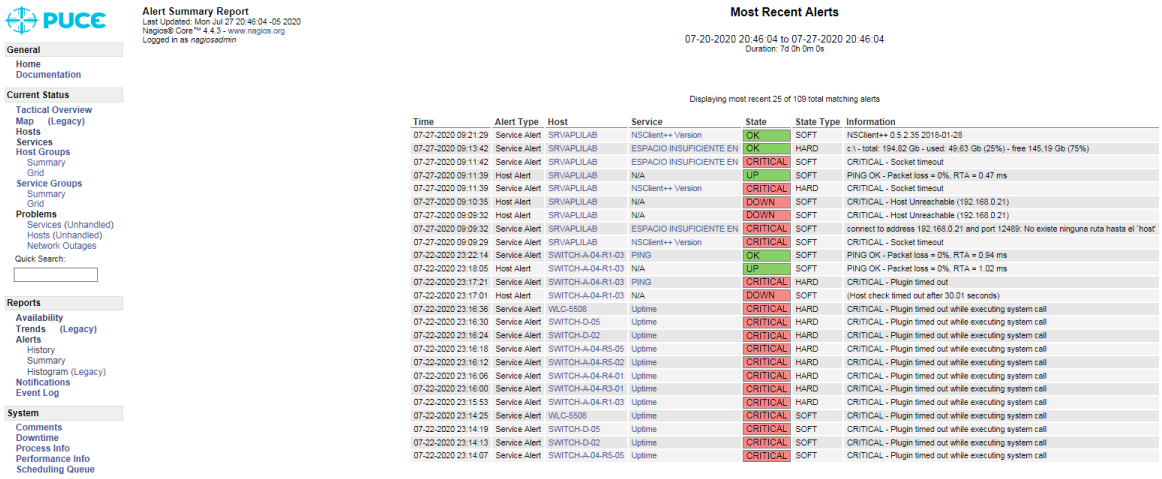


Figura 39. Reporte de resumen de alertas recientes
Fuente: Software de gestión Nagios

El reporte mostrado en la figura 44 resumen las alertas durante 7 días, con los parámetros como:

Tiempo: Se refiere al día y a la hora exacta en la cual se suscitó la alerta.

Tipo de alerta: Si se trata de un host o un servicio

Host: El nombre del host afectado.

Servicio: Si la falla proviene de un servicio, si no se mostrará N/A

Estado: Indicando dentro de los umbrales propios de Nagios en qué estado se encuentra la falla.

Tipo de Estado: Si la alerta se refiere a hardware o software

Información: Se detalla aún mas de donde proviene el fallo

1.4.3.3. Histograma

Cumple la función de mostrar gráficos por dispositivo o servicio durante un periodo de tiempo de las alertas se ha generado.

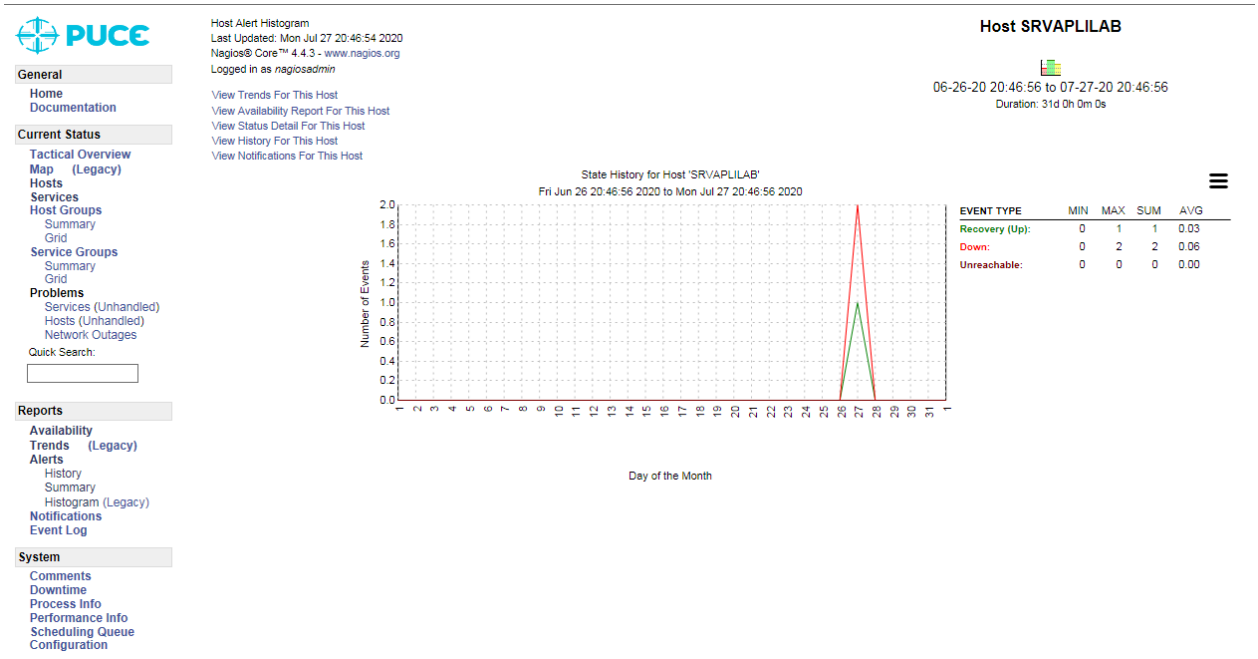


Figura 40. Reporte en Histograma de un host
Fuente: Software de gestión Nagios

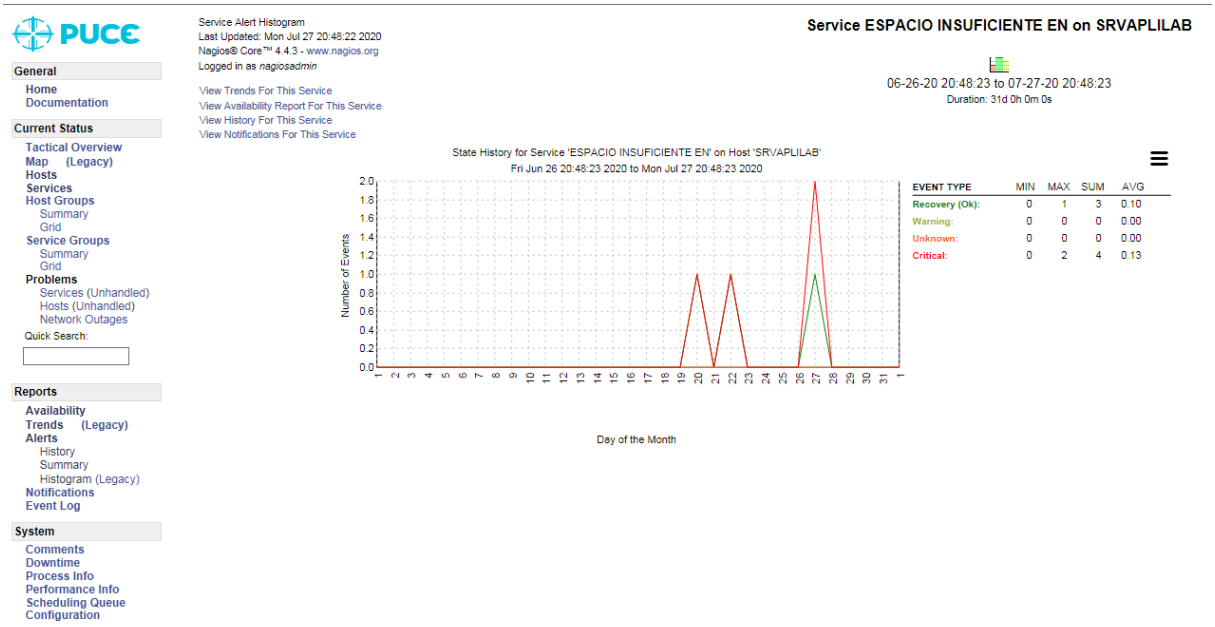


Figura 41. Reporte en Histograma de un servicio
Fuente: Software de gestión Nagios

1.4.4. Notificaciones

Se genera un reporte que muestra la información y la fecha en la que se enviaron las notificaciones.

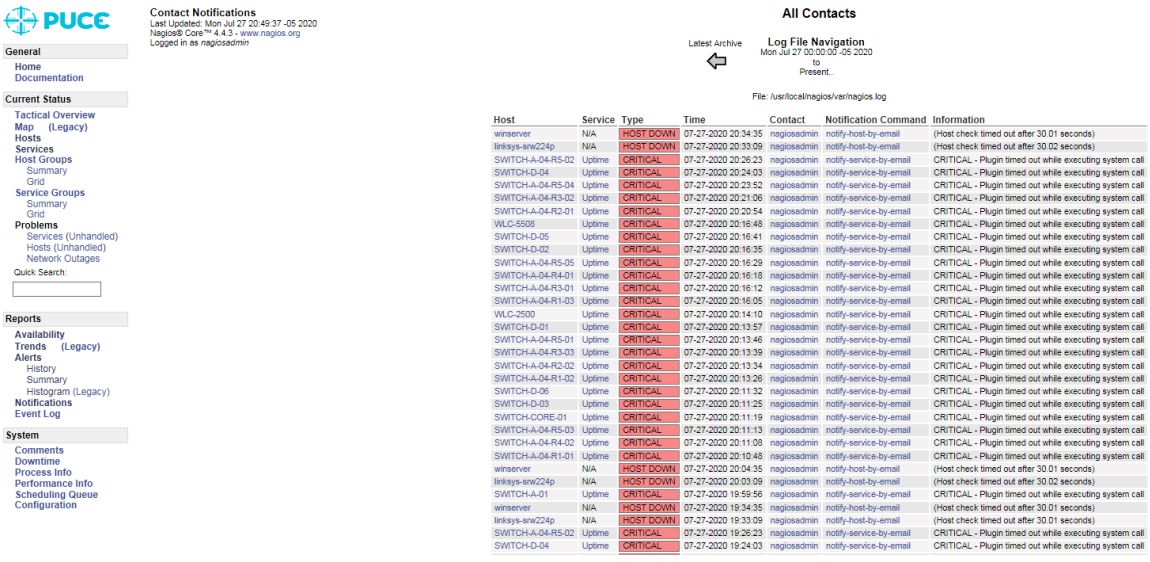


Figura 42. Reporte de notificaciones
Fuente: Software de gestión Nagios

1.4.5. Registro de eventos

También conocido como logs, en donde se presenta la actividad general dentro del software de gestión Nagios

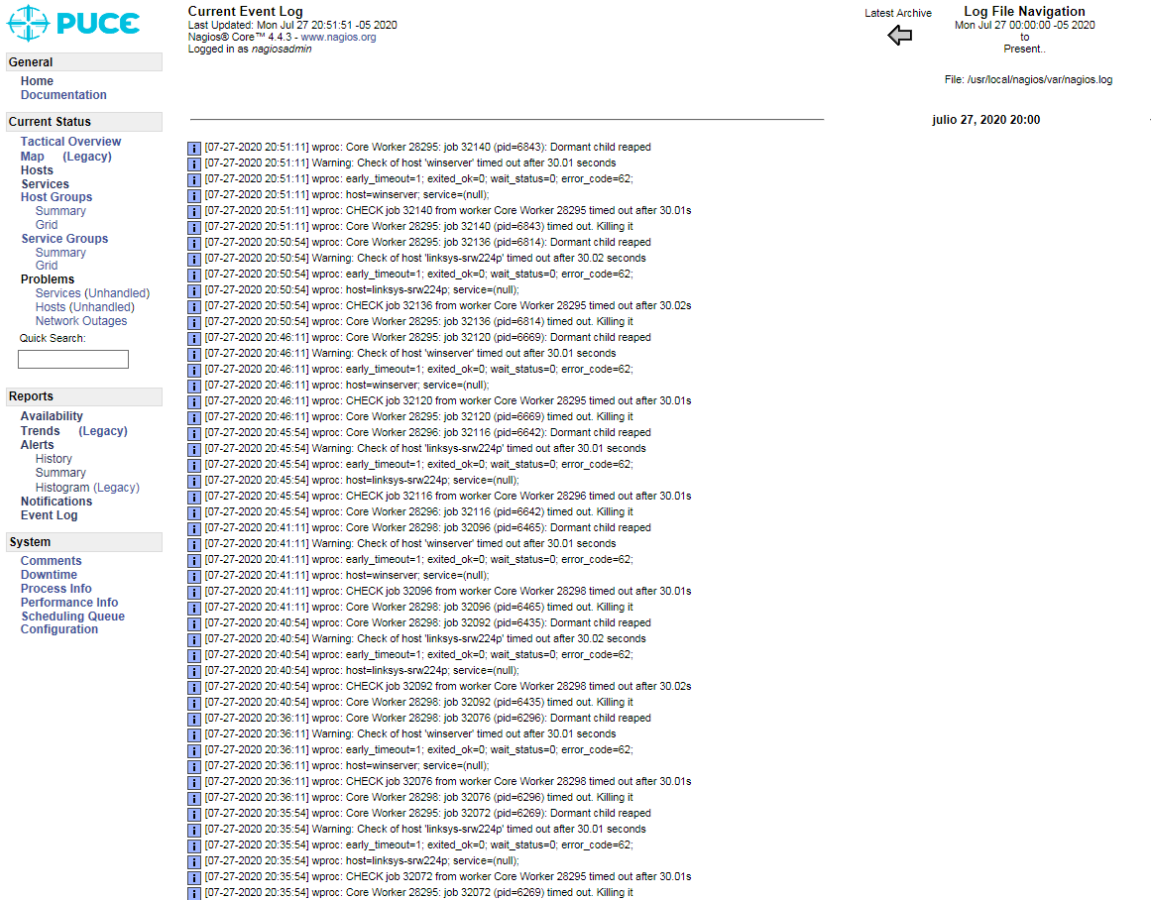


Figura 43. Reporte de logs
Fuente: Software de gestión Nagios

CONCLUSIONES

El desarrollo del proyecto denominado “Implementación de un sistema de monitoreo y modelo de gestión de la red de datos de la PUCE – SI basada en herramientas open source” presenta las siguientes conclusiones, considerando los objetivos planteados y el alcance de la investigación:

Un paso determinante para la puesta en marcha del proyecto fue la investigación y elección del modelo de gestión para la red y el software como herramienta de monitoreo el cual se eligió en a la información recopilada. Optando por el modelo de gestión FCAPS respaldado por la ISO y Nagios como gestor del monitoreo así cumpliendo el uso de software libre para el proyecto.

Gracias al análisis obtenido de la situación actual de la red se permitió determinar una jerarquía de criticidad para los equipos y servicios de TI, así como también una nueva nomenclatura para cada componente de la red, de esta manera permitir que el administrador de la red conozca la ubicación y funcionalidad del mismo.

Basado en necesidades y requerimientos técnicos de la Unidad de Sistemas de la PUCE -SI el presente trabajo se delimitó a desarrollar únicamente tres fases del modelo de gestión FCAPS cubriendo así los requerimientos exigidos.

Disponer de un sistema de alarmas mediante correo electrónico faculta al administrador conocer el estado del fallo ocurrido, el equipo y lugar donde se encuentra. Logrando así optimizar el tiempo de respuesta y resolución a cualquier problema que se haya suscitado dentro de la red y sus dispositivos.

Para el cumplimiento de cada proceso del modelo de gestión se ha elaborado una política y documentación que determina los lineamientos y actividades que el personal técnico debe cumplir, de esta forma la red y dispositivos gestionados de la institución estén monitoreados para garantizar la disponibilidad de servicios y recursos.

RECOMENDACIONES

Conforme al desarrollo e implementación, tanto como los resultados obtenidos se ha decidido realizar las siguientes recomendaciones:

Una vez realizado el análisis de la situación actual de la red se recomienda a la Unidad de Sistemas mejorar la topología en cuanto a una mejor aplicación del modelo jerárquico, esto ayudará al administrador a optimizar y llevar a cabo funciones específicas dentro de una capa.

Es recomendable aumentar el monitoreo de otros servicios para los dispositivos gestionados ya que el proyecto brinda la posibilidad de que se agregue nuevos servicios a ser monitoreados con sus parámetros dentro del gestor, de esta manera se podrá mejorar el control de la red.

Se recomienda que al ingresar un nuevo dispositivo para la red se siga el manual de procesos para cada área de gestión, de esta manera se estará cumpliendo con los lineamientos propuestos del modelo de gestión FCAPS de la ISO y la política monitoreo aprobada para la Unidad de Sistemas de la PUCE – SI.

Para el ingreso de los servidores de alta criticidad en el gestor, se recomienda realizar un plan de instalación con el administrador de dicho servidor, teniendo en cuenta los potenciales fallos y un plan de contingencia para actuar ante un posible error o problema, en consecuencia, evitando la perdida de disponibilidad de los servicios de TI de la Universidad.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez García, N. (s.f.). *Monitorización de red de sensores para Autoridad Portuaria de Gijón.* Barcelona: Universidad Abierta de Cataluña.

Artica Soluciones Tecnológicas. (Mayo de 2014). *Pandora FMS.* Obtenido de https://pandorafms.com/downloads/funcionalidades_DEF_ES.pdf

Badger, M. (2011). *Zenoss Core 3.x Network and System Monitoring.* Birmingham: Packt Publishing .

Báez Cheza, J. E. (2017). *Diseño e implementación de un modelo de gestión de red para la red de área local del edificio central de la Universidad Técnica del Norte en base al modelo de gestión OSI con el protocolo SNMP.*

Báez Cheza, J. E. (2017). *Diseño e implementación de un modelo de gestión de red para la red de área local del edificio central de la Universidad Técnica del Norte en base al modelo de gestión OSI con el protocolo SNMP.* Ibarra: Universidad Técnica del Norte.

Barth, W. (2008). *Nagios, 2nd Edition: System and Network Monitoring.* San Francisco : Munich.

Centreon. (2018). *Centreon*. Obtenido de Centreon: https://www.centreon.com/

Cisco. (2 de Junio de 2008). *CISCO*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/simple-network-management-protocol-snmp/13506-snmp-traps.html

Ding, J. (2010). *Advances in Network Management.* Auerbach Publications Taylor & Francis Group.

Dondich, T. (2006). *Network Monitoring with Nagios.* O'Reilly Media.

Force, I. E. (mayo de 1990). *IETF(Internet Engineering Task Force)*.

Guerrero Pantoja , C. D. (2011). *Evaluación de gestión de redes bajo software libre de la administración zonal norte "Eugenio Espejo".* Quito: Universidad Politécnica Salesiana.

IEEE-STD-830. (1998). *Especificación de Requisitos de Software.*

Inuca Gonza, C. M. (2015). *Administración y gestión de la red de área local del Gobierno Autónomo Descentralizado Municipal del Cantón Cayambe, basado en el modelo*

funcional de Gestión de Red ISO/OSI con el protocolo SNMP y uso de herramientas de software libre. Ibarra: Universidad Técnica del Norte.

Inuca Gonza, C. M. (2016). *Administración y gestión de la red de área local del Gobierno Autónomo Descentralizado Municipal del Cantón Cayambe, basado en el modelo funcional de Gestión de Red ISO/OSI con el protocolo SNMP y uso de herramientas de software libre.*

ISO/IEC. (1989). *ISO / IEC 74984:*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=14258

Martí, A. B. (1999). *Gestión de Red.* Barcelona.

Microsoft. (s.f.). *Documentos Microsoft*. Obtenido de http://technet.microsoft.com/es-es/library/cc850692(v=office.14).aspx

Nagios. (s.f.). *Assets Nagios*. Obtenido de https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/timeperiods.html

Nagios. (s.f.). *Assets Nagios*. Obtenido de https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-routers.html

Orozco, P. (2010). *Gestión de Red del boli al SNMP.* Castelldefels: UPCnet.

Ortega Acosta, J. E., & Sinche Cruz , E. G. (2011). *Análisis del Rendimiento de Sistemas VoIP bajo condiciones de red variable.* Guayaquil: ESPOL.

Pandora FMS Enterprise. (2014). Obtenido de https://pandorafms.com/docs/index.php?title=Main_Page

Ramos Gaibor, J. L. (2016). *Análisis e implementación de un sistema integrado de gestión, para la red de datos de la Universidad Estatal de Bolívar matriz, en software libre.* Quito: Pontificia Universidad Católica del Ecuador.

Sáiz Diez, J. M., Marticorena Sánchez, R., & López Nozal, C. (2009). Herramienta de simulación para la realización de pruebas en la gestión de red basada en SNMP. *Jornadas de Enseñanza Universitaria de la Informática (JENUI) - JENUI 2009* . Barcelona.

Saydam, T., & Magedanz, T. (1996). *Gestión de redes y servicio de administración.*

The Cacti Group. (s.f.). *Cacti*. Obtenido de Cacti: https://www.cacti.net

Tlv, P. (2010). *Calameo.* Obtenido de Planificación y Gestión de Red: https://es.calameo.com/books/0049907372ca704547380

Torres Chicaiza, L. E. (2015). *Administración y gestión de la Red Inalámbrica del Gobierno Autónomo Descentralizado (GADIP) del Cantón Cayambe basada en el modelo funcional FCAPS de la ISO.* Ibarra : Universidad Técnica del Norte.

Torres Chicaiza, L. E. (2016). *Administración y gestión de la Red Inalámbrica del Gobierno Autónomo Descentralizado (GADIP) del Cantón Cayambe basada en el modelo funcional FCAPS de la ISO.*

Vega Mateo, R. (s.f.). *Administración y auditoría de los servicios de mensajería electrónica* . Editorial Elearning S.L.

Vicente Altamirano, C. (Julio de 2003). *Un modelo funcional para la administración de redes.* Ciudad de México: UNAM - DGSCA. Obtenido de Un modelo funcional para la administración de Redes: https://s3.amazonaws.com/academia.edu.documents/36534024/Apuntes_1_-_Un_modelo_funcional_para_la_administracion_de_redes.pdf?response-content-disposition=inline%3B%20filename%3DIndustrial_No_4_Jose_Menendez.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Crede

Wolfgang, B. (2008). *Nagios: System and Networking Monitoring.* Munich: Starch Press.

Zabbix Company. (s.f.). *Documentación de Zabbix 4.4.* Obtenido de https://www.zabbix.com/documentation/4.4/manual/introduction/about

ANEXOS

ANEXO I

INSTALACIÓN Y CONFIGURACIÓN

Instalación y Configuración de Nagios Core 4.4.3

a) Se instala las dependencias para Nagios en el servidor Centos utilizando el siguiente comando:

yum install gd gd-devel gcc make glibc glibc-common wget unzip net-snmp* openssh-server httpd which file gnutls-devel postgresql-devel perl-DBI less openldap-devel mysql-devel mysql-libs freeradius-devel bind-utils rpcbind samba-client sudo postfix php php-gd

b) Existen algunas dependencias que no se encuentran en los repositorios que tiene Nagios por defecto, por esta razón se instala el repositorio EPEL

yum install epel-release
yum install fping qstat
yum install "perl(Net::SNMP)"

c) Se crea un usuario para Nagios con su respectiva contraseña.

useradd -m nagios
passwd nagios

d) Posteriormente se establece un grupo con la finalidad de ejecutar scripts o plugins.

groupadd nagcmd

e) Al grupo creado se le añade a nagios y apache.

usermod -a -G nagcmd nagios
usermod -a -G nagcmd apache

f) Descarga de Nagios Core del sitio oficial.

wget -c https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.3.tar.gz

g) Descarga de Nagios plugins.

wget -c https://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz

h) Se descomprime el archivo de Nagios

tar xzvf nagios-4.4.3.tar.gz

i) Se procede a entrar al directorio de Nagios

cd nagios-4.4.3

j) Se ejecuta el siguiente comando que debe ejecutarse sin errores, si todas las dependencias están instaladas

./configure --with-command-group=nagcmd

k) Compilar e instalar el código fuente de Nagios

make all

make install

l) Instalar el script de inicio de Nagios

make install-init

m) Se activa el servicio de Apache

make install-webconf

n) Se instala archivos de ejemplo de la configuración, para una guía.

make install config

o) Habilitar la ejecución de scripts y comandos al usuario nagios

make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

p) Se crea una cuenta para el uso exclusivo de la interfaz web de Nagios Core con el usuario

nagiosadmin con su respectiva contraseña
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

q) Se compila e instala los plugins previamente descargados.

tar xzvf nagios-plugins-2.2.1.tar.gz
cd nagios -plugins-2.2.1
. /configure –with-nagios-user=nagios –with-nagios-group=nagios
make
make install

r) Se activa y reinicia el servicio apache

systemctl enable httpd
systemctl restart httpd
systemctl status httpd

s) Una vez compilado e instalado Nagios, como buena práctica se verifica que no haya errores, para esto se ejecuta.

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

t) Activar el servicio de Nagios en Centos

systemctl enable nagios
systemctl start nagios
systemctl status nagios.

Instalación de SNMP en el gestor

Es probable que SNMP ya venga instalado en nuestro sistema. Podemos comprobarlo con:

dpkg -l snmp

En caso de no estarlo podemos instalarlo con:

yum install snmp

Instalación del agente SNMP en switchs

a) Ingresar al switch

b) Habilitar el modo enable

Switch > enable

Switch #

c) Ingresar al modo de configuración

Switch # configure terminal

Switch(config)#

d) Habilitar snmp y configurar la comunidad de acceso

Switch (config)# snmp-server community public pucesisnmp

e) Salir del modo de configuración

Switch(config)# exit

f) Guardar y escribir la configuración

Switch # copy running-config startup-config

Instalación de Postfix

Si se ha instalado Nagios desde el repositorio EPEL no es necesario la instalación de POSTFIX ya que ya viene como dependencia si no se debe seguir los siguientes pasos:

a) Instalar con el siguiente comando

#yum install -y postfix

b) Modificar el fichero "main.cf" en la ruta /etc/postfix/main.cf

#relayhost =[smtp.gmail.com]:587
#smtp_sasl_auth_enable = yes
#smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
#smtp_sasl_security_options = noanonymous

#smtp_tls_CAfile = /etc/postfix/cacert.pem
#smtp_use_tls = yes

c) Modificar el fichero “sasl_passwd”

#smtp.gmail.com]:587 correogmail@gmail.com:Micontraseña

d) Establecer permiso para el fichero “sasl_passwd”

#chmod 600 /etc/postfix/sasl_passwd
#postmap /etc/postfix/sasl_passwd
#chmod 600 /etc/postfix/sasl_passwd.db

e) Reiniciar el servicio

#service postfix reload

f) Probar el funcionamiento

#echo "Probando Postfix + nagios" | mail -s "mi primera notificacion nagios" correodestino@servidor.com

Instalación de PNP4Nagios

a) Para instalar se ejecuta el comando

yum install rrdtool
yum install ruby xorg-x11-fonts-Type1 php-xml

b) Cambiar la ruta a la carpeta temporal para descargar PNP4Nagios

cd /tmp/

wget https://sourceforge.net/projects/pnp4nagios/files/PNP-0.6/pnp4nagios-0.6.25.tar.gz
tar -xvf pnp4nagios-0.6.25.tar.gz
cd pnp4nagios-0.6.25
./configure --with-rrdtool=/usr/bin/rrdtool --with-nagios-user=nagios --with-nagios-group=nagcmd

c) Compilar e instalar

make all
make install-webconf
make install-config
make install-init
make fullinstall

d) Reiniciar los servicios web y Nagios

systemctl enable npcd
systemctl start npcd
systemctl restart nagios
systemctl restart httpd

e) Verificar la configuración

cd pnp4nagios-0.6.25/scripts
./verify_pnp_config_v2.pl -m bulk -c /usr/local/nagios/etc/nagios.cfg -p /usr/local/pnp4nagios/etc/

f) Editar el archivo principal de configuración localizado en la ruta /usr/local/nagios/etc/nagios.cfg

service performance data
#service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata

service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTATE$\tSERVICESTATETYPE::$SERVICESTATETYPE$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-perfdata-file
# host performance data starting with Nagios 3.0

host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECKCOMMAND::$HOSTCHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$

host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file`

g) Buscar en el archivo las siguientes líneas y cambiar el 0 por 1

process_performance_data=1
enable_environment_macros=1

Configuración de NSClient++

a) Ejecutar el instalador NSClient++

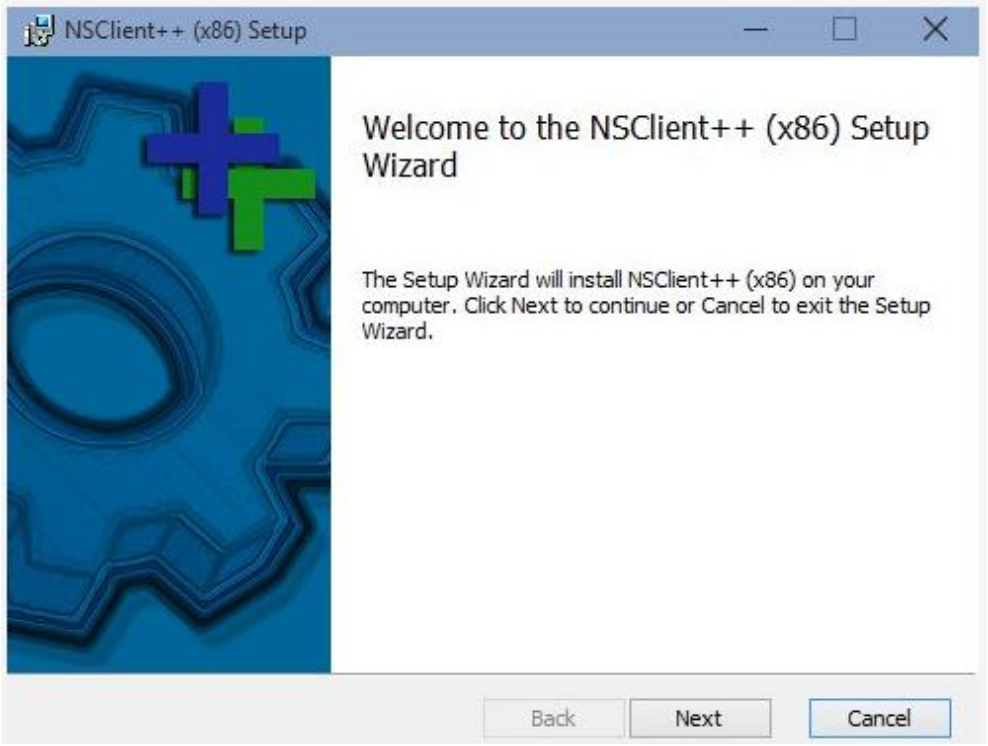


Figura 44. Ejecución para la instalación NSClient++
Fuente: NSClient++

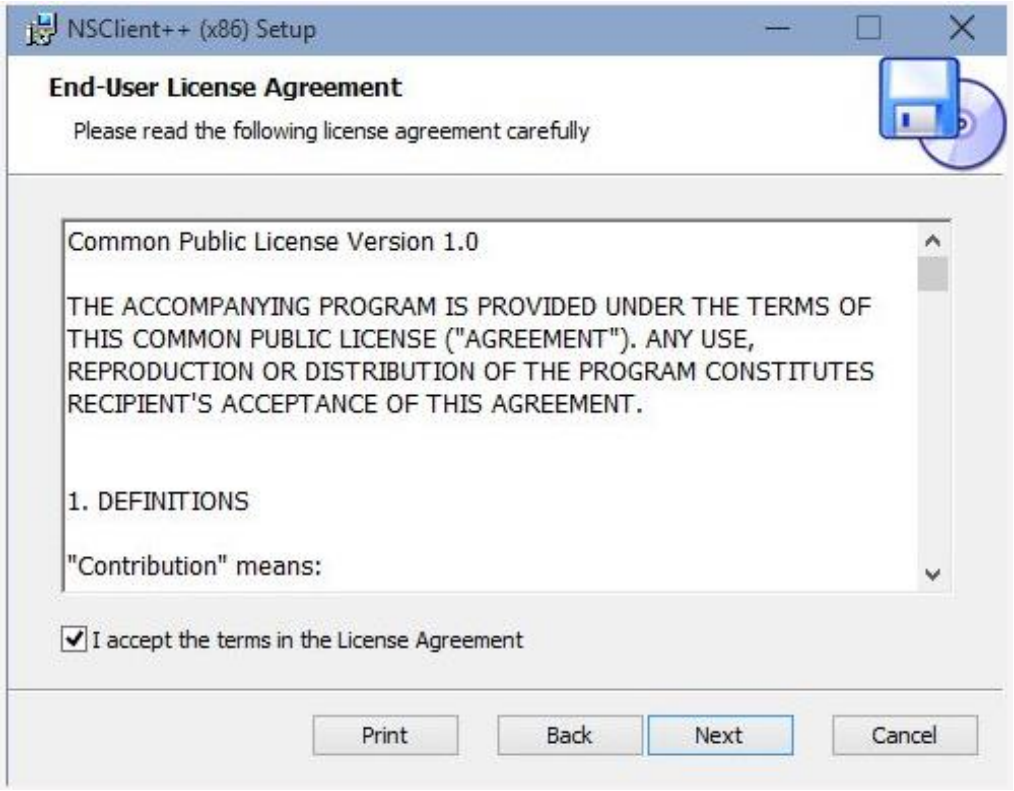


Figura 45. Ventana de instalación de NSClient++
Fuente: NSClient++

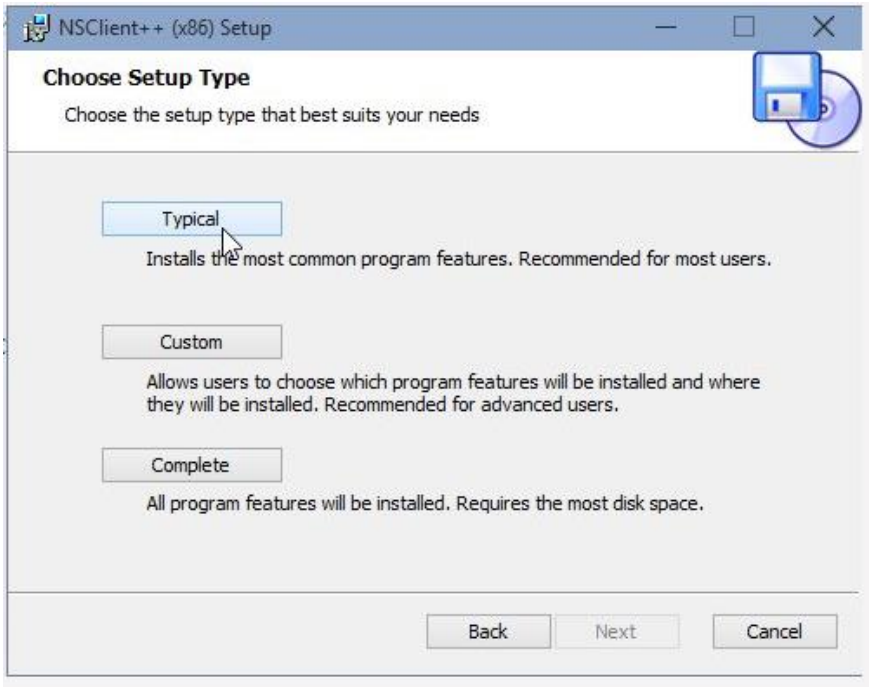


Figura 46 Elección del tipo de instalación de NSClient++
Fuente: NSClient++

Se activará la siguiente ventana de instalación en la cual se debe colocar la IP del gestor y una contraseña, se activa el check list de "Enable Web Server".

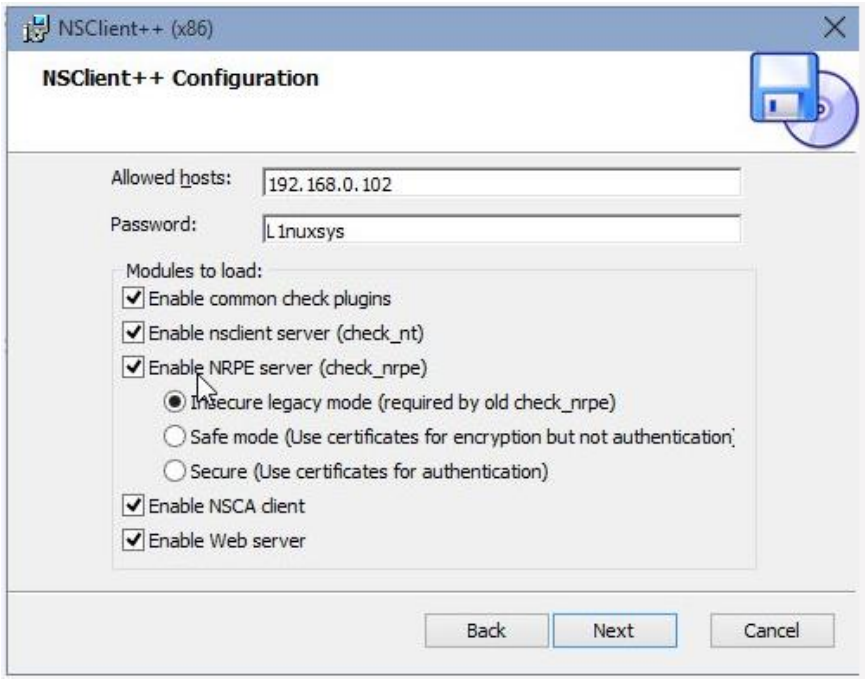


Figura 47. Configuración de NSClient++
Fuente: NSClient++

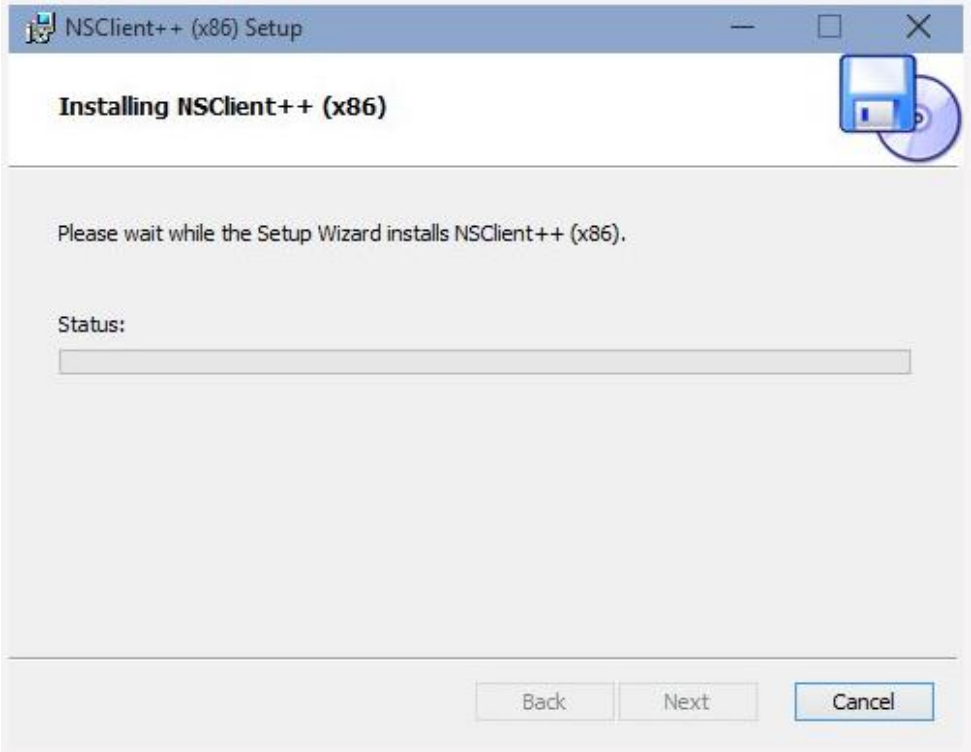


Figura 48. Proceso de avance de instalación NSClient++
Fuente: NSClient++

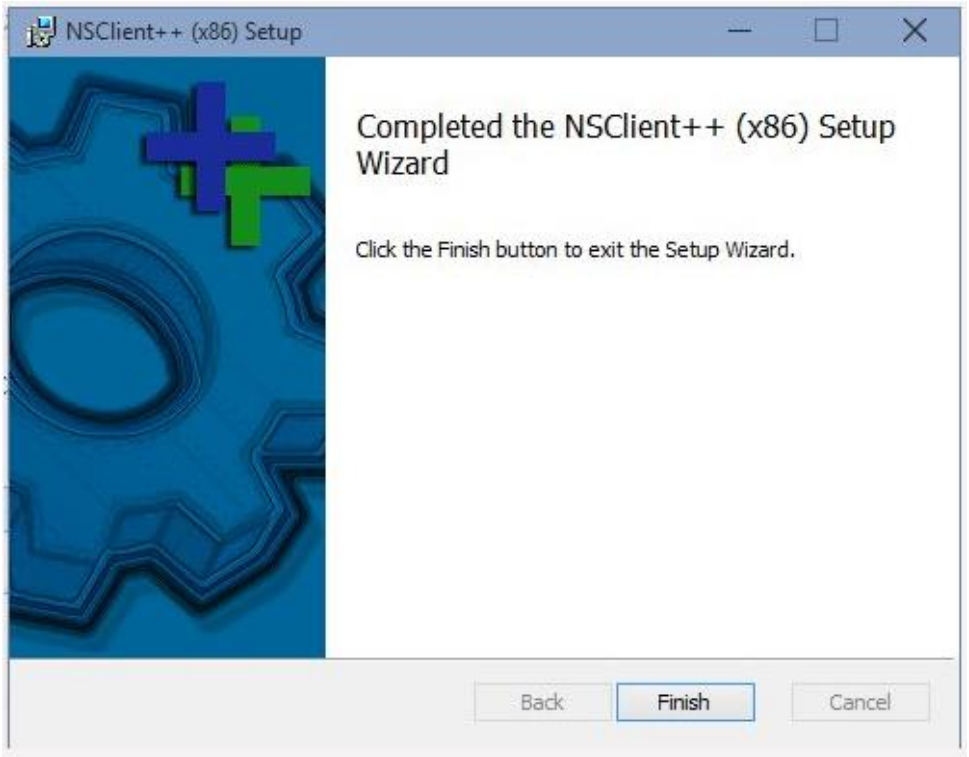


Figura 49. Instalación de NSClient ++ finalizada
Fuente: NSClient++

b) Modificar el archivo “nsclient.ini” con la siguiente información

```
# If you want to fill this file with all available options run the following command:
#   nscp settings --generate --add-defaults --load-all
# If you want to activate a module and bring in all its options use:
#   nscp settings --activate-module <MODULE NAME> --add-defaults
# For details run: nscp settings --help


; in flight - TODO
[/settings/default]

; Undocumented key
allowed hosts = 192.168.0.118

; in flight - TODO
[/settings/NRPE/server]

; Undocumented key
ssl options = no-sslv2,no-sslv3

; Undocumented key
verify mode = peer-cert

; Undocumented key
insecure = false

; in flight - TODO
[/modules]

; Undocumented key
CheckExternalScripts = disabled
```

; Undocumented key
CheckHelpers = disabled

; Undocumented key
CheckNSCP = disabled

; Undocumented key
CheckDisk = disabled

; Undocumented key
CheckSystem = disabled

; Undocumented key
NSClientServer = enabled

; Undocumented key
CheckEventLog = disabled

; Undocumented key
NSCAClient = enabled

; Undocumented key
NRPEServer = enabled

ANEXO II

Pontificia Universidad Católica del Ecuador
SEDE IBARRA
UNIDAD DE SISTEMAS

PUCE

POLÍTICA PARA MONITOREO DE LA RED DE DATOS PUCE-SI

Visión

Dentro de una organización, las comunicaciones en la actualidad están sujetas al rendimiento y disponibilidad de la red de datos. Sin embargo, no todas disponen de un constante monitoreo del estado y rendimiento de los dispositivos que componen esta infraestructura de red. Por tanto, es necesario implementar una política para cumplir este propósito, independientemente de la herramienta que se use para aquello.

Propósito

El propósito de esta política es definir reglas y requisitos para establecer un monitoreo constante, periódico y efectivo de los dispositivos de red, que ayuden a minimizar el riesgo de tiempos caídos y reducir las incidencias de disponibilidad que puedan afectar a las comunicaciones dentro de la PUCESI.

Alcance

Es responsabilidad del administrador de red, técnicos del área y personal backup, la revisión permanente y actualización de esta política, así como su socialización y cumplimiento de lo establecido en la misma.

Todo dispositivo nuevo de red, deberá ser previamente registrado en el inventario de dispositivos, indicando los parámetros técnicos y de identificación necesarios para su rápida ubicación y así mantener actualizado el inventario de la infraestructura de red con sus respectivos servicios de acuerdo al siguiente formato:

DISPOSITIVO	MARCA	MODELO	NRO SERIE	NOMBRE	IP v4	UBICACIÒN
Switch	Cisco	SG300 28P	DNI23887 QW	SW-A-03-01	192.168.X.X	Edif4 Rack3

Los dispositivos que se integran a la red, deberán tener una configuración básica y adecuada para que permita el monitoreo del mismo a través del protocolo SNMP.

Se deberá llevar documentación de los dispositivos gestionados, así como también los que no se encuentran configurados dentro de la herramienta seguido por la razón u observación del porque no se los configuró.

El Administrador de red o su personal backup deberá revisar periódicamente los umbrales establecidos a través de la herramienta de monitoreo y notificar si es necesario a las instancias pertinentes.

El Administrador de red o su personal backup será notificado a través de la herramienta sobre las alertas configuradas de acuerdo a lo establecido en el documento de categorización de alertas.

El Administrador de red deberá analizar la alerta recibida y buscar una pronta solución al problema, para reanudar el servicio.

EL Administrador de red deberá establecer un período de tiempo para la obtención y presentación de reportes necesarios que ayuden a determinar el rendimiento adecuado de la red de datos.

Únicamente el Administrador de red, Jefe de la Unidad de Sistemas y/o personal backup descritos en este documento tendrán acceso a la herramienta de monitoreo y sus notificaciones.

Cumplimiento de políticas

Medida de cumplimiento

El jefe de la unidad de sistemas verificará el cumplimiento de esta política a través de varios métodos, que incluyen monitoreo periódico, monitoreo de video, informes de herramientas internas, externas, propias y comerciales, auditorías e inspección, y proporcionará retroalimentación al administrador de red.

Excepciones

El monitoreo o respuesta ante un incidente en días no hábiles, feriados y vacaciones serán bajo demanda y en la medida de las posibilidades del personal responsable o su personal backup. Cualquier excepción a la política debe ser aprobada por anticipado por la unidad de sistemas.

Incumplimiento

El no cumplimiento a esta política puede estar sujeto a medidas disciplinarias y administrativas determinadas en los reglamentos internos.

Estándares, políticas y procesos relacionados

- Política de umbrales aceptables en equipos de comunicación.
- Acuerdo de terceros.
- Estándares de configuración de hardware y software en la PUCESI.
-

Historial de revisiones

Fecha de actualización	**Responsables**	**Resumen de la actualización**

Elaborado por:

Nombre	Firma	Fecha

Revisado por:

Nombre	Firma	Fecha

Aprobado por:

Nombre	Firma	Fecha

ANEXO III

Pontificia Universidad Católica del Ecuador
SEDE IBARRA
UNIDAD DE SISTEMAS

PUCE

MANUAL DE PROCESOS DEL MODELO DE GESTIÓN FCAPS

Visión

Proporcionar al administrador de red, técnicos del área y personal backup documentación la cual indique los pasos a seguir según establece el modelo de gestión aplicado.

Propósito

El propósito de este modelo de gestión es definir reglas y objetivos para administrar de forma integral la red datos, de esta manera preservar la calidad del servicio, reducir las incidencias de disponibilidad, maximizar el rendimiento de la red de datos de la PUCESI.

Alcance

Este manual aplica para el ingreso de dispositivos al software de gestión, para el establecimiento de umbrales para los servicios y recursos que serán gestionados. Permitirá dar seguimiento a cualquier evento que ocurra dentro de los dispositivos gestionados o servicios de la red de la PUCESI.

Abreviaturas

Nomenclatura	Definición
PUCESI	Pontificia Universidad Católica del Ecuador sede Ibarra
FCAPS	Fault, Configuration, Accounting, Performance, Security
SNMP	Protocolo simple de administración de la red

Tabla 29. Abreviaturas - Manual de Procesos FCAPS
Fuente: María Fernanda Pinto

Definiciones

Término	Definición
Software de gestión	Herramienta la cual mantiene monitoreados los dispositivos pertenecientes a la red mediante una interfaz centralizada
Dispositivo gestionado	Equipo monitorizado por el software de gestión
Umbrales	Se refiere al porcentaje de funcionamiento normal de un dispositivo gestionado.
Parámetros de monitoreo	Las características técnicas de los dispositivos gestionados que van a ser monitoreadas.
Reportes	Informes acerca del rendimiento de los dispositivos gestionados y sus servicios

Tabla 30. Definiciones - Manual FCAPS
Fuente: María Fernanda Pinto

PROCESO PARA LA GESTIÓN DE LA CONFIGURACIÓN

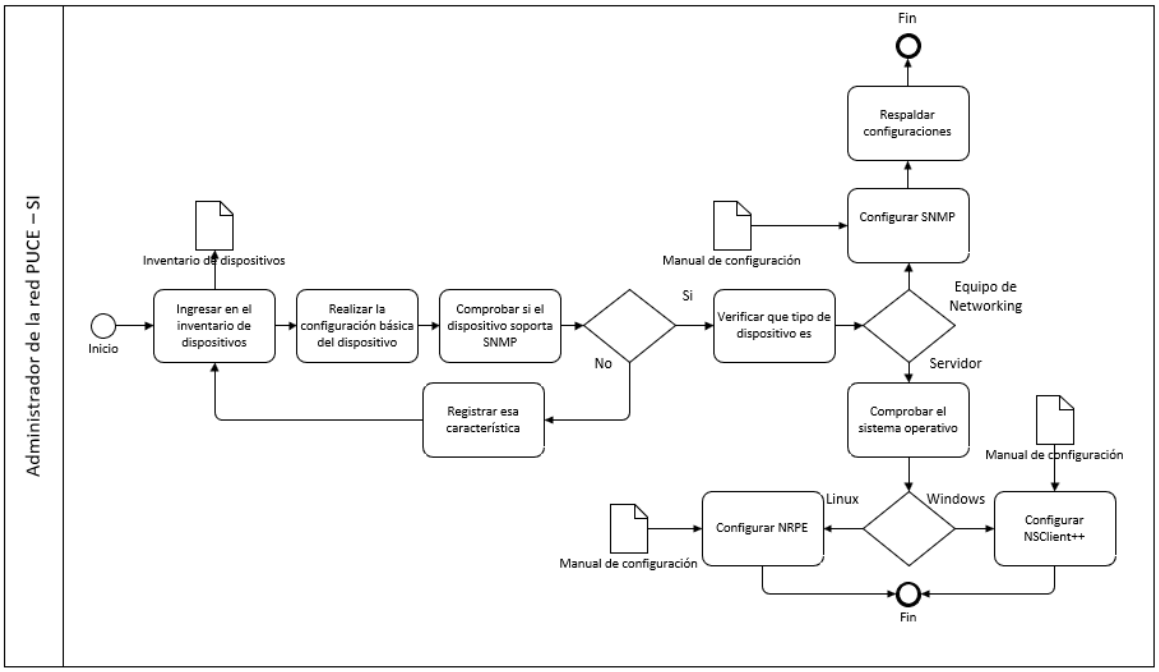


Figura 50. Proceso para la Gestión de la Configuración
Fuente: Modelo de gestión FCAPS

Descripción

Ingresar en el inventario de dispositivos: Documentar el dispositivo dentro del inventario de dispositivos siguiendo lo planteado en la política.

Realizar la configuración básica del dispositivo: Configurar la parte inicial de los dispositivos.

Comprobar si el dispositivo soporta SNMP: Verificar si soporta la habilitación del protocolo SNMP si es así:

Verificar que tipo de dispositivo: Si el dispositivo nuevo es un equipo de networking o servidor.

Equipo de Networking

Configurar SNMP: Dentro del switch siguiendo los pasos descritos en el manual de configuración, se habilita el protocolo simple de administración de red para permitir la comunicación con el sistema de administración de red.

Respaldar configuraciones: Dentro del dispositivo guardar la configuración y verificar que se realice de manera correcta.

Servidor

Comprobar el sistema operativo: Verificar si el servidor dentro de las configuraciones iniciales que sistema operativo fue instalado.

Windows

Configurar NSClient++: Proceder a configurar el agente NSClient++ como se muestra en el manual de configuración.

Linux

Configurar NRPE: Configurar el agente NRPE dentro del servidor siguiendo los procedimientos del manual de configuración.

No soporta SNMP

Registrar esa característica: Si el dispositivo no soporta el protocolo es preciso registrarlo en el inventario.

PROCESO PARA LA GESTIÓN DE FALLOS

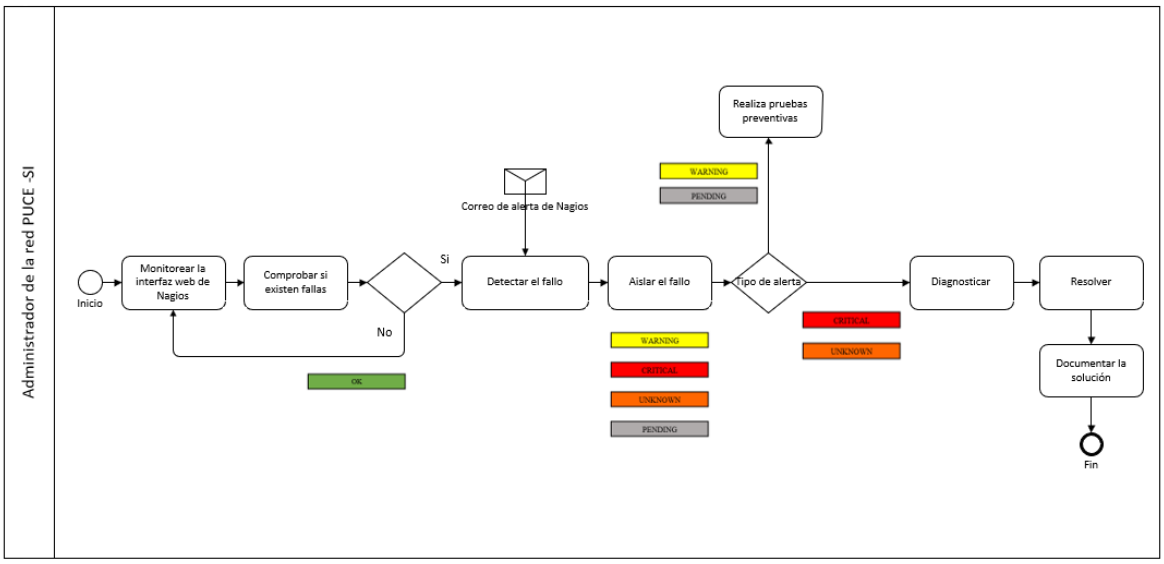


Figura 51. Proceso para la Gestión de Fallos
Fuente: Modelo de gestión FCAPS

Monitorear la interfaz web de Nagios: El gestor en su interfaz web indica el estado de los dispositivos de la red.

Comprobar si existen fallas

Si

Detectar el fallo mediante correo electrónico: Se envía un correo a la cuenta del administrador informando la alarma e indicando en que equipo ocurrió el fallo.

Aislar el fallo: Si el dispositivo gestionado ha sobrepasado los umbrales establecidos para su funcionamiento normal. Nagios presenta los estados representados por un color específico.

WARNING

Si se detectó problemas en la última comprobación del dispositivo gestionado o de un servicio, se interpreta que el mismo se encuentra en advertencia (warning) que es un paso antes de volverse crítico.

CRITICAL

Si un dispositivo o servicio se encuentra abajo (down) o inalcanzable (unreacheable) y si sobrepasa los umbrales establecidos para su funcionamiento normal en la última comprobación de estado, dicho dispositivo o servicio se ubica en estado crítico (critical).

UNKNOWN

Cuando un servicio o dispositivo no está bien definido presenta un estado desconocido (unknown)

PENDING

Si una nueva configuración está siendo reconocida por Nagios el estado es pendiente (pending)

Definir el tipo de alerta:

Si el host o servicio se encuentra en estado de advertencia o pendiente

WARNING PENDING

Realizar pruebas preventivas: Verificar el estado de las conexiones y estado físico del dispositivo las cuales permiten detectar los fallos ocultos para el sistema de monitoreo Nagios.

Si el host o servicio se encuentra en estado crítico o desconocido.

CRITICAL UNKNOWN

Diagnosticar: El administrador es el encargado de buscar la causa del problema en base a su experticia y conocimiento.

Resolver: El administrador de la red soluciona el fallo.

Documentar la solución: Para futuras soluciones si el problema se vuelve a repetir en otros equipos es importante registrar el fallo y como se solucionó dicho error.

No

OK

Es decir, el host o servicio se encuentra funcionando bajo los umbrales establecidos o cuando un dispositivo gestionado o un servicio está en el estado recuperado (recovery) en la comprobación realizada después de un tiempo determinado dentro de la configuración.

Una vez aplicadas las pruebas preventivas o correctivas se debe verificar si el procedimiento empleado para resolver el fallo funciona mediante un periodo de prueba, si es así y ha pasado el tiempo de prueba sin ningún nuevo fallo el dispositivo se considera nuevamente en producción, este cambio de estado registra un log en el sistema.

Mientras si durante el periodo de prueba ocurre un fallo nuevamente, es registrado en el documento denominado Bitácora de pruebas. Es importante resaltar que se genera logs al ingresar al software de gestión para realizar la verificación de dispositivos gestionados.

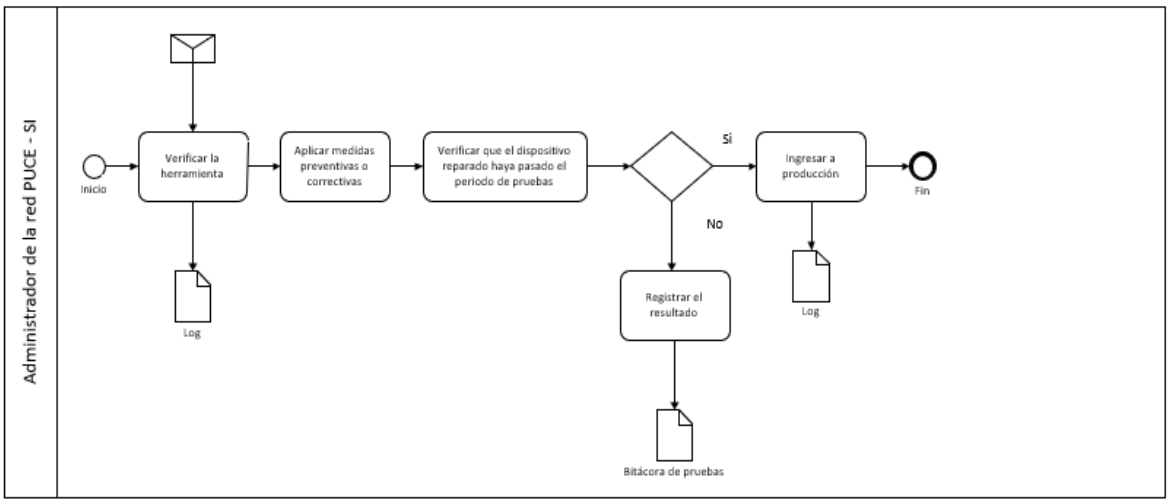


Figura 52. Proceso para la generación de Logs
Fuente: María Fernanda Pinto

PROCESO PARA LA GESTIÓN DE LA CONTABILIDAD

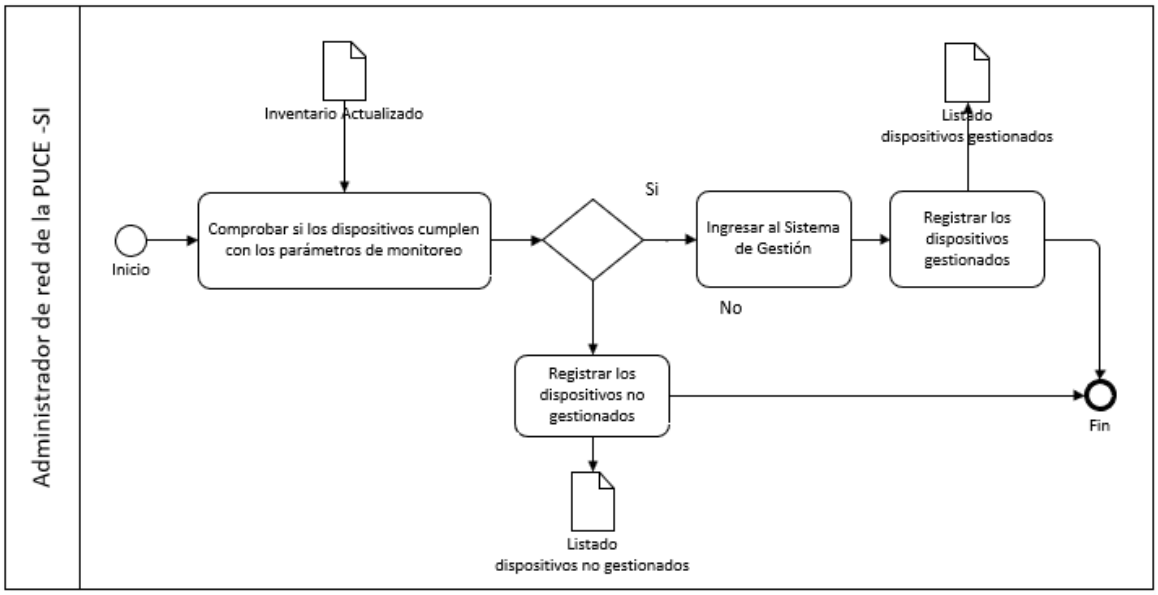


Figura 53. Proceso para la Gestión de la Contabilidad
Fuente: Modelo de Gestión FCAPS

Comprobar si el dispositivo cumple con los parámetros: Se comprueba si los dispositivos cumplen con soportar el protocolo SNMP, esta característica se encuentra en el inventario de dispositivos actualizado.

Si cumplen

Ingresar al Sistema de gestión: Se procede a ingresar al dispositivo dentro del software de gestión siguiendo los lineamientos del área de Gestión de la Configuración.

Registrar los dispositivos gestionados: Se llevará un listado de los dispositivos que se encuentran dentro del software de gestión.

Si no cumplen

Registrar los dispositivos no gestionados: Después de esta actividad se obtendrá un listado de los dispositivos que no están definidos dentro del software de gestión

Historial de revisiones

Fecha de actualización	Responsables	Resumen de la actualización

ANEXO IV

Pontificia Universidad Católica del Ecuador
SEDE IBARRA
UNIDAD DE SISTEMAS

PUCE

DISPOSITIVOS GESTIONADOS

Descripción / Modelo		**Marca**	**Ubicación**
ENRUTADOR	switch catalyst 4500	Cisco	EDIF#3 Data center
SWITCHES	Switch Catalyst 3560G Series	Cisco	EDIF#3 Data center
	Switch Baseline 2024	3com	#3 Rack Secundario Lab
	Switch Baseline 2024	3com	#3 Rack Secundario Lab
	Switch Baseline 2024	3com	#3 Rack Secundario Lab
	Switch Baseline SuperStack 3	3com	#3 Rack Secundario Lab
	Switch Catalyst 2960G Series	Cisco	#3 Rack Principal
	Switch Catalyst 2960G Series	Cisco	#1 secundario ENCI
	Switch Catalyst 2960G Series	Cisco	#2 Rack secundario
	Switch Catalyst 2960G Series	Cisco	#2 Rack secundario
	Switch Catalyst 3560G Series	Cisco	#3 Rack Principal
	Switch LinkSys SRW2024P	Cisco	#2 Rack secundario planta baja
	Switch LinkSys SRW2024	Cisco	#2 UCI

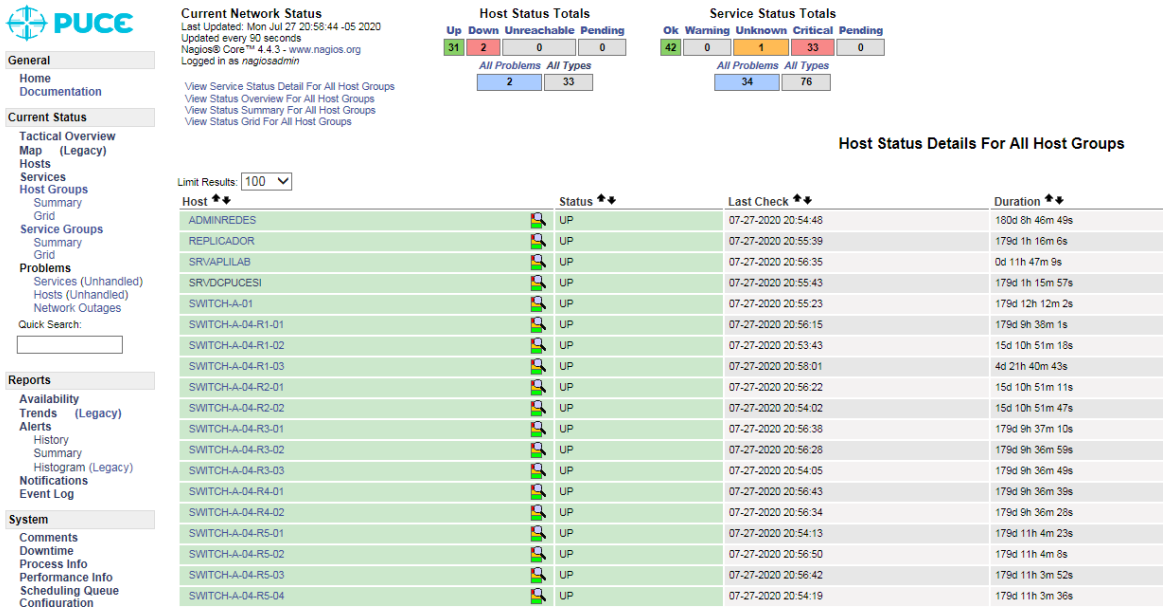
	Switch LinkSys SRW2024	Cisco	#3 ECAA
	Switch LinkSys SRW2024	Cisco	#2 Rack secundario planta baja
	Switch LinSys SRW2024P	Cisco	#1 Rack secundario Biblioteca
	Switch LinSys SRW2024P	Cisco	#3 rack Secundario Sala 9
	Switch LinSys SRW2024P	Cisco	#1 secundario ENCI
	Switch ProCurve HP 4000M	HP	#3 Rack Principal
	Switch ProCurve HP 4104GL	HP	#3 Rack Principal
	Switch Catalyst 2960G Series	Cisco	#2 Rack secundario
	Switch LinkSys SRW2024P	Cisco	#3 Rack secundario ECAA
	Switch LinkSys SRW2024P	Cisco	#3 Rack Secundario Lab
	Switch LinkSys SRW2024P	Cisco	Centro interactivo ECAA
	switch small business SG300 28P	Cisco	#2 rack secundario Aula Magna
	Access Point Small Business Pro	Cisco	#1 rack secundario Docentes T. Completo
	switch small business SG300 28P	Cisco	#2 rack sala docentes general
	switch small business SG300 28P	Cisco	#2 rack Oficina adquisiciones

	switch small business SF300 48P	Cisco	#3 Rack Secundario Lab
	switch small business SG300 28P	Cisco	#1 rack secundario ENCI
	switch small business SG300 28P	Cisco	#2 rack secundario
	switch small business SG300 28P	Cisco	#2 rack secundario UCI
	switch small business SG300 28P	Cisco	#1 rack secundario Biblioteca
	switch cisco catalys 2960S	Cisco	#1 rack secundario ENCI
	switch cisco catalys 2960S	Cisco	#2 rack secundario
	switch cisco catalys 2960S	Cisco	#3 rack principal
	wireless cisco 2500 AIR-CT2504-K9	Cisco	#3 rack principal
	switch small business SG300 28P	Cisco	#2 rack Sala DTCFrente adquisiciones
	switch small business SG300 28P	Cisco	Sala DTC Edif#1 piso1.2.1
	switch small business SG300 28P	Cisco	EDIF #1 rack principal
	switch small business SG300 28P	Cisco	EDIF #1 Sala DTC 1.2.x
	switch small business SG300 28P	Cisco	SALA12 EDIF3 PISO1
	wireless LAN controller 5508	Cisco	data center

	switch cisco catalys 2960S	Cisco	EDIF#4 Piso1 Rack Principal SW1
	switch small business SG300 52P	Cisco	EDIF#4 Piso1 Rack Principal SW2
	switch small business SG300 28P	Cisco	EDIF#4 Piso1 Rack Principal SW3
	switch small business SG300 52P	Cisco	EDIF#4 Piso2 Rack secundario SW1
	switch small business SG300 28P	Cisco	EDIF#4 Piso2 Rack secundario SW2
	switch small business SG300 28P	Cisco	EDIF#3 Sala 13 piso3
	switch small business SG300 28P	Cisco	EDIF#3 Sala 14 piso3
	switch small business SG300 28P	Cisco	Nueva Capilla sala de reuniones
	small business sg200 8p	Cisco	garita seguridad
	switch small business SG300 28P	Cisco	Sala de audiencias 2.1.14
	switch cisco catalys 2960S	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW1
	switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW2
	switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW3
	switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso1 Rack Principal SW4
	switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso2 Rack secundario SW5
	switch small business 28PP	Cisco	EDIF#4 ETAPA2 Piso2 Rack secundario SW6

	catalyst 2960S	Cisco	SW1 EDIF 4 ET3
	switch small business 28PP	Cisco	SW3 EDIF 4 ET2
	switch small business 28PP	Cisco	SW4 EDIF 4 ET3
	switch small business 28PP	Cisco	SW5 EDIF 4 ET3
	switch small business 28PP	Cisco	SW6 EDIF 4 ET3
	switch small business 28PP	Cisco	SW2 EDIF 4 ET3
	switch small business 28PP	Cisco	EDIF#3 SALA 6
	switch small business 28PP	Cisco	EDIF#3 SALA 5
	switch small business 28PP	Cisco	EDIF#3 SALA 9
	switch small business 28PP	Cisco	BODEGA SISTEMAS PARA REDES TEMPORALES
	switch cisco sg200-10fp	Cisco	OFICINA INFORMACION
	switch small business 28PP	Cisco	BANCO DE GERMOPLASMA
	switch small business 28PP	Cisco	ARCHIVO INACTIVO DIR ESTUADINTES
	switch small business 28PP	Cisco	EDIF #3 RACK ASO INGENIERIA
	switch small business 28PP	Cisco	EDIF #2 SALA 2.3.18

	switch small business 28PP	Cisco	BODEGA SISTEMAS STOCK
	switch small business 28PP	Cisco	BODEGA SISTEMAS STOCK



DISPOSITIVOS NO GESTIONADOS

Descripción / Modelo		Marca	Ubicación	Observación
ACCESS POINT	AIR-LAP1041N-A-K9	Cisco	Edif #1_piso6_ biblioteca	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #1 piso4_Arquitectura	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #1 piso2_AEPUCESI	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #1 piso5_aula1.5.3	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #1 piso3_aula 1.3	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #1 piso1_aula1.1	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 piso2_Maestrias	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 piso2_Ecoms	Monitoreadas por WLC

	externo AIR-LAP1310G-A-K9R	Cisco	Edif #1 piso4_parte exterior forntal	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 1 _aula2.2.2	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 Planta baja SALA DTC	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 Piso1 planata física	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 planta baja PLANIFICACION	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 parte posterior ADQUISICIONES	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 2 SALA DE GRADOS	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 2 SALA CONFERENCIAS	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 piso 1 PRORECTORADO	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #2 planta baja HALL PRINCIPAL	Monitoreadas por WLC

	AIR-LAP1041N-A-K9	Cisco	Edif #2 planta baja AULA MAGNA	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #3 piso 2 ECAA	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #3 piso1	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #3 planta baja (laboratorios sistemas)	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #3 Piso 1 sala Imac	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #3 piso1 pasillo	Monitoreadas por WLC
	AIR-LAP1041N-A-K9	Cisco	Edif #3 planta baja pasillo	Monitoreadas por WLC
	AIR-CAP1602I-A-K9	Cisco	EDIF#4 Planta baja fin pasillo 4.1.5	Monitoreadas por WLC
	AIR-CAP1602I-A-K9	Cisco	EDIF#4 Planta baja inicio pasillo	Monitoreadas por WLC
	AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 1 fin pasillo	Monitoreadas por WLC

	AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 1 inicio pasillo	Monitoreadas por WLC
	AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 2 fin pasillo	Monitoreadas por WLC
	AIR-CAP1602I-A-K9	Cisco	EDIF#4 PISO 2 inicio pasillo	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 1	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 2	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 3	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 BIBLIOTECA 4	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 PISO2 PASILLO JUNTO SSHH	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 PISO2 PASILLO MITAD	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA2 PISO2 PASILLO INICIO	Monitoreadas por WLC

	AIR-CAP2702I-A-K9	Cisco	EDIF#3_P3_PASILLO IDIOMAS	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	TALLERES GESTHUR AULA 2.1.26	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#1 PISO1 AULA 1.3.1	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#1 PISO2 SALA DTC 1.1.2	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF #1 PISO 5 DERECHA AULA 1.5.2	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF #1 PISO 3 DERECHA AULA 1.3.6	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF #1 PISO 5 IZQUIERDA AULA 1.5.4	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	REDES TEMPORALES EN AREAS ESPECIFICAS	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	REDES TEMPORALES EN AREAS ESPECIFICAS	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	REDES TEMPORALES EN AREAS ESPECIFICAS	Monitoreadas por WLC

	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO1 F	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO1 P	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO2 F	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO2 P	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO3 F	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 AUDITORIO3 P	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 PLANTA BAJA NUEVA SALA DE GRADOS	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 SECRETARIA PASILLO JARDINERA	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 COUNTER INFORMACION	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	CASA EVENTOS ECAA	Monitoreadas por WLC

	AIR-CAP2702I-A-K9	Cisco	EDIF#2 USE OFICINAS	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3 GALERIA ARQUEOLOGICA	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	HERBARIO	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#3 PISO2 SALA IMAC	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#2 SALA 2.3.16	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#2 SALA 2.3.17	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 OFICINAS CONTABILIDAD	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 HALL ENTRADA PRINCIPAL	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 PB BIBLIOTECA CERCA AL COUNTER	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 PB BIBLIOTECA CERCA A CUBICULOS	Monitoreadas por WLC

	AIR-CAP2702I-A-K9	Cisco	EDIF4_P1_MITAD PASILLO	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF4_PISO3_AULA4_3_17	Monitoreadas por WLC
	AIR-CAP2702I-A-K9	Cisco	EDIF#4 ETAPA3	Monitoreadas por WLC

ANEXO V

Pontificia Universidad Católica del Ecuador
SEDE IBARRA
UNIDAD DE SISTEMAS

PUCE

REGISTRO DE FALLOS

En este documento se detalla la información de fallos ocasionados dentro de los dispositivos gestionados de la red.

Los parámetros para llenar un registro de fallo son los siguientes

Número	Descripción	Fecha	Responsable	Lugar	Observaciones

Numero: Importante organizar las incidencias que se presentan en la red

Descripción: Realizar una pequeña reseña del fallo ocurrido

Fecha: La fecha en que sucedió que se encuentra en la herramienta

Responsable: La persona que registra el fallo

Lugar: El lugar en el que se encuentra el dispositivo

Observaciones: Utilizar si se necesita realizar explicaciones extras sobre lo ocurrido

Una vez superado el fallo es importante realizar un seguimiento cercano al dispositivo corregido sugerido por esta bitácora de pruebas:

Ping	**Temperatura**	**Memoria**	**Procesador**
☐	☐	☐	☐

Ibarra, 16 de septiembre del 2019

No. Of. 012-DS

Mgs.
Stalin Arciniegas
DIRECTOR DE LA ESCUELA DE INGENIERIA

Reciba un fraterno saludo en nombre de la Unidad de Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ibarra, a su vez me permito poner en su conocimiento que es de necesidad institucional, la elaboración del proyecto denominado "**IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y MODELO DE GESTIÓN DE LA RED DE DATOS DE LA PUCE-SI BASADA EN HERRAMIENTAS OPEN SOURCE**".

En tal virtud, pongo en su conocimiento que el mencionado proyecto lo realizará la Srta. Estudiante MARIA FERNANDA PINTO CAÑIZARES, portadora de la cédula de ciudadanía No. 1004660849, como trabajo de titulación, requisito previo para la obtención de su título académico.

Particular que informo para los fines pertinentes.

Atentamente,

Ing. Franklin Sánchez E., Msc
JEFE DE LA UNIDAD DE SISTEMAS PUCESI

c.c. Archivo

Pontificia Universidad Católica del Ecuador
Sede Ibarra

Ibarra a, 03 de agosto del 2020
No. Of. 014-DS

Mgs.
Stalin Arciniegas
DIRECTOR DE LA ESCUELA DE INGENIERÍA

Reciba un fraterno saludo en nombre de la Unidad de Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ibarra, a su vez me permito informar que la Estudiante MARÍA FERNANDA PINTO CAÑIZARES portadora de la cédula de ciudadanía No. 1004660849 desarrolló su trabajo de titulación denominado: **"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y MODELO DE GESTIÓN DE LA RED DE DATOS DE LA PUCE-SI BASADA EN HERRAMIENTAS OPEN SOURCE"**.

Siendo el objetivo del trabajo, elaborar un modelo de gestión e implementar una herramienta de monitoreo constante para la red, cumpliendo de manera satisfactoria con las funcionalidades que se exigían.

Particular que informo para los fines pertinentes.

Atentamente,

Firmado digitalmente por Franklin Sánchez E.

Franklin Sánchez E., Ing. Msc
UNIDAD DE SISTEMAS PUCESI
c.c. Archivo

Av. Jorge Guzmán Rueda y Av. Aurelio Espinosa Pólit, Cdla "La Victoria"
Código: 100112
Telf.: (+593) 06 2615 500 / 2615 453

Turnitin Informe de Originalidad

Procesado el: 2021年06月14日 13:22 -05
Identificador: 1606448501
Número de palabras: 20490
Entregado: 1

Tesis_FernandaPinto Por Maria Fernanda PINTO CAÑIZARES

Índice de similitud	Similitud según fuente
5%	Internet Sources: 4% Publicaciones: 1% Trabajos del estudiante: 1%

< 1% match (Internet desde 08-dic.-2020)
https://www.coursehero.com/file/51723197/teorema-de-conservacion-1docx/

< 1% match (Internet desde 18-dic.-2020)
https://www.coursehero.com/file/41815806/EUTANASIA-DE-DELITO-A-DERECHO-HUMANO-FUNDAMENTAL-UN-AN%C3%81LISIS-DE-LA-VIDA-A-PARTIR-DE-LOS-PRINCIPIOS/

< 1% match (Internet desde 25-may.-2020)
https://www.coursehero.com/file/39347462/A8-MLOApdf/

< 1% match (trabajos de los estudiantes desde 24-jul.-2018)
Submitted to Escuela Politecnica Nacional on 2018-07-24

< 1% match (trabajos de los estudiantes desde 20-sept.-2013)
Submitted to Escuela Politecnica Nacional on 2013-09-20

< 1% match (trabajos de los estudiantes desde 26-jul.-2018)
Submitted to Escuela Politecnica Nacional on 2018-07-26

< 1% match (trabajos de los estudiantes desde 04-dic.-2015)
Submitted to Universidad Católica de Santa María on 2015-12-04

< 1% match (Internet desde 12-may.-2020)
http://docplayer.es/95841254-Fuerte-y-productiva-maravillosamente-rentable.html

< 1% match (Internet desde 28-jul.-2017)
http://docplayer.es/7929560-Modelo-de-gestion-de-internet.html

< 1% match (Internet desde 23-oct.-2020)
https://pt.scribd.com/document/346865405/TUAEXCOMIEAN013-2015

< 1% match ()
Mora Grijalva, Ney Fernando. "Modelo de Gestión Gerencial para disminuir los riesgos en la cooperativa de Ahorro y Crédito Tulcán.", 2014

< 1% match (Internet desde 31-mar.-2016)
http://repositorio.utn.edu.ec/handle/123456789/4

< 1% match (Internet desde 31-oct.-2019)
http://x1nux.blogspot.com/2009/06/monitor-nagios.html

< 1% match (trabajos de los estudiantes desde 05-ago.-2016)
Submitted to Universidad Militar Nueva Granada on 2016-08-05

< 1% match (Internet desde 18-ene.-2021)
https://doaj.org/article/f495f5d3ec40448995fc131b53c0fbd3

< 1% match (Internet desde 15-ene.-2021)
https://doaj.org/article/000d6e1b50bc458cb427fae177dca397

< 1% match (Internet desde 19-jul.-2020)
http://www.utn.edu.ec/fica/carreras/electronica/wp-content/uploads/2016/07/ANTEPROYECTOS-APROBADOS.pdf

< 1% match (Internet desde 26-nov.-2020)
https://aisel.aisnet.org/cgi/viewcontent.cgi?amp=&article=1946&context=amcis2007

< 1% match ()
http://fcae.ua.es/boe/20020404.htm

< 1% match (Internet desde 14-mar.-2014)
http://nopalitux.net/

< 1% match (trabajos de los estudiantes desde 23-mar.-2016)
Submitted to Universidad Cesar Vallejo on 2016-03-23

< 1% match (Internet desde 16-jul.-2020)
http://repositorio.espe.edu.ec/bitstream/21000/10790/1/T-ESPE-048979.pdf

< 1% match (trabajos de los estudiantes desde 22-may.-2021)
Submitted to unsaac on 2021-05-22

< 1% match (trabajos de los estudiantes desde 16-jun.-2016)
Submitted to University of Wales central institutions on 2016-06-16