SISTEMA TELEMÁTICO PARA CENTRALIZAR EL CONSUMO DE MENSAJERÍA XML SOBRE EL PROTOCOLO HTTP

EDGAR ANDRÉS PÉREZ MORA

ANDRÉS FELIPE MORA OJEDA

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

FACULTAD TECNOLÓGICA

INGENIERÍA TELEMÁTICA

BOGOTÁ

2016

SISTEMA TELEMÁTICO PARA CENTRALIZAR EL CONSUMO DE MENSAJERÍA XML SOBRE EL PROTOCOLO HTTP

EDGAR ANDRÉS PÉREZ MORA

ANDRÉS FELIPE MORA OJEDA

Tesis

Director

Miguel Ángel Leguizamón Páez

Ingeniero de Sistemas

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

FACULTAD TECNOLÓGICA

INGENIERÍA TELEMÁTICA

BOGOTÁ

2016

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del Jurado

Bogotá, 11 de abril de 2016

Dedicado a:

Todos aquellos miembros de la comunidad estudiantil de la Universidad Francisco José de Caldas que hicieron parte integral de nuestra formación como personas y como profesionales.

A nuestros padres, familiares y amigos quienes durante todo el proceso de formación fueron un apoyo fundamental para llevar a feliz término todos nuestros objetivos personales y profesionales.

Agradecimientos

Al profesor Miguel Ángel Leguizamón quien como tutor del proyecto nos colaboró de manera abnegada e incondicional. Sus aportes con base en la fundamentación teórica y los amplios conocimientos sobre el manejo de proyectos fueron indispensables para sacar el proyecto adelante.

A todos los profesores del proyecto curricular de Ingeniería Telemática pues cada uno aporto una gran cantidad de conocimiento que se refleja en el presente proyecto.

Al profesor Guillermo Hurtado quien auspicia de jurado del presente proyecto pues sus correcciones e indicaciones sobre cómo se debió desarrollar el proyecto fueron fundamentales en el proceso de desarrollo del mismo.

CONTENIDO

Contenido
INTRODUCCION ..... **¡Error! Marcador no definido.**
OBJETIVOS 11
GENERAL 11
ESPECIFICOS ..... **¡Error! Marcador no definido.**
1. IDENTIFICACION DE LAS NECESIDADES 12
1.1. ANALISIS DE METAS Y LIMITACIONES 12
1.1.1. Metas 12
1.1.2. Limitaciones 14
1.2. ANALISIS DE METAS TECNICAS Y COMPROMISOS 14
1.3. CARACTERIZACION DE LA SITUACION ACTUAL 15
2. DISEÑO LOGICO DEL SISTEMA 16
2.1. DISEÑO DE LA ARQUITECTURA DEL SISTEMA 16
2.2. DISEÑO DE RED DE LOS COMPONENTES DEL SISTEMA 19
2.3. DISEÑO DE COMPONENTES DE SEGURIDAD DEL SISTEMA 20
2.4. DISEÑO DE ESTRATEGIAS DE ADMINISTRACION DEL SISTEMA 21
3.1. SELECCIÓN DE DISPOSITIVOS A SER EMPLEADOS EN EL SISTEMA 28
4. PRUEBA DOCUMENTACION Y OPTIMIZACION DEL SISTEMA 31
4.1. PRUEBA INTEGRAL DEL SISTEMA 31
4.2. DOCUMENTACION DEL SISTEMA 34
5. CONCLUSIONES 48
6. RECOMENDACIONES 49
BIBLIOGRAFIA ..... **¡Error! Marcador no definido.**

TABLA DE ILUSTRACIONES.

Ilustración 1: Situación Actual. Fuente: Los Autores. 16
Ilustración 2: Arquitectura del Middleware. Fuente: Los Autores. 17
Ilustración 3: Modelo de datos. Fuente: Los Autores. 18
Ilustración 4: Caso de uso. Fuente: Los autores. 18
Ilustración 5: Percepción del middleware. Fuente: Los Autores. 19
Ilustración 6: Topología de red. Fuente: Los Autores. 19
Ilustración 7: Consola WEB VMWARE. Fuente: Los autores. 22
Ilustración 8: Consola vsphere Client. Fuente: Los autores. 23
Ilustración 9: Consola WEB FortiGate. Fuente: Los autores. 23
Ilustración 10: Consola SSH FortiGate. Fuente: Los autores. 24
Ilustración 11: Consola WEB Microsoft Azure. Fuente: Los autores. 25
Ilustración 12: Acceso WebLogic. Fuente: Los autores. 26
Ilustración 13: Configuraciones WebLogic. Fuente: Los autores. 26
Ilustración 14:Conexion a la base de datos WebLogic. Fuente: Los autores. 27
Ilustración 15: Middleware del aplicativo. Fuente: Los autores. 27
Ilustración 16: Configuración de Namespaces. Fuente: Los autores. 31
Ilustración 17: Configuración de destinos. Fuente: Los autores. 31
Ilustración 18: Configuración de contenidos. Fuente: Los autores. 31
Ilustración 19: Configuración de documentos. Fuente: Los autores. 32
Ilustración 20: Configuración de nodos. Fuente: Los autores. 32
Ilustración 21: Servicio WEb SOAP. Fuente: Los autores. 32
Ilustración 22: Ubicación de servicios. Fuente: Los autores. 33
Ilustración 23: Servicio de consulta de usuario por cedula. Fuente: Los autores. 33
Ilustración 24: Servicio para consultar el rol de cada usuario. Fuente: Los autores. 33
Ilustración 25: Servicio para consultar los permisos del rol. Fuente: Los autores. 33
Ilustración 26: Interfaz middleware. Fuente: Los autores. 34
Ilustración 27: Administración de discos NAS. Fuente: Los autores. 35
Ilustración 28: Discos ISCSI de NAS. Fuente: Los autores. 36
Ilustración 29: Configuración tarjetas de red NAS. Fuente: Los autores. 36
Ilustración 30: Interfaces FortiGate. Fuente: Los autores. 37
Ilustración 31: DNS FortiGate. Fuente: Los autores. 38
Ilustración 32: Rutas estáticas. Fuente: Los autores. 39
Ilustración 33: Ruta estática Columbus. Fuente: Los autores. 39
Ilustración 34: Políticas de enrutamiento FortiGate. Fuente: Los autores. 40
Ilustración 35: Políticas de enrutamiento Columbus FortiGate. Fuente: Los autores. 40
Ilustración 36: Políticas de enrutamiento ETB FortiGate. Fuente: Los autores. 41
Ilustración 37: VPN Site to Site Fortigate-Azure. Fuente: Los autores. 41
Ilustración 38: Usuarios FortiGate. Fuente: Los autores. 42
Ilustración 39: Ventana de estado VMWARE. Fuente: Los autores. 43
Ilustración 40: Configuración de storage VMWARE. Fuente: Los autores. 43
Ilustración 41: Datastore 1 VMWARE. Fuente: Los autores. 44
Ilustración 42: Datastore UD VMWARE. Fuente: Los autores. 44
Ilustración 43: Datastore UDStorage VMWARE. Fuente: Los autores. 45
Ilustración 44: Configuración tarjetas de red servidor 1 VMWARE. Fuente: Los autores. 45

Ilustración 45: Configuración tarjetas de red servidor 2 VMWARE. Fuente: Los autores. 46
Ilustración 46: Licencia adquirida VMWARE. Fuente: Los autores. 46
Ilustración 47: Perfil de seguridad VMWARE. Fuente: Los autores. 47

INTRODUCCIÓN

Los servicios web son tecnologías basadas en estándares y protocolos que realizan el intercambio de información entre distintas aplicaciones. Este tipo de servicios cumplen el propósito de estandarizar la forma como se intercambia información y además garantizan que exista una interoperabilidad entre distintas plataformas tecnológicas.

En la actualidad existe un gran número de servicios web que exponen cierta cantidad de información a los usuarios (o clientes), lo cual de una u otra forma facilita el proceso de intercambio de información.

Uno de los lenguajes más utilizados para realizar el intercambio de información es el XML, el cual además es parte fundamental de tecnologías de servicios web como SOAP.

El presente proyecto se realiza con el fin de crear un sistema que facilite las labores de integración entre servicios web para generar un valor agregado por medio de las nuevas tecnologías de la información y la aplicación de una arquitectura bien definida como es la arquitectura orientada a servicios.

En el primer capítulo del documento parte de un análisis de la situación actual de una entidad financiera que tiene una gran cantidad de servicios web que exponen mensajería XML sobre el protocolo HTTP pero que no están integrados ni documentados, razón por la cual se identifica la necesidad de proveer un sistema que permita un control más adecuado de los servicios web que existen al interior de la entidad.

En el segundo capítulo del documento se identifica una serie de elementos y de TI que pueden ser útiles para el desarrollo de una solución tecnológica adecuada que permita la integración de mensajería expuesta por los servicios web. Se tiene en cuenta tanto el Hardware como el Software y se incluyen elementos que dan un valor agregado a la implementación como el uso de tecnologías en la nube.

En el diseño del sistema se prioriza en la disponibilidad del mismo y se establece una serie de medidas que dan una mayor disponibilidad fiabilidad y seguridad al sistema.

En cuanto a la parte de la integración de la mensajería XML, se desarrolló un componente específico en leguaje de programación Java el cual se instalara sobre la infraestructura definida y se encargara principalmente del procesamiento y traducción de la mensajería.

Las conexiones entre los diferentes proveedores de servicios y el componente desarrollado se realizaran utilizando el protocolo HTTP debido a que es un protocolo conocido y documentado.

En el tercer capítulo del documento se realizan unas pruebas integrales del mismo y se detalla el resultado en el presente documento con el fin de que sirva como un marco de referencia para futuras implementaciones similares.

Finalmente, se discuten algunos temas de implementación, recomendaciones y problemas obtenidos para dar una retroalimentación adecuada a la fase de desarrollo del proyecto.

La metodología aplicada para el desarrollo del proyecto fue top down pues ayuda a aterrizar varios conceptos de cómo se puede desarrollar un proyecto en el ámbito de ingeniería. Se escolio esta metodología porque ayuda al desarrollo adecuado del proyecto y porque incluye elementos no solo conceptuales sino que también a nivel de implementación.

OBJETIVOS

GENERAL

Crear un sistema telemático utilizando arquitectura SOA para centralizar el consumo de servicios web que exponen mensajería XML sobre el protocolo HTTP.

ESPECÍFICOS

- Analizar las propiedades y componentes fundamentales que tienen los sistemas de integración orientados a servicios web.
- Diseñar un sistema que permita integración de servicios que exponen mensajería XML sobre el protocolo HTTP utilizando el paradigma de arquitectura SOA.
- Implementar el sistema propuesto por medio de una metodología de desarrollo orientada a servicios.
- Evaluar el comportamiento del sistema en un ambiente propuesto y controlado en el cual se requiera integrar la funcionalidad de varios servicios web.

1. IDENTIFICACIÓN DE LAS NECESIDADES

1.1. ANÁLISIS DE METAS Y LIMITACIONES

1.1.1. Metas

El presente proyecto se realizó con base en un caso de estudio planteado, el cual se centra en una empresa del sector financiero que tiene un gran número de aplicaciones y servicios distribuidos.

Para realizar el proyecto se caracterizó una empresa del sector financiero definiendo algunas de las características más frecuentes con que cuenta este tipo de organizaciones, con el fin de aterrizar el sistema propuesto a un ambiente controlado y a la vez muy cercano a la realidad.

La realización de este proyecto tiene como meta poder brindar una alta disponibilidad y confiabilidad para la organización, presentado un modelo hibrido entre la infraestructura tecnológica de la organización y las nuevas tecnologías en la nube.

Para lograr lo anterior se plantea una solución que permita la integración de mensajería XML sobre el protocolo HTTP soportada sobre una arquitectura en la nube. Para lo cual se recurrirá a proveedores que provean este servicio y que además brinden funcionalidades robustas como los RPO (Recovery Point Objective) y los RTO (Recovery Time Objective).

- Para que la organización no sufra pérdidas considerables de información se debe tener un tiempo de RPO bajo, con ello las transacciones realizadas en un determinado periodo de tiempo serán almacenadas y así las operaciones que generen información dentro de la organización no se verán afectadas por fallos dentro del sistema. Se define entonces que el RPO en este caso debe estar por debajo de los 30 minutos.

- Para garantizar la continuidad del servicio de la organización es necesario tener un buen tiempo de RTO, con esto el sistema podrá presentar el servicio sin interrupción tanto para aplicativos de uso interno como para servicios expuestos en internet. Se define entonces que el tiempo ideal de RTO debe estar por debajo de los 30 minutos.

- En cuanto a la integración de la información, se considera que el sistema encargado de centralizar la mensajería XML sobre el protocolo HTTP debe ser capaz de garantizar unos tiempos óptimos de respuesta, los cuales no deben exceder los 5 segundos.

- Es importante además, tener en cuenta que el objetivo del proyecto es reducir el número de interfaces XML con las cuales debe interactuar un servicio con el fin de establecer comunicación con otros servicios, por lo

cual se define que el sistema propuesto debe servir de interfaz de integración entre servicios.

Referente a la infraestructura tecnológica de la organización se debe contar con alta disponibilidad de los servicios para no depender únicamente de servicios enfocados en la recuperación de desastres. Por ello se hará uso de tecnologías como clústeres, virtualización, failover y seguridad perimetral de los servidores de la organización:

- La tecnología de clústeres permite poder utilizar más de un host para prestar un mismo servicio, con ellos es posible evitar indisponibilidad en el servicio. El funcionamiento básico de un clúster radica en la existencia de dos host capaces de prestar el mismo servicio con el fin de que si uno de los dos nodos falla entrara el otro a prestar el servicio por los dos host mientras se logra reestablecer el host que fallo.

- Con la virtualización es posible llevar acabo la creación de servidores virtuales dentro de un mismo host, con ello es posible hacer mejor uso de los recursos informáticos disponibles en la organización ya que se pueden distribuir en servidores virtuales. Un gran beneficio de tener los servidores virtualidades es que se pueden mover de un host a otro sin afectar el servidor o el servicio, también es posible realizar backups y hacer uso de varias opciones que mejoran el uso de los servidores virtuales para poder brindar una mayor disponibilidad que con servidores físicos.

- Mediante un failover en el canal de internet se tendrá la opción de tener un respaldo en el canal principal de internet para con esto aumentar en porcentajes la disponibilidad de los servicios que se tiene hacia los clientes donde el proveedor principal llegase a presentar fallas o caída total del servicios se pueda tener acceso por el otro canal, permitiendo la continuidad de los servicios expuestos.

- En cuanto a seguridad perimetral es posible lograr aumentar el porcentaje de disponibilidad a los servicios debido a que la seguridad perimetral ayuda a detectar y detener posibles ataques informáticos, virus y demás posibles infecciones o acciones que puedan llegar a dañar e interrumpir los servicios expuestos por la compañía.

Con la unión de estas tres tecnologías se obtendrá una disponibilidad de servicio mayor al 99.90% y con ello no tener que recurrir a servicios en la nube para recuperación de fallos a menos de que sea estrictamente necesario.

Finalmente se plantea como meta la implementación del sistema haciendo uso de una arquitectura orientada a servicios debido a que es la arquitectura más adecuada para alinear los servicios tecnológicos que presta la organización con

los objetivos corporativos de la misma y permite una fácil integración entre arias aplicaciones.

1.1.2. Limitaciones

Debido al alto costo de poder tener una alta disponibilidad se tendrá las siguientes limitaciones:

- **Nube:** Se contratara a un único proveedor que brinde los mejores RPO y RTO por cuestiones de costo del proyecto.

- **Clúster:** Únicamente se tendrá un host físico para soportar múltiples host virtuales debido a la disponibilidad que se tiene en cuanto a equipos.

- **Virtualización:** Se utilizaría un hipervisor que nos brinde la posibilidad de poder virtualizar los servidores requeridos.

- **Seguridad perimetral:** se configurara los aspectos necesarios que se requiera para poder tener los servicios en su mayor tiempo disponible, sin realizar configuraciones a las demás opciones que brinde el appliance que se implemente.

- **Pruebas:** No se realizaran pruebas adicionales a los sistemas que o componentes que ayudan a generar el proyecto, específicamente se realizara las pruebas a los sistemas o componentes que lleven a cabo el funcionamiento del proyecto.

1.2. ANÁLISIS DE METAS TÉCNICAS Y COMPROMISOS

Con la implementación que se realizaría en la organización espera poder brindar un sistema con alta disponibilidad, con el fin de que las operaciones dentro de la organización no se vean afectadas por temas de falta de servidores. Con la implementación de un clúster, uso de la virtualización, un DRP (Plan de recuperación ante desastres) en la nube y un sistemas de seguridad perimetral se espera que el servicio tenga una disponibilidad del 99.90% al mes es decir que este podría estar fuera de servicio un máximo de 43.2 minutos al mes

El compromiso con esta implementación es poder lidiar con cualquier tipo de inconvenientes, desastres o imprevistos que se llegasen a presentar a los servidores que alojan los servicios de la organización y que la disponibilidad siempre este presente siendo transparente para los usuarios del sistema.

En cuanto al servicio de integración de mensajería XML, se establece que este debe facilitar y centralizar el manejo de mensajería XML sobre el protocolo HTTP. Para esto, es necesario que este sistema además de garantizar la

comunicación de servicios, también sirva como un repositorio de mensajería que podrá ser reutilizada por diferentes aplicativos de la organización de manera centralizada.

El compromiso que se hace en el desarrollo del proyecto es el de brindar a la organización en cuestión un sistema:

- **Robusto:** con el uso de la tecnología de virtualización y de clúster se puede tener un sistema el cual tendrá los recursos más que necesarios para desarrollar las tareas sin tener cuellos de botellas o la necesidad de parar el servicio para agrandar las características del hardware que lo soportan.
- **Fiable:** las consideraciones que se toman para tener una alta disponibilidad del 99.90% brinda una fiabilidad al cliente de poder tener el servicios requerido en la mayoría de los casos accesible con una posible interrupción de 43.2 minutos al mes.
- **Escalable:** si el uso de los servicios se ve en la necesidad de reducir números de solicitudes o de aumentar el número de solicitudes esto se podría realizar en tiempo real o en un periodo de tiempo corto mediante el uso de la infraestructura de virtualización.

Con el fin de facilitar la administración de la mensajería XML en la organización.

1.3. CARACTERIZACIÓN DE LA SITUACIÓN ACTUAL

El estado actual del sistema de la organización es de una disponibilidad moderada de los servicios, que aunque permite desempeñar las actividades relacionadas con el Core de negocio, no es suficiente para una empresa del sector financiero debido a la criticidad de cada una de las transacciones que se ejecutan.

Esta situación se da debido que no se tiene ninguna implementación que garantice redundancia en los servicios con el fin de garantizar una buena disponibilidad, actualmente no se cuenta con sistemas de respaldo o recuperación de la información y los que están disponibles dentro de la empresa son usados con fines completamente diferentes, tampoco existe un sistema de seguridad perimetral con las configuraciones adecuadas que pueda repeler ataques, virus y otras amenazas que puedan afectar la prestación del servicio.

A continuación se presentan un diagrama donde se pueden ver los dispositivos con los cuales cuenta la organización y se da una breve descripción de cada uno y de la forma como este se está utilizando en la empresa.

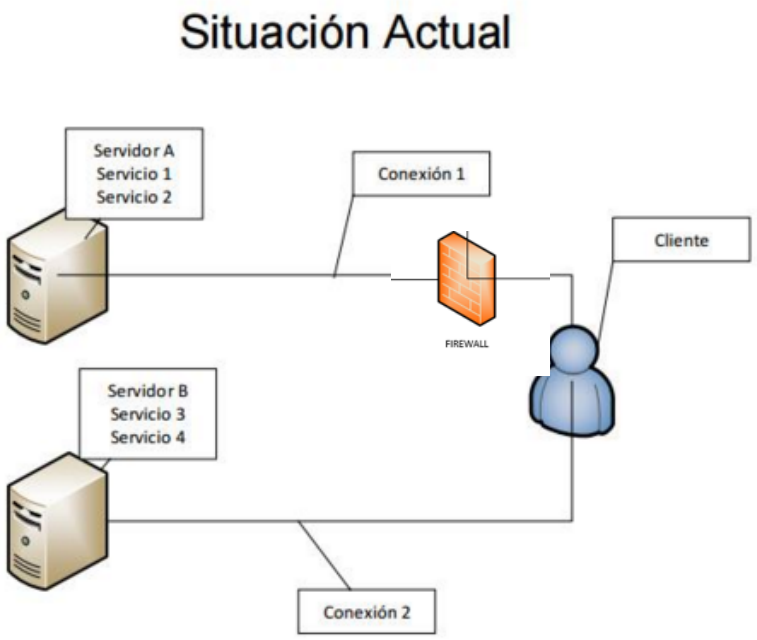


Ilustración 1: Situación Actual. Fuente: Los Autores.

IBM Blade Center S

Para un ahorro en espacio, energía y recursos se posee un Blade el cual está destinado para poder ser modular de tal forma que pueda ser armado a la necesidad del usuario, por lo cual se tiene para manejar los servidores de la compañía por cada cuchilla desperdiciando la capacidad de cada cuchilla debido a que poseen procesadores Intel Xeon de 6 procesadores físicos y 12 virtuales con una memoria RAM de 49 Gb ocasionando un sobredimensionamiento por encima de las necesidades que cumple los roles del sistema operativo instalado en cada cuchilla o cada host.

Fortigate 100D

Siendo un UTM se tiene con la opción única de realizar la conexión entre el ISP y la red local desperdiciando así todas las posibles configuraciones que tiene al nivel de seguridad perimetral.

2. DISEÑO LÓGICO DEL SISTEMA

2.1. DISEÑO DE LA ARQUITECTURA DEL SISTEMA

En cuanto al aplicativo que realizara la centralización de la mensajería se establece la siguiente distribución lógica:

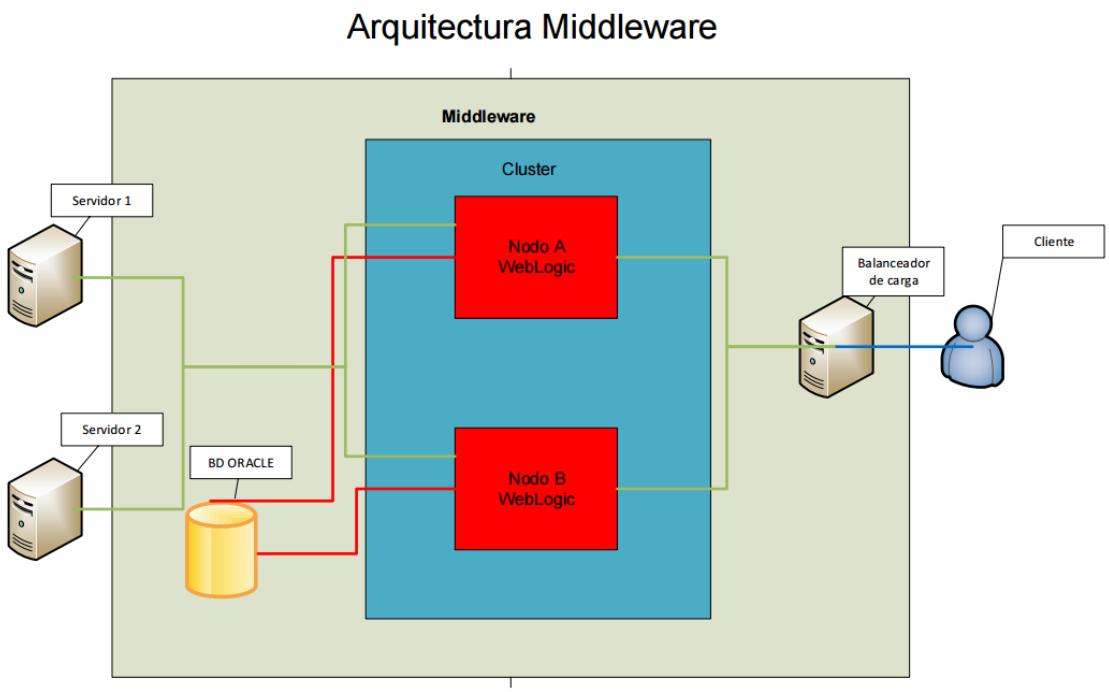


Ilustración 2: Arquitectura del Middleware. Fuente: Los Autores.

El sistema de integración realizara una mediación de mensajería XML, por lo cual lo más apropiado es definirlo con el nombre de middleware y se encargara de centralizar la mensajería XML por medio de una única interfaz que estará expuesta de cara a los clientes que requieren mensajería XML.

El middleware expondrá una interfaz por medio de un servicio de balanceo que se encargada de distribuir las peticiones que realicen los clientes a alguno de los dos nodos que tendrá el middleware internamente.

Cada nodo cuenta con un servidor de aplicaciones Weblogic, en el cual estará desplegada la aplicación que implementa la lógica de integración de mensajería XML basada en una serie de parametrizaciones.

El middleware contara con una base de datos en la cual estará almacenada la información de la mensajería XML y toda la parametrización respectiva para el correcto funcionamiento de las integraciones de mensajes.

A continuación se presenta el modelo de base de datos sobre el cual estará soportado el sistema:

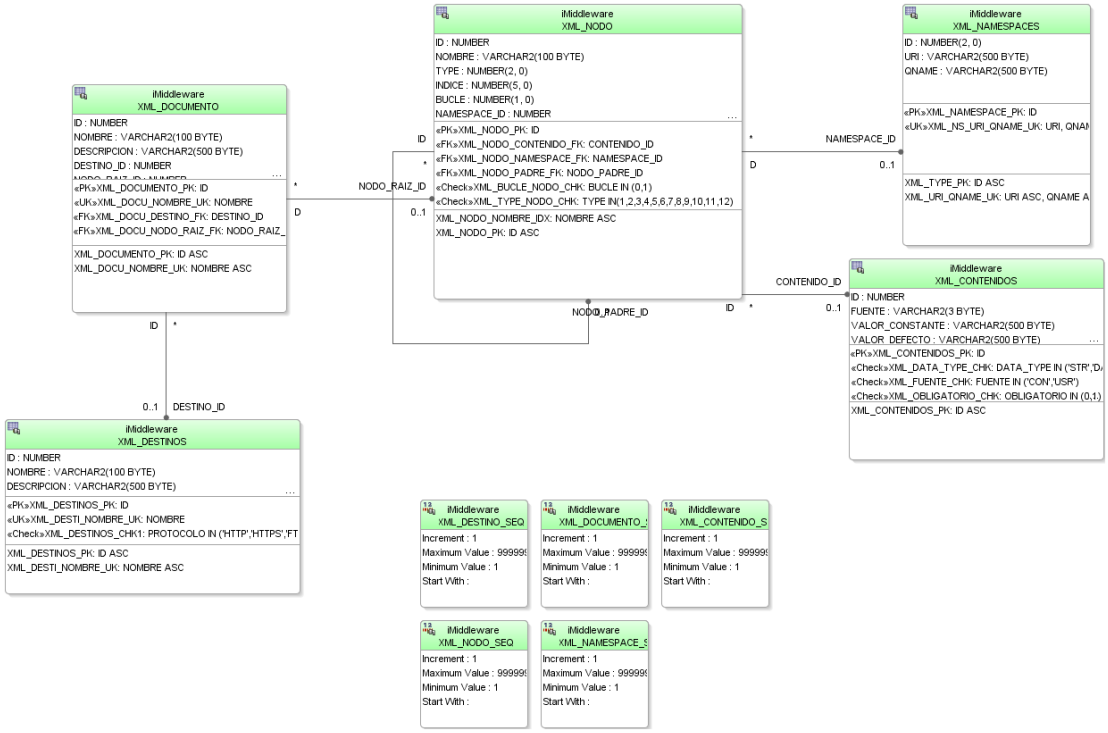


Ilustración 3: Modelo de datos. Fuente: Los Autores.

Finalmente, el middleware se conectara a los repositorios de servicios que exponen mensajería XML, la finalidad de esto es que el cliente solo establezca una conexión con el servicio de balanceo expuesto y no con una serie de servidores, donde se encontrara en el siguiente caso de uso del sistema de producción:

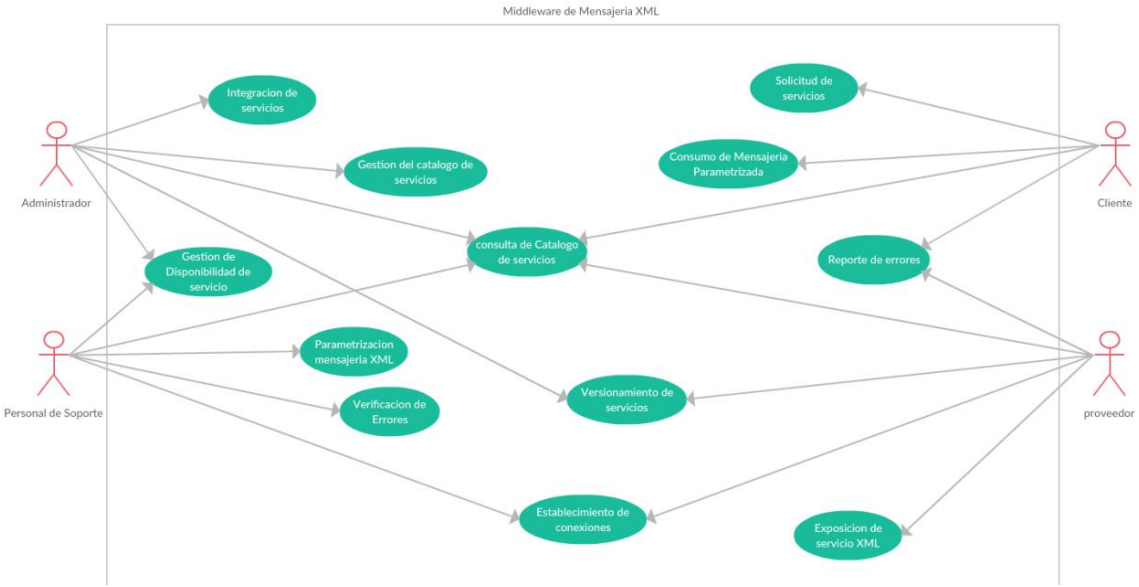


Ilustración 4: Caso de uso. Fuente: Los autores.

La percepción que tendrá el cliente del middleware será algo así como la expuesta en la siguiente figura:

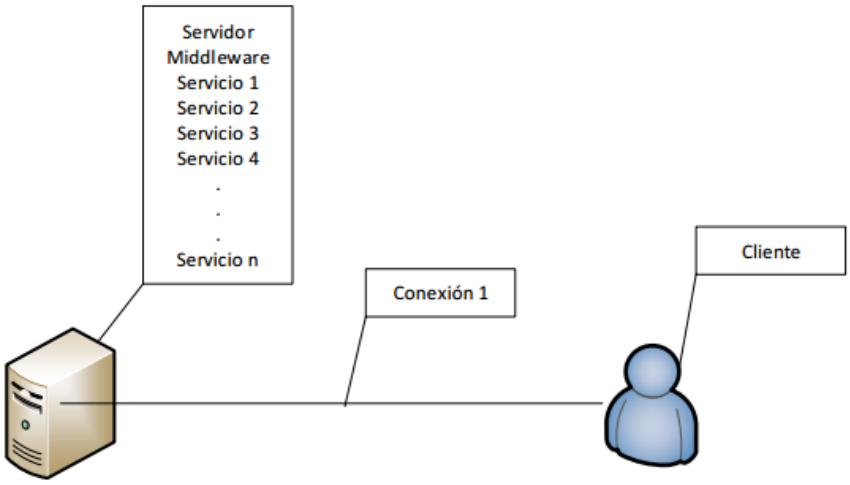


Ilustración 5: Percepción del middleware. Fuente: Los Autores.

2.2. DISEÑO DE RED DE LOS COMPONENTES DEL SISTEMA

La arquitectura está prevista de una forma que pueda ser entendible rápidamente por el usuario de una mera fácil y clara la cual llevara el siguiente modelo:

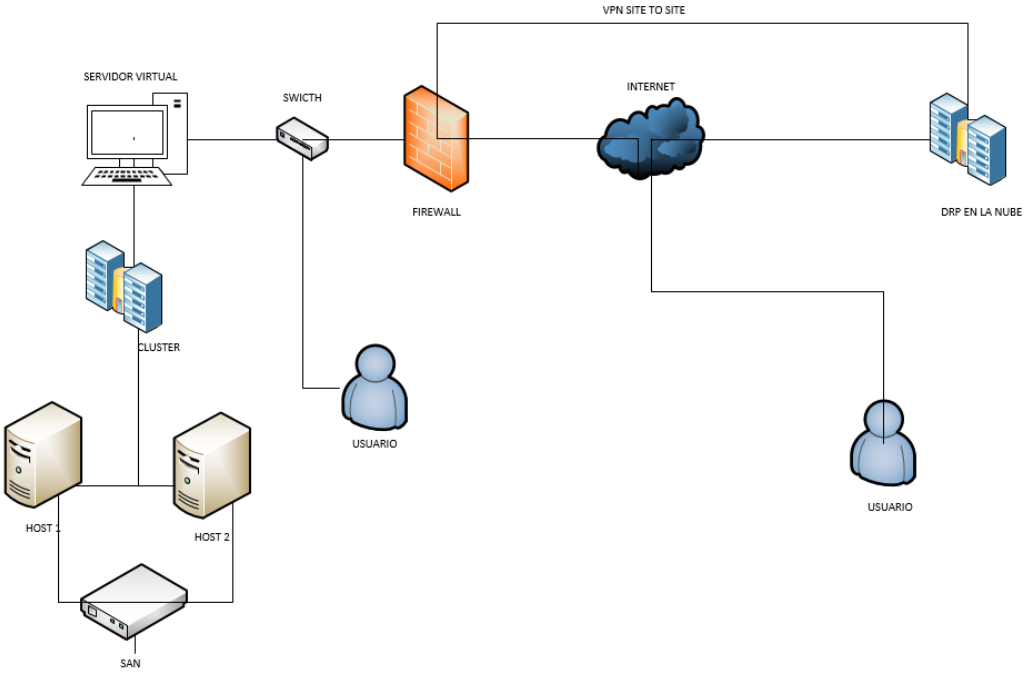


Ilustración 6: Topología de red. Fuente: Los Autores.

Con este modelo es posible obtener una arquitectura que permite tener una alta disponibilidad de los servicios expuestos por el servidor que alojara el aplicativo de integración

Los dispositivos físicos y configuración que componen el modelo de arquitectura son:

- **Dos Servidores IMB BladeCenter S:** En cada uno de estos host contendrá el sistema operativo de VMWare ESXI 6.0 que se utilizara para virtualizar las maquinas que se llegue a necesitar entre estas la máquina que tendrá el aplicativo para el montaje del clúster.
- **Un appliance FortiGate 100D:** Este otorgara la seguridad perimetral del sistema en general donde se realizara análisis de cada paquete que se transporte dentro de la LAN como de los datos que ingresen desde la WAN. También realizara la conexión vía VPN Site to Site hacia el DRP ubicado en la nube que será del proveedor Microsoft y el servicio será Microsoft Azure.
- **Un sistema de almacenamiento centralizado:** Este almacenamiento que brindar la tecnología ISCSI permite tener un almacenamiento compartido entre los host que se utilizarían para virtualizar pudiendo así tener un almacenamiento en conjunto donde se podrá compartir la información de los dos host para el guardado de la información de las máquinas virtuales.

En el aspecto de los aplicativos que se utilizara para poder realizar esta implementación se encontrara los siguientes:

- Sistema de Virtualización VMWare.
- Sistema de creación y gestión de Cluster VCenter.
- Sistema operativo Windows Server 2012 Standard.
- Cuenta en Windows Azure.
- Sistema operativo FortiOS.

2.3. DISEÑO DE COMPONENTES DE SEGURIDAD DEL SISTEMA

Para tener una fuerte seguridad perimetral en el sistema y que este no corra riesgos de ser vulnerado se implementara un sistema UTM (Unified Threat Management) el cual implementa seguridad tanto de salida como entrada de paquetes, el cual puede manejar las siguientes funcionalidades:

- UDP.
- VPN.
- Antispam.
- Antiphishing.

- Antispyware.
- Filtro de contenidos.
- Antivirus.
- IDS/IPS.

La configuración que realizara a nivel de seguridad es la siguiente:

- Tendrá habilitado la funcionalidad de antivirus para la entrada sobre las interfaces WAN y LAN.
- Tendrá habilitado la funcionalidad de antivirus para la salida sobre las interfaces WAN y LAN.
- Tendrá habilitado la funcionalidad de IDS/IPS para la entrada sobre las interfaces WAN y LAN.
- Tendrá habilitado la funcionalidad de IDS/IPS para la salida sobre las interfaces WAN y LAN.
- Tendrá habilitado la funcionalidad de Antiphishing para la entrada sobre las interfaces WAN y LAN.
- Tendrá habilitado la funcionalidad de Antiphishing para la salida sobre las interfaces WAN y LAN.
- Tendrá habilitado la funcionalidad de Filtro de contenido para la entrada sobre las interfaces WAN y LAN.
- Tendrá habilitado la funcionalidad de Filtro de contenido para la salida sobre las interfaces WAN y LAN.
- Tendrá comunicación por medio de VPN por el protocolo cifrado IPsec que va dirigido hacia el DRP alojado en la nube que es Windows Azure.

Con esta configuración se tendrá una protección por medio del firewall a un nivel alto para con ello poder tener control de los datos transportados y de las conexiones que se realizan tanto hacia afuera como hacia adentro de la red donde se está alojado los servidores.

Se creara una VPN Site to Site que se conectara directamente al sistema DRP alojado en nube con el proveedor que es Windows Azure, permitiendo poder trasportas datos vía internet pero por un canal seguro y totalmente administrable.

2.4. DISEÑO DE ESTRATEGIAS DE ADMINISTRACION DEL SISTEMA

La administración de los recursos que se tiene será llevada a cabo por medio del centro de administración que cada plataforma ofrece para con esto poder tener plena seguridad que las configuraciones realizadas sean certificadas y homologadas por el fabricante.

Virtualización por medio del hipervisor VMWare

La consola de administración de la plataforma de virtualización VMWare VCenter se puede realizar el acceso mediante dos formas las cuales son:

1. WEB: Es la opción más fácil y con más opciones de administración que se puede acceder mediante un navegador WEB por medio de la dirección IP del servidor donde se encuentre instalado o alojado el servidor de VCenter.

   En esta se encontraran las configuraciones de cada host como las configuraciones como tal del cluster donde se podran crear máquinas virtuales, crear storage, crear redes, etc. Al ser un entorno WEB presenta lentitud a la hora de presentar las tareas hacia el usuario lo que ocasiona que algunas veces se deba recargar la página para visualizar el cambio de la información.

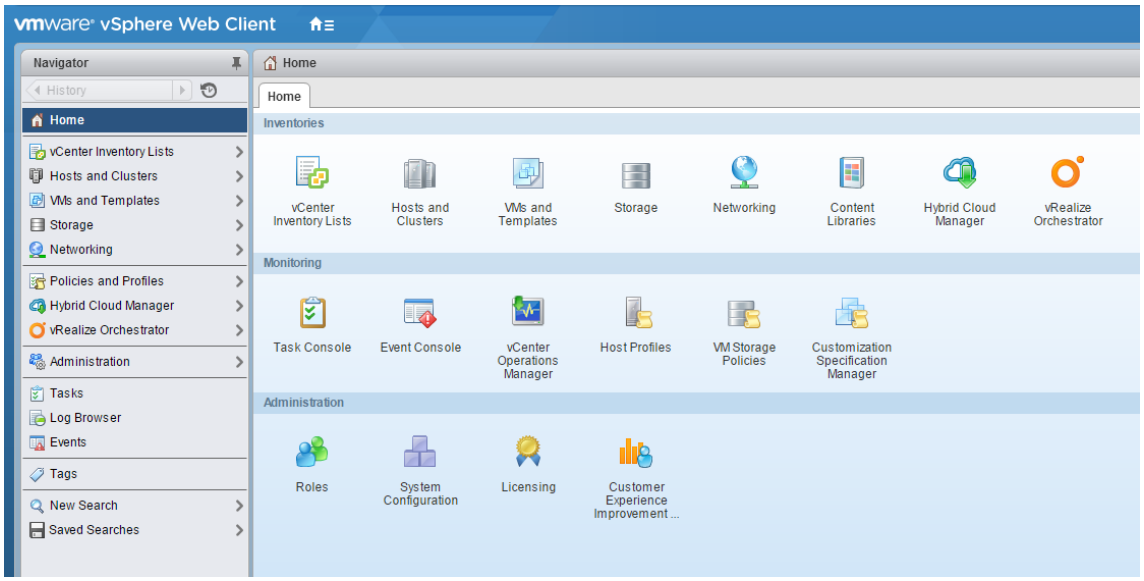


Ilustración 7: Consola WEB VMWARE. Fuente: Los autores.

2. vSphere Client: Esta opción permite tener un control de las configuraciones rápidas hacia el cluster para con ellos poder administrar las máquinas y las configuraciones de una manera más fácil al poder otorgar mejores ventanas y velocidad a la hora de poder realizar estos cambios o nuevas implementaciones. Para ello se debe descargar el aplicativo directamente desde la página de VMWare o accediendo vía WEB hacia uno de los hosts que tengan instalado el sistema operativo de virtualización y realizar la instalación en el equipo desde donde se desea acceder a la consola de administración.

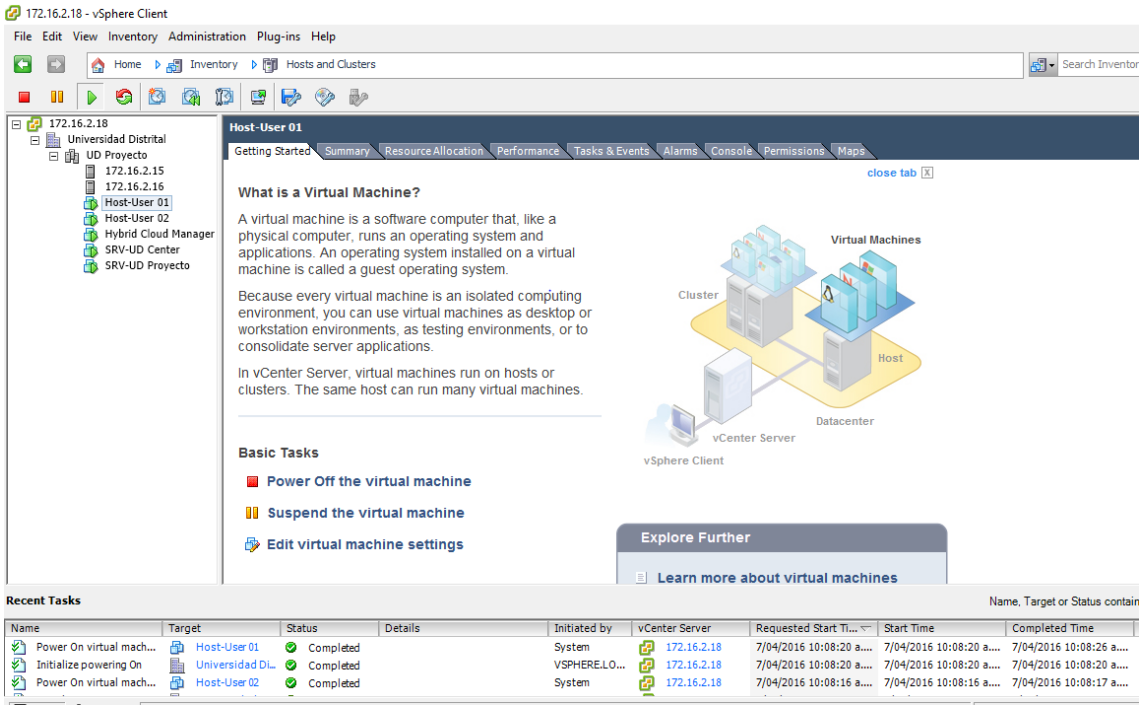


Ilustración 8: Consola vsphere Client. Fuente: Los autores.

Seguridad perimetral por medio de UTM FortiGate 100D

La administración de este appliance se puede realizar por medio de dos formas las cuales son:

1. WEB: Es la opción más fácil en que se puede acceder mediante un navegador WEB por medio de la dirección IP del appliance.

   En esta opción se encontrara las configuraciones más globales acerca de las configuraciones de las interfaces, políticas de seguridad, publicaciones, VPN, etc. Gracias a ser WEB tiene gran facilidad de administración debido a que su entorno es gráfico y muy intuitivo con la opción de botones de ayuda que guiaran al usuario o administrador en los pasos de configuraciones o de implementaciones.

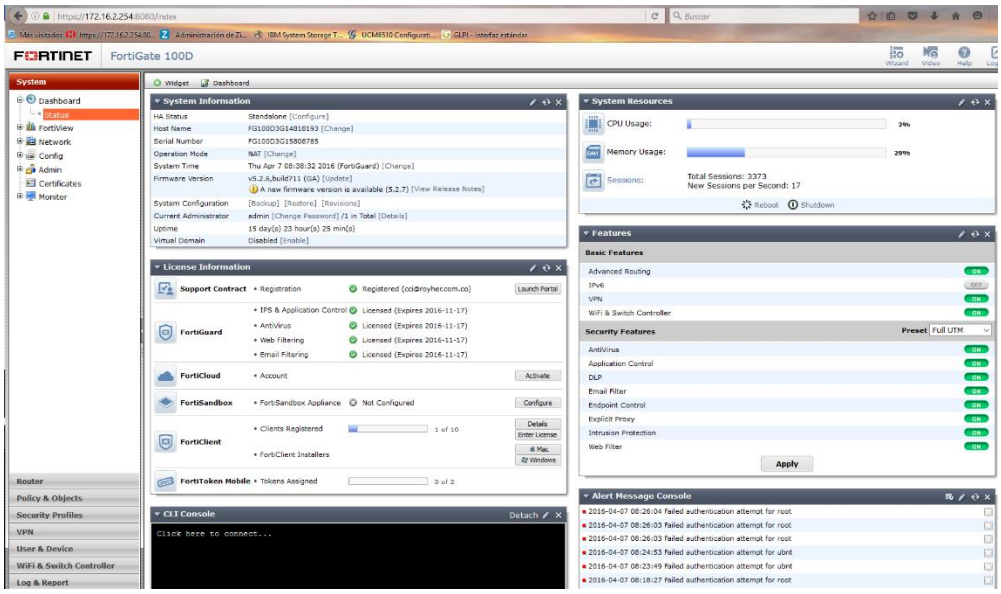


Ilustración 9: Consola WEB FortiGate. Fuente: Los autores.

2. Consola: Por este medio se puede ingresar mediante el puerto de consola que trae el appliance por medio de un cable RJ45 a puerto COM DB9 por medio de una terminal o un programa que pueda manejar protocolo SSH. La otra forma es ingresar por medio de una terminal o un programa que maneje protocolo SSH por medio de la dirección IP que se le haya proporcionado a appliance.

Este método de administración tiene un nivel de dificultad mayor debido que solo se puede realizar la administración, consultas o implementaciones por medio de comandos lo cual se debe tener conocimiento previo de los comandos designados por el fabricante. La gran ventaja que se posee al poder realizar la administración por medio de la consola es que se puede realizar cualquier tipo de configuraciones y varias configuraciones que por el ambiente WEB no posee la opción.

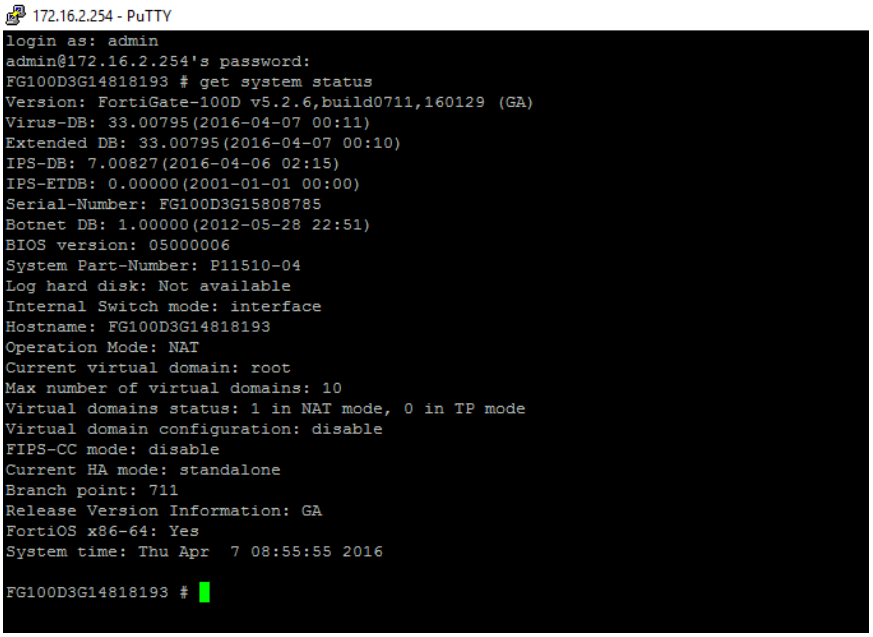


Ilustración 10: Consola SSH FortiGate. Fuente: Los autores.

DRP hacia la nube mediante Microsoft Windows Azure

La consola de administración del DRP se realiza mediante la misma consola de administración de todos los servicios que dispone Windows Azure dado que presenta más servicios independientes al que se utilizara.

El acceso se realiza mediante un navegador WEB donde se tiene las opciones de configuración adicionando el mismo inconveniente de tener que realizar la recarga de la página en ocasiones que se realiza alguna modificación debido a que no se visualiza el cambio lo cual ocasiona errores debido a que se envía la misma solicitud más de una vez.

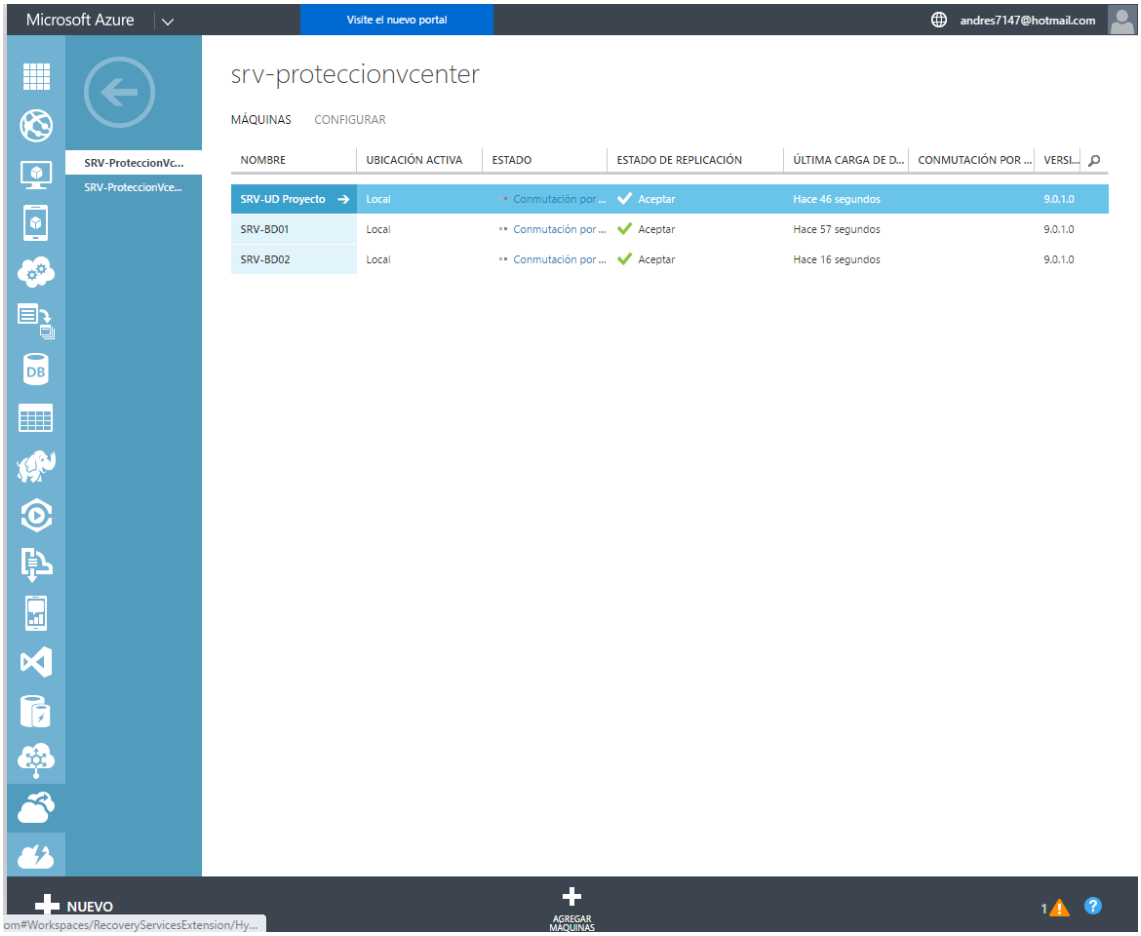


Ilustración 11: Consola WEB Microsoft Azure. Fuente: Los autores.

Servidor de Aplicaciones Weblogic Server (versión 12.2.1.0)

Es un servidor de aplicaciones Java EE y también un servidor HTTP; este servidor se instalará en los dos nodos del clúster y contendrá el middleware de mensajería que será encargado de centralizar los mensajes XML, se escogió este servidor de aplicaciones debido a que es uno de los más robustos y tiene múltiples opciones de configuración. Es un servidor que además cuenta con un amplio soporte y tecnología de punta.

Ilustración 12: Acceso WebLogic. Fuente: Los autores.

Dentro de sus múltiples configuraciones, es posible crear clúster y asignar máquinas virtuales a nodos del clúster, así como también configurar el dominio completo de trabajo.

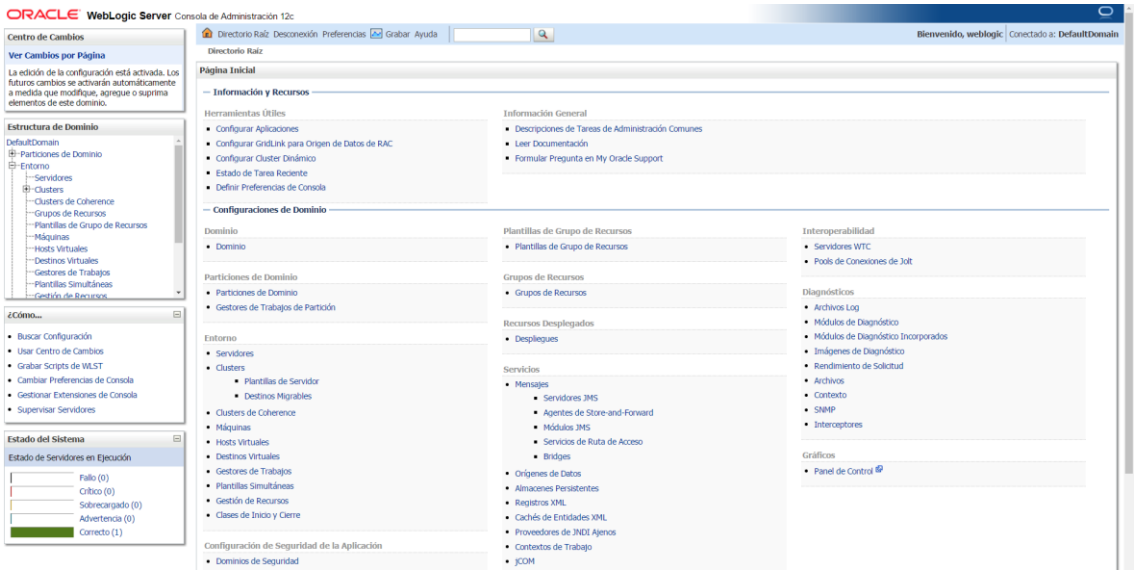


Ilustración 13: Configuraciones WebLogic. Fuente: Los autores.

Es importante denotar que el servidor de aplicaciones Weblogic se adapta muy bien a la arquitectura instalada en el sistema y permite la modificación y configuración de varias opciones importantes al momento de requerir cambios en el sistema.

Tanto la conexión con la base de datos como el despliegue del aplicativo de integración (middleware) pueden realizarse de manera fácil y rápida, y no dependen la infraestructura en caso de que se requiera algún tipo de migración.

La conexión con la base de datos se realiza en la configuración de orígenes de datos.

Resumen de Orígenes de Datos JDBC

Configuración | Supervisión

Un origen de datos JDBC es un objeto enlazado al árbol JNDI que proporciona conectividad de base de datos a través de un pool de conexiones JDBC. Las aplicaciones pueden buscar un origen de datos en el árbol JNDI y tomar prestada una conexión de base de datos de un origen de datos.

En esta página, se resumen los objetos del origen de datos que se han creado en este dominio.

Personalizar esta Tabla

Orígenes de Datos (Filtrado: Existen Más Columnas)

Nuevo | Suprimir — Mostrando 1 a 6 de 6 Anterior | Siguiente

Nombre	Tipo	Nombre de JNDI	Destinos	Ámbito	Particiones de Dominio
jdbc/IMIDDLEWAREDS	Genérico	jdbc/IMIDDLEWAREDS	DefaultServer	Global	
LocalSvcTblDataSource	Genérico	jdbc/LocalSvcTblDataSource	DefaultServer	Global	
mds-owsm	Genérico	jdbc/mds/owsm	DefaultServer	Global	
opss-audit-DBDS	Genérico	jdbc/AuditAppendDataSource	DefaultServer	Global	
opss-audit-viewDS	Genérico	jdbc/AuditViewDataSource	DefaultServer	Global	
opss-data-source	Genérico	jdbc/OpssDataSource	DefaultServer	Global	

Nuevo | Suprimir — Mostrando 1 a 6 de 6 Anterior | Siguiente

Ilustración 14:Conexion a la base de datos WebLogic. Fuente: Los autores.

El aplicativo Middleware es el aplicativo encargado de la integración.

Resumen de Despliegues

Configuración | Control | Supervisión

Esta página muestra la lista de aplicaciones Java EE y módulos de aplicación autónomos instalados en este dominio.

Puede actualizar (volver a desplegar) o suprimir las aplicaciones y módulos instalados desde el dominio activando la casilla de control situada junto al nombre de la aplicación y, a continuación, utilizando los controles de esta página.

Para instalar una nueva aplicación o módulo para el despliegue de destinos en este dominio, haga clic en **Instalar**.

Personalizar esta Tabla

Despliegues

Instalar | Actualizar | Suprimir — Mostrando 1 a 10 de 33 Anterior | Siguiente

Nombre	Estado	Estado	Tipo	Destinos	Ámbito	Particiones de Dominio	Orden de Despliegue
adf.oracle.businesseditor(1.0,12.2.1.0.0)	Activo		Biblioteca	DefaultServer	Global		100
adf.oracle.domain(1.0,12.2.1.0.0)	Activo		Biblioteca	DefaultServer	Global		100
adf.oracle.domain.webapp(1.0,12.2.1.0.0)	Activo		Biblioteca	DefaultServer	Global		100
coherence-transaction-rar	Activo	OK	Adaptador de Recursos	DefaultServer	Global		100
DMS Application (12.2.1.0.0)	Activo	OK	Aplicación Web	DefaultServer	Global		5
IMiddleware	Activo	OK	Aplicación de Empresa	DefaultServer	Global		100
jsf(2.0,1.0.0.0_2-2-8)	Activo		Biblioteca	DefaultServer	Global		100
jstl(1.2,1.2.0.1)	Activo		Biblioteca	DefaultServer	Global		100
odl.clickhistory(1.0,12.2.1)	Activo		Biblioteca	DefaultServer	Global		100
odl.clickhistory.webapp(1.0,12.2.1)	Activo		Biblioteca	DefaultServer	Global		100

Instalar | Actualizar | Suprimir — Mostrando 1 a 10 de 33 Anterior | Siguiente

Ilustración 15: Middleware del aplicativo. Fuente: Los autores.

3. DISEÑO FÍSICO DEL SISTEMA

3.1. SELECCIÓN DE DISPOSITIVOS A SER EMPLEADOS EN EL SISTEMA

Se utilizara los recursos que dispone la empresa debido a que no presentan una desactualización en sus componentes, los cuales se mencionaran las características principales:

Fortigate 100D

Se utiliza para describir los cortafuegos de red que engloban múltiples funcionalidades en una misma máquina. Algunas de las funcionalidades que puede incluir son las siguientes:

- UDP
- VPN
- Antispam
- Antiphishing
- Antispyware
- Filtro de contenidos
- Antivirus
- Detección/Prevención de Intrusos (IDS/IPS)

Se trata de cortafuegos a nivel de capa de aplicación que pueden trabajar de dos modos:

- Modo proxy: Hacen uso de proxys para procesar y redirigir todo el tráfico interno.
- Modo Transparente: no redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones de hardware.

Desventajas:

Se crea un punto único de fallo y un cuello de botella, es decir si falla este sistema la organización queda desprotegida totalmente. Tiene un coste fijo periódico.

Ventajas:

Se pueden sustituir varios sistemas independientes por uno solo facilitando su gestión.

Por lo cual se obtiene múltiples funciones añadidas, trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo.

Para gestionar la seguridad informática perimetral a nivel de Firewall, VPN, Router, antivirus y antispam perimetral. También requiere conocimientos propios de este tipo de servicios y del equipo en mención. Es recomendable que la persona que gestione este equipo tenga certificación sobre el mismo.

IBM Blade Center S.

Todos en uno: integra servidores, almacenamiento de red de área de almacenamiento (SAN), redes y entrada/salida (E/S) en un único chasis. No se necesita cableado especial: utiliza cables de alimentación estándar de oficina compatibles con 100 – 240 V.

Tecnología modular flexible: integra una familia de servidores blade de IBM® compatibles con una amplia gama de sistemas operativos (SO) y aplicaciones. Fácil de implementar, usar y gestionar.

Ayuda a crear infraestructuras de TI mejores para el medio ambiente: la tecnología Cool Blue de IBM proporciona una gama de herramientas que ayudan a planificar, gestionar y controlar la alimentación y la refrigeración.

Tanto las grandes empresas como las pequeñas dependen de sus sistemas de TI para ofrecer el alto nivel de rendimiento, disponibilidad y resistencia que demandan socios y clientes. Pero para seguir siendo competitivas, las empresas deben encontrar una forma económica de simplificar y gestionar de forma eficiente los requisitos tecnológicos, en constante evolución. Las pequeñas y medianas empresas (PYMES), en concreto, se ven obligadas a hacer más con menos espacio, menos recursos de TI y presupuestos más ajustados.

Para muchas empresas, IBM BladeCenter es la respuesta. Muchas grandes empresas saben desde hace tiempo que los sistemas blade pueden contribuir a:

- Reducir las redes de servidores físicas relacionadas con las empresas habituales.
- Minimizar el personal de TI que se necesita para gestionar las aplicaciones esenciales para llevar a cabo las funciones empresariales cotidianas.
- Reducir costes gracias a la posibilidad de añadir más servidores, almacenamiento y redes simplemente cuando sea necesario.
- Ahorrar energía gracias a un consumo de energía reducido en comparación con los servidores de bastidor.

IBM ofrece la potencia de BladeCenter a las PYMES. IBM BladeCenter S ofrece el primer chasis de blade del sector diseñado exclusivamente para las oficinas

pequeñas y medianas y los entornos distribuidos. BladeCenter S, que ofrece simplicidad y ahorro, está diseñado para obtener grandes resultados de TI incluso con el personal de TI más reducido.

El recurso que se adquirirá será un almacenamiento compartido por medio de una NAS (Network Attached Storage) que presenta la tecnología de poder realizar discos duros compartidos por medio de la tecnología ISCSI que se presentara a los host para realizar el almacenamiento de las máquinas que se virtualizaran, la NAS escogida es:

LENOVO® EMC® PX12-400R

Almacenamiento centralizado en red la cual presenta los siguientes beneficios:

Alto rendimiento: Fue creado con base en el procesador Intel Xeon para dar soporte a las exigentes cargas de trabajo, tales como la virtualización, la deduplicación, la administración de bases de datos y la vigilancia por video.

Acronis ATI Lite: Completar la protección de backup a través de toda tu red de pequeña empresa con Acronis. Protege tus PC con ATI Lite 2013 (3 licencias incluidas). Las aplicaciones opcionales Acronis ABR 11.5 OEM Server y NAS (se venden por separado) ofrecen protección de copias de seguridad automática y continua para tu Windows.

Tecnología de virtualización integrada: Haz funcionar múltiples máquinas virtuales (VM) en un solo dispositivo LenovoEMC. Permite que aplicaciones de Windows y almacenamiento de Linux se ejecuten de manera simultánea. Es ideal para la lectura-escritura de bases de datos, servidores para impresión y copias de seguridad de servidores de intercambio.

Copias de seguridad Active Snapshot: Copias de seguridad en el momento exacto para una imagen de volumen completo, incluyendo la capacidad Active Snap. También se utiliza .VSS y .VDS para compatibilidad con huéspedes Windows y VMware.

Alta disponibilidad de Active Directory (ADHA) y autenticación híbrida: Active Directory de Windows, incluyendo IVX (Extensión de virtualización integrada), ADHA (Autenticación híbrida de directorios activos), dominios confiables, Cluster Server de Microsoft y soporte para migración Hyper-V Live.

Caché SSD: para lectura y escritura más veloz Configura SSD específicos para escritura y lectura más rápidas de la información a la que se accede con frecuencia, proporcionando un mayor rendimiento de las aplicaciones exigentes de I/O, como por ejemplo, las bases de datos.

Copias de seguridad Personal Cloud de LenovoEMC: Sincroniza la información entre los sistemas miembros del personal cloud y tu dispositivo de almacenamiento en red.

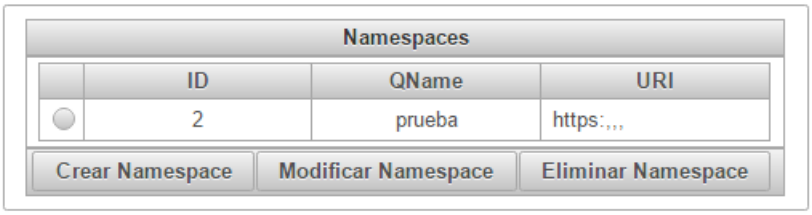
McAfee VirusScan Enterprise incorporado: Les brinda a las pequeñas empresas la posibilidad de implementar el almacenamiento en red en lugares donde previamente podría haber habido un virus y/o una vulnerabilidad ante un malware.

4. PRUEBA DOCUMENTACIÓN Y OPTIMIZACIÓN DEL SISTEMA

4.1. PRUEBA INTEGRAL DEL SISTEMA

Lo primero que se debe hacer en el sistema es configurar los mensajes XML que serán utilizados.

Configuración de Namespaces:



Namespaces

	ID	QName	URI
	2	prueba	https:,,,

Crear Namespace | Modificar Namespace | Eliminar Namespace

Ilustración 16: Configuración de Namespaces. Fuente: Los autores.

Configuración de Destinos:

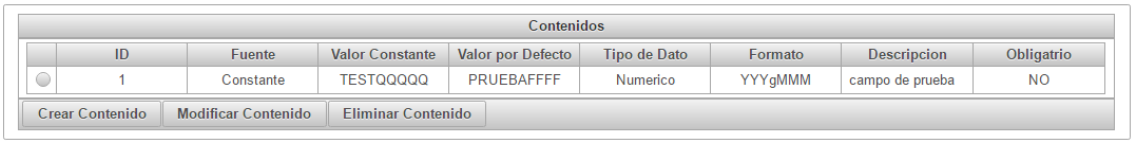
Destinos

	ID	Nombre	Descripción	Protocolo	URI
	41	WS_CONSULTA_ROLES	Servicio web que permite consultar un rol	HTTPS	http://localhost:7101/servicios/ConsultaRolesPort
	43	WS_CONSULTA_USUARIOS	Servicio web que permite consultar un usuario	HTTP	http://localhost:7101/servicios/ConsultaUsuariosPort
	7	WS_CONSULTA_PERMISOS	Servicio web que permite consultar un permiso	HTTPS	http://localhost:7101/servicios/ConsultaPermisosPort

Crear Destino | Modificar Destino | Eliminar Destino

Ilustración 17: Configuración de destinos. Fuente: Los autores.

Configuración de Contenidos:



Contenidos

	ID	Fuente	Valor Constante	Valor por Defecto	Tipo de Dato	Formato	Descripcion	Obligatrio
	1	Constante	TESTQQQQQ	PRUEBAFFFF	Numerico	YYYgMMM	campo de prueba	NO

Crear Contenido | Modificar Contenido | Eliminar Contenido

Ilustración 18: Configuración de contenidos. Fuente: Los autores.

Configuración de Documentos:

Documentos

	ID	Nombre	Descripción	Destino	Nodo Raiz
	1	DOC_CONSULTA_USUARIO	XML del servicio de consulta de usuarios	WS_CONSULTA_USUARIOS	ROOT
	2	DOC_CONSULTA_ROLES	XML del servicio de consulta de roles	WS_CONSULTA_ROLES	LEVEL1
	5	DOC_CONSULTA_PERMISOS	XML del servicio de consulta de permisos	WS_CONSULTA_PERMISOS	LEVEL2

Crear Documento | Modificar Documento | Eliminar Documento

Ilustración 19: Configuración de documentos. Fuente: Los autores.

Configuración de Nodos:

Nodos

ID	Nombre	Type	Indice	Bucle	Namespace Id	Contenido Id	Nodo Padre Id
1	ROOT	ELEMENT_NODE	0	NO			
2	LEVEL1	ATTRIBUTE_NODE	0	SI			1
3	LEVEL2	TEXT_NODE	0	NO	2	1	2
7	LEVEL3	CDATA_SECTION_NODE		NO			3
6	LEVEL4	ENTITY_REFERENCE_NODE	0	NO			7
8	NIVEL2	ENTITY_NODE		NO			2
9	TEMP	PROCESSING_INSTRUCTION_NOD		NO			2
10	TEST	COMMENT_NODE		NO			3
11	DOC	DOCUMENT_NODE		NO			7
12	DOCTYPE	DOCUMENT_TYPE_NODE		NO			7
13	FRAGMENT	DOCUMENT_FRAGMENT_NODE		NO			12
14	NOTATION	NOTATION_NODE		NO			3

Crear Nodo | Modificar Nodo | Eliminar Nodo

Ilustración 20: Configuración de nodos. Fuente: Los autores.

Las pruebas integrales del sistema se realizaron con ayuda del software SOAPUI que permite realizar pruebas de servicios web SOAP (estos servicios utilizan XML sobre HTTP).

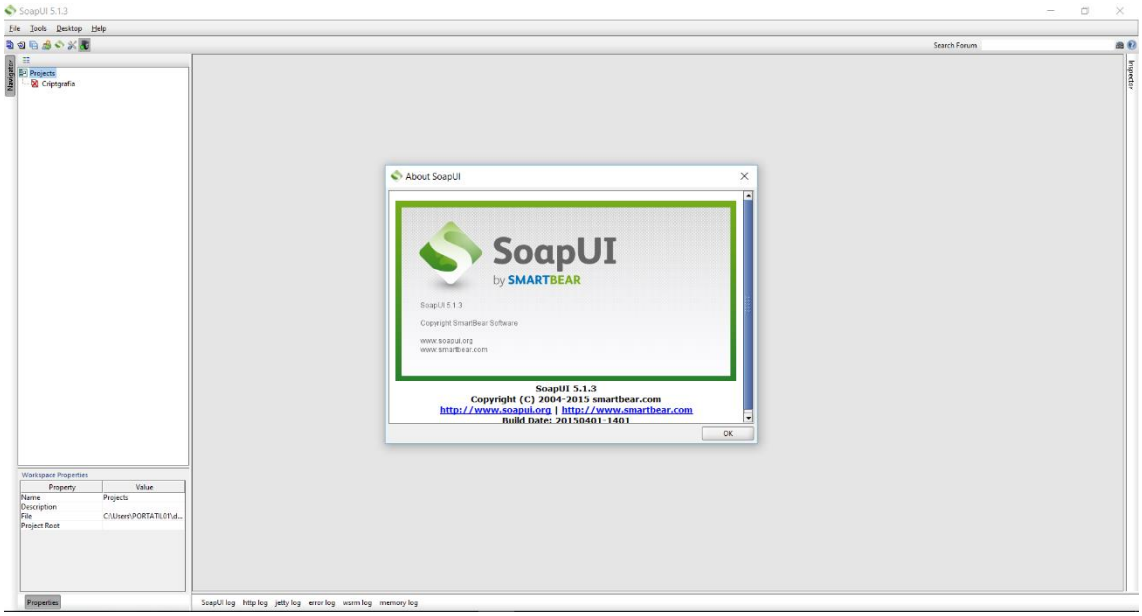


Ilustración 21: Servicio WEb SOAP. Fuente: Los autores.

Para las pruebas se crearon tres servicios en ubicaciones de red diferentes que retornan información referente a los usuarios del sistema.

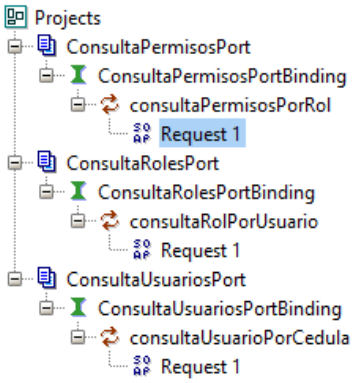


Ilustración 22: Ubicación de servicios. Fuente: Los autores.

Un servicio para consulta de usuarios por cedula:

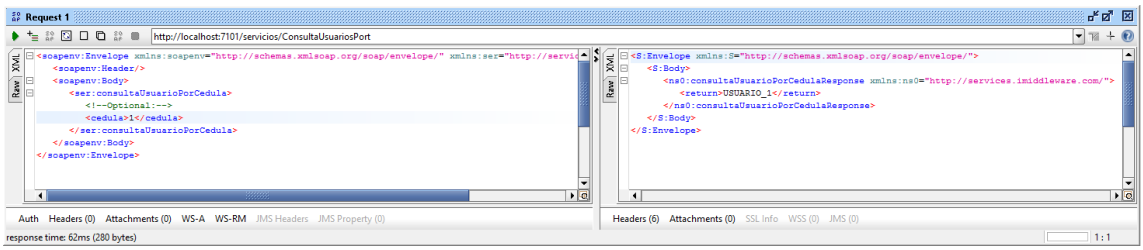


Ilustración 23: Servicio de consulta de usuario por cedula. Fuente: Los autores.

Un servicio para consultar el rol de cada usuario:

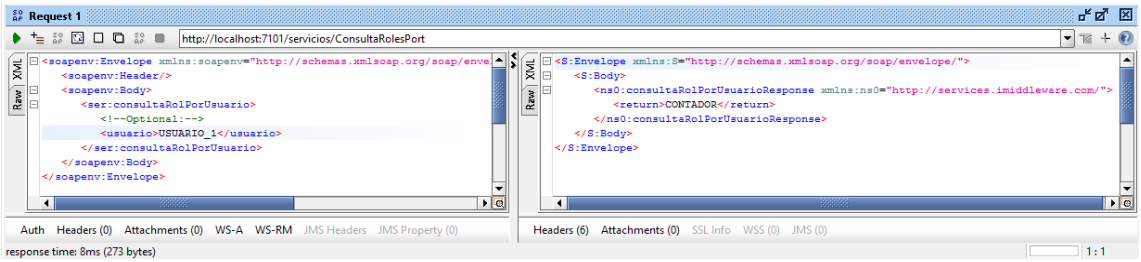


Ilustración 24: Servicio para consultar el rol de cada usuario. Fuente: Los autores.

Y un servicio para consultar los permisos del rol:

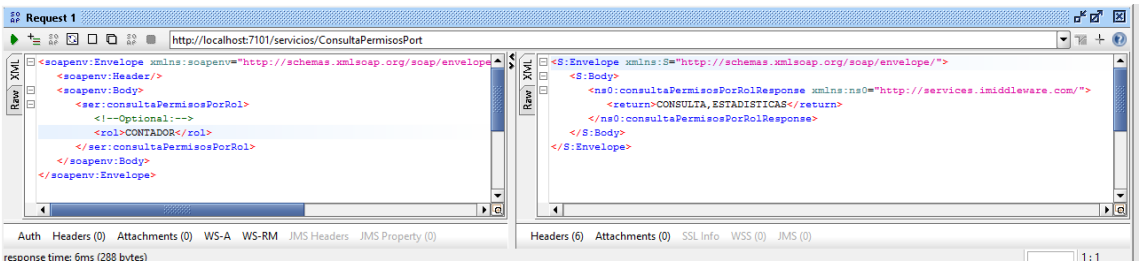


Ilustración 25: Servicio para consultar los permisos del rol. Fuente: Los autores.

Finalmente se utiliza el servicio del middleware que expone la interfaz genérica y se consulta la información completa del usuario sin tener que consumir cada servicio de manera individual.

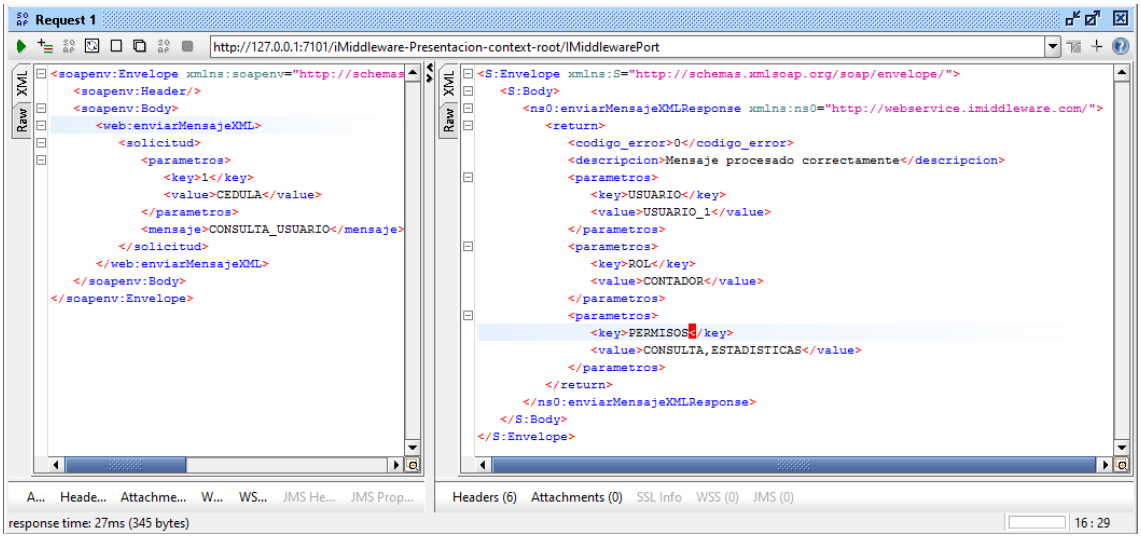


Ilustración 26: Interfaz middleware. Fuente: Los autores.

4.2. DOCUMENTACIÓN DEL SISTEMA

DOCUMENTACIÓN DESARROLLADA PARA NAS LenovoEMC™ px12-400r

CARACTERÍSTICAS DEL EQUIPO.

La NAS tiene las siguientes características:

- Procesador Intel® Core i3 a 3,3Ghz E3-1265Lv2 para un rendimiento mejorado y bajo consumo energético.
- 4GB de RAM DDR3.
- Unidades de disco duro de clase servidor con compatibilidad para unidades SSD.
- Tarjetas de red GbE cuádruples.
- Compatibilidad con 10GbE a través de una tarjeta PCI opcional de 10GbE de doble puerto (se vende porseparado)
- Con certificación para Windows®, VMware® y Citrix®
- Capacidad: Desde 0 TB (sin unidades de disco) hasta una capacidad máxima de 48 TB (12 unidades de disco duro SATA de 4 TB).

De las cuales posee actualmente 9 discos de 3 terabytes para un total de 24 TB.

INGRESO A LA NAS

El ingreso a la NAS se realiza via web por la IP 172.16.2.42 con 2 tipos de autenticación:

1. Ingreso por usuario local el cual tiene como
   Usuario: Udistrital
   Contraseña: UDistrital2016.

2. Ingreso por usuario del dominio.

CONFIGURACIÓN DE STORAGE.

Se tiene un total de 24 TB de lo cual está repartido en 9 discos duros de 3 TB en un RAID 5.

Las demás slots se encuentran libres para la instalación de discos duros normales con interfaz SATA, SAS, compatible con SSD.

Ilustración 27: Administración de discos NAS. Fuente: Los autores.

VOLÚMENES.

Los volúmenes manejados son 2 de los cuales se tiene en la opción de carpetas compartidas las cuales se tienen permisos por el directorio activo o usuarios locales y discos ISCSI en lo cual solo se está manejando discos ISCSI.

Se cuenta con 2 volúmenes de la siguiente manera:

- UDistrital.
- UDistrital2.

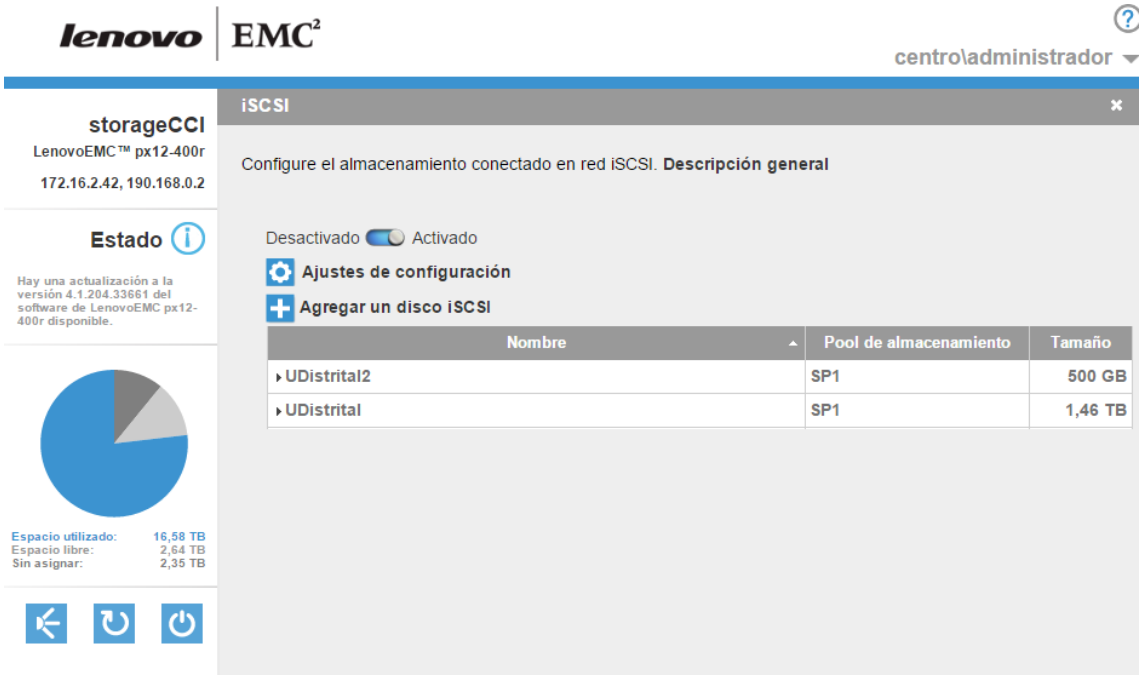


Ilustración 28: Discos ISCSI de NAS. Fuente: Los autores.

CONFIGURACIÓN DE TARJETAS DE RED.

La NAS posee cuantro puertos de red 10/1000 de las cuales se tiene vincula el puerto 1 y 2 en una sola con la IP 172.16.2.42.

Los puertos 3 y 4 se encuentran libres.

Acceso a IQN de los discos ISCSI

Ilustración 29: Configuración tarjetas de red NAS. Fuente: Los autores.

Para realizar la conexión desde cualquier tipo de host hacia los discos creados en el almacenamiento centralizado por red se debe tener una dirección IQN que

se debe colocar en las opciones de conexión de discos ISCSI del dispositivo el cual las direcciones son:

- iqn.2012-07.com.lenovoemc:px12-400r.storageCCI.UDistrital
- iqn.2012-07.com.lenovoemc:px12-400r.storageCCI.UDistrital2

DOCUMENTACION DESARROLLADA PARA EL FIREWALL FORTIGATE 100D

CONFIGURACIÓN DE INTERFACES

Actualmente se encuentran configuradas las siguientes interfaces:

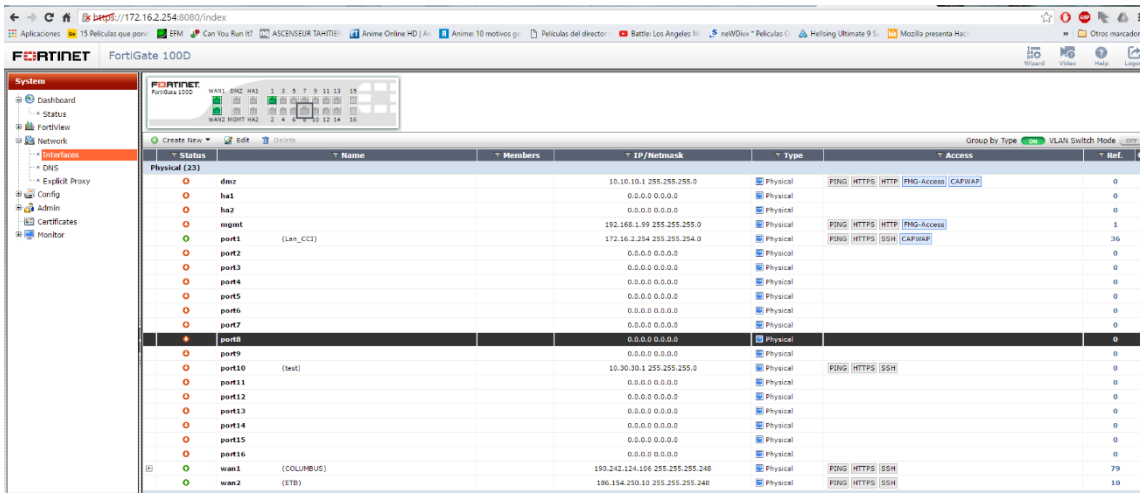


Ilustración 30: Interfaces FortiGate. Fuente: Los autores.

Port1

Se encuentra conectada la red lan (Fisicamente directo a un switch). Con las siguientes configuraciones:

- Segmento de la Red LAN: 172.16.2.0/23.

Wan1

Se encuentra conectado el router del proveedor de servicios de internet en este caso Columbus. Con las siguientes configuraciones:

- IP configurada dada por el proveedor de internet: 190.242.124.106/29

- IP secundarias: 190.242.124.108/29, 190.242.124.107/29, 190.131.194.253/29, 190.131.194.251/29.

Wan2

Se encuentra conectado el router del proveedor de servicios de internet en este caso ETB. Con las siguientes configuraciones:

- IP configurada dada por el proveedor de internet: 186.154.250.10/255.255.255.248

Todas las interfaces tienen actualmente acceso administrativo por ping, https, ssh.

CONFIGURACIÓN DE DNS

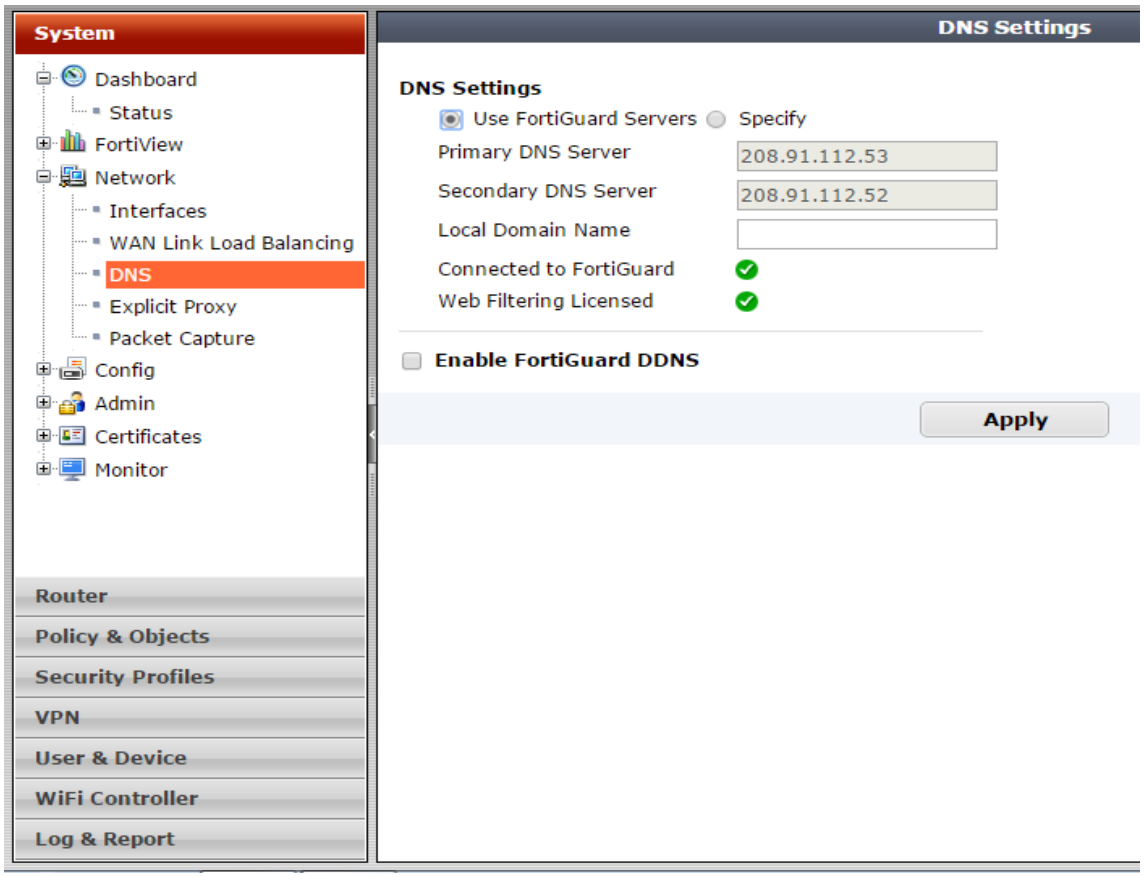


Ilustración 31: DNS FortiGate. Fuente: Los autores.

Los DNS que se encuentran configurados son los DNS del FortiNet para conectarse a los servicios de FortiGuard, técnicamente se pueden utilizar otros DNS que puedan resolver nombres a nivel mundial.

CONFIGURACIÓN DE RUTAS ESTÁTICAS

Actualmente se cuenta con 2 rutas, las cuales se describen a continuación:

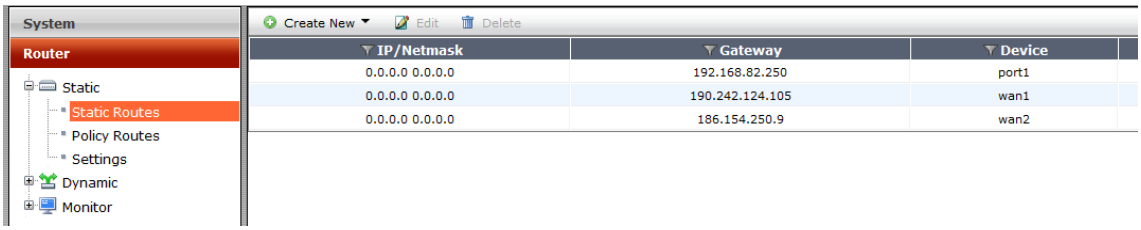


Ilustración 32: Rutas estáticas. Fuente: Los autores.

Ruta Columbus

Es la ruta que se crea hacia el Gateway del ISP Columbus, dentro de ella se encuentra con una distancia administrativa de 10 y prioridad 0. (Imagen dentro de la ruta estática)

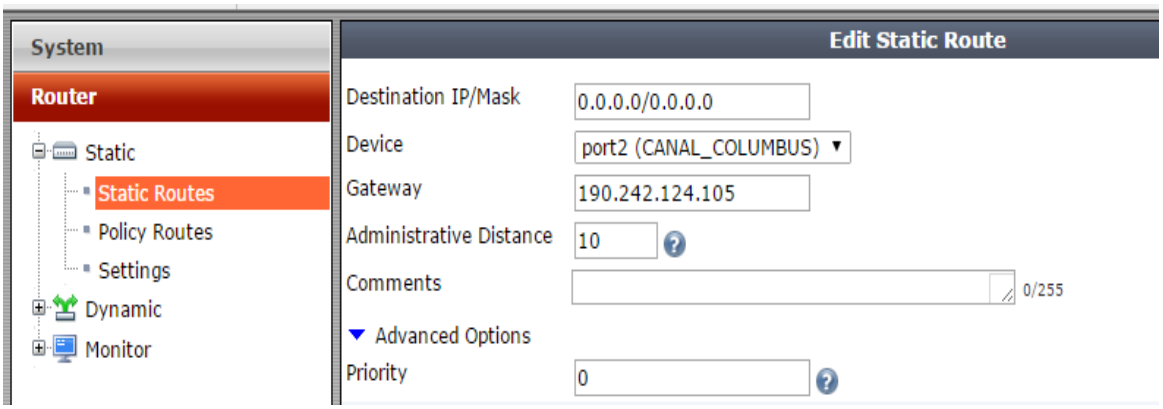
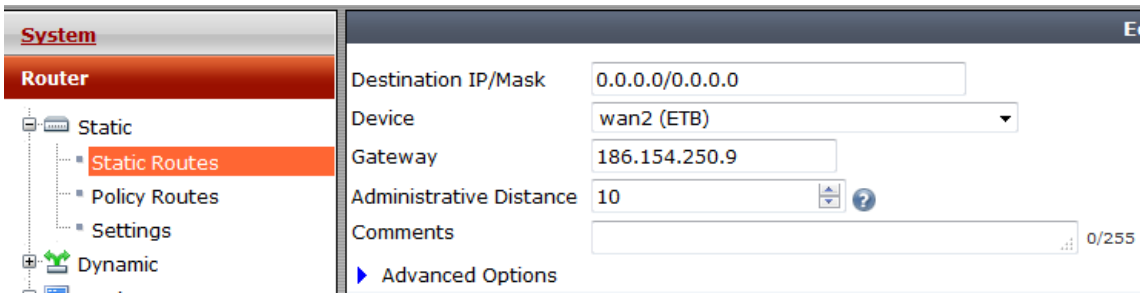


Ilustración 33: Ruta estática Columbus. Fuente: Los autores.

Ruta ETB

Es la ruta que se crea hacia el Gateway del ISP ETB, dentro de ella se encuentra con una distancia administrativa de 10 y prioridad 0. (Imagen dentro de la ruta estática).



POLÍTICAS DE ENRUTAMIENTO

Las políticas que se encuentran actualmente configuradas son:

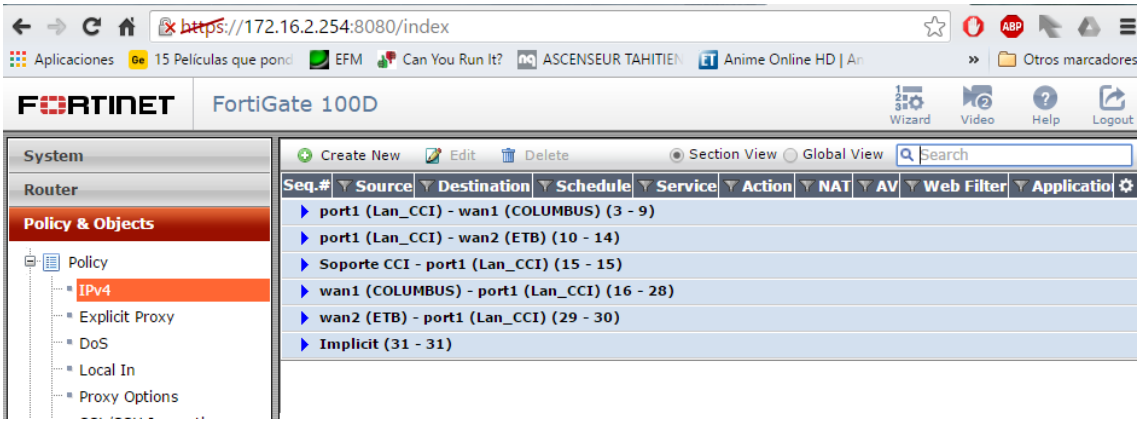


Ilustración 34: Políticas de enrutamiento FortiGate. Fuente: Los autores.

PORT1-WAN1

Esta política es la encargada de conectar la red LAN con Internet, en donde se tienen dos políticas las cuales son:

- Da acceso a todos los dispositivos MAC sin restricciones de navegación hacia internet. (Estas restricciones se verán en la parte de restricciones).
- Da acceso a los todos los dispositivos que se encuentren en el grupo de Navegación Total hacia internet sin restricciones de navegación. (Estas restricciones se verán en la parte de restricciones).
- Da acceso a los todos los dispositivos que se encuentren en el grupo de Navegación Restringida hacia internet con restricciones de navegación. (Estas restricciones se verán en la parte de restricciones).
- Da acceso a los todos los dispositivos que se encuentren en la red hacia internet con restricciones de navegación. (Estas restricciones se verán en la parte de restricciones).

Ilustración 35: Políticas de enrutamiento Columbus FortiGate. Fuente: Los autores.

PORT1-WAN2

Esta política es la encargada de conectar la red LAN con Internet, en donde se tienen dos políticas las cuales son:

- Da acceso a todos los dispositivos MAC sin restricciones de navegación hacia internet. (Estas restricciones se verán en la parte de restricciones).
- Da acceso a los todos los dispositivos que se encuentren en el grupo de Navegación Total hacia internet sin restricciones de navegación. (Estas restricciones se verán en la parte de restricciones).
- Da acceso a los todos los dispositivos que se encuentren en el grupo de Navegación Restringida hacia internet con restricciones de navegación. (Estas restricciones se verán en la parte de restricciones).
- Da acceso a los todos los dispositivos que se encuentren en la red hacia internet con restricciones de navegación. (Estas restricciones se verán en la parte de restricciones).

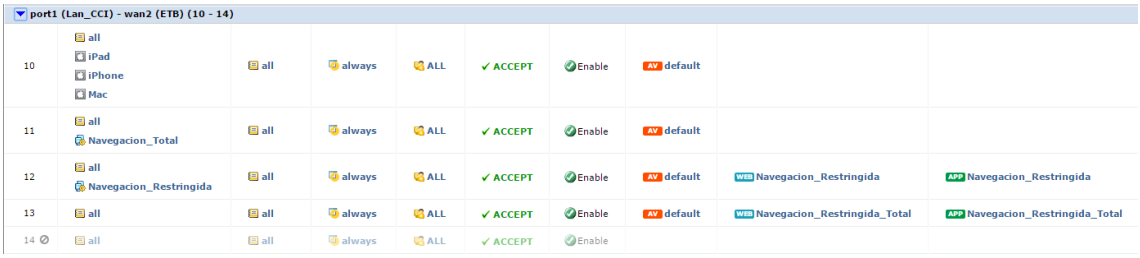


Ilustración 36: Políticas de enrutamiento ETB FortiGate. Fuente: Los autores.

VPN

Se encuentra creada una VPN tipo client to site que se utiliza para realizar soporte remoto.

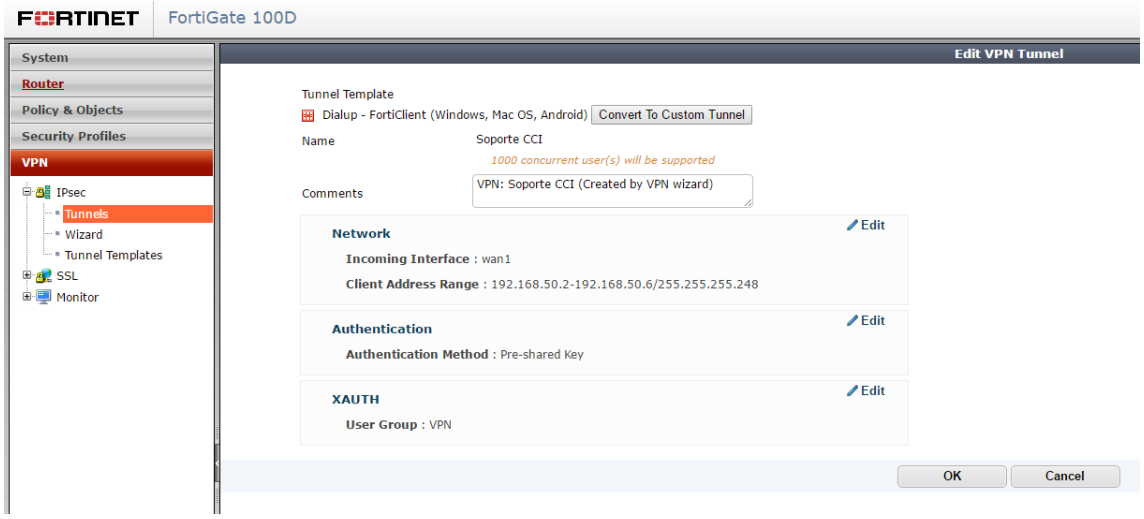


Ilustración 37: VPN Site to Site Fortigate-Azure. Fuente: Los autores.

El orden en el cual se encuentra configurada la VPN es:

- Se crea un usuario llamada soporte.
- Se crea el grupo llamado grupo_vpn.
- Los objetos hay uno llamado vpn_udistrital_range.
- Se crea la VPN.

Se genera automáticamente la política de VPN (Esto solo en los firmware 5.2).

USUARIOS

Actualmente solo se encuentra creado un usuario llamado soporte el cual es utilizado por una VPN de soporte. El otro usuario llamado guest es un usuario por defecto que tiene el sistema.

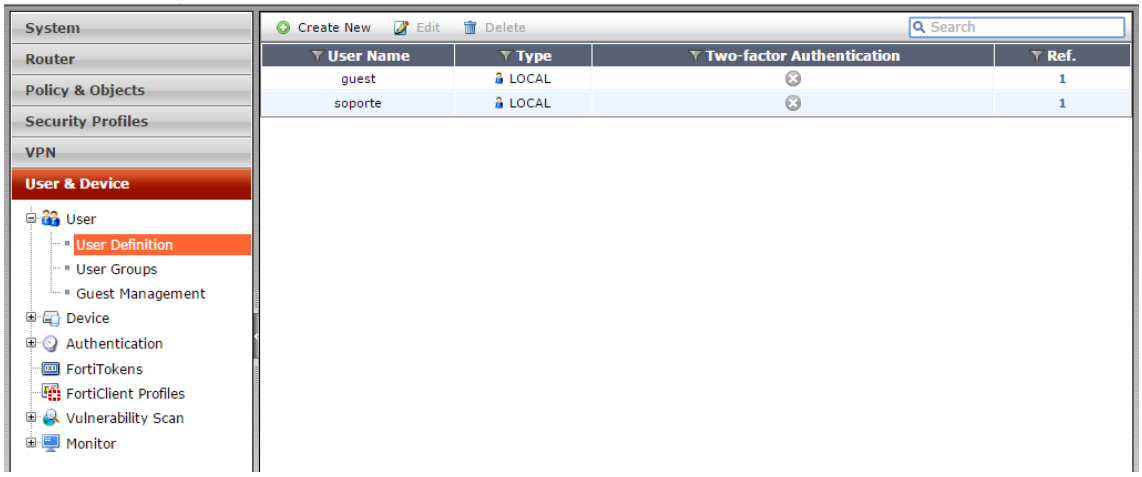


Ilustración 38: Usuarios FortiGate. Fuente: Los autores.

DOCUMENTACIÓN DESARROLLADA PARA EL VMWARE

CARACTERÍSTICAS DEL EQUIPO ANFITRIÓN

El VMWare actualmente está montado en el Blade Center S de la CCI en la cuchilla número 2 y 4 con un procesador Intel XEON E5-2620 de 6 núcleos y un total de 65 GB de memoria RAM cada uno, está conectado al data store del Blade donde tiene almacenada las máquinas virtuales. Las cuchillas poseen las IP 172.16.2.15 y 172.16.2.16 con las siguientes credenciales:

- Usuario: root
- Contraseña: UDistrital2016.

El cual es administrable por vSphare Client, donde la versión del sistema operativo es VMWARE ESXI 6.0.0.

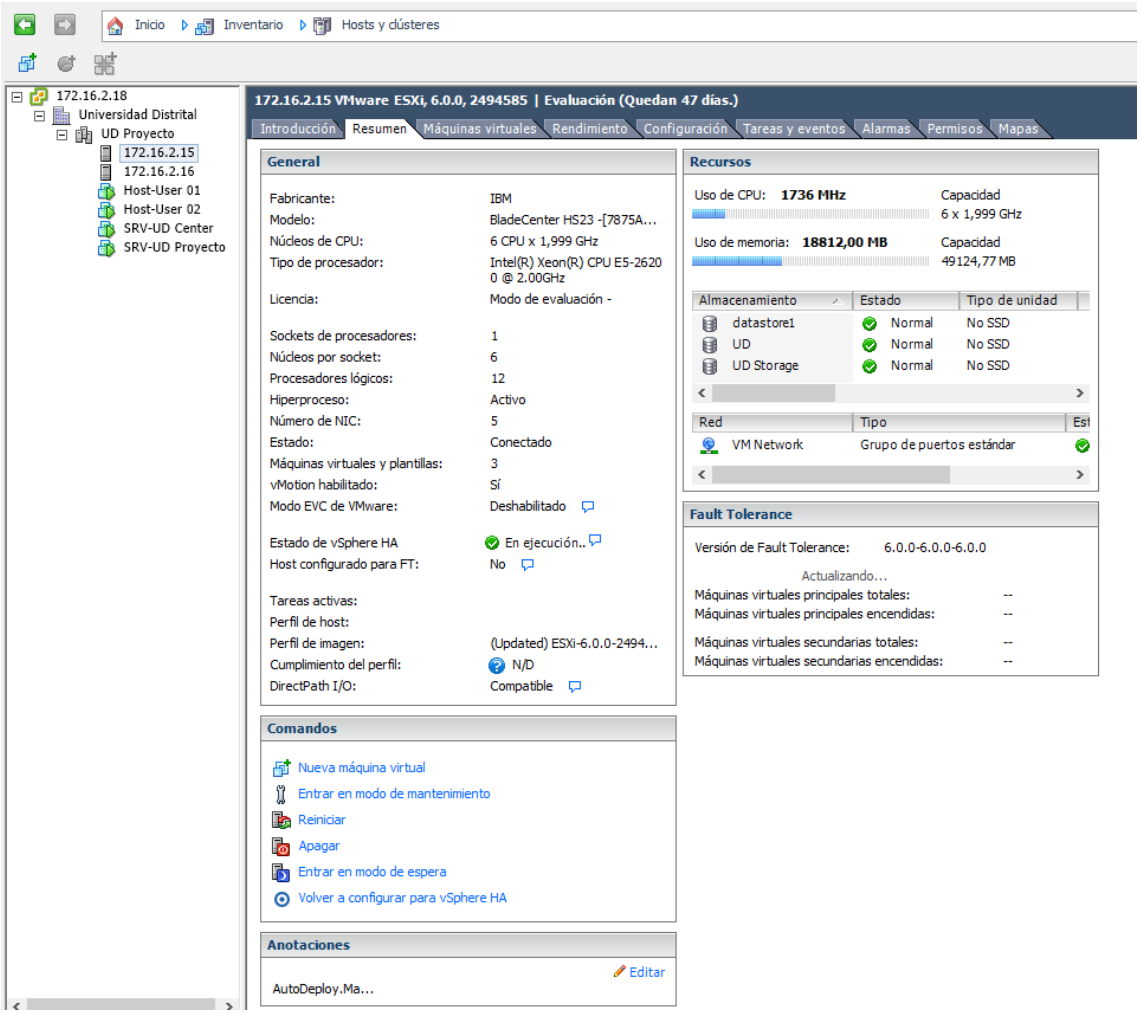


Ilustración 39: Ventana de estado VMWARE. Fuente: Los autores.

CONFIGURACIÓN DE STORAGE

Se menaje 2 volúmenes los cuales están distribuidos de la siguiente manera:

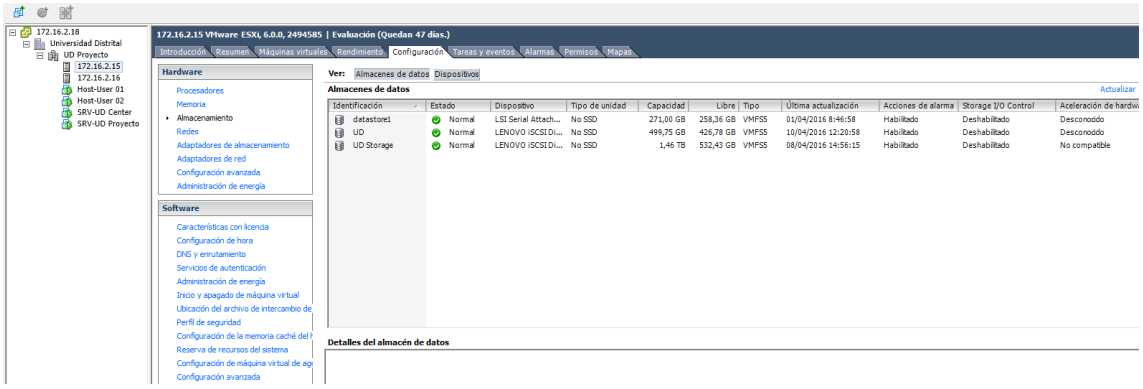


Ilustración 40: Configuración de storage VMWARE. Fuente: Los autores.

- datastore1: Este volumen de 271 GB se encuentran las ISO que por lo general se manejan dentro de la organización como son:

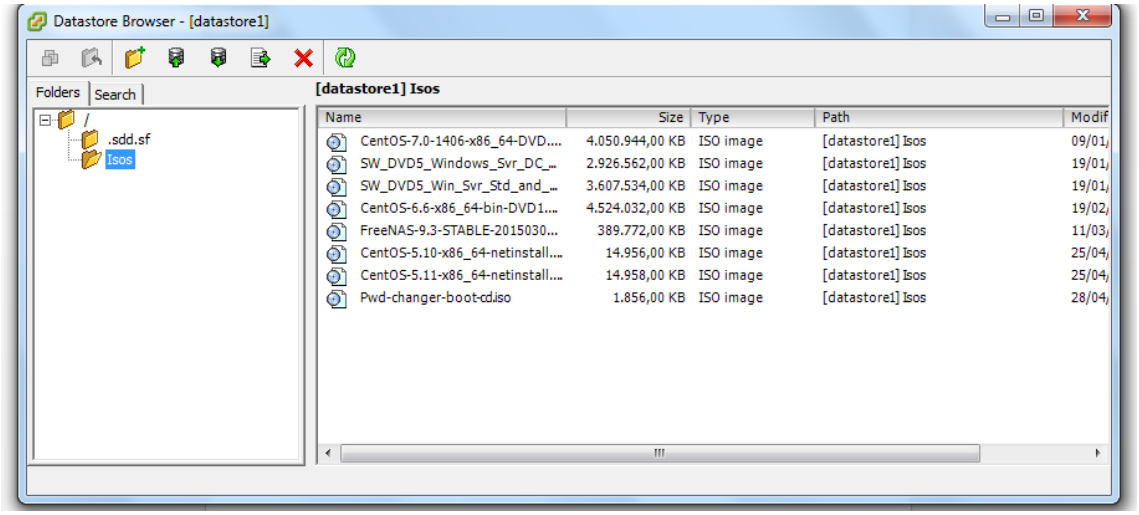


Ilustración 41: Datastore 1 VMWARE. Fuente: Los autores.

- UD: En este volumen de 500 GB se encuentran los archivos de las máquinas virtuales como su configuración y su disco duro virtual el cual está en el storage de a NAS la cual es compartida a los dos servidores de virtualización donde están ubicadas las máquinas de cliente para realizar pruebas de conexión con el servidor central.

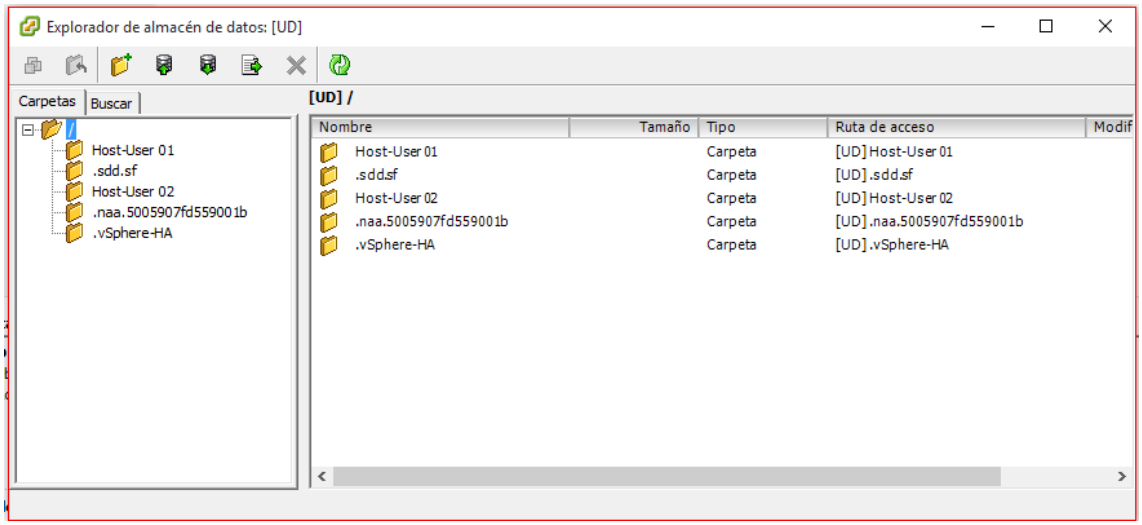


Ilustración 42: Datastore UD VMWARE. Fuente: Los autores.

- UD Storage: En este volumen de 1.5 TB se encuentran los archivos de las máquinas virtuales como su configuración y su disco duro virtual el cual está en el storage de a NAS la cual es compartida a los dos servidores de virtualización donde están ubicadas las máquinas de del servidor principal del aplicativo como del

administrador del cluster para realizar pruebas de conexión con el servidor central.

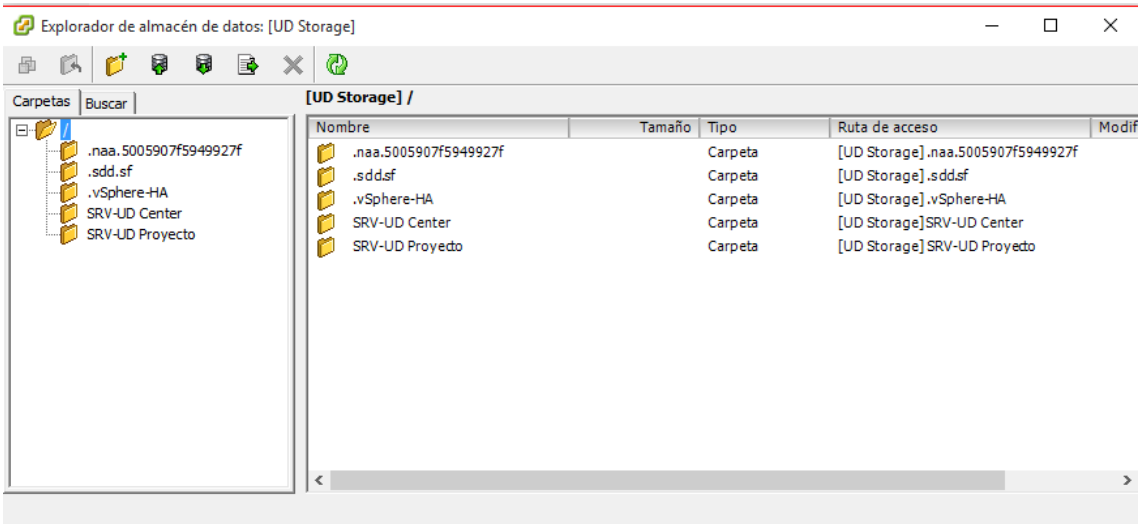


Ilustración 43: Datastore UDStorage VMWARE. Fuente: Los autores.

CONFIGURACIÓN DE TARJETAS DE RED.

El Blade cuenta con 2 tarjetas de red las cuales cada una posee 4 puertos de red para un total de 8 puertos de red, la cuchilla número 2 y 4 tiene conectada 2 de estos puertos que están divididas en 3 las cuales todas salen por la Vlan 23. Las cuales están divididas de la siguiente manera:

- Servidor 172.16.2.15:

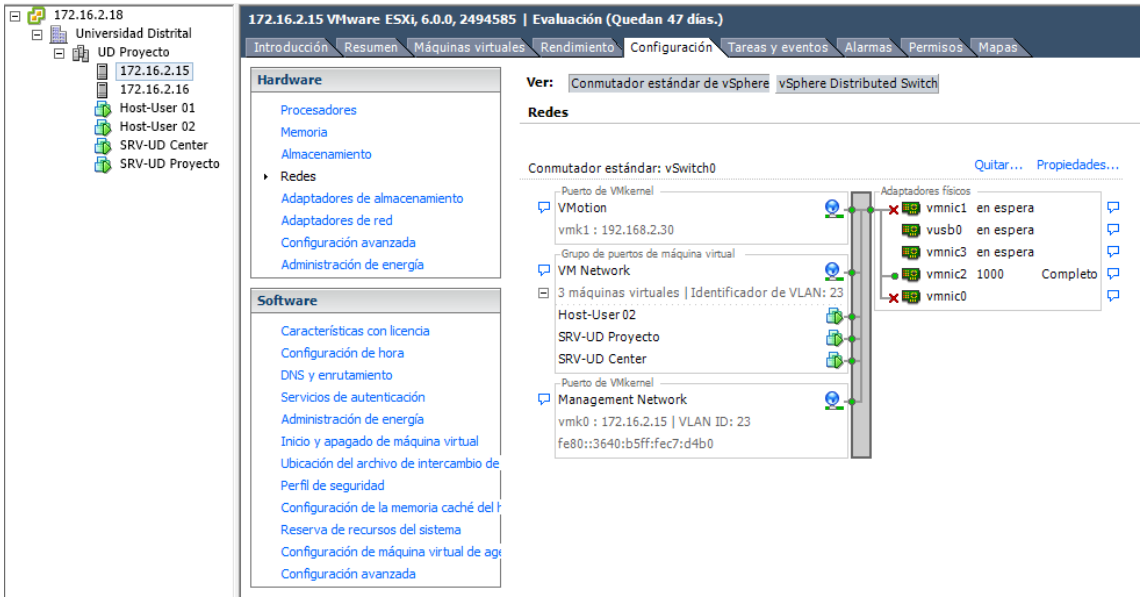


Ilustración 44: Configuración tarjetas de red servidor 1 VMWARE. Fuente: Los autores.

- Servidor 172.16.2.16:

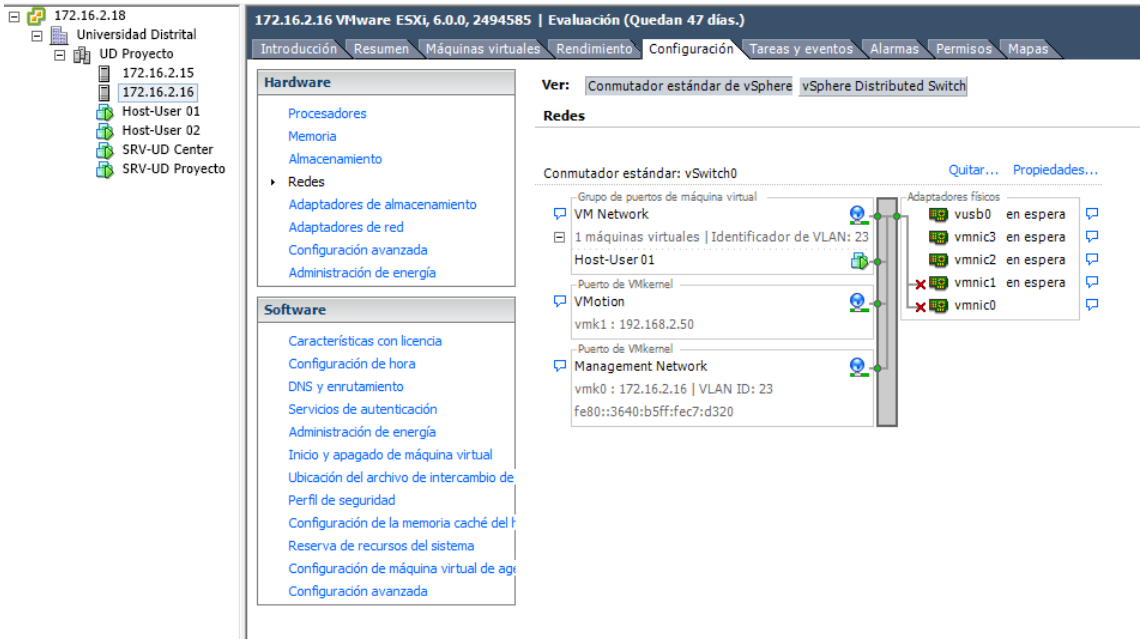


Ilustración 45: Configuración tarjetas de red servidor 2 VMWARE. Fuente: Los autores.

LICENCIAS ADQUIRIDA

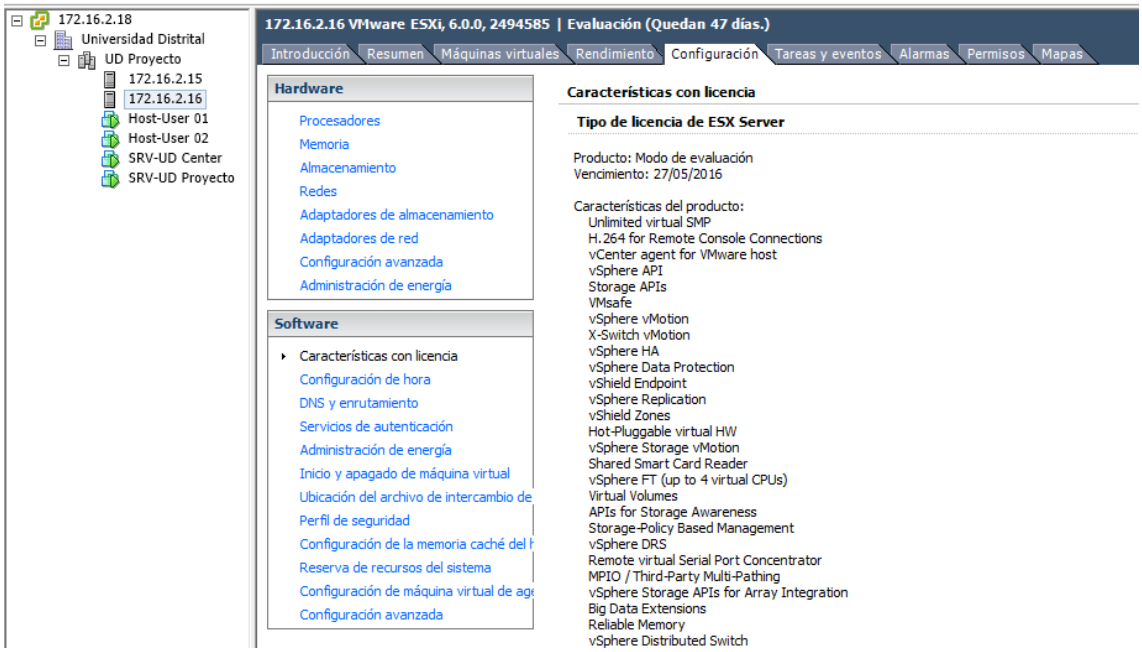


Ilustración 46: Licencia adquirida VMWARE. Fuente: Los autores.

PERFIL DE SEGURIDAD

El perfil de seguridad manejado por el VMWare es el que se configura por defecto.

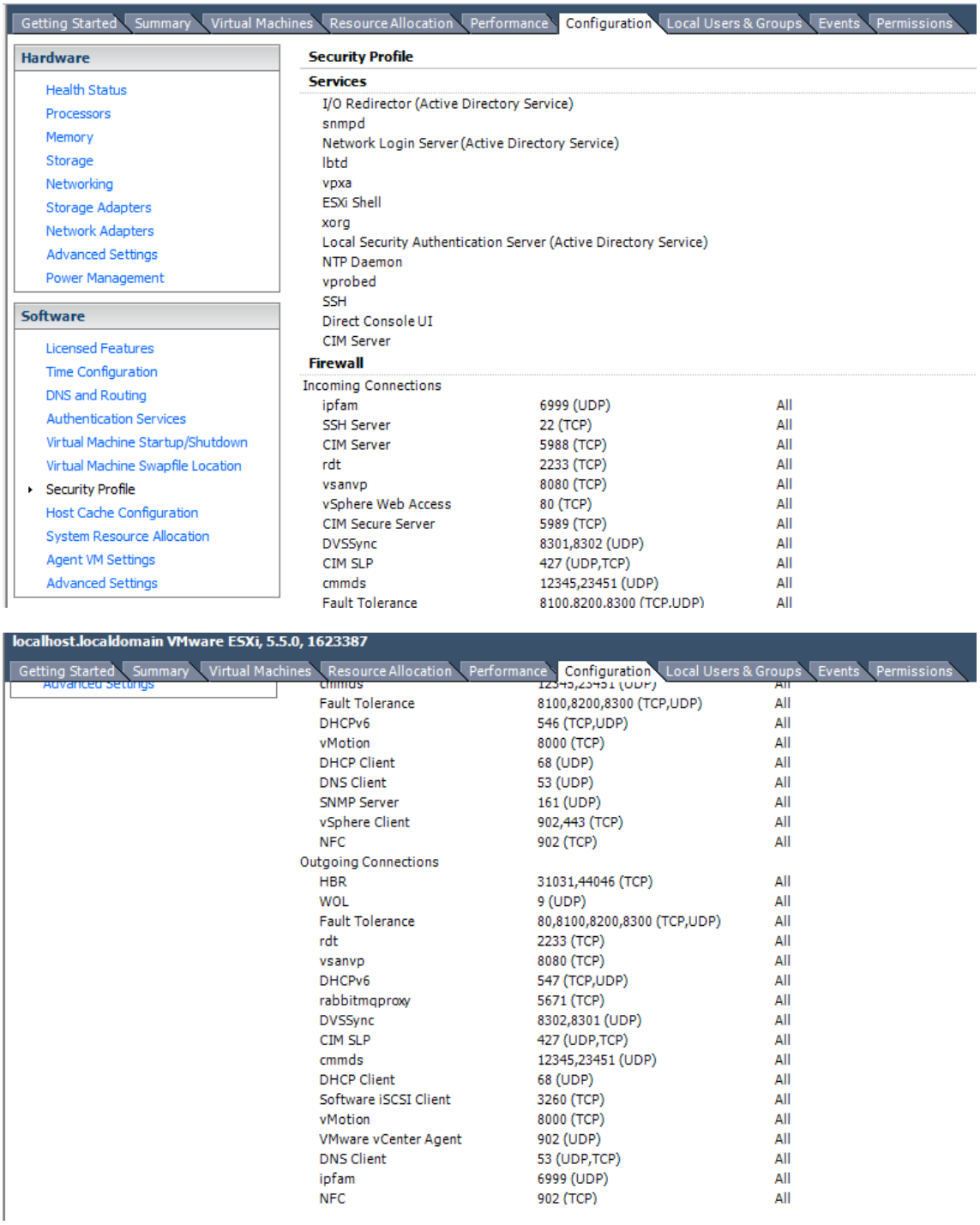


Ilustración 47: Perfil de seguridad VMWARE. Fuente: Los autores.

5. CONCLUSIONES

- En la actualidad existe una gran variedad de opciones tecnológicas que permiten reducir costos y tiempos en implementación, sin embargo, es necesario saber identificar cuál de estas opciones es la más indicada al momento de implementar un proyecto en específico.
- La disponibilidad y la seguridad son dos de los factores más importantes al momento de implementar una solución tecnológica pues estos dos factores reflejan la confiabilidad de la implementación.
- Actualmente la integración de servicios es una de las tareas más comunes en las áreas de desarrollo de una organización y esto se debe básicamente a que al existir un gran número de servicios distribuidos es necesario recurrir a varias fuentes de información.
- La arquitectura orientada a servicios sirve como fundamento teórico para diseñar soluciones en ambientes donde la información no está unificada o no es uniforme.
- En la actualidad uno de los métodos más comunes de intercambio de información es el lenguaje XML.
- El proyecto desarrollado evidencia la importancia que tiene para un ingeniero telemático el hecho de manejar conceptos de integración y de conocer tecnologías de la información que faciliten esta integración.

6. RECOMENDACIONES

- El presente proyecto se hace con base en un caso de estudio, por lo cual se debe tener en cuenta que muchos de los componentes que integran el sistema desarrollado se seleccionaron para adaptarse al ambiente propuesto.
- La integración de mensajería XML que se realizó en el presente proyecto es una integración básica que no incluye aspectos como la codificación de la mensajería.
-

BIBLIOGRAFÍA

- https://msdn.microsoft.com/en-us/library/azure/dn251004.aspx
- https://msdn.microsoft.com/en-us/library/azure/dn251004.aspx
- http://shop.lenovo.com/mx/es/servidores/almacenamiento/lenovoemc/px12-400r/
- https://lenovopress.com/tips0977?cm_mc_uid=48473303780014602574453&cm_mc_sid_50200000=1460257445
- http://www.fortinet.com/products/fortigate/100Series.html
- http://docs.oracle.com/middleware/1221/wls/index.html