UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación y Configuración de un Sistema de Monitoreo y Servicios de Red

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Vicente Mercado Almeida

ASESOR DE INFORME

Ing. Jesús Reyes García

Ciudad Universitaria, Cd. Mx., 2023

Índice

Figuras

Tablas

Código

Objetivo

El objetivo de este trabajo es presentar el planteamiento, la implementación, los resultados y las conclusiones, de dos de las actividades que realicé en una pequeña empresa mexicana de monitoreo de medios de comunicación en el periodo de octubre del 2014 hasta julio del 2019. Estas dos actividades fueron la implementación de un sistema de monitoreo de red y la configuración e implementación de varios servicios de red.

Aunque las actividades que desarrollé en este periodo son mucho más extensas. Sólo me enfocaré en estas dos ya que son las que más requirieron de mis conocimientos como estudiante de la carrera de telecomunicaciones. En especial los aprendidos en la especialización de redes de datos. Pero debido a que existe una estrecha relación entre estas y las demás actividades que realicé en algunos momentos será necesario mencionar, aunque sea de forma superficial, otras de las actividades.

Introducción

Antes de entrar a profundidad a las actividades que conciernen directamente a este trabajo, empezaré por dar un poco del contexto de la empresa y de todas las actividades que yo desempeñaba.

Contexto de la Empresa

Las principales actividades de la empresa, hasta el momento de mi partida, eran:

- Monitoreo de noticieros y contenido de información en:
  - Radio abierta
  - Televisión abierta
  - Televisión de paga
  - Canales digitales
- Monitoreo de comerciales en:
  - Radio abierta
  - Televisión abierta
  - Televisión de paga
- Monitoreo de noticias y contenidos en medios impresos en:
  - Periódicos locales (Ciudad de México)
  - Revistas de distribución nacional
  - Suplementos
- Monitoreo de publicaciones oficiales, como:
  - Diario Oficial de la Federación

La forma en la que se entregaba la información a los usuarios variaba dependiendo del tipo de contenido. Para el monitoreo radio y televisión, la información se presentaba usando un sitio web personalizado por cliente. Basado en una plantilla que se ajustaba dependiendo de las necesidades particulares. El contenido multimedia se distribuía por medio de archivos Windows Media Audio y Video. Se empleaban algunos formatos más recientes, pero todo derivaba de los archivos de Windows Media. La empresa daba valor agregado a la información por medio de la clasificación, análisis, marcado de tiempos, generación de testigos y transcripción del contenido para su consulta. El servicio de monitoreo de contenido informativo lo prestaba la empresa desde su fundación. Unos años después agregaron el monitoreo de comerciales en radio y televisión.

El monitoreo de medios impresos fue un servicio que inició con mi llegada. Se me contrató directamente para desarrollar el sistema de captura para esta área en el 2014. Y oficialmente se comenzó a prestar el servicio en el 2016. El contenido del servicio se distribuía por medio de un sitio web dedicado alojado en un subdominio. La información consistía en imágenes de alta resolución de los medios originales y los textos obtenidos por el sistema de OCR de las imágenes. El valor agregado del servicio era el motor de búsqueda (que permitía búsquedas por palabra o clasificación), las transcripciones y los testigos. Adicionalmente se realizaban entregas de archivos .pdf vía correo electrónico o descarga por vínculo; con los testigos para los clientes que lo solicitaban. Estos documentos estaban compuestos por las notas que cumplían los criterios establecidos por los clientes de los diferentes medios a los que tenían acceso.

Al ser una empresa pequeña, la estructura no estaba completamente bien definida y yo no pertenecía a ningún departamento en particular. Trabajaba directamente bajo las órdenes de los dueños de la empresa, quienes se encargaban de programar la mayoría de las aplicaciones y herramientas que se usaban en la empresa. Las únicas otras aplicaciones de uso interno fueron las que desarrollé cuando trabajé allí durante los años del 2001 al 2005 y en el periodo del 2014 al 2019. La otra responsabilidad directa que yo tenía era con el departamento de soporte, a ellos los ayudaba a resolver problemas complicados con los equipos de la empresa, los programas/servicios que desarrollé/implementé y con los imprevistos que surgían de los servicios/programas que desarrollaron mis jefes (cuando ellos no estaban disponibles).

En la Figura 1 - Organigrama de la empresa, se muestra un organigrama general de la estructura de la empresa y mi posición en ella.

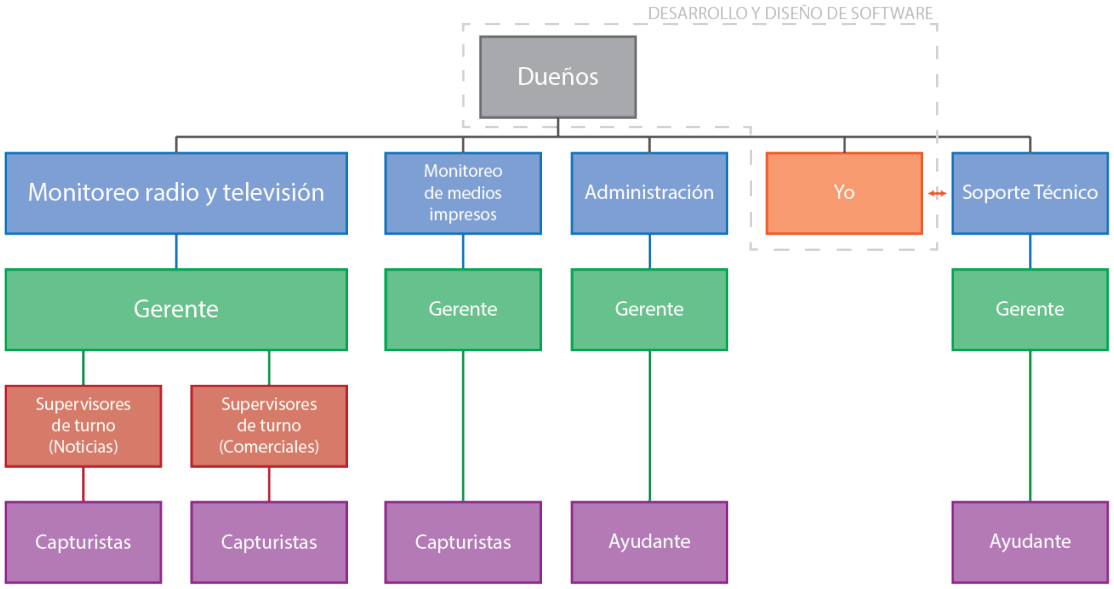

Figura 1[1] - Organigrama de la empresa

Actividades desarrolladas

Las actividades que desarrollé en la empresa fueron principalmente, implementación de soluciones de red, soporte técnico y programación. La siguiente es una lista de dichas actividades:

- Implementación de un sistema de monitoreo de red
  - Monitoreo de servidores
  - Monitoreo de equipos de usuarios
  - Monitoreo de equipos de red
  - Monitoreo de servicios
- Configuración, despliegue y mantenimiento de servicios de red:
  - Active Directory
  - DHCP

[1] Fuente Propia.

    - DNS
    - NTP
    - FTP
    - Servicios de reconocimiento óptico de caracteres (OCR)
    - Solr (indexación y búsqueda de textos)
- Diseño y programación de:
    - Sistema de captura para el monitoreo de medios impresos
    - Sistema de generación de documentos y reportes de medios impresos
    - Aplicación web para la consulta de medios impresos
    - Sistema de grabación de emisiones de audio y video por internet
    - Sistema para revisión y validación de archivos de audio y video
    - Sistema de clasificación y procesamiento de archivos xml
- Soporte técnico (cuando la gente del área no se encontraba o cuando no podían resolver algún problema en particular)
    - Servidores
    - Equipos de los usuarios
    - Equipos de red

Para motivos de este trabajo me enfocaré exclusivamente en el trabajo que desempeñé en la implementación del sistema de monitoreo de red y la configuración, despliegue y mantenimiento de los servicios de red asociados, ya que son los temas que más conciernen a la carrera y mi especialización de redes de datos.

Antecedentes

Teóricos Generales

Modelo OSI

La Organización Internacional de Estándares (ISO por sus siglas en inglés) creó el modelo de interconexión de sistemas abiertos (OSI por sus siglas en inglés) en 1974. El cual fue publicado oficialmente por primera vez en 1980. En 1983 el Comité Consultivo Internacional Telegráfico y Telefónico, ahora conocido como la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), junto con la Organización Internacional de Normalización, publicaron el modelo como lo conocemos hoy en día en los documentos X.200 e ISO 7498 respectivamente.

El propósito principal de la creación de un modelo de referencia era, proveer una serie de estándares que garantizaran gran compatibilidad e interoperabilidad entre diferentes tecnologías de red, producidas por diferentes compañías a nivel mundial. Esta es la razón por lo que el modelo de referencia tenía que ser abierto.

El modelo OSI divide la comunicación entre sistemas en siete diferentes capas, para permitir la facilidad de compresión de cómo viaja la información a través de la red. Lo que permite entender la comunicación de una capa sin necesidad de saber los pormenores de las demás capas. Hoy en día este es el modelo que se considera como la mejor herramienta para enseñar a las personas como se envía y transmite la información a través de una red. En la Tabla 1 – Capas del Modelo OSI se muestran cada una de las capas con su nombre, descripción y ejemplos de protocolos.

Las capas superiores, desde la 4 hasta la 7, se enfocan exclusivamente en las funciones de extremo a extremo, como las aplicaciones de usuario, establecimiento de sesión, servicios de usuario y la interfaz de usuario. Las capas inferiores, 1 a 3 son las de "interfaz", las de mayor interés desde la perspectiva de la infraestructura de telecomunicaciones.

Tabla 1[2] – Capas del Modelo OSI

		Nombre	Descripción	Protocolos
Extremo a Extremo	Capa 7	Aplicación	Es la capa que está más cerca del usuario. Provee los servicios de red a las aplicaciones. Se diferencia de las otras capas ya que no provee servicios a ninguna otra capa del modelo. Provee servicios únicamente a aplicaciones que se encuentran fuera del modelo.	• HTTP • Telnet
	Capa 6	Presentación	Esta capa se encarga de enviar la información de la capa de aplicación de un equipo para que pueda ser leída por la capa de aplicación de otro equipo. En caso de ser necesario, la capa de presentación traduce entre múltiples formatos de datos usando un formato común. Una de las tareas más importantes de esta capa es el cifrado y descifrado de la información.	• SSL • LPP
	Capa 5	Sesión	Como su nombre lo implica establece, maneja y termina sesiones entre dos anfitriones (host). Provee servicios a la capa de presentación.	• NFS

[2] Fuente Propia. Basado en las fuentes (1) y (4) de la bibliografía.

			También sincroniza el dialogo entre las capas de presentación de dos anfitriones y maneja el intercambio de datos ente ellos.	• ASP
	Capa 4	Transporte	La capa de transporte segmenta la información que envía el host transmisor y lo vuelve unir en el host receptor. Esta capa intenta proveer un servicio de transporte de datos que protege a las capas superiores de los detalles de implementación.	• TCP • UDP • SPX
Interfaz	Capa 3	Red	La capa de red es una capa compleja que provee conectividad y selección de rutas entre dos hosts que se encuentran en redes separadas geográficamente. Adicionalmente, la capa se ocupa del direccionamiento lógico.	• IP • IPX • AppleTalk
	Capa 2	Enlace de Datos	Provee el transito confiable de datos a través de la capa física. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico, la topología de la red, el acceso al medio, la detección de errores, el control de flujo, y el envío y recepción ordenado de las tramas.	• ARP • MLT • CAN • PPP
	Capa 1	Física	La capa física define las especificaciones, físicas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar la conexión física entre los sistemas destino.	• T1 • X.25 • DSL

Datagrama

La unidad básica de transferencia de información de la capa 4 es el datagrama[3], a veces también llamado segmento de información. Que se compone del encabezado y la información (payload). Que este a su vez se convierte en el "payload" de la trama de la capa inferior.

La definición de datagrama establecida en el RFC 1594, queda, al traducirse, de la siguiente forma.

"Una entidad independiente de información, autocontenida, que transporta suficiente información para ser conmutada desde su equipo de origen hasta el equipo de destino, sin depender de los intercambios previos entre origen, destino y la red de transporte"[4].

TCP/IP

Protocolo de internet (IP)

El protocolo IP es usado para transmitir datagramas entre equipos remotos. Cada encabezado del datagrama IP contiene la dirección de destino, la cual es la información completa de ruteo utilizada para entregar el datagrama a su destino. Por lo cual, la red sólo puede trasmitir los datagramas individualmente. Los datagramas IP de una sesión pueden ser transmitidos a través de diferentes rutas y por lo tanto pueden ser recibidos por el destino en un orden diferente al que fueron enviados. Cada interfaz de red de Internet tiene una o más direcciones IP que son únicas

[3] El término datagrama es utilizado de forma diferente dependiendo el contexto. Pero en este trabajo siempre se dará por hecho que es en el contexto de redes de conmutación de paquetes. Y se referirá el en el contexto de la capa 4. Siguiendo la definición establecida en el RFC 1594.

[4] Página 32 del RFC 1594. Versión en línea https://datatracker.ietf.org/doc/html/rfc1594.

globalmente. El Internet se compone de redes individuales que se interconectan por medio de enrutadores.

El modelo de capas de TCP/IP está compuesto por las capas de Aplicación, Transporte, Internet y Acceso a la Red. Aunque las capas en este modelo tienen nombres similares o iguales al del modelo OSI, no se deben confundir en función o numeración.

La capa de aplicación en el modelo TCP/IP corresponde a las tres capas superiores del modelo OSI (Aplicación, Presentación y Sesión). En este modelo todo lo relacionado con la aplicación se agrupa en una sola capa para asegurar que la información sea recibida correctamente.

TCP/IP no sólo incluye las especificaciones de la capa de Transporte y de Internet, sino también especificaciones para aplicaciones comunes, como lo son: HTTP, TFTP, FTP, NFS, SMTP, Telnet, SNMP y DNS.

Como su nombre lo indica la capa de transporte provee los servicios de transporte desde el host de origen hasta el host de destino. Constituye la conexión lógica entre los puntos finales de la red: el host que envía y el host que recibe. Los protocolos de transporte segmentan y ensamblan la información que envía la capa de aplicación, en el mismo flujo de datos entre los puntos finales.

El propósito de la capa de Internet en el modelo TCP/IP es enviar paquetes entre puntos finales. La determinación de la mejor ruta y la conmutación de paquetes sucede en esta capa. Hay varios protocolos que operan en esta capa, como lo son: protocolo de internet (IP), protocolo de control de mensajes de Internet (ICMP), protocolo de resolución de direcciones (ARP), protocolo de resolución de direcciones inverso (RARP). En el modelo OSI es la capa de red.

El protocolo de Internet IP realiza las siguientes operaciones:

- Definir el paquete y definir el esquema de direccionamiento.
- Transferir datos entre la capa de internet y la capa de acceso a la red.
- Direccionar los paquetes a los hosts remotos.

Una característica del protocolo de Internet es que no se encarga de la revisión y corrección de errores, esto lo realizan los protocolos de las capas superiores del modelo.

La capa de acceso a la red, o también llamada capa host a red, es la capa que se enfoca en todo lo que requiere un paquete IP para hacer un vínculo físico con el medio de la red. Esto incluye los detalles tecnológicos de la red de área local (LAN) y la red de área amplia (WAN), como lo son: el crear la relación entre las direcciones IP y las direcciones físicas, y la encapsulación de paquetes en las tramas.

La capa de acceso a la red en el modelo TCP/IP es el equivalente de las capas 1 y 2 del modelo de referencia OSI.

Dirección IP

Los dispositivos usan un esquema de direccionamiento para determinar cómo se mueve la información en la red. En la actualidad hay dos versiones relevantes de direcciones IP, IPv4 e IPv6[5].

[5] Para el propósito de este informe solo me enfocaré en la versión IPv4 y las direcciones de redes privadas.

Las direcciones IPv4 son una secuencia binaria de 32 bits. La notación que normalmente se utiliza para representar de forma escrita una dirección IPv4 es por medio de cuatro números decimales (octetos) separados por puntos. Cada número decimal puede tener un valor de 0 a 255 (valore decimales de un número de 8 bits).

Para acomodar diferentes tamaños de redes y ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases. La dirección IP se puede dividir de tal forma que la primera parte es la parte de red (número de red o net id en inglés) y la segunda parte son la parte del host. Existen 5 diferentes clases: A, B, C, D y E. En la Tabla 2 – Clases de redes, se muestra la información de cada una de las clases.

Tabla 2[6] – Clases de redes

	Primeros bits de la dirección	**Tamaño del número de red**	**Número de redes**	**No. de direcciones en la red**	**Máscara de red predeterminada**	**Notación CIDR**
Clase A	0	8	128 (2^{24})[7]	16 777 216 (2^{24})	255.0.0.0	/8
Clase B	10	16	16 284 (2^{14})	65 534 (2^{16})	255.255.0.0	/16
Clase C	110	24	2 097 152 (2^{21})	256 (2^{8})	255.255.255.0	/24
Clase D	1110	28	-	-	-	/4
Clase E	1111	-	-	-	-	-

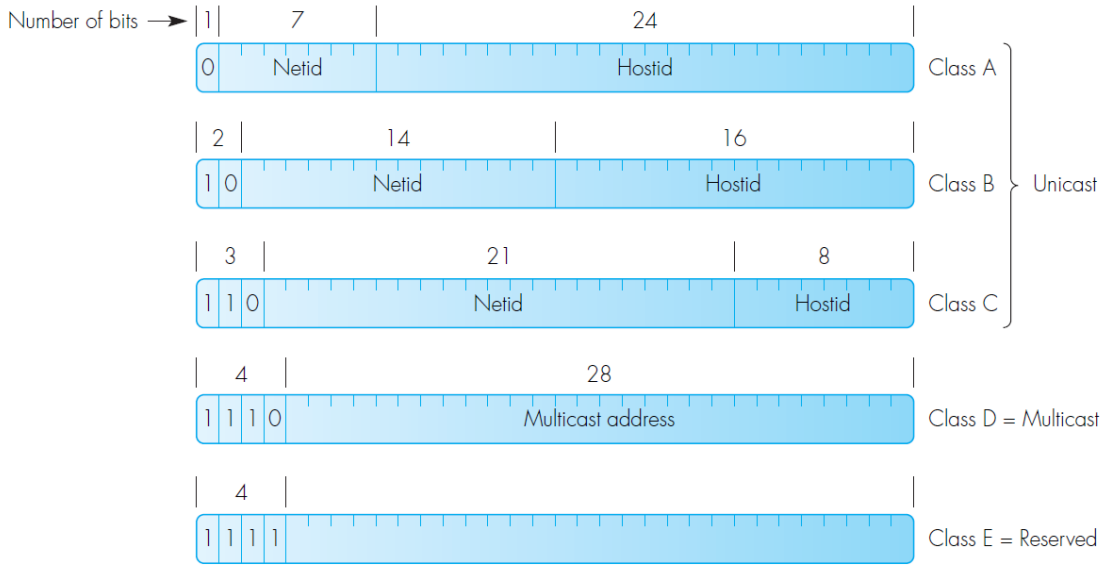

Figura 2[8] – Formatos de las direcciones IP de las clases de redes

[6] Fuente propia. Basado en las fuentes (3) y (4) de la bibliografía.
[7] En realidad, son 126 ya que la red 0.0.0.0/8 se usa para referirse a "esta red" y la red 127.0.0.0/8 es el bucle local.
[8] Tomado de la página 329 de la fuente (8) de la bibliografía.

Esta fue la forma inicial de asignar las direcciones IP en Internet. No era una forma muy eficiente, en la actualidad se emplean otras formas más eficientes de asignación, entre las cuales se encuentran: el uso de subredes, direcciones sin clase y la traducción de direcciones de red (NAT por sus siglas en inglés). Por el alcance de este trabajo sólo NAT es de interés, ya que en la empresa nunca hizo uso de subredes ni de direcciones sin clase.

El uso de la NAT es importante para las redes internas y requiere de la comprensión de las clases de redes. Existen 3 rangos de direcciones privadas que se emplean comúnmente, una de clase A (10.0.0.0), 16 clase B (172.16.0.0 – 172.32.0.0) y 256 clase C (192.168.0.0 – 192.168.255.0). En la Tabla 3 - Redes IP privadas, se listan las características de cada uno de los rangos.

Tabla 3[9] - Redes IP privadas

ID de Red	Número de Redes	IP Inicial	IP Final	Número de Direcciones por red	Máscara de red
10.0.0.0	1	10.0.0.0	10.255.255.255	16 777 216 (2^{24})	255.0.0.0
172.16.0.0 – 172.32.0.0	16	172.16.0.0[10]	172.166.255.255[11]	65 534 (2^{16})	255.255.0.0
192.168.0.0 – 192.168.255.0	256	192.168.0.0[12]	192.168.0.255[13]	256 (2^{8})	255.255.255.0

Los rangos de direcciones mostrados en Tabla 3 - Redes IP privadas, fueron declarados como privados, y se reservaron para uso en redes internas. Está definido en el RFC 1918. Cualquier persona o entidad puede utilizarlas sin necesidad de obtener permiso.

Esta forma de asignar direcciones IP surgió de la necesidad de poder asignar una dirección IP a todos los equipos de una red en la que se tienen más equipos que direcciones IP públicas. Lo que permite que un gran número de equipos usen un número limitado de direcciones públicas. Esto se logra por medio de un enrutador o puerta de enlace que administra una tabla de NAT, en donde se registra la dirección interna del equipo, el puerto del equipo, la dirección del equipo de destino (en la red externa o pública) y el puerto de destino. El mismo equipo tiene que administrar la asignación de puertos a los equipos internos para evitar conflictos. De esta forma las conexiones entre los equipos internos y externos se pueden mantener por medio de esta tabla, en donde la combinación única de puertos y direcciones IP permite realizar la comunicación. Esto fue creado principalmente para combatir el problema del número limitado de direcciones IP en la versión 4.

TCP y UDP

Con el propósito de aislar a los protocolos de aplicación de los servicios que proveen los diferentes tipos de protocolos de red, se utilizan los protocolos de transporte. Estos protocolos de transporte permiten a las aplicaciones hacer un intercambio de información independiente del protocolo de

[9] Fuente Propia. Basado en las fuentes (3) y (4) de la bibliografía.
[10] Es la dirección inicial (Id de la Red) de la primera red (172.16.0.0/16)
[11] Es la dirección final (Broadcast) de la primera red (172.16.0.0/16)
[12] Es la dirección inicial (Id de la Red) de la primera red (192.168.0.0/24)
[13] Es la dirección final (Broadcast) de la primera red (192.168.0.0/24)

red. En el caso de la suite TCP/IP estos protocolos son el protocolo de control de transmisión (TCP por sus siglas en inglés) y el protocolo de datagramas de usuario (UDP por sus siglas en inglés). TCP provee un servicio orientado a la conexión, en la cual la información puede ser transferida simultáneamente en las dos direcciones (full-duplex) en la cual la integridad de la información es garantizada, y UDP provee un servicio sin conexión (mejor esfuerzo) en el cual no hay control de flujo ni se garantiza la integridad de la información. Ambos protocolos suelen estar disponibles para su uso, siendo las necesidades de la aplicación lo que determinan cual se emplea.

La forma más fácil de entender cómo funciona la suite TCP/IP es: el protocolo IP permite la comunicación entre dos computadoras en el Internet y los protocolos TCP/UDP permiten la comunicación entre dos aplicaciones que corren en dichas computadoras.

Tanto en TCP como en UDP las partes terminales de la conexión se representan por medio de un número de puerto con valores de 0 a 65535 (dos bytes). Para los puertos se suele escribir la abreviatura del protocolo en minúsculas después del número de puerto, separado por una diagonal (ejemplo 80/tcp). El puerto sirve para identificar la aplicación, de entre todas las que pueden estar corriendo, en ambos equipos de la conexión.

ICMP

El protocolo de mensajes de control de internet (ICMP por sus siglas en inglés) es parte integral de todas las implementaciones del protocolo IP. Está definido en el RFC 1256, y es usado tanto por los hosts como por todos los equipos de comunicaciones. En la Tabla 4 - Funciones y mensajes ICMP se muestran las funciones y mensajes más comunes de ICMP.

Tabla 4[14] - Funciones y mensajes ICMP

Función	Mensaje ICMP	Uso
Reporte de errores	El destino no se puede alcanzar (Destination Unreachable)	Un datagrama se descartó por la razón contenida en el mensaje.
	Tiempo excedido (Time Exceeded)	El parámetro de tiempo de vida en el datagrama expiro y el datagrama se descartó.
	Error de parámetro (Parameter Error)	Un parámetro en el encabezado del datagrama no se reconoce.
Pruebas de alcance	Solicitud/Respuesta de echo (echo request/reply)	Revisar si un host o puerta de enlace se pueden contactar.
Control de congestión	Fuente Saciable (Source quench)	Solicitar a un host que reduzca la tasa de envió de datagramas.
Notificaciones de cambio de ruta	Redireccionar (Redirect)	Usado por una puerta de enlace para informar un host asociado en una de sus redes que use una puerta alternativa en la misma red para enviar datagramas a un destino específico.
Mediciones de desempeño	Solicitud/Respuesta de marca de tiempo (Time-stamp request/reply)	Determina el retraso de tránsito ente dos hosts.
Direccionamiento de subredes	Solicitud/Respuesta de máscara de red (Adress mask request/reply)	Usado por un host para determinar la máscara asociada con la subred.

[14] Traducido de la página 387 de la fuente (8) de la bibliografía.

DHCP

El protocolo de configuración dinámica de host (DCHP por sus siglas en inglés) es un protocolo de red tipo cliente/servidor que permite asignar una dirección IP de forma dinámica, sin necesidad de que exista, previamente, un perfil configurado para la máquina en el servidor. Lo único que se requiere para usar DCHP es definir un rango de direcciones IP, de las cuales el servidor puede asignar a los diferentes hosts cuándo se conectan. Esto permite asignar una configuración completa de TCP/IP a los equipos por medio de un solo mensaje. El protocolo utiliza los puertos 67/udp y 68/udp para el servidor y los clientes respectivamente. El protocolo se encuentra definido en el RFC 2131 (versión actual IPv4) y RFC 3315 (IPv6).

HTTP

El protocolo de transferencia de hipertexto (HTTP por sus siglas en inglés) es un protocolo de red tipo cliente/servidor que permite transferir información a través de archivos en la World Wide Web. Por medio de un navegador web se presenta la información multimedia contenida en los archivos (HTML, XML, JS, CSS, MP4, MP3, JPEG, …) al usuario. Las páginas en general se crean usando el lenguaje de programación HTML (lenguaje de marcado de hipertexto). Este lenguaje le informa al navegador qué y cómo mostrar la información contenida en los archivos. El protocolo original se encuentra definido en el RFC 1945 y la versión 3, la más reciente, en el RFC 9114.

DNS

Las direcciones numéricas funcionan muy bien para el direccionamiento de paquetes de internet. Pero no son amigables con los usuarios. Ya que son difíciles de recordar y si se cambia un solo dígito o punto llevan a un equipo/red completamente diferente. Es por eso que para asociar el contenido de un sitio con su dirección se creó el sistema de nombres de dominio (DNS por sus siglas en inglés). Con el propósito de simplificar para el usuario el acceso a dicho contenido. Este sistema se usa en Internet para traducir los nombres de dominio y los nodos públicos de la red asociados en direcciones IP.

Existen tres componentes en el sistema de nombres de domino: el cliente, los servidores y las zonas de autoridad. El cliente se ejecuta en la computadora del usuario y genera las peticiones DNS a un servidor DNS. El servidor se encarga de contestar las peticiones de los clientes. Si el servidor es capaz de convertir el nombre en su dirección IP asociada, lo hace y regresa el resultado al cliente. Si no puede traducir el nombre, y el servidor es recursivo, pasa la solicitud a un servidor DNS de un nivel superior, que pueda ser capaz de traducir la dirección. Y esto se repite hasta que algún servidor en la cadena puede resolver el nombre de dominio, o hasta que llega a los servidores de más alto nivel. Si dichos servidores no pueden resolver el nombre se regresa el mensaje de error correspondiente. Una zona de autoridad es una parte del espacio de nombres de dominio, la cual tiene designado un servidor DNS responsable, el cual es la autoridad final para resolver esos nombres, dicho servidor puede tener autoridad sobre varias zonas. Un ejemplo son los subdominios de cada uno de los países (ejemplo MX para México).

SSH

El protocolo Secure Shell (SSH por sus siglas en inglés) es un protocolo con arquitectura servidor cliente que sirve para operar servicios de forma segura sobre una red no segura. Es una solución

completamente basada en software, en la cual toda la información es cifrada en el origen y se descifra en el destino. SSH es utilizado principalmente para autenticación remota, transferencia de archivos y ejecución de comandos remotos.

El protocolo define la autentificación, encriptación y garantiza la integridad de la información. Está definido en una serie de RFCs, el que define la arquitectura del protocolo es el RFC 4251.

NTP

El protocolo de tiempo de red (NTP por sus siglas en inglés) es un protocolo de red para la sincronización de relojes entre sistemas de computadoras que operan en redes de enrutamiento de paquetes con latencia variable. Este protocolo tiene el propósito de sincronizar todas las computadoras participantes en un rango de unos cuantos milisegundos del tiempo universal coordinado (UTC por sus siglas en inglés). El protocolo está definido en el RFC 5905 y está en operación desde 1985. La versión actual es la 4.

El protocolo normalmente se describe en términos del modelo cliente-servidor, sin embargo, se puede usar en redes entre iguales. Las implementaciones envían y reciben marcas temporales utilizando el protocolo UDP por el puerto 123.

FTP

FTP es un protocolo de la capa de aplicación que es usado ampliamente en internet. Fue diseñado para habilitar a un usuario en una terminal a iniciar la transferencia de un archivo de una computadora a otra usando la suite TCP/IP. Las dos computadoras pueden tener diferentes sistemas operativos con diferentes sistemas de archivos y, posiblemente, codificaciones de caracteres diferente. Este protocolo está definido en el RFC 959.

SNMP

El protocolo SNMP (protocolo simple de administración de red) es un estándar que permite recolectar información y administrar una gran variedad de dispositivos y/o servicios. El protocolo está regulado por el Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés). Existen 3 versiones del protocolo, cada una con sus propios estándares.

- SNMPv1 está definido en el RFC 1157. Esta es la implementación principal y la que más servicios y/o dispositivos soportan.
- SNMPv2 está definido en los RFC 3416, RFC 3417 y RFC 3418. Esta versión incorporó una serie de mejoras de rendimiento, seguridad y de compatibilidad a futuro implementando contadores de 64 bits.
- SNMPv3 está definido en los RFC 3410-3418 y RFC 2576 es la única que se considera un estándar actualizado y la versión a implementar en nuevos dispositivos. Dejando a las dos versiones anteriores como obsoletas. Aunque en la parte principal del protocolo no se hicieron cambios, si representó un cambio de paradigma e implementación. Se enfocó en hacer el protocolo más seguro, agregando soporte para una autenticación más fuerte y comunicación privada entre los dispositivos administrados.

Debido a que SNMPv3 tomó mucho tiempo en ser adoptado, hoy en día muy común el tener que administrar dispositivos que solo soportan las versiones anteriores. Una gran cantidad de equipos de red solo soportan SNMPv1. Aunque en su momento SNMP fue revolucionario, hoy en día es

insuficiente. Algunos vendedores han creado otros protocolos para sus equipos, pero sin mucho éxito para su estandarización.

Existen 4 conceptos básicos en SNMP:

1. Los equipos que se encargan de recopilar la información de los demás dispositivos, llamados administradores (“managers”).
2. Los equipos de los que se recolecta la información, llamados dispositivos administrados (“managed devices”).
3. El software que corre en los dispositivos administrados que procesa las solicitudes de los administradores, llamado agente SNMP.
4. El software que corre en los administradores, que se conoce con las siglas de NMS (“Network Managment System”).

En términos de la recolección de información existen dos formas básicas: la recolección de información (polling), cuando el NMS solicita la información a los agentes, y las trampas en donde los agentes envían información directamente al administrador. Hay 2 tipos de trampas, las genéricas y las específicas de empresa. De las genéricas existen 6 tipos básicos definidas en el RFC 1215, las cuales son: “coldStart”, “warmStart”, “linkDown”, “linkUp”, “authenticationFailure” y “egpNeighborLoss”. Las trampas específicas de empresa son trampas definidas por los fabricantes para enviar información específica de sus dispositivos.

SNMP es un protocolo basado en UDP que utiliza los puertos 161 y 162 para SNMPv1 y SNMPv2. Los puertos 10161/udp y 10162/udp para SNMPv3. El polling se hace por el puerto 161/udp o 10161/udp mientras que las y las trampas se envían por el puerto 162/udp o 10162/udp.

Toda la información en polling se presenta en forma de árbol, compuesta por identificadores de objeto (OID por sus siglas en inglés). Los OIDs se representan por una serie de número enteros precedidos por un punto (ejemplo, .1.3.6.1.2.1.1.1.0). En donde el punto inicial representa la raíz y el número la rama correspondiente. En la Figura 3 - Árbol de OIDs, se puede apreciar la estructura de árbol. La serie de números, correspondientes a la rama, se puede traducir a un formato de texto por medio de archivos de la base de información gestionada (MIB).

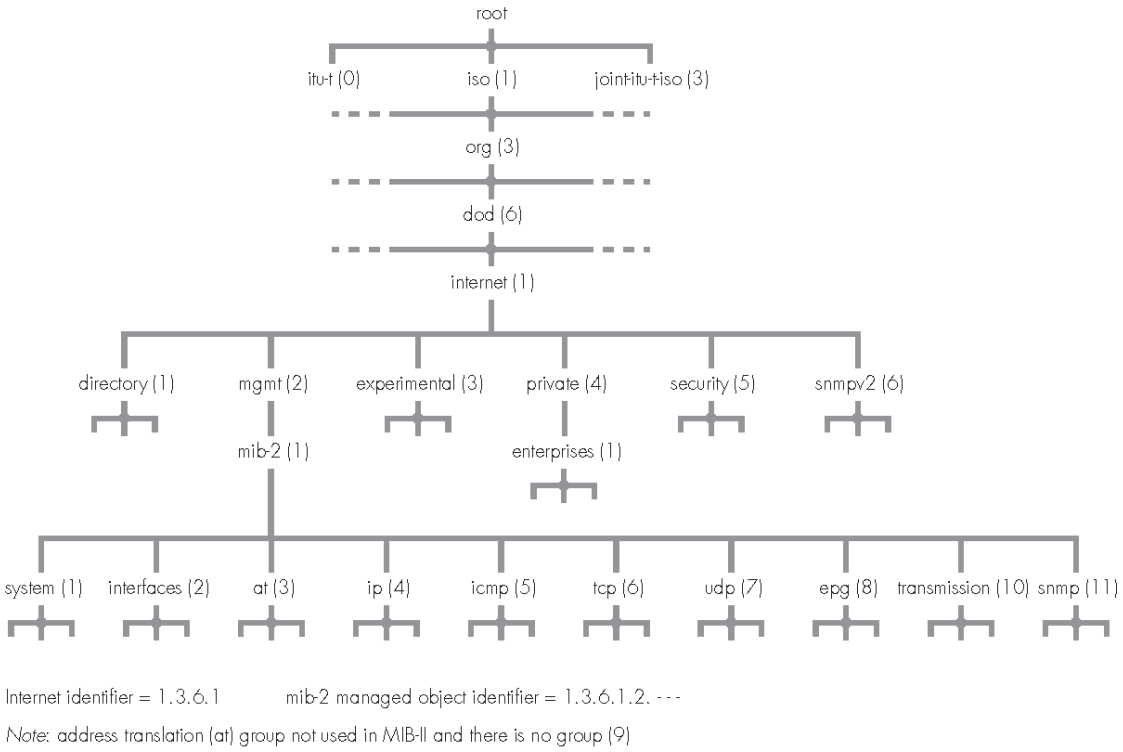

Figura 3[15] - Árbol de OIDs

Un agente puede implementar varias MIB simultáneamente, pero todos los agentes deben de implementar una en particular llamada MIB-II, la cual es la versión más reciente de MIB y está definida en el RFC 1213. Esta base tiene el propósito de proporcionar información general de administración de TCP/IP y no cubre la información particular de las funciones de los dispositivos, o la información particular de los diferentes vendedores.

Existen varios estándares de MIB para diferentes tipos de equipos, servicios y funciones. En la Tabla 5 - Estándares comunes de MIB, se muestran algunos de ellos.

Tabla 5[16] - Estándares comunes de MIB

MIB	**RFC**
ATM	2515
Frame Relay DTE Interface Type	2115
BGP Version 4	1657
RDBMS	1697
RADIUS Authentication Server	2619
Mail Monitoring	2789
DNS Server	1611

[15] Tomado de la página 557 de la fuente (8) de la bibliografía.
[16] Fuente Propia.

Una MIB es como un diccionario que permite darle interpretar el OID. En ella se define un nombre textual y se explica su significado. Cuando un vendedor implementa funcionalidad específica para uno de sus equipos, es necesario obtener la MIB correspondiente del fabricante. Con el propósito de poder interpretar la información que el agente provee y poder obtener la representación de texto de la rama del árbol correspondiente. El OID 1.3.6.1.4.1 es la rama reservada para la información específica de los vendedores.

Servicios de directorio

Un servicio de directorio sirve para llevar una asociación entre los nombres de los recursos de red con sus respectivas direcciones de red. Es una infraestructura de información compartida para localizar, manejar, administrar y organizar elementos y recursos de red, entre los cuales se pueden incluir: volúmenes, folders, archivos, impresoras, usuarios, grupos, dispositivos, números telefónicos y otros objetos. Cada recurso en la red es considerado como un objeto por el servidor del directorio (el equipo que provee el servicio de directorio). La información de un servicio en particular se almacena como una colección de atributos asociados al objeto respectivo.

Un servicio de directorio define un nombre de espacio para la red, el cual es utilizado para asignar un nombre (identificador único) a cada uno de los objetos que lo componen. De esta forma un usuario no tiene que recordar la dirección física del recurso, siempre y cuando se acuerde del nombre.

LDAP

El protocolo ligero de acceso a directorios (LDAP por sus siglas en inglés) sirve para acceder y mantener servicios de directorio distribuidos a través de la suite TCP/IP. Es una implementación simplificada del protocolo creado por la ITU en la serie de estándares X.500, llamado protocolo de acceso a directorios. Existen tres iteraciones de LDAP la más reciente es la versión 3, definida en el RFC 4511. Esta última versión, publicada en 1997, hizo a LDAP lo suficientemente robusto y expandible, lo que llevo a fuera ampliamente adoptado en la mayoría de los equipos de red y sistemas operativos.

LDAP es un protocolo de tipo cliente-servidor. El cliente se conecta al puerto 389/tcp/udp o por el puerto 636/tcp/udp del servidor si es de forma segura (conexión cifrada). El uso más común del protocolo es para proveer un lugar central donde se almacenen nombres de usuario y contraseñas. Esto permite que muchas aplicaciones y servicios diferentes se conecten con el servidor LDAP para validar usuarios.

Active Directory

El directorio activo (AD por sus siglas en inglés) es un sistema operativo de red diseñado por Microsoft. Fue originalmente construido para operar encima de Windows 2000. Con el tiempo ha evolucionado con cada iteración de Windows Server.

AD permite a los administradores manejar información de forma eficiente desde un repositorio central que se puede distribuir de forma global. Una vez que la información acerca de usuarios, grupos, computadoras, impresoras, aplicaciones y servicios ha sido agregada al directorio, se puede disponer de ella en toda la institución para su uso en por tantas personas o tan pocas como los administradores deseen.

Como lo suelen hacer todos los sistemas operativos de red AD provee autenticación, autorización y manipulación de cuentas. Adicionalmente asigna y hace cumplir las políticas de seguridad e instala y/o actualiza software.

El directorio activo utiliza LDAP versión 2 y 3, kerberos y DNS como partes fundamentales de sus servicios. En la Tabla 6 - Servicios de Active Directory, se muestran los servicios de directorio que AD provee.

Tabla 6[17] - Servicios de Active Directory

Servicio	**Descripción**
Servicios de dominio (Domain Services)	Es la estructura básica de cualquier dominio de red de Windows. Almacena la información de los miembros de dominio. Al equipo que corre este servicio se le conoce como controlador de dominio. Todos los demás servicios excepto los servicios de directorio ligeros (LDS por sus siglas en inglés) dependen de este servicio.
Servicios de directorio ligero (Lightweight DIrectory Services)	Es la implementación de LDAP empleada en AD.
Servicios de certificados (Certificate Services)	Permite crear una infraestructura de llaves públicas dentro de la organización. Con este servicio se pueden crear, validar, revocar certificados de llaves públicas para uso interno de la organización. Los certificados pueden ser usados para cifrar información (archivos, correo, tráfico de red, …) en el interior de la organización.
Servicios de federación (Federation Services)	Permite agrupar las credenciales de un usuario para el uso de servicios o recursos de red.
Servicios de gestión de derechos (Right Managment Services)	Permite limitar el acceso a la información (archivos, correo, páginas web, …) que es parte de la red y las operaciones (ver, editar, copiar, guardar o imprimir) que los usuarios autorizados pueden realizar sobre ella.

[17] Fuente Propia. Basado en fuente (12) de la bibliografía.

Contexto de la participación profesional

Definición del Problema - Monitoreo de red

En el mundo de los servicios basados en las TIC (Tecnologías de la información y comunicación) la alta disponibilidad suele ser un requisito. Dependiendo de la complejidad del servicio, el número de equipos y número de clientes; mantener una alta disponibilidad puede ser una tarea muy difícil. La forma más fácil de lograr una alta disponibilidad es por medio de un sistema de monitoreo. El cual recopile información de los equipos y elementos que forman parte del servicio y permita prevenir o, en el peor de los casos, notificar de los fallos lo más rápido posible. El problema con los sistemas de monitoreo es que tiene un costo de implementación inicial alto y no suelen ser costeables en sistemas relativamente simples, pero al aumentar la complejidad de las redes, al aumentar el número de equipos, clientes o servicios; se vuelven indispensables.

En la empresa se requería una disponibilidad alta en: el sitio web, la base de datos y los servidores de grabación de radio y televisión (24 horas). La compañía desde el inicio contaba con un sistema de monitoreo rudimentario, que reportaba el estado de algunos de los servicios críticos. Esto se hacía por medio de una tabla en la base de datos principal, donde se registraban la hora de ejecución y otros datos básicos. Esto permitía estar al tanto del estado de algunos servicios. Si alguno de los servicios no actualizaba su registro en la base de datos en cantidad determinada de minutos se enviaba un mensaje de texto por beeper o un correo electrónico a las personas de soporte. Esto era una forma bastante precaria de monitoreo, cuyos problemas eran:

- Era necesario agregar código en cada una de las aplicaciones internas para actualizar el estado en la base de datos del servicio correspondiente.
- Si la aplicación era una aplicación o servicio comercial se tenía que escribir una aplicación dedicada para su monitoreo.
- No tenía ningún tipo de redundancia. Lo que provocaba que hubiera muchos puntos críticos de falla.
- Se empleaba la misma base de datos que se utilizaba para dar servicio a los clientes. Lo que generaba una carga innecesaria en el servidor más importante de la empresa.
- No permitía prevenir problemas, solo servía para notificar de su existencia.
- No recolectaba ningún tipo de información adicional. Lo que hacía difícil el encontrar la causa del problema.
- Solo permitía notificar vía email y beeper.
- El principal punto crítico de falla del sistema era la aplicación de envío de mensajes que, si fallaba o se detenía por cualquier motivo, lo cual era común, las notificaciones nunca llegaban a los usuarios.
- No monitoreaba la disponibilidad de los servicios.
- No podía monitorear el estado de los equipos de red.

Por lo cual, al momento de proponer el uso de un sistema de monitoreo profesional, lo hice teniendo en cuenta los siguientes requerimientos:

- El almacenamiento de información de monitoreo debería de ser independiente de la base de datos principal de la empresa. Y de preferencia correr en un equipo independiente.
- Debería de poder monitorear los siguientes elementos:

    - Servicios
    - Procesos
    - Estado físico de los discos duros (temperatura y S.M.A.R.T.)
    - Recursos del equipo (Uso del procesador, disco duro, memoria y red)
    - Estado del equipo (apagado o encendido)
    - Estado de las conexiones de red
    - Equipos de red
        - Switches de red
        - Puntos de Acceso Inalámbricos
        - Enrutadores
- Tener clientes configurables para:
    - Windows XP y posterior
    - Windows Server 2003 y posterior
    - CentOS 6 y posterior
- Debía poder ser redundante
- No debía tener limite en la cantidad de equipos a monitorear.

Al presentar la propuesta mi jefe agregó tres criterios adicionales: el software debería ser de uso gratuito, correr en un sistema operativo de código abierto (preferentemente Linux) y debería poder correr en uno de los equipos que ya no se empleaban.

El servidor que se destinó para este propósito fue: un equipo con un procesador Xeon de 12 núcleos, 128 GB de memoria RAM, un par de discos duros SAS de 250 GBi mecánicos de 7200 RPM en configuración RAID 1, dos fuentes de poder y dos interfaces de red Gigabit con conectores RJ-45.

La Tabla 7 – Equipos a Monitorear, muestra los equipos que se requerían monitorear.

Tabla 7[18] – Equipos a Monitorear

Nombre del Equipo[19]	Tipo de Monitoreo	Funcionalidad	Parámetros por monitorear
Codificador01	Agente Zabbix (Windows)	Equipo de grabación de audio y video para monitoreo de radio y televisión. Estos equipos corrían múltiples instancias de un programa de grabación (desarrollo interno) para audio y video. El número de instancias dependía de la configuración específica de cada equipo. La cual iba de 0-4 capturas de canales de televisión y 1-6 estaciones de radio.	• Estado de los procesos de captura de audio y video. • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Temperatura del procesador. • Parámetros S.M.A.R.T. de los discos duros.
Codificador02			
Codificador03			
Codificador04			
Codificador05			
Codificador06			
Codificador07			
Codificador08			
Codificador09			
Codificador10			
Codificador11			
Codificador12			
Codificador14			
Codificador15			
Codificador16			

[18] Fuente Propia.
[19] No se utilizaron los nombres de verdaderos de los equipos por motivo de seguridad.

Codificador17 Codificador18 Codificador19			
Servidor SQL	Agente Zabbix (Windows)	Servidor principal de la base de datos	• Estado del servicio de SQL • Estado de todos los servicios principales de Windows. • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Temperaturas internas del equipo. • Estado las fuentes de alimentación. • Parámetros S.M.A.R.T. de los discos duros. • Desempeño de los discos duros • Estado del arreglo RAID
Servidor SQL de Respaldo		Servidor de respaldo de la base datos.	
Servidor WEB de Radio y Televisión	Agente Zabbix (Windows) y HTTP	Servidor (virtualizado) en donde se corría el servicio IIS (Internet Information Services) que permite el hospedaje y funcionamiento correcto del sitio WEB de radio y televisión de la empresa.	• Estado del servicio IIS • Funcionamiento del sitio web de radio y televisión • Estado de todos los servicios principales de Windows. • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Temperaturas internas del equipo. • Estado las fuentes de alimentación. • Parámetros S.M.A.R.T. de los discos duros.
Servidor WEB de Prensa	Agente Zabbix (CentOS) y HTTP	Servidor (virtualizado) en donde se corría el servicio de servidor de Apache HTTP que permite el hospedaje y funcionamiento correcto del sitio WEB de prensa.	• Estado del servicio httpd • Funcionamiento del sitio web de prensa • Estado de todos los servicios principales de CentOS • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Temperaturas internas del equipo. • Estado las fuentes de alimentación.
Servidor Respaldo WEB Prensa			
Servidor de Archivos Multimedia	Agente Zabbix (Windows)	Servidor (virtualizado) usado para correr el servidor de Windows Media Server que permitía transmitir los archivos de audio y video por medio del protocolo MMS (Microsoft Media Server)	• Estado del servicio Windows Media Server • Estado de todos los servicios principales de Windows. • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro).

			• Temperaturas internas del equipo. • Estado las fuentes de alimentación. • Parámetros S.M.A.R.T. de los discos duros.
Servidor de Servicios Servidor de Respaldo de Servicios	Agente Zabbix (Ubuntu)	Equipo utilizado para los siguientes servicios: • Correo • Active Directory • DNS • Jabber • Gateway • DHCP	• Estado del servicio httpd • Estado de los procesos de Active Directory. • Estado de los procesos de Correo. • Estado de los procesos de Jabber. • Estado de los procesos de DNS. • Estado de los procesos del servicio de la puerta de enlace. • Estado del servicio dhcpd • Estado de todos los servicios principales de CentOS • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Temperaturas internas del equipo. • Estado las fuentes de alimentación. • Parámetros S.M.A.R.T. de los discos duros.
Servidor de Respaldo de DNS	Agente Zabbix (Windows)	Equipo empleado para grabación de estaciones locales en Guadalajara y para respaldo de DNS.	• Estado de los procesos de captura de audio y video. • Estado de los procesos de DNS. • Estado de todos los servicios principales de CentOS • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Temperaturas internas del equipo. • Estado las fuentes de alimentación. • Parámetros S.M.A.R.T. de los discos duros.
Noticias 01 Noticias 02 Noticias 03 Noticias 04 Noticias 05 Noticias 06 Noticias 07 Noticias 08 Noticias 09	Agente Zabbix (Windows)	Equipo usado por el personal de monitoreo de contenido de noticias en radio y televisión. Equipo que sólo requería correr un navegador, aplicaciones básicas de procesamiento de palabras, aplicaciones de comunicación interna y aplicaciones de uso interno.	• Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros.

Noticias 10			
Noticias 11			
Noticias 12			
Noticias 14			
Noticias 15			
Noticias 16			
Noticias 17			
Comerciales 01	Agente Zabbix (Windows)	Equipo usado por el personal de monitoreo de contenido de comerciales en radio y televisión. Equipo que solo requería correr un navegador, aplicaciones básicas de procesamiento de palabras, aplicaciones de comunicación interna y aplicaciones de uso interno.	
Comerciales 02			
Comerciales 03			
Comerciales 04			
Comerciales 05			
Comerciales 06			
Comerciales 07			
Comerciales 08			
Comerciales 09			
Comerciales 10			
Prensa 01	Agente Zabbix (Ubuntu)	Equipo usado por el personal de captura de prensa. Equipo que sólo requería correr un navegador, aplicaciones básicas de procesamiento de palabras, aplicaciones de comunicación interna y aplicaciones de uso interno.	• Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros.
Prensa 02			
Prensa 03			
Prensa 04			
Fotografía Prensa	Agente Zabbix (Windows)	Máquina empleada para hacer la captura de las imágenes de los periódicos y revistas por medio de la cámara de alta resolución.	• Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros.
Servidor Captura Audio y Video de Internet	Agente Zabbix (CentOS)	Máquina empleada para la captura de streams de video y audio de internet	• Estado del servicio de control de grabación de streams de internet. • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros.
Servidor de Virtualización 01	Agente Zabbix (XenServer) y SNMP	Servidor de virtualización empleado para hospedar varios de los servidores mostrados en esta lista de forma virtual.	• Estado de las diferentes máquinas virtuales. • Estado de los servicios principales de XenServer. • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro).

Servidor de Virtualización 02	Agente Zabbix (XenServer) y SNMP		• Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros.
Servidor Servicios de Prensa 01	Agente Zabbix (CentOS)	Servidor encargado de realizar el reconocimiento de texto y la indexación de este. Así como la generación de imágenes de los diferentes recortes de las publicaciones y generación de archivos .pdf y documentos solicitados por los usuarios del sitio WEB de prensa.	• Estado del servicio de Solr. • Estado de los servicios de las aplicaciones, de desarrollo interno, para la generación de archivos .pdf, imágenes y reconocimiento de caracteres. • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros.
Servidor Servicios de Prensa 02	Agente Zabbix (CentOS)		
Servidor de Monitoreo	Agente Zabbix (CentOS)	Servidor de Monitoreo Zabbix	• Estado de todos los servicios principales de CentOS • Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros.
Servidor de Monitoreo de Respaldo		Servidor de Monitoreo Zabbix (virtualizado) de respaldo.	
NAS 01	SSH, SNMP	Servidor de almacenamiento en red para los archivos de audio y video del servicio de radio y televisión.	• Recursos del equipo (memoria, uso de red, uso CPU y espacio disponible en el disco duro). • Estado de funcionamiento del equipo (encendido o apagado) • Parámetros S.M.A.R.T. de los discos duros. • Temperaturas internas del equipo • Estado del RAID por software • Estado del servicio de Samba • Estado del servicio SSH
NAS 02	SSH, SNMP		
NAS 03	SSH, SNMP		
NAS 04	SSH, SNMP		
NAS Prensa	SSH, SNMP	Servidor de almacenamiento en red para las imágenes y archivos .pdf de prensa.	
Switch 01	SNMP	Switch para la conexión de red de los equipos en el área de servidores.	• Estado y estadísticas de las interfaces de ethernet (UTP y fibra óptica) • Estado de funcionamiento del equipo (encendido o apagado)
Switch 02		Switch para la conexión de red de los equipos de los capturistas de radio y televisión.	
Switch 03		Switch para la conexión de red de los equipos del personal de prensa.	
Switch 04		Switch para la conexión de red de los equipos del personal administrativo.	

Enrutador Principal	SNMP	Equipo encargado de la conexión principal a internet de la empresa.	• Estado y estadísticas de las interfaces de ethernet (UTP y fibra óptica) • Estado de funcionamiento del equipo (encendido o apagado)
Enrutador Secundario		Equipo encargado de la conexión a internet de respaldo.	
Enrutador Servicio Usuarios	ICMP	Equipo encargado de la conexión a internet	• Estado de funcionamiento del equipo (encendido o apagado) • Estado de la conectividad del equipo.
Servidor VPN Y Firewall	SNMP	Equipo de seguridad de cortafuegos y VPN	• Estado de funcionamiento del equipo (encendido o apagado). • Estado de la conectividad del equipo. • Estado del servicio de VPN • Estado y estadísticas del cortafuegos.
Access Point 01	SNMP	Equipo de red encargado de dar cobertura de WiFi en las oficinas de la empresa.	• Estado y estadísticas de las interfaces de ethernet (UTP) • Estado de funcionamiento del equipo (encendido o apagado) • Lista de equipos conectados
Access Point 02	SNMP		

En la Figura 4 - Mapa de Red, se muestra como estaban interconectados los equipos de la Tabla 7 – Equipos a Monitorear.

Dos cosas que se tuvieron que resolver al momento de planificar el sistema de monitoreo fue la recolección de la información S.M.A.R.T. de los discos duros, las temperaturas del procesador, las temperaturas placa madre y velocidad de los ventiladores. Para esto se investigaron las opciones disponibles y se decidió emplear las utilerías de smartmontools y lm-sensors para obtener esa información de los equipos.

La utilería de smartmontools se seleccionó porque estaba incluida en los servidores NAS que se empleaban en la empresa y porque tenían paquetes de instalación para Windows y CentOS. Lo que permitiría simplificar las configuraciones y la instalación en los equipos. La cantidad de información que esta herramienta podía recopilar dependía del fabricante y modelo del disco, en algunos se podía monitorear hasta la temperatura, pero en todos se podían monitorear los parámetros básicos de salud.

El programa de lm-sensors se decidió emplear para monitorear las temperaturas internas de los equipos y las velocidades de los ventiladores. Era posible, en la mayoría de los casos, monitorear la temperatura del procesador y varios sensores de temperatura de la tarjeta madre. La información de la velocidad de los ventiladores no estaba disponible en todos los equipos, dependía de la compatibilidad del software con la tarjeta madre.

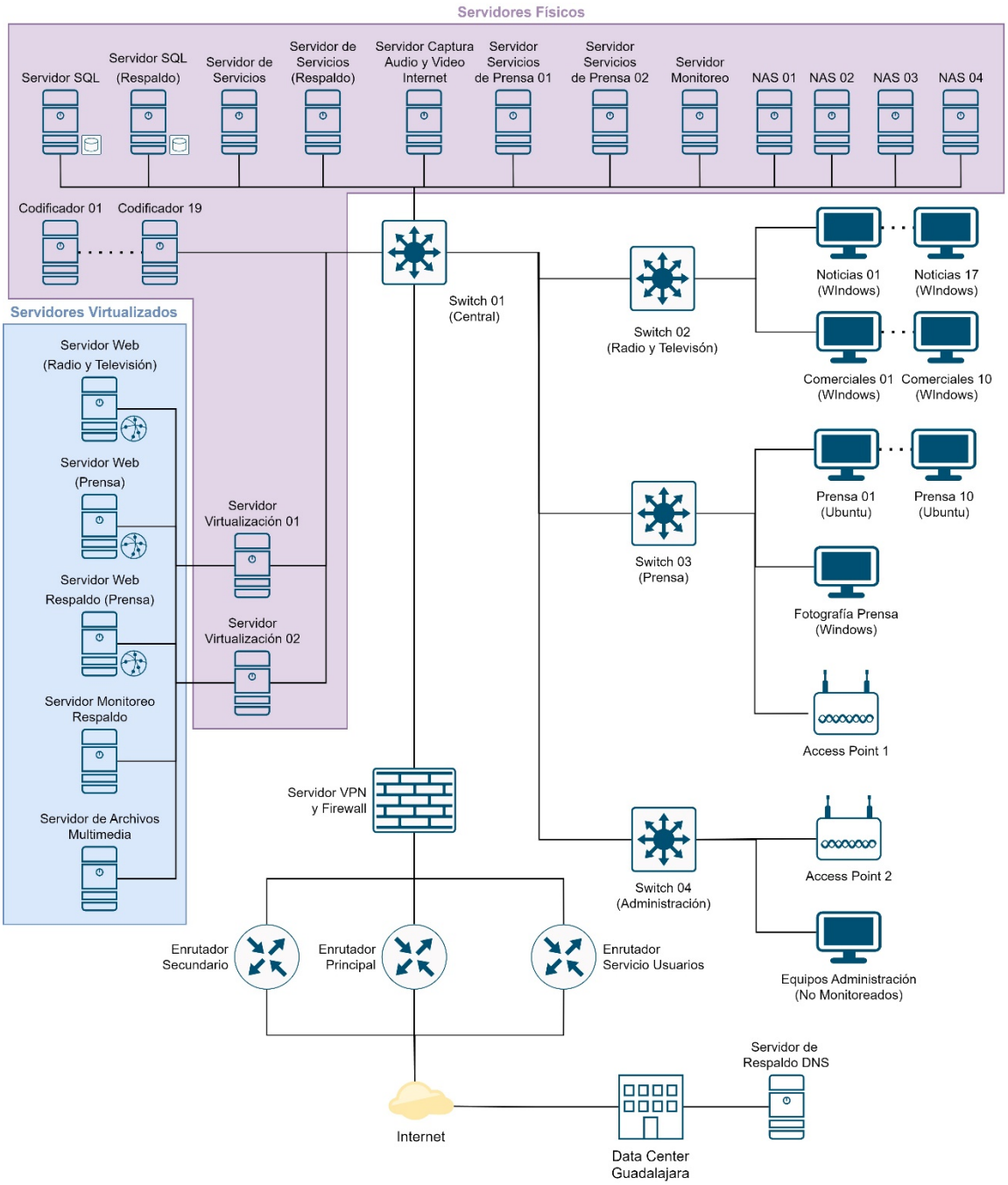

Figura 4[20] - Mapa de Red

Definición del Problema - Configuración, despliegue y mantenimiento de servicios

Active Directory, DHCP, DNS, NTP y FTP

Cuando yo llegué a la empresa se utilizaba Windows Server para proporcionar múltiples servicios a los equipos de red, como lo eran: HTTP, Active Directory, DHCP, DNS, NTP y FTP. Esto se hacía en servidores virtuales por separado, un servidor por servicio. Debido a problemas de licencias de

[20] Fuente propia.

Windows se me requirió buscar soluciones que permitieran consolidar los servicios y disminuir el costo de licenciamiento tanto como fuera posible. En la forma en la que se estaba empleando el servidor, se tenían que pagar licencias a Microsoft por cada equipo que conectaba al servidor (CAL) y una licencia adicional si el equipo era parte del dominio (CAL Active Directory). Todo esto llevó a que el proyecto fuera prioritario para la empresa. Y que el proyecto tuviera los siguientes requerimientos:

1. Que todo se pudiera correr en un sistema operativo de uso libre (Linux o Unix).
2. Consolidar los servicios lo más posible.
3. Que el sistema tuviera una interfaz de usuario relativamente amigable. De tal forma de que las personas de soporte pudieran tomar control sin mucha capacitación y conocimientos de Linux.
4. Que la solución fuera de código abierto y/o uso libre comercial.
5. La posibilidad de tener redundancia. Utilizando un servidor físico y uno virtual.

En especial había que prestar especial atención al servicio de NTP, ya que todas las grabaciones de radio y televisión se registraban con el tiempo local del equipo en el que se grababan. En caso de que hubiera una discrepancia entre el tiempo del equipo y la hora oficial se presentaban problemas. Si eran unos segundos no era muy grave, sin embargo, si la desincronización llegaba al orden de minutos podía ser bastante grave. En especial cuando se hacía capturas de las notas usando la transmisión en vivo.

Para el servicio de HTTP era necesario utilizar el servidor web de Windows Server ya que todo el sitio del servicio de radio y televisión estaba diseñado usando páginas activas de servidor, ASP por sus siglas en inglés, que es una tecnología propietaria de Microsoft. Al final, la idea era terminar con un solo servidor de Windows Server y un mínimo número de servidores de uso libre para prestar los demás servicios. La configuración del servidor de Windows fue responsabilidad del encargado de soporte, la configuración de los demás servicios fueron mi responsabilidad.

Reconocimiento óptico de caracteres

Una de las principales razones por las que la empresa me contrató fue para crear el sistema que se emplearía para hacer la captura y procesamiento de la información. Esto lo realizaría en conjunto con el dueño de la empresa. La idea era crear el sistema para segmentar y procesar las imágenes de alta resolución de los medios impresos, clasificar la información y crear herramientas de búsqueda. Todo debía partir de separar las páginas de los diferentes medios impresos en notas individuales. Cada una con su encabezado, cuerpo, clasificaciones (manuales y automáticas) y texto (obtenido de forma automatizada).

Al inicio mi trabajo se enfocó en diseñar la interfaz gráfica y la estructura de la base de datos. Mientras que el dueño de la empresa experimentaba y decidía la forma en la que se iban a procesar los textos. Una vez terminada la experimentación. Mi jefe resolvió que emplearíamos Tesseract, la herramienta de OCR desarrollada por Google.

Una vez tomada esa decisión, se me solicitó que implementara las siguientes herramientas basadas en el motor de OCR:

1. Una herramienta que permitiera obtener fácilmente el texto del encabezado de la nota, para ahorrar tiempo a los capturistas. El programa debería correr en el servidor de prensa y responder de forma instantánea.
2. Un programa que, una vez que la nota se hubiera segmentado y clasificado por el capturista, hiciera el reconocimiento de texto y guardara la información en la base de datos.
3. Una herramienta que hiciera OCR a todas las páginas, de tal manera que tuviera todo el texto, incluyendo las partes que no eran procesadas por los capturistas.

Todo esto se debía implementar en Linux y utilizando programas de código abierto y/o de uso comercial gratuito.

Búsqueda de texto completo

Mientras yo me encargaba de la implementación de las herramientas de reconocimiento de texto, mi jefe se dedicó a buscar herramientas de búsquedas de texto completo. Esto era necesario ya que versión del servidor de SQL que se empleaba en la empresa no era apto para esta tarea, y existían herramientas más especializadas y robustas con este propósito. Le tomó a mi jefe un par de semanas elegir la solución, inmediatamente después inicié el desarrollo.

Una vez concluidas las primeras versiones de las herramientas de OCR, se hicieron pruebas de producción del sistema de prensa. En las que se presentó un problema de desempeño con el software de búsquedas de texto completo, el procesador del servidor se saturaba al procesar más de 10 indexaciones de textos en paralelo. Lo cual era causado por que los textos incluían caracteres especiales (acentos, tildes y diéresis). Como todos los textos que se iban a procesar estaban en español, se requirió buscar otra solución. Mi jefe ya no tuvo el tiempo para encargarse el mismo y a partir de ese momento la responsabilidad de encontrar la nueva solución recayó en mí.

Los requisitos del proyecto fueron:

1. La solución tenía que estar basada en programas de código abierto o de uso libre.
2. Debía tener mayor funcionalidad que la que se tenía en la versión de SQL Server que se empleaba en la empresa.
3. Debía de poder correr en Linux.
4. De preferencia debía contar con una gran cantidad de documentación.
5. Tenía que poder manejar con facilidad millones de textos.
6. No debía demandar muchos recursos del sistema.
7. Debía poder procesar adecuadamente texto con una gran cantidad de caracteres especiales.

Metodología utilizada

Implementación - Monitoreo de Redes

En condiciones normales el primer paso para la implementación del sistema de monitoreo hubiera sido el realizar una evaluación de las opciones del software disponible, para confirmar que cumpliera con todos los requerimientos. Sin embargo, ese fue uno de los proyectos que realicé en mi servicio social en una institución pública. En ese proyecto hice una investigación de los programas profesionales de monitoreo de licencia abierta y uso comercial libre, que corrían en Linux. Esta investigación se hizo para evaluar las opciones disponibles y determinar si era viable el migrar del software de monitoreo que se empleaba, de licencia comercial, a una que no tuviera costo el programa y el costo de soporte fuera menor.

El programa más prometedor que se encontró en esa investigación fue Zabbix, en ese momento en su versión 2.0 (2013). El programa no cumplía con todas las necesidades de la institución, pero fue la opción que cubría mejor las necesidades de la institución. A parte de ser el que contaba con más documentación y con el agente oficial con mayor soporte para diferentes sistemas operativos.

Con el paso del tiempo Zabbix maduró, y para cuando se planteó el proyecto en la empresa en 2016, ya estaba en su versión 3.2 y contaba con mucha más funcionalidad, la cual era suficiente para los requerimientos de la empresa. Por lo que sugerí su uso para la implementación del sistema de monitoreo.

Al inicio mi jefe me solicitó que hiciera una demostración sencilla del monitoreo de algunos de los equipos para ver si continuábamos con el proyecto. Esto se realizó utilizando una máquina virtual como servidor, algunos de los equipos de remplazo y otras máquinas virtuales como equipos a monitorear. Esto tomo un par de semanas. Después de la demostración, mi jefe aprobó el proyecto y comencé con la implementación final.

Implementación del monitoreo usando Zabbix

Zabbix es un servidor de monitoreo que se puede instalar en múltiples sistemas operativos, por lo cual el primer paso fue determinar cuál sería el más adecuado para el proyecto. Se seleccionó CentOS 7, porque se empleaba para los servidores del área de prensa y le eran familiares a todo el personal de soporte. Otra ventaja de este sistema operativo era que existían contenedores nativos de Zabbix, permitiendo una instalación sencilla sin necesidad de tener que compilar ningún paquete.

El procedimiento que seguí para la implementación se puede resumir en los siguientes pasos.

1. Instalación del sistema operativo.
2. Instalación del servidor de Zabbix.
3. Instalación y configuración del agente de Zabbix en el mismo servidor.
4. Creación de los scripts para el monitoreo de características especiales.
    a. Scripts de monitoreo de sensores de temperatura, velocidad y voltaje por medio de “lmsensosrs”
    b. Scripts de monitoreo de estado de los discos duros por medio se “smartmontools” y la tecnología S.M.A.R.T.
5. Configuración en el servidor de los equipos que se iban a monitorear sin agente. De este tipo de monitoreo existían tres diferentes opciones.

a. Equipos que se monitoreaban por el protocolo ICMP (Esto se hacía para todos los equipos. Pero había equipos que solo se monitoreaban de esta forma).
b. Equipos que se monitoreaban por SNMP.
    i. Configuración del MIB
c. Equipos que se monitoreaban por SSH.

6. Instalación y configuración de los agentes en los diferentes equipos que lo requerían.
    a. Agente de Linux
        i. CentOS 6 y CentOS 7
            1. Instalación y configuración de “lm-sensors”
            2. Instalación y configuración de “smartmontools”
        ii. FreeNas
    b. Agente de Windows
        i. Instalación y configuración de “lm-sensors”
        ii. Instalación y configuración de “smartmontools”
7. Monitoreo HTTP
    a. Monitorear el sitio de radio y televisión
    b. Monitorear el sitio de prensa
8. Crear los mapas en Zabbix
    a. Mapa para las computadoras del área de prensa
    b. Mapa para las computadoras del área de comerciales
    c. Mapa para las computadoras del área informativa
    d. Mapa para las computadoras de grabación de radio y televisión
    e. Mapa para interconexión de los equipos en la red
    f. Mapa para los equipos de red
    g. Mapa para los servidores de prensa
    h. Mapa para los servidores de radio y televisión
    i. Mapa para los servidores de almacenamiento
    j. Mapa para los servidores web
    k. Mapa para los servidores de los demás servicios
    l. Mapa global (incluye vínculos a las demás pantallas y mapas que se crearon).
9. Crear las pantallas de Zabbix
    a. Pantallas para los servidores de virtualización
    b. Pantallas para los servidores de almacenamiento
    c. Pantallas para los servidores web
    d. Pantallas para los servidores SQL
    e. Pantallas para los servidores de los demás servicios
    f. Pantallas para los equipos de red
10. Ajustar la prioridad de las alertas
    a. Elementos detectados automáticamente
    b. Elementos configurados manualmente

El proceso inicial de configuración se puede realizar siguiendo la documentación en línea de Zabbix, o usando uno de los múltiples libros de la editorial Packt[21]. Por lo cual no considero que sea necesario colocar los pormenores. Sin embargo, en algunos de los pasos si fue necesario un poco más de "creatividad" e investigación para resolver las necesidades del proyecto y en estos casos los detalles si son importantes y es necesario mencionarlos.

El primer paso para monitorear un equipo con Zabbix o cualquier otro sistema de monitoreo es determinar cuál es la información que nos interesa obtener de cada equipo. Una vez que se sabe cuáles son los elementos por monitorear, es necesario seleccionar una o varias formas de monitoreo que lo permitan. Lo ideal en cada equipo era usar el mínimo número de métodos de monitoreo, con el propósito de ahorrar recursos en el servidor y en cada uno de los equipos. Pero algunos métodos tienen capacidades limitadas de recolección de datos por lo cual fue necesario múltiples métodos de monitoreo.

Para el proyecto la selección de los datos a monitorear y el método se determinaron al momento de la planeación. En la Tabla 7 – Equipos a Monitorear, se muestran los métodos con los cuales se monitoreo a cada uno de los equipos y los elementos que se monitorearon en cada uno. Considero que es necesario explicar a detalle las ventajas y desventajas de cada una de las formas de monitoreo. En la Tabla 8 – Métodos de monitoreo se muestra cada una de las formas de monitoreo, los datos que se pueden monitorear y sus ventajas y desventajas.

Aunque uso del agente de Zabbix suele ser el método de monitoreo más completo, no siempre se podía utilizar, era muy complicado obtener información específica o existía una forma mucho más simple para obtener ciertos elementos. En la mayoría de los equipos la información que determinó los métodos de monitoreo fueron los parámetros SMART de los discos duros y las temperaturas internas. En los servidores de marca comercial la información se podía obtener por medio del agente SNMP. En los equipos armados fue necesario el usar el software smartmontools y de lm-sensors. En los NAS más viejos (NAS01 y NAS02) fue imposible de instalar lm-sensors, porque tenían una versión muy antigua del sistema operativo y ya no tenía soporte para muchas de las librerías que se requerían. Se habría podido lograr, pero se requería compilar una gran cantidad de elementos y no había certeza de que funcionara al final, por lo cual se decidió no invertir el tiempo.

En la Tabla 8 – Métodos de monitoreo, se muestran los diferentes métodos que se emplearon, así como la información que se recolectaba y algunas de sus ventajas y desventajas.

[21] Para el proyecto se utilizó la segunda edición del libro titulado "Mastering Zabbix" escrito por Andrea Dalle Vacche y el libro titulado "Zabbix: Enterprise Network Monitoring Made Easy" escrito por Rihards Olups. Andrea Dalle Vacche y Patrik Uytterhoeven. Ambos de la editorial Packt. Ambos forman parte de la bibliografía de este trabajo siendo las fuentes (7) y (6) respectivamente.

Tabla 8[22] – Métodos de monitoreo

Método de Monitoreo	Forma de configuración	Datos para recolectar	Ventajas	Desventajas
Chequeos simples (ICMP y TCP/UDP)	La configuración se hace directamente en el servidor y no se requiere acceso al equipo remoto (host).	Solamente se puede recolectar valores básicos de la conexión de red. Permitiendo: • Saber si el equipo responde a un ping. • Si hay perdida de paquetes en la conexión. • Saber si un puerto TCP/UDP está respondiendo. • Saber si un servicio específico está activo en el equipo remoto.	No requiere acceso al equipo. Se puede implementar para cualquier equipo de red que no bloque paquetes ICMP o bloquee activamente al servidor.	La información que se obtiene es limitada. Y es más para notificar de un problema en la interfaz de red que si el equipo o servicio están funcionando adecuadamente.
SSH	La configuración requiere de credenciales para establecer la conexión. Por lo cual si no se tienen las credenciales o el servicio de SSH no está activado en el equipo remoto es necesario hacer las configuraciones correspondientes directamente en el equipo. Adicionalmente dependiendo de los valores a monitorear puede ser necesario crear scripts/programas que se encarguen de recolectar la información. Los cuales cada uno tienen que ser configurados de manera independiente en el equipo remoto (host).	Por medio de esto se puede recolectar casi cualquier tipo de información. El servidor va a tener un acceso tan amplio al sistema como las credenciales y los programas/comandos/scripts tengan.	La gran mayoría de equipos tiene servidores SSH y por lo cual es la forma más amplia que existe para acceder a una gran cantidad de equipos. Incluyendo una gran cantidad de equipos viejos que no tienen interfaz gráfica. Se puede obtener casi cualquier parámetro si se conocen los comandos o se tiene la aplicación/script adecuado para recolectar los valores.	Tiene riesgos de seguridad. Ya que se da acceso a una conexión a la consola de forma remota es necesario tener en consideración el acceso que tienen las credenciales que se usen para el monitoreo. La configuración puede ser relativamente compleja. Entre más segura más complicada es la conexión. Es necesario contar con los comandos o hacer un programa/script que colecte la información que se requiere.
SNMP	La configuración se hace tanto en el servidor como en el equipo remoto.	Se puede recolectar tanta información como el servidor SNMP del equipo provea. Esto es variable dependiendo del fabricante del equipo.	Es una forma de monitoreo que no requiere de agente.	No está disponible en todos los equipos.

[22] Fuente Propia.

	Es necesario confirmar que el servidor SNMP está activado en el equipo remoto y que se puede establecer la conexión. Cuando se da de alta este tipo de monitoreo la plantilla básica incluye solo los elementos más básicos. Por lo que cualquier dato específico del equipo que se desee monitorear es necesario darlo de alta utilizando el sistema de referencia OID del módulo MIB correspondiente.		La cantidad de información que se puede obtener es vasta en casi cualquier equipo que cuenta con este servidor. La configuración de cada uno de los elementos a configurar suele ser sencilla una vez que se conoce el módulo MIB del equipo remoto. Es un sistema seguro ya el acceso al equipo está limitado por el protocolo SNMP.	En equipos viejos o con poca documentación puede ser difícil navegar e identificar la información que se requiere. Normalmente esto se debe a la falta de documentación de los módulos MIB.
Agente	Esto requiere acceso tanto al servidor como al equipo remoto y es necesario instalar el agente en el equipo remoto. La configuración de los elementos a monitorear depende de si son elementos predeterminados del agente o si son elementos personalizados. En el caso de los elementos predeterminados la configuración se hace directamente en el servidor. Y por medio de las plantillas de agente para cada sistema operativo, incluidas con el servidor, la configuración de los elementos más utilizados es relativamente simple. Si se requiere de algún elemento personalizado es necesario hacer la configuración en el agente del equipo remoto, así como en el servidor.	La cantidad de datos que puede recolectar es muy grande. Y los elementos incluidos en las plantillas de cada sistema operativo es más que suficiente para el monitoreo profundo (no específico) de cualquier sistema.	Permite monitorear grandes cantidades de elementos fácilmente. Adicionalmente permite monitorear cualquier cosa en el equipo, ya que se tiene acceso a ejecutar código en el equipo remoto (con los permisos que tenga el agente). En general es la opción más simple para recolectar la mayor cantidad de información de un sistema con la menor cantidad de configuración. Normalmente no es necesario usar otro método de monitoreo para obtener todos los datos que se requieren.	Es necesario que exista el cliente adecuado para el sistema operativo que corre el equipo remoto. Consume recursos adicionales del equipo remoto. Tiene riesgos de seguridad si no se configura adecuadamente.
HTTP	La configuración se hace directamente en el servidor. Sin embargo; si se requiere de credenciales para el acceso a las páginas es necesario configurar eso en el sistema/equipo correspondiente.	Permite recolectar información del tiempo que se tardó en cargar la página web, si se cargó exitosamente o si se encontraron errores al momento de cargar. Así como revisar el contenido de la página para determinar si es el adecuado.	Permite monitorear un sitio o aplicación web para tener una idea de la experiencia del usuario y ver que todo funcione adecuadamente.	No es un proceso simple y en caso de haya formularios, accesos o múltiples redirecciones la configuración puede ser complicada

Monitoreo por ICMP

Es importante mencionar que todos los equipos se monitoreaban por medio del ICMP, adicionalmente a los métodos listados en la Tabla 7 – Equipos a Monitorear. Esto se hizo ya que es la forma predeterminada de las plantillas de Zabbix (Figura 5 - Alta de nuevo host e Figura 6 - Librería de Plantillas de Zabbix 3) y provee información útil para detectar problemas en la red.

El único equipo que solamente se monitoreo por ICMP fue el enrutador de los usuarios. Se hizo así porque era el equipo entregado por el proveedor de internet y no se tenía acceso a la consola para poder activar las opciones de monitoreo.

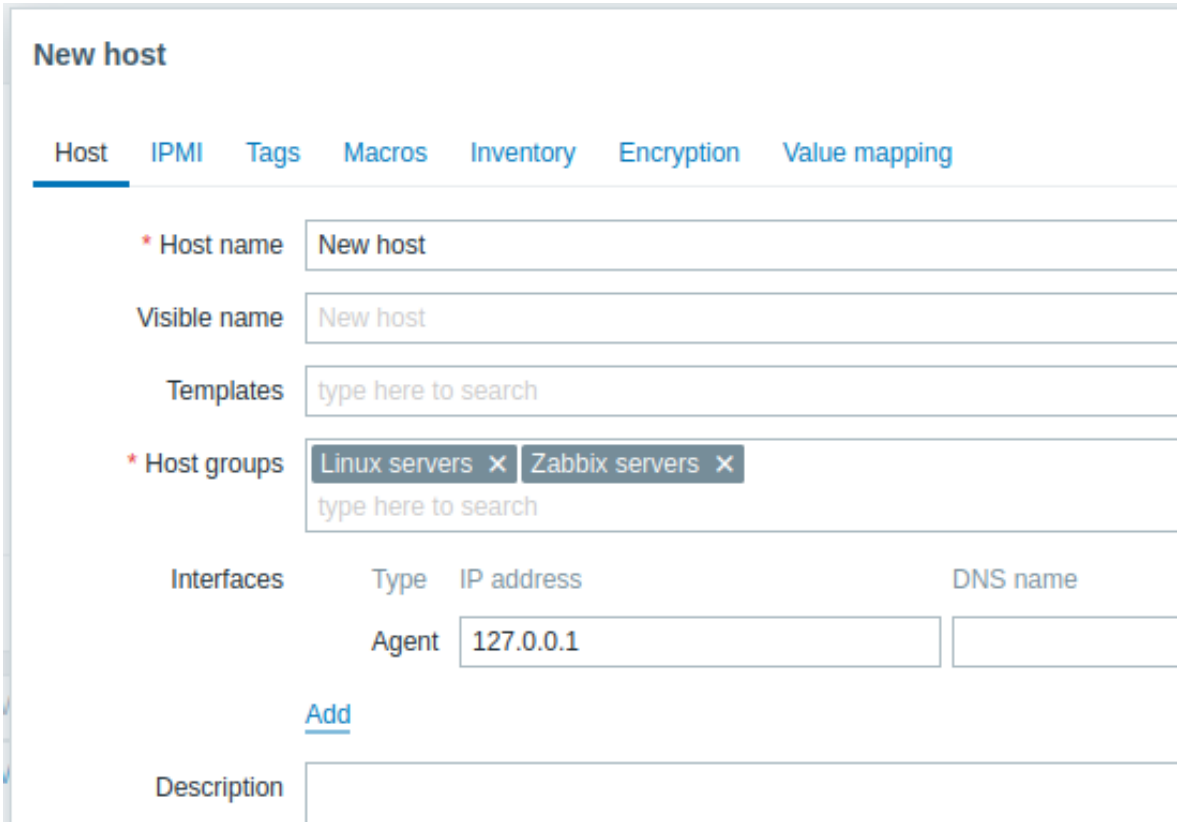

Figura 5[23] - Alta de nuevo host

[23] Tomado de la fuente (11) de la bibliografía. De la dirección: https://www.zabbix.com/documentation/current/es/manual/quickstart/host

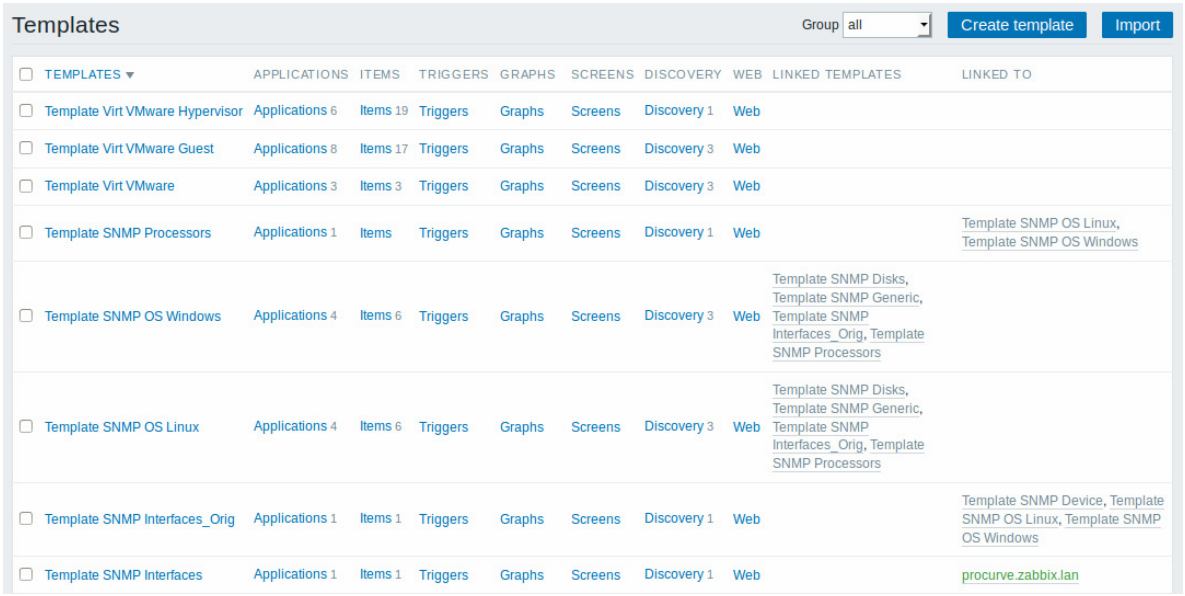

Figura 6[24] - Librería de Plantillas de Zabbix 3

Para monitorear a un equipo por medio de ICMP solo se requiere de la dirección IP y determinar qué se va a monitorear. Los chequeos simples, disponibles en Zabbix son: ping, tiempo de respuesta al ping, pérdida de paquetes, tiempo de respuesta y accesibilidad de puertos tcp y udp. En todos los equipos se empleaba el ping y el tiempo de respuesta. En cualquier equipo que proveía un servicio de red, se hacía el monitoreo de puertos. En los servidores de FTP, correo, web, NTP y LDAP (Active Directory) se hacía adicionalmente el monitoreo de tiempo de respuesta de los puertos. Los mismo se hizo para los servidores que se monitoreaban por medio de SSH.

Monitoreo por SSH

Todos los equipos que se monitorearon por medio de SSH requirieron de la creación del archivo de llave en el servidor de Zabbix, que luego se debe copiar en el servidor a monitorear. Esto para evitar el almacenar las contraseñas en la configuración de Zabbix y que en ningún momento se transmitieran por la red. Por medio de la llave el servidor se podía conectar al equipo remoto sin necesidad de una contraseña. Dicha llave estaba asociada no solo al servidor, sino a un usuario en el equipo remoto, para evitar problemas de seguridad por el uso del superusuario root, se creó un usuario llamado Zabbix en los equipos remotos y se le asignaron los permisos necesarios para ejecutar los comandos necesarios para el monitoreo.

La decisión de monitorear equipos por medio de SSH era el último recurso. Solo se usaba si el equipo no contaba con SNMP, o se requería de más información de la que proporcionaba el agente SNMP y no era posible instalar el agente de Zabbix. Los principales elementos que se querían monitorear eran la información del SMART, de los discos duros y la información de temperatura del procesador y la tarjeta madre. Para lograr esto era necesario instalar en cada uno de los equipos las utilerías de smartmontools y la de lm-sensors. Dependiendo del sistema operativo del equipo el procedimiento

[24] Tomado de la fuente (11) de la bibliografía. De la dirección: https://www.zabbix.com/documentation/3.0/en/manual/web_interface/frontend_sections/configuration/templates

era diferente. En el caso de los servidores NAS las herramientas de SMART ya estaban instaladas y solo era necesario instalar lm-sensors cuando existía una versión para el sistema operativo

Una vez realizado esto simplemente se configuraban los parámetros en el servidor de Zabbix (Figura 7 - Configuración SSH de un host en Zabbix).

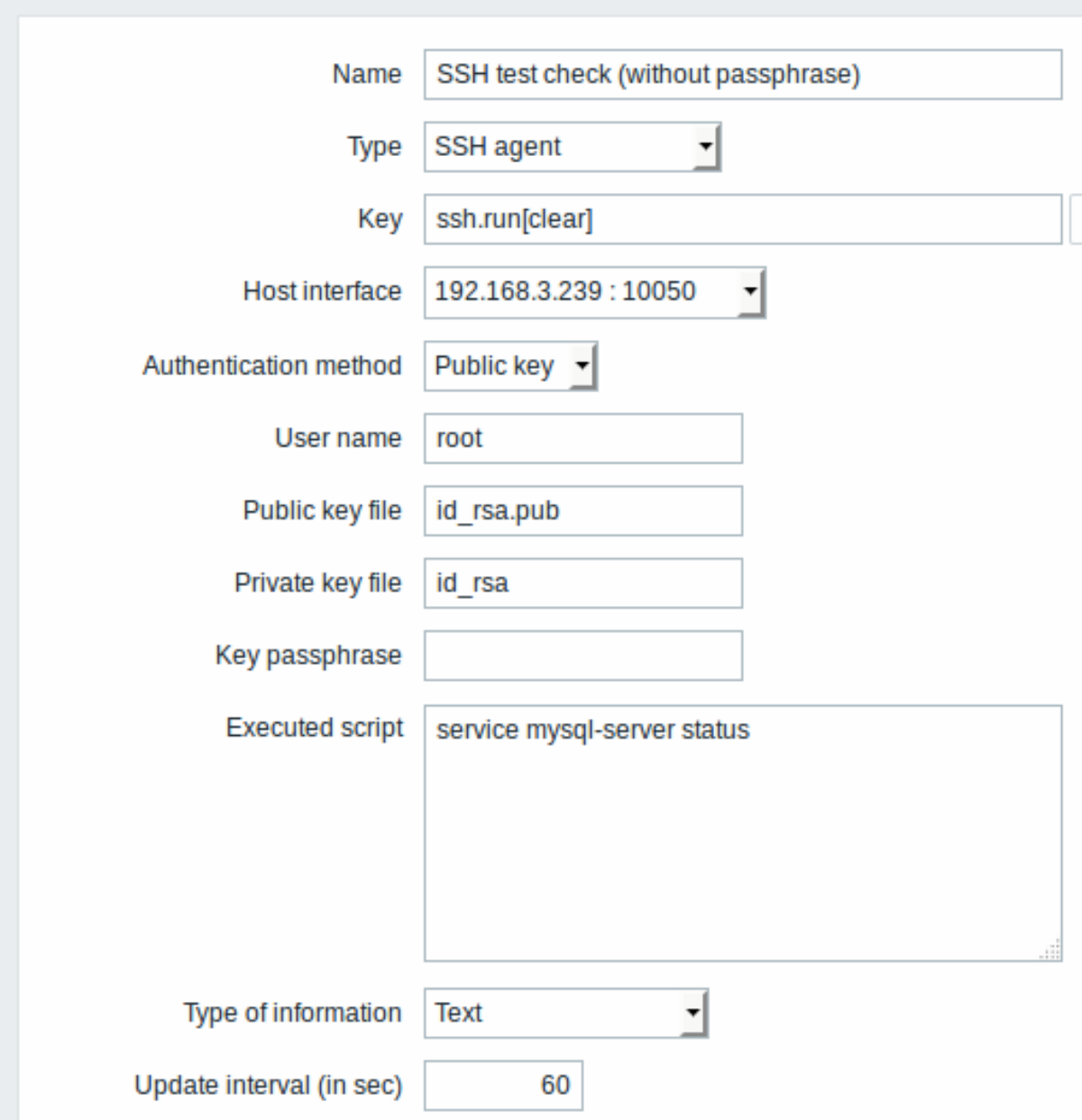

Figura 7[25] - Configuración SSH de un host en Zabbix

[25] Tomado de la fuente (11) de la bibliografía. De la dirección: https://www.zabbix.com/documentation/3.2/en/manual/config/items/itemtypes/ssh_checks

Monitoreo SNMP

El monitoreo por agentes SNMP se hizo utilizando la versión 2. Esto fue porque varios de los equipos no soportaban la versión 3 del protocolo. Y con la intención de simplificar la administración y configuración se decidió usar la versión 2 para todos los equipos.

La configuración de los equipos a monitorear por SNMP se puede dividir en 4 grandes grupos:

- Servidores de almacenamiento (NAS): El monitoreo de estos equipos se hizo utilizando los parámetros básicos definidos en el MIB-II.
- Servidores Virtualización. En este caso se requirió consultar el MIB del fabricante para el modelo cada uno de los servidores. Y crear una plantilla para agregar los OIDs que eran de interés. Los datos que se monitorearon fueron:
    - Utilización de los núcleos de los CPUs
    - Temperatura de los procesadores
    - Estado de las fuentes de alimentación: Esto con el propósito de alertar si fallaba alguna de las dos fuentes para poder realizar el cambio.
    - Estado de los discos duros SAS
    - Estado de las interfaces de red
    - Estado y velocidad de los ventiladores
- Switches de red
    - Estado de cada una de las interfaces de red
- Equipo de red: Cada uno de los equipos requirió consultar el MIB del fabricante para determinar qué información adicional se podía monitorear.
    - Enrutadores (Principal y Secundario)
        - Estado de las interfaces
        - Información del último acceso
        - Fecha del último cambio a la configuración
        - Utilización de las interfaces
    - Servidor VPN Y Firewall
        - Estado de las interfaces
        - Estado del servicio de firewall
        - Estado del servicio de VPN
        - Número de conexiones activas del servidor VPN
        - Fecha del último cambio a la configuración
        - Información del último acceso a la página de configuración
        - Trampas para las alertas del cortafuegos
        - Trampas para las alertas y notificaciones del VPN
    - Access Points
        - Estado de las interfaces
        - Número de equipos inalámbricos conectados
        - Fecha del último cambio a la configuración
        - Información del último acceso a la página de configuración

Monitoreo Agente

El monitoreo por medio de los agentes de Zabbix fue la parte más tardada del proyecto. No solo porque la mayoría de los equipos se monitorearon de esta forma, sino porque cada uno requería de

tiempo con el equipo y, en muchos casos, el instalar el agente y los programas de smartmontools y lm-sensors. En la mayoría de los equipos esto implicaba el tener que reiniciar el equipo. Esto llevo a tener que hacer todo un plan con horarios en los que se podía realizar la instalación en cada uno de los equipos. En muchos casos se aprovechó la oportunidad para dar mantenimiento e instalaran las actualizaciones pendientes del sistema, lo que hizo más complicado el proceso.

En los equipos en donde se instalaba smarmontools y lm-sensors era necesario hacer cambios al archivo de configuración del agente, copiar los scripts necesarios y reiniciar el servicio del agente. Los scripts los escribí para Linux y Windows, en Perl y Batch respectivamente. Para el monitoreo de los discos duros solo se requería un script detectaba todos los discos en el equipo y reportaba todos los parámetros para cada uno. Para lm-sensor se requirieron dos scripts, uno para detectar los sensores disponibles en cada computadora y otro para obtener la información de los sensores. En el servidor de Zabbix se creó una plantilla para smartmontools y otra para lm-sensors, las cuales cualquier sistema operativo.

La configuración de los agentes se puede dividir en 4 grandes grupos.

1. **Equipos de grabación de audio y video.** En estos equipos se requería instalar el agente de Windows, smartmontools y lm-sensors. La complicación con estos equipos eran los recursos limitados (procesador y menoría) y que funcionaban 24/7. Lo limitado de los recursos impedía el instalar aplicaciones y actualizaciones sin detener los programas de grabación. Y debido a que era necesario reiniciar había que planificarlo. En la mayoría de los casos se logró hacer la instalación en un horario en donde no hubiera contenido importante en los canales/estaciones que se grababan. Si alguna de las estaciones era crítica era necesario grabarla en otro equipo mientras se hacia la instalación. El monitoreo de los procesos de grabación de audio y video se hizo por medio de una plantilla en Zabbix que auto descubría los procesos con el nombre del programa y los agregaba como elementos a monitorear.
2. **Equipos de usuarios.** Los equipos de los usuarios únicamente requerían la instalación del agente de Zabbix para Windows y Ubuntu (prensa). Esto se hacía cuando el equipo no se utilizaba.
3. **Servidores de Virtualización.** Los servidores de virtualización fueron un problema particular. Ya que en ellos corrían servidores virtuales que eran críticos para la empresa. Por lo cual se tenía que trasladar y ejecutar las máquinas virtuales en el otro servidor mientras se realizaba la instalación. Para esto se tuvo que comprar más memoria y procesadores adicionales para que se pudieran ejecutar todos los servidores en cada uno de los servidores de virtualización. En estos servidores solo se instaló el agente.
4. **Servidores restantes.** En estos servidores no fue necesario el reiniciar. Por lo que la configuración fue simple y se realizó desde un principio. En todos se instaló el agente de Zabbix, smartmontools y lm-sensors. En cada uno de los servidores se realizó el monitoreo de los procesos relacionados a los servicios que cada servidor proveía.
    a. Servidores de Windows.
    b. Servidores CentOS
    c. Servidores Ubuntu (Zentyal)

Monitoreo HTTP

El monitoreo de HTTP solo se utilizó para monitorear 3 servidores; el servidor web de radio y televisión, el servidor web de prensa y su respaldo. El propósito era monitorear estos elementos para determinar si el servicio de las páginas estaba funcionando adecuadamente. Por lo que se emplearon, al dar de alta los elementos, las direcciones IP públicas de los servidores y no las internas. Además, se tuvo que configurar como puerta de enlace en el equipo uno de los servicios de internet adicionales que no formaba parte de la red en donde se encontraban los servidores. Con el propósito de simular los tiempos de espera que experimentaban los clientes al acceder al servicio, se dio de alta a un usuario en el sistema como si fuera un cliente y se le asignó una contraseña y todos los parámetros de configuración de una cuenta con accesos tanto para el portal de prensa como para el de radio y televisión.

El proceso de configuración de los elementos resultó relativamente complicado. Porque se requería cargar la página inicial de cada uno de los portales, que pasara las credenciales y esperar a la carga de la página inicial. A todos estos pasos se le llama escenario en Zabbix. Los tiempos de cada uno de los pasos se registraban en el servidor y permitían comparar el desempeño del sitio a lo largo del tiempo (Figura 8 - Tiempos de los pasos de un escenario Web). Pero para esto fue necesario descomponer en sus partes, el proceso del usuario, de tal forma que se pudiera plasmar en la configuración de Zabbix. En la parte de prensa fue más sencillo, ya que yo programé el sitio del servicio y conocía más a detalle de todo lo que se necesitaba para hacer una autenticación exitosa. El portal de radio y televisión fue mucho más complicado ya que se empleaban muchos encabezados y yo no estaba familiarizado con el funcionamiento del sitio a detalle. Esto se realizó por medio del uso de las herramientas de desarrollador de Chrome y Firefox en donde se tenían que registrar los encabezados y la información que se enviaba del navegador al servidor y viceversa.

Figura 8[26] - Tiempos de los pasos de un escenario Web

Mapas y Pantallas de Zabbix

La parte más útil de Zabbix es que permite condensar la información de las alertas y otros datos por medio de diferentes páginas. La más elemental es el dashboard (Figura 9 - Dashboard de Zabbix 3), en el cual se muestran los últimos problemas en una tabla y en un cuadro se muestra el estado de todos los grupos que a su vez depende del estado de los equipos que lo componen. Otras de las secciones del dashboard son: mapas favoritos, gráficas favoritas, pantallas favoritas, estado del

[26] Tomado de la fuente (11) de la bibliografía. De la dirección: https://www.zabbix.com/documentation/3.2/en/manual/web_monitoring

servidor Zabbix, monitoreo de páginas y el estado de descubrimiento de equipos/servicios/elementos. Sin embargo, esta pantalla no es apta para todos los usuarios, ya que presenta más información de la necesaria para la mayoría de ellos.

La meta final del proyecto de monitoreo era: el realizar los mapas y pantallas que permitirían, a las personas responsables, observar el estado de los equipos a su cargo y determinar, a simple vista, si había algún problema o si se requería realizar alguna acción. La diversidad de personas que iban a usar estos elementos era grande. Desde los jefes de turno de los capturistas hasta el personal de soporte. Los jefes de turno requerían el mapa de los equipos de su área para determinar si un equipo estaba encendido sin ser utilizado y enviar el comando de apagar. Los de soporte necesitaban muchas más pantallas con el propósito de tratar de prevenir problemas que afectaran la disponibilidad de los servicios.

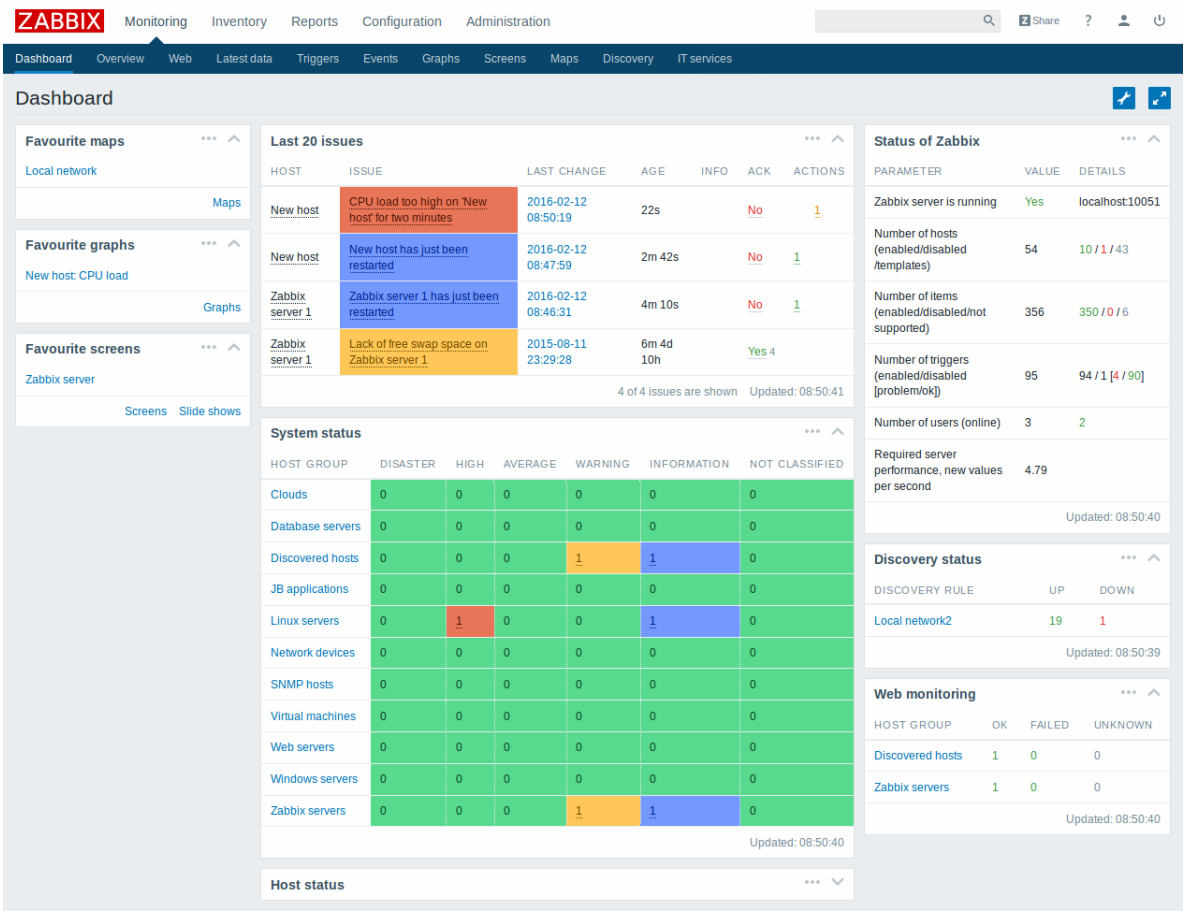

Figura 9[27] *- Dashboard de Zabbix 3*

Los mapas que se crearon se pueden agrupar en 5 grandes grupos con funciones similares que son los siguientes:

[27] Tomado de la fuente (11) de la bibliografía. De la dirección: https://www.zabbix.com/documentation/3.2/en/manual/web_interface/frontend_sections/monitoring/dashboard

1. **Mapas para monitorear los equipos de captura.** Estos mapas mostraban los equipos en la forma en la que estaban colocados físicamente en su área correspondiente usando como fondo el plano arquitectónico del área. En cada equipo se mostraba el fondo del icono del equipo con color gris si el equipo estaba apagado. Si el equipo estaba encendido se mostraba el estado de alerta del equipo (verde, amarillo o rojo). Por medio del menú contextual del elemento se agregó la opción de apagar el equipo de forma remota. Con la intención de ahorrar luz y evitar que los equipos se quedaran encendidos cuando no se usaban. Cuando se daba doble clic en el ícono de la computadora se mostraba la tabla de alertas del equipo (una pantalla similar a la mostrada en la Figura 10 - Pantalla de eventos de Zabbix 3, en la que solo se mostraban los eventos del equipo en específico).
    a. **Mapa para las computadoras del área de comerciales**
    b. **Mapa para las computadoras del área informativa**
    c. **Mapa para las computadoras del área de prensa**

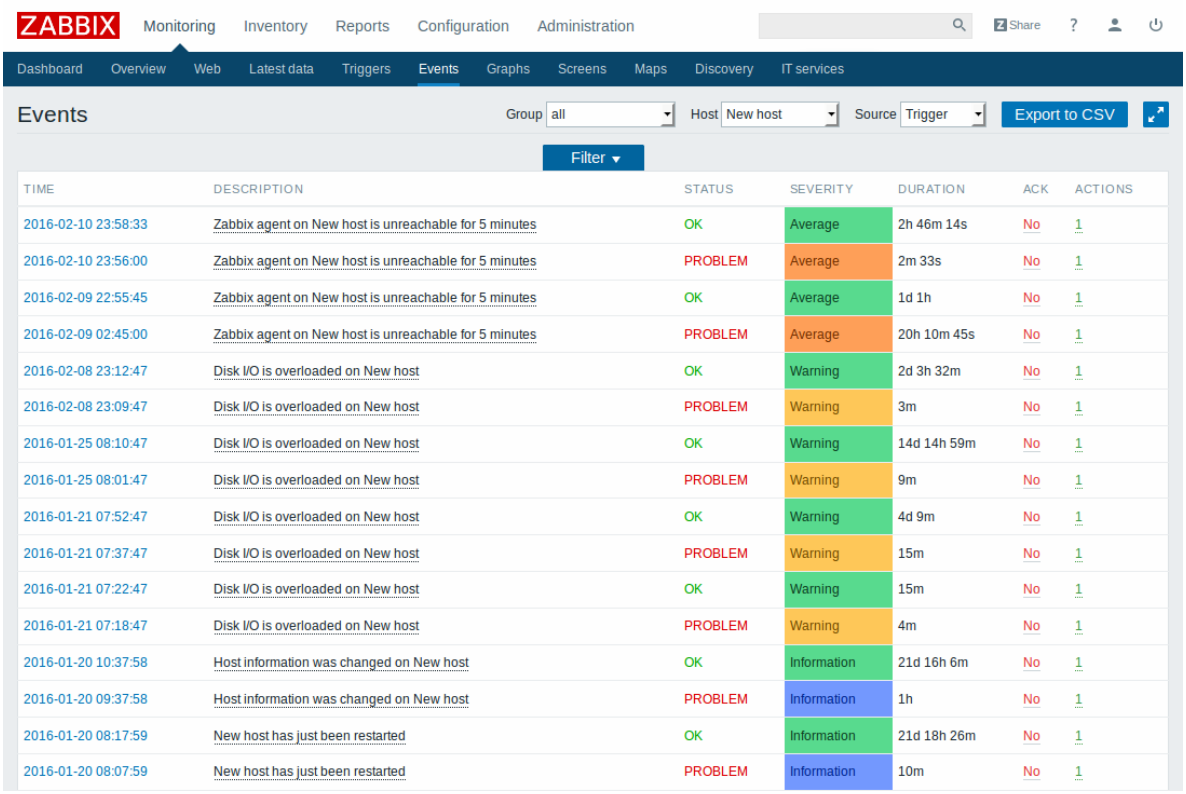

Figura 10[28] - Pantalla de eventos de Zabbix 3

2. **Mapas para los servidores de diferentes áreas.** En cada uno de estos mapas se mostraban los diferentes servidores del área, alineados en una cuadrícula. El fondo de los iconos estaba asociado al estado de alerta y la etiqueta se mostraba en la parte inferior con el nombre del equipo, la dirección IP de sus interfaces, las MACs y la ubicación física del equipo. Al dar doble clic en el ícono se abría la pantalla de alertas del servidor específico. Dentro del menú

[28] Imagen tomada de: https://medium.com/zenduty/real-time-alerts-from-zabbix-and-escalation-with-zenduty-dd2a53335b87

contextual cuando estaba sobre uno de los servidores se podía acceder a la opción “Pantalla Principal” que llevaba directamente a la pantalla personalizada del equipo.

   a. **Mapa para los servidores de prensa**
   b. **Mapa para los servidores de radio y televisión**
   c. **Mapa para los servidores de los demás servicios**

3. **Mapa para los equipos de red.** Este era simplemente un mapa en donde se colocaron todos los equipos de red (switches, enrutadores, puntos de acceso y el servidor de VPN) para poder observarlos todos juntos sin tener la información de los equipos de los usuarios o los servidores. En la Figura 11 - Mapa de Zabbix, se puede apreciar un ejemplo similar. Cada uno de los iconos llevaba a la pantalla de alertas y por medio de la opción “Pantalla Principal” del menú contextual se podía acceder a las pantallas personalizadas de cada uno de los equipos.

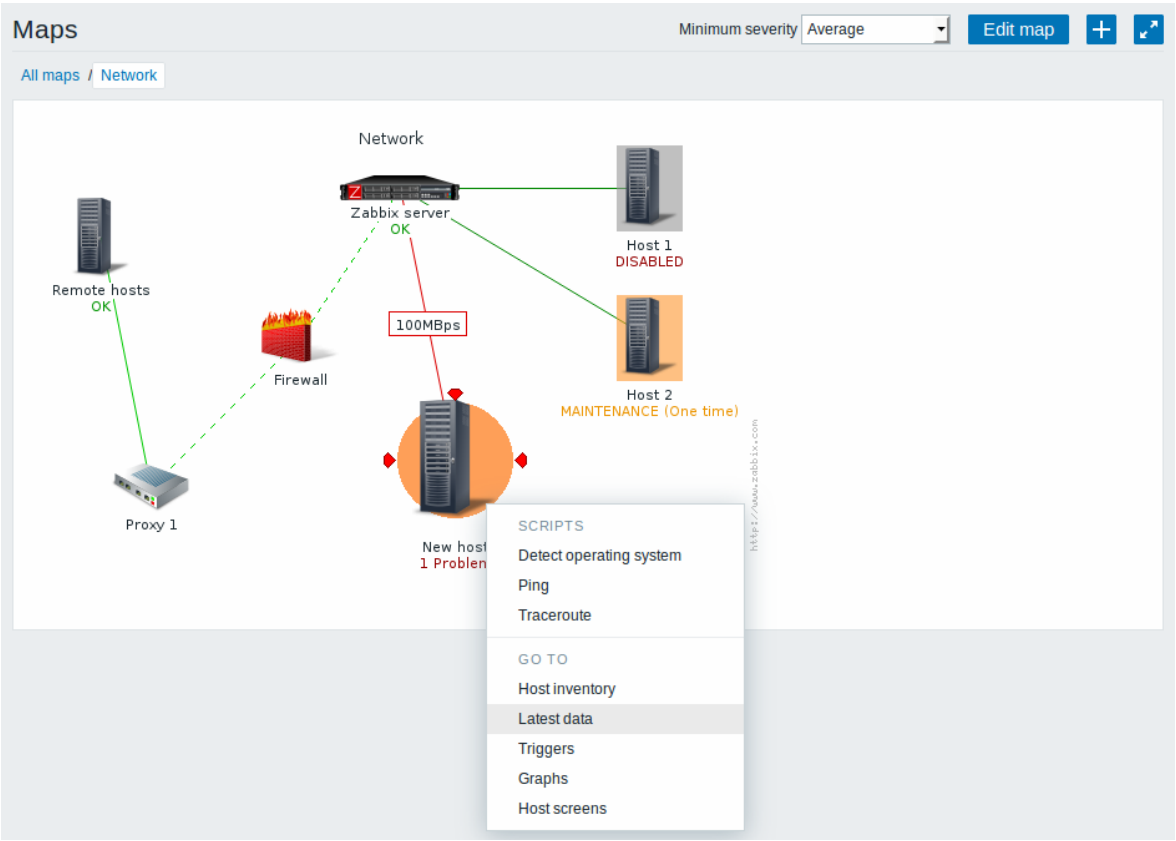

Figura 11[29] - Mapa de Zabbix

4. **Mapa para la interconexión de los equipos de red.** Este mapa era simplemente un mapa de la red en donde se mostraba como era la conexión física de los equipos en la red. Incluía todos los equipos y mostraba agrupados los equipos de captura y los servidores por áreas.
5. **Mapa global (incluye vínculos a las demás pantallas y mapas que se crearon).** En este mapa se presentaban en 4 columnas las áreas de prensa, informativo, comerciales y adicionales.

[29] Tomado de la fuente (11) de la bibliografía. De la dirección: https://www.zabbix.com/documentation/3.2/en/manual/web_interface/frontend_sections/monitoring/maps

En las columnas de las áreas había un icono para los servidores y uno para los equipos de los usuarios, en el área de adicionales estaba un vínculo para el mapa de los demás servicios y el mapa de la interconexión de la red.

Las pantallas de detalle de los equipos casi siempre eran las generadas por las plantillas de los agentes o de SNMP, muy similares a la mostrada en la Figura 12 - Utilización de Recursos del Servidor Zabbix (Monitoreo por Agente). Pero en varios casos fue necesario crear pantallas personalizadas para mostrar información relevante para el equipo. Los casos más particulares fueron:

1. Switches de red. Estos equipos requerían una gráfica de utilización de cada uno de los 24 puertos. Una tabla que mostrara los puertos activos y la lista de los eventos del equipo.
2. Puntos de acceso inalámbricos. En estos equipos era necesario que se mostrara una gráfica con el número de clientes conectados.
3. Servidores de virtualización. En estas pantallas se requería el monitoreo de los recursos del sistema (CPU, memoria e interfaces de red), los eventos del sistema y una tabla que mostrara cada una de las máquinas virtuales que estaban corriendo en el servidor.
4. Servidores de almacenamiento. Para estos servidores era necesario que se mostrara en la pantalla principal varios de los parámetros SMART de los discos duros (número de sectores defectuosos y temperatura principalmente), el estado del RAID por software y su utilización. Así como el estado de los servicios de Samba, SSH y los recursos del sistema.
5. Servidores Web. Las pantallas para estos servidores debían mostrar la información básica de desempeño, el estado del servicio relacionado con la página web (IIS y httpd) y los resultados de los tiempos de los escenarios del monitoreo HTTP.
6. Servidores SQL. En estos servidores era necesario mostrar en la pantalla los recursos del sistema, la utilización de los discos duros, el estado del arreglo RAID y el desempeño de los discos duros, ya que esto suele ser un cuello de botella en las consultas de base de datos. Adicionalmente se necesitaba monitorear el estado de las fuentes de poder de los equipos y las temperaturas internas.

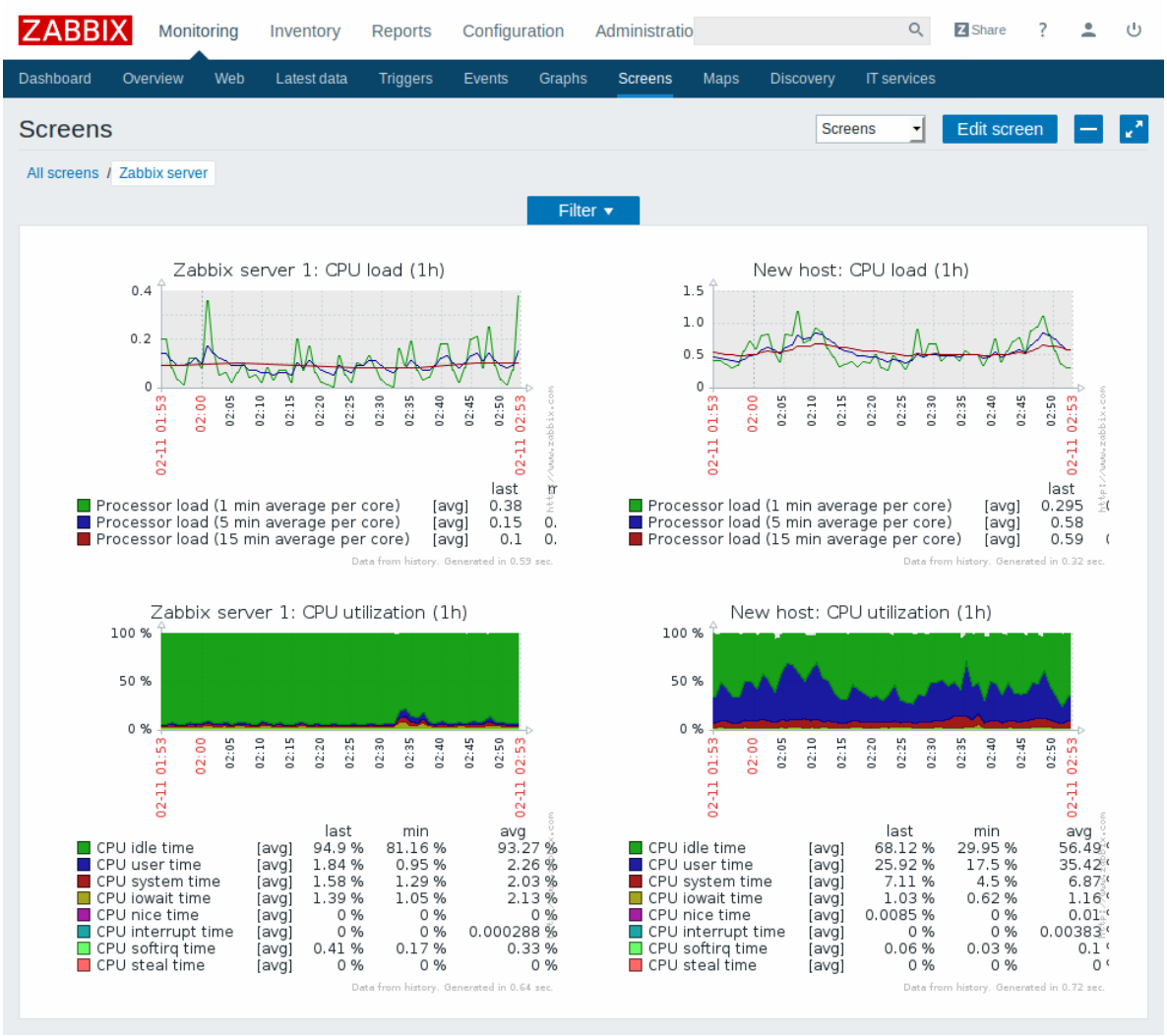

Figura 12[30] - Utilización de Recursos del Servidor Zabbix (Monitoreo por Agente)

Configuración de Alertas

La parte más complicada de todo el proyecto de monitoreo fueron las alertas. Muchos fueron los factores que hicieron el proceso tortuoso. El primero fue el autodescubrimiento de elementos de las plantillas predeterminadas de Zabbix, que agregaron una gran cantidad de elementos con alertas en cada equipo, principalmente servicios del sistema operativo. Cuando estos servicios se detenían o reiniciaban, se enviaba una alerta, aunque fuera el comportamiento normal. Por lo que los primeros días se tuvo que desactivar el envío de todas las alertas, para poder seleccionar los elementos que si eran relevantes de los que no.

Una vez que se lidio con los elementos que se descubrían automáticamente por los agentes de Zabbix, se tuvieron que ajustar los valores límite en muchas de las alertas de las plantillas. Las razones fueron variadas, desde malas prácticas, hasta problemas con algunos de los sensores de los

[30] Tomado de la fuente (11) de la bibliografía. De la dirección: https://www.zabbix.com/documentation/3.2/en/manual/web_interface/frontend_sections/monitoring/screens

equipos. El caso más representativo de las malas prácticas era el tratar de utilizar los equipos de grabación al máximo, lo que hacía que muchos de los equipos corrieran a más 95% de utilización del procesador. Esto para la plantilla predeterminada de los agentes de Zabbix era un criterio de alerta cuando se presentaba por periodos largos de tiempo (más de 5 minutos). Primero se intentó subir el límite a 97% pero esto limitó la detección de problemas en otros equipos. Al final se optó por dejar el límite del uso del procesador en 95% y simplemente desactivar las alertas para ese elemento en algunos equipos específicos. Con la intención de en un futuro reducir la carga del equipo transfiriéndola a un equipo diferente.

Un problema muy común al inicio fue que: algunos de los sensores reportaban valores constantes superiores a los máximos establecidos en las plantillas de lm-sensors y smartmontools. Esto se debía a la antigüedad de los equipos y que algunos sensores ya no funcionaban adecuadamente y reportaban un valor fijo superior al límite. Cuando esto sucedía se deshabilitaban dichas alertas en los equipos específicos.

Otro problema que se presentó múltiples veces fueron las alertas cuando se ejecutaban tareas programadas en los servidores. Los dos principales ejemplos fueron: la creación de respaldos y la optimización de las bases de datos. Estos procedimientos se realizaban periódicamente en las noches cuando la carga de trabajo era baja. Sin embargo, la cantidad de recursos que ocupan era muy alta y esto provocaba que se dispararan las alertas en medio de la noche. Para evitar que estas alertas se enviaran, se modificó la alerta para que no se enviara si era el día en el que se iba a realizar el procedimiento.

Todo el proceso de depuración de alertas tardó aproximadamente un mes para estabilizarse. Esta parte fue la más desgastante del proyecto porque cada vez que se presentaba una falla se generaba fricción con el personal de soporte o simplemente era otro problema que resolver. Siendo aún más grave cuando las alertas llegaban fuera de las horas laborales.

Implementación - Configuración, despliegue y mantenimiento servicios

Active Directory, DHCP, DNS, NTP y FTP

Considerando los requerimientos del proyecto. El primer paso fue buscar cuales podían ser las posibles soluciones que permitirían lograr los objetivos. La solución que tenía en mente al momento de tomar el proyecto era: usar diferentes aplicaciones de Linux para cada uno de los servicios y consolidarlos por medio de Webmin. La parte más importante del proyecto era el servidor de Active Directory. Por lo que se analizaron las opciones disponibles y se redujo a 3 opciones ApacheDS, OpenLDAP y Zentyal. Las tres soluciones cumplían con todos los requisitos. Decidí iniciar con Zentyal ya que era una distribución completa de Linux e incluía la posible solución para varios de los servicios. Así como que parecía ser la más fácil de implementar.

De la misma forma que se hizo para la parte de monitoreo se decidió que se haría una prueba de configuración con algunos equipos. Esto con el propósito de evaluar y aprender a usar Zentyal. Adicionalmente esto permitiría hacer una configuración desde cero para el sistema que se iba utilizar para producción.

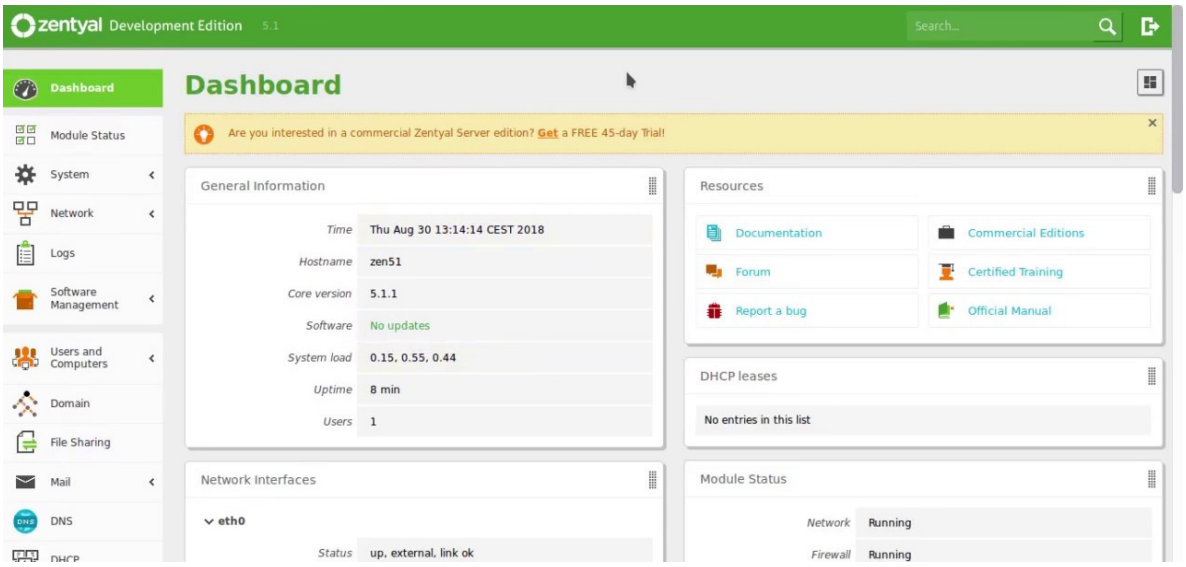

Figura 13[31] *– Dashboard de Zentyal 5.1*

Efectivamente la instalación y configuración inicial de Zentyal fue fácil y la distribución incluía el servidor de Active Directory, DNS, FTP, NTP y DHCP. Todas las configuraciones se hicieron por medio de la interfaz web, parte integral de Zentyal. En la Figura 13 – Dashboard de Zentyal 5.1 se muestra la página inicial (Dashboard) de Zentyal.

Es importante mencionar que para los servicios incluidos en Zentyal no se requiere hacer las configuraciones en el cortafuegos ya que las reglas se agregan automáticamente al activar el servicio.

Active Directory

Como se mencionó previamente, el Active Directory era la parte más importante. Por lo que se inició por la configuración de este servicio. Para configurar el directorio activo se siguieron los siguientes pasos:

1. Instalar y configurar el servidor de respaldo.
2. Dar de alta el dominio.
3. Hacer la configuración para la replicación de los volúmenes, para que se sincronizaran las políticas de grupo en el servidor de respaldo.
4. Crear los grupos de usuarios.
    a. Se crearon los siguientes grupos.
        i. Administradores. Grupo simplemente para mi jefe, el jefe de soporte y yo.
        ii. Jefes. Solamente estaban incluidos los dueños de la empresa.
        iii. Soporte. Todo el personal de soporte.
        iv. Administración. Todo el personal administrativo.
        v. Supervisores. El personal que supervisaba a los capturistas.

[31] Fuente propia. Captura de pantalla durante el proceso de inicial de configuración.

vi. Capturistas. Grupo para las 3 cuentas básicas de capturista (Prensa, Informativo y Comerciales) y algunos capturistas que si tenían cuentas personalizadas.
vii. Prensa. Grupo para todo el personal de prensa
viii. Informativo. Grupo para todo el personal de monitoreo de radio y televisión informativa.
ix. Comerciales Grupo para todo el personal de monitoreo de comerciales de radio y televisión.
x. Invitados. Grupo designado para gente que no pertenecía a la empresa o para clientes que visitaban las instalaciones. Se tenían cuentas predeterminadas para dar accesos a ciertas partes de la red.

5. Crear las cuentas de los usuarios. Se dieron de alta alrededor de 40 cuentas diferentes.
6. Modificar y crear los objetos de las políticas de grupo.
    a. Políticas de los capturistas
        i. Bloquear la modificación del escritorio
        ii. Establecer los íconos que aparecen en el escritorio
        iii. Establecer los programas que aparecen en la barra de tareas
        iv. Establecer el papel tapiz que se mostraba dependiendo del grupo al que pertenecía el usuario
        v. Bloquear el uso de los puertos USB
    b. Políticas de los supervisores
        i. Establecer los íconos que aparecen en el escritorio
        ii. Establecer los programas que aparecen en la barra de tareas
        iii. Configurar las impresoras que se pueden utilizar
    c. Políticas de los administradores y demás grupos.
        i. Configurar las impresoras que se pueden utilizar
7. Se agregaron los equipos al dominio
    a. Sacar del dominio previo cada uno de los equipos
    b. Dar de alta en el nuevo dominio cada uno de los equipos
8. Se editaron los permisos de las carpetas compartidas usando los nuevos grupos y usuarios del dominio

En la interfaz web de Zentyal se pueden administrar los usuarios (Figura 14 - Alta de usuario en Zentyal), los grupos y las computadoras directamente en el la interfaz Web. Pero para las funciones más avanzadas como lo son las políticas de grupo se tuvo que usar la herramienta oficial de Microsoft, el editor de políticas de grupo (Figura 15 - Editor de políticas de grupo de Microsoft). Esta herramienta se incluye en cualquier versión reciente de Windows Profesional. Simplemente es necesario agregar la funcionalidad ya que no se incluye por defecto en la instalación del sistema operativo.

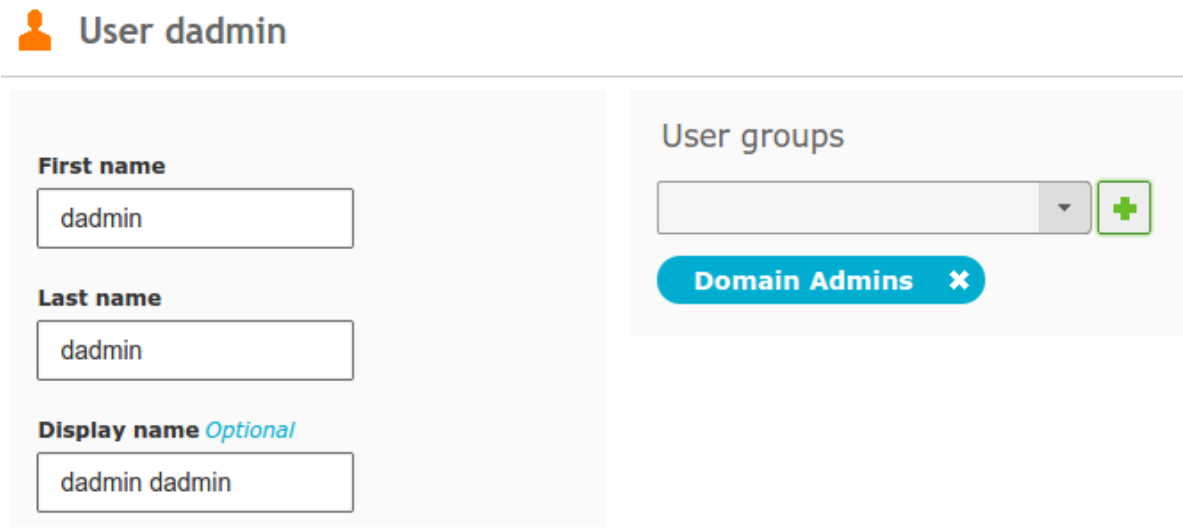

Figura 14[32] - Alta de usuario en Zentyal

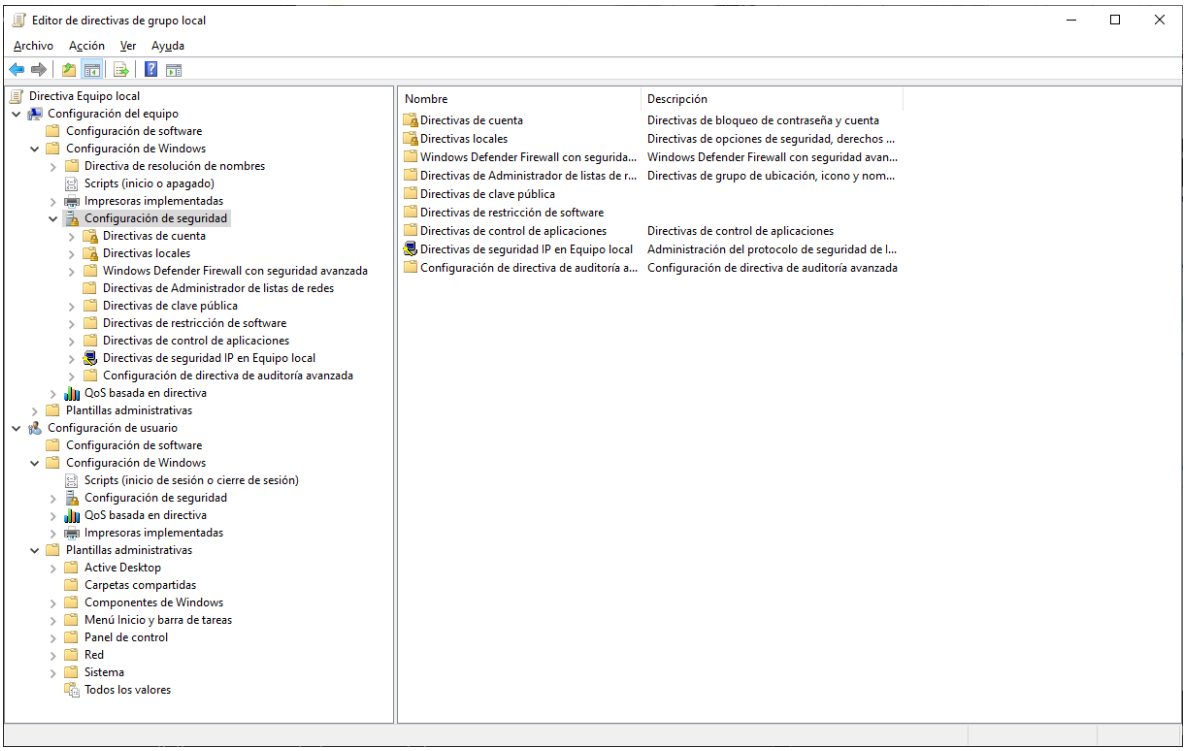

Figura 15[33] - Editor de políticas de grupo de Microsoft

La parte más complicada del proceso fue la parte de la replicación de volúmenes, que se necesita para garantizar que las políticas de grupo se sincronicen entre el servidor principal y el secundario. De otra forma las políticas solo residirían en el servidor principal. Zentyal no cuenta con una solución oficial para el problema. Sin embargo, en la documentación se provee un vínculo[34] a una guía con el

[32] Tomado de la fuente (13) de la bibliografía. De la dirección https://doc.zentyal.org/5.1/en/directory.html
[33] Fuente propia. Captura de pantalla de la ventana del editor de políticas de grupo de Microsoft Windows.
[34] El vínculo es: https://wiki.samba.org/index.php/Rsync_based_SysVol_replication_workaround

procedimiento para lograrlo. Una vez que se realiza el procedimiento, las políticas de grupo se pasan del servidor principal al secundario, por medio del uso de la utilería de línea de comando, Cron. Este proceso no validaba la integridad de la información de las políticas de grupo como suele suceder en un servidor de directorio activo de Windows.

La falta de validación terminó siendo un problema un año después. Cuando el disco duro del servidor principal falló y se dañó uno de los elementos del volumen. Lo cual daño irreversiblemente el servicio de directorio activo tuvo que volver a configurar todo el servicio. Esos son los costos/compromisos de implementar este tipo de soluciones en programas de código abierto. La parte más crítica del todo el proceso fue la migración de los equipos del dominio anterior al nuevo.

DNS

Es importante mencionar que la configuración del DNS del dominio interno la hace Zentyal de forma automática y se maneja de forma separada. Normalmente se le agrega al nombre dominio al final el término "lan" separado por un punto. Esto se debe a que el DNS es parte integral del Active Directory. Por lo que las configuraciones aquí mencionadas son solo para el dominio público de la empresa, que se usa para dar servicio a los clientes a través de Internet.

La configuración del DNS para el dominio público de la empresa en Zentyal se hizo en minutos, tanto para el servidor primario como para el secundario. Lo que tomó más tiempo fue la configuración e instalación del tercer servidor en Guadalajara. El jefe de soporte fue el encargado de esa configuración. Para dicho servidor se usó Mara DNS, porque el equipo de Guadalajara usaba Windows 10 y Mara es uno de los pocos servidores de código abierto que corre en Windows.

Para que en la práctica haya redundancia y alta disponibilidad en un servidor DNS es necesario que al menos uno de los respaldos se encuentre en una red diferente. Esto con el propósito de evitar que una falla en esa red afecte la visibilidad del servidor. Es por eso por lo que el servidor de Guadalajara era sumamente importante, ya que era el único respaldo que se encontraba en una red distinta.

Una vez configurados los 3 servidores de DNS y que se sincronizaban adecuadamente entre ellos. Se hicieron las configuraciones necesarias para SPF (Sender Policy Framework) que se necesitaban para el servidor de correos. Esto tiene el propósito de evitar que los demás servidores de correo bloqueen o marquen como spam los correos provenientes del dominio de la empresa.

Después se procedió a dar de baja la dirección IP en el servidor de producción y darla de alta en el servidor Zentyal primario de tal forma que no se tuvieran que hacer cambios con el proveedor del dominio.

Para validar todas las configuraciones se utilizó las herramientas en línea de la página https://dnschecker.org/ que permitió ajustar los últimos detalles. Este proceso fue tardado ya que muchas de las transacciones DNS tiene tiempos de caducidad largos y se tiene que esperar a que se actualicen.

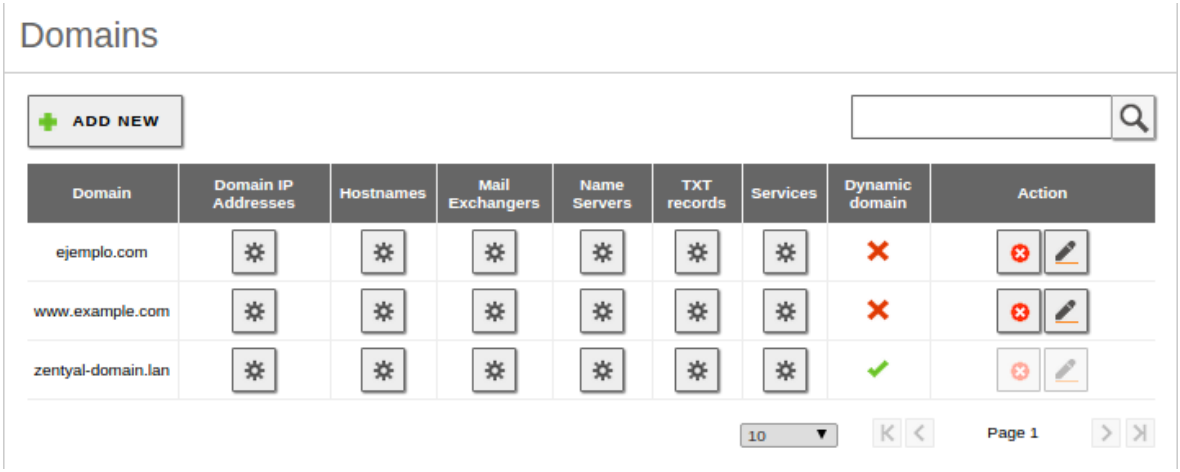

Figura 16[35] - Dominios del DNS

FTP

El único propósito del servidor de archivos era recibir los archivos de Notimex. Por lo que se requería el acceso de un solo usuario, con una contraseña específica asignada por la agencia. Esta cuenta debía tener acceso a una sola carpeta; donde se almacenaban todos los archivos que enviaba Notimex.

La configuración del servicio fue bastante básica. Se bloqueó el acceso anónimo, los directorios personales y se marcó la conexión SSL como opcional. Hubiera sido deseable forzar la conexión segura, pero Notimex no lo soportaba. Para dar de alta al usuario se tuvo que crear un usuario en el controlador de dominio, asignándole la contraseña especificada por Notimex. Y dar los permisos correspondientes al usuario en la carpeta en donde se recibirían los archivos xml con las notas. Los permisos de la carpeta se asignaron directamente en el explorador de archivos de Windows en un equipo con una cuenta de administrador.

A diferencia de los demás servicios fue necesario habilitar las reglas del cortafuegos para permitir la conexión al servidor. En este caso los puertos a emplear son los puertos 20/tcp, 21/tcp y 22/tcp para la conexión segura.

NTP

La configuración del servidor de tiempo fue trivial. Solo hubo que habilitar la sincronización con servidores externos y agregar los servidores que se muestran en Tabla 9- Servidores de Tiempo.

Tabla 9[36]- Servidores de Tiempo

Servidor de tiempo	**Notas**
cronos.cenam.mx	Servidor del Centro Nacional de Metrología que es el que lleva la Hora Oficial de los Estados Unidos Mexicanos.
time.nist.gov	Servidor global del Instituto de Estándares y Tecnología de Estados Unidos (NIST por sus siglas en inglés)
pool.ntp.org	Proyecto de lista de servidores a nivel global.

[35] Tomado de la fuente (13) de la bibliografía. De la dirección https://doc.zentyal.org/5.1/en/dns.html
[36] Fuente propia.

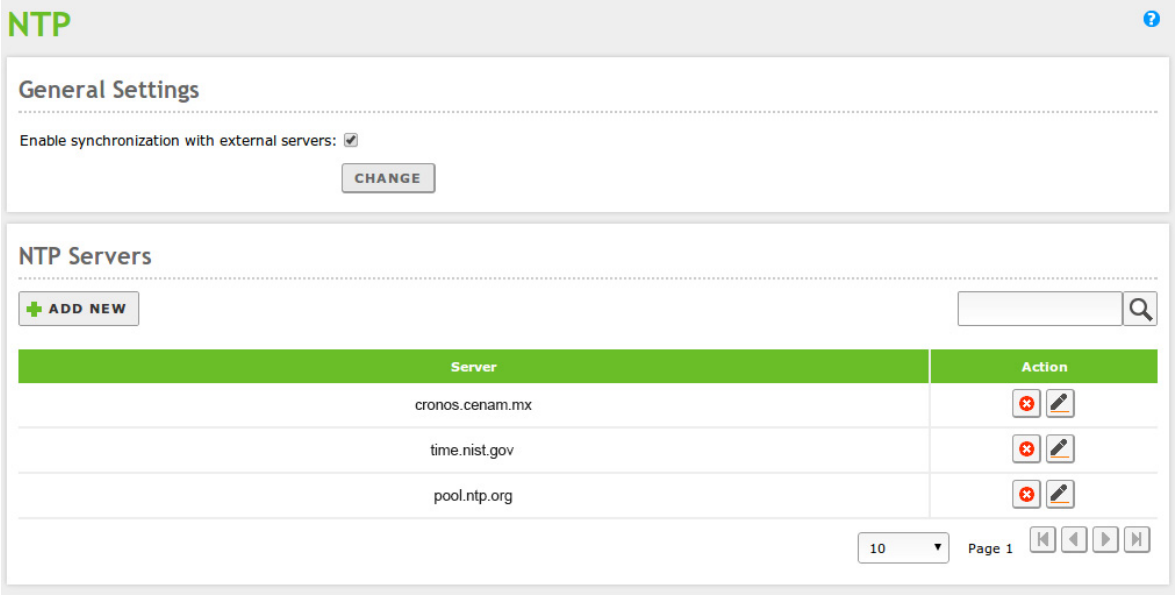

Figura 17[37] - Configuración de Zentyal del servidor de tiempo (NTP)

Para la sincronización del reloj de los equipos que no utilizaban el DHCP se tuvo que configurar directamente en el equipo y agregar la dirección IP del servidor de Zentyal como el servidor primario de reloj y el de respaldo como segunda opción.

DHCP

Para la configuración del servidor de DCHP se tuvieron que considerar los siguientes factores:

- Los servidores de la empresa tenían asignados IP estáticas y no se podían cambiar ya que las direcciones de red se habían usado en el código de varias herramientas de uso interno. Y cualquier cambio podía hacer que partes del servicio fallaran.
- Se necesitaba asignar una puerta de salida específica a cada equipo de escritorio.
- Se necesitaba crear otra red para los equipos móviles y equipos de uso temporal.

El primer paso fue hacer una tabla de Excel en la que se listaron todos los equipos de la empresa. En el documento se registró el nombre de la máquina, la dirección física (MAC), si el equipo requería de IP fija asignada de forma manual, la dirección IP que se le asignaría y que puerta de enlace le correspondía. Aunque todos los equipos necesitan de una dirección IP, se decidió que los equipos de los usuarios, no se tuviera que configurar manualmente en el equipo, sino que el servidor de DHCP le asignaría dicha dirección. Esto con el propósito de ahorrarle tiempo al personal de soporte cuando se recargaban las máquinas y evitar posibles errores de configuración, que pudieran causar conflictos en la red. Así como evitar la configuración manual en cada uno de los equipos.

El documento de Excel resultó sumamente útil, tanto para planificar, evitar problemas de configuración, tener una idea de que componía la red y diagnosticar problemas de conectividad o

[37] Tomado de la fuente (13) de la bibliografía. Y editado para mostrar las direcciones de los servidores de tiempo mostrados en la Tabla 9- Servidores de Tiempo. De la dirección https://doc.zentyal.org/5.1/en/ntp.html

configuración. Posteriormente en el mismo documento se incluyó un plano de cada piso y la ubicación de los equipos. Que se usó para referencia de las vistas de equipos en Zabbix.

Una vez que ya se tuvo toda la información se procedió a configurar el servicio en Zentyal (Figura 18 - Opciones de configuración del servidor DHCP). El servidor donde se implementó contaba con dos interfaces de red. A una se le asignó una IP en el rango usual que se empleaba en la empresa y la otra se creó una red privada Clase C para conectar a los equipos móviles y equipos que no queríamos que estuvieran en la misma red que los servidores y equipos de captura. Esto con el propósito de aislar un poco de problemas.

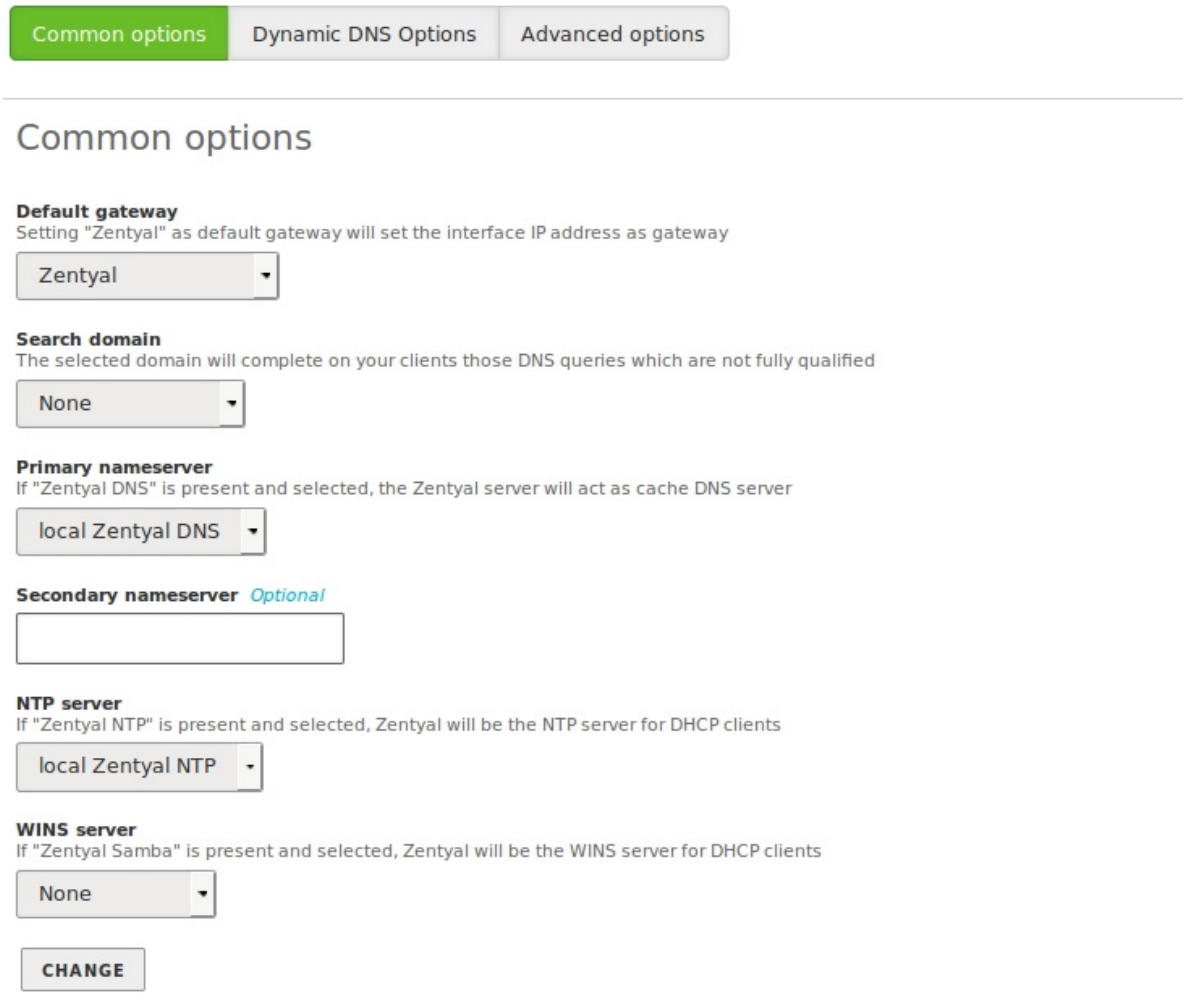

Figura 18[38] - Opciones de configuración del servidor DHCP

Crear la red de Clase C, desde el aspecto técnico y de seguridad, no era una buena solución, ya que se podrían haber empleado VLANs para esto. Lo que hubiera sido mucho más seguro y tendría otras ventajas adicionales. Sin embargo; mi jefe se negó. Principalmente por que requería de tiempo y de planeación adicional y por otro lado por que el personal de soporte no conocía nada de VLANs. Lo

[38] Tomado de la fuente (13) de la bibliografía. De la dirección https://doc.zentyal.org/5.1/en/dhcp.html#dhcp-server-configuration-with-zentyal

que llevó a la conclusión de que era un poco más seguro si se creaba la red privada de clase C y que todo equipo que no tuviera su MAC registrada en el servidor le fuera asignada una dirección de esa red, de tal forma que no formara parte de la misma red que los equipos registrados de la empresa. Aunque esto no serviría de mucho para un ataque intencionado de alguien con conocimiento, si podía evitar algunos problemas causados por infecciones de malware y/o virus en los equipos que se conectaban. Y en el caso de que alguien se conectara de forma no autorizada por cualquier motivo reduciría la posibilidad de causar algún conflicto en la red.

Con la información compilada en documento de Excel se dieron de alta en Zentyal (Figura 19 - Sección para agregar una dirección de IP fija) los equipos que no requerían de una dirección de IP fija configurada de forma manual. Registrando el nombre del equipo, la MAC, la dirección y puerta de enlace designadas. Después se configuró el rango para los equipos móviles.

Figura 19[39] - Sección para agregar una dirección de IP fija[40]

Reconocimiento óptico de caracteres

La instalación de Tesseract es un proceso sencillo una vez que se sabe cuáles son las librerías y dependencias que se requieren o hay paquetes para el sistema operativo en el que se va a instalar. Sin embargo; cuando se inició el proyecto la documentación para la instalación en CentOS no era muy clara y no existían paquetes precompilados. Por lo cual se tuvo que hacer de la forma difícil. Intentando compilar y leyendo el log de errores del compilador para determinar cuáles eran las librerías faltantes. Al final los comando para la compilación de Tesseract 3.0 en CentOS se muestra en el Código 1 - Comandos para la compilación de Tesseract 3.0 en CentOS 7.

Código 1 - Comandos para la compilación de Tesseract 3.0 en CentOS 7

```
yum -y install gcc gcc-c++ git automake autoconf make pkgconfig xmlto giflib-
devel libtool autoconf-archive zlib-devel openjpeg-devel openjpeg2-devel
libjpeg-turbo-devel libpng-devel libicu-devel pango-devel cairo-devel libtiff-
devel libwebp-devel
```

[39] Tomada la dirección https://doc.zentyal.org/en/dhcp.html. De la documentación de la versión actual de Zentyal.
[40] Imagen de la última versión de Zentyal 7.0 no de la versión 5.1 que se usó en la empresa

```
cd ~
wget http://www.leptonica.com/source/leptonica-1.75.3.tar.gz
tar zxvf leptonica-1.75.3.tar.gz
cd leptonica-1.75.3
./configure
make
make install
ldconfig

cd ~
git clone https://github.com/tesseract-ocr/tesseract.git
cd tesseract/
./autogen.sh
PKG_CONFIG_PATH=/usr/local/lib/pkgconfig/ ./configure
make
make install

cd /usr/local/share/tessdata/
wget https://raw.githubusercontent.com/tesseract-
ocr/tessdata_best/master/spa.traineddata
wget https://raw.githubusercontent.com/tesseract-
ocr/tessdata_best/master/eng.traineddata
wget https://github.com/tesseract-ocr/tessdata_best/blob/master/osd.traineddata
```

El procedimiento realizado en los comandos mostrados (Código 1 - Comandos para la compilación de Tesseract 3.0 en CentOS 7) se pueden resumir en 3 simples pasos. Cargar las librerías y herramientas de compilación necesarias, descargar y compilar leptónica, descargar y compilar Tesseract y bajar los archivos de entrenamiento para los idiomas que se iban a utilizar.

Hoy en día con las versiones 4 y 5 de Tesseract el procedimiento es mucho más simple. Ya existen paquetes para múltiples distribuciones de Linux. Y nada más se requiere ejecutar el comando de instalación de manejador de paquetes de la distribución de Linux que se esté utilizando.

Una vez instalado el programa se puede procesar una imagen por medio de la línea de comandos. Lo único que se necesita es la ruta a la imagen, los formatos de archivo de salida, el idioma en el que se espera que esté el texto a reconocer y seleccionar uno de los modos de segmentación de página. Siendo obligatorios simplemente el archivo de la imagen y el nombre base de los archivos de salida.

Código 2 - Commando Tesseract

```
tesserac imagen.tiff imagen_ocr -l spa --psm 3 txt pdf
```

El comando mostrado procesa el archivo “imagen.tiff” y genera dos archivos llamados “imagen_ocr.txt” e “imagen_ocr.pdf” considera que el texto está en español y utiliza el algoritmo de segmentación de página automático (el parámetro 3). El archivo .txt tiene todo el texto que se pudo reconocer de la imagen y el archivo .pdf contiene la imagen con el texto reconocido sobrepuesto en la imagen (Figura 20 - Página en formato PDF generada por Tesseract). La segmentación de página tiene múltiples opciones, pero las únicas que se empleaban era la de automático y la de una sola línea (opción 7).

Por medio de un programa en Java, se automatizaba la generación de los archivos de las imágenes de las notas y el reconocimiento de caracteres. Esto se hacía por medio de la librería “tess4j”. El texto contenido en el archivo .txt se extraía y se guardaba en la base de datos y en el sistema de

búsqueda de texto completo. El archivo .pdf se guardaba para su uso futuro, principalmente en la generación de archivos .pdf.


MILENIO

DIARIO NACIONAL

Wimbledon. Avanza la niña de 15 años a octavos

Franco. "Tenemos pésimas salas para tocar barroco"

CNDH. González Pérez, titular del organismo, también señaló que rechazar la recomendación sobre estancias infantiles es propio de un "régimen autoritario"

Admite Corte recursos del *ombudsman* contra la Guardia Nacional

Van por Lozoya y familia en caso Odebrecht; en EU, por lavado

López Obrador

No hay avances en la PF

Fridamanía. Fiesta de colores en el Zócalo por cumpleaños 112

Molotov, insolente y desenchufado

En ocho meses, 3,400 huérfanos por feminicidios, revela Inmujeres

Alcalde infiltrado. Se disfraza y comprueba vejaciones a viejitos

ESCRIBEN HOY

Xavier Velasco

Verónica Muza

Liébano Sáenz

Miope, visión sobre la ciencia: Lazcano

Figura 20[41] *- Página en formato PDF generada por Tesseract*

Todo el texto es buscable dentro de Acrobat Reader y se puede seleccionar y copiar.

Búsqueda de texto completo

La instalación de Solr 6.0 es un proceso peculiar. Lo único que se requiere para correr el servidor es java 1.8 instalado, el archivo "jar" y ejecutar el comando adecuado (Código 3 - Código para iniciar el servidor de Solr). Una vez que el servidor está corriendo se puede administrar el servido por medio de la interfaz web (Figura 21 - Interfaz Web de Solr) que se encuentra corriendo en el servidor en el puerto 8983/tcp (http://localhost:8983/solr/). Pero esto no configura el servicio para que se inicie de forma automática con el sistema. ni permite administrar el servicio con las herramientas disponibles para servicios en el sistema operativo. Para ello fue necesario crear un script (Código 4 - Script de Inicio del servicio Solr en Linux) con el fin de iniciar, detener y reiniciar el servicio. Para que el servicio arrancara de forma automática era necesario registrar el servicio, habilitarlo y arrancarlo. En CentOS todo este procedimiento se realizaba por medio de la herramienta de comandos systemctl con comandos muy simples. El único paso necesario adicional era el copiar el archivo del script de arranque a la carpeta init.d en el servidor.

[41] Portada del periódico Milenio del día 16 de julio del 2019. Capturada con la cámara de alta resolución en el área de medios impresos de la empresa.

Código 3 - Código para iniciar el servidor de Solr

```
java -Xmx1024m -DSTOP.PORT=8079 -DSTOP.KEY=mustard -jar start.jar
```

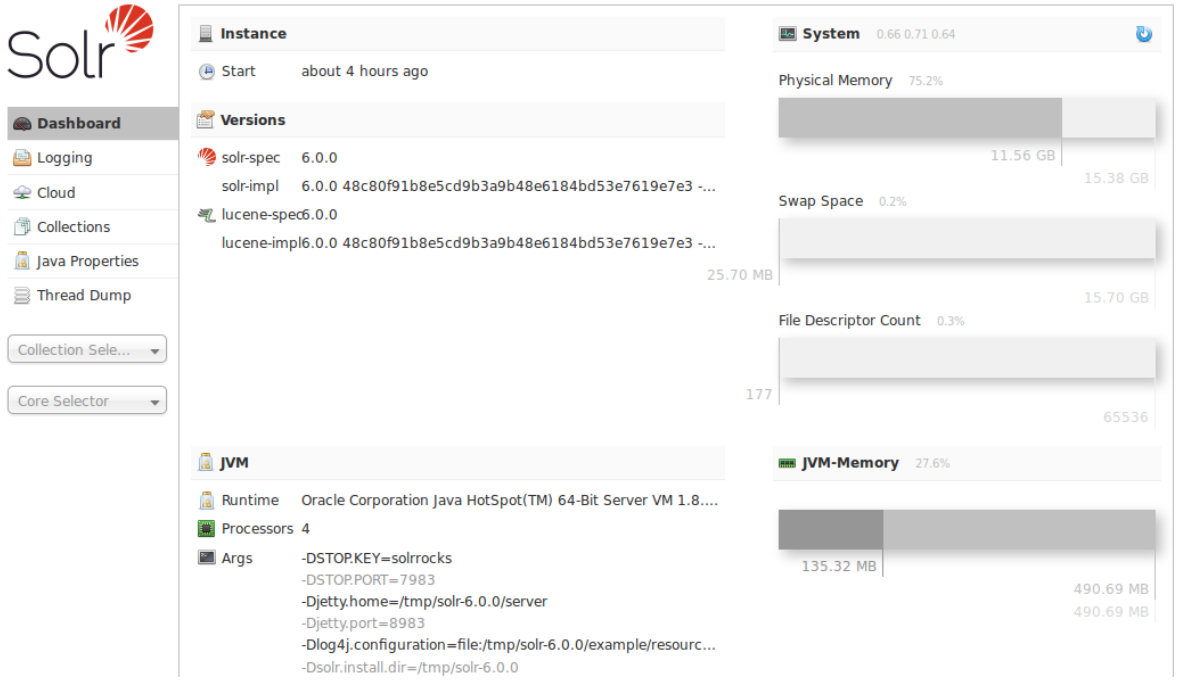

Figura 21[42] - Interfaz Web de Solr

Código 4 - Script de Inicio del servicio Solr en Linux

```
#!/bin/sh

# Starts, stops, and restarts Apache Solr.
#
# chkconfig: 35 92 08
# description: Starts and stops Apache Solr

SOLR_DIR="/prensa/mediatextos/IndiceTexto"
JAVA_OPTIONS="-Xmx1024m -DSTOP.PORT=8079 -DSTOP.KEY=mustard -jar start.jar"
LOG_FILE="/var/log/solr.log"
JAVA="java"

case $1 in
    start)
        echo "Starting Solr"
        cd $SOLR_DIR
        $JAVA $JAVA_OPTIONS > $LOG_FILE &
        ;;
    stop)
        echo "Stopping Solr"
        cd $SOLR_DIR
        $JAVA $JAVA_OPTIONS --stop
        ;;
    restart)
```

[42] Tomado de la fuente (14) de la bibliografía. De la dirección https://solr.apache.org/guide/6_6/overview-of-the-solr-admin-ui.html

```
        $0 stop
        sleep 1
        $0 start
        ;;
    *)
        echo "Usage: $0 {start|stop|restart}" >&2
        exit 1
        ;;
esac
```

Una vez completada la instalación de servicio, mi jefe realizó las configuraciones necesarias para crear el núcleo de Solr y poder iniciar a procesar los documentos por medio del programa que yo diseñe. La comunicación entre el servidor de Solr y el programa de procesamiento de documentos se hizo por medio de las librerías para Java que provee Apache para Solr.

Para probar el funcionamiento del núcleo se realizaron consultas directamente en la interfaz WEB utilizando la herramienta de consulta (Figura 22 - Pantalla para realizar consultas en Solr), el resultado lo devuelve Solr en un objeto JSON (). Y el procedimiento para hacer las consultas para el servicio se hacían de la misma forma, pero se enviaba la consulta directamente desde una página activa (PHP). La cual procesaba el objeto JSON y lo utilizaba para obtener el resto de la información de la base de datos.

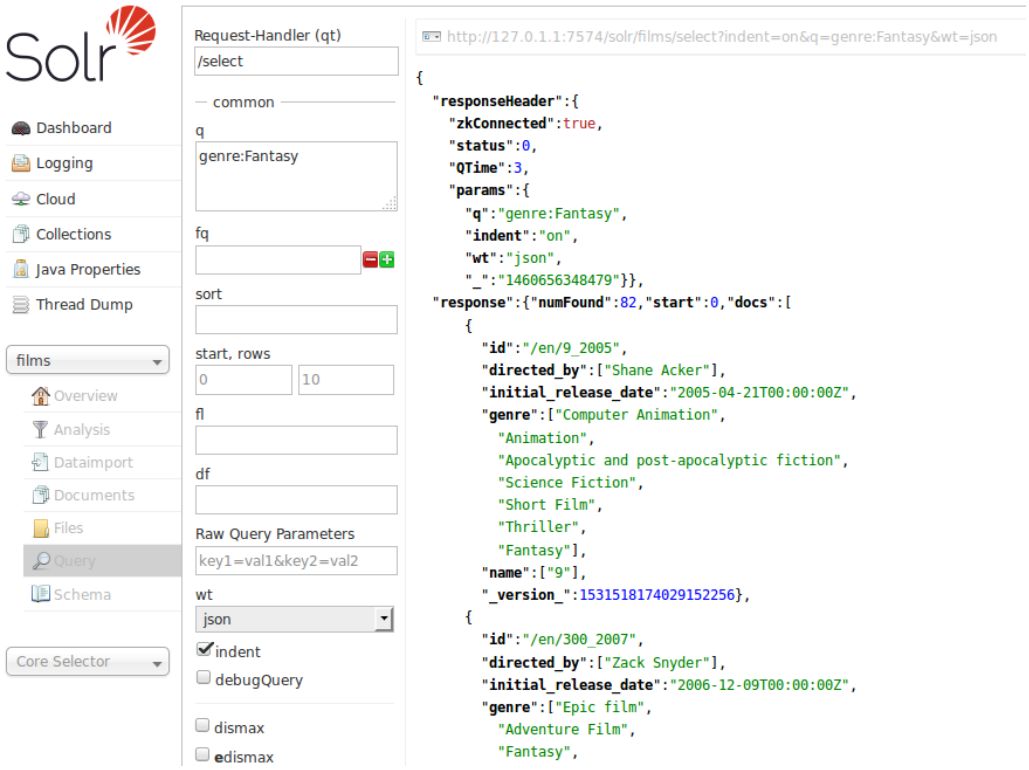

Figura 22[43] - Pantalla para realizar consultas en Solr

[43] Tomado de la fuente (14) de la bibliografía. De la dirección https://solr.apache.org/guide/6_6/query-screen.html#query-screen

Resultados

Monitoreo de Redes

Aunque la configuración de todos los equipos en el servidor de Zabbix fue algo tardado, duró aproximadamente 1 año y medio. Se pudieron apreciar algunos de los resultados de forma inmediata. El primer resultado apreciable fue la reducción en consumo de electricidad, causado por equipos que se quedaban prendidos cuando no estaban en uso por periodos largos. Gracias a que se podía monitorear el estado de los equipos y apagarlos de forma remota, directamente en un mapa de Zabbix al cual tenían acceso los encargados de turno y los gerentes de las áreas.

Otro caso que se presentó casi inmediatamente fue el incremento repentino en el parámetro sectores dañados (SMART) en dos de los discos duros en un servidor NAS. Gracias a esta información se pudo evitar que un volumen (RAID 5) presentara un doble fallo, que hubiera sido catastrófico para el volumen. Permitiéndonos cambiar uno de los discos y que se sincronizara adecuadamente antes de que fallara por completo el volumen. Con esto se evitó el tener que buscar la información en los respaldos y volver a construir el volumen. Lo que hubiera tomado semanas por el tamaño del volumen, 100 TB. Eso sin contar el tiempo que la información hubiera estado fuera de línea.

Unos meses después se presentó un problema particular con los switches de red, que Zabbix permitió resolver rápidamente. Todo inicio cuando se hizo una ampliación del área de prensa, donde se agregó un nuevo switch de 24 puertos. Los contratistas responsables de la instalación cometieron un error y conectaron el nuevo switch al del área contigua en vez de conectarlo al switch central. Esto provocó que en las horas pico de demanda (entre las 7 y 10 de la mañana) se presentaran problemas de saturación en los puertos de interconexión. Esto generaba problemas al azar en los programas de captura de radio y televisión en las áreas de noticias y comerciales. El video se trababa y generaba problemas con el tiempo de marcación de las notas y comerciales. Esto repercutía en el servicio de los clientes, los cuales al momento de iniciar la reproducción de la nota o comercial veían que no coincidía el texto capturado con punto en el que iniciaba el video. Al no ser un problema constante pudo haber pasado desapercibido por mucho tiempo y/o aparentar ser errores de los capturistas, pero gracias a que a las alertas de Zabbix de la saturación de interfaces en el switch, se pudo localizar el problema.

Otros beneficios menores del sistema de monitoreo fueron:

1. Poder ver la utilización general de los equipos de virtualización. Esto permitió aprovechar mejor los recursos de estos equipos.
2. Monitorear las conexiones a Internet. Lo que permitió identificar intermitencias en el servicio.
3. Detectar usos de memoria altos en los servidores. Esto llevó a concluir que había errores en el código en algunos programas de desarrollo interno.
4. Monitorear la utilización de espacio en el disco en múltiples servidores en donde se generaban archivos temporales, y evitar problemas de falta de espacio.

Aunque el sistema de monitoreo trajo consigo un gran número de ventajas y terminó siendo algo muy provechoso para la empresa, no fue una transición fácil. Se sufrió mucho con las alertas al inicio y esto generó mucha fricción con el área de soporte. Conforme se fueron refinando las configuraciones en el servidor la fricción disminuyó. Esto principalmente fue culpa de mi

inexperiencia con Zabbix, lo variado de los métodos de monitoreo y mi falta de conocimiento de muchas de las variantes en los sistemas operativos y los equipos de red que se utilizaban en la empresa. Si tuviera que implementar hoy en día un sistema similar creo que sería un proceso mucho más terso, pero por desgracia el aprendizaje tuvo su costo.

Un problema que se presentó fue con los agentes en algunos los equipos de grabación. Debido a que eran equipos viejos con poca memoria y procesadores lentos; se saturaban y generaban problemas con las grabaciones de audio y video. Lo que provocaba una de dos cosas: que los archivos de video no se indexaran de forma correcta, o que los no iniciaran la reproducción correctamente (perdiéndose unos minutos de grabación). Esto se presentaba de forma esporádica en equipos que grababan estaciones de baja prioridad, haciendo más difícil la corrección del problema, ya que el contenido no se monitoreaba todos los días. Lo que complicó aún más el problema fue que en algunos de estos equipos se deshabilitaron las alertas y nadie se dio cuenta por ser estaciones de baja prioridad. Conforme se fue viendo que existía un patrón se comenzó a estudiar la información histórica de los recursos del equipo; esto permitió ubicar el problema. La solución fue migrar algunas de las estaciones a otros equipos menos saturados y reactivar las alertas.

Pero el problema más importante en todo el proceso, al menos a mi parecer, no fue de carácter técnico, sino más bien de personal y de complejidad. De personal porque las personas de soporte de la empresa no tenían conocimientos teóricos y técnicos suficientes al inicio del proyecto para entender o configurar el sistema de monitoreo. Lo cual los hizo reticentes a usar Zabbix. Los problemas con las alertas aumentaron el recelo. A pesar de eso, con el paso del tiempo ellos empezaron a entender el sistema y Zabbix empezó a servir como herramienta para prevenir e identificar problemas. Cuando salí de la empresa ya era algo que usaban cotidianamente.

Configuración, despliegue y mantenimiento servicios

Active Directory, DHCP, DNS, NTP y FTP

El Cambio a Zentyal para todos los servicios resultó ser sumamente provechoso para la empresa. El mantenimiento y la operación diaria se simplificó. Y el personal de soporte lo aprendió a usar casi inmediatamente sin mucha capacitación.

Si se hubiera empleado Windows Server para proveer estos servicios se habría tenido que pagar:

- La licencia del sistema operativo.
- Una licencia para cada equipo que tenía acceso al servidor (CAL Servidor).
- Una licencia por cada equipo conectado al dominio (CAL Active Directory).
- Licencia para el servidor de Exchange.

El gasto en CALs para la mayoría de los equipos fue inevitable, todos los equipos de captura, la mayoría de los servidores y los equipos de los usuarios se conectaban directamente al equipo con SQL Server. Esto ameritaba una CAL para cada uno de esos equipos. Y era imposible, por la versión que se empleaba de SQL Server, instalarlo en otro sistema operativo que no fuera Windows. Pero se pudo ahorrar en las CALs del directorio activo y evitar el uso del Exchange server y sus CALs, que en su totalidad ascendía a cientos de miles de pesos, una cantidad nada despreciable. Claro que la implementación de Zentyal requirió un poco más de tiempo de lo que se hubiera requerido si se hubiera usado Windows. Adicionalmente se tiene que considerar el tiempo de aprendizaje del

personal y el tiempo adicional por el fallo con la sincronización de volúmenes, los cuales generaron un costo. Pero al final considero que hubo un balance económico positivo para la empresa.

Varios beneficios de Zentyal se manifestaron de forma inesperada al implementar y configurar el servidor de DHCP. Permitiéndonos encontrar y resolver los siguientes problemas:

- Detectar y bloquear dispositivos no autorizados en la red.
- Asignar diferentes puertas de salida a los diferentes dispositivos de red.
- Notificar cuando un dispositivo nuevo se le asignaba una dirección IP.

El servidor de archivos (FTP), el servidor de tiempo (NTP) y el Active Directory funcionaron adecuadamente. La única mejora fue que se pudo centralizar y simplificar su administración.

Reconocimiento óptico de caracteres

Tesseract fue un pilar fundamental para la creación del sistema de captura de prensa y toda el área correspondiente. Después de un par de actualizaciones y de hacer ajustes a la configuración el sistema entregaba textos con un número de errores muy bajo. La cantidad de imágenes que se podían procesar de manera simultánea era sorprendente. Quizá se habrían podido obtener mejores resultados si se entrenado el programa para los tipos de documentos que se procesaban en la empresa. Sin embargo, por limitaciones de tiempo jamás se pudo explorar.

Uno de los beneficios inesperados de Tesseract fue la generación de los archivos .pdf con el texto superpuesto. Estos archivos permitieron crear compilaciones de notas en formato PDF muy profesionales, cuya principal ventaja era que se podía buscar texto directamente en las imágenes. Esto evitó agregar el texto por separado, lo que hubiera aumentado considerablemente el tamaño de los documentos, invaluable por el tamaño de los documentos que se generaban (100-300 hojas). Lo mejor de todo es que esto se podía hacer sin pagar por librerías o herramientas adicionales. Los únicos costos extra eran el procesamiento para genera los .pdf y el espacio para almacenarlos.

Búsqueda de texto completo

La plataforma de Solr es una de las herramientas más sorprendentes con las que he trabajado. Tiene la capacidad de realizar búsquedas en milisegundos sobre cantidades de documentos que en algún momento hubiera pensado imposible. Para cuando salí de trabajar la cantidad de documentos procesados excedía la decena de millones. Y las consultas seguían tomando más o menos el mismo tiempo que al inicio.

Algo que resulto extremadamente útil fueron las búsquedas con expresiones regulares. Aunque requirió capacitar al personal que se encargaba de crear las reglas de autoclasificación. Los resultados fueron mucho mejores de los que obteníamos con búsquedas simples de texto. Esto nunca fue parte de los requisitos del proyecto, pero en retrospectiva pienso que debió de haber sido.

Conforme el personal fue utilizando cada vez más las expresiones regulares, la eficiencia de las reglas se incrementó drásticamente y se volvió indispensable para encontrar la información que los clientes buscaban. Fue tal el éxito de Solr que se comenzó a usar para las notas de radio y televisión, como una herramienta de respaldo para la clasificación de las notas, por si los capturistas no agregaban las clasificaciones correspondientes.

Conclusiones

Monitoreo de Redes

Después de haber implementado todo el proyecto y haberlo usado por tiempo considerable (más de un año). Estas serían mis conclusiones:

- Un sistema de monitoreo sólo es útil cuando se tiene personal capacitado para entender la información que este presenta y lo pueden ajustar a las necesidades de la empresa. Por lo que es ideal que los usuarios del sistema estén lo más involucradas desde el inicio y que los huecos de conocimiento se vayan llenando en el camino.
- Los sistemas de monitoreo tienen una dificultad de implementación directamente proporcional a la complejidad de la infraestructura a monitorear. Por lo que es mejor iniciar el monitoreo mientras se va creciendo la infraestructura. No sólo hace más manejable la implementación, sino que ayuda a diagnosticar problemas que de otra forma pasarían desapercibidos. También el proceso de capacitación se reduce y se hace más simple.
- La homogenización de equipos y de servicios es algo que puede ahorrar una gran cantidad de tiempo y de ser posible debe ser parte de la filosofía al momento de agregar nuevos equipos o servicios. Ya que no sólo implica tiempo adicional de configuración, sino complejidad a la capacitación del personal.
- No siempre más información es mejor. Hay cosas básicas que siempre es bueno monitorear. Pero hay otros elementos que sólo consumen recursos innecesarios, y que pueden confundir al momento de diagnosticar un problema. Por eso recomendaría tomar una mentalidad minimalista al momento de dar de alta los equipos y parámetros. Monitoreando únicamente lo básico al inicio, e ir aumentando poco a poco en vez de iniciar al revés.
- Si existe un sistema previo de monitoreo por más rudimentario que sea, sería bueno migrar su funcionalidad al nuevo sistema, con el propósito de mantener unificada la información. Esto puede tener un costo alto de implementación, pero evita la duplicidad, simplifica el mantenimiento y concentra los esfuerzos de capacitación.
- Como complemento del monitoreo hubiera sido adecuado el implementar un servidor de registros (log server) que compilara la mayoría de la información de los equipos en un sólo lugar. El mismo Zabbix lo soporta, pero al momento de plantear el proyecto yo no conocía dicha funcionalidad y nunca había trabajado directamente con un servidor de registros.

Configuración, despliegue y mantenimiento servicios

Active Directory, DHCP, DNS, NTP y FTP

La implementación de los múltiples servicios usando Zentyal fue una gran enseñanza para mí. Antes de configurar este sistema, jamás habría pensado que existe un sistema gratuito que permita conglomerar tantos servicios de una forma tan amable para el usuario. Implementar lo mismo en Windows es un trabajo relativamente sencillo pero muy costoso.

Claro esto no viene sin compromisos. El perfecto ejemplo fue el problema de sincronización de volúmenes que se presentó al momento de la implementación, pero para una empresa pequeña considero que son aceptables. Aun así, no pensaría en ocupar Zentyal en una empresa con cientos de equipos que usan Windows: el riesgo es muy grande y la redundancia se vuelve aún más indispensable.

Reconocimiento óptico de caracteres

Tesseract es, sin lugar a duda, una de las herramientas de código abierto más potente con la que he trabajado. La facilidad con la que se pueden obtener excelentes resultados es sorprendente. Una vez que se compila y configura el programa los resultados son inmediatos, eso era con la versión 3. Hoy en día con la nueva versión (5.3.0) los resultados son aún más impresionantes.

Búsqueda de texto completo

Cuando inicie en la empresa yo pensaba que todas las búsquedas de texto se realizaban utilizando una base de datos tradicional, sin importar el volumen de información En el que se deseaba realizar la búsqueda, claramente estaba completamente equivocado. Cuando hice la investigación de los sistemas para búsquedas de texto completo quedé muy sorprendido de las herramientas que están a nuestra disposición. Lucene y Solr en particular, las cuales sorprenden por ser herramientas tan complejas que se encuentran disponibles de forma gratuita. Al igual que otros desarrollos de la Fundación de Software Apache tanto Lucene como Solr son herramientas que tienen el potencial de convertirse en las soluciones más representativas de su ramo como lo es hoy en día el servidor web Apache.

Conclusiones Generales

Si hay algo que me quedó completamente claro después de haber trabajado 5 años en la empresa. Es que hay programas de código abierto y de uso comercial libre que están al nivel o por arriba de aplicaciones comerciales conocidas, que, si se aprovechan adecuadamente, representan un recurso invaluable. Y que, gracias a este tipo de herramientas, micro, pequeñas y medianas empresas pueden competir contra empresas mucho más grandes. Aunque esto viene con sus problemas y limitaciones particulares, que son: requerir de personal más capacitado y periodos más largos de desarrollo.

Un par de ejemplos son Tesseract y Solr. Dos herramientas que en sus respectivos nichos son ejemplos de software eficiente y eficaz que abren las puertas a la innovación. Y son este tipo de proyectos los que nivelan un poco el acceso a la tecnología para países menos desarrollados. Sin embargo, existen una serie de problemas que las PYMES tienen que enfrentar cuando usan soluciones como estas. La más importante es la capacitación del personal. Este tipo de programas requieren de personal más capacitado, ya que la información disponible es menor y en muchos casos no se cuenta con soporte técnico, lo que demanda más conocimientos y tiempo del personal. Esto se presentó muchas veces a lo largo de todos los proyectos que realicé en la empresa.

Algo que es indispensable tratar de evitar es acarrear problemas de diseño y planeación cuando se hacen modificaciones a los servicios o equipos importantes de la red. En la empresa que trabajé, existían problemas de diseño de la red, la parte física de la red estaba bien, pero la configuración no era la ideal. Esto produjo una serie de problemas durante la implementación de muchos de los proyectos. Aunque estos problemas no fueron graves, se siguieron arrastrando problemas de seguridad y de saturación de la red. Lo ideal hubiera sido resolverlos antes de iniciar con el proyecto de monitoreo, pero cuando propuse hacer cambios de fondo en la red, estos fueron rechazados por miedo a que solo yo fuera capaz de administrar la red. La solución podría haber sido contratar personal más capacitado, pero esto estaba completamente fuera del presupuesto. Lo que reitera el problema de la necesidad de personal más capacitado. Claro que esto no sólo es un problema de las PYMES, pero estas empresas son las que más lo sufren debido a los recursos económicos limitados.

Bibliografía

1. **Wetteroth, Debbra.** *OSI Reference Model for Telecommunications.* Estados Unidos de América : McGraw-Hill, 2003.

2. **Mauro, Douglas R. and Schmidt, Kevin J.** *Essential SNMP.* Estados Unidos de América : O'Reilly, 2005.

3. **Dostálek, Libor and Kabelová, Alena.** *Understanding TCP/IP. A clear and comprenhensive guide to TCP/IP protocols.* Birmingham, Reino Unido : Packt Publishing, 2006. 1-904811-71-X.

4. **Cisco Systems, Inc.** *CCNA 1 and 2 Companion Guide.* Indianapolis, Estados Unidos de América : Cisco Press, 2003. 1-58713-110-2.

5. **Julian, Mike.** *Practical Monitoring: Effective Strategies for the Real World.* Estados Unidos de América : O'Reilly, 2018.

6. **Olups, Rihards, Dalle Vacche, Andrea and Uytterhoeven, Patrik.** *Zabbix: Enterprise Network Monitoring Made Easy.* Birmingham, Reino Unido : Packt, 2017.

7. **Dalle Vacche, Andrea.** *Mastering Zabbix, 2 Ed.* Birmingham, Reino Unido : Packt, 2013.

8. **Halsall, Fred.** *Computer Networking and the Internet, 5 Ed.* Estados Unidos de América : Pearson Education, 2005. 0-321-26358-8.

9. **Desmond, Brian, et al.** *Active Directory: Designing, Deploying, and Running Active Directory.* Estados Unidos de América : O'Reilly Media, Inc, 2013. 1449369863.

10. **Barret, Daniel J., Silverman, Richard E. and Byrnes, Robert G.** *SSH, The Secure Shell: The Definitive Guide.* Estados Unidos de América : O'Reilly Media, Inc, 2009. 9781449324810.

11. **Zabbix LLC.** Zabbix Manual (Inglés). [En línea] 2023. https://www.zabbix.com/documentation/current/en/manual.

12. **Microsoft Corporation.** Windows Server 2012 R2 and Windows Server 2012. *Active Directory.* [En línea] 2016. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn283324(v=ws.11).

13. **Zentyal Community.** Zentyal 5.1 Official Documentation. [En línea] 2018. https://doc.zentyal.org/5.1/en/.

14. **Apache Software Foundation.** Apache Solr Reference Guide. [En línea] 2023. https://solr.apache.org/guide/6_6/index.html.