RES - 2023 - 3367 - R # UNNE

VISTO:

El Expte 01-2023-04921 y

CONSIDERANDO:

Que en el marco del Programa "Sistema de Innovación Estratégica de la Universidad Nacional del Nordeste" y que siguiendo la misma línea de trabajo haciendo foco en en la innovación y modernización del sistema de monitoreo del backbone de la Red Informática Integral de la Universidad Nacional del Nordeste (RII UNNE) y de las distintas redes locales, la DGITI propone la implementación en los distintos "nodos" que conforman la RII UNNE de la herramienta del tipo software de red denominada Observiun, la cual actúa esencialmente como un "guardián virtual" colectando información de los equipo de red para la toma de decisiones.

Que la red Informática Integral de la UNNE está conformada por distintos nodos de red que vinculan al Rectorado con las distintas unidades académicas, institutos dependientes y los centros regionales en Corrientes y Chaco; utilizando tecnologías como fibra óptica, radio enlace, redes ethernet e inalámbricas, servicios punto a punto y "lantolan" entre otros;

Que el equipamiento que da soporte a la RII UNNE está conformado por hardware heterogéneo, multimarcas y que presenta una gran dispersión geográfica; donde la gestión de la misma requiere de herramientas adecuadas y un enfoque integral para garantizar una conectividad confiable en el mundo digital actual;

Que en el Instituto Rectorado, desde hace unos años, ya se viene utilizando la herramienta "Observium" para el monitoreo de los equipos de la red que conforman el backbone de la RII UNNE y la red local del Rectorado, equipamiento administrados centralmente desde la DGITI;

Que la misma ha resultado efectiva a la hora de detectar inconvenientes de distinto tipo relacionados con el funcionamiento de los equipos, el tráfico generado por cada uno de los dispositivos de red y sus interfaces de conexión y que, además, permite el almacenamiento de datos históricos y en tiempo real;

Que Observium resulta ser una herramienta esencial e indispensable para los administradores de redes porque permite monitorear, analizar, alertar y visualizar de manera integral lo que ocurre sobre los dispositivos, facilitando la gestión de los mismos;

Que resulta fundamental y necesario la implementación de un mecanismo de monitorización de redes moderno para las distintas redes locales de las unidades académicas e institutos dependientes cuya envergadura así lo requiera;

Que resulta conveniente para el logro del objetivo propuesto, designar a un responsable técnico que lleve a cabo el monitoreo y la gestión de los equipos de su unidad académica o instituto dependiente;

Que se deberá establecer un mecanismo que permita gestionar las incidencias detectadas y definir qué acciones deberán ser abordadas por el administrador de la red local;

Que desde la DGITI del Rectorado se llevarán adelante distintas instancias de capacitación y entrenamiento en el uso de la herramienta con el fin de lograr el mejor rendimiento de la misma para cada caso en particular;

Que la presente medida se toma en virtud de las atribuciones conferidas al suscripto por el artículo 24º del Estatuto de la Universidad Nacional del Nordeste;

Por ello:

EL RECTOR DE LA
UNIVERSIDAD NACIONAL DEL NORDESTE
RESUELVE:

ARTICULO 1º - APROBAR la implementación de la herramienta Observium para el monitoreo y gestión de la Red Informática Integral de la Universidad Nacional del Nordeste, con alcance a los distintos nodos que conforman la red.

ARTICULO 2º - INVITAR a las Unidades Académicas e Institutos dependientes de la Universidad a adherirse a la implementación del software de monitoreo de red para garantizar y mejorar el rendimiento de las redes locales.

ARTICULO 3° - SOLICITAR la designación de un responsable técnico de llevar adelante la gestión y el uso de la herramienta, personal que deberá estar en permanente contacto con el Dpto. de Redes y Comunicaciones de la DGITI del Rectorado.

ARTICULO 4° - COMUNICAR las incidencias o eventos detectados al Dpto. de Redes y Comunicaciones de la DGITI del Rectorado con el fin de abordar o planificar la mejor solución posible a lo acontecido o detectado por el administrador de la red local.

ARTICULO 5° - REGÍSTRESE, comuníquese y archívese.

CRA. ANALIA C. FALCON
SEC. GRAL. ADMINISTRATIVA

PROF. GERARDO OMAR LARROZA
RECTOR

Proyecto Despliegue de Monitoreo y Control de la RII UNNE

Contextualización

En un mundo hiperconectado y dependiente de la tecnología, la robustez y estabilidad de las redes son esenciales para el funcionamiento fluido de las organizaciones. En este escenario, la supervisión y gestión efectiva de la red se han convertido en pilares fundamentales.

A su vez, esta gestión ha ido adquiriendo cada vez mayor complejidad dado que lo que en un principio sólo estaba constituida por una red LAN y los enlaces WAN, en la actualidad las redes son más heterogéneas, enlazando sistemas de telecomunicaciones, equipos informáticos, Internet, servicios multimedia como videoconferencia, telefonía IP, las aplicaciones remotas y hasta las compras a través de medios electrónicos.

La Red Informática Integral de la UNNE está conformada por Campus Cabral, Roca, Medicina, Resistencia, también Rectorado e Institutos dependientes además por Centros Regionales en Corrientes como en Chaco. Utilizando tecnologías como fibra óptica, equipos de radio enlace, ethernet, redes inalámbricas, servicios LAN2LAN, etc. con hardware heterogéneo, multimarca y gran dispersión geográfica.

Por todo ello gestionar la RII UNNE es una tarea ardua, y hace indispensable contar con herramientas adecuadas para lograr estos objetivos.

La Trascendencia del Software de Monitoreo:

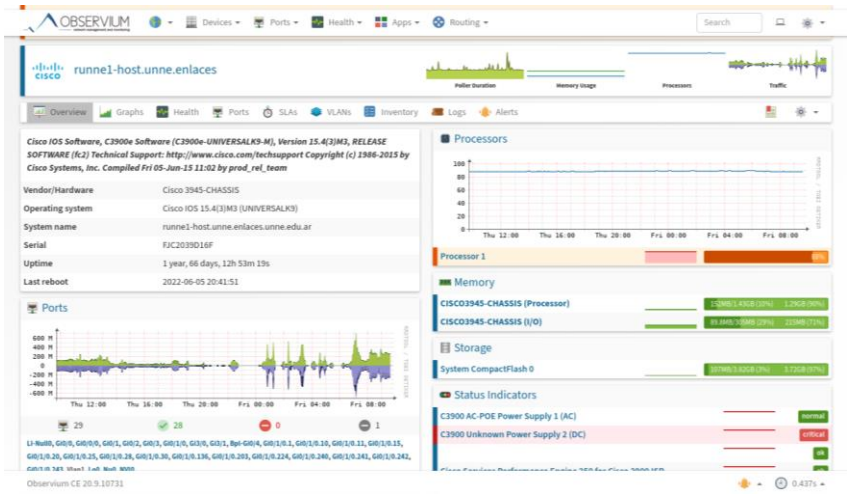
En un entorno donde la interconexión digital es el latido de la vida organizacional, mantener una red saludable es crucial. Los problemas de red no resueltos a tiempo pueden generar pérdidas económicas, caídas de productividad y, en última instancia, afectar la reputación de esta Universidad. Aquí es donde entra en juego el software de monitoreo de red, actuando como un "guardián virtual" que vigila constantemente la salud de la infraestructura de red y alerta sobre cualquier problema potencial antes de que cause un daño significativo.

Estas herramientas de software hacen posible prevenir y detectar problemas en la red con la mayor anticipación posible, buscando minimizar errores, y obtener un funcionamiento adecuado.

¿Por qué Observium?

Observium es una plataforma de monitoreo y gestión de red que proporciona información en tiempo real sobre la salud y el rendimiento de la red. Puede descubrir automáticamente dispositivos y servicios de red, recopilar métricas de rendimiento y generar alertas cuando se detectan problemas.

Desarrollado y mantenido profesionalmente por un equipo de ingenieros de red y administradores de sistemas experimentados.



Visualización de panel de un rúter.

Ventajas de Observium:

Observium, en este contexto, se presenta como una solución altamente efectiva. Su interfaz de usuario intuitiva y visual proporciona una representación en tiempo real del estado de la red, permitiendo a los administradores identificar de manera rápida y sencilla los puntos problemáticos y optimizar el rendimiento. Pero su alcance no se limita solo a su apariencia. Observium puede monitorizar una amplia gama de dispositivos y protocolos, abarcando desde equipos de red tradicionales hasta dispositivos inalámbricos y servidores, lo que lo convierte en una herramienta versátil para redes heterogéneas.

- **La Importancia de las Métricas y el Historial:**

Uno de los aspectos más valiosos de Observium radica en su capacidad para recopilar y almacenar meticulosamente métricas y datos históricos. Esta funcionalidad se vuelve esencial para la identificación de patrones de comportamiento y la anticipación de problemas potenciales. Al tener acceso a datos históricos, los administradores de red pueden realizar análisis de tendencias y pronósticos, permitiéndoles *tomar decisiones informadas* para optimizar la red a largo plazo y planificar la expansión de manera efectiva y elaborar estrategias de *recuperación ante desastres.*

- **Capacidades de Monitoreo Multimarca:**

Observium se destaca por su capacidad para monitorear equipos de diversas marcas y modelos. Esto es esencial debido a que la red está compuesta por una mezcla de dispositivos de diferentes proveedores. No importa si se trata de equipos Cisco, Juniper, HP o de otras marcas, Observium puede proporcionar una visión completa y unificada de todos estos dispositivos, simplificando aún más la gestión y el mantenimiento.

- **Visualización con Gráficos y Análisis:**

La capacidad de generar gráficos y visualizaciones claras es una ventaja adicional de Observium. Estos gráficos permiten a los administradores comprender rápidamente el rendimiento y el estado de la red, lo que facilita la identificación de *tendencias y patrones*. Cuenta con un sorprendente nivel de detalle y granularidad, se puede filtrar el historial por día y hora minutos y segundos.

Tráfico de interfaz

Esta visualización enriquece la toma de decisiones y ayuda al equipo del Depto. de Redes a comunicar información técnica de manera más efectiva a las partes interesadas no técnicas.

- **Alertas en Tiempo Real:**

El sistema de alertas automatizadas de Observium es otro aspecto que no debe pasarse por alto. Esta característica permite la configuración de umbrales y condiciones para generar alertas automáticas cuando se detectan anomalías, lo que posibilita una respuesta proactiva ante posibles problemas. Esta funcionalidad garantiza que los administradores estén informados de los problemas de manera instantánea, permitiéndoles tomar medidas inmediatas antes de que los usuarios finales se vean afectados.

- **Alertas Configuradas:**

A fin de estar al tanto de eventos críticos se configuraron distintas alertas que nos permite actuar en consecuencia y prevenir o minimizar caídas de servicio.

A continuación, se detallan las alertas más relevantes:

- **Equipo VoIP caído:** Nos alerta en caso de detectar la caída de un equipo VoIP, por ejemplo, una central PBX.
- **Equipo de red caído:** Es la más utilizada dada la cantidad de equipos de red administrados y el impacto que provoca una falla de este tipo.
- **Punto a punto inalámbrico caído:** Equipo punto a punto inalámbrico caído, su detección es de especial importancia por implicar la caída de toda la red del edificio que se encuentre del otro lado del radio enlace. Esto dispara acciones inmediatas para resolver el problema con la mayor celeridad.
- **Temperatura Crítica:** Se monitorean los sensores de temperatura de los equipos, es crucial detectar cuando se supera el umbral de temperatura crítica, esto nos permite tomar acciones para evitar la avería del dispositivo. Además, ante reiterados eventos de este tipo se toman medidas más preventivas, como revisión de forzadores o aire acondicionado del lugar.
- **Uso de Procesador:** Detecta elevado uso de Procesador en equipo de WiFi. Gracias a estos indicadores se detectó que esto provoca mal funcionamiento de las redes wifi por lo que se toman las medidas pertinentes para restaurar el funcionamiento óptimo.
- **Velocidad igual a 10 Mbps:** Se detecta cambio en la velocidad de la interfaz de red de equipos de radio enlace, si es inferior a lo esperado, provoca bajo rendimiento del enlace y problemas de transmisión.
- **Voltaje Entrada UPS:** Se monitorean los sensores de voltaje de entrada, indica corte de suministro cuando el voltaje es inferior al necesario y la UPS entra en modo batería. Contar con esta información nos permite accionar en función del tiempo de autonomía restante.

Caso de éxito: Detección de uso excesivo de red por parte de un dispositivo:

A modo de ejemplo de beneficios de este despliegue se detalla un caso ocurrido en la Facultad de Ciencias Exactas y Agrimensura de nuestra Universidad que permitió identificar situación de tráfico anormal.

En este sentido, los gráficos de ancho de banda logrados con Observium, mostraban un consumo de red muy por encima de lo normal en el Campus Roca. Esta nos llevó a ver en detalle los gráficos de los equipos involucrados hasta detectar que se trataba de un switch en el edificio de Física de FaCENA, concretamente la interfaz gi1/0/3, correspondiente a un servidor que se encontraba realizando tareas de investigación y necesitaba descargar desde internet grandes volúmenes de información, según pudimos averiguar con los responsables.

Por consiguiente, se coordinó para que esa actividad se haga por la noche y de esa manera no perjudicar a la red en horas pico.

Tráfico de interfaz en roc-swexafisicamdf.unne.enlaces

Conclusiones:

Gracias a la utilización de la plataforma de gestión Observium, es posible lograr una mejor calidad de servicio, dado que su sistema permite administrar una base de datos con todas las configuraciones de los equipos, pudiendo monitorizarlos gráficamente, detectar incidencias mediante el .aviso de alertas que se obtiene de los mensajes SNMP, cómo prevenir futuros fallos de red y actuar con la mayor brevedad posible.

Es una herramienta esencial e indispensable para los administradores de redes modernos. Su capacidad para monitorear, analizar, alertar y visualizar de manera integral convierte la compleja tarea de gestionar redes en una tarea más eficiente y efectiva. Al brindar información valiosa y en tiempo real sobre el estado de la red, Observium nos permite a los administradores *anticipar problemas, tomar decisiones informadas y mantener una conectividad confiable* en el mundo digital actual.

Con Observium, los administradores de red podemos estar seguros de que contamos con una herramienta poderosa y versátil para respaldar nuestra tarea crítica en la era de la conectividad ininterrumpida.

Plan de ejecución: despliegue de Observium en Unidades Académicas y dependencias

Dadas las características de la red, la cantidad de dispositivos, la cantidad de usuarios conectados, los servicios desplegados y la necesidad de brindar calidad y confiabilidad en toda la red de la universidad; se hace evidente lo indispensable de extender el alcance del monitoreo a todos los nodos.

Por tal motivo se prevé incorporar las UAs al monitoreo, para ello se definirán las etapas a seguir:

1. Determinación de alcance
2. Capacitación de Referentes Técnicos
3. Dar acceso a la herramienta
4. Definir equipos que se deben incorporar al monitoreo
5. Definir un plan de acción ante incidentes o eventos detectados
6. Definir un plan de recuperación ante desastres
7. Despliegue final.

1. Determinación de alcance

Será necesario dimensionar el escenario, de forma de poder determinar la infraestructura necesaria para cubrir las necesidades.

Como primer paso se identificarán las unidades académicas participantes y referentes técnicos de cada una de ellas. También el parque de equipos alcanzados.

Se hará una evaluación técnica sobre el tráfico SNMP que inundará la red, se tendrá que determinar si afectará el normal funcionamiento de la red y en tal caso se definirá topología alternativa para minimizarlo.

Luego se procederá a la configuración de la herramienta según las necesidades de cada unidad.

Es importante tener en cuenta el grado de injerencia y responsabilidad que deberán tener los referentes técnicos.

2. Capacitación de Referentes Técnicos

Se realizarán capacitaciones sobre Observium a los Referentes Técnicos a fin de impartir el conocimiento necesario para la implementación en cada nodo de la red.

Se dará una introducción a los conceptos de monitoreo de red y su importancia, con prácticas para familiarizarse con la herramienta.

Se abordarán paso a paso las diferentes secciones del software. Los parámetros a configurar en los distintos equipos.

Serán requeridos conocimientos mínimos sobre protocolo SNMP.

3. Dar acceso a la herramienta

Se crearán perfiles de usuario para cada UUAA, se definirán roles y responsabilidades.
Se establecerán políticas de acceso y permisos según los roles.

4. Definir equipos que se deben incorporar al monitoreo

En esta etapa se resolverá en conjunto con los RT las necesidades específicas de cada nodo, teniendo en cuenta su criticidad, necesidad de métrica e historial, etc.

Se solicitará un diagrama de topología con el cual se definirán las formas más adecuadas de incorporar los dispositivos a la monitorización, definiendo nomenclatura de nombres y asignación en DNS en los casos que sea necesario.

Una vez identificados los equipos a monitorear se establecerán los parámetros adecuados para ser configurados.

Seguidamente se dará lugar a la integración de estos dispositivos (routers, switches, servidores, etc.) en Observium.

Se establecerán umbrales y alertas para eventos anormales que deban ser reportados.

5. Definir un plan de acción ante incidentes detectados

Para cada tipo de alerta se debe definir un plan de acción a ser llevado a cabo, teniendo en cuenta actores y recursos. Debe ser claro y preciso.

El plan consta de pasos a seguir luego de que se toma conocimiento del incidente,
Se elaborarán protocolos de respuesta a incidentes, definiendo niveles de gravedad y necesidad de escalado.

Será necesario definir el rol de cada administrador en respuesta a incidencias o eventos.

6. Definir un plan de recuperación ante desastres

Un escenario de desastre o catástrofe para una infraestructura de red se refiere a situaciones extremas o eventos inesperados que pueden causar daños significativos o interrupciones en la operación de la red, que pueden tener un impacto significativo en la disponibilidad y funcionalidad de la red.

Para mitigar estos riesgos, es necesario implementar planes de recuperación ante desastres y medidas de seguridad para proteger la infraestructura de red y garantizar la continuidad de las operaciones en caso de que ocurra alguno de estos eventos catastróficos.

Los escenarios de catástrofes pueden incluir: desastres naturales, ataques cibernéticos masivos, fallos de hardware o software, cortes de energía prolongados, errores humanos, fallos de proveedores de servicios, ataques físicos, sabotaje o el vandalismo, etc.

Ante una catástrofe se debe actuar de inmediato, por lo cual es de vital importancia contar con un plan bien elaborado que asegure la mitigación en el plazo más corto posible.
Se diseñará un plan de contingencia para situaciones de emergencia identificando escenarios de catástrofe y acciones a tomar.

Se determinará en qué casos se deben reemplazar equipos o restaurar configuraciones.

7. Despliegue final

Al concluirse la integración de todas las unidades académicas se harán pruebas y validaciones en busca de determinar, en primer lugar, el comportamiento de la herramienta en distintos escenarios, en segundo lugar, efectividad de las alertas y notificaciones.

Se harán los ajustes finales que sean necesarios.

8. Plan de trabajo:

En síntesis, de lo expuesto es importante resaltar que se definirán actualizaciones y capacitaciones constantes a lo largo del ciclo de vida de Observium.

Como se ha manifestado, la implementación de Observium en las Unidades Académicas permitirá una gestión eficiente de la infraestructura de red, la detección temprana de problemas y la respuesta rápida a incidentes.

En este sentido, el proyecto busca asegurar la estabilidad y disponibilidad de la red universitaria, así como garantizar la preparación para enfrentar situaciones críticas en relación con las actividades que se están llevando a cabo respecto de la seguridad de la información.

Comentario [1]: Desastres naturales, Ataques cibernéticos masivos, Fallos de hardware o software
Cortes de energía prolongados, Errores humanos, Fallos de proveedores de servicios, Ataques físicos, sabotaje o el vandalismo

Desastres naturales: Eventos como terremotos, inundaciones, huracanes, tornados, incendios forestales y tsunamis pueden dañar infraestructuras físicas, como cables de fibra óptica, torres de comunicación y centros de datos, lo que lleva a la interrupción de la red.

Ataques cibernéticos masivos: Los ataques cibernéticos a gran escala, como ataques distribuidos de denegación de servicio (DDoS) o ataques de ransomware, pueden sobrecargar o comprometer la infraestructura de red, causando interrupciones importantes.

Fallos de hardware o software: Los fallos inesperados en los componentes de red, como routers, switches, servidores o sistemas de gestión, pueden resultar en interrupciones en la red.

Cortes de energía prolongados: La falta de suministro eléctrico a largo plazo puede afectar negativamente a los equipos de red y a los centros de datos, lo que provoca la caída de la red.

Errores humanos: Los errores cometidos por personal de operaciones o mantenimiento de la red pueden tener consecuencias graves, como la configuración incorrecta de dispositivos, la eliminación accidental de datos o la exposición de información sensible.

Fallos de proveedores de servicios: Si un proveedor de servicios de Internet o un proveedor de servicios de nube experimenta una interrupción en sus operaciones, esto puede afectar a las redes que dependen de sus servicios.

Ataques físicos: La sabotaje o el vandalismo dirigido a la infraestructura de red, como la destrucción de cables o equipos, puede interrumpir la conectividad.

Epidemias o pandemias: Eventos como una epidemia o pandemia pueden llevar a la falta de personal necesario para mantener y operar la ...

El compromiso de los Referentes Técnicos y la formación constante serán fundamentales para el éxito y la sostenibilidad de esta iniciativa.

A continuación, se presenta el plan de trabajo inicial para lograr el despliegue necesario para el monitoreo y control de la herramienta en toda la RII UNNE, dado que el seguimiento y el uso de la herramienta es un ejercicio que se debe mantener constante a través del tiempo.

				oct-23				nov-23				dic-23			
etapa	Proyecto	Actividad	Responsable	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
(*)	**Monitoreo y Gestion - Redes locales**														
1	Determinación de alcance	Relevamiento red cableada y Wifi	Tecnico UA												
2	Capacitacion de Referentes Técnicos	Capacitaciòn en el uso de la herramienta	DGITI Retorado												
3	Dar acceso a la herramienta	Configuracion de usuarios y privilegios de acceso	DGITI Retorado												
4	Definir equipos que se deben incorporar al monitoreo	Elegir que equipos de red se incorporan al monitoreo	Tecnico UA/DGITI Rectorado												
5	Definir un plan de acción ante incidentes o eventos detectados	Definir mecanismo de reporte de eventos detectados o sufridos	Tecnico UA/DGITI Rectorado												
6	Definir un plan de recuperación ante desastres	Definir mecanismo de restauraciòn del equipo o servicio afectado	Tecnico UA/DGITI Rectorado												
7	Despliegue final.	Ajustar y verificar da uno de los entornos de trabajo de los RT de facukltad	Tecnico UA/DGITI Rectorado												

	Referencias
S1	Primer Semana
S2	Segunda Semana
S3	Tercer Semana
S4	Cuarta Semana

Hoja de firmas

Sistema: ARAI-Documentos
Firmado por: UNNE Sudocu
Fecha: 29/09/2023 12:18:50
Razon: Cargado por SIU-Documentos

Sistema: ARAI-Documentos
Firmado por: UNNE Sudocu
Fecha: 02/10/2023 19:00:54
Razon: Autorizado por ANALIA C. FALCON BOISSIERE

Sistema: ARAI-Documentos
Firmado por: UNNE Sudocu
Fecha: 03/10/2023 07:51:42
Razon: Autorizado por GERARDO OMAR LARROZA