UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

TRABAJO DE INVESTIGACIÓN

IMPLEMENTACIÓN DE UN SISTEMA WEB DE MONITOREO PARA MEJORAR EL CONTROL DE LOS SERVICIOS DEL NUEVO CORE BANCARIO – LIMA 2022

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

AUTOR:

RIOS OSNAYO PEDRO ALEJANDRO
CÓDIGO ORCID: 0000-0003-1820-9200

ASESOR: Mg.

AGUILAR MONTERREY SEGUNDO FREDDY
CÓDIGO ORCID: 0000-0002-7208-4878

LÍNEA DE INVESTIGACIÓN: INTELIGENCIA ARTIFICIAL Y GESTIÓN DE LA INFORMACIÓN

LIMA, PERÚ

JUNIO, 2022

RESUMEN

Luego de la implementación del nuevo Core Bancario “Bantotal” en la Financiera, pasamos de un sistema nivel escritorio a un sistema de entorno web, uno de los principales objetivos es el buen desempeño de la plataforma en toda la red de agencias a nivel nacional. Los recursos que demanda el nuevo segmento bancario en el Perú nos han llevado a ampliar enormemente la infraestructura de los servidores principales para este nuevo entorno web, teniendo así múltiples fuentes de datos distribuidos en todo el ecosistema bancario.

Con el nuevo sistema Core se necesita tener fluides al momento de la atención tanto en horario operativo para no presentar lentitudes, encolamientos o caídas en el flujo de la atención, como también en el proceso de cierre de oficina y mantener activos los servicios principales enlazados con los proveedores.

La siguiente investigación tiene como objetivo presentar una herramienta que nos permita enlazar, almacenar de una forma distribuida millones de eventos que ocurren en cada servidor para poder procesarlos, el control de estados de los servicios tomcat y procser en Linux, saturación del procesador nodo por nodo para todo el Clúster de la empresa, lectura de sentencias con mayor tiempo en conexión a la base de datos y hacer que todo esto se conviertan en gráficos dinámicos para su monitoreo constante ante cualquier incidencia presentada.

Es por ello por lo que se presenta la implementación del empaquetado Elastick Stack, donde podremos realizar lo mencionado y mejorar el tiempo de atención ante problemáticas que podrían ocurrir.

Palabras clave: Core Bancario, Bantotal, Tomcat, Procser, Elastick Stack

ABSTRACT

After the implementation of the new Banking Core "Bantotal" in the Financial, it went from a desktop system to a web environment system, one of the main objectives is the good performance of the platform in the entire network of agencies nationwide.

The resources demanded by the new banking segment in Peru have led us to expand and improve the infrastructure of the main servers for this new web environment, thus having multiple sources of data distributed throughout the banking ecosystem.

With the new Core system, it is necessary to have fluids at the time of service both during operating hours so as not to present slowness, queuing or falls in the flow of service, as well as in the process of closing the office and keeping the main services linked with Providers.

The following research aims to present a tool that allows us to link, store in a distributed way millions of events that occur in each server to be able to process them, the state control of tomcat and procser services in Linux, node-by-node processor saturation for the entire cluster of the company, reading sentences with more time in connection to the database and turning all this into dynamic graphics for constant monitoring in the event of any incident presented.

That is why the implementation of the Elastick Stack packaging is presented, where we can do the aforementioned and improve the time of attention to problems that could occur.

Keywords: Cire Banking, Bantotal, Tomcat, Procser, Elastick Stack

Tabla de Contenidos

RESUMEN 3
ABSTRACT 4
TABLA DE FIGURAS 6
1. INTRODUCCION 7
2. ANTECEDENTE NACIOANLES E INTERNACIONALES 8
2.1 ANTECEDENTES NACIONALES 8
2.2 ANTECEDENTES INTERNACIONALES 10
2. BASES TEORICAS 13
a. ELASTIC STACK 13
b. LOGSTASH 14
c. ELASTICSEARCH 15
d. KIBANA 16
3. DESARROLLO DEL TEMA 17
4. DESCRIPCION DE LA REALIDAD PROBLEMÁTICA 11
5. OBJETIVOS DE LA INVESTIGACIÓN 12
a. Objetivos General 13
b. Objetivos Específicos 13
6. JUSTIFICACIÓN 13
7. CONCLUSIONES 14
8. APORTE DE LA INVESTIGACION 15
9. RECOMENDACIONES 16
10. REFERENCIAS 17

TABLA DE FIGURAS

Figura 1 – Arquitectura Elastic Stack

Figura 2 – Estructura Logstash

Figura 3 – Plataforma Kibana

Figura 4 – Grafico de medición del CPU en KIBANA

Figura 5 – Medición de conexiones para los servicios

Figura 6 – Medición de tiempo de respuesta para los servicios

1. INTRODUCCION

El mundo de la informática y las telecomunicaciones ha crecido muy grande en la última década y una de las implicaciones más inmediatas es el incremento de dispositivos, aplicación y servicios en miles de sectores, esto implica que hoy en día independiente del sector que trabajemos tendremos aplicaciones y servicios, diferentes arquitecturas de redes, dispositivos fijos o móviles y desde hace menos años las redes sociales se han acoplado en nuestra sociedad, algo que tienen en común todos estos sectores es que soportan información, generan log de su funcionamiento, muestran el estado actual de sí mismo como es el estado de monitorización dentro de los equipos, antiguamente la cantidad dispositivos y eventos que estos generaban se podrían tratar mediante otros métodos, pero en esta última década han crecido de una forma exponencial el número de ellos y la cantidad de log y eventos que generan, esto provoca que los métodos usados para la gestión de sus log no valgan hoy en día, ya sea por problemas en el almacenamiento de tales cantidades de información o la dificultad de procesarlo.

En la actualidad en el sistema financiero una de las principales misiones es el buen servicio tecnológico en performance que se presenta para los clientes, tanto como plataformas web donde se brinda el flujo desde el registro de datos de un cliente hasta el desembolso de un crédito y/o apertura de cuentas de ahorros, la financiera a adquirido un nuevo Core bancario que apunta a la fluides en la atención, esto conlleva a diversos servicios que componen dicha plataforma web, el cual debe ser monitoreado al milímetro para garantizar el correcto funcionamiento en las sucursales a nivel nacional.

2. ANTECEDENTE NACIOANLES E INTERNACIONALES

2.1 ANTECEDENTES NACIONALES

Navarro, J (2022) en su tesis titulada "Seguimiento y Monitoreo de los Diagnósticos Técnicos Legales Mediante un Sistema Web en COFOPRI"; plantea como objetivo principal que la oficina zonal Lima Callao del Organismo de Formalización de la Propiedad Informal no cuenta con un sistema adecuado de seguimiento y monitoreo de los diagnósticos técnicos legales y hacerlo mediante la hoja de cálculo de Microsoft Excel 2013, ocasiona un problema, que se tratará en la presente investigación. El tipo de la investigación es aplicada, el nivel es explicativo y el diseño es pre experimental, la muestra está conformada por 72 seguimientos, el resultado, de acuerdo al método científico demuestra como la implementación del sistema web mejorará el seguimiento y monitoreo de los diagnósticos técnicos legales. El sistema web SMDIAG, registrará las actividades de los diagnósticos técnicos legales, emitirá reportes y mostrará consultas, por consiguiente, mejorará el seguimiento y monitoreo de los diagnósticos técnicos legales en la Oficina Zonal Lima Callao del Organismo de Formalización de la Propiedad Informal (COFOPRI). Para la construcción del software SMDIAG, se desarrolló mediante la metodología Scrum, se utilizó herramientas como Git, Git Bash, Visual Studio Code, Angular, TypeScript, Node.js, Strapi, GraphQL, MongoDB.

Gerónimo, M (2021) en su tesis titulada "Aplicativo web para el monitoreo del Data Center en la Institución Educativa Senati, Sede Independencia", plantea como objetivo el desarrollo de un aplicativo web para el monitoreo del data center en la institución educativa SENATI, sede Independencia, ya que la situación de la organización antes de la

implementación del aplicativo web presentaba deficiencias en cuanto el control de monitoreo que nos permitía saber el estado de los dispositivos de comunicaciones y servidores que a su vez les dificultaba y demoraba en conocer el status actual. El objetivo de esta investigación fue determinar el efecto del uso de un aplicativo web para el monitoreo de la data center en la institución educativa SENATI. Por ello, en la presente tesis, se describió los aspectos teóricos del nivel de disponibilidad del centro de datos, además de la metodología a utilizar para el desarrollo del software del aplicativo web, en este caso la metodología adoptada fue la de Scrum, ya que fue la que más se acomodó a las necesidades de etapas del proyecto. La presente investigación fue de tipo aplicada, de diseño pre- experimental y de enfoque cuantitativo. Se contó con una población de 275 incidencias para el indicador de eficiencia en la disponibilidad y 275 incidencias para el indicador de ratio de resolución de incidencias, los cuales fueron estratificados según fechas en 28 agrupaciones. El muestreo fue probabilístico aleatorio simple. La técnica de recolección de datos fue el fichaje y su instrumento fue la ficha de registro, los cuales fueron validadas por tres expertos. La implementación del aplicativo web para el monitoreo de la data center en la institución, permitió aumentar la eficiencia en la disponibilidad (ED) de un valor de 53, a un valor de 84. A su vez aumentar ratio de resolución de incidencias (RRI) de un valor de 43, a un valor de 77. Los resultados mencionados permitieron llegar a la conclusión de que el aplicativo web influye en la mejora para el monitoreo de la data center en la institución educativa SENATI.

2.2 ANTECEDENTES INTERNACIONALES

Zavala, B (2022) en su tesis titulada “Aplicación Web para el monitoreo de proyectos de Investigación UNAMBA 2018”, plantea como objetivo mejorar el proceso de monitoreo de los proyectos de investigación producidos en la UNAMBA haciendo uso de una aplicación web, la cual fue implementada bajo el subdominio que administra la Universidad: https://observatorio.unamba.edu.pe (Observatorio de Investigación). Las problemáticas que se encontraron con respecto al monitoreo de proyectos de investigación, era que Vicerrectorado de Investigación “carecía de información sobre el avance y/o estado de los proyectos de tesis de pregrado puesto que esta información era manejada en cada escuela profesional y/o facultad; así mismo, el registro de proyectos de investigación docente se llevaba a cabo a través de documentos Excel, lo cual dificulta mantener una data actualizada sobre el estado y/o avance de los proyectos de investigación docente.” La aplicación web fue desarrollada principalmente con tecnologías como: Laravel, uno de los framework de backend PHP más utilizados actualmente, capaz de facilitar un desarrollo ordenado, modular, seguro y escalable. Vue.js, framework de frontend basado en javascript que asegura la escalabilidad a través de su enfoque progresivo y la orientación al uso de web components. Finalmente es debido mencionar la implementación de métodos de autentificación de usuarios a través de los servicios de Google, Microsoft y Github que facilitan la autentificación y un mayor nivel de seguridad con el uso de un doble factor de autentificación. Luego de haber aplicado este proyecto de investigación, se cumplió satisfactoriamente con los requisitos establecidos en la resolución Nº 0054-2017-SUNEDU en su condición IV. “Líneas de investigación a ser desarrolladas” ítems IV.2 y IV.3 de suma importancia tal como se corroboran en la resolución N° 002-2021-VRIN-UNAMBA (Anexo

07); de igual manera se solucionó los problemas anteriormente mencionados. El Vicerrectorado de Investigación ya cuenta con una herramienta estratégica capaz de facilitar la actualización de la data, la obtención de información del estado y/o avance de los proyectos de tesis de pregrado e investigaciones docente y la facilidad de accesibilidad a la información. Como información concluyente, tras la aplicación de la presente tesis, se determinó que se ha podido mejorar el monitoreo de los proyectos de investigación docente y tesis de pregrado en más del 50%.

Araya, D (2021) en su tesis titulada "Sistema de monitoreo y análisis del mercado laboral para el Sence" planea como objetivo que la investigación SENCE es una entidad gubernamental encargada de apoyar el mercado laboral en Chile, a través de cursos y capacitaciones a los trabajadores. A través de ellas estas personas adquieren o mejoran sus competencias, particularmente aquellas que se consideren relevantes en el mercado. Para decidir la forma y las temáticas que abordarán estas capacitaciones, SENCE monitorea el mercado laboral, y para ello se basa en diversas fuentes de información tales como encuestas y publicaciones concernientes a dicho mercado. El principal problema que tiene ese mecanismo de recopilación de datos, es que las fuentes de información mencionadas son actualizadas de forma esporádica, y la frecuencia de actualización es más baja que la requerida. Por lo tanto, éstas generan un perfil (o diagnóstico) poco actualizado del estado del mercado laboral. Debido a eso, anualmente se desarrollan capacitaciones que pueden no ser las más adecuadas para los trabajadores, ni las que necesita el país. Para paliar este problema, SENCE desea basar sus decisiones en fuentes con datos más estables, actualizadas y confiables en el tiempo. Por esa razón, se firmaron convenios con plataformas \textit{on-line} de ofertas de empleo (por ejemplo, Trabajando.com, Laborum.cl, etc.) para obtener los

datos que se publican e ingresan en estos sitios (información actualizada mensualmente), tanto de las ofertas publicadas como de los candidatos y las postulaciones que estos realizan. El presente trabajo de título tiene como objetivo diseñar y construir una herramienta de software que permita a SENCE monitorear el mercado laboral de mejor manera (mediante visualizaciones adecuadas), a partir de datos más actualizados. La información utilizada para realizar este monitoreo se obtiene desde sitios web de ofertas de empleo. La solución construida consistió en una aplicación web que muestra visualmente distintos indicadores definidos por SENCE, que le permiten perfilar y entender la situación puntual del mercado laboral. El software también hace que los indicadores se actualicen periódicamente y de forma automática, desde las fuentes de datos (plataformas web de ofertas de empleo). La aplicación obtenida es extensible y multiplataforma, y permite visualizar de manera gráfica los distintos indicadores que fueron señalados y discutidos como relevantes para SENCE. Esta aplicación fue evaluada por un grupo de cuatro funcionarios del SENCE, mediante la aplicación de pruebas que permitieron determinar la usabilidad y utilidad de la solución. Los resultados obtenidos a partir de estas pruebas muestran que, en términos de usabilidad los usuarios hallaron la herramienta usable y buena. Sin embargo, se hicieron algunos reparos hacia la utilidad de la aplicación, pues, aunque fue calificada como “útil”, claramente es aún un prototipo que se deberá seguir extendiendo a futuro. Tal como se planificó al inicio de esta memoria, la versión actual del sistema representa una prueba de concepto para SENCE, y permite establecer las bases para las siguientes versiones de la aplicación.

2. BASES TEORICAS

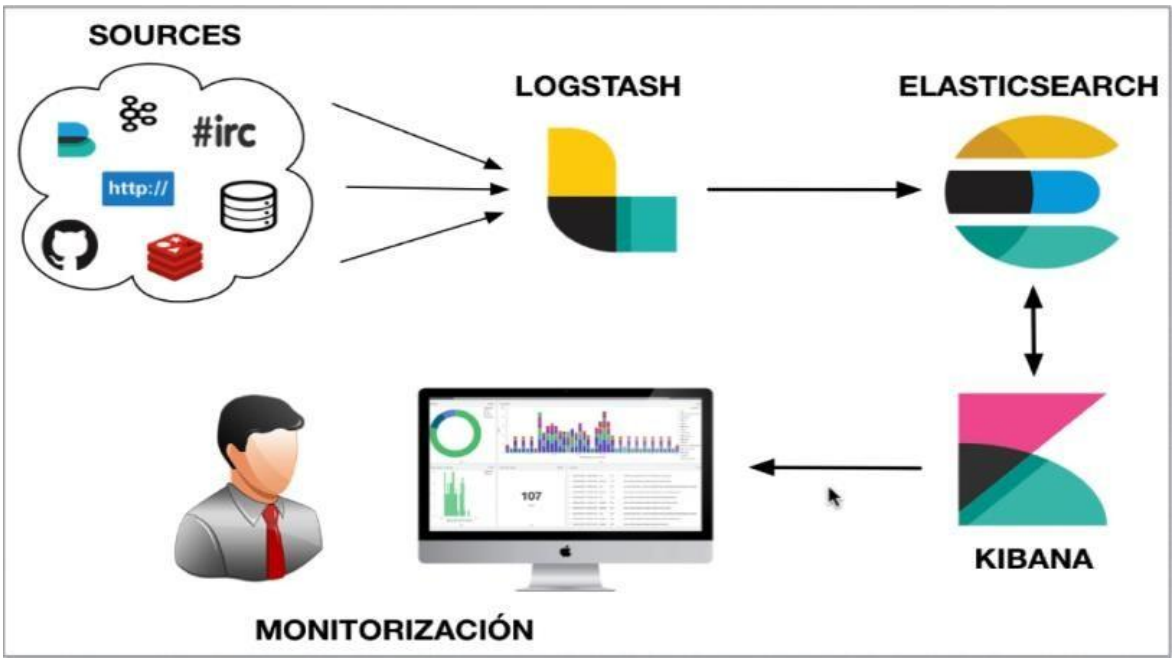
a. ELASTIC STACK

Según Pestaña, D (2021) Elastick Stack es un conjunto de componentes en código abierto: ElasticSearch, Logtash y Kibana, que a sido desarrollado y es administrador en la actualidad por la empresa Elastic.

La implementación de estos 3 componentes nos permitirá gestionar log o registros, un almacenamiento distribuido en estructura de datos, el procesamiento y finalizará con la visualización de Dashboard.

Esto nos dará un amplio panorama para la monitorización en tiempo real, para ser analizado, identificar y resolver los errores presentados en las aplicaciones y sistemas, como ejemplo visualizar el número de error de un aplicativo web, saturaciones del CPU o Memoria RAM en un servidor.

Figura 1 – Arquitectura Elastic Stack



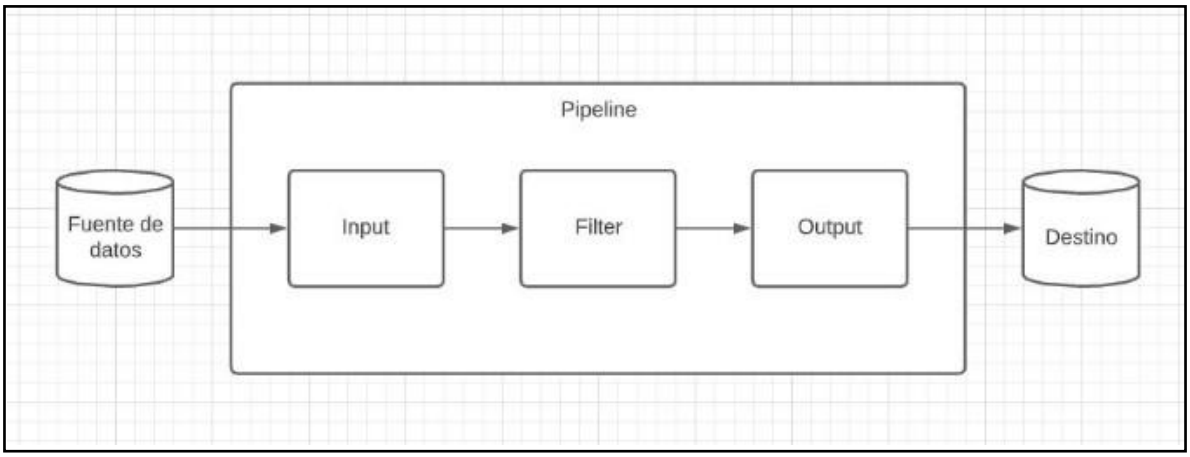
b. LOGSTASH

Según Sergio, D (2020) Logstash es una herramienta que nos permite la recolección de información, normalizarla y centralizarla en diferentes medios.

Logstash contempla un paso denominado “pipeline” que es básicamente un proceso ETL con tres principales etapas, la primera etapa nos da la facilidad de recoger datos de múltiples fuentes (inputs), para luego proceder a su tratamiento de datos (filters) y finalizar con la distribución en múltiples plataformas (outputs) según se describe:

- Inputs: Es la etapa que cuenta con una variedad de plugins que nos permitirá la recolección de eventos en diferentes orígenes de datos.
- Filters: Llegando a esta etapa donde aplicaremos la transformación necesaria y filtros de datos según nuestro criterio y/o necesidad requerida.
- Output: Esta es la última etapa donde podremos adaptar la estructura según sea el requerimiento del sistema al que llevaremos.

Figura 2 – Estructura Logstash



c. ELASTICSEARCH

Según Cuervo, V (2019) Elasticsearch es considerado un motor de búsqueda que nos permite encontrar y analizar datos complejos en una gran cantidad de texto. Es una de las herramientas más escalables que existe en la actualidad para motores de búsqueda, por lo cual nos permite almacenar, encontrar y analizar mucho volumen de datos.

El desarrollo de ElasticSearch está basado la librería de Apache Lucene y que el código fuente de su motor está en lenguaje Java que nos permite búsquedas en tipo texto, autocompletado y geolocalización, su modelo de desarrollo es OPEN SOURCE.

Como parte de su desarrollo algunas de esta base de datos entidad-relación implementaron en su contenido la utilidad llamada “full search text” para el caso que almacenan gran cantidad de datos en tipo texto, permita buscar algo especifico como una cadena de texto.

ElasticSearch es una base de datos NOSQL que esta orientado a tipos de documentos JSON, algo similar a Mongo DB, esto nos da oportunidad de no definir esquemas en lo que se va insertando datos.

Esta herramienta como base de datos distribuida, nos permite la escalabilidad dinámica en forma horizontal, por lo cual si tenemos más demanda de datos podemos crecer en nodos y así llegar a amanecer hasta petabytes de datos.

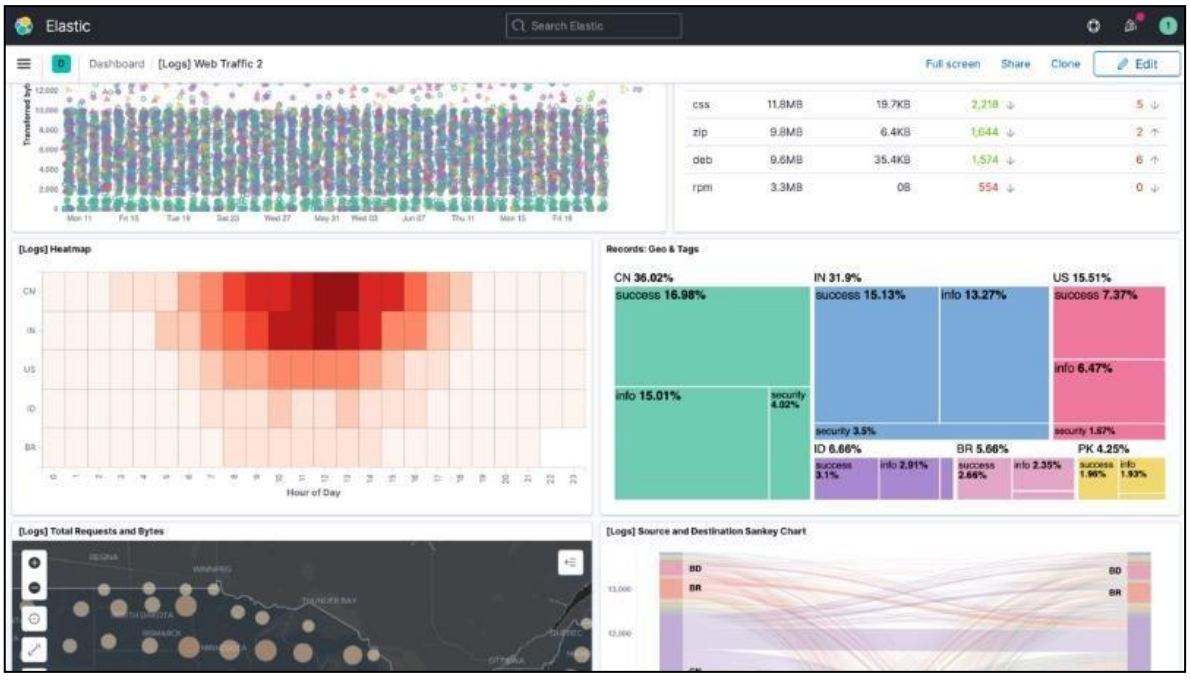
d. KIBANA

De acuerdo con Echarrotti, C (2015) es una plataforma open-source que pertenece a Elastic, dicha herramienta nos permitirá visualizar y explotar los datos que nos brindará la herramienta ElasticSearch.

Kibana es una plataforma FrondEnd, esto nos permitirá la visualización de datos, analizar preparar y crear entornos o reportes acorde a la necesidad de cada empresa, cuenta con múltiples gráficos como Tablas, histogramas, circulares y mapas adaptando a cada log indexado

Esta herramienta actuara directamente como la interfaz del usuario final es aquí donde realizara el monitoreo y análisis de esta.

Figura 2 – Plataforma KIBANA



+

3. DESARROLLO DEL TEMA

Teniendo en cuenta la arquitectura actual de la financiera contando con 2 Cluster principales distribuidos en 8 nodos, 4 nodos BackEnd y 4 nodos FrondEnd con 16 Instancias de Tomcat y 8 instancias de procser.

Cada instancia que son en total 24 nos brinda un “log” especifico de lo que ocurre cada segundo en dicho servidor es por ello que se busca segmentar todos los logs y tener una visualización en vivo de lo que ocurre en el Core.

El nivel de la presente investigación tiene como nivel descriptiva y experimental.

Descriptiva: Se procederá a describir todas las características de mayor impacto ante la gestión y lectura de los eventos en múltiples plataformas.

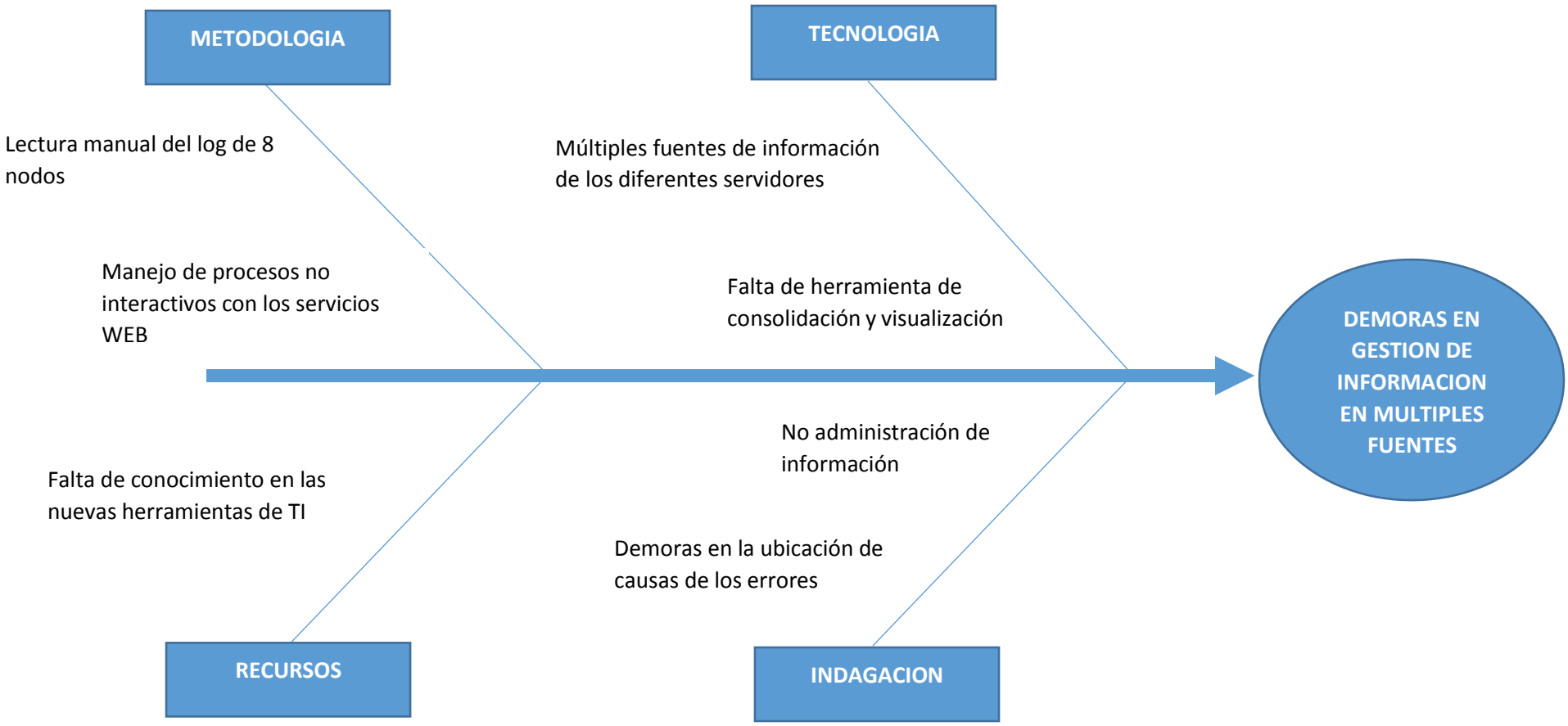
Experimental: El contenido presentado nos permitirá controlar y a su vez observar el comportamiento de todos los métodos presentados para la implementación.

- Las técnicas que se emplean para la presentación de la implementación son:
- Observación directa
- Carácter espontaneo
- Personal
- Observación Indirecta
- Verificación de documentos laborales
- Consulta de informes de adecuación de sistemas

Algunos de los instrumentos que se están empleando para la presente investigación son los siguientes:

- Documentos de proveedores
- Reporte de incidentes
- Notas
- Grabación de Capacitaciones

Con el fin de poder tener claro la causa de la problemática, se propone el siguiente diagrama de Ishikawa.



Nota: "La figura muestra los problemas que se tienen en la gestión de la información de los nodos del nuevo Core". Fuente Propia

Teniendo en cuenta en el diagrama de Ishikawa, se procede a profundizar cada punto que provoca la dificultad de visualización de la información de cada servidor.

Tecnología:

- Múltiples fuentes de información de los diferentes servidores, al contar con muchos nodos que contemplan el ecosistema bancario, se tiene mucha data para su lectura en tiempo real.
- Falta de herramienta de consolidación y visualización, no se cuenta con herramientas de última tecnología que facilite la lectura de log al presentarse una incidencia.

Metodología:

- Lectura manual de log de 8 nodos, se realiza una lectura por cada archivo log en particular ingresando a nodo por nodo para encontrar la causa del problema.
- Manejo de procesos obsoletos, la lectura manual de cada log es un proceso muy obsoleto que se usa para encontrar la raíz de la problemática.

Recursos:

- Falta de capacitación continua en las nuevas herramientas de TI, se necesita la capacitación constante en cuanto a las nuevas herramientas de monitoreo.

Indagación:

- No administración de Información, no se tiene administrado por segmento de error los logs de cada nodo.
- Demoras en la ubicación de causas de errores, al tener muchas fuentes de información se dificulta la lectura del log ante un incidente presentado.

A continuación, se presenta la infraestructura a implementar para el empaquetado Elastic Stack.

1. INFRAESTRUCTURA PARA NECESITAR:

Teniendo en cuenta la arquitectura actual de la financiera se opta por la siguiente solución

- 1 nodo que alojara todos los componentes de ELK PACK

N°	Características	Capacidad
1	CPU	4 Core
2	Memoria RAM	16 GB
3	Disco Duro	154 GB
4	Sistema Operativo	Linux 8.2

2. ELEMENTOS DE INSTALACION:

Consideraremos los siguientes instaladores:

- elasticsearch-7.13.0-x86_64.rpm
- kibana-7.13.0-x86_64.rpm
- logstash-7.13.0-x86_64.rpm
- filebeat-7.13.0-x86_64.rpm

De no contar con los instaladores se podrán obtener de los siguientes enlaces:

- https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.13.0-x86_64.rpm
- https://artifacts.elastic.co/downloads/kibana/kibana-7.15.2-x86_64.rpm
- https://artifacts.elastic.co/downloads/logstash/logstash-7.13.0-x86_64.rpm
- https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.13.0-x86_64.rpm

3. CONFIGURACION:

3.1 CONFIGURACION DE ELASTICSEARCH

Luego de la instalación de ElasticSearch nos dirigiremos a la siguiente ruta "/etc/elasticsearch/elasticsearch.yml" y procederemos con editar según siguientes características:

N°	NODO	Elasticsearch.yml
1	Node Elasticsearch	cluster.name: **<cluster_name>** node.name: <node_name> network.host: 0.0.0.0 http.port: 9200 discovery.seed_host: ["<node_hostname>"] cluster.initial_master_nodes: ["<node_name>"] xpack.security.enabled: true xpack.security.http.ssl.enabled: true xpack.security.http.ssl.key: <path_private_key>.key xpack.security.http.ssl.certificate: <path_certificate>.crt xpack.security.http.ssl.certificate_authorities: ["<path_ca_certificate>.crt"] xpack.security.transport.ssl.enabled: true xpack.security.transport.ssl.key: <path_private_key>.key xpack.security.transport.ssl.certificate: <path_certificate>.crt xpack.security.transport.ssl.certificate_authorities: ["<path_ca_certificate>.crt"] node.master: true node.data: true

Tendremos en cuenta cada significado según corresponda:

N°	DIRECTIVA	DESCRIPCION
1	cluster.name	Nombre del clúster
2	node.name	Nombre del nodo
3	network.host	Comunicación del nodo en la red
3	http.port	Puerto de comunicación http
4	discovery.seed_host	Listar nodos tantos maestros o no, agregar por su nombre host o dirección IP
5	cluster.initial_master_nodes	Listar solo nodos maestros elegibles, agregar por su nombre de nodo
6	xpack.security.enabled	Habilitar autenticación por usuario de ELASTICSEARCH

7	xpack.security.http.ssl.enabled	Habilitar http seguro (https), por default el valor es false
8	xpack.security.http.ssl.key	Path de la clave privada del certificado
9	xpack.security.http.ssl.certificate	Path del certificado auto firmado
10	xpack.security.http.ssl.certificate_authorities	Path del certificado propio de la CA
11	xpack.security.transport.ssl.enabled	Habilitar capa de transporte seguro, por default el valor es false
12	xpack.security.transport.ssl.key	Path de la clave privada del certificado
13	xpack.security.transport.ssl.certificate	Path del certificado auto firmado
14	xpack.security.transport.ssl.certificate_authorities	Path del certificado propio de la CA
15	node.master	Indicar si el nodo es maestro, por default el valor es true
16	node.data	Indicar si el nodo es de almacenamiento de data, por default el valor es true

Nota:

- Para habilitar una directiva de deberá descomentar, la forma correcta es quitar el símbolo "#"
- Si la directiva no se encuentra, se deberá agregar con su valor correspondiente
- Para las directivas "XPACK" es opcional, una recomendación es utilizarlos para comunicaciones de forma segura "SSL/TLS".

3.1.1 Asignar permisos para el usuario ELASTICSEARCH

Al realizar la instalación del ELASTICSEARCH se creó automáticamente un usuario llamado "elastichsearch" y un grupo llamado "elasticsearch", por tal motivo dicho usuario se podrá ejecutar con permisos de usuario "root", por ello debemos asignar los siguientes permisos por medio de consola CMD:

- "chown elasticsearch:elasticsearch -R /usr/share/elasticsearch"

- “chown elasticsearch:elasticsearch -R /var/log/elasticsearch”
- “chown elasticsearch:elasticsearch -R /var/lib/elasticsearch”
- “chown elasticsearch:elasticsearch -R /etc/elasticsearch”

Nota:

Una opción de verifica que el usuario y grupo este creado podemos usar el siguiente comando:

- “less /etc/passwd | grep elasticsearch”
- “less /etc/group | grep elasticsearch”

3.1.2 Reservar cantidad de MEMORIA RAM

Para esta configuración iremos a la siguiente ruta “/etc/elasticsearch/jmv.options”

Editaremos el archivo “jvm.options”, según el cuadro colocar los valores correspondientes:

- -XMS8g
- -XMS8g

3.1.3 Habilitar el servicio ELASTICHSEARCH

Podremos realizar la habilitación por el siguiente comando:

- “systemctl enable elasticsearch”
- “systemctl start elasticsearch”
- “systemctl status elasticsearch”

3.2 CONFIGURACION DE LOGSTASH

Para esta parte de la configuración se procederá con crear un archivo “logstash.config” en la siguiente ruta “/etc/logstash/conf.d” se detallara lo siguiente:

```
“input {
  beats {
    port => 5044
    ssl => true
    ssl_key => "<path_private_key >.key"
    ssl_certificate =>  "<path_certificate>.crt"
    ssl_certificate_authorities => ["<path_ca_certificate>.crt"]
  }
}
filter {
  #If log line contains tab character followed by 'at' then we will tag that entry as stacktrace
  if [message] =~ "\tat" {
    grok {
      match => ["message", "^(\tat)"]
      add_tag => ["stacktrace"]
    }
  }
  #Parsing out timestamps which are in timestamp field thanks to previous grok section
  grok {
    match => [ "message",
            "(?<timestamp>%{YEAR}-%{MONTHNUM}-%{MONTHDAY} %{TIME})  %{LOGLEVEL:level} %{NUMBER:pid} ---
\[(?<thread>[A-Za-z0-9-]+)\] [A-Za-z0-9.]\.(?<class>[A-Za-z0-9#_]+)\s:\s+(?<logmessage>.*)",
            "message",
            "(?<timestamp>%{YEAR}-%{MONTHNUM}-%{MONTHDAY} %{TIME})  %{LOGLEVEL:level} %{NUMBER:pid} ---
.+? :\s+(?<logmessage>.*)"
          ]
  }
    date {
    match => [ "timestamp" , "yyyy-MM-dd HH:mm:ss.SSS" ]
  }
}
output {
    elasticsearch {
      hosts => ["protocol://domain_or_ip_address:port>"]
      manage_template => false
      index => "<index_name>_%{+YYYY.MM.dd}"
      user => "elastic"
```

3.2.1 Habilitación del servicio LOGSTASH

- “systemctl enable logstash”
- “systemctl start logstash”
- “systemctl status logstash”

3.2.2 Debuggear LOGSTASH

- “/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/logstash.conf”

3.3 CONFIGURACION DE FILEBEAT

Ingresaremos a la siguiente ruta “/etc/filebeat/filebeat.yml” según el cuadro cololar los valores indicados en la directiva:

N°	NODO	FILEBEAT.YML
1	Nodo Filebeat	enabled: true - type: log paths: - <path_log>/*.log tags: ["<tag_name>"] fields: { log_type: <log_type>, index_name: <index_name>} output.logstash: hosts: ["<domain_or_ip_address:port>"] ssl.certificate_authorities: ["<path_ca_certificate>.crt”] ssl.certificate: "<path_certificate>.crt " ssl.key: "<path_private_key>.key "

Nota:

- FILEBEAT solo se utiliza para enviar “log” que requerimos de una aplicación(satélite) en un servidor.
- Puerto por default de LOGTASH es 5044 para los FILEBEATS

3.3.1 Habilitación servicio FILEBEAT

- “systemctl enable filebeat”
- “systemctl start filebeat”
- “systemctl status filbeat”
-

3.3.2 Debugear en FILEBEAT

- "/usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml"

3.4 CONFIGURACION DE KIBANA

Para dicha configuración emplearemos lo siguiente en la ruta: "/etc/kibana/kibana.yml" y editaremos el archivo "kibana.yml", según el cuadro coloremos los valores correspondientes a las directivas:

N°	NODO	KIBANA.YML
1	Node Kibana	server.port: 5601 server.host: 0.0.0.0 server.name: "<node_name>" elasticsearch.hosts: ["<protocol://domain_or_ip_address:port>"] elasticsearch.username: "kibana_system" elasticsearch.password: "<password>" server.ssl.enabled: true server.ssl.certificate: <path_certificate>.crt server.ssl.key: <path_private_key>.key elasticsearch.ssl.verificationMode: none

Se detalla los significados para cada parámetro:

N°	DIRECTIVA	DESCRIPCION
1	server.port	Puerto de comunicación http
2	server.host	Comunicación del nodo en la red
3	server.name	Nombre del servidor
4	elasticsearch.hosts	Listar nodos de ELASTICSEARCH, agregar por URL del nodo
5	elasticsearch.username	Nombre de usuario para conectarse con ELASTICSEARCH
6	elasticsearch.password	Password para conectarse con ELASTICSEARCH
7	server.ssl.enabled	Habilitar http seguro (https), por default el valor es false
8	server.ssl.certificate	Path del certificado auto firmado
9	server.ssl.key	Path de la clave privada del certificado
10	elasticsearch.ssl.verificationMode	Modo de Verificación

Nota:

- Puerto por default para ELASTICSEARCH es 9200

3.4.1 Habilitación de servicio KIBANA

- “systemctl enable kibana”
- “systemctl start kibana”
- “systemctl status kibana”

3.4.2 Verificar despliegue de KIBANA

Ingresamos por navegador en la siguiente ruta, ingresa con las credenciales del usuario integrado “elastic” que previamente se configuro y se asignó una contraseña:

SIN CERTIFICADO	CON CERTIFICADO
http://<ip_address>:5601	https://<domain>:5601

Luego culminar con la configuración total de ELK PACK, podremos segmentar los gráficos de las siguientes formas:

Figura 4 – Grafico de medición del CPU en KIBANA

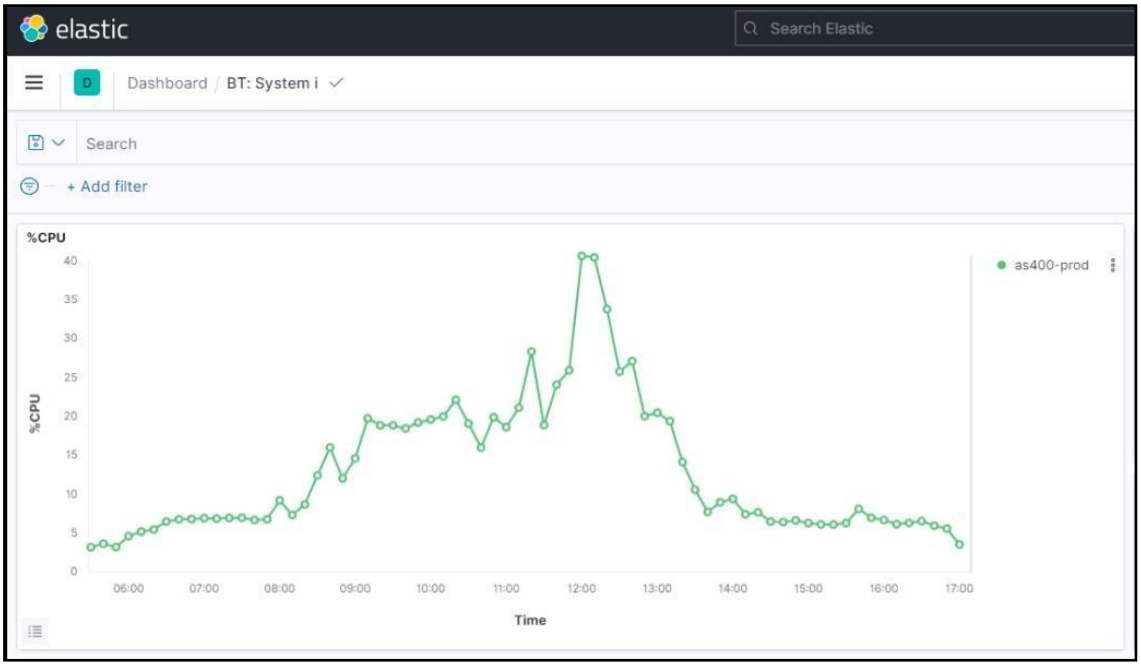


Figura 5 – Medición de conexiones para los servicios

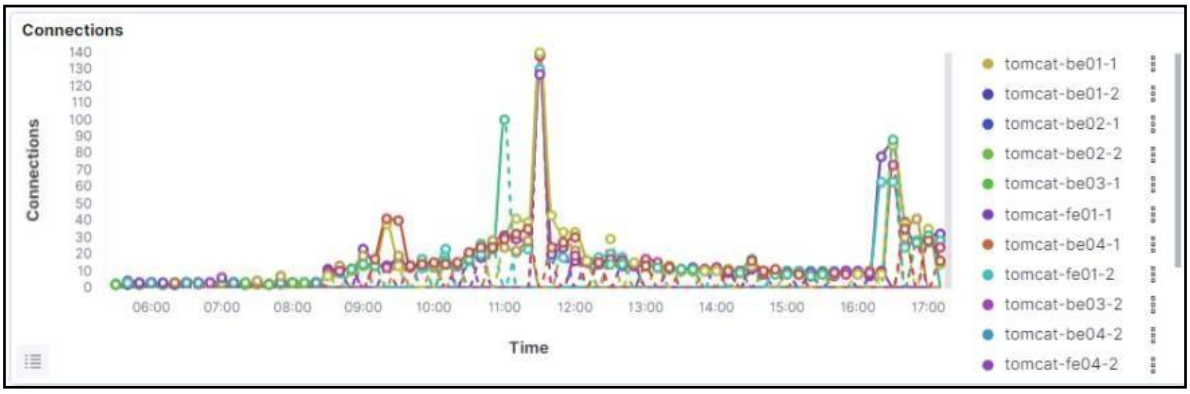
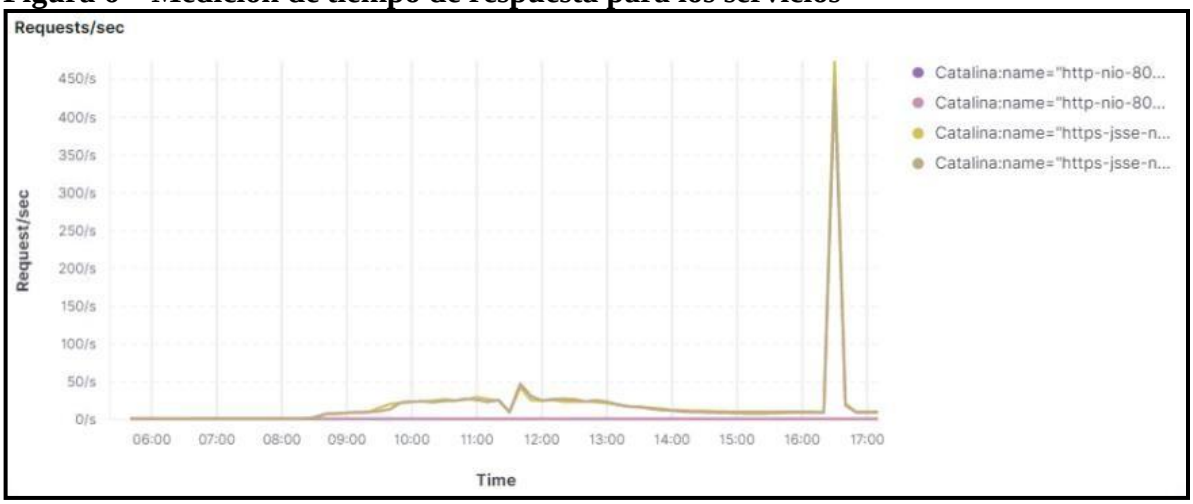


Figura 6 – Medición de tiempo de respuesta para los servicios



4. DESCRIPCION DE LA REALIDAD PROBLEMÁTICA

Actualmente la Financiera cuenta con múltiples servidores en diferentes sistemas operativos, el cual no se tiene un sistema de monitoreo que centraliza toda la información que arroja los servidores que generan en tiempo real, la forma que se realiza la visualización de los logs es de manera manual ingresando en cada instancia para realizar la descarga debida y empezar a analizar línea por la línea de texto cuales son los posibles errores presentados en los servidores de aplicaciones.

Formulación del problema general:

- ¿En qué medida la implementación de un sistema web de monitoreo mejorará el control de los servicios del nuevo core bancario?

Problemas específicos 1:

- ¿En qué medida la implementación de un sistema web de monitoreo para mejorar el control de los servicios del nuevo core bancario reducirá los incidentes presentados en los servicios?

Problemas específicos 2:

- ¿En qué medida la implementación de un sistema web de monitoreo para mejorar el control de los servicios del nuevo core bancario mejorará la caída o lentitud de la plataforma web usado en agencias?

Problemas específicos 3:

- ¿En qué medida la implementación de un sistema web de monitoreo para mejorar el control de los servicios del nuevo core bancario aportara la ayuda en la identificación específica del error presentado?

5. OBJETIVOS DE LA INVESTIGACIÓN

El objetivo principal de la presente investigación es poder resolver la problemática de la visualización de información e interpretación del log de múltiples nodos de un clusster, ya que cada instancia contiene log de miles de líneas en los cuales debemos encontrar patrones, anomalías, tendencias que en tiempo real es imposible la toma de decisiones en el horario operativo que se encuentran abiertos la red de agencias a nivel nacional, donde el tiempo es crucial para la atención al público.

a. Objetivos General:

Elaborar un sistema web para mejorar el control de los servicios del nuevo core bancaraio.

b. Objetivos Específicos:

Objetivos Específicos 1:

- Elaborar un sistema web para mejorar el control de los servicios de manera que nos permitirá reducir los incidentes presentados en los servicios.

Objetivos Específicos 2:

- Elaborar un sistema web para mejorar el control de los servicios permitirá reducir la caída o lentitud de la plataforma web que es usado en agencias.

Objetivos Específicos 3:

- Elaborar un sistema web para mejorar el control de los servicios nos ayudara en la identificación específica del error presentado

6. JUSTIFICACIÓN

De acuerdo a la implementación del sistema web, se mejorará mucho la calidad de los procesos de medición de las posibles caídas del servidor del banco, el cual nos permite a los ingenieros un constante monitoreo, vigilia en línea de producción para el avance tecnológico, ello beneficiará al banco en la solución de fallas electrónicas, en funcionamiento para reducir el tiempo de productividad. la implementación de un sistema web de monitoreo mejorará el control de los servicios del nuevo core bancaraio

7. CONCLUSIONES

Primero: la implementación de un sistema web de monitoreo mejorará el tiempo de respuesta ante cualquier incidente.

Segundo: la implementación de un sistema web de monitoreo mejorará la integración de diferentes fuentes hacia una sola visualización, se ahorra mucho tiempo en el análisis de esta.

Tercero: la implementación de un sistema web de monitoreo mejorará el control de los servicios reduciendo los reportes mensuales, que permitirá la toma de decisiones adecuada para la infraestructura de la Financiera.

Cuarto: la implementación de un sistema web de monitoreo mejorará el control de los servicios asegurando la performance de la atención al público en toda la red de agencias a nivel nacional.

En conclusión, la implementación de un sistema web de monitoreo en una entidad del rubro financiero se asegura que la performance de la atención al público no se vea afectado con caídas o degradaciones de los servicios web, esto es muy importante ya que una de las normas por la Super Intendencia de Banca y Seguros para el dicho rubro es que no se vea afectado en su totalidad la atención al público.

8. APORTE DE LA INVESTIGACION

Primero: EL aporte recolectado por mi persona muestra como resultado que la implementación del sistema web monitore los servicios Core de un sistema financiero podría integrarse con mensajería instantáneas como Telegram por medio de API´s.

Segundo: Con esta ejecución de mi proyecto de investigación nos permitirá a organizar los procesos de resolver incidentes presentados en la operativa diaria de una empresa.

Tercero: Con la implementación del sistema web aportará mejoras en la infraestructura en caso se vea muy saturado la actual en las organizaciones.

Cuarto: Disponibilidad de 24/7, ya que el sistema de monitorio recopila la información sin desconexiones y nos permite alertar en cuanto se tengan saturaciones o caídas.

Quinto: Ayudará a la toma de decisiones, con la reportería de los principales servicios afectados en un periodo de tiempo, se podrá realizar mejoras o actualizaciones a nivel de programación.

Sexto: La centralización de información que se consolida desde múltiples plataformas.

9. RECOMENDACIONES

Primero: Los sistemas de monitoreo de servicios web en una entidad es muy importante porque nos aportara mucha trazabilidad en vivo de la performance de la infraestructura empleada, al ser una implementación de última tecnología, se recomienda en corto plazo realizar escalamientos y actualizaciones en ELK Pack.

Segundo: De presentar saturación en los principales componentes como CPU o Memoria RAM, según la información se recomienda la ampliación o mejora para llegar al nivel óptimo que conlleva el Core.

Tercero: Se recomienda realizar análisis mensuales de los servicios con mayor afectación, para derivar al equipo correspondiente en su revisión.

10. REFERENCIAS

Araya Poblete, D. E. (21 de 05 de 2021). *Universidad de Chile.* Obtenido de Universidad de Chile: https://repositorio.uchile.cl/handle/2250/181842

CUERVO, V. (26 de 02 de 2019). *arquitectoit.* Obtenido de arquitectoit: https://www.arquitectoit.com/elasticsearch/que-es-elasticsearch/

Echarrouti, C. A. (27 de 12 de 2015). *adictosaltrabajo.* Obtenido de adictosaltrabajo: https://www.adictosaltrabajo.com/2015/12/27/introduccion-a-kibana/#:~:text=Kibana%20es%20una%20herramienta%20open,Logstash

Geronimo Morales, M. &. (21 de 05 de 2021). *Universidad Cesar Vallejo.* Obtenido de Universidad Cesar Vallejo: https://repositorio.ucv.edu.pe/handle/20.500.12692/72308

Navarro Gomez, J. S. (18 de 02 de 2022). *Universidad Peruana los Andes.* Obtenido de Universidad Peruana los Andes: https://repositorio.upla.edu.pe/handle/20.500.12848/3507

Pestaña, D. (26 de 05 de 2021). *BIGEEK.* Obtenido de BIGEEK: https://blog.bi-geek.com/que-es-el-elk-stack/

Sergio, G. (12 de 05 de 2020). *Davincigroup.* Obtenido de Davincigroup: https://www.davincigroup.es/que-es-logstash-ejemplo-practico-de-uso/

Zavala Huamani, B. R. (30 de 03 de 2022). *INSTITUCION UNAMBA.* Obtenido de INSTITUCION UNAMBA: http://repositorio.unamba.edu.pe/handle/UNAMBA/1071