Implementación y puesta en servicio de un Sistema de Gestión y Monitoreo de Redes para los equipos de la red OT (Tecnología de las Operaciones) de ANDE

Ricardo M. Loreiro, Chrystian Ruiz Díaz

ADMINISTRACIÓN NACIONAL DE ELECTRICIDAD (ANDE)

Paraguay

1.1 Resumen

La Administración Nacional de Electricidad - ANDE, actualmente posee más de cien subestaciones eléctricas integradas al sistema Supervisión Control y Adquisición de Datos - SCADA ubicadas en distintas ciudades a lo largo del territorio paraguayo, constituyendo los nodos del Sistema Interconectado Nacional (SIN). La ANDE cuenta con cinco Centros de Control para transmisión y en algunos casos para distribución, distribuidos de la siguiente manera; uno en la zona metropolitana, una el sur, una en el este y otra en el Norte del País. La topología implementada es mixta o hibrida y los medios de comunicación son una combinación enlaces propios como; Fibras Ópticas ADSS - *All Dielectric Self Supported*, Fibras Ópticas OPGW-*Optical Ground Wire*, enlaces microondas, red MPLS/IP - *Multiprotocol Label Switching/Internet Protocol*, en algunos casos ondas portadoras, adicionalmente se arrendan VPN - *Virtual Private Network* o servicios de terceros para redundancia de los enlaces. Esta infraestructura OT - - *Operational Technology* la conforman los servidores centralizados y distribuidos, *router, switches, firewall*, multiplexores y equipos de comunicación desplegados en las diversas subestaciones y centros de control. Por lo expuesto gestionar de manera eficiente esta infraestructura se vuelva sumamente complejo y complicado sin apoyo de un sistema de monitoreo automatizado.

La infraestructura tecnológica en la red OT es una parte vital de los sistemas SCADA y debe garantizar la disponibilidad de las comunicaciones del SCADA con las Subestaciones, la creciente evolución tecnológica de operar de un entorno aislado a una red convergente. En este sentido, con la convergencia surge la necesidad de realizar la monitorización y supervisión de forma más proactiva, la cual se vuelve un factor crítico tanto para la prevención, la atención inmediata de incidencias, y la reducción de los tiempos de inactividad de los servicios y equipos de comunicación de la red.

En este artículo se presenta algunos elementos considerados para la incorporación e implementación de un conjunto de soluciones de gestión OT, una propuesta integral compuesta por un sistema de monitoreo para la supervisión de servidores, equipos de *networking* y servicios de infraestructura de misión crítica para la reducción de los tiempos de respuesta ante fallas de la red, un software de análisis, supervisión y monitoreo de tráfico de red, ancho de banda y análisis de flujo de datos de toda la infraestructura OT, y una aplicación para la administración, gestión, búsqueda y notificación de datos de registro.

La finalidad de esta implementación además de los beneficios mencionados anteriormente es la de dotar a la institución de una herramienta eficaz, flexible, adaptativa y escalable para la supervisión y control de una red que está constantemente en proceso de actualización y expansión.

1.2 Palabras clave

Monitoreo, SCADA, Supervisión, Subestación, OT, Redes,

1.3 Cuerpo del trabajo

1. INTRODUCCIÓN

El presente trabajo ofrece una descripción rápida sobre el trabajo de implementación ejecutado por el Departamento de Ingeniería de Sistemas de Control (DTE/ISC) de la Administración Nacional de Electricidad (ANDE) para la puesta en servicio de un conjunto de soluciones para la gestión y el monitoreo de la infraestructura OT de la misma. Debido principalmente a la extensión del trabajo ejecutado se intenta hacer una descripción concisa y breve de cada una de las herramientas y elementos configurados en su proceso de implementación.

2. INFRAESTRUCTURA OT DE LA ADMINISTRACIÓN NACIONAL DE ELECTRICIDAD.

La Administración Nacional de Electricidad (ANDE), actualmente posee más de cien subestaciones eléctricas integradas al sistema Supervisión Control y Adquisición de Datos - SCADA ubicadas en distintas ciudades a lo largo del territorio paraguayo, constituyendo los nodos del Sistema Interconectado Nacional (SIN). La ANDE La topología implementada es mixta o hibrida y los medios de comunicación son una combinación enlaces propios como Fibras Ópticas ADSS, Fibras Ópticas OPGW, enlaces microondas, red MPLS/IP, ondas portadoras, adicionalmente se arrendan VPN o servicios de terceros para redundancia de los enlaces.

La tecnología de Operaciones u *Operational Technology (OT)* se refiere al empleo de soluciones, ya sea a nivel de *hardware* o *software* que detectan, causan y afectan directamente el monitoreo y/o control de dispositivos físicos, eventos y procesos dentro de una organización [1]**.** En el caso de ANDE esta la conforman los servidores centralizados y distribuidos, *router, switches, firewall,* multiplexores y equipos de comunicación desplegados en las diversas subestaciones y centros de control, siendo el principal desafío el establecer las medidas de seguridad las cuales se centran principalmente en el tiempo de actividad y disponibilidad de los equipos. [2], siendo esta tarea sumamente compleja sin apoyo de un sistema de monitoreo automatizado.

Teniendo en cuenta que la red OT de la ANDE es una infraestructura en constante proceso de actualización y expansión, el Departamento de Ingeniería de Sistemas de Control (DTE/ISC) de la institución implementa un propuesta integral conformada por un sistema de monitoreo para la supervisión de servidores, equipos de *networking* y servicios de infraestructura de misión crítica con el objetivo de reducir los tiempos de respuesta ante fallas, un sistema para la gestión, búsqueda y notificación de datos de registro, un sistema encargado del análisis, supervisión y monitoreo de tráfico de la red y flujo de datos, y una plataforma del mismo fabricante que permite la creación sencilla de *dashboards*, vistas y pantallas de visualización de modo a que el monitoreo y control se pueda ejecutar de forma más intuitiva y práctica.

3. SOLUCIONES IMPLEMENTADAS.

3.1 Sistema de Monitoreo de equipos de *Networking.*

El sistema implementado consiste en poderosa herramienta para el monitoreo de la infraestructura OT, basado en el software de monitoreo *open source* Nagios Core 4, el cual permite el monitoreo de elementos críticos como servidores, equipamiento de la infraestructura de red, métricas del sistema, servicios y aplicaciones alertando cuando el comportamiento de los mismos no es el deseado. El mismo mediante una extensa cantidad de *plugins* propios y de terceros lo convierten en una herramienta altamente escalable y personalizable. [3]

Entre las funcionalidades implementadas cabe destacar el monitoreo de servicios de red y recursos de los mismos, el acceso vía interfaz web, personalización de *dashboards* y vistas por usuario, reportes de monitoreo

automatizados, gestión de usuarios para la creación de grupos de trabajo integrable a *Active Directory (AD)*, gestión de notificaciones vía email o servicios de mensajería como Telegram.

3.2 Sistema para gestión de *logs* y datos de registro

La propuesta implementada consiste en aplicación empresarial para el monitoreo, administración y análisis de registros o *Logs*, el cual permite visualizar, consultar y analizar registros de forma rápida y centralizada, facilitando la resolución de problemas que puedan surgir y corrección de eventos en la infraestructura. [3]

Algunas de las funciones principales implementadas son la búsqueda y análisis de logs mediante *queries* y filtros personalizados por usuario, la visualización de *logs* en tiempo real, gestión de notificaciones y alertas vía email, gestión de reportes automatizados y gestión de usuarios con integración a AD.

3.3 Sistema para el análisis de flujo y tráfico de red.

Esta herramienta brinda una visión del tráfico de red y la detección de comportamientos anormales y amenazas de seguridad, monitoreo profundo de las fuentes tráfico y ancho de banda asegurando así el correcto funcionamiento de los sistema y servicios integrados y la recopilación de información de alto nivel. [3]

Entre las funcionalidades implementadas podemos mencionar la definición de alertas de comportamiento anómalo, el análisis avanzado del tráfico mediante *queries* y vistas, la gestión de usuarios vía AD.

3.4 Sistema de visualización centralizada y creación de *dashboards*

Este sistema tiene la función de brindar una vista centralizada de las soluciones, otorgando una descripción de alto nivel los sistemas. Podemos resaltar entre las funcionalidades implementadas la integración con el sistema de Monitoreo de *Networking* y el Gestor de *Logs*, la creación y personalización de *dashboards* según preferencias del usuario, creación de vistas y tableros rotativos con visualización de métricas configuradas. [3]

4. INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO.

La instalación fue implementada en máquinas virtuales con sistema operativo CentOS a través del *hypervisor* VMware EXSi, utilizando la bibliografía *online* del proveedor [3]. Los recursos de cada máquina virtual fueron aprovisionados según los requerimientos recomendados.

4.1 Integración con *Active Directory (AD).*

La gestión de credenciales de usuario en la ANDE se efectúa mediante el AD de la organización. La integración se puede efectuar directamente a través de la interfaz gráfica de cada herramienta, siendo requeridos datos como la Base DN para la ubicación de los usuarios en el árbol de direcciones del AD, datos de dominio, sufijo de las cuentas, el protocolo de seguridad del servidor y el certificado de autenticación.

Una vez verificada la conexión con el servidor los usuarios pueden ser agregados obteniéndose las ID, credenciales y emails para las notificaciones. El rol de cada usuario es asignado según requerimientos del departamento, pudiendo ser *admin* o *user*. En la configuración de roles para el Sistema de Monitoreo en particular pueden ser definidos ciertos permisos en caso de *users* con responsabilidades puntuales.

4.2 Configuración y Monitoreo del Sistema de Monitoreo de equipos de *Networking*

Debido a la diversidad de elementos que conforman la red OT de ANDE como la gran gama de dispositivos integrables al sistema la presente sección se limita a la descripción breve y concisa del procedimiento para la

integración de los principales elementos de la red como la configuración de reportes, notificación, alertas y características esenciales.

Los objetos de monitoreo en el sistema se pueden dividir en dos tipos, *host* y *services*, teniendo los *hosts* uno o más *services* asociados. Los *hosts* cuentan con tres estados posibles en el sistema, *Up*, *Down* y *Unreacheable*, mientras que los servicios tienen cuatro, *Ok*, *Warning*, *Critical* o *Unknown*. Los *hosts* se refieren a terminales físicos o virtuales de la red, como servidores, estaciones de trabajo, *routers*, conmutadores de red, entre otros, mientras que un *service* se refiere a un atributo de un *host*, como uso de la CPU, disco duro, estado de puertos

4.2.1 Agrupación y jerarquía

Tanto *hosts* como *services* pueden agruparse en grupos (*host groups, service groups)* donde se agrupan elementos con funciones lógicas similares, por ejemplo “Switches”, “Routers”, “Servidores Windows”; esta práctica es recomendada para facilitar al sistema el gerenciamiento centralizado de todos los elementos.

Otra práctica recomendada es la jerarquización entre *hosts*, algo habitual en una infraestructura de red. Esto define el orden de operación lógica de monitoreo de modo a que cuando el *host parent* esté inactivo, aquellos *hosts* dependientes no sean monitoreados ahorrando recursos al ser estos dispositivos inalcanzables en la red.

4.2.2 Monitoreo de Servidores

En el caso de la supervisión de servidores Windows en la red OT de ANDE se efectúa mediante el uso de agentes que se encargan de la comunicación con el sistema a la hora del monitoreo. La instalación del agente en el servidor destino se ejecuta según las recomendaciones dadas en la documentación y se proveen de datos como la IP y puerto del Sistema de Monitoreo, y el *token* para la autenticación entre las partes.

Luego en la interfaz web del Sistema de Monitoreo se define el objetivo a monitorear a través de su IP y puerto y el *token* de acceso. Una vez enlazada la conexión se definen los servicios a ser monitoreados, los umbrales de *Warning* y *Critical* para la definición del estado de los mismos, tiempos de monitoreo y notificación. Finalizada la configuración del *host*, se puede observar su estado desde la interfaz web, véase Figura 1.

Service Status for this Host

Service	Status	Duration	Attempt	Last Check	Status Information
CPU Usage	Ok	13d 8h 5m 0s	1/5	2022-04-25 01:42:44	OK: Percent was 16.77 %
Disk Usage on C:/	Ok	19d 16h 47m 13s	1/5	2022-04-25 01:43:15	OK: Used_percent was 37.90 %
Disk Usage on D:/	Ok	4d 12h 29m 41s	1/5	2022-04-25 01:42:37	OK: Used_percent was 43.00 %
Memory Usage	Ok	11d 14h 1m 56s	1/5	2022-04-25 01:43:14	OK: Used memory was 32.50 % (Available: 10.80 GiB, Total: 16.00 GiB, Free: 10.80 GiB, Used: 5.20 GiB)
Proccess count for: Explorador de windows	Ok	29d 19h 41m 44s	1/5	2022-04-25 01:42:17	OK: Process count for processes named explorer.exe was 0
Proccess count for: Explorer	Ok	40d 22h 4m 49s	1/5	2022-04-25 01:42:27	OK: Process count for processes named explorer.exe was 0
Proccess count for: FEP primario	Ok	4d 12h 29m 40s	1/5	2022-04-25 01:42:45	OK: Process count for processes named scada.exe was 1
Service status for: W3SVC	Ok	21h 27m 7s	1/5	2022-04-25 01:42:16	OK: W3SVC is running
Swap Usage	Ok	29d 19h 41m 38s	1/5	2022-04-25 01:42:32	OK: Used swap was 30.90 % (Total: 18.37 GiB, Used: 5.67 GiB, Free: 12.70 GiB)

Figura 1: Servidor Windows integrado al sistema de monitoreo

4.2.3 Plataformas de Monitoreo VMware.

La integración de plataformas de virtualización ESX proporcionadas por VMware se ejecuta mediante un *Wizard* encargado para el efecto. Como configuración previa se requiere de la instalación del kit de desarrollo VMware Perl SDK el cual se descarga de la web de VMware y es instalada por conexión SSH al Sistema.

Una vez finalizado este proceso se procede a la configuración mediante el *Wizard* ingresando la dirección IP, nombre usuario y contraseña de la plataforma de virtualización. Los servicios monitoreables son configurados, así como los umbrales críticos, tiempos de monitoreo y notificación de forma análoga a la sección anterior.

4.2.4 Monitoreo de dispositivos vía SNMP

Para el caso de dispositivos como *switches*, *routers* o *firewalls* se opta por el monitoreo mediante protocolo SNMP versión 3, siendo la configuración de los dispositivos de forma manual atendiendo las indicaciones proveídas por cada fabricante. Luego se procede a la configuración del sistema a través de *wizards* donde se define la IP del dispositivo, credenciales SNMP, umbrales de los servicios y los tiempos de monitoreo y notificación. Este proceso puede agilizarse mediante el uso del *wizard* "*Bulk Host Colning and Import"* que permite la duplicación de *hosts* con sus servicios asociados en caso de dispositivos con la misma configuración.

En la Figura 2, se observa un *host* ingresado en el sistema, en este caso en particular un *router*, en el cual puede observarse el estado y consumo de banda de cada uno de los puertos.

Service Status for this Host

Service	Status	Duration	Attempt	Last Check	Status Information
Ping	Ok	8d 13h 43m 18s	1/5	2022-04-25 01:52:22	OK - 10.200.104.254 rta 1.197ms lost 0%
Port 2 Bandwidth	Ok	312d 14h 38m 38s	1/5	2022-04-25 01:53:15	OK - Current BW in: 0Mbps Out: 0Mbps
Port 2 Status	Ok	8d 13h 43m 41s	1/5	2022-04-25 01:54:13	OK - Interface NULL0 (index 2) is up.
Port 3 Bandwidth	Ok	312d 14h 39m 20s	1/5	2022-04-25 01:52:42	OK - Current BW in: 0Mbps Out: 0Mbps
Port 3 Status	Ok	8d 13h 43m 11s	1/5	2022-04-25 01:52:43	OK - Interface GigabitEthernet0/0/0 (index 3) is down
Port 5 Bandwidth	Ok	312d 14h 38m 47s	1/5	2022-04-25 01:52:54	OK - Current BW in: 0Mbps Out: 0Mbps
Port 5 Status	Ok	8d 13h 43m 7s	1/5	2022-04-25 01:52:29	OK - Interface GigabitEthernet0/0/2 (index 5) is down
WAN SE_BMO a ES_PBO Status	Ok	8d 13h 43m 17s	1/5	2022-04-25 01:52:40	OK - Interface GigabitEthernet0/0/7 (index 10) is up.
WAN SE_BMO a ES_PBO Bandwidth	Ok	222d 11h 19m 4s	1/5	2022-04-25 01:53:26	OK - Current BW in: 0Mbps Out: 0Mbps
LAN SE_BMO Status	Ok	8d 13h 43m 45s	1/5	2022-04-25 01:54:29	OK - Interface GigabitEthernet0/0/1 (index 4) is up.
LAN SE_BMO Bandwidth	Ok	222d 11h 19m 19s	1/5	2022-04-25 01:53:28	OK - Current BW in: .03Mbps Out: 0Mbps
WAN_BMO_VAU Bandwidth	Ok	222d 11h 18m 46s	1/5	2022-04-25 01:53:27	OK - Current BW in: 0Mbps Out: 0Mbps
WAN_BMO_VAU Status	Ok	8d 13h 42m 54s	1/5	2022-04-25 01:53:02	OK - Interface GigabitEthernet0/0/8 (index 11) is up.

Figura 2: *Router* monitoreado en Nagios XI

La herramienta forma predeterminada toma los puertos no utilizados o configurados como caídos, lo cual los califica como un *Critical* en el sistema, esto puede crear confusión y dificultar la atención a otros eventos de mayor prioridad. Para modificar esto, se procede a la creación de un comando nuevo (Configure < Core Config Manager < Commands) basado en el mismo ejecutado para la consulta de estados. Este es comando es asignado de forma manual a cada puerto que sea necesario mediante la configuración del servicio asociado al mismo.

En caso de los *Firewalls*, donde se necesitan de monitorear más parámetros además del estado de los puertos se procede a descargar el *Management Information Base* (MIB) proveído por el fabricante el cual es ingresado a la plataforma en la sección de extensiones del sistema (Admin < System Extensions < Manage MIBs), para luego ser utilizado en el *wizard* "SNMP Walk" en el cual debe especificarse además de los datos para el enlace con el dispositivo de los correspondientes *Object Identifiers (OID)* contenidos en el MIB.

4.2.5 Notificaciones y alarmas

Las notificaciones y alertas pueden definidas a través de la interfaz gráfica del sistema, en este trabajo se implementa como método de envío el correo electrónico y el servicio de mensajería Telegram. Las notificaciones pueden ser enviadas según necesidad, pudiendo ser tan pronto se detecte el inconveniente, después de un número definido de consultas o en ningún caso.

Para la notificación a los correos electrónicos asociados a los usuarios se hace mediante un servidor de correo electrónico previamente configurado a través de la interfaz web (Admin < Email Settings). El mensaje a enviar puede ser editado mediante lenguaje de código HTML (Admin < Users < Notification Management).

Las notificaciones vía Telegram se configuran mediante la configuración de un comando con un *token* correspondiente a un grupo creado en Telegram para el efecto, este comando se ejecuta en conjunto con el correspondiente de las notificaciones vía email.

Cabe mencionar que la plataforma permite crear grupos de trabajo para la notificación de *hosts* y servicios asociados y un sistema de escalamiento para la notificación por niveles según jerarquía, permitiendo escalar los avisos a usuarios de nivel superior en caso de no ser atendidos previamente por usuarios de nivel inferior.

4.2.6 Vistas rápidas y *dashboards* de la interfaz web.

La interfaz web permite la creación de *dashboards* personalizables por usuario, para el despliegue de información relevante y acceso rápido a parámetros de interés. En la Figura 3 se observa un *dashboard* creado para la visualización de las últimas alertas existentes, el estado general de *hosts* y *services*, y el estado de métricas de dispositivos.

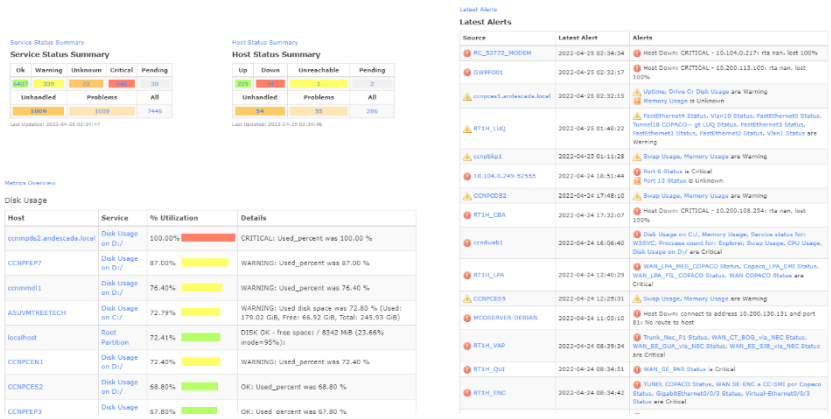

Figura 3: *Dashboard* personalizado creado por usuario

A su vez el sistema permite la creación de vistas rotatorias, utilizando pantallas ya predefinidas en la plataforma como personalizadas a través de un complemento que permite la creación de vistas mediante elementos gráficos, mapas geográficos y figuras asociadas al estado de *hosts* y servicios, Figura 4.

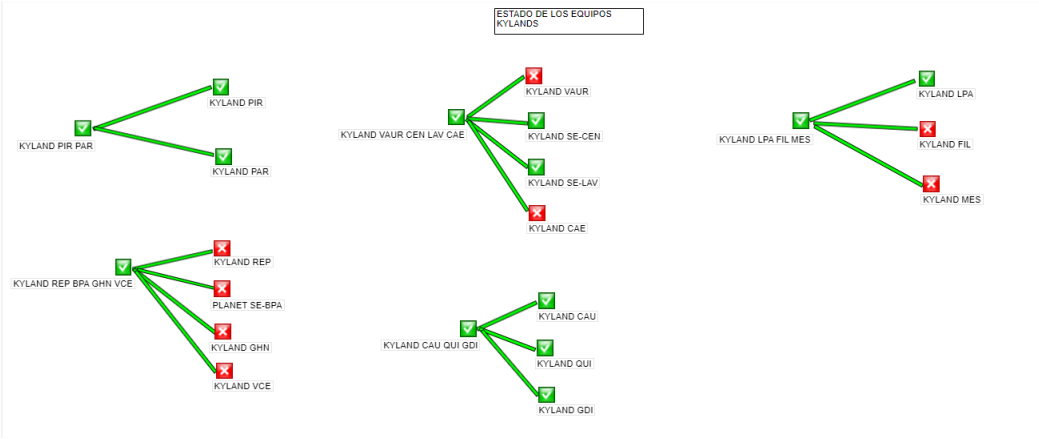

Figura 4: Vista creada a partir de complemento en el Sistema

4.2.7 Generación de reportes

El sistema puede generar reportes de los *hosts* y *services* monitoreados y el estado de la infraestructura en general con los mismos elementos gráficos o *dashlets* incluidos en la herramienta. Estos pueden ser

programados para su envió en intervalos definidos de tiempo vía correo electrónico. Los reportes son de gran utilidad a la hora de tomar decisiones y la evaluación del estado de la infraestructura OT de la institución.

4.3 Configuración del sistema de gestión de *logs* y datos de registro

Este segundo sistema al cual denominaremos Gestor está basado en la herramienta *open source* ElasticSearch, y tiene la capacidad de colectar, filtrar y analizar *logs* o registros de una variedad de dispositivos, como eventos de Windows, *syslogs* de Linux y dispositivos de red. En las secciones siguientes se trata el procedimiento para la integración de dispositivos y configuración de algunas funcionalidades implementadas en la herramienta.

4.3.1 Integración de *logs* de dispositivos.

La integración de dispositivos se efectúa siguiendo las recomendaciones brindadas por el fabricante del gestor. Para sistemas operativo Windows se precisa de la edición del archivo “nxlog.conf” en la ruta “C:\Program Files(x86)\nxlog\conf\nxlog.conf”, agregando un *script* el cual no se expone en este trabajo por cuestiones de practicidad. Para los dispositivos de red, el procedimiento varía según las indicaciones de cada fabricante, teniéndose que configurar manualmente cada uno. Para casos donde el puerto es distinto al definido en el gestor, la herramienta permite la configuración de nuevos puertos que sirvan para la entrada de registros (Configure < Global (All Instances) < Global Config)

Finalizadas las configuraciones de dispositivos, estos son integrados directamente al gestor sin necesidad de alguna configuración posterior. El gestor permite la creación de filtros personalizados para aplicar a los *logs* antes de su envío al ElasticSearch, esto permite descartar mensajes que no se desean indexar.

4.3.2 Análisis de *Logs*.

El gestor permite la creación de *dashboards* personalizados a través de un sistema de paneles, estos permiten el análisis de registros mediante *queries* y filtros, a través de la pestaña “Dashboards” de la plataforma.

Para la búsqueda de registros se debe definir el periodo de tiempo de análisis para luego hacer *queries* a través de entradas de texto, pudiéndose enlazar múltiples *queries* mediante el operador “+”. En la Figura 5 se observa un *dashboard* con tres *queries* (php, warning y apache), puede notarse en el gráfico como cada resultado es resaltado en un color diferente, los cuales pueden ser configurados en la interfaz. Todas estas configuraciones a su vez pu

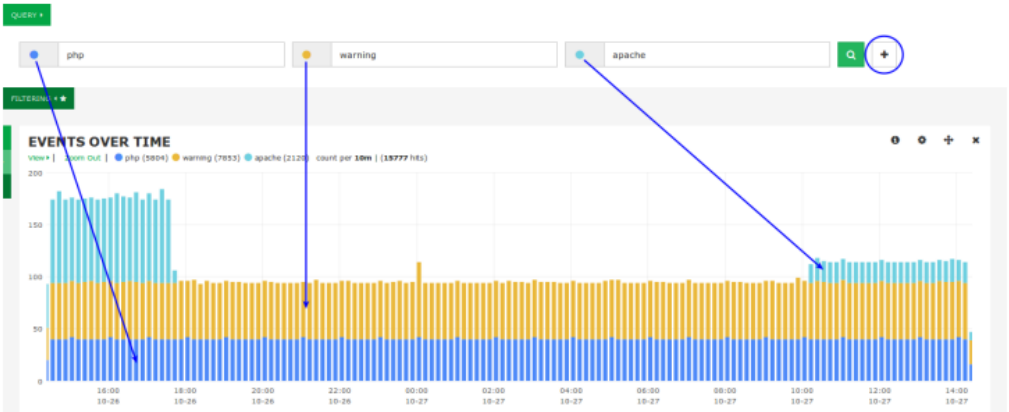

Figura 5: *Dashboard* con múltiples *queries* en el gestor

La herramienta permite la aplicación de filtros, cuya finalidad es parecida a los *queries* pero con el propósito de reducir el volumen de datos a analizar teniendo en cuenta la gran cantidad de *logs* almacenados.

4.3.3 Definición de Alertas

Las alertas configuradas pueden ser de tres tipos, *Query*, basado resultados de búsquedas previamente definidas en los *dashboards*, *Real-Time*, para alertas críticas en tiempo real y Host *Freshness* para host configurados que dejan de enviar registros. Estas se crean a través de la pestaña "Alerting" en la interfaz.

Existen múltiples métodos para el envío de alertas, siendo configurados en este trabajo los avisos vía email a los usuarios agregados, como las alertas NDRP para el envío al Sistema de monitoreo mencionado en la sección 3.1. La primera opción requiere la integración de un servidor de correo electrónico y la definición de un *template* para la alerta, mientras que el método NRDP se hace a través de un *token* entre ambas plataformas.

4.3.4 Reportes automatizados

Los reportes automatizados pueden ser en formato PDF, JPG o CSV y su configuración requiere definir la frecuencia de envío, correos a los cuales ser enviados, el asunto y cuerpo del mensaje. A diferencia del Sistema de Monitoreo, el registro de correos debe hacerse de forma manual.

4.4 Configuración del Sistema de Análisis de Flujo y Tráfico de Red.

Este sistema denominado de aquí en adelante colector permite el análisis de flujo de datos de una variedad de dispositivos, además de brindar una gran cantidad de herramientas como generación de *queries*, alertas, reportes, vistas. En esta sección hace una descripción general de las configuraciones para las funcionalidades implementadas para el monitoreo de tráfico de red OT de la ANDE. Esta herramienta puede ser integrada al Sistema de Monitoreo. sección 3.1, para que la última muestre información sobre el tráfico en su interfaz.

4.4.1 Integración de dispositivos

El flujo de red o *Network Flow* se refiere a paquetes con información referentes al tráfico de datos, como ser IP origen y destino, protocolo, puerto origen y destino, interfaz de ingreso, IP ToS. El uso de un *flow collector* como este sistema permite la evaluación y análisis de estos datos para obtener información acerca de lo que sucede en la red. El sistema soporta variedad de protocolos como ser Netflow, jFlow, cFlow, sflow, entre otros.

La configuración del envío de flujo de datos en los dispositivos varía de un proveedor a otro, incluso entre modelos de un mismo fabricante, por lo cual este proceso debe ser ejecutado mediante la bibliografía aportada de los proveedores. En caso de servidores es requerida la instalación de *exporters* encargados de esta tarea. En la plataforma la configuración consiste en la creación de un *Source* asociado al dispositivo con un nombre y puertos únicos, la dirección IP del dispositivo, el tipo de dato *flow* y el periodo de almacenamiento de la información en la herramienta, una vez finalizado el periodo definido en este último parámetro la información se comprime quedando solo datos mínimos como para la visualización en gráficos y otras tareas del colector, esto con la finalidad de optimizar el uso de espacio en disco. El colector permite la creación *Source Groups* para agrupar dispositivos con características similares, para su uso en el análisis y generación de reportes.

4.4.2 Análisis del Flujo de Datos

El colector permite el análisis del flujo de datos a través de *queries* personalizados, para esto debe ingresarse en la interfaz web al menú Sources < Queries. Mediante los *queries* puede filtrarse la información según parámetros como origen, destino, IP's y puertos, pudiendo hacer búsquedas múltiples enlazando los comandos a través de operadores lógicos para mejorar la granularidad de los datos. A su vez la herramienta permite fijar periodos de tiempo para el análisis de datos como hacer búsquedas de información a través de entrada de texto.

Los *queries* pueden ser ejecutados a un *source* en particular y *source groups* definidos, pueden ser guardados, editados y eliminados en la plataforma. En la Figura 6 se observa un *query* definido para un host en particular.

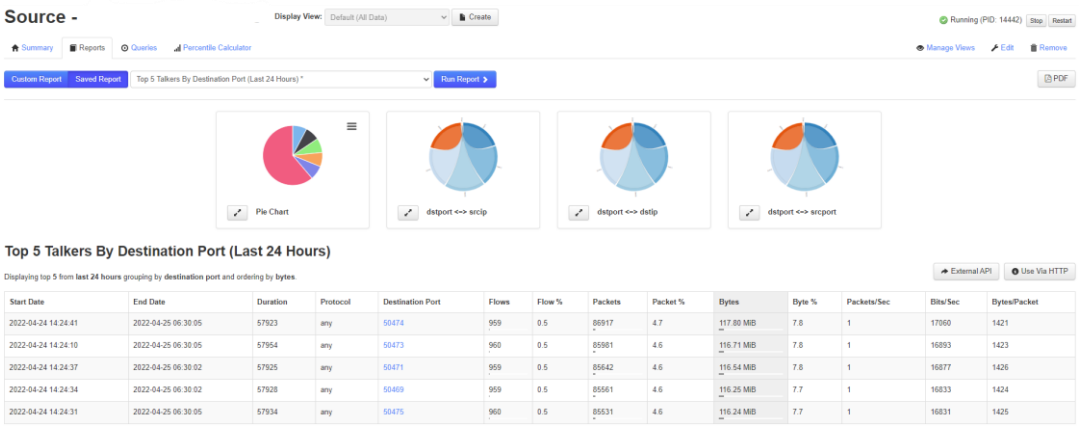

Figura 6: *Query* personalizado para host integrado en el sistema

4.4.3 Alertas y Notificaciones

La herramienta permite la configuración de alertas a través de su interfaz gráfica en la pestaña “Alerting”. En la implementación dada se utilizaron los métodos NRDP para la notificación al Sistema de Monitoreo y las alertas vía email. Deben configurarse a su vez los datos del *source* o *source group* a monitorear para la alerta, los *thresholds* para el criterio y el tipo de datos a analizar, ya sea paquetes, bytes, bit/sec o *flows.*

4.4.4 Reportes y Vistas

El sistema brinda la posibilidad de generar reportes a través de plantillas predefinidas o *queries* definidos por el usuario, los cuales pueden ser exportadas en formato PDF. Las vistas son una funcionalidad que permite el almacenamiento de la información granular del flujo de datos de manera prolongada, más allá del límite definido en la integración de los dispositivos. Para su creación basta con entrar en la pestaña “Views” donde se crea la vista definiendo el periodo de almacenamiento y el limitador el cual puede ser una IP o un puerto definido usando la misma sintaxis que los *queries*. Posteriormente es necesario asociar dicha vista a un *Source*.

4.5 Configuración del Sistema de visualización centralizada y creación de *dashboards*

Este sistema denominado de aquí en adelante como Visualizador permite la integración de las demás soluciones. Para el Sistema de Monitoreo en particular es requerido un usuario con privilegios de administrador y un *key* que permite la autenticación, en caso del Gestor de *Logs* basta con el *API key* para poder enlazar ambas herramientas.

4.5.1 *Dashboards* y Vistas.

El visualizador puede hacer uso de todas los *dashlets* o gráficos de cada sistema para poder ser integrados en una única vista personalizada por el usuario en la sección Home < Add Dashlets < Available Dashlets. También permite el uso de *dashlets* desarrollados por terceros siendo este material público compartido por diversos colaboradores en los foros del proveedor. Las vistas son conjuntos de *dashboards* los cuales pueden ser configuradas por cada usuario para su visualización en forma de paneles rotativos. En la Figura 7 se observa una los paneles que conforman una de las vistas configuradas en el sistema.

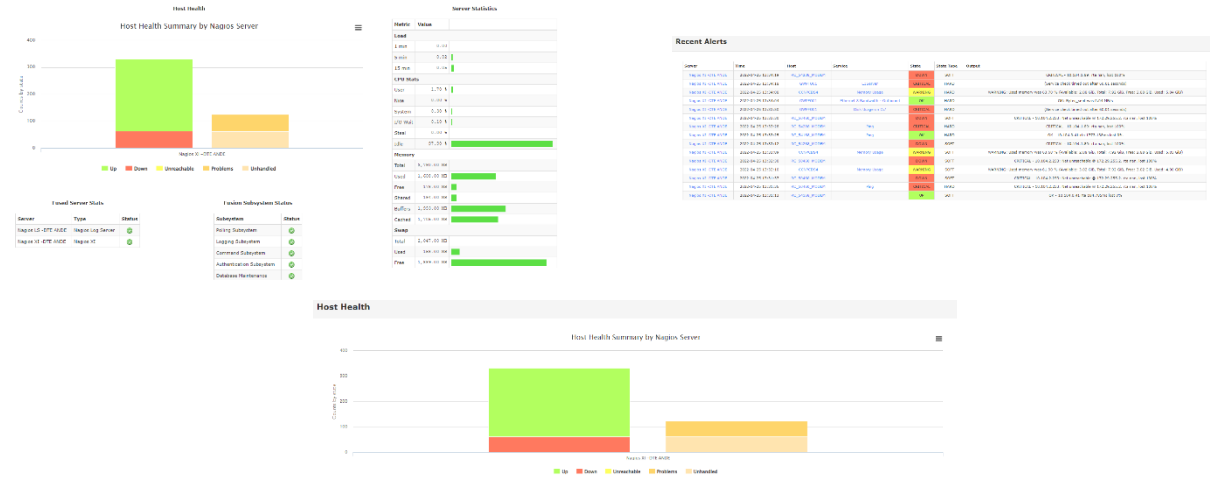

Figura 7: Vista con tres *dashboards* asociados en la plataforma

5. CONCLUSIONES Y TRABAJO FUTURO

Mediante la implementación del presente proyecto el cual involucró una gran cantidad de horas de trabajo se prevé que la ANDE cuente con las herramientas necesarias para un mejor control y monitoreo de toda la infraestructura OT siendo este uno los principales objetivos impulsados por la dirección de Telemática de la institución. Cabe mencionar que durante el proceso de implementación el cual requirió de la colaboración y conocimiento aportado por gran cantidad de funcionarios dependientes de diversas unidades, se dilucidó la necesidad de aplicación de las buenas prácticas recomendadas por el proveedor, al ser este un proceso iterativo y continuo basado bastante en la prueba y error hasta la obtención de un resultado óptimo pulcro.

Actualmente el proyecto sigue en etapa de soporte y mantenimiento, esto debido a la gran dimensión de la infraestructura de la red, aprovechando este proceso para la implementación de mejoras como la optimización de los mensajes vía Telegram, la creación de nuevos *dashboards* y vistas generadas de forma manual, y la creación de alertas y notificaciones más específicas que las ya implementadas.

6. BIBLIOGRAFÍA

[1] Piggin, R. “Industrial systems: cyber-security's new battlefront [Information Technology Operational Technology]”, Engineering & Technology, 2014, vol. 9, no 8, páginas 70-74.

[2] Hahn, A. “Operational technology and information technology in industrial control systems”. Cyber-security of SCADA and other industrial control systems. Springer, Cham, 2016. páginas 51-68.

[3] Nagios Enterprises. Nagios, The Industry Standard In IT Infrastructure Monitoring. Obtenido de Nagios, The Industry Standard In IT Infrastructure Monitoring: https://www.nagios.com/, 2022