

UNIVERSIDAD NACIONAL DE EL SALVADOR
FACTULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA EN SISTEMAS INFORMATICOS



PROTOTIPO DE INFRAESTRUCTURA DE NUBE GEO-DISTRIBUIDA ENFOCADO A
EMPRESAS QUE REQUIERAN SERVICIOS DE PBX

PRESENTADO POR:

ALFARO PÉREZ, CARLOS ASISCLO
MARTÍNEZ VÁSQUEZ, ISAÍ RONALDO
PINEDA DELGADO, JOSÉ GUSTAVO

PARA OPTAR AL TÍTULO DE:

INGENIERO DE SISTEMAS INFORMÁTICOS

CIUDAD UNIVERSITARIA, NOVIEMBRE 2024

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSC. JUAN ROSA QUINTANILLA QUINTANILLA

SECRETARIO GENERAL:

LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO:

ING. LUIS SALVADOR BARRERA MANCÍA

SECRETARIO:

ARQ. RAUL ALEXANDER FABIAM ORELLANA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

DIRECTOR:

ING. CESAR AUGUSTO GONZÁLEZ RODRÍGUEZ

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Trabajo de Graduación previo a la opción al Grado de:
INGENIERO DE SISTEMAS INFORMÁTICOS

Título:

**PROTOTIPO DE INFRAESTRUCTURA DE NUBE GEO-DISTRIBUIDA
ORIENTADO A EMPRESAS QUE REQUIEREN SERVICIO DE PBX**

Presentado por:

ALFARO PÉREZ, CARLOS ASISCLO
MARTÍNEZ VÁSQUEZ, ISAÍ RONALDO
PINEDA DELGADO, JOSÉ GUSTAVO

Trabajo de Graduación Aprobado por:

Docente asesor:

MSC. JULIO DAMIÁN MORALES AYALA

SAN SALVADOR, NOVIEMBRE 2024

Trabajo de Graduación Aprobado por:

Docente asesor:

MSC. JULIO DAMIÁN MORALES AYALA

AGRADECIMIENTOS

Quiero agradecer a Dios primeramente por permitirme llegar a este momento a pesar de las dificultades y aprender a confiar en él, a mis padres (María Galicia, Daniel Alfaro) y hermano (Daniel Alfaro) por el apoyo que me han dado desde que inició mi carrera universitaria y quienes se preocuparon y esforzaron por brindarme lo necesario para llegar a este punto de mi vida.

Agradecer a Pamela Nieto quien ha sido un apoyo incondicional y quien me motivo a seguir hasta el final. De igual manera agradecer a mis familiares y amigos que fueron apoyo para poder ser una mejor persona y llegar a finalizar este proyecto.

Carlos Asisclo Alfaro Pérez

Le agradezco a Dios por guiarme a lo largo de estos años y permitirme alcanzar este logro, a mis padres que con su esfuerzo diario me han ayudado a finalizar este proyecto, a mi hermana por su apoyo moral y a mis mascotas, quienes me han acompañado desde el inicio de la carrera.

Isaí Ronaldo Martínez Vásquez

Quiero dar las gracias a Dios, por darme la oportunidad de crecer y cumplir otro logro en mi vida, a mis padres que siempre han estado presentes brindándome su apoyo incondicional, a mis hermanos que han sido mis amigos más cercanos y todas las personas que de alguna manera contribuyeron a mi desarrollo personal y académico.

José Gustavo Pineda Delgado

TABLA DE CONTENIDO

1	Introducción	10
2	Definición del problema	11
2.1	Identificación de la organización	11
2.2	Contexto del proyecto	11
2.3	Antecedentes	12
2.4	Justificación.....	15
2.5	Alcances	16
3	Marco teórico	17
3.1	Virtualización.....	17
3.2	Hipervisores	17
3.2.1	Tipos de hipervisores	17
3.2.2	Hipervisor tipo 1	17
3.2.3	Hipervisor tipo 2	18
3.3	Cloud computing.....	18
3.3.1	Nube.....	18
3.3.2	Modelos de despliegue de nube	18
3.3.3	Modelo de servicio en la nube	20
3.3.4	Gestión y seguridad de la infraestructura en la nube	26
3.4	Despliegue de nube	30
3.4.1	Servicios esenciales en la nube.....	30
3.5	Clúster	32
3.5.1	Clúster de base de datos.....	32
3.5.2	Clúster de almacenamiento.....	32
4	Marco de la investigación.....	34

4.1	Pregunta de investigación.....	34
4.2	Objetivos	34
4.2.1	Objetivo general.....	34
4.2.2	Objetivos específicos	34
5	Metodología de la investigación	36
5.1	Enfoque de la investigación	36
5.1.1	Enfoque cuantitativo	36
5.1.2	Enfoque cualitativo	36
5.2	Población y muestreo	37
5.3	Instrumentos y técnicas de recolección de datos.....	37
5.3.1	Encuesta por muestreo	37
5.3.2	Entrevista estructurada.....	38
5.4	Análisis de los resultados	39
5.4.1	Análisis de los datos cuantitativos	39
5.4.2	Análisis de los datos cualitativos	43
5.5	Conclusión de los resultados y de la investigación	46
6	Prototipo.....	48
6.1	Requerimientos.....	48
6.2	Arquitectura.....	49
6.3	Configuración.....	50
6.3.1	Nodo controller	50
6.3.2	Nodo identidad.....	51
6.3.3	Clúster de base de datos	51
6.3.4	Clúster de almacenamiento	52
6.3.5	Nodos controller por región.....	52

6.3.6	Nodos compute por región.....	53
6.4	Topología de red.....	54
7	Caso de estudio	56
8	Factibilidad	58
8.1	Factibilidad técnica	58
8.2	Factibilidad económica	60
9	Conclusiones	67
10	Recomendaciones	69
11	Limitaciones.....	70
12	Referencias bibliográficas.....	71
13	Anexos	76

INDICE DE FIGURAS

Ilustración 1 Arquitectura de la infraestructura de nube geo-distribuida. Autoría Propia.....	49
Ilustración 2 Topología de red de la infraestructura de nube geo-distribuida. Autoría Propia.....	54

INDICE DE TABLAS

Tabla 1: Requerimientos para nodo controller.....	50
Tabla 2: Requerimientos para nodo Identidad.....	51
Tabla 3: Requerimientos para clúster de base de datos.....	51
Tabla 4: Requerimientos para clúster de almacenamiento.....	52
Tabla 5: Requerimientos para nodo controller por región.....	52
Tabla 6: Requerimientos para nodo compute.....	53
Tabla 7 Cuadro comparativo de los principales componentes de proveedores de nube.....	58
Tabla 8 Resultados de pruebas de la capacidad operativa del servidor de PBX.....	60
Tabla 9 Requerimientos necesarios para la implementación de la infraestructura.....	61
Tabla 10 Servicios equivalentes Google Cloud.....	62
Tabla 11 Servicios equivalentes en Azure.....	62
Tabla 12: Precios anuales de los servicios requeridos.....	63
Tabla 13 Precios del hardware requerido para la infraestructura.....	63
Tabla 14 Inversión requerida para la infraestructura de nube geo-distribuida (primer año).....	64
Tabla 15 Costo de mantenimiento y operación de la infraestructura de nube geo-distribuida anual.....	64
Tabla 16 Comparación de precios de los proveedores y la compra del hardware para el primer año.....	65
Tabla 17 Comparación de precios para 1, 3 y años.....	65

1 INTRODUCCIÓN

En la actualidad, existen muchas empresas que requieren emplear un servicio de PBX o ya hacen uso de uno, pero puede no ser óptimo. Una solución basada en la nube es una respuesta viable para abordar estas demandas, ofreciendo flexibilidad y redundancia. Sin embargo, la implementación de una infraestructura de nube geo-distribuida eficiente requiere un diseño cuidadoso y la adopción de tecnologías adecuadas.

El presente trabajo de investigación tiene como objetivo diseñar y configurar una infraestructura de nube geo-distribuida, que permita el alojamiento de un servicio de PBX. En primer lugar, se propone un diseño y construcción de una infraestructura utilizando herramientas open source, las cuales fueron seleccionadas por ser una solución robusta, económicamente viable y escalable.

Para permitir la gestión y el monitoreo de los servicios desplegados se proveerá de una interfaz web, esto permitirá a los administradores una supervisión eficaz y en tiempo real. Para garantizar una gestión segura y eficiente de los datos, se configurará una plataforma de base de datos, que soporte las necesidades de almacenamiento. Finalmente, se implementará un servicio de identificación y autenticación para asegurar que el acceso a la infraestructura esté restringido a usuarios autorizados, protegiendo así la integridad y confidencialidad de los datos.

Este estudio no solo busca contribuir al conocimiento teórico sobre el diseño y construcción de una infraestructura de nube geo-distribuida, sino también ofrecen una solución práctica y aplicable.

2 DEFINICIÓN DEL PROBLEMA

2.1 Identificación de la organización

Esta investigación se centra en empresas que utilizan o requieren servicios de PBX, con un enfoque particular en aquellas del sector de call centers a nivel nacional. Estas empresas, cuya actividad principal se basa en la gestión y atención de comunicaciones telefónicas, dependen de una infraestructura para gestionar sus servicios de llamadas. Se analizan las necesidades específicas de estas organizaciones con el fin de desarrollar una solución que mejore la gestión de sus sistemas de comunicación.

2.2 Contexto del proyecto

Los centros de atención telefónica que operan en múltiples regiones y enfrentan una alta demanda de servicios necesitan una infraestructura robusta y eficiente. Esta debe garantizar bajas latencias y alta disponibilidad, evitando interrupciones con las comunicaciones de los clientes. Tales características son fundamentales para mantener la confianza de los clientes y asegurar la continuidad de las operaciones empresariales. Así mismo, es crucial garantizar la persistencia de sesiones, permitiendo a los usuarios utilizar los servicios de forma continua y sin interrupciones, sin importar la región en la que se encuentren.

Para lograr una gestión eficiente, es esencial disponer de una interfaz web centralizada que administre todas las regiones y sus respectivas operaciones de manera ágil. Es necesario ofrecer una respuesta eficiente, por lo que la interfaz debe adaptarse a los cambios en las demandas.

Como parte de los requisitos de estas empresas, la base de datos es muy importante, por lo que se debe contar con una infraestructura que permita un escalado eficiente y una alta disponibilidad, manteniendo la fiabilidad de los servicios.

2.3 Antecedentes

En 1997 surge la primera central virtual a través de una nueva tecnología (VoIP) que facilitó la transmisión de multimedia a través de internet, estos sistemas eliminaron la necesidad de contar con elementos físicos y facilitaron la escalabilidad sin grandes inversiones. (Amorín, 2016)

Durante la década de los 60, el empresario Henry Ford hizo uso del teléfono, el cual era una herramienta muy importante, para poder acercarse a nuevos mercados y así conseguir más clientes. Puso en marcha una iniciativa donde los vendedores de la empresa tendrían que usar sus teléfonos y contactar a más de 20,000 personas para poder aumentar así las entrevistas con clientes potenciales. (Silva, 2023)

A medida que las empresas crecieron y se globalizaban, las necesidades de comunicación aumentaban, al punto de requerir infraestructuras más robustas y adaptables, infraestructuras capaces de reducir los tiempos de respuesta al mínimo, asegurar una alta disponibilidad de los servicios y garantizar la seguridad de los datos sin importar las barreras geográficas.

Entre 1970 y 1980 se adoptó el termino de “Call Center” basando en la idea de Henry Ford, los cuales eran centros de contacto que generaron un impacto inmediato en cuanto a reducción de costos y aumento de la productividad. (Silva, 2023)

En una industria cuyo principal servicio son las comunicaciones en tiempo real, la nube se ha convertido en un pilar fundamental para satisfacer las demandas crecientes de las empresas de atención telefónica. Esta evolución hacia infraestructuras de nube con múltiples regiones ha sido crucial permitiendo a las empresas distribuir eficientemente sus recursos de comunicación y datos en ubicaciones estratégicas globalmente dispersas.

El “Cloud Computing” se remonta a la década de los 60, expertos atribuyen este concepto a John McCarthy, a quien también se le adjudica el concepto de “inteligencia artificial.

(Adaptixnetworks, s.f.)

Otros atribuyen este concepto a Joseph Carl Robnett Licklider, quien se dice que pretendía que todo el mundo pudiese estar interconectado para acceder a los programas y datos desde cualquier lugar dando el concepto de “red de ordenadores intergalácticas” en 1962. (Cisga, s.f.)

Douglas Parkhill también forma parte al explorar muchas de las características del Cloud Computing con el libro “Desafío de la utilidad de la computadora”.

En 1999, la empresa Salesforce abre paso al modelo de negocio “Software-as-a-Service” para el cual, se desarrollaron aplicaciones empresariales sobre páginas web, con licencia por usuario, el cual eliminaba por completo el modelo tradicional de software empresarial “on-premise” (grandes inversiones en hardware, implementaciones, mantenimiento y actualizaciones). (Salesforce, s.f.)

Es desde este hito en adelante, donde grandes empresas posan su mirada y fijan una meta, el Cloud Computing.

La siguiente en unirse e implementar este concepto fue Amazon en 2004, con **Amazon Web Services** (Services, s.f.). En 2006 Google logra dar a conocer el Cloud Computing al público con sus servicios **Google Docs**. En este mismo año se introduce **EC2** por Amazon bajo demanda de AWS implementando lanzamientos de tantos servidores virtuales como se necesite, configuración de la seguridad y las redes, administración del almacenamiento, entre muchas más funciones, lo cual permite reducir los costos de hardware, desarrollar e implementar aplicaciones con mayor rapidez (Adaptixnetworks, s.f.). En 2007 surge una colaboración entre empresas de

tecnología y una serie de universidades de Estados Unidos, en 2008 aparece “**Eucalyptus**” el cual se convirtió en la primera plataforma de código abierto compatible para el despliegue de nubes privadas, (Adaptixnetworks, s.f.) al igual que “**OpenNebula**”, siendo el primer software de código abierto para la implementación de nubes privadas e híbridas. En 2009 Microsoft se une al barco del Cloud Computing con **Microsoft Azure** y en 2010 surgen servicios de múltiples capas de servicio. En 2011, Apple lanza **iCloud**, consolidándolo como su sistema de almacenamiento en la nube para documentos, música, imágenes, aplicaciones, calendarios, etc. (Adaptixnetworks, s.f.)

Con el aumento de tecnologías y la demanda de herramientas y aplicaciones que faciliten la ejecución de las tareas laborales de manera remota, las organizaciones exploran diversas alternativas informáticas, incluyendo la computación en la nube, la cual ofrece flexibilidades que en los sistemas locales no pueden ofrecer, con la opción de adaptar los requerimientos según necesidades de cada empresa, sin embargo, la ubicación geográfica de los usuarios es una de las dificultades a vencer. Es ahí, cuando concepto de nube geo distribuida comienza a tener auge.

La nube geo distribuida implica la dispersión de servicios en la nube pública en múltiples ubicaciones físicas. Es un servicio de infraestructura tecnológica que se comparte entre diversas organizaciones o empresas, las cuales mantienen objetivos similares, intereses a fines o necesidades específicas. Se trata de una nube implementada y gestionada por las mismas entidades, ofreciendo como principal ventaja, el acceso constante a la información entre sí constantemente, sin importar en la región del mundo en la que se encuentren los usuarios. (Networks, 2021) La implementación de esta ha sido relativamente reciente e impulsada por empresas de tecnologías líderes en la industria, siendo pioneras en la innovación de este campo satisfaciendo requerimientos cambiantes de sus clientes:

- Google Cloud Platform (GCP) a finales de los 2000, quienes implementaron su red global de centros de datos para ofrecer sus servicios de nube geo distribuida el cual permite a los usuarios el despliegue de aplicaciones y servicios mejorando la latencia y disponibilidad.
- Amazon Web Service (AWS) quienes a finales de los 2000 permitieron a los usuarios implementar aplicaciones y servicios de nube geo distribuida, cumpliendo con los requisitos de redundancia y rendimiento.
- Microsoft Azure, que desde el 2010 ha permitido implementar los servicios de nube geo distribuida proporcionando herramientas de gestión unificada de recursos.

2.4 Justificación

La implementación de una infraestructura en la nube geo-distribuida para empresas que utilizan servicios de PBX, tiene la capacidad de mejorar significativamente la calidad y disponibilidad del servicio. Este enfoque permite distribuir los servidores en múltiples ubicaciones estratégicas, lo que garantiza una disponibilidad continua, incluso frente a fallas locales, y una respuesta más rápida para los usuarios, mejorando así su experiencia.

Además, las empresas que requieren este tipo de servicio suelen manejar un alto volumen de comunicaciones, lo que implica la necesidad de una solución escalable que pueda adaptarse al crecimiento y a la demanda. La naturaleza escalable de la nube geo-distribuida no solo permite expandir la capacidad del servicio, sino que también optimiza el uso de los recursos, maximizando la eficiencia y minimizando los costos. Por lo que la adopción de esta infraestructura es clave para mejorar el rendimiento y la sostenibilidad de las empresas en el sector de las comunicaciones.

2.5 Alcances

- Diseño y construcción de una infraestructura de nube geo-distribuida, enfocada a empresas que requieren servicios de PBX.
- Configuración de una plataforma de almacenamiento, que proporcione servicios de almacenamiento a la infraestructura de nube geo-distribuida.
- Configuración de una plataforma de base de datos, que proporcione servicios de gestión de datos a la infraestructura de nube geo-distribuida.
- Configuración de un servicio de identificación, para restringir el acceso a los datos de la infraestructura de nube geo-distribuida, de las empresas que requieren servicios de PBX.
- Implementación de una interfaz web, que facilite la gestión de los servicios brindados en la nube geo-distribuida, a las empresas que utilizan los servicios de PBX.
- Configuración de un servicio de PBX, que permita a la organización comunicarse entre las diferentes sucursales que la componen.

3 MARCO TEÓRICO

3.1 Virtualización

La virtualización es un tipo de tecnología que permite a los usuarios crear versiones virtuales de servidores, incluyendo almacenamiento, redes y otras máquinas físicas. El software virtual limita las funciones del hardware físico para ejecutar varias máquinas virtuales a la vez en una única máquina física. (AWS, s.f.)

3.2 Hipervisores

Los hipervisores son programas que crean y ejecutan máquinas virtuales (VMM), también se les llama supervisores de máquinas virtuales. Estos separan el sistema operativo y los recursos de las máquinas virtuales para poder crearlas y gestionarlas. El hardware físico que funciona como hipervisor se denomina "host", y las máquinas virtuales que utilizan estos recursos se llaman "guests". El hipervisor trata a los recursos (la CPU, la memoria y el almacenamiento, entre otros) como un conjunto de elementos que puede redistribuirse con facilidad entre los guests actuales o las máquinas virtuales nuevas. (Red Hat, 2023)

3.2.1 Tipos de hipervisores

3.2.2 Hipervisor tipo 1

También conocido como hipervisor original o dedicado (bare metal), se ejecuta directamente en el hardware del host para gestionar los sistemas operativos guest. Este sistema operativo host se encarga de administrar los recursos de la máquina virtual directamente en el hardware. Usualmente se utiliza este tipo de hipervisor en entornos empresariales o servidores en los centros de datos. Algunos ejemplos de hipervisores de tipo 1 son KVM, Microsoft Hyper-V y VMware vSphere. (Red Hat, 2023)

3.2.3 Hipervisor tipo 2

También conocido como hipervisor alojado, se ejecuta en un sistema operativo convencional como una capa de software o aplicación. Su funcionamiento se basa en extraer los sistemas operativos de los usuarios del servidor principal. Los recursos de la máquina virtual son programados en un sistema operativo host y luego se ejecutan en el hardware. Este tipo de hipervisor es ideal para los usuarios individuales que desean ejecutar varios sistemas operativos en una computadora personal. Algunos ejemplos de hipervisores de tipo 2 son VMware Workstation y Oracle VirtualBox. (Red Hat, 2023)

3.3 Cloud computing

3.3.1 Nube

El acceso remoto a softwares, almacenamiento de archivos y procesamiento de datos a través de Internet es una alternativa a la ejecución en una computadora, gracias a la tecnología que lo permite. En el modelo de nube, no hay necesidad de instalar aplicaciones localmente en computadoras. La computación en la nube brinda a las personas y compañías la posibilidad de acceder a recursos de computación compartidos, seguros, mantenidos de forma adecuada, fáciles de usar y disponibles según sea necesario. (Sales Force, s.f.)

3.3.2 Modelos de despliegue de nube

Se han desarrollado modelos de implementación comúnmente conocidos como tipos de cloud o tipos de computación en la nube. Inicialmente, estos modelos se separaban en dos dimensiones, nubes privadas y nubes públicas. Sin embargo, a partir de estos, han surgido otros tipos de nube que no son más que la combinación de uno o los dos modelos anteriores. (Flores, 2021)

3.3.2.1 Nube Pública

En este modelo se ofrecen recursos (potencia de cómputo, almacenamiento, bases de datos, plataforma para desarrollo, aplicaciones, etc.) bajo demanda y de forma inmediata a través de Internet. El proveedor es dueño de los recursos físicos y tecnológicos, como el hardware y el software, y se encarga de su mantenimiento y gestión. Este modelo permite a los desarrolladores, administradores de sistemas y empresas enfocarse en lo más importante para el negocio, sin preocuparse por la planificación de capacidad informática, la adquisición o administración de hardware, y otras tareas del departamento de TI. Ejemplos de nube pública son AWS, Microsoft Azure y Google Cloud Platform. (Flores, 2021)

3.3.2.2 Nube Privada

En este modelo el cliente no confía la seguridad al proveedor. Las organizaciones consideran que deben tener el control total de su entorno con su equipo de trabajo y su propia infraestructura. La cual está compuesta por recursos informáticos utilizados únicamente por una institución, la infraestructura siempre se mantiene en una red privada, y el hardware y software es dedicado para la propia organización, una nube privada no es lo mismo que una infraestructura local con virtualización tradicional, para ello debe de cumplir con ciertas características de Cloud Computing. OpenStack, OpenNebula y CloudStack son alternativas de código abierto para implementar este modelo. (Flores, 2021)

3.3.2.3 Nube híbrida

Este modelo es una composición de dos tipos diferentes (nube pública y nube privada), que se perciben como entidades separadas, pero a la vez, están conectadas a través de una tecnología común que hace más fácil la comunicación, la transferencia de datos y las aplicaciones. Lo que se pretende es combinar los dos modelos de implementación y obtener lo

mejor de ambos. Algunas compañías han logrado implementar una nube privada de forma eficiente y han alcanzado un alto nivel de madurez, pero ahora necesitan obtener más recursos de los que pueden generar internamente, por tanto, necesitan de un tercero (proveedor de nube pública) para no perder eficiencia, es entonces cuando se realizan la integración, obteniendo así, un modelo híbrido. (Flores, 2021)

3.3.2.4 Nube geo-distribuida

En este modelo, toda la pila tecnológica de un proveedor de nube pública se distribuye a diferentes ubicaciones, donde quiera que el cliente la necesite. Esto puede incluir ubicaciones locales en el propio centro de datos o nube privada del cliente, o en centros de datos o centros de terceros en todo el mundo, todo ello gestionado desde un plano de control central. Ofrecer más control sobre dónde se almacenan los datos para cumplir con las normas. (Akamai, s.f.)

3.3.3 Modelo de servicio en la nube

La diversidad de servicios en la computación en la nube ha generado desafíos en su clasificación. Para abordar esta complejidad, varios autores han desarrollado taxonomías que buscan agrupar estos servicios de manera sistemática. Entre estas taxonomías, algunas son ampliamente reconocidas, mientras que otras crean categorías distintas basadas en características específicas de los servicios

Un ejemplo destacado es la taxonomía propuesta por el NIST (Mell & Grance, 2011), que se ha convertido en un estándar ampliamente aceptado. Esta clasificación considera diversos enfoques, como modelos, proveedores y nichos de mercado, para crear un marco de referencia uniforme. Dentro de este marco, el NIST presenta el modelo SPI, que clasifica los servicios en tres categorías principales: SaaS, PaaS e IaaS. (Merizalde Almeida, 2017)

3.3.3.1 Infraestructura como servicio (IaaS – Infrastructure as a Service)

Infraestructura como Servicio (IaaS) es un modelo de computación en la nube que proporciona a los usuarios acceso a recursos informáticos esenciales como almacenamiento, procesamiento, redes, y otros componentes necesarios para ejecutar software, incluyendo sistemas operativos y aplicaciones. A través de IaaS, las empresas pueden aprovisionar y gestionar máquinas virtuales en tiempo real, lo que permite una escalabilidad y flexibilidad significativamente mayor en comparación con la implementación tradicional de infraestructura física. Aunque los usuarios no tienen control directo sobre la infraestructura subyacente de la nube, si tienen control total sobre los sistemas operativos y las aplicaciones que instalan y ejecutan. (García Orozco, 2020)

Este modelo es particularmente útil en entornos de nube pública, donde IaaS puede mejorar el rendimiento y ofrecer soluciones que incluyen el uso temporal de software especializado sin necesidad de instalaciones locales, reduciendo así los costos operativos. Una vez finalizado el período de prueba o uso gratuito de estos servicios, las empresas deben pagar según el consumo real de los recursos de infraestructura, lo que permite una gestión de costos más eficiente y ajustada a las necesidades específicas. (García Orozco, 2020)

IaaS se considera un modelo completo en el ámbito de la computación en la nube, pues integra todos los recursos necesarios para su operación. Además, en combinación de algunos modelos como el Software como Servicio (SaaS) y la Plataforma como Servicio (PaaS), se convierte en el fundamento sobre el que se pueden gestionar las aplicaciones y los sistemas. (García Orozco, 2020)

3.3.3.1.1 Ejemplos de proveedores de IaaS

- **Amazon Web Services (AWS):** Servicios: Amazon EC2 (instancias de servidores virtuales), Amazon S3 (almacenamiento de objetos), Amazon RDS (base de datos relacional), AWS Lambda (computación sin servidor). (AWS, s.f.)
- **Microsoft Azure:** Servicios: Azure Virtual Machines (instancias de servidores virtuales), Azure Blob Storage (almacenamiento de objetos), Azure SQL Database (base de datos relacional), Azure Functions (computación sin servidor). (Productos de Azure, s.f.)
- **Google Cloud a (GCP):** Servicios: Google Compute Engine (instancias de servidores virtuales), Google Cloud Storage (almacenamiento de objetos), Google Cloud SQL (base de datos relacional), Google Cloud Functions (computación sin servidor). (Google Cloud, s.f.)
- **IBM Cloud:** Servicios: IBM Cloud Virtual Servers (instancias de servidores virtuales), IBM Cloud Object Storage (almacenamiento de objetos), IBM Db2 on Cloud (base de datos relacional), IBM Cloud Functions (computación sin servidor).
- **Oracle Cloud Infrastructure (OCI):** Servicios: Oracle Compute (instancias de servidores virtuales), Oracle Cloud Infrastructure Object Storage (almacenamiento de objetos), Oracle Autonomous Database (base de datos relacional), Oracle Functions (computación sin servidor). (IBM Cloud, s.f.)
- **Alibaba Cloud:** Almacenamiento de Objetos (OSS), Instancias de servidores virtuales (ECS), Base de datos relacional (RDS), Computación sin servidor. (Alibaba Cloud Products & Services, s.f.)

- **DigitalOcean:** Servicios: Droplets (instancias de servidores virtuales), Spaces (almacenamiento de objetos), Managed Databases (base de datos relacional), App Platform (plataforma de aplicaciones sin servidor). (Digital Ocean, s.f.)
- **Vultr:** Instancias de Servidores Virtuales, Almacenamiento en Bloques, Almacenamiento de objetos. (Vultr - The Everywhere Cloud, s.f.)

3.3.3.2 *Plataforma como Servicio (PaaS)*

Las PaaS son una herramienta que puede simplificar el despliegue y desarrollo de aplicaciones en la nube, descartando la instalación de herramientas de manera local. PaaS está dirigida a desarrolladores de software y aplicaciones web o móviles, y se construye sobre la capa de Infraestructura como Servicio (IaaS). Ofrece sistemas operativos preconfigurados, frameworks de aplicaciones, y APIs para el desarrollo de software, buscando simplificar el despliegue de aplicaciones en máquinas virtuales. (Vera-Rivera & Gaona Cuevas, 2017)

3.3.3.2.1 *Características*

- **Ciclo de vida completo:** Proveen los medios necesarios para soportar el ciclo de vida de creación y entrega de servicios, aplicaciones web y móviles en la nube.
- **Componentes principales:** Incluyen herramientas de desarrollo, una plataforma virtual para la ejecución de aplicaciones y un componente de almacenamiento tipo FaaS (File as a Service).
- **Recursos centralizados:** Los usuarios acceden a todas las herramientas y programas necesarios a través de Internet, sin necesidad de adquirir hardware o instalar software.
- **Arquitectura multitenant:** Los recursos y herramientas de desarrollo son compartidos entre múltiples clientes, permitiendo una infraestructura eficiente.

- **Interfaz de usuario configurable:** Facilita la creación de interfaces de usuario flexibles sin necesidad de escribir código complejo.
- **Soporte integral:** Los proveedores se encargan de la administración, configuración y actualización de servidores e infraestructura, permitiendo que los desarrolladores se centren en la creación y despliegue de sus aplicaciones.
- **Opciones de precios flexibles:** Ofrecen precios adaptados y modelos de pago por uso.
- **Bases de datos gestionadas:** Permiten la configuración y mantenimiento ilimitado de bases de datos, simplificando la creación y modificación de modelos de datos.
- **Automatización de procesos:** Incluyen capacidades para definir procesos de flujo de trabajo y reglas empresariales de manera fácil y automatizada.
- **Seguridad multinivel:** Proporcionan control de seguridad multinivel para compartir funcionalidades y recursos dentro de las aplicaciones.
- **Biblioteca de contenidos integrada:** Ofrecen una librería de elementos comunes que amplían las funcionalidades principales y aceleran el desarrollo.
- **Integración flexible de servicios:** Facilitan una integración fluida de aplicaciones y servicios en la nube.
 - **Entorno completo de desarrollo:** Sirven como entornos de alojamiento, pruebas, implementación y desarrollo de aplicaciones. (Vera-Rivera & Gaona Cuevas, 2017)

3.3.3.2.2 Ejemplos de proveedores de PaaS

- **OpenShift:** Plataforma desarrollada por Red Hat que soporta múltiples lenguajes como Ruby, Java, PHP, Node.js, Python, y Perl. (Red Hat OpenShift, s.f.)

- **Google App Engine:** Plataforma de Google que permite desarrollar y ejecutar aplicaciones en Java, Python y Go, integrando APIs de servicios como Gmail, Google Drive y Google Maps. (App Engine, s.f.)
- **Heroku:** Permite la implementación de aplicaciones en diversos lenguajes como Java, Ruby, Python, Clojure, Node.js y Scala, con opciones de ampliación mediante recursos adicionales. (The Heroku Platform, s.f.)
- **Microsoft Azure:** Brinda a sus usuarios servicios de almacenamiento bajo demanda, una plataforma que permite desplegar aplicaciones web y móviles. (Azure App Service, s.f.)
- **Amazon Web Services (AWS):** Permite implementar y escalar servicios y aplicaciones web utilizando diversos lenguajes y tecnologías, con servicios como AWS Elastic Beanstalk para la gestión de aplicaciones. (AWS Elastic Beanstalk, s.f.)
- **Vercel:** Plataforma especializada en el desarrollo y despliegue de aplicaciones web, especialmente optimizada para frameworks como Next.js y React. Ofrece despliegues rápidos, integraciones con sistemas de control de versiones como Git, y escalabilidad automática, lo que la convierte en una opción popular entre los desarrolladores de frontend. (Vercel, s.f.)
- **DigitalOcean App Platform:** Servicio PaaS que facilita el desarrollo, despliegue y escalabilidad de aplicaciones web. Permite a los desarrolladores implementar aplicaciones desde el código fuente y ofrece soporte para múltiples lenguajes y frameworks. DigitalOcean App Platform se integra con GitHub, GitLab y otros repositorios de código, y simplifica la gestión de la infraestructura subyacente. (Digital Ocean App Platform, s.f.)

3.3.3.3 *Software como Servicio (SaaS)*

Las SaaS son un tipo de modelo que permite acceder a infraestructura TI, aplicaciones de software y soporte a través de Internet. A diferencia del software tradicional, que se vende y se instala en la infraestructura del cliente, el SaaS se entrega como un servicio, con el software y los datos alojados en un centro de datos administrado por el proveedor. Este modelo ofrece ventajas significativas, como costos más bajos de soporte, actualizaciones automáticas y una mayor flexibilidad, ya que los usuarios solo pagan por lo que realmente utilizan. Empresas líderes como IBM, Oracle y Microsoft han adoptado este enfoque, impulsando un crecimiento acelerado del mercado SaaS. Para muchas organizaciones, SaaS representa una alternativa eficiente y rentable frente a las soluciones de software tradicionales. (Ma, 2007)

3.3.4 *Gestión y seguridad de la infraestructura en la nube*

La gestión y seguridad en la nube son dos componentes diferentes mas no aislados, ambos contribuyen a un enfoque integral que abarca la administración eficiente de los recursos informáticos y los servicios que se encuentran dentro del entorno de la nube, contando desde la configuración, monitoreo, automatización, la optimización de servicios, almacenamiento y la configuración de redes virtuales, optimización de costos incluyendo hasta los controles, estrategias y normas implementadas para proteger los recursos antes mencionados de amenazas como ataques cibernéticos, accesos no autorizados, monitoreo de amenazas y respuesta ante incidentes como pérdida de datos. (Kavis, 2014)

La gestión se enfoca en la administración eficiente de recursos y servicios, mientras que la seguridad, protege los recursos de amenazas y asegura la continuidad del negocio, siendo aspectos indispensables para empresas u organizaciones que utilicen la nube como infraestructura tecnológica.

3.3.4.1 Región

Una región es la ubicación geográfica definida por el proveedor de servicios en la nube, quien alberga uno o más centros de datos interconectados. Cada región está compuesta por múltiples zonas de disponibilidad, y son estas regiones quienes permiten la elección de donde almacenar los datos, lo cual, se hace indispensable su correcta elección para optimizar el rendimiento de las aplicaciones y servicios en la nube, reduciendo la latencia, incrementando la disponibilidad y asegurando el cumplimiento normativo, regulaciones locales o internacionales que exigen que los datos permanezcan dentro de una jurisdicción específica. (Google - Ubicaciones de Google Cloud, s.f)

3.3.4.2 Zona de disponibilidad

Las zonas de disponibilidad son el conjunto de centros de datos con infraestructuras físicas independientes pero que se encuentran dentro de la misma Región (AWS - Zonas de disponibilidad y regiones, s.f). Estas zonas permiten a los proveedores de nube, ofrecer disponibilidad, ya que se encuentran diseñadas para ser resilientes ante fallos, de manera que si una zona falla, las demás deben continuar operando sin interrupciones, esto se logra mediante conexiones de baja latencia, lo que permite la réplica sincrónica de datos y el balanceo de cargas entre ellas. (AWS - Zonas de disponibilidad y regiones, s.f)

Las zonas de disponibilidad permiten a las empresas la construcción de aplicaciones, bases de datos altamente disponibles, replicando los datos dentro de toda su región, siendo crucial para la continuidad del negocio, incluso en situaciones de fallos o desastres naturales. (Google - Ubicaciones de Google Cloud, s.f)

3.3.4.3 Dominio

En el Cloud Computing se refiere a un área de administración específica dentro de la red, generalmente vinculada a la administración y organización de recursos y políticas de seguridad, gestión de accesos, usuarios y permisos, ya que un dominio puede incluir usuarios, grupos, dispositivos y aplicaciones que comparten configuraciones y permisos comunes. (Azure, s.f)

3.3.4.4 Proyecto

En el Cloud Computing, se le conoce como proyecto a una unidad organizativa, el cual permite gestionar y segmentar recursos como máquinas virtuales, bases de datos y demás servicios que componen la nube, de forma lógica, definiendo accesos y estableciendo políticas para tales recursos creando permisos y asignando roles a usuarios grupos específicos del dominio, esto facilita la organización de múltiples servicios bajo una administración unificada, permiten segmentar la nube en distintos entornos, como el de desarrollo, pruebas y producción, además son clave para gestionar la facturación y el control de recursos en diversas plataformas que ofertan servicios Cloud (Google Cloud - Crear y administrar proyectos, s.f.)

3.3.4.5 Rol

Un rol es un conjunto de permisos y accesos que se le asigna a uno o varios usuarios para acceder o gestionar los recursos dentro del entorno de la nube (Microsoft Docs, 2023). Los roles permiten especificar las acciones a realizar por cada usuario, como crear, modificar, leer o modificar los recursos de la nube, teniendo esto en cuenta, los roles se clasifican en básicos, predefinidos y personalizados, permitiendo ajustar los permisos a las necesidades específicas de la organización. (AWS - IAM Roles, s.f)

Los roles son clave para aplicar el principio de privilegio mínimo, que garantiza que los usuarios tengan acceso a los recursos necesarios para realizar sus tareas, ayudando a controlar el

acceso de manera granular y segura. (Google Cloud - IAM basic and predefined roles reference, s.f.)

3.3.4.6 Usuarios

Un usuario es una entidad tratada de persona, aplicación o dispositivo, con derechos de acceso a los recursos de una infraestructura en la nube, quienes, a su vez, están gestionados a través de sistemas de gestión de identidades y accesos, quienes se encargan de controlar las acciones que pueden realizar y sobre que recursos y/o servicios, aplicando políticas específicas, asignando roles y permisos según las necesidades de cada entidad. (Microsoft Azure - Manejo de usuarios y accesos en Azure, s.f.)

Cada usuario puede estar asignado a uno o más roles en función a sus responsabilidades, facilitando la aplicación del principio de privilegio mínimo, asegurando que solo tenga acceso a los recursos y servicios para cumplir sus funciones. (Google Cloud - Manejo de usuarios IAM en la nube , s.f.).

3.3.4.7 Control de acceso basado en roles (RBAC)

El RBAC es un modelo de seguridad que se utiliza con mayor amplitud en Cloud Computing, este permite gestionar los permisos y accesos a recursos y servicios según los roles que se asignen a los usuarios en la nube. El RBAC funciona agrupando los permisos en roles predefinidos que reflejan las responsabilidades de las labores de los usuarios. El administrador asigna los roles a los usuarios en base a las asignaciones dentro de la organización, asegurando la aplicación coherente de los permisos.

Este modelo hace más simple la administración de los permisos y asegura que los usuarios tengan accesos solo a los recursos que necesitan para realizar sus funciones dentro de la organización. (Sandhu, 1996).

3.4 Despliegue de nube

3.4.1 Servicios esenciales en la nube

3.4.1.1 Servicio de cómputo

Los proveedores externos ofrecen infraestructuras, plataformas o sistemas de software a través de Internet para que los usuarios puedan acceder y utilizarlos hasta los servidores backend, permitiendo una comunicación rápida y eficiente entre ambas partes (p. ej., los servidores, las tabletas y las computadoras portátiles o de escritorio; es decir, cualquier sistema del usuario) hasta los sistemas de los proveedores, y viceversa. Además, promueven la creación de aplicaciones en la nube y la posibilidad de trabajar de forma flexible en ellas. Para usar estos servicios, solo se necesitan una computadora, un sistema operativo y conexión a Internet.

(RedHat, 2023)

3.4.1.2 Servicio de red

La finalidad de una red es que los usuarios de los sistemas informáticos de una organización puedan usarlos mejorando así el rendimiento global de la organización. Las computadoras pueden compartir recursos a través de aplicaciones especiales gracias a los servicios de red. Para la prestación de servicios de red se requiere que existan sistemas en la red con capacidad para actuar como servidores. Los servidores y servicios de red se basan en los sistemas operativos de red. (Garcia, s.f.)

3.4.1.3 Servicio de identidad

La identidad como servicio, o IDaaS, hace referencia a una amplia variedad de servicios alojados en la nube para la gestión de identidad y acceso (IAM). En esencia, IDaaS es una categoría de funciones tecnológicas que tienen que ver con la identidad del usuario y están

alojadas en la nube. Los proveedores de IDaaS verifican la identidad de los usuarios para prevenir accesos no autorizados a información confidenciales. (CloudFlare, s.f.)

3.4.1.4 Servicio de imágenes

Los servicios de imágenes permiten compartir fotos con muchas personas de manera fácil. Ofrecen mucha flexibilidad y capacidad de crecimiento para guardar, procesar, analizar y compartir imágenes y datos rasterizados.

Los servicios de imágenes son flexibles y robustos, y pueden estar compuestos por una variedad de tipos de datos acordes con sus necesidades y aplicaciones. Si tienes varias imágenes, puedes optar por hacer un mosaico o una colección de imágenes en una sola capa, o tener una capa separada para cada imagen. También puede crear una capa de imágenes a partir de una sola entrada de imagen. (Enterprise, 2023)

3.4.1.5 Servicio de panel de control

Las aplicaciones de paneles de control para servicios hospedados son herramientas en línea que ofrecen proveedores de hospedaje y WEBVAP para gestionar servicios como sitios web, bases de datos, correo electrónico y recursos. Los paneles de control son una forma eficaz de generar ingresos con servidores web y servicios de alojamiento de productos básicos. Los proveedores de hospedaje utilizan paneles de control para simplificar y automatizar la configuración rápida de servidores web y sitios web. Esto permite a los clientes acceder a sus servicios de forma fácil y rápida, desde cualquier lugar y en cuestión de minutos. Además de las funciones básicas del sitio web, la mayoría de los fabricantes del panel de control también proporcionan un sistema de facturación completo con informes extensos e información de facturación detallada. (Microsoft, s.f.)

3.4.1.6 Servicio de gestión de claves

La Gestión de claves es fundamental para la seguridad de un criptosistema y se refiere a las claves a nivel de usuario e incluye generar, intercambiar, almacenar, usar y reemplazar las llaves, además posee protocolos criptográficos de diseño, servidores de claves, procedimientos de usuario y otros protocolos. En las organizaciones es importante definir una política de gestión de claves, que es un conjunto de reglas que establecen cómo se generan, almacenan, distribuyen, borran, actualizan, recuperan, protegen y aplican las claves en una red; se establece al personal autorizado a realizar dichas acciones. (Rguez, 2016)

3.5 Clúster

3.5.1 Clúster de base de datos

Es una arquitectura en la que tenemos varios equipos con parte de los datos del usuario trabajando al unísono como un solo sistema. La arquitectura de un clúster de base de datos viene definida por la manera en que se almacenan los datos en cada nodo. (Dávalos, 2014)

Un clúster es un conjunto de servidores que funcionan juntos para ofrecer alto rendimiento, alta disponibilidad, balance de carga y escalabilidad como si fuesen uno solo.

Se compone de una o varias instancias de base de datos y de un volumen de clúster que administra los datos de esas instancias de base de datos. (Amazon, s.f.)

3.5.2 Clúster de almacenamiento

Los clústeres de almacenamiento permiten a los servidores leer y escribir simultáneamente en un sistema de archivos compartido, proporcionando una imagen consistente a través de los servidores en el clúster. Un clúster de almacenamiento simplifica la administración de almacenamiento al limitar la instalación de aplicaciones a un sistema de archivos. Asimismo, con un sistema de archivos a lo largo del clúster, un clúster de

almacenamiento elimina la necesidad de copias de más de los datos de la aplicación y simplifica la creación de copias de seguridad y recuperación contra desastres. (Documentation, s.f.)

4 MARCO DE LA INVESTIGACIÓN

4.1 Pregunta de investigación

¿Es posible diseñar y configurar una infraestructura de nube geo-distribuida basada en software open source, que permita a las empresas alojar su servicio de PBX?

4.2 Objetivos

4.2.1 Objetivo general

Desarrollar una solución de infraestructura de nube geo-distribuida, que permita a las empresas alojar su servicio de PBX, utilizando herramientas open-source, que integre una interfaz web para la gestión de servicios, una plataforma de base de datos para la administración de datos, y un sistema de identificación que garantice la seguridad del acceso.

4.2.2 Objetivos específicos

- Diseñar una solución de infraestructura de nube geo-distribuida para empresas que requieran utilizar servicios de PBX.
- Construir una nube geo distribuida empleando herramientas del tipo open-source.
- Proporcionar una interfaz web para las empresas que permita gestionar los servicios que se encuentren en la nube geo-distribuida.
- Configurar una plataforma de almacenamiento, que proporcione servicios de almacenamiento.
- Configurar un gestor de base de datos que permita administrar los datos de la infraestructura de nube.
- Configurar un servicio gestor de identificación, para restringir el acceso a los datos de la infraestructura de nube geo-distribuida de la empresa.

- Configurar un servicio de PBX, que permita a la organización comunicarse entre las diferentes sucursales.

5 METODOLOGÍA DE LA INVESTIGACIÓN

5.1 Enfoque de la investigación

Este estudio emplea un enfoque de investigación de tipo mixto que permita comprender la infraestructura de las empresas que requieren emplear un servicio de PBX. Este enfoque garantiza evaluar de manera integral la viabilidad de desarrollar un prototipo de nube geo-distribuida que ofrezca a las empresas una plataforma para alojar y gestionar su servicio de PBX.

5.1.1 Enfoque cuantitativo

Este enfoque está orientado a evaluar las características y necesidades tecnológicas de las empresas que requieren emplear un servicio de PBX, permitiendo analizar a partir de los datos obtenidos mediante una encuesta por muestreo, variables clave como el tipo de infraestructura utilizada, los proveedores de nube empleados y los servicios de nube esenciales para su operación. Estas variables son fundamentales para comprender el estado actual de la infraestructura tecnológica del sector y determinar la viabilidad de configurar una infraestructura de nube geo-distribuida adaptada a las empresas que requieren servicios de PBX.

5.1.2 Enfoque cualitativo

Este enfoque está orientado a recopilar información de líderes dentro de las empresas, con el fin de identificar los elementos que consideran necesarios, para incorporar una infraestructura de nube geo-distribuida en la organización, para el alojamiento de su servicio de PBX, así como las barreras que enfrentan en caso de que no hayan implementado soluciones de este tipo. Para ello, se llevarán a cabo entrevistas estructuradas que permitan comprender qué aspectos evalúan las empresas al implementar un servicio de PBX, incluyendo las necesidades operativas, estratégicas y aspectos económicos que determinan su adopción. Este análisis

proporcionará una visión clara de la situación actual de las organizaciones en cuanto a su adopción tecnológica, facilitando la identificación de necesidades y desafíos.

5.2 Población y muestreo

Para esta investigación, el universo considerado está compuesto por las empresas de atención telefónica en El Salvador, que suman un total de 35 según fuentes consultadas de ofertas de empleo (TRABAJOS EN Call Center EN El Salvador, s.f.) y sitios recopilatorios de empresas del sector (Listado de Call centers, 2019) (Ramón, 2022). Debido a la falta de un listado completo de las empresas que prestan estos servicios en el país, se utilizó un enfoque no probabilístico para determinar la muestra. En este caso, se optó por un muestreo subjetivo por decisión razonada, seleccionando las empresas en función de características clave alineadas con el objetivo de la investigación. Entre estas características se consideraron el número de sucursales que las empresas tienen para prestar sus servicios, así como su presencia tanto a nivel nacional como internacional. Con base en estos criterios, se seleccionaron 18 de las 35 empresas identificadas en el país (Tabla de empresas de Atención Telefónica, Anexo 1). De esta muestra representativa, se eligieron 5 empresas ya que existen contactos personales entre los investigadores y las empresas seleccionadas, lo que facilitó la recolección de datos.

5.3 Instrumentos y técnicas de recolección de datos

Dado que, el proyecto tiene aspectos cuantitativos y cualitativos, es necesario destacar herramientas adecuadas para la recolección de datos acordes a este enfoque. Para ello, se han seleccionado los siguientes instrumentos:

5.3.1 Encuesta por muestreo

Como parte del desarrollo del caso de estudio, se creó una encuesta que pudiera ayudar a comprender las soluciones de infraestructura tecnológicas con las que cuentan las empresas del

sector. Esta encuesta busca identificar el tipo de infraestructura con el que cuentan, los servicios de nube que utilizan para sus operaciones, y los proveedores que les suministran dichos servicios. Estos aspectos permiten comprender cuales son las necesidades tecnológicas que presentan las empresas de este sector.

Para recolectar los datos de empleo una encuesta estructurada haciendo uso de la plataforma Google Forms y se aplicó a través de contactos personales de los investigadores en las empresas. Esto permitió obtener información directa y relevante de personas con conocimiento sobre los servicios de PBX y la infraestructura tecnológica utilizada en sus organizaciones. La elección de esta herramienta se basó en su practicidad y eficiencia, facilitando el análisis de la situación actual de la infraestructura tecnológica de las organizaciones.

La encuesta está dirigida a profesionales del sector de atención telefónica, especialmente a personal técnico quienes interactúan y gestionan servicios de PBX. Además, poseen un conocimiento sobre las herramientas tecnológicas utilizadas para brindar dicho servicio. (Guía de encuesta, Anexo 2)

5.3.2 Entrevista estructurada

Se elaboró una entrevista estructurada con el objetivo de identificar los factores clave que las empresas consideran al implementar un servicio de PBX, incluyendo sus necesidades operativas, estratégicas y económicas. Asimismo, se busca explorar las barreras que han enfrentado en caso de no utilizar servicios de infraestructura de nube.

Para llevar a cabo la recolección de los datos, se realizó mediante videoconferencias a través de contactos personales de los investigadores en las empresas, por medio de la plataforma de Google Meet, la elección de esta herramienta se basó en su facilidad de uso y capacidad para

conectar a participantes desde distintas ubicaciones, permitiendo una comprensión de las necesidades y factores que intervienen en las organizaciones en la adopción tecnológica.

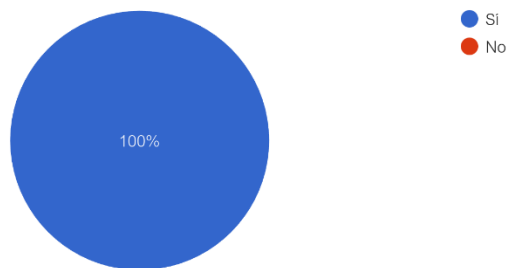
La entrevista está dirigida a profesionales del sector de atención telefónica, especialmente a los líderes de área, quienes poseen un conocimiento de los aspectos operativos, estratégicos y económicos necesarios para incorporar una infraestructura de nube, para el alojamiento de su servicio de PBX, quienes aportaron información relevante sobre las consideraciones que tienen para la adopción de estas tecnologías. (Guía entrevista, Anexo 3)

5.4 Análisis de los resultados

5.4.1 Análisis de los datos cuantitativos

A continuación, se presentan los resultados de la encuesta (Guía de Encuesta, Anexo 2), realizada en septiembre de 2024 y dirigida a 5 profesionales de empresas dedicadas a la atención telefónica.

1. ¿Conoce si la nube puede mejorar las operaciones internas de una empresa?
5 respuestas



El 100% de las empresas encuestadas afirmó tener conocimiento sobre cómo la nube puede optimizar sus operaciones internas, lo que indica que están conscientes de los beneficios que esta tecnología puede aportar a sus procesos.

2. ¿Qué tipo infraestructura utilizan para brindar los servicios?

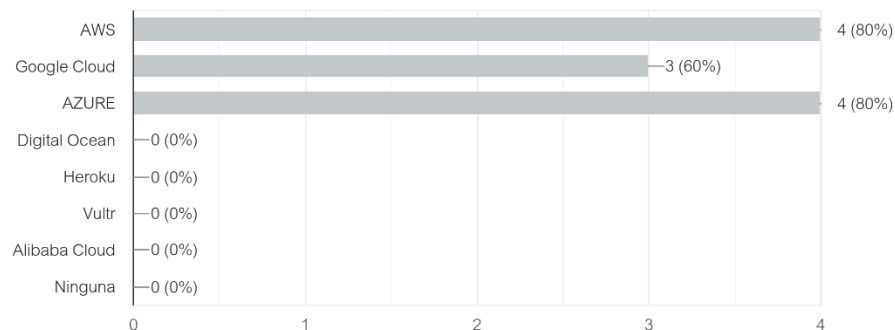
5 respuestas



El 100% de las empresas encuestadas indicó que emplean una infraestructura de nube privada para ofrecer sus servicios. Esto sugiere una preferencia por este tipo de entorno, posiblemente motivada por factores como mayor control, seguridad y personalización que una nube privada puede proporcionar en comparación con otras opciones como la nube pública o híbrida.

3. ¿Cuáles de las siguientes infraestructuras de nubes utiliza su empresa?

5 respuestas

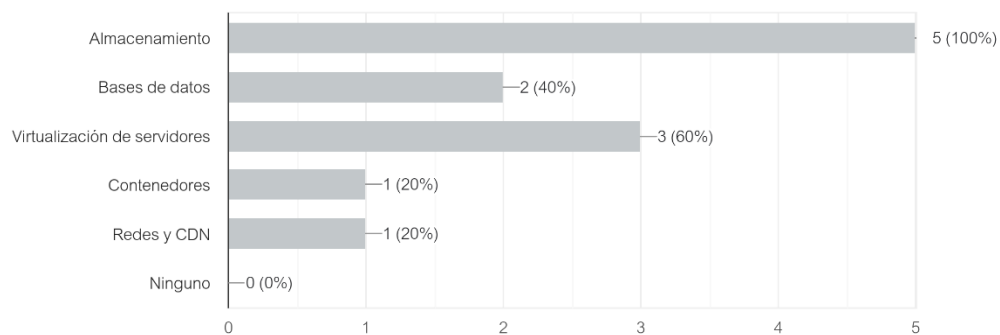


El 80% de las empresas encuestadas muestra una clara preferencia por AWS y Azure como infraestructuras para alojar sus servicios, lo que refleja la confianza en estas plataformas líderes por su robustez, escalabilidad y conjunto de herramientas. Sin embargo, el 60% también

considera Google Cloud, lo que sugiere que esta plataforma está ganando terreno como una opción viable, probablemente debido a su enfoque en la innovación, análisis de datos y precios competitivos. Esto indica que, aunque AWS y Azure dominan, las empresas mantienen abiertas sus opciones hacia otras alternativas en la nube.

4. ¿Cuáles de los siguientes servicios en la nube utiliza su empresa?

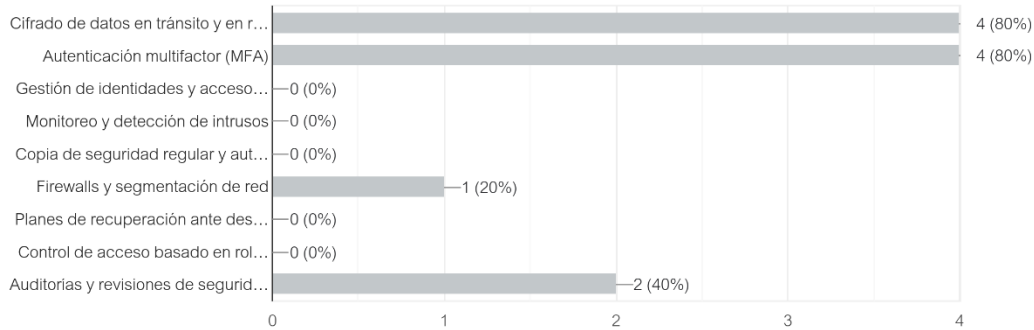
5 respuestas



El 100% de las empresas encuestadas afirmó que utiliza servicios de almacenamiento en la nube, lo que indica la importancia de este servicio como una necesidad básica para la mayoría de las organizaciones. Además, el 60% emplea la virtualización de contenedores, lo que refleja un interés creciente en tecnologías que permiten mayor flexibilidad y eficiencia en la gestión de aplicaciones. Por otro lado, el 40% utiliza bases de datos en la nube, lo que indica que una parte significativa de las empresas está adoptando soluciones gestionadas que facilitan la escalabilidad y el rendimiento en la gestión de datos.

5. ¿Qué medidas de seguridad implementan para resguardar los datos?

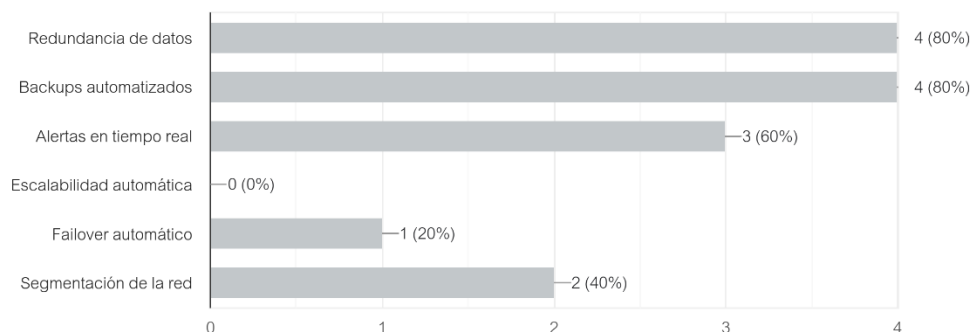
5 respuestas



El 80% de las empresas encuestadas aseguró que implementa medidas de seguridad, como el cifrado de datos tanto en tránsito como en reposo, así como la autenticación multifactor (MFA), esto refleja un compromiso sólido con la protección de la información. Además, el 40% de las empresas realiza auditorías y revisiones de seguridad, lo que sugiere una proactividad en la identificación y gestión de vulnerabilidades, donde esta combinación de estrategias indica que las organizaciones son conscientes de la importancia de resguardar sus activos digitales en un entorno cada vez más amenazante.

6. ¿Qué medidas de contingencia utilizan para garantizar la alta disponibilidad y continuidad operativa de sus servicios?

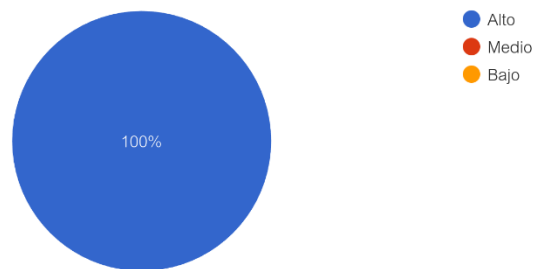
5 respuestas



El 80% de las empresas encuestadas utiliza medidas como redundancia de datos y copias de seguridad automatizadas para garantizar la disponibilidad y continuidad operativa de sus servicios. Sin embargo, solo el 60% emplea alertas en tiempo real, y el 40% implementa segmentación de la red. Estos resultados indican que, aunque muchas organizaciones están adoptando buenas prácticas, aún hay espacio para fortalecer sus estrategias de monitoreo y seguridad.

7. ¿Qué nivel de relevancia asigna su empresa a la adopción de tecnologías actuales en infraestructuras de nube?

5 respuestas



El 100% de las empresas encuestadas afirmó que asigna un alto nivel de relevancia a la adopción de tecnologías en infraestructuras de nube. Esto indica una clara comprensión de la importancia de la transformación digital y su impacto en la competitividad y eficiencia operativa de sus organizaciones.

5.4.2 Análisis de los datos cualitativos

Para el análisis de la entrevista a José Luis Munguia (Manage of client Operations), se utilizó un análisis hermenéutico debido a que este enfoque permite una interpretación profunda

de los textos. Este enfoque también explora percepciones, intenciones y contextos, lo que enriquece el análisis de resultados.

El círculo hermenéutico, con sus etapas, la precompresión, la función de horizontales y "oír al texto", permite un proceso reflexivo y dinámico. En la precompresión se identifican los prejuicios particulares y generales, que tanto el analista como el entrevistado podrían tener, lo que puede distorsionar la interpretación. La fusión de horizontes implica la unificación de las perspectivas del entrevistador y el entrevistado, lo que permite al analista abordar un mejor entendimiento del trasfondo empresarial y tecnológico y la situación en la que se colocan las respuestas. Por último, "oír al texto" significa leer detenidamente, prestando atención no solo al texto explícito, sino a las implícitas y a las intenciones inherentes al texto. (Villamizar de Camperos, s.f.)

5.4.2.1 Precompresión

Se refiere al conjunto de conocimientos que tiene el investigador previo al análisis de fenómeno estudiado. (Manchola, 2017)

El entrevistado demuestra un conocimiento claro sobre los servicios en la nube, dado que su empresa, Teleperformance, ya utiliza plataformas como AWS, Azure y Google Cloud. A partir de sus comentarios, se puede inferir que ha tenido experiencias positivas con estas tecnologías, ya que describe la infraestructura tecnológica actual de la empresa como eficiente.

5.4.2.2 Reconocimiento de prejuicios

Permiten entender las ideas que subyacen y componen los argumentos presentados por el entrevistado. (Manchola, 2017)

El entrevistado también menciona que los elementos prioritarios para la adopción de nuevas tecnologías son los beneficios, la seguridad, los costos y la productividad. Estos factores

pueden reflejar ciertos prejuicios típicos de un entorno corporativo, donde las decisiones se basan principalmente en la eficiencia operativa y en asegurar el retorno de la inversión. Aquí, el prejuicio positivo hacia la nube se vincula con la creencia en que estas plataformas mejoran la productividad y reducen costos.

5.4.2.3 *Fusión de horizontales*

Se refiere a las perspectivas del entrevistado al fenómeno estudiado y como se contrastan con el contexto actual del investigador. (Manchola, 2017)

José Luis menciona que "la adaptabilidad y capacitación para el uso de nuevas herramientas" son barreras potenciales debido al alto número de empleados. Esto refleja su preocupación no solo por la infraestructura tecnológica en sí, sino también por el impacto que los cambios en la infraestructura tecnológica de la empresa puede tener en el personal y su capacidad para adaptarse a nuevas herramientas. Esta fusión de horizontes entre la tecnología y la gestión del capital humano revela un enfoque holístico en su visión.

5.4.2.4 *Oír el texto*

Permite que el investigador encuentre el sentido del fenómeno estudiado a través de los argumentos presentados por el entrevistado, y entenderlo en su propio contexto. (Manchola, 2017)

Al describir la experiencia como "positiva" para los clientes, se puede interpretar a generado un impacto positivo en el rendimiento operativo de la empresa y en la percepción de calidad de parte de los clientes y empleados. Es posible identificar que el entrevistado ve a la nube como una solución que permite la mejora continua.

5.4.2.5 *Aplicación del sentido*

El investigador encuentra sentido en los argumentos presentados por el entrevistado, a través de la relación que existe entre las ideas de cada uno, que permiten entender el fenómeno estudiado. (Manchola, 2017)

La expectativa de “innovación y mejora continua” mencionada por el entrevistado implica que la adopción de una infraestructura en la nube no es vista como una solución estática, sino como una forma de crecimiento y avance tecnológico para Teleperformance.

5.4.2.6 *Interrogarse*

El investigador se interroga sobre los argumentos presentados por el entrevistado, para interpretar y entender lo que quiere dar a conocer sobre el fenómeno estudiado. (Manchola, 2017)

Al analizarse de forma profunda las respuestas, se puede inferir que, la experiencia con la nube en Teleperformance ha sido principalmente positiva, para la empresa y en general para cualquier empresa la gestión del cambio es fundamental al adoptar nuevas tecnologías y en el caso de infraestructuras en la nube es importante planificar considerando tanto aspectos técnicos como humanos.

5.5 Conclusión de los resultados y de la investigación

Basado en los resultados obtenidos tanto de las encuestas como la entrevista se puede concluir que las empresas seleccionadas tienen conocimientos sobre la nube y hacen uso de algunas infraestructuras para la prestación de sus servicios. Además, poseen los conocimientos necesarios para el gestionamiento de estos, así como la implementación de ciertas medidas de seguridad y contingencia.

Para nuestra investigación, estos resultados nos indican que es posible implementar una infraestructura de nube geo distribuida dentro de las empresas encuestadas, pues todas ellas ya hacen uso de una infraestructura en la nube para la prestación de sus servicios, por lo que el tema no es algo desconocido.

6 PROTOTIPO

6.1 Requerimientos

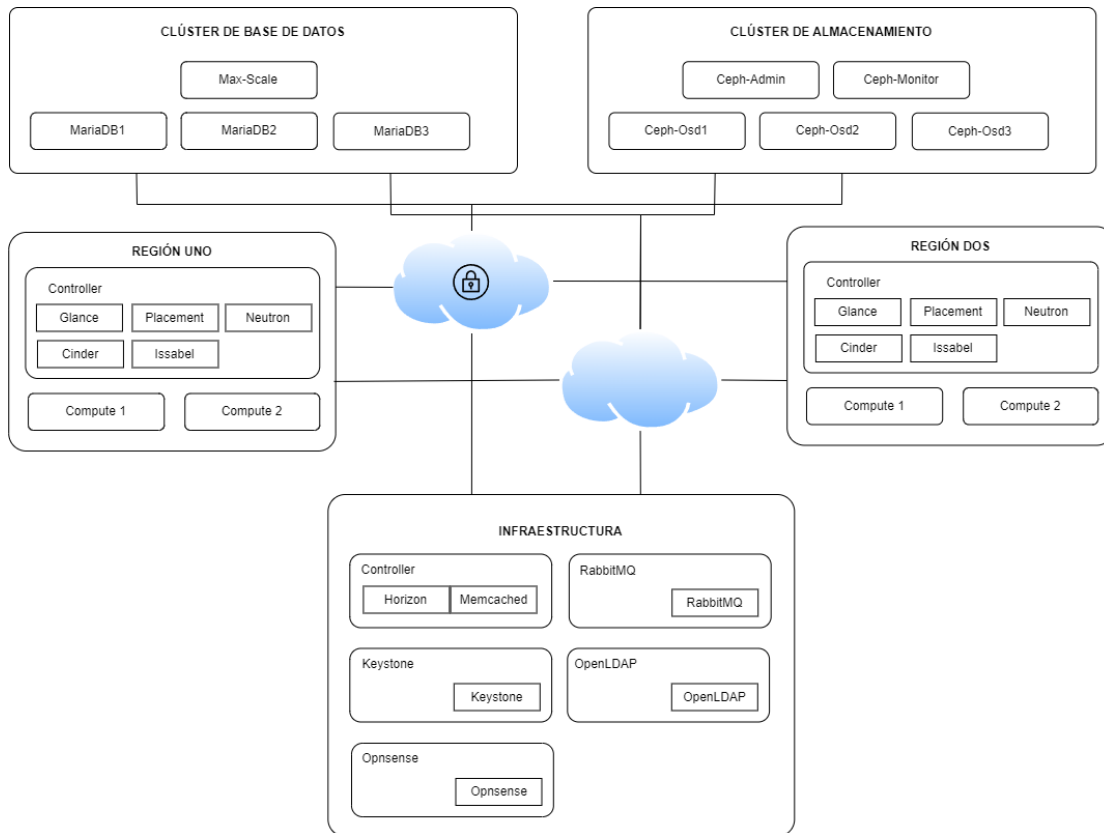
Con base en el contexto de la investigación se ha diseñado y configurado una infraestructura de nube geo-distribuida basada en software open source, capaz de gestionar múltiples regiones. Estas regiones utilizan los servicios proporcionados por la infraestructura.

Los requisitos clave para el diseño y configuración del prototipo de software open source son los siguiente:

- Proporcionar un servicio de identidad a todas las regiones que forman parte de la nube geo-distribuida para la autenticación y autorización, gestionándolo a través de un servicio de usuarios federados centralizado con un único repositorio disponible para todas las regiones.
- Proveer almacenamiento de caché de sesiones dentro de la plataforma, y el servicio de cola de mensajes para coordinar las operaciones e información de estado entre los servicios.
- Proporcionar un servicio de base de datos centralizado.
- Propiciar una interfaz para la gestión y administración de la infraestructura y las regiones alojadas.

6.2 Arquitectura.

Ilustración 1 Arquitectura de la infraestructura de nube geo-distribuida. Autoría Propia.



La infraestructura está dividida en tres regiones: una región principal llamada "Infraestructura" y dos regiones adicionales denominadas "Región Uno" y "Región Dos". La región de Infraestructura se encarga de proporcionar servicios a las demás regiones a través de diversas APIs. Los servicios ofrecidos desde la región de Infraestructura son:

Servicio de Cola de Mensajes: Se implementa mediante RabbitMQ, este servicio facilita la comunicación entre las diferentes regiones, gestionando los eventos de manera eficiente y asegurando una comunicación asíncrona y confiable.

Servicio de Base de Datos: Se proporciona a través de un clúster de MariaDB, este servicio ofrece una base de datos centralizada que da soporte a todas las regiones, garantizando una gestión eficiente y unificada de los datos.

Servicio de Almacenamiento: Se implementa mediante un clúster de Ceph, este servicio proporciona almacenamiento centralizado para todas las regiones, asegurando la disponibilidad y escalabilidad de los datos.

Panel de Administración: Se provee a través del componente Horizon de OpenStack, este panel permite la gestión de los recursos en cada región. La administración de usuarios se realiza mediante el componente Keystone de OpenStack, que se integra con un servicio LDAP para el aprovisionamiento de usuarios federados en todas las regiones.

6.3 Configuración

A continuación, se detallan cada uno de los nodos utilizados en el prototipo a nivel de máquina virtual y hardware utilizado.

6.3.1 Nodo controller

Este nodo contiene el núcleo de la solución, incluyendo la interfaz para la gestión y administración de la infraestructura. Además, gestiona la cola de mensajes, facilitando la comunicación eficiente y confiable entre servicios distribuidos, y asegurando la sincronización y escalabilidad del sistema.

Tabla 1: Requerimientos para nodo controller.

Nodo	CPU	RAM	Almacenamiento	OS
Controller	2	8	50	Ubuntu
RabbitMQ	2	4	50	Ubuntu

Nota: Requisitos necesarios en nodo controller, incluyendo CPU, RAM, almacenamiento y sistema operativo para la infraestructura de una nube comunitaria basada en OpenStack.

Autoría propia.

6.3.2 Nodo identidad

Este nodo se encarga de administrar la autenticación, autorización y directorio de usuarios, brindando una solución centralizada para la gestión de identidades y accesos a la infraestructura.

Tabla 2: Requerimientos para nodo Identidad.

Nodo	CPU	RAM	Almacenamiento	OS
Keystone	2	4	50	Ubuntu
OpenLDAP	2	4	50	Ubuntu

Nota: Requisitos necesarios en nodo identidad, incluyendo CPU, RAM, almacenamiento y sistema operativo para la infraestructura de una nube comunitaria basada en OpenStack.
Autoría propia.

6.3.3 Clúster de base de datos

Este nodo integra un sistema de gestión de bases de datos con herramientas para balanceo de carga y enrutamiento de consultas, proporcionando una solución escalable para el almacenamiento y gestión de datos en la infraestructura.

Tabla 3: Requerimientos para clúster de base de datos.

Nodo	CPU	RAM	Almacenamiento	OS
MaxScale	2	2	50	Ubuntu
MariaDB 1	2	2	50	Ubuntu
MariaDB 2	2	2	50	Ubuntu
MariaDB 3	2	2	50	Ubuntu

6.3.4 Clúster de almacenamiento

Se encarga de proporcionar un sistema de archivos distribuidos y escalables, brindando un almacenamiento eficiente y de confianza para grandes volúmenes de datos.

Tabla 4: Requerimientos para clúster de almacenamiento.

Nodo	CPU	RAM	Almacenamiento	OS
ADMIN	2	4	50	Ubuntu
Monitor	2	2	50	Ubuntu
OSD 1	2	2	50	Ubuntu
OSD 2	2	2	50	Ubuntu
OSD 3	2	2	50	Ubuntu

Nota: Requisitos necesarios para el clúster de almacenamiento, incluyendo CPU, RAM, almacenamiento y sistema operativo, para una infraestructura de nube comunitaria basada en OpenStack. Autoría propia.

6.3.5 Nodos controller por región.

Este nodo gestiona la infraestructura local, coordinando las operaciones y recursos específicos de su región. Se encarga de la administración de servicios de nube, como la orquestación y el control de las máquinas virtuales, así como la integración y sincronización con otros nodos Controller en diferentes regiones.

Tabla 5: Requerimientos para nodo controller por región.

Nodo	CPU	RAM	Almacenamiento	OS
Controller	2	8	50	Ubuntu

Nota: Requisitos necesarios para nodo controller por cada región, incluyendo CPU, RAM, almacenamiento y sistema operativo, para una infraestructura de nube comunitaria basada en OpenStack. Autoría propia.

6.3.6 Nodos compute por región.

Cada nodo Compute en las regiones proporciona recursos de procesamiento para ejecutar máquinas virtuales y cargas de trabajo. Estos nodos utilizan el almacenamiento del clúster de CephFS en lugar de almacenamiento local, y gestionan la ejecución de instancias y la comunicación entre recursos computacionales dentro de su región.

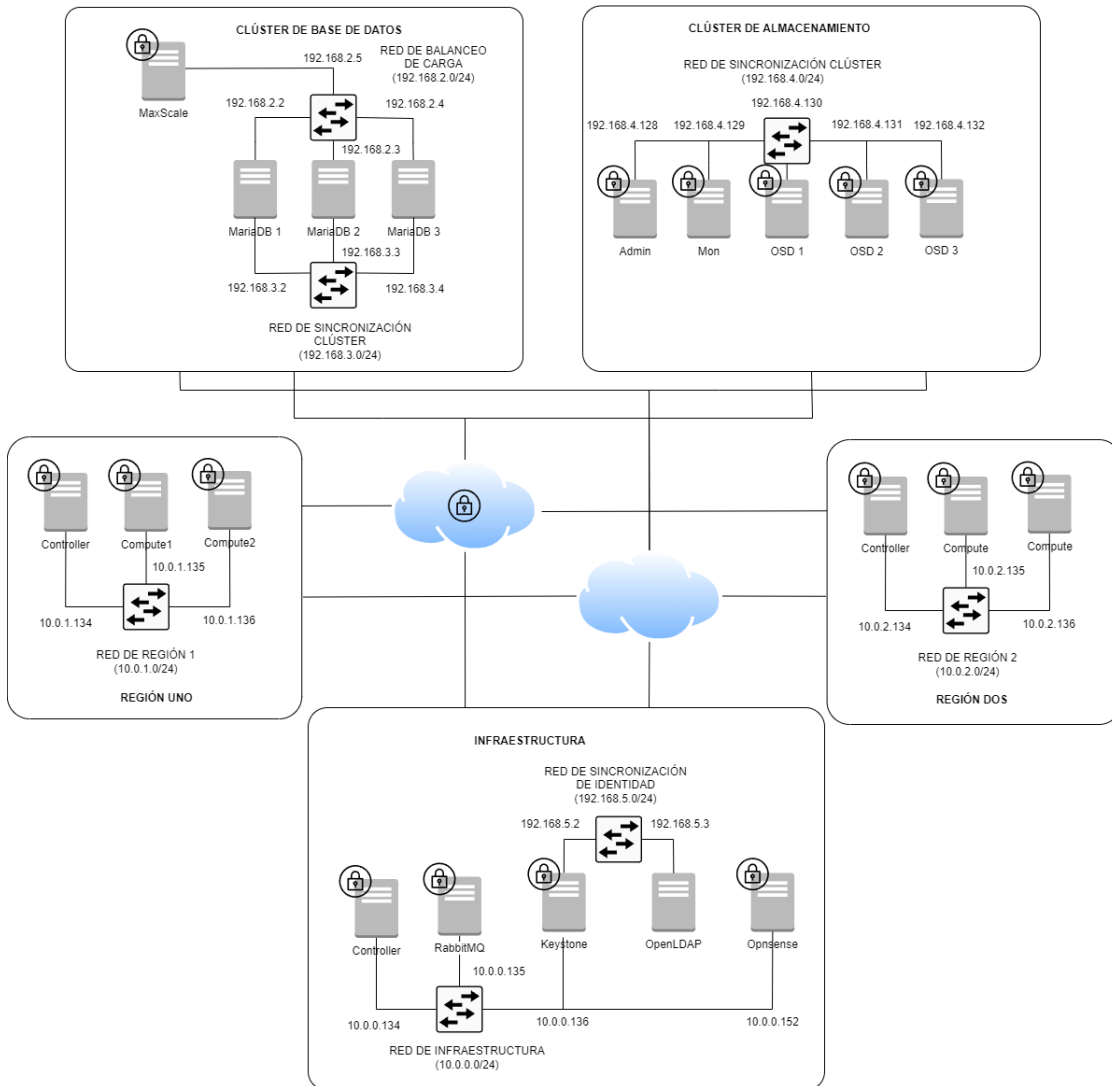
Tabla 6: Requerimientos para nodo compute.

Nodo	CPU	RAM	Almacenamiento	OS
Compute	4	8	50	Ubuntu

Nota: Requisitos necesarios para nodo compute por región, incluyendo CPU, RAM, almacenamiento y sistema operativo, para una infraestructura de nube comunitaria basada en OpenStack. Autoría propia.

6.4 Topología de red

Ilustración 2 Topología de red de la infraestructura de nube geo-distribuida. Autoría Propia.



La topología de red de la infraestructura se organiza en función de diversas redes especializadas. Cada región está conectada a una red principal, que se encarga de interconectar todos los componentes y está expuesta a Internet para permitir el acceso a los servicios públicos.

El clúster de base de datos está compuesto por dos redes distintas. La primera red se utiliza para gestionar el balanceo de carga entre MaxScale y cada uno de los nodos de la base de datos, mientras que la segunda red está dedicada a la sincronización de la información entre los nodos.

Por otro lado, el clúster de Ceph cuenta con una red específica para la sincronización entre los nodos del clúster. Además, esta red permite el monitoreo de los recursos en el nodo de monitor y en los nodos de almacenamiento.

El servicio de identidad, proporcionado por OpenStack, utiliza una red particular para que el componente Keystone se comuniquen con el servicio LDAP, el cual se encarga de la gestión de los usuarios federados.

Finalmente, se ha implementado una red privada virtual (VPN) para garantizar que los servicios de la región principal sean accesibles desde cada una de las regiones que conforman la infraestructura.

7 CASO DE ESTUDIO

El caso de estudio explora el diseño y la configuración de un prototipo de infraestructura de nube geo-distribuida, destinada a empresas que utilizan servicios de PBX y operan en múltiples zonas geográficas. La infraestructura propuesta debe ser escalable, ofrecer servicios a usuarios federados, garantizar la persistencia de sesiones y proporcionar una base de datos como servicio. Además, debe contar con una interfaz web que permita gestionar las diferentes regiones, facilitando a los centros de llamadas el control del flujo de comunicaciones entre las diversas zonas operativas de la empresa, asegurando así la continuidad del negocio.

El centro de datos central, el cual nombramos como “INFRAESTRUCTURA”, actúa como el núcleo y proporciona los servicios fundamentales para gestionar la nube utilizada por los centros de llamada en cada región. Este centro de datos está formado por tres clústeres, cada uno con una responsabilidad clave:

El nodo controller se encarga de coordinar todos los servicios de la nube, utiliza RabbitMQ para asegurar una comunicación fluida entre los diferentes componentes de OpenStack, es el nodo permite integrar los diferentes nodos de computación distribuidos en las diferentes regiones.

El nodo de identidad proporciona autenticación y autorización centralizada para los usuarios y servicios a través de Keysone y OpenLDAP. Estos servicios aseguran que los usuarios puedan acceder a los servicios de la nube en cada una de las regiones, garantizando la seguridad y el control de acceso a los servicios necesarios para montar los sistemas de PBX.

El clúster de base de datos está compuesto por múltiples instancias de MariaDB y un balanceador MaxScale, lo que garantiza una alta disponibilidad de los datos críticos, además de permitir el manejo y procesamiento de la información en cada región de la nube."

El clúster de almacenamiento, basado en Ceph, ofrece almacenamiento y redundancia de datos a cada una de las regiones. Esto permite que cada nodo compute acceda a los datos de forma rápida y segura.

Cada región está compuesta por sus propios controllers locales y dos nodos compute, lo que permite que las cargas de trabajo se gestionen localmente, minimizando la latencia. Sin embargo, dependen de la sede principal para servicios críticos como la autenticación y la replicación de datos, lo que permite alta disponibilidad en toda la infraestructura.

La comunicación entre cada nodo de la infraestructura se realiza a través de la VPN Tailscale, lo que garantiza el intercambio de paquetes entre cada región de forma segura y encriptada.

Para este caso de estudio, se considera una empresa de centros de atención telefónica con dos sucursales: una en Guatemala y otra en El Salvador. La compañía cuenta también con una sede central, ubicada en otra área de El Salvador, donde se alojan los recursos principales para ofrecer el servicio a las sucursales. Cada sucursal dispone de su propio servicio de PBX, alojado en una infraestructura de nube geo-distribuida, a través de la cual los clientes pueden comunicarse con la sucursal de su elección. De igual manera, las sucursales pueden comunicarse entre sí.

A continuación, se presenta el estudio de la factibilidad de la infraestructura para evaluar si esta es viable y eficiente.

8 FACTIBILIDAD

Evaluar la factibilidad de un proyecto es un paso clave en el proceso de toma de decisiones estratégicas para su implementación. En este caso de estudio, se ha creado un prototipo basado en OpenStack, una plataforma de código abierto que permite a las empresas desplegar infraestructuras en la nube. No obstante, antes de proponerla como la solución definitiva, es importante analizar si esta opción es la más conveniente en comparación con otras alternativas de referencia en el mercado.

8.1 Factibilidad técnica

Para evaluar si la solución propuesta cuenta con los aspectos técnicos necesarios para implementarse como infraestructura de nube geo-distribuida, es fundamental analizar las alternativas disponibles en el mercado. A continuación, se presenta un cuadro comparativo que detalla los principales servicios ofrecidos por OpenStack y su equivalente en otras plataformas líderes del sector.

Tabla 7 Cuadro comparativo de los principales componentes de proveedores de nube

Servicio	OpenStack	Azure	Google Cloud
Computación	Nova	Azure Virtual Machines	Google Compute Engine
Red	Neutron	Azure Virtual Network	Google VPC
Identidad	Keystone	Azure Active Directory	Google Cloud Identity and Access Management (IAM)
Recursos	Placement	Azure Resource Manager	Google Cloud Resource Manager
Almacenamiento de Bloques	Cinder	Azure Disks	Google Persistent Disks

Almacenamiento de Objetos	Swift	Azure Blob Storage	Google Cloud Storage
Panel de Control	Horizon	Azure Portal	Google Cloud Console
Imágenes	Glance	Azure Managed Images	Google Cloud Images

Además, es fundamental evaluar la capacidad del prototipo para dar respuesta ante diferentes cargas de trabajo, para ello se considerará el rendimiento del servidor de PBX de acuerdo a ciertas configuraciones técnicas, teniendo en cuenta el número de núcleos de CPU, la memoria RAM y el almacenamiento en disco.

Con ese fin, se ha utilizado la herramienta SIPp como simulación de llamadas y el dashboard de monitoreo de recursos que provee Issabel, para medir y analizar el desempeño del servidor de PBX, permitiendo así identificar la cantidad de llamadas simultaneas que el prototipo soporta.

Las características del servidor de PBX son:

Núcleos de CPU: 4

Memoria RAM: 4GB

Almacenamiento Disco: 50GB

Cabe resaltar que, según las especificaciones de la infraestructura del prototipo, se pueden tener 4 servidores de PBX con las características descritas anteriormente. Donde para efectos de demostración solo se configuraron dos, uno por cada región, pero se podría agregar

uno adicional a cada región según se considere conveniente. O aumentar las características de los dos ya configurados.

Para el análisis, las pruebas se configuraron con una duración de la llamada de cinco minutos, donde se obtuvieron los siguientes resultados: (Resultados de Pruebas, Ver Anexo 6)

Tabla 8 Resultados de pruebas de la capacidad operativa del servidor de PBX

Canta. Llamadas	CPU	RAM	SWAP
50	65%	57%	0%
100	84%	59%	0%
150	75%	72%	0%
200	89%	80%	1%

Obteniendo así que el servidor de PBX, soporta aproximadamente 200 llamadas simultaneas con un uso bastante alto de los recursos, sin embargo, con un uso moderado de los recursos el servidor soporta 100 llamadas simultaneas.

8.2 Factibilidad económica

Con el objetivo de analizar económicamente la viabilidad de la implementación de una infraestructura de nube geo-distribuida se realizó una comparación de dos proveedores de nubes públicas (Azure y Google Cloud) con respecto a la adquisición del hardware necesario para la construcción de la infraestructura de nube geo-distribuida descrita en el documento.

Se han utilizado los precios proporcionados por las herramientas de cálculo cada proveedor, es importante destacar que los precios se hacen con base en los servicios proporcionados por los mismo, por ejemplo, se han comparado los precios de la implementación de un clúster CEPH con los precios de los servicios “Azure Managed Disks” y “Cloud Persistent Disks” de Azure y Google Cloud respectivamente.

Para la implementación de la infraestructura en un ambiente de producción es necesario contar con los siguientes elementos:

Tabla 9 Requerimientos necesarios para la implementación de la infraestructura

Nodo	Cantidad	CPU (Núcleos)	RAM (GB)	Almacenamiento (GB)
Controlador	1	2	8	50
Keystone	1	2	2	50
RabbitMQ	1	2	2	50
OpenLDAP	1	2	2	50
OPNSense	1	2	2	50
Base de datos	4	2	2	50
Ceph admin	1	2	2	50
Ceph Monitor	1	2	2	50
Ceph OSD	3	2	2	100
Controlador (regiones)	2	4	8	50
Compute	4	4	8	50

Con base en las características descritas en la tabla 9 “Requerimientos necesarios para la implementación de la infraestructura”, la nube diseñada es capaz de alojar 2 instancias de Issabel por cada región. Con base en ello, se muestran los precios de los servicios necesarios para alojar 4 instancias de Issabel, 1 red privada con 1 TB de transferencia y una instancia de OPNSense en las nubes de Google Cloud y Azure.

Tabla 10 Servicios equivalentes Google Cloud

Producto	Cantidad	Servicio	Precio unitario	Precio total
Issabel	4	(Cloud Engine) N1 - 4 Cores - 50 GB SSD	\$118.40	\$473.60
Red	1	Cloud Load Balancing	\$34.25	\$39.20
OPNSense	1	N1 - 2 Cores - 50 GB SSD	\$ 63.45	\$63.45
Total				\$571.30

Tabla 11 Servicios equivalentes en Azure

Producto	Cantidad	Servicio	Costo unitario	Precio total
Issabel	4	(Virtual machines) A4 V2 - 4 Cores - 50GB SSD - 10000 T	\$144.43	\$577.72
Red	1	Virtual Network	\$39.20	\$39.20
OPNSense	1	A2 - 2 Cores - 50 GB SSD	\$ 62.67	\$62.67
Total				\$679.59

Para tener un panorama más amplio de los precios que brindan los proveedores se muestra a continuación los costos de cada servicio de forma anual:

Tabla 12: Precios anuales de los servicios requeridos

Nodo	Cantidad	Servicio	Google Cloud	Azure
		Cloud		
Issabel	4	Engine/Virtual Machine	\$5,683.2	\$6,932.64
		Cloud load		
Red	1	balancing / Virtual Network	\$411.00	\$470.40
		Cloud		
OPNSense	1	Engine/Virtual Machine	\$ 761.40	\$752.04
Total			\$ 6,855.60	\$ 8,155.08

Para la implementación de nuestra infraestructura se ha realizado un cálculo del costo de una máquina estándar que permita cumplir con los requerimientos óptimos en un ambiente de producción:

Tabla 13 Precios del hardware requerido para la infraestructura

Nodo	Cantidad	Infraestructura física
Controlador	1	\$1,654.65
Keystone	1	\$1,654.65
RabbitMQ	1	\$1,654.65
OpenLDAP	1	\$1,654.65
OPNSense	1	\$1,654.65
Base de Datos	4	\$6,618.60
Ceph	5	\$8,273.25
Controlador (regiones)	2	\$3,309.30
Compute	4	\$6,618.60
Total		\$33,093.00

Sin embargo, para la implementación de una infraestructura los costos no se limitan solamente en el hardware, si no que tiene costos relacionados con la gestión y monitoreo de la infraestructura, por lo que podemos destacar los siguientes: el mantenimiento y operación, así que la inversión inicial en el primer año para la implementación de una infraestructura se determina de la siguiente forma:

Tabla 14 Inversión requerida para la infraestructura de nube geo-distribuida (primer año)

Descripción	Precio
Hardware	\$33,093.00
Mantenimiento	\$ 1,980.00
Operación	\$ 2,880.00
Total	\$37,953.00

Tabla 15 Costo de mantenimiento y operación de la infraestructura de nube geo-distribuida anual

Descripción	Precio
Mantenimiento	\$ 1,980.00
Operación	
Electricidad: \$30 / región	\$ 1,080.00
Internet (250MB): \$50 / región	\$ 1,800.00
Total	\$ 4,860.00

En la siguiente tabla podemos ver un resumen de los costos que se han mostrado en las tablas anteriores para tener una mejor comparación de los precios proporcionados:

Tabla 16 Comparación de precios de los proveedores y la compra del hardware para el primer año.

Proveedor	Precio anual
Google Cloud	\$ 6,855.60
Azure	\$ 8,155.08
Infraestructura física	\$37,953.00

Tabla 17 Comparación de precios para 1, 3 y años.

Año	Google Cloud	Azure	Infraestructura Física
1	\$6,855.60	\$8,155.08	\$37,953.00
2	\$6,855.60	\$8,155.08	\$4,860.00
3	\$6,855.60	\$8,155.08	\$4,860.00
4	\$6,855.60	\$8,155.08	\$4,860.00
5	\$6,855.60	\$8,155.08	\$4,860.00
6	\$6,855.60	\$8,155.08	\$4,860.00
7	\$6,855.60	\$8,155.08	\$4,860.00
8	\$6,855.60	\$8,155.08	\$4,860.00
9	\$6,855.60	\$8,155.08	\$4,860.00
10	\$6,855.60	\$8,155.08	\$4,860.00
Total	\$68,556.00	\$81,550.80	\$81,693.00

Teniendo en cuenta que los precios son estimados y podrían variar en base a muchos factores internos de las empresas que deseen implementarlos, podemos ver que los precios de los proveedores son un poco más bajos en comparación a adquirir una infraestructura física. Sin embargo, a partir del segundo año los costos de una infraestructura física tienden a disminuir debido que la inversión en hardware será menor, lo que la hace más rentable a largo plazo.

Un análisis adecuado debe contemplar no solo los costos, sino también los beneficios únicos que este tipo de inversión puede ofrecer. Esto permite equilibrar el alto costo inicial frente

a las ventajas específicas que difícilmente una solución estándar de un proveedor podría igualar, entre las cuales se destacan:

- Se cuenta con un control total para gestionar y personalizar la infraestructura según las necesidades específicas de la organización.
- Existe un mayor control sobre la seguridad de los datos y la infraestructura, ya que se encuentran alojados dentro de su área local, sin depender de políticas de externas.
- Una mejora considerable en el rendimiento ya que el hardware es configurado de acuerdo a las demandas de la organización, sin tener que compartir los recursos con otras organizaciones.
- Facilidad para adaptarse y escalar la infraestructura sin tener restricciones que le impidan llevarlas a cabo.
- Facilidad para cumplir con las normas o regulaciones del país en el que se encuentre la organización.

Por lo que podemos concluir, que los costos iniciales de adquirir una infraestructura física pueden ser superiores a los precios ofrecidos por los proveedores. Sin embargo, a largo plazo, estos costos tienden a disminuir, convirtiéndose en una opción más rentable para las organizaciones. Es importante destacar que estos altos costos se compensan con beneficios significativos, como el control total sobre la personalización y gestión de la infraestructura, la mejora en la seguridad de los datos, el aumento del rendimiento, la flexibilidad para escalar y la facilidad para cumplir con regulaciones locales. Estos aspectos, que aportan un valor incalculable a las organizaciones, son difíciles de igualar por las soluciones ofrecidas por los proveedores.

9 CONCLUSIONES

La implementación de una infraestructura de nube geo-distribuida ha demostrado ser efectiva para las empresas de atención telefónica, permitiendo la integración de múltiples sucursales sin afectar el rendimiento de los servicios de PBX. Esto garantiza la continuidad del servicio y mejora la capacidad de respuesta ante las necesidades de los clientes.

La configuración de una infraestructura de nube geo-distribuida utilizando OpenStack para empresas que requieren servicios de PBX resulta en una solución flexible y altamente escalable. OpenStack, como plataforma de computación en la nube de código abierto, proporciona herramientas robustas para la gestión de recursos en múltiples ubicaciones geográficas, lo que permite la integración eficiente de diversas sucursales.

La implementación de Ceph como plataforma de almacenamiento para proporcionar servicios a una infraestructura de nube representa una solución robusta y escalable. Ceph ofrece características como alta disponibilidad, escalabilidad horizontal y redundancia de datos, lo que lo convierte en una opción ideal para satisfacer las demandas de almacenamiento en entornos de nube.

La configuración de una plataforma de base de datos utilizando MariaDB junto con MaxScale para proporcionar servicios de gestión de datos en una infraestructura de nube resulta en una solución eficiente. MariaDB, como un sistema de gestión de bases de datos relacional, ofrece características robustas de rendimiento y escalabilidad, lo que lo hace adecuado para manejar cargas de trabajo en entornos de nube.

La configuración de un servicio de PBX utilizando Issabel permite a la organización establecer una comunicación efectiva entre sus diferentes sucursales, resultando en una solución integral para la gestión de las comunicaciones. Issabel, como plataforma de código abierto,

ofrece características avanzadas de gestión de llamadas, integración de aplicaciones y personalización, lo que la hace ideal para satisfacer las necesidades específicas de comunicación de las organizaciones.

Los costos iniciales de una infraestructura de nube física son superiores a los de un proveedor de nube, y a largo plazo puede resultar más rentable. Esta inversión ofrece beneficios clave sobre la infraestructura, como control total, mayor seguridad, rendimiento optimizado, flexibilidad para escalar y facilidad para cumplir con normativas locales. Estos aspectos son de gran valor para las organizaciones y difícilmente igualables por los proveedores de soluciones en la nube.

10 RECOMENDACIONES

Es fundamental contar con un equipo que disponga de recursos de hardware suficientes para permitir la expansión de la infraestructura de nube geo-distribuida a medida que surjan nuevas necesidades. Esto garantiza que el sistema pueda crecer y adaptarse a demandas adicionales sin limitaciones, asegurando tanto la eficiencia operativa como la capacidad de respuesta ante los requerimientos futuros de la organización.

El presente trabajo se realizó con una conexión a internet de entre 20 a 100 Mb, lo cual presento cierta lentitud en la conexión de las zonas que conforman la red de la infraestructura de nube geo-distribuida. Para tener una mejor comunicación entre las regiones, se debe contar con una conexión a internet como mínimo de 50 Mb, para mejorar la experiencia del usuario al ingresar al dashboard de OpenStack, la creación de máquinas virtuales o carga de imágenes para quienes administren las zonas.

Al momento de crear una máquina virtual haciendo uso de la imagen de Issabel es necesario modificar el tiempo de sesión en OpenStack, ya que, debido al peso fue necesario extender el tiempo de sesión para que esta pudiera cargarse y crear una instancia a partir de ella. Por defecto el tiempo de sesión es de una hora, pero para poder crear una instancia será necesario extender la sesión para más de una hora o tomar en cuenta la velocidad del internet.

11 LIMITACIONES

De las 18 empresas de atención de telefónica en el país con presencia en varias regiones, solo se logró acceder a información de cinco, debido a la relación previa y el conocimiento que los investigadores tenían con ellas. Esta elección, aunque facilitó el acceso a la información, puede haber restringido la variedad de datos obtenidos y la representatividad de los resultados en un contexto más amplio.

El prototipo desarrollado en esta investigación se construyó utilizando OpenStack 23.2, Ceph Quincy, OpenLDAP 2.5.8 y máquinas virtuales de Issabel 5 para el servicio de PBX. Es importante señalar que la documentación proporcionada es específica para las versiones mencionadas, lo que limita su aplicabilidad a otras versiones de estas herramientas. Por lo tanto, se requiere verificar la compatibilidad del prototipo con versiones alternativas.

La presente investigación se enfoca en la implementación de sistemas PBX en una nube geo-distribuida utilizando OpenStack. En este contexto, se omiten otros aspectos importantes de los PBX, como la tarificación de conexiones telefónicas, los componentes físicos y la conexión a la red móvil pública.

12 REFERENCIAS BIBLIOGRÁFICAS

- Adaptixnetworks. (s.f.). *Antecedentes de la Nube*. Recuperado el 4 de Mayo de 2024, de adaptix networks: <https://www.adaptixnetworks.com/antecedentes-la-nube/>
- Admin-Factoria. (30 de Marzo de 2022). *¿Cuáles son los perfiles Cloud más demandados en la actualidad?* Obtenido de Ausum Cloud: Servicios y Soluciones Cloud: <https://ausum.cloud/cuales-son-los-perfiles-cloud-mas-demandados-en-la-actualidad/>
- Akamai. (s.f.). Obtenido de Akamai: <https://www.akamai.com/es/glossary/what-is-a-distributed-cloud>
- Akamai. (2024). *¿Qué es cloud computing?* Obtenido de <https://www.akamai.com/es/glossary/what-is-cloud-computing>
- Alibaba Cloud Products & Services. (s.f.). Obtenido de Alibaba : https://www.alibabacloud.com/en/product?_p_lc=1
- Amazon. (s.f.). *Clústeres de base de datos de Amazon Aurora*. Obtenido de https://docs.aws.amazon.com/es_es/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html
- Amorín, D. (15 de Septiembre de 2016). *LinkedIn*. Obtenido de <https://es.linkedin.com/pulse/qu%C3%A9-es-la-centralita-virtual-historia-detr%C3%A1s-del-servicio-amor%C3%ADn>: <https://es.linkedin.com/pulse/qu%C3%A9-es-la-centralita-virtual-historia-detr%C3%A1s-del-servicio-amor%C3%ADn>
- App Engine. (s.f.). Obtenido de Google Cloud: <https://cloud.google.com/appengine>
- Arévalo Navarro, J. M. (2012). *Cloud Computing: fundamentos, diseño y*. Obtenido de Universidad Rey Juan Carlos: <https://burjcdigital.urjc.es/bitstream/handle/10115/5945/MemoriaTFMFINAL-2.pdf?sequence=1>
- AWS. (s.f.). Obtenido de Amazon Web Service: <https://aws.amazon.com/es/what-is/virtualization/>
- AWS - IAM Roles. (s.f.). *Amazon Web Services*. Obtenido de Amazon Web Services: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
- AWS - Zonas de disponibilidad y regiones. (s.f.). *Amazon Web Services*. Obtenido de Zonas de disponibilidad y regiones: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
- AWS Elastic Beanstalk. (s.f.). Obtenido de AWS: <https://aws.amazon.com/es/elasticbeanstalk/>
- Azure App Service. (s.f.). Obtenido de <https://azure.microsoft.com/en-us/products/app-service/>

- Azure, M. A.-M. (s.f). *Microsoft Learn*. Obtenido de <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-domains-manage>
- CISCO. (s.f.). *¿Qué es un sistema PBX?* Recuperado el 12 de 07 de 2024, de Cisco.com: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/collaboration/what-is-a-pbx.html
- Cisga. (s.f.). *¿Conoces el origen del cloud computing o nube informática?* Recuperado el 4 de Mayo de 2024, de Cisga innovación y servicios: <https://www.cisga.es/conoces-origen-del-cloud-computing-nube-informatica/#:~:text=El%20origen%20del%20Cloud%20Computing,-El%20origen%20del&text=Algunos%20expertos%20indican%20que%20fue,el%20concepto%20de%20inteligencia%20artificial.>
- Cloud Native DevSecOps Platform*. (s.f.). Obtenido de Cloudbees: <https://www.cloudbees.com/>
- CloudFlare. (s.f.). *CloudFlare*. Obtenido de <https://www.cloudflare.com/es-es/learning/access-management/what-is-identity-as-a-service/>
- Corbetta, P. (2007). *Metodología y Técnicas de Investigación Social*. Madrid: Mcgraw Hill.
- Dávalos, R. E. (06 de junio de 2014). *Cluster Bases de Datos*. Obtenido de <https://prezi.com/wds39vhg4frl/cluster-bases-de-datos/>
- Deploy and run apps on today's most innovative Platform as a Service*. (s.f.). Obtenido de Heroku: <https://www.heroku.com/platform>
- Digital Ocean*. (s.f.). Obtenido de <https://www.digitalocean.com/>
- Digital Ocean App Platform*. (s.f.). Obtenido de Digital Ocean: <https://www.digitalocean.com/products/app-platform>
- Documentation, R. (s.f.). *Capítulo 1. Visión general de adición de alta disponibilidad*. Obtenido de https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/6/html/high_availability_add-on_overview/ch.gfscs.cluster-overview-cso#ch.gfscs.cluster-overview-CSO
- Enterprise, A. (2023). *¿Qué es un servicio de imágenes?* Obtenido de <https://enterprise.arcgis.com/es/image/11.2/get-started/windows/what-is-an-image-service.htm>
- Escobar Gómez, J. J. (5 de Septiembre de 2007). *Sistemas de identidad federados en Openstack*. España: Universidad de la Laguna.
- Flores, F. (22 de Marzo de 2021). *Open Webinars*. Obtenido de Open Webinars: <https://openwebinars.net/blog/tipos-de-cloud-computing/>

- Galarza, B. Z. (Junio de 2015). Análisis de despliegue de una IaaS utilizando Openstack. *Congreso Argentino de Ciencias de la Computación*.
- García Orozco, D. (13 de Enero de 2020). OpenStack: una alternativa de Infraestructura como servicio para instituciones de educación superior . *Revista de Investigación en Tecnologías de la Información RITI*, 7. Obtenido de <https://dialnet.unirioja.es/descarga/articulo/7237680.pdf>
- García, M. (s.f.). *profmatiasgarcia*. Obtenido de <https://profmatiasgarcia.com.ar/uploads/tutoriales/Redes-9Servicios.pdf>
- Google - Ubicaciones de Google Cloud. (s.f.). *Ubicaciones de Google Cloud*. Obtenido de <https://cloud.google.com/about/locations?hl=es>
- Google Cloud*. (s.f.). Obtenido de <https://cloud.google.com/?hl=es>
- Google Cloud - Crear y administrar proyectos. (s.f.). *Google Cloud - Crear y administrar proyectos*. Obtenido de <https://cloud.google.com/resource-manager/docs/creating-managing-projects?hl=es-419>
- Google Cloud - IAM basic and predefined roles reference. (s.f.). *Google Cloud*. Obtenido de <https://cloud.google.com/iam/docs/understanding-roles>
- Google Cloud - Manejo de usuarios IAM en la nube . (s.f.). *Google Cloud - Manejo de usuarios IAM en la nube* . Obtenido de <https://cloud.google.com/iam/docs/>
- Hat, R. (s.f.). *Red Hat OpenShift*. Obtenido de <https://www.redhat.com/en/technologies/cloud-computing/openshift>
- IBM. (s.f.). *¿Qué es la nube distribuida?* Obtenido de IBM: <https://www.ibm.com/mx-es/topics/distributed-cloud>
- IBM Cloud*. (s.f.). Obtenido de <https://www.ibm.com/cloud/why-ibm>
- Kavis, M. J. (2014). *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*.
- Listado de Call centers*. (Agosto de 2019). Obtenido de English4CallCenters: <https://english4callcenters.com/student/wp-content/uploads/2019/08/Call-Centers-addresses.pdf>
- Ma, D. (Julio de 2007). The business model of" software-as-a-service. *Ieee international conference on services computing*. Obtenido de https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1571&context=sis_research
- Manchola, K. S. (5 de Abril de 2017). *slideshare*. Obtenido de slideshare: <https://es.slideshare.net/slideshow/ciclo-hermeneutico/74493201#2>

- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud*. Obtenido de <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
- Merizalde Almeida, N. A. (2017). Estudio y clasificación de características y atributos de servicios cloud para la definición de un modelo de valor para servicios cloud.
- Microsoft Azure - Manejo de usuarios y accesos en Azure. (s.f.). *Microsoft Azure - Manejo de usuarios y accesos en Azure*. Obtenido de <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-manage>
- Microsoft. (s.f.). *Paneles de control de servicios hospedados*. Obtenido de <https://learn.microsoft.com/es-es/iis/manage/provisioning-and-managing-iis/hosted-services-control-panels>
- Networks, E.-d. (12 de Enero de 2021). *Conoce qué es la nube distribuida y cuáles son los tipos que existen*. Recuperado el 12 de Mayo de 2024, de E-dea Networks: <https://www.e-dea.co/blog/que-es-la-nube-distribuida>
- Openstack. (s.f.). *OpenStack Documentation*. Recuperado el 12 de Mayo de 2024, de Openstack: <https://docs.openstack.org/2024.1/>
- Productos de Azure*. (s.f.). Obtenido de Azure: <https://azure.microsoft.com/es-es/products>
- Ramón, M. (17 de Agosto de 2022). *Listado de Call Centers en El Salvador para conseguir trabajo*. Obtenido de SV El Salvador: <https://svelsalvador.com/listado-de-call-centers-trabajo/>
- Red Hat*. (23 de Marzo de 2023). Obtenido de Red Hat: <https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor>
- Red Hat OpenShift*. (s.f.). Obtenido de Red Hat OpenShift: <https://www.redhat.com/en/technologies/cloud-computing/openshift>
- RedHat. (10 de julio de 2023). *Servicios de nube gerenciados*. Obtenido de <https://www.redhat.com/es/topics/cloud-computing/what-are-cloud-services>
- Rguez, I. H. (17 de enero de 2016). *Gestión de Claves en la Cloud Computing*. Obtenido de <https://nube.villanett.com/2016/01/17/gestion-de-claves-en-la-cloud-computing/>
- Rodier, R. (16 de Noviembre de 2021). *The History of VoIP: From IP-PBX to Hosted PBX to UCaaS*. Obtenido de Lightyear: <https://lightyear.ai/blogs/the-history-of-voip-hosted-pbx-to-ucaas>
- Sales Force*. (s.f.). Obtenido de Sales Force: <https://www.salesforce.com/mx/cloud-computing/>
- Salesforce. (s.f.). *¿Qué es Cloud Computing?* Recuperado el 4 de Mayo de 2024, de Salesforce: <https://www.salesforce.com/mx/cloud-computing/>

Sandhu, R. C. (1996). *Role-Based Access Control Models*.

Services, A. W. (s.f.). *¿Qué es Amazon EC2?* Recuperado el 4 de Mayo de 2024, de Amazon Web Services:

https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html

Silva, D. d. (19 de Septiembre de 2023). *Zendesk*. Obtenido de

<https://www.zendesk.com.mx/blog/call-center-historia/>

The Heroku Platform. (s.f.). Obtenido de Heroku : <https://www.heroku.com/platform>

TRABAJOS EN Call Center EN El Salvador. (s.f.). Recuperado el 7 de Septiembre de 2024, de Tecoloco: <https://www.tecoloco.com.sv/trabajo-call-center>

Vera-Rivera, F. H., & Gaona Cuevas, C. M. (2017). *PLATAFORMA COMO SERVICIO – PAAS PARA LA GESTIÓN DE TECNOLOGÍAS EN*. Calí: Universidad del Valle, Universidad Francisco de Paula Santander.

Vercel. (s.f.). Obtenido de <https://vercel.com/>

Villamizar de Camperos, Y. (s.f.). *Pasos para hacer análisis hermenéutico*. Obtenido de Universidad de Pamplona: <https://pdfcoffee.com/pasos-para-hacer-analisis-hermeneutico-gadamer-pdf-free.html>

Vultr - The Everywhere Cloud. (s.f.). Obtenido de Vultr: <https://www.vultr.com/>

13 ANEXOS

- Anexo 1: Listado de empresas que brindan servicio de atención telefónica (Call Center).
- Anexo 2: Encuesta de exploración de soluciones en la nube en empresas de atención telefónica.
- Anexo 3: Entrevista de exploración de soluciones en la nube en empresas de atención telefónica.
- Anexo 4: Transcripción de entrevista
- Anexo 5: Resultados de pruebas de la capacidad operativa del servidor de PBX
- Anexo 6: Documento HLD
- Anexo 7: Documento LLD

13.1 Anexo 1: Listado de empresas que brindan servicio de atención telefónica (Call Center).

NOMBRE	Zona Geográfica	Nº Sucursales	URL
1. AMERICATEL CALL CENTER S.A. DE C.V.	El Salvador	1	Sitio Web
2. ATENTO	El Salvador / Internacional	Más de 2	Sitio Web
3. BENSON COMMUNICATIONS S.A. DE C.V.	El Salvador	1	Sitio Web
4. BLACKHAWK SUPPORT SERVICES	El Salvador	1	Sitio Web
5. BPC	El Salvador	1	Sitio Web
6. CENTERCOM GLOBAL BPO	El salvador	1	Sitio Web
7. COGNIZANT	El Salvador / Internacional	Más de 2	Sitio Web
8. COMDATA	El Salvador	1	Sitio Web
9. CONCENTRIX	El Salvador / Internacional	Más de 2	Sitio Web
10. CONNECTING S.A DE C.V.	El Salvador	1	Sitio Web
11. FOCUS SERVICES LLC	El Salvador / Internacional	Más de 2	Sitio Web
12. FUSION BPO SERVICES	El Salvador / Internacional	Más de 2	Sitio Web
13. GLASS MOUNTAIN BPO	El Salvador / Internacional	2	Sitio Web
14. GLOBE TECH INDUSTRIES	El Salvador	1	Sitio Web
15. INDIGO	El Salvador	1	Sitio Web
16. MANPOWER GROUP	El Salvador / Internacional	Más de 2	Sitio Web
17. NEBO BPO	El Salvador / Internacional	2	Sitio Web
18. NEW PEOPLE	El Salvador	1	Sitio Web

19. WEBHELP ONELINK	El Salvador / Internacional	Más de 2	Sitio Web
20. OSI OUTSOURCING SERVICES INTERNATIONAL (OSI)	El Salvador / Internacional	2	Sitio Web
21. PERFORMATTEL	El Salvador / Internacional	2	Sitio Web
22. PROFESSIONAL TELESALLES S.A. DE C.V.	El Salvador	1	Sitio Web
23. RISTEL	El Salvador	1	Sitio Web
24. SKYCOM	El Salvador / Internacional	2	Sitio Web
25. STREAM GLOBAL SERVICES	El Salvador	1	Sitio Web
26. SYKES	El Salvador / Internacional	Más de 2	Sitio Web
27. TALK AMERICAS	El Salvador	1	Sitio Web
28. TECH AMERICAS S.A. DE C.V.	El Salvador / Internacional	2	Sitio Web
29. TELECEL CONTACT CENTER	El Salvador	1	Sitio Web
30. TELEPERFORMANCE	El Salvador / Internacional	Más de 2	Sitio Web
31. TELUS	El Salvador / Internacional	Más de 2	Sitio Web
32. THE OFFICE GURUS	El Salvador / Internacional	Más de 2	Sitio Web
33. UBIQUITY GLOBAL SERVICES	El Salvador / Internacional	Más de 2	Sitio Web
34. WINGMAN	El Salvador	1	Sitio Web
35. YELLOWBERRY HUB	El Salvador	1	Sitio Web

13.2 Anexo 2: Guía de Encuesta.

Descripción: La siguiente encuesta tiene como propósito recolectar información sobre las tendencias para adoptar soluciones en la nube en el sector de las empresas del área de atención telefónica. Deseamos comprender mejor, cómo estas tecnologías están siendo utilizadas para mejorar la calidad de los servicios ofrecidos. Su respuesta nos permitirá identificar las principales áreas de interés y desarrollo, siendo clave para obtener una visión completa del estado actual y del potencial futuro de estas tecnologías en el ámbito empresarial.

Indicaciones: Responder las siguientes preguntas según la situación actual de su organización.

Preguntas:

1. ¿Conoce si la nube puede mejorar las operaciones internas de una empresa?

- Sí.
- No.

2. ¿Qué tipo infraestructura utilizan para brindar los servicios?

- Nube pública.
- Nube privada.
- Nube mixta.
- Desconozco.

3. ¿Cuáles de las siguientes infraestructuras de nubes utiliza su empresa?

- AWS
- Google Cloud
- AZURE
- Digital Ocean

- Heroku
- Vultr
- Alibaba Cloud
- Otra
- Ninguna

4. ¿Cuáles de los siguientes servicios en la nube utiliza su empresa?

- Almacenamiento
- Bases de datos
- Virtualización de servidores
- Contenedores
- Redes y CDN
- Otros
- Ninguno

5. ¿Qué medidas de seguridad implementan para resguardar los datos?

- Cifrado de datos en tránsito y en reposo
- Autenticación multifactor (MFA)
- Gestión de identidades y accesos (IAM)
- Monitoreo y detección de intrusos
- Copia de seguridad regular y automatizada
- Firewalls y segmentación de red
- Planes de recuperación ante desastres
- Control de acceso basado en roles (RBAC)
- Auditorías y revisiones de seguridad periódicas.

- Otra

6. ¿Qué medidas de contingencia utilizan para garantizar la alta disponibilidad y continuidad operativa de sus servicios?

- Redundancia de datos
- Backups automatizados
- Alertas en tiempo real
- Escalabilidad automática
- Failover automático
- Segmentación de la red
- Otra

7. ¿Qué nivel de relevancia asigna su empresa a la adopción de tecnologías actuales en infraestructuras de nube?

- Alto
- Medio
- Bajo

13.3 Anexo 3: Guía de Entrevista.

Objetivo: Analizar el contexto y las expectativas de las empresas del sector de atención telefónica, en la adopción de una infraestructura en la nube para ofrecer servicios de llamadas, explorando su experiencia con el servicio actual y su percepción sobre los servicios en la nube, con el fin de identificar los factores que influyen en su incorporación tecnológica, así como las barreras y beneficios percibidos.

1. ¿Cómo describiría el desempeño de la infraestructura tecnológica actual para el servicio de llamadas?
2. ¿Su empresa ha hecho uso de infraestructuras de nube, como los son AWS, Azure, Google Cloud?
3. ¿Qué elementos considera prioritarios para su empresa al evaluar la adopción de nuevas tecnologías?
4. ¿Cuáles son o han sido las principales dificultades a las que se han enfrentado al momento de implementar una infraestructura en la nube?
5. ¿Cómo describe las experiencias ha tenido su empresa utilizando infraestructuras o servicios en la nube?
6. ¿Cuáles son las expectativas que tiene con respecto a la adopción de una infraestructura en la nube para el servicio de llamadas telefónicas?

13.4 Anexo 4: Transcripción de Entrevista

Entrevista a Gerente de operaciones de Cliente de Teleperformance

Entrevista a: Msc. Jose Luis Munguia

Realizada: 29 de septiembre de 2023

Hora de inicio: 16:00

Duración: 10:45 minutos

Lugar: Sala de videoconferencias Google Meet

Isaí: Buen día, José Luis. Para iniciar, le agradecemos que haya apartado el tiempo para hablar con nosotros este día. El objetivo de la entrevista es conocer las expectativas que pueden tener las empresas como Teleperformance con respecto a la adopción una infraestructura en la nube para alojar e implementar un servicio de llamadas.

Con esto en mente, ¿cómo describiría el desempeño de la infraestructura tecnológica actual para este servicio?

José Luis: Buen día, gracias a ustedes por la invitación. Para responder a la pregunta, me parece que la mejor forma de describir el desempeño actual de nuestra infraestructura es como eficiente, no tenemos quejas.

Isaí: ¿Su empresa ha hecho uso de infraestructuras en la nube como AWS, Azure o Google Cloud?

José Luis: Sí, actualmente utilizamos las tres mencionadas. AWS, Azure y Google Cloud nos brindan la flexibilidad y escalabilidad que necesitamos para nuestras operaciones globales.

Isaí: ¿Qué elementos considera prioritarios para su empresa al evaluar la adopción de nuevas tecnologías?

José Luis: Los elementos prioritarios para nosotros son los beneficios que la nueva tecnología puede aportar, la seguridad que garantice la protección de los datos, los costos asociados y, por supuesto, la mejora en la productividad.

Isaí: ¿Cuáles cree que son los principales obstáculos que podrían dificultar la implementación de una infraestructura en la nube en su empresa?

José Luis: Las principales barreras estarían relacionadas con la adaptabilidad y la capacitación del personal para el uso de nuevas herramientas, sobre todo debido a la alta cantidad de empleados con los que contamos. Es retador asegurar que todos puedan manejar eficientemente las nuevas herramientas.

Isaí: ¿Qué describe las experiencias que ha tenido su empresa utilizando infraestructuras o servicios en la nube?

José Luis: En general ha sido muy positiva, tanto desde la perspectiva de nuestros clientes externos como de nuestros equipos internos. La nube nos ha permitido ser más ágiles.

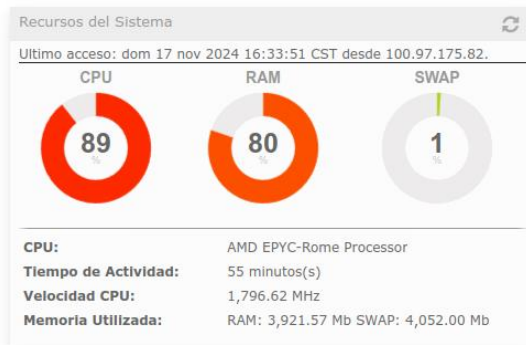
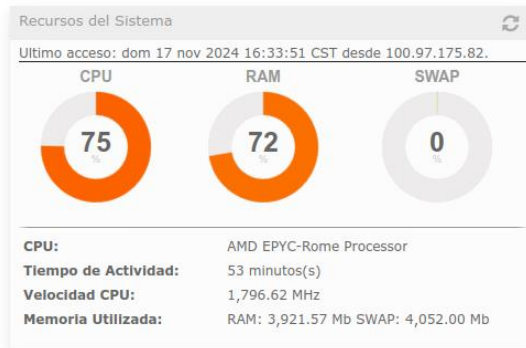
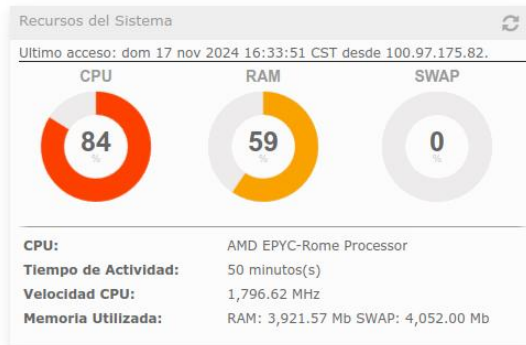
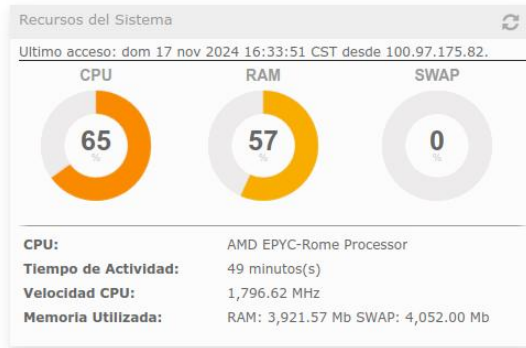
Isaí: ¿Cuáles son sus expectativas respecto a la adopción de una infraestructura en la nube para el servicio de llamadas telefónicas?

José Luis: Esperamos que la adopción de una infraestructura en la nube nos permita seguir innovando y mejorando continuamente.

Isaí: Muchas gracias, José Luis, por compartir su experiencia y perspectivas sobre la adopción de tecnologías en la nube en el sector de atención telefónica.

José Luis: Ha sido un placer. Gracias a ustedes.

13.5 Anexo 5: Resultados de pruebas de la capacidad operativa del servidor de PBX



**UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA**

**DOCUMENTO DE DISEÑO DE ALTO NIVEL
HIGH LEVEL DESIGN DOCUMENT**

**PROTOTIPO DE INFRAESTRUCTURA DE NUBE GEO-DISTRIBUIDA,
ORIENTADO A EMPRESAS QUE REQUIEREN SERVICIOS DE PBX**

NOVIEMBRE 2024

VERSIÓN 3.0 27/10/2024

TABLA DE CONTENIDO

1	Introducción	3
2	Objetivos	4
2.1	General	4
2.2	Específicos	4
3	Arquitectura de la infraestructura	5
3.1	Servicio de cola de mensajes.....	5
3.2	Servicio de base de datos.	6
3.3	Servicio de almacenamiento.....	6
3.4	Panel de administración.	6
3.5	Controlador regional	6
3.6	Nodos compute regionales	6
4	Topología de red de la infraestructura	7
5	Descripción de caso	8

1 INTRODUCCIÓN

El presente documento muestra el diseño de un prototipo de infraestructura en la nube geo-distribuida que es capaz de gestionar múltiples regiones geográficas. Estas regiones se integran para formar una nube comunitaria, donde los recursos se comparten de manera eficiente y, al mismo tiempo, pueden consumir los servicios proporcionados por la infraestructura central.

La solución se basa en OpenStack, una plataforma de código abierto reconocida en el ámbito de la computación en la nube. En esta implementación, la infraestructura principal está compuesta por varios componentes esenciales, distribuidos en clústeres para garantizar su escalabilidad.

Cada región conectada a esta infraestructura principal contiene su propio Controlador y varios nodos de Cómputo, lo que permite ejecutar cargas de trabajo locales y distribuidas. Este diseño asegura una infraestructura robusta y flexible, capaz de escalar horizontalmente agregando más regiones cuando sea necesario, manteniendo alta disponibilidad y redundancia geográfica.

A lo largo de este documento, se detallarán los aspectos técnicos de esta arquitectura, así como los pasos necesarios para implementar esta solución de manera efectiva. El objetivo es proporcionar una guía clara para replicar este prototipo y asegurar su operación óptima en un entorno de nube comunitaria.

2 OBJETIVOS

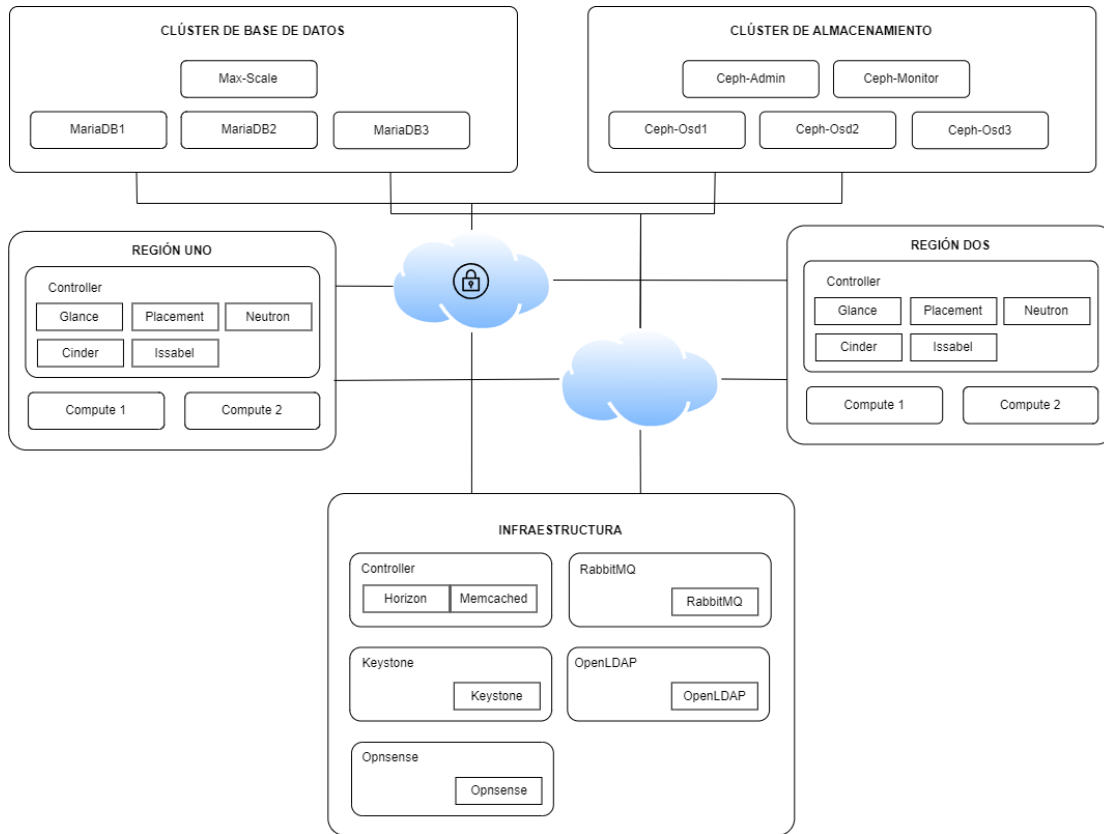
2.1 General

Presentar un diseño de alto nivel (High-Level Design) que describa la arquitectura y los componentes clave de una solución de nube geo distribuida basada en OpenStack

2.2 Específicos

- Describir la arquitectura general de la solución OpenStack multirregión, explicando la distribución de los componentes críticos (controlador, identidad, base de datos, almacenamiento y cómputo) en una configuración geo distribuida.
- Definir los componentes clave del sistema y sus interacciones a nivel de red, almacenamiento, autenticación y cómputo.
- Documentar el diseño de la conectividad de red entre las regiones distribuidas en distintas ubicaciones geográficas, especialmente con mecanismos de seguridad e interconexión.

3 ARQUITECTURA DE LA INFRAESTRUCTURA



La infraestructura está dividida en tres regiones diferentes: la región principal llamada "Infraestructura" y dos regiones adicionales denominadas "Región Uno" y "Región Dos". La región de Infraestructura se encarga de proporcionar servicios a las demás regiones a través de diversas APIs. Los servicios ofrecidos desde la región de Infraestructura son:

3.1 Servicio de cola de mensajes.

Se implementa mediante RabbitMQ, este servicio facilita la comunicación entre las diferentes regiones, gestionando los eventos de manera eficiente y asegurando una comunicación asíncrona y confiable.

3.2 Servicio de base de datos.

Se proporciona a través de un clúster de MariaDB, este servicio ofrece una base de datos centralizada que da soporte a todas las regiones, garantizando una gestión eficiente y unificada de los datos.

3.3 Servicio de almacenamiento.

Se implementa mediante un clúster de Ceph, este servicio proporciona almacenamiento centralizado para todas las regiones, asegurando la disponibilidad y escalabilidad de los datos.

3.4 Panel de administración.

Se provee a través del componente Horizon de OpenStack, este panel permite la gestión de los recursos en cada región. La administración de usuarios se realiza mediante el componente Keystone de OpenStack, que se integra con un servicio LDAP para el aprovisionamiento de usuarios federados en todas las regiones.

3.5 Controlador regional

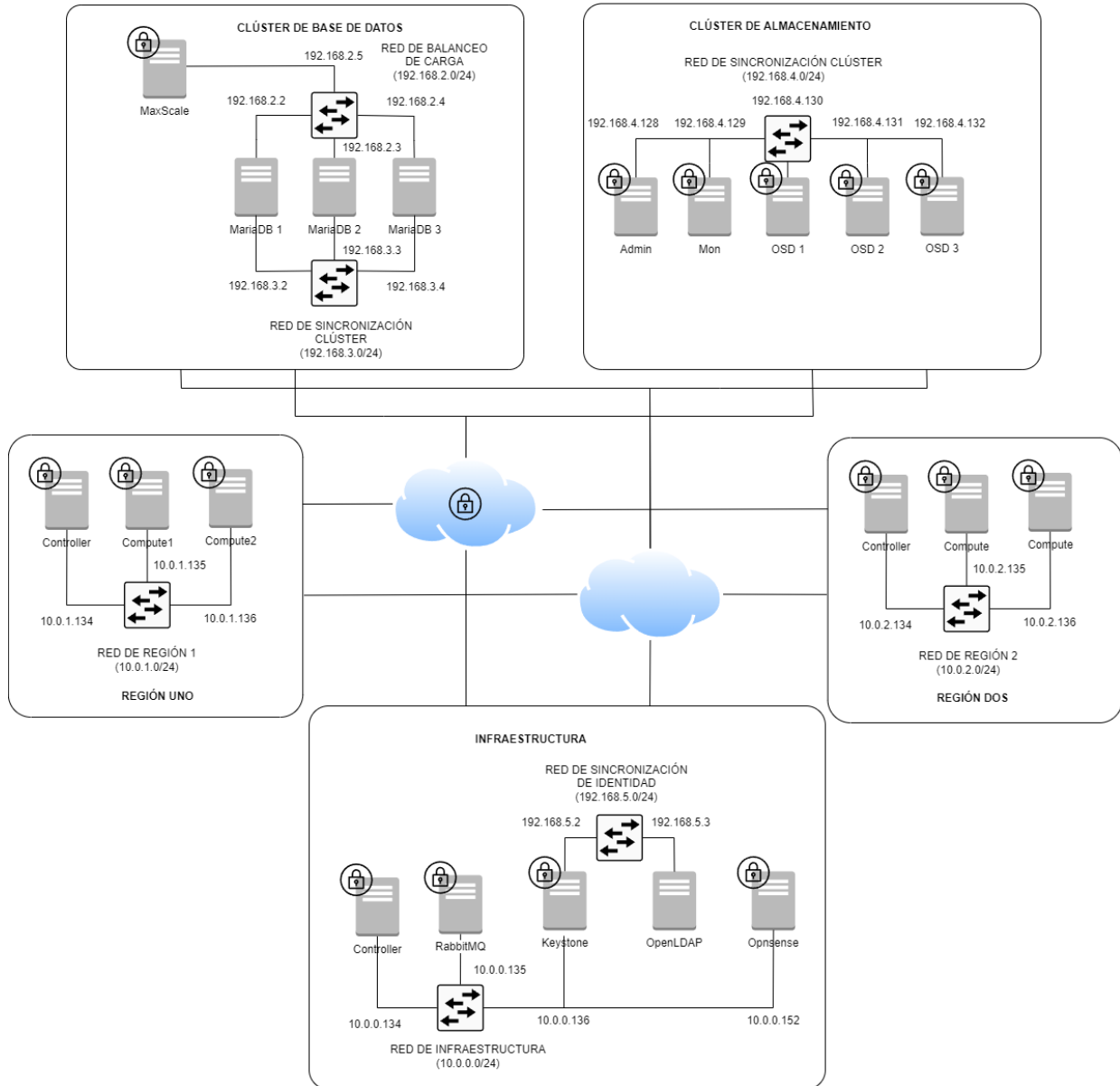
Cada región tiene su propio controller el cual está enfocado en la orquestación local de recursos, como instancias de cómputo (VMs), redes locales y almacenamiento temporal. Sin embargo, componentes clave como la mensajería interna (RabbitMQ), el cacheo de datos (Memcached), la interfaz de gestión web (Horizon) y la base de datos relacional, son consumidos directamente desde la región central.

3.6 Nodos compute regionales

Los nodos de cómputo de cada región distribuyen y ejecutan las cargas de trabajo localmente, gestionando instancias de VMs, redes y almacenamiento temporal. Sin embargo, dependen de la región central para servicios críticos, como la autenticación de usuarios

(Keystone), mensajería (RabbitMQ), bases de datos (MariaDB) y almacenamiento persistente (Ceph).

4 TOPOLOGÍA DE RED DE LA INFRAESTRUCTURA



La infraestructura de red está conformada por una topología de red en función de redes específicas. Cada región está conectada a una red principal, que se encarga de interconectar todos los componentes y está expuesta a Internet para permitir el acceso a los servicios públicos.

El clúster de base de datos está compuesto por dos redes distintas. La primera red se utiliza para gestionar el balanceo de carga entre MaxScale y cada uno de los nodos de la base de datos, mientras que la segunda red está dedicada a la sincronización de la información entre los nodos. Por otro lado, el clúster de Ceph cuenta con una red específica para la sincronización entre los nodos del clúster. Además, esta red permite el monitoreo de los recursos en el nodo de monitor y en los nodos de almacenamiento.

El servicio de identidad, proporcionado por OpenStack, utiliza una red particular para que el componente Keystone se comuniquen con el servicio LDAP, el cual se encarga de la gestión de los usuarios federados.

Finalmente, se ha implementado una red privada virtual (VPN) para garantizar que los servicios de la región principal sean accesibles desde cada una de las regiones que conforman la infraestructura.

5 DESCRIPCIÓN DE CASO

El caso de estudio explora el diseño y la configuración de un prototipo de infraestructura de nube geo-distribuida, destinada a empresas que utilizan servicios de PBX y operan en múltiples zonas geográficas. La infraestructura propuesta debe ser escalable, ofrecer servicios a usuarios federados, garantizar la persistencia de sesiones y proporcionar una base de datos como servicio. Además, debe contar con una interfaz web que permita gestionar las diferentes regiones, facilitando a los centros de llamadas el control del flujo de comunicaciones entre las diversas zonas operativas de la empresa, asegurando así la continuidad del negocio.

El centro de datos central, el cual nombramos como “INFRAESTRUCTURA”, actúa como el núcleo y proporciona los servicios fundamentales para gestionar la nube utilizada por los

centros de llamada en cada región. Este centro de datos está formado por cuatro clústeres, cada uno con una responsabilidad clave:

La región de infraestructura se encarga de coordinar todos los servicios de la nube, utiliza RabbitMQ para asegurar una comunicación fluida entre los diferentes componentes de OpenStack, lo que permite integrar los diferentes nodos de computación distribuidos en las diferentes regiones. Además, proporciona autenticación y autorización centralizada para los usuarios y servicios a través de KeyStone y OpenLDAP. Estos servicios aseguran que los usuarios puedan acceder a los servicios de la nube en cada una de las regiones, garantizando la seguridad y el control de acceso a los servicios necesarios para montar los sistemas de PBX.

El clúster de base de datos está compuesto por múltiples instancias de MariaDB y un balanceador MaxScale, lo que garantiza una alta disponibilidad de los datos críticos, además de permitir el manejo y procesamiento de la información en cada región de la nube."

El clúster de almacenamiento, basado en Ceph, ofrece almacenamiento y redundancia de datos a cada una de las regiones. Esto permite que cada nodo compute acceda a los datos de forma rápida y segura.

Cada región está compuesta por sus propios controllers locales y dos nodos compute, lo que permite que las cargas de trabajo se gestionen localmente, minimizando la latencia. Sin embargo, dependen de la sede principal para servicios críticos como la autenticación y la replicación de datos, lo que permite alta disponibilidad en toda la infraestructura.

La comunicación entre cada nodo de la infraestructura se realiza a través de la VPN Tailscale, lo que garantiza el intercambio de paquetes entre cada región de forma segura y encriptada.

Para este caso de estudio, se considera una empresa de centros de atención telefónica con dos sucursales: una en Guatemala y otra en El Salvador. La compañía cuenta también con una sede central, ubicada en otra área de El Salvador, donde se alojan los recursos principales para ofrecer el servicio a las sucursales. Cada sucursal dispone de su propio servicio de PBX, alojado en una infraestructura de nube geo-distribuida, a través de la cual los clientes pueden comunicarse con la sucursal de su elección. De igual manera, las sucursales pueden comunicarse entre sí.

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA

DOCUMENTO DE DISEÑO DE BAJO NIVEL
LOW LEVEL DESIGN DOCUMENT

PROTOTIPO DE INFRAESTRUCTURA DE NUBE GEO-DISTRIBUIDA,
ORIENTADO A EMPRESAS QUE REQUIEREN SERVICIOS DE PBX

NOVIEMBRE 2024

VERSIÓN 3.0 27/10/2024

TABLA DE CONTENIDO

1	Introducción	3
2	Objetivos	4
2.1	Objetivo general	4
2.2	Objetivos específicos.....	4
3	Configuraciones Iniciales.....	5
3.1	KVM (Kernel-base Virtual Machine)	5
3.2	Instalación de Virt-Manager.....	5
3.3	Creación de redes virtuales	6
3.4	Creación de máquinas virtuales.....	8
3.5	Configuración de la VPN	14
4	Configuración de Componentes.....	16
4.1	Clúster de base de datos	16
4.2	Configuración de balanceador MaxScale.....	19
4.3	Clúster de almacenamiento	22
4.3.1	Instalación de Docker	25
4.3.2	Configuración del servicio	25
4.3.3	Configuración del clúster Ceph	26
4.3.4	Registro de nodos para incluirlos en el clúster	27
4.3.5	Inflando el clúster	28
5	Configuración de la Región Principal.....	29
5.1	Configuración del módulo controller	29

5.1.1	Configuración del controller	30
5.1.2	Configuración de RabbitMQ.....	32
5.2	Configuración de módulo identidad.....	33
5.2.1	Configuración del servicio de Keystone	34
5.2.2	Configuración del servicio LDAP	36
5.3	Configuración del módulo de monitoreo	43
5.3.1	Instalación de OPNSense	43
5.3.2	Integración de OPNsense con la VPN de Tailscale.....	47
6	Conectar Regiones a la región principal	48
6.1	Controller	49
6.2	Nodos compute.....	49
6.3	Configurar nodos para consumir Ceph.....	49
6.4	Configuración de Cinder.	50
6.5	Conectar regiones.....	54
6.5.1	Glance	54
6.5.2	Placement.....	55
6.5.3	Nova.....	56
6.5.4	Neutron	57
6.5.5	Horizon	57
7	Configuración del servicio de PBX.	58

7.1	Instalación del servidor de Issabel en cada región.	58
-----	--	----

1 INTRODUCCIÓN

El despliegue de una infraestructura de cloud requiere de una correcta configuración de todos los elementos o herramientas que formaran parte de la solución. En el presente documento se detallará los pasos a seguir para realizar la correcta configuración de un prototipo de nube geo-distribuida. Se mostrará una descripción de cada una de las configuraciones de las máquinas virtuales utilizadas con los requerimientos necesarios para su despliegue, así como la configuración de las redes para poder comunicar las regiones. En el presente trabajo se mostrará la configuración de los servicios utilizados para la comunicación de las regiones a utilizar, tomando en cuenta que se hará uso de una región principal y dos regiones secundarias ubicadas en zonas geográficas distintas.

Cada una de las máquinas virtuales requiere tener instalados ciertos servicios que nos permitirán desplegar de forma correcta OpenStack, por lo que en este documento se describe cada uno de los servicios empleados y los parámetros de configuración que se utilizaron. Para un mejor detalle de cada una de las configuraciones, el documento cuenta con las ilustraciones y comandos empleados durante el despliegue de la infraestructura.

2 OBJETIVOS

2.1 Objetivo general

Presentar un diseño de bajo nivel (Low-Level Design) que describa la configuración necesaria de los componentes clave de una solución de nube geo distribuida basada en OpenStack.

2.2 Objetivos específicos

- Indicar la configuración necesaria para el entorno de virtualización inicial de un prototipo de infraestructura de nube geo distribuida.
- Explicar la configuración necesaria para implementar un clúster de base de datos en una infraestructura de nube geo distribuida.
- Mostrar la configuración necesaria para desplegar un clúster de almacenamiento en una infraestructura de nube geo distribuida.
- Indicar la instalación de cada uno de los servicios utilizados para el despliegue de OpenStack.
- Explicar la configuración de más de una región en distintas ubicaciones y su incorporación a la infraestructura final.
- Mostrar la configuración necesaria para desplegar un servicio de PBX, para una infraestructura de nube geo distribuida.

3 CONFIGURACIONES INICIALES

Para las configuraciones especificadas en esta guía, se han realizado sobre el sistema operativo Ubuntu 22.04. Antes de iniciar deberá actualizar todos los paquetes.

```
sudo apt update && sudo apt upgrade -y
```

3.1 KVM (Kernel-base Virtual Machine)

Primero verificamos si el procesador soporta la virtualización.

```
kvm-ok
```

Se instalan los paquetes que permiten gestionar KVM.

```
sudo apt -y install bridge-utils cpu-checker libvirt-clients libvirt-daemon qemu qemu-kvm bridge-utils
```

3.2 Instalación de Virt-Manager

Se instala la interfaz gráfica para poder gestionar las máquinas virtuales.

```
sudo apt install virt-manager
```

Se habilita el servicio libvirt para la administración de los recursos de virtualización.

```
sudo systemctl enable libvirtd --now && sudo systemctl start libvirtd
```

Se verifica el estado del servicio libvirtd, que se encuentre corriendo.

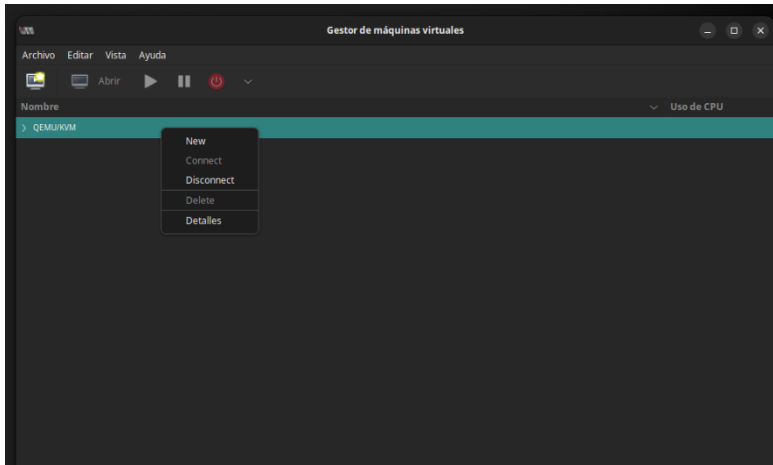
```
sudo systemctl status libvirtd
```

Se agrega el usuario actual al grupo kvm y libvirt, para que tenga acceso a la interfaz gráfica.

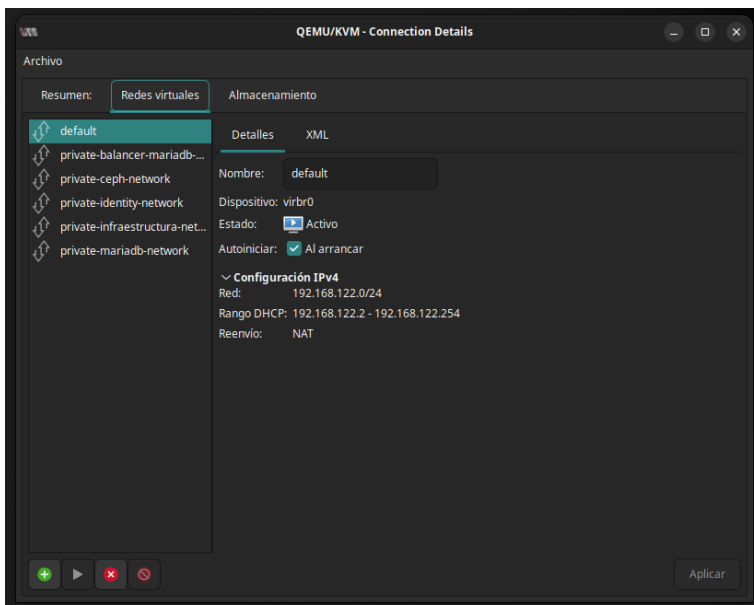
```
sudo usermod -aG kvm $USER && sudo usermod -aG libvirt $USER
```

3.3 Creación de redes virtuales

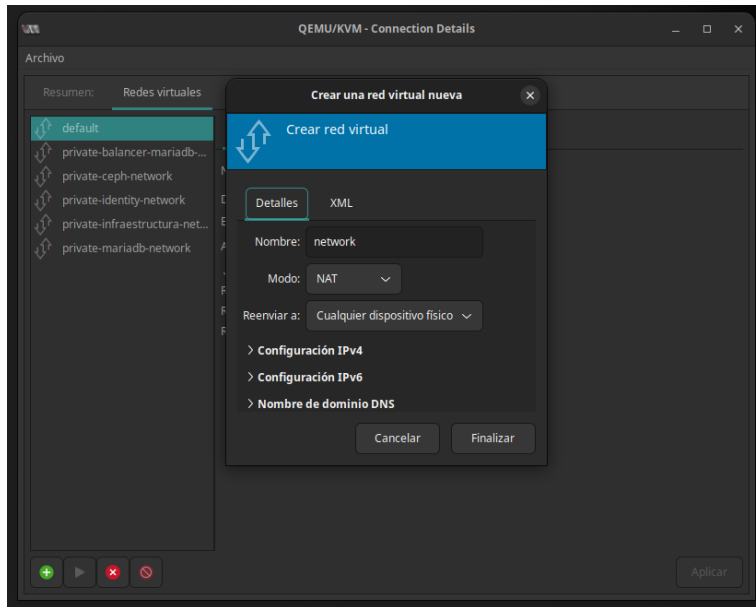
Accedemos a Virt Machine Manager y seleccionamos la conexión “QEMU/KVM” y hacemos clic derecho sobre esta, y seleccionamos del menú la opción “Detalles”.



Se abre una nueva ventana para gestionar las redes virtuales, donde se encuentra listada la red creada por defecto. En la esquina inferior izquierda se encuentran los botones para gestionar las redes virtuales, para agregar una nueva red debemos seleccionar el botón con signo “+”. Junto a él se encuentran los botones que permiten gestionar el inicio de una red, detener una red, y eliminar una red.



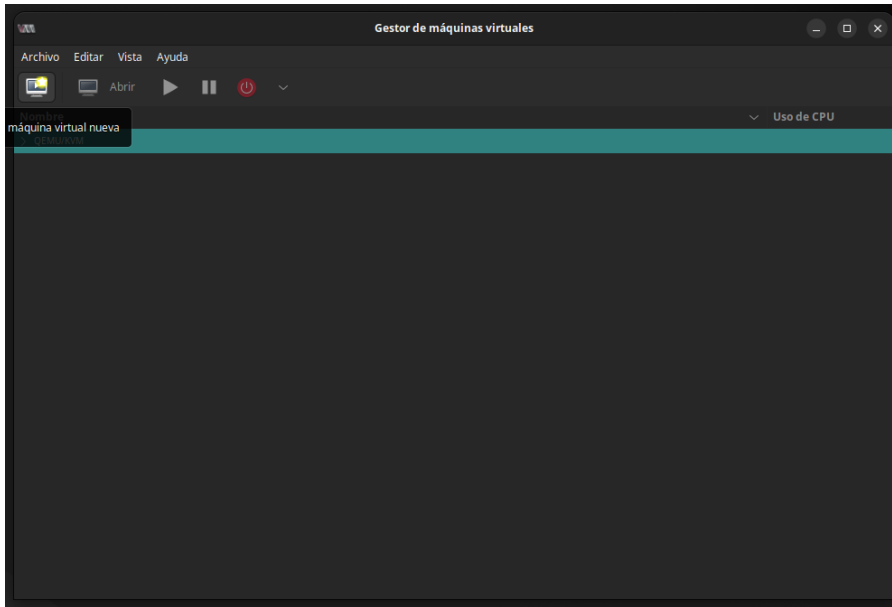
Al seleccionar el botón para agregar una nueva red, se abre una ventana donde podremos indicar el nombre de la red, el tipo de conexión a utilizar, el tipo de redirección, la configuración de los protocolos IPV4 y IPV6 con sus respectivos rangos de direcciones.



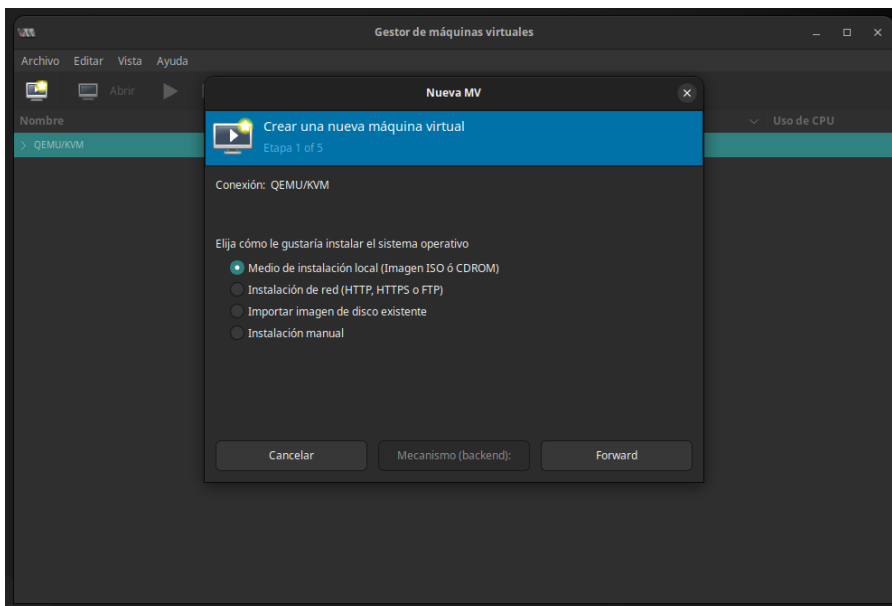
Cuando ya se hayan terminado de completar los parámetros de configuración de la red, presionamos el botón con nombre “Finalizar” para crear la red.

3.4 Creación de máquinas virtuales

Para crear máquinas virtuales hacemos clic en el icono de monitor en la esquina superior izquierda.

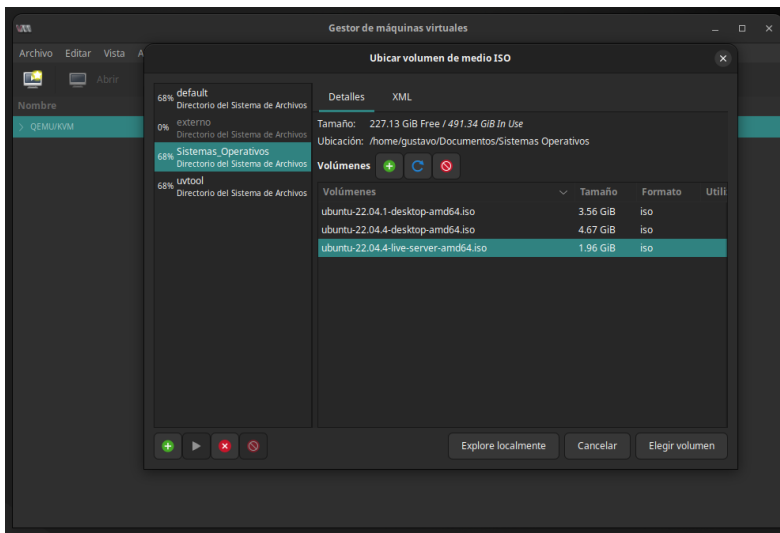


Se abrirá una ventana donde seleccionamos la forma en que se creará la máquina virtual, para nuestro caso seleccionaremos la opción de Instalación Local vía imagen ISO o CDROM y hacemos clic en el botón con nombre “Siguiente”.

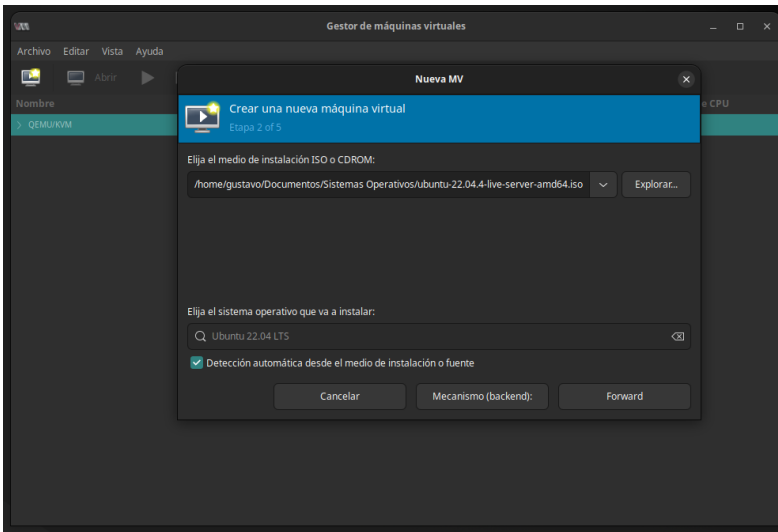


A continuación, debemos indicar la imagen ISO o la unidad de CD para realizar la instalación.

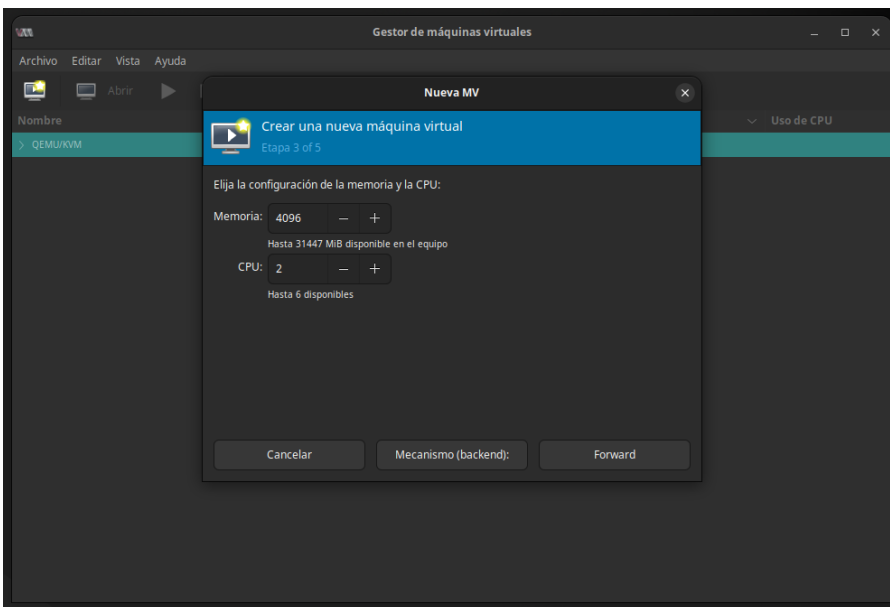
Para poder seleccionar la imagen ISO ya se cuenta con un directorio predeterminado para alojar los archivos de imágenes, sin embargo, podemos agregar otro directorio haciendo clic en el botón con signo “+” de la esquina inferior izquierda. Junto a él se encuentran los botones que permiten gestionar los directorios.



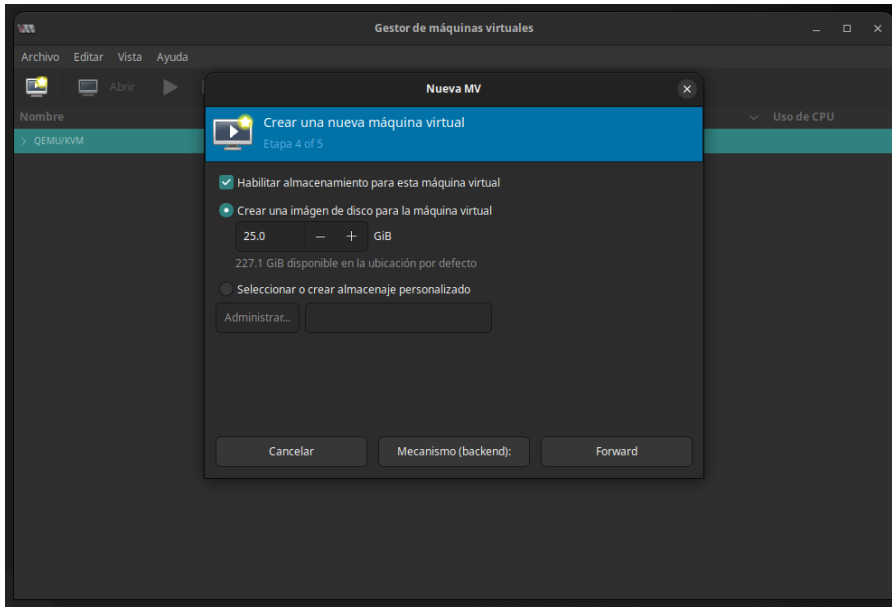
Cuando ya tengamos el directorio agregado podemos seleccionar la imagen ISO y luego hacer clic sobre el botón con nombre “Elegir volumen” para agregar la imagen ISO a la máquina virtual, y hacemos clic en el botón con nombre “Siguiente”.



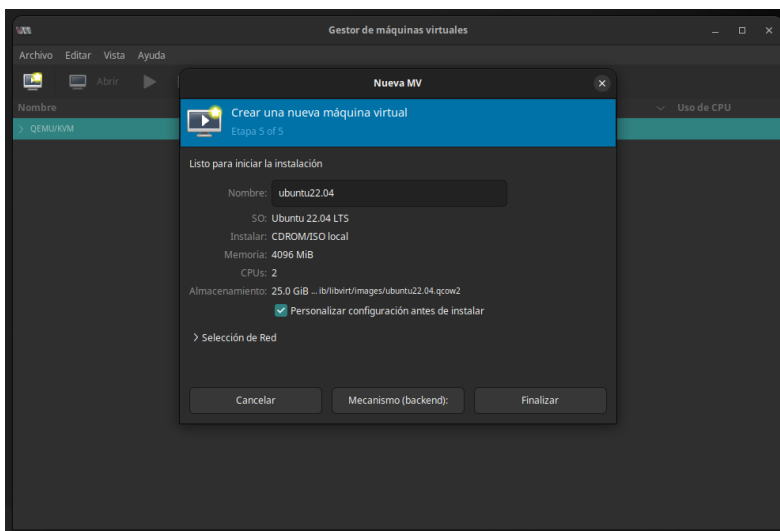
Se seleccionan los recursos de la máquina virtual indicando la cantidad de memoria RAM y CPUs, luego de indicarlo hacemos clic en el botón con nombre “Siguiente”.



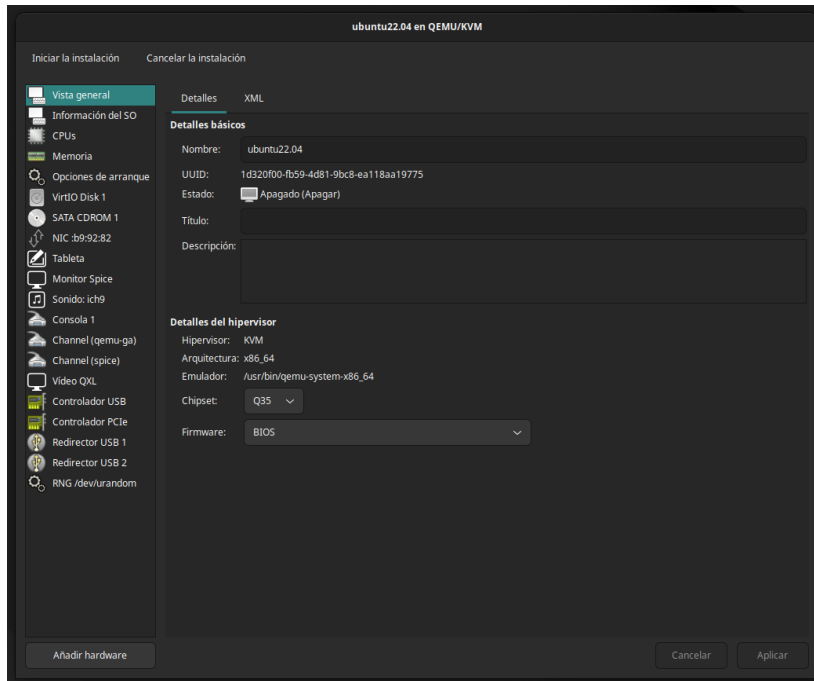
Se seleccionan los recursos de la máquina virtual indicando la cantidad de almacenamiento de disco, luego de indicarlo hacemos clic en el botón con nombre “Siguiente”.



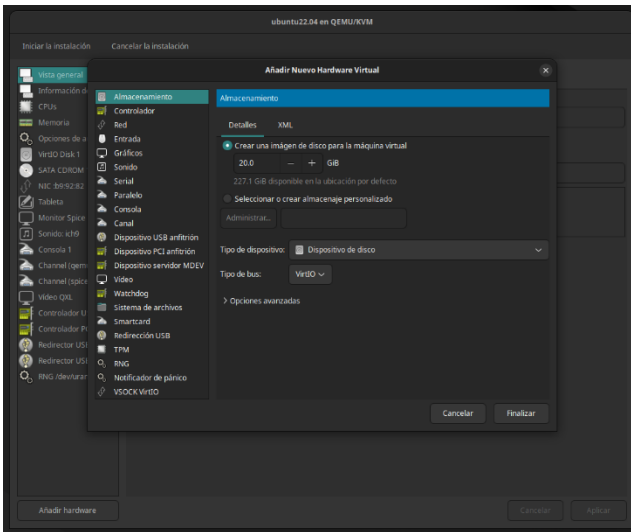
A continuación, debemos indicar el nombre de la máquina virtual y podríamos iniciar la instalación del sistema operativo, haciendo clic en el botón con nombre “Finalizar”. Sin embargo, si queremos agregar más recursos a la máquina virtual, podemos hacer clic en la opción con nombre “Personalizar la configuración antes de instalar” y especificar los recursos queremos agregar en la máquina virtual.



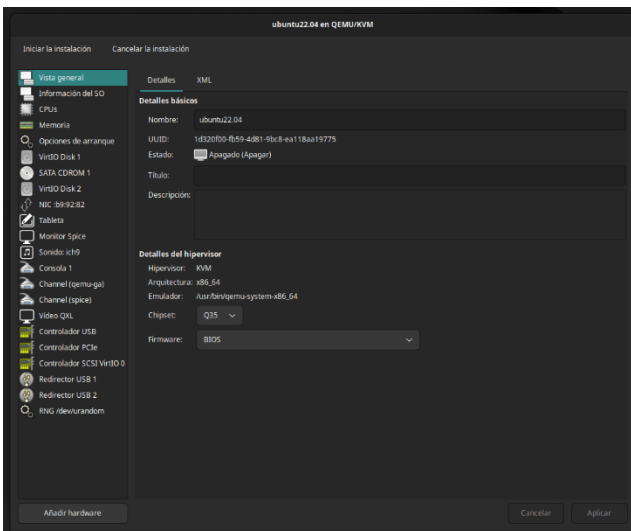
Se abrirá una ventana en la que podemos modificar las configuraciones por defecto de la máquina virtual. Para agregar un recurso a la máquina virtual podemos hacer clic en el botón de la esquina inferior izquierda con nombre “Agregar hardware”.



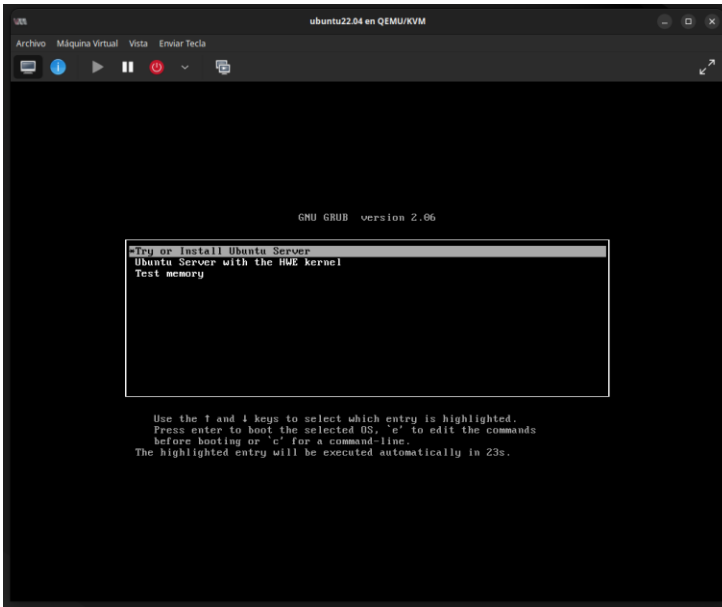
Se abrirá una venta donde podremos seleccionar en el menú los recursos que queremos agregar, por mencionar algunos pueden ser los adaptadores de red y discos de almacenamiento, con sus respectivos parámetros de configuración, y al hacer clic en el botón con nombre “Finalizar” se agregan los recursos a la máquina virtual.



Cuando ya se tienen especificados los recursos de la máquina virtual procedemos a la instalación del sistema operativo haciendo clic en el botón con nombre “Iniciar instalación” en la esquina superior izquierda.



A continuación, se dará inicio a la instalación donde las configuraciones serán de acuerdo con el sistema operativo previamente seleccionado.



3.5 Configuración de la VPN

La VPN seleccionada para la configuración es TailScale, para ello accedemos al sitio web de la herramienta, y creamos una cuenta donde en automático se creará una red predeterminada.

Luego procedemos a instalar la herramienta en uno de los nodos que se van a agregar en la red, ejecutando la siguiente orden.

```
curl -fsSL https://tailscale.com/install.sh | sh
```

Luego de realizar la instalación, se unirá a la red a la que pertenece la cuenta. Para consultar la dirección IP obtenida ejecutamos la siguiente orden.

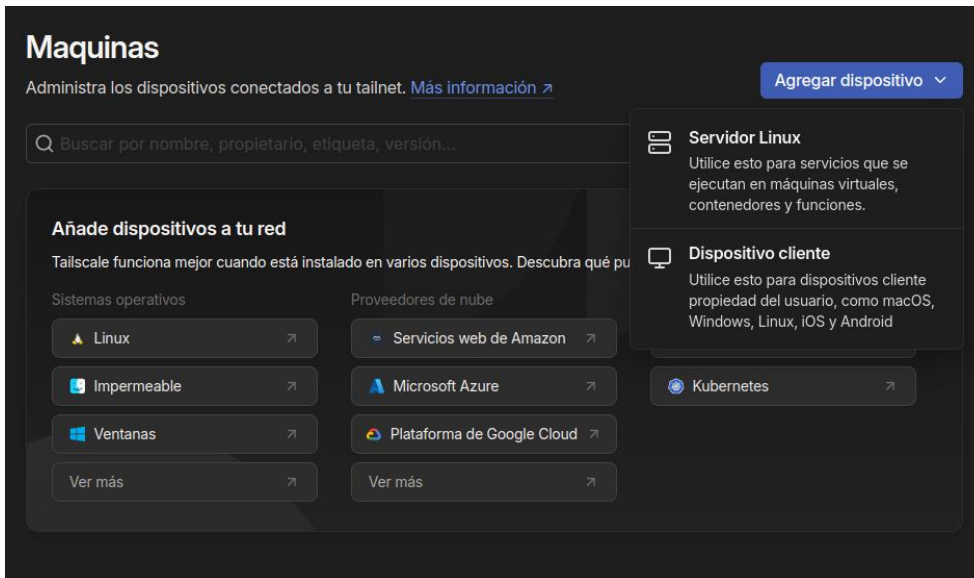
```
tailscale ip -4
```

Para agregar más nodos a la red debemos acceder a la consola de administración y generar un enlace para el acceso, el cual se ejecutará en el nodo que se desea agregar a la red.

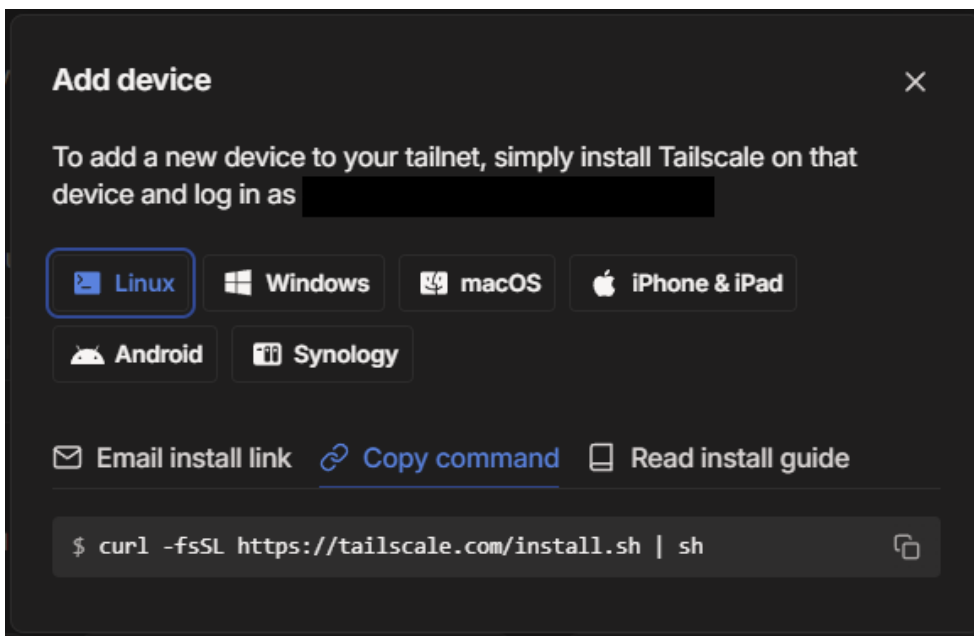
Para acceder a la consola de administración se debe ejecutar la siguiente orden.

```
sudo tailscale up
```

Cuando tengamos acceso a la consola de administración hacemos clic sobre el botón “Agregar dispositivo” y seleccionamos la opción “Dispositivo cliente”.



Se abrirá una ventana donde copiaremos el enlace y es el que compartiremos al nodo que deseamos agregar.



4 CONFIGURACIÓN DE COMPONENTES

4.1 Clúster de base de datos

Configuración de máquinas virtuales para el clúster.

Cantidad	Nombre	Recursos
1	maxscale	2CPU, 2GB RAM, 50GB Almacenamiento
3	maria1 maria2 maria3	2CPU, 2GB RAM, 50GB Almacenamiento

Configuración de red de los nodos del clúster.

Nodo	Interfaz de Red	IP
maxscale	enp1s0	10.0.0.133
	enp7s0	192.168.2.5
	ztiv5nmu5h	100.123.47.17
maria1	enp1s0	192.168.122.122
	enp7s0	192.168.2.2
	enp9s0	192.168.3.2
maria2	enp1s0	192.168.122.123
	enp7s0	192.168.2.3
	enp9s0	192.168.3.3
maria3	enp1s0	192.168.122.124
		192.168.2.4

	enp7s0	192.168.3.4
	enp9s0	

Primero se configuran las interfaces de red, para ello debemos modificar el archivo de configuración de netplan, ejecutar la siguiente orden.

```
sudo nano /etc/netplan/00-installer-config.yaml
```

Debemos de configurarlo de la siguiente forma.

```
network:
```

```
  ethernets:
```

```
    enp1s0:
```

```
      dhcp4: false
```

```
      addresses: [10.0.0.133/24]
```

```
      gateway4: 10.0.0.1
```

```
      nameservers:
```

```
        addresses: [8.8.8.8, 4.4.4.4]
```

```
    enp7s0:
```

```
      dhcp4: false
```

```
      addresses: [192.168.2.5/24]
```

```
version: 2
```

Luego de completar la configuración de las interfaces de red, debemos agregar el repositorio de MariaDB en el MaxSacale y en cada uno de los nodos, ejecutando la siguiente orden:

```
sudo apt install curl && curl -LsS https://r.mariadb.com/downloads/mariadb_repo_setup | sudo bash
```

Luego realizamos la actualización de los paquetes y procedemos a realizar la instalación de los siguientes paquetes ejecutando la siguiente orden:

```
sudo apt update && sudo apt install -y mariadb-server rsync
```

Al finalizar la instalación, procedemos a realizar la configuración del clúster de base de datos, para ello ejecutamos la siguiente orden:

```
sudo nano /etc/mysql/conf.d/mariadb.cnf
```

Debemos de configurarlo de la siguiente forma.

```
[mysqld]
```

```
query_cache_size=0
```

```
binlog_format=ROW
```

```
default-storage-engine=innodb
```

```
innodb_autoinc_lock_mode=2
```

```
query_cache_type=0
```

```
bind-address=0.0.0.0
```

```
# Galera Provider Configuration
```

```
wsrep_on=ON
```

```
wsrep_provider=/usr/lib/galera/libgalera_smm.so
```

```
#wsrep_provider_options="gcache.size=32G"
```

```
# Galera Cluster Configuration
```

```
wsrep_cluster_name="ClusterMaria"
```

```
wsrep_cluster_address="gcomm://192.168.3.2,192.168.3.3,192.168.3.4"
```

```
# Galera Synchronization Congifuration
```

```
wsrep_sst_method=rsync
```

```
#wsrep_sst_auth=user:pass
```

```
# Galera Node Configuration
```

```
wsrep_node_address="192.168.3.2"
```

```
wsrep_node_name="maria1"
```

Debemos de modificar en los demás nodos

```
# Galera Node Configuration  
wsrep_node_address="192.168.3.3"  
wsrep_node_name="maria2"
```

```
# Galera Node Configuration  
wsrep_node_address="192.168.3.4"  
wsrep_node_name="maria3"
```

Para iniciar el clúster debemos detener el servicio de mariadb en todos los nodos, ejecutando la siguiente orden.

```
sudo service mariadb stop
```

Para iniciar el clúster debemos ejecutar la siguiente orden en cualquiera de los nodos.

```
galera_new_cluster
```

Luego debemos revisar si el clúster inicio correctamente para ello debemos verificar el estado del servicio de mariadb y el estado del clúster, ejecutando la siguiente orden.

```
sudo service mysql status  
mysql -u root -p -e "SHOW STATUS LIKE 'wsrep_cluster_size'"
```

Al verificar que se ha iniciado el clúster, debemos iniciar el servicio de mariadb en los nodos restantes, ejecutando la siguiente orden.

```
sudo service mariadb start
```

4.2 Configuración de balanceador MaxScale

Primero debemos de configurar el usuario que utilizará MaxScale para comunicarse y realizará el monitoreo y consultas sql en cada uno de los nodos, ejecutando las siguientes órdenes.

```
sudo su  
mysql  
CREATE USER 'maxscale'@'%' IDENTIFIED BY 'admin';
```

```

GRANT SELECT ON mysql.user TO 'maxscale'@'%';
GRANT SELECT ON mysql.db TO 'maxscale'@'%';
GRANT SELECT ON mysql.tables_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.columns_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.proxies_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.procs_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.roles_mapping TO 'maxscale'@'%';
GRANT SHOW DATABASES ON *.* TO 'maxscale'@'%';
GRANT REPLICATION CLIENT on *.* to 'maxscale'@'%';
GRANT ALL ON infinidb_vtable.* TO 'maxscale'@'%';
CREATE USER 'maxscale_monitor'@%' IDENTIFIED BY 'admin';
GRANT REPLICATION CLIENT, FILE, SUPER, RELOAD, PROCESS, SHOW
DATABASES, EVENT ON *.* TO 'maxscale_monitor'@'%';

```

Luego realizamos la configuración de MaxScale, ejecutando la siguiente orden.

```
sudo nano /etc/maxscale.cnf
```

Debemos de configurarlo de la siguiente forma.

```

[maxscale]
threads=auto
log_augmentation = 1
ms_timestamp = 1
syslog = 1
admin_host = 0.0.0.0
admin_secure_gui = false

[maria1]
type=server
address=192.168.2.2
port=3306
protocol=MariaDBBackend

[maria2]
type=server

```

address=192.168.2.3
port=3306
protocol=MariaDBBackend

[maria3]
type=server
address=192.168.2.4
port=3306
protocol=MariaDBBackend

[MariaDB-Monitor]
type=monitor
module=mariadbmon
servers=maria1,maria2,maria3
user=maxscale_monitor
password=admin
monitor_interval=25s

[Read-Con-Route-Service]
type=service
router=readconnroute
router_options=synced
servers=maria1,maria2,maria3
user=maxscale
password=admin

[Read-Con-Route-Listener]
type=listener
service=Read-Con-Route-Service
protocol=MariaDBClient
port=3306
address=0.0.0.0

```

[Read-Write-Service]
type=service
router=readwritesplit
servers=maria1,maria2,maria3
user=maxscale
password=admin

```

```

[Read-Write-Listener]
type=listener
service=Read-Write-Service
protocol=MariaDBClient
port=4008
address=0.0.0.0

```

Quando ya esté completada la configuración debemos iniciar el servicio de MaxScale, ejecutando la siguiente orden.

```

sudo service maxscale start

```

Para verificar como MaxScale ha asociados los nodos, debemos ejecutar la siguiente orden.

```

maxctrl list servers

```

4.3 Clúster de almacenamiento

Configuración de máquinas virtuales para el clúster.

Cantidad	Nombre	Recursos
1	ceph-admin	2CPU, 2GB RAM, 50GB Almacenamiento
1	ceph-monitor	2CPU, 2GB RAM, 50GB Almacenamiento

3	ceph-osd1 ceph-osd2 ceph-osd3	2CPU, 2GB RAM, 2x50GB Almacenamiento
---	-------------------------------------	---

Configuración de red de los nodos del clúster.

Nodo	Interfaz de Red	IP
ceph-admin	enp1s0	10.0.0.128
	enp7s0	192.168.4.128
	ztiv5nmu5h	100.112.235.104
ceph-monitor	enp1s0	10.0.0.129
	enp7s0	192.168.4.129
	ztiv5nmu5h	100.118.54.77
ceph-osd1	enp1s0	10.0.0.130
	enp7s0	192.168.4.130
	ztiv5nmu5h	100.107.41.105
ceph-osd2	enp1s0	10.0.0.131
	enp7s0	192.168.4.131
	ztiv5nmu5h	100.97.178.33
ceph-osd3	enp1s0	10.0.0.132
	enp7s0	192.168.4.132
	ztiv5nmu5h	100.75.46.110

Primero se configuran las interfaces de red, para ello debemos modificar el archivo de configuración de netplan, ejecutar la siguiente orden.

sudo nano /etc/netplan/00-installer-config.yaml

Debemos de configurarlo de la siguiente forma.

network:

ethernets:

enp1s0:

dhcp4: false

addresses: [10.0.0.128/24]

gateway4: 10.0.0.1

nameservers:

addresses: [8.8.8.8, 4.4.4.4]

enp7s0:

dhcp4: false

addresses: [192.168.4.128/24]

version: 2

A continuación, debemos configurar en cada uno de los nodos la resolución de nombres, ejecutando la siguiente orden.

sudo nano /etc/hosts

Debemos de configurarlo de la siguiente forma.

100.112.235.104 ceph-admin

100.118.54.77 ceph-mon

100.107.41.105 ceph-osd1

100.97.178.33 ceph-osd2

100.75.46.110 ceph-osd3

Luego debemos de configurar crony para que el ceph-admin sirva el servicio de reloj al resto de nodos. Para ello realizamos la instalación del servicio con la siguiente orden.

sudo apt install chrony

Una vez instalado debemos de configurar el servicio agregando el servidor ntp.

Ejecutando la siguiente orden.

sudo nano /etc/chrony/chrony.conf

Debemos de configurarlo de la siguiente forma para el caso del ceph-admin.

```
server ntp.ues.edu.sv iburst  
allow 10.0.0.0/24  
allow 172.26.0.0/16
```

Para los demás nodos solo realizamos esta modificación.

```
server ceph-admin iburst
```

Cuando tengamos completada la configuración reiniciamos el servicio.

```
sudo service chrony restart
```

4.3.1 Instalación de Docker

Para la instalación de ceph se realizará por medio del método manual, por lo que es necesario contar con docker en cada uno de los nodos. Para ello ejecutamos la siguiente orde.

```
sudo apt install apt-transport-https ca-certificates curl gnupg-agent software-properties-  
common -y  
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -  
echo "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -sc)  
stable" | sudo tee /etc/apt/sources.list.d/docker-ce.list
```

Luego de realizar el registro del repositorio procedemos a actualizar los paquetes y la instalación de docker. Ejecutando la siguiente orden.

```
sudo apt update  
sudo apt install docker-ce docker-ce-cli containerd.io -y  
systemctl enable --now Docker
```

4.3.2 Configuración del servicio

Primero debemos de crear el usuario cephadmin y asignarle permisos de super usuario en los nodos monitor y osds, ejecutando la siguiente orden.

```
useradd -m -s /bin/bash cephadmin  
passwd cephadmin
```

```
echo "cephadmin ALL=(ALL:ALL) NOPASSWD:ALL" >> /etc/sudoers.d/cephadmin  
chmod 0440 /etc/sudoers.d/cephadmin
```

Luego permitimos el acceso del usuario root vía ssh, ejecutando la siguiente orden.

```
sudo nano /etc/ssh/sshd_config
```

Debemos de configurarlo de la siguiente forma.

```
PermitRootLogin yes
```

Cuando tengamos completada la configuración debemos reiniciar el servicio.

```
/etc/init.d/ssh restart
```

También es necesario cambiar la contraseña del usuario root

```
sudo su
```

```
passwd
```

4.3.3 Configuración del clúster Ceph

Primero debemos realizar la instalación de ceph-admin en el nodo ceph-admin, ejecutando la siguiente orden:

```
sudo su
```

```
wget -q https://github.com/ceph/ceph/raw/quincy/src/cephadm/cephadm -P /usr/bin/  
chmod +x /usr/bin/cephadm
```

Para verificar la instalación debemos obtener “cephadmin” al ejecutar la siguiente orden.

```
su - cephadmin
```

```
whoami
```

Para iniciar el clúster debemos ejecutar la siguiente orden, teniendo en cuenta que el parámetro cluster-network es la red que se utilizará para la sincronización de los nodos, y el parámetro mon-ip es la ip del ceph-admin, la cual será la red que se utilizará para consumir el servicio.

```
sudo cephadm bootstrap --cluster-network 192.168.4.0/24 --mon-ip
```

Luego de haber iniciado el clúster en pantalla se nos mostrará un mensaje indicando la url para ingresar al panel donde vamos a gestionarlo, además del usuario y contraseña provisional.

Ceph Dashboard is now available at:

URL: <https://ceph-admin:8443/>

User: admin

Password: 8964vjghsi

Para poder gestionarlo desde la terminal es necesario contar con las librerías que lo permiten, para obtenerlas debemos ejecutar la siguiente orden.

```
sudo cephadm add-repo --release quincy
```

```
sudo cephadm install ceph-common
```

```
sudo ceph -s
```

4.3.4 Registro de nodos para incluirlos en el clúster

Primero agregar el nodo monitor debemos de copiar la llave por medio de la siguiente orden.

```
sudo ssh-copy-id -f -i /etc/ceph/ceph.pub root@ceph-monitor
```

Para agregar el nodo al clúster debemos ejecutar la siguiente orden.

```
sudo ceph orch host add ceph-monitor
```

Para asignarle una etiqueta ejecutamos la siguiente orden.

```
sudo ceph orch host label add ceph-monitor mon/osd
```

Para registrar los nodos osd en el clúster debemos instalar en cada uno de los nodos una librería que nos permita hacer operaciones en los discos ejecutando la siguiente orden.

```
sudo apt install lvm2
```

Del mismo modo que el nodo monitor, realizamos la copia de la llave con la siguiente orden.

```
for i in ceph-osd1 ceph-osd2 ceph-osd3; do sudo ssh-copy-id -f -i /etc/ceph/ceph.pub root@$i; done
```

Luego procedemos al registro de los nodos al clúster, ejecutando la siguiente orden.

```
sudo ceph orch host add ceph-osd1
```

```
sudo ceph orch host add ceph-osd2
```

```
sudo ceph orch host add ceph-osd3
```

Una vez completado el registro le asignamos la etiqueta a cada uno de los nodos.

```
for i in ceph-osd1 ceph-osd2 ceph-osd3; do sudo ceph orch host label add $i osd; done
```

Para verificar que los nodos han sido agregados correctamente al clúster debemos ejecutar la siguiente orden.

```
sudo ceph orch host ls
```

4.3.5 Inflando el clúster

En cada uno de los nodos debemos de listar los discos disponibles y crear un volumen en el segundo disco que tenemos asignado, ejecutando la siguiente orden.

```
sudo fdisk -l
```

```
vgcreate vg01 /dev/vdb
```

```
lvcreate -L 49G -n lv01 vg01
```

Cuando tengamos preparados los discos procedemos a agregarlos al clúster ejecutando la siguiente orden en el nodo ceph-admin.

```
sudo ceph orch daemon add osd ceph-osd1:vg01/lv01
```

```
sudo ceph orch daemon add osd ceph-osd2:vg01/lv01
```

```
sudo ceph orch daemon add osd ceph-osd3:vg01/lv01
```

Podemos revisar la salud luego de completadas las configuraciones ejecutando la siguiente orden en el nodo ceph-admin.

```
sudo ceph -s
```

5 CONFIGURACIÓN DE LA REGIÓN PRINCIPAL

5.1 Configuración del módulo controller

Configuración de máquinas virtuales para el módulo controller.

Cantidad	Nombre	Recursos
1	Controller	2CPU, 8GB RAM, 50GB Almacenamiento
1	RabbitMQ	2CPU, 2GB RAM, 50GB Almacenamiento

Configuración de red de los nodos del módulo controller.

Nodo	Interfaz de Red	IP
Controller	enp1s0	10.0.0.134
	ztiv5nmu5h	100.91.68.101
RabbitMQ	enp1s0	10.0.0.135
	ztiv5nmu5h	100.79.203.120

Primero se configuran las interfaces de red, para ello debemos modificar el archivo de configuración de netplan, ejecutar la siguiente orden.

```
sudo nano /etc/netplan/00-installer-config.yaml
```

Debemos de configurarlo de la siguiente forma.

```
network:
```

```
  ethernets:
```

```
    enp1s0:
```

```
      dhcp4: false
```

```
addresses: [10.0.0.134/24]  
gateway4: 10.0.0.1  
nameservers:  
addresses: [8.8.8.8, 4.4.4.4]  
version: 2
```

5.1.1 Configuración del controller

Debemos de configurar crony para que el controller sirva el servicio de reloj al resto de nodos. Para ello realizamos la instalación del servicio con la siguiente orden.

```
sudo apt install chrony
```

Una vez instalado debemos de configurar el servicio agregando el servidor ntp.

Ejecutando la siguiente orden.

```
sudo nano /etc/chrony/chrony.conf
```

Debemos de configurarlo de la siguiente forma para el caso del controller.

```
server ntp.ues.edu.sv iburst  
allow 10.0.0.0/24  
allow 100.0.0.0/32
```

Para los demás nodos solo realizamos esta modificación.

```
server 100.91.68.101 iburst
```

Cuando tengamos completada la configuración reiniciamos el servicio.

```
sudo service chrony restart
```

Una vez completada la configuración de chrony, agregamos el paquete de openstack en cada uno de los nodos, ejecutando la siguiente orden.

```
sudo add-apt-repository cloud-archive:bobcat
```

Luego realizamos la actualización de los paquetes y la instalación del cliente de openstack en cada uno de los nodos, ejecutando la siguiente orden.

```
sudo apt update
```

```
sudo apt install python3-openstackclient
```

5.1.1.1 Configuración de Memcached

Para ello instalamos los servicios en el nodo controller ejecutando los siguientes comandos.

```
sudo apt install memcached python3-memcache
```

Realizamos la configuración de memcached ejecutando la siguiente orden.

```
sudo nano /etc/memcached.conf
```

Se debe configurar las interfaces por las que el servicio va escuchar las peticiones.

```
-l 10.0.0.134 100.91.68.101
```

Reiniciamos el servicio.

```
service memcached restart
```

5.1.1.2 Configuración de ETCD

Para ello instalaremos el servicio en el nodo controller con el siguiente comando.

```
sudo apt install etcd
```

Procedemos a configurar etcd.

```
sudo nano /etc/default/etcd
```

Agregamos la siguiente configuración.

```
ETCD_NAME="controller"
```

```
ETCD_DATA_DIR="/var/lib/etcd"
```

```
ETCD_INITIAL_CLUSTER_STATE="new"
```

```
ETCD_INITIAL_CLUSTER_TOKEN="etcd-cluster-01"
```

```
ETCD_INITIAL_CLUSTER="controller=http://10.0.0.134:2380"
```

```
ETCD_INITIAL_ADVERTISE_PEER_URLS="http://10.0.0.134:2380"
```

```
ETCD_ADVERTISE_CLIENT_URLS="http://10.0.0.134:2379"
```

```
ETCD_LISTEN_PEER_URLS="http://0.0.0.0:2380"
```

```
ETCD_LISTEN_CLIENT_URLS="http://10.0.0.134:2379"
```

Habilitamos e iniciamos el servicio.

```
sudo systemctl enable etcd  
sudo systemctl restart etcd
```

5.1.2 Configuración de RabbitMQ

Para instalar rabbitMQ, ejecutamos la siguiente orden en el nodo rabbitMQ.

```
sudo apt install rabbitmq-server
```

Agregamos el usuario de rabbitmq a openstack, reemplazando “RABBIT_PASS” por la contraseña que hemos seleccionado, ejecutando la siguiente orden.

```
rabbitmqctl add_user openstack RABBIT_PASS
```

Una vez agregado el usuario le concedemos los permisos ejecutando la siguiente orden.

```
rabbitmqctl set_permissions openstack ".*" ".*" ".*"
```

A continuación, configuramos las colas para cada una de las regiones, sustituyendo “region” por la región que vamos a configurar.

```
sudo rabbitmqctl add_user region PASS  
sudo rabbitmqctl add_vhost /region  
sudo rabbitmqctl set_permissions -p /region region ".*" ".*" ".*"
```

Cuando tengamos asignadas las colas para cada región, procedemos a habilitar la interfaz web para poder gestionar de mejor manera el servicio, para ello debemos configurar el usuario que utilizaremos para acceder, por medio de la siguiente orden.

```
sudo rabbitmqctl add_user USER PASS  
rabbitmqctl add_vhost /VHOST  
sudo rabbitmqctl set_permissions -p /VHOST USER ".*" ".*" ".*"  
sudo rabbitmqctl set_user_tags main administrator
```

Al tener creado el usuario procedemos a habilitar la interfaz web para poder gestionar de mejor manera el servicio, ejecutando la siguiente orden.

rabbitmq-plugins enable rabbitmq_management

Y para acceder al navegador ingresaremos a la siguiente URL.

http://100.79.203.120:15672/

5.2 Configuración de módulo identidad

Configuración de máquinas virtuales para el módulo identidad.

Cantidad	Nombre	Recursos
1	Keystone	2CPU, 2GB RAM, 50GB Almacenamiento
1	OpenLDAP	2CPU, 2GB RAM, 50GB Almacenamiento

Configuración de red de los nodos del módulo identidad.

Nodo	Interfaz de Red	IP
Keystone	enp1s0	10.0.0.136
	enp7s0	192.168.5.2
	ztiv5nmu5h	100.118.19.86
OpenLDAP	enp7s0	192.168.5.3

Primero se configuran las interfaces de red, para ello debemos modificar el archivo de configuración de netplan, ejecutar la siguiente orden.

sudo nano /etc/netplan/00-installer-config.yaml

Debemos de configurarlo de la siguiente forma.

network:

ethernets:

enp1s0:
dhcp4: false
addresses: [10.0.0.136/24]
gateway4: 10.0.0.1
nameservers:
addresses: [8.8.8.8, 4.4.4.4]
enp7s0:
dhcp4: false
addresses: [192.168.5.2/24]
version: 2

5.2.1 Configuración del servicio de Keystone

5.2.1.1 Creación de base de datos.

Se debe crear una base de datos en el clueter de MariaDB para almacenar los registros de Keystone.

```
CREATE DATABASE keystone;
```

Creamos y asignamos usuarios a la nueva base de datos.

```
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'localhost' |  
IDENTIFIED BY 'KEYSTONE_DBPASS';
```

```
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'%' |  
IDENTIFIED BY 'KEYSTONE_DBPASS';
```

5.2.1.2 Instalación de paquetes.

Agregamos el repositorio de OpenStack bobcat.

```
sudo add-apt-repository cloud-archive:bobcat
```

Instalamos los paquetes de keystone.

```
sudo apt update
```

```
sudo apt install keystone
```

```
sudo apt install python3-openstackclient
```

Configuramos el siguiente archivo de Keystone.

```
sudo nano /etc/keystone/keystone.conf
```

Agregamos la siguiente configuración en las secciones correspondientes.

```
[database]
```

```
connection = mysql+pymysql://keystone: KEYSTONE_DBPASS @10.0.0.133/keystone
```

```
[token]
```

```
provider = fernet
```

Procedemos a poblar la base de datos.

```
su -s /bin/sh -c "keystone-manage db_sync" keystone
```

Iniciamos los servicios de Fernet:

```
keystone-manage fernet_setup --keystone-user keystone --
```

```
keystone-group keystone
```

```
keystone-manage credential_setup --keystone-user keystone -
```

```
-keystone-group keystone
```

Agregamos las credenciales a la región principal

```
keystone-manage bootstrap --bootstrap-password ADMIN_PASS
```

```
--bootstrap-admin-url http://100.118.19.86:5000/v3/
```

```
--bootstrap-internal-url http://100.118.19.86:5000/v3/
```

```
--bootstrap-public-url http://100.118.19.86:5000/v3/
```

```
--bootstrap-region-id RegionOne
```

Configuramos apache

```
sudo nano /etc/apache2/apache2.conf
```

Agregamos el ServerName

```
ServerName controller
```

Reiniciamos Apache

```
sudo service apache2 restart
```

Creamos un archivo de variables de entorno

nano admin-openrc

Con los siguientes datos.

```
export OS_PROJECT_DOMAIN_NAME=Default  
export OS_USER_DOMAIN_NAME=proyecto  
export OS_PROJECT_NAME=admin  
export OS_USERNAME=admin  
export OS_PASSWORD=admin  
export OS_AUTH_URL=http://100.118.19.86:5000/v3  
export OS_IDENTITY_API_VERSION=3  
export OS_IMAGE_API_VERSION=2  
export OS_REGION_NAME=RegionOne
```

Cargamos las variables

. admin-openrc

Procedemos a crear un dominio y servicios nuevos.

```
openstack domain create --description "An Example Domain" example  
openstack project create --domain default --description "Service Project" service
```

5.2.2 Configuración del servicio LDAP

5.2.2.1 Instalación de OpenLDAP

Primero instalamos los paquetes de slapd y ldap-utils, ejecutando la siguiente orden. (Nos solicitará una contraseña que será la del administrador)

```
sudo apt install slapd ldap-utils
```

Luego agregamos la configuración de la resolución de nombres ejecutando la siguiente orden.

```
sudo nano /etc/hosts
```

Debemos de configurarlo de la siguiente forma.

192.168.5.3 openldap.identity.net openldap

Luego realizamos las configuraciones del servicio ejecutando la siguiente orden.

```
sudo dpkg-reconfigure slapd
```

Se nos preguntará una serie de preguntas para lo cual debemos responder.

¿Desea omitir la configuración del servidor OpenLDAP? ***No***

Introduzca el nombre de dominio DNS: ***identity.net***

Contraseña del administrador: (***La que escribimos previamente del administrador***)

¿Desea que se borre la base de datos cuando se purge el paquete slapd? ***No***

¿Desea mover la base de datos antigua? ***Si***

Cuando hayamos completado las preguntas reiniciamos el servicio, ejecutando la siguiente orden.

```
sudo systemctl restart slapd
```

A continuación, habilitamos el firewall, para permitir el acceso solo a los puertos que brindan el servicio.

```
sudo ufw enable
```

```
sudo ufw allow ldap
```

```
sudo ufw allow ldaps
```

```
sudo ufw allow ssh
```

```
sudo ufw reload
```

Para verificar las reglas definidas previamente, ejecutamos la siguiente orden.

```
sudo ufw status
```

5.2.2.2 Creación de árbol de direcciones y usuarios de acceso

Primero debemos crear un archivo ejecutando la siguiente orden.

```
sudo nano identity.ldif
```

Debe contener la siguiente información.

dn: cn=accounts,dc=identity,dc=net

objectClass: organizationalRole

cn: accounts

dn: cn=users,cn=accounts,dc=identity,dc=net

objectClass: organizationalRole

cn: users

dn: cn=groups,cn=accounts,dc=identity,dc=net

objectClass: organizationalRole

cn: groups

Para agregar el árbol de direcciones al servicio ejecutamos la siguiente orden.

ldapadd -x -D "cn=admin,dc=identity,dc=net" -W -f identity.ldif

A continuación, creamos los usuarios que se van a autenticar en keystone, ejecutando la siguiente orden.

sudo nano usuarios.ldif

Debe contener la siguiente información.

dn: uid=carlos,cn=users,cn=accounts,dc=identity,dc=net

objectClass: top

objectClass: person

objectClass: organizationalPerson

objectClass: inetOrgPerson

uid: carlos

cn: Carlos

sn: Neptuno

givenName: Carlos

mail: carlos@example.com

userPassword: admin

dn: uid=isai,cn=users,cn=accounts,dc=identity,dc=net

objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: isai
cn: Isai
sn: Neptuno
givenName: isai
mail: isai@example.com
userPassword: admin

dn: uid=gustavo,cn=users,cn=accounts,dc=identity,dc=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: gustavo
cn: Gustavo
sn: Neptuno
givenName: Gustavo
mail: gustavo@example.com
userPassword: admin

dn: uid=admin,cn=users,cn=accounts,dc=identity,dc=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: admin
cn: Admin
sn: Proyecto
givenName: Admin
mail: admin@example.com

userPassword: admin

Para agregar los usuarios al servicio ejecutamos la siguiente orden.

```
ldapadd -x -D "cn=admin,dc=identity,dc=net" -W -f usuarios.ldif
```

5.2.2.3 Configuración del certificado

Copiamos el certificado al nodo de keystone, por medio de la siguiente orden.

```
scp /etc/ssl/certs/ca-certificates.crt admin@192.168.5.2:/home/admin
```

Con el archivo copiado en el nodo de keystone, creamos el certificado desde el nodo de keystone ejecutando el siguiente formato.

```
openssl x509 -in ca-certificates.crt -out ca-certificates.pem -outform PEM
```

Agregamos los archivos generados al directorio de llaves.

```
sudo cp ca-certificates.pem /usr/local/share/ca-certificates/
```

```
sudo cp ca-certificates.crt /usr/local/share/ca-certificates/
```

Creamos un directorio en el nodo de Keystone, para alojar las nuevas configuraciones para el nuevo dominio, ejecutando la siguiente orden.

```
sudo mkdir /etc/keystone/domains/
```

```
sudo chown keystone /etc/keystone/domains/
```

Agregamos las nuevas configuraciones en el nodo de keystone ejecutando la siguiente orden.

```
sudo nano /etc/keystone/keystone.conf
```

Debe de tener la configuración de la siguiente forma.

```
[assignment]
```

```
driver = sql
```

```
[identity]
```

```
domain_specific_drivers_enabled = true
```

domain_config_dir = /etc/keystone/domains

Cuando ya tengamos realizada la configuración procedemos a crear el dominio en openstack, siempre desde el nodo de keystone, ejecutando la siguiente orden.

openstack domain create proyecto

Creamos un archivo para la configuración de la conexión de ldap con el nuevo dominio, por medio de la siguiente orden.

sudo nano /etc/keystone/domains/keystone.proyecto.conf

La configuración debe contener la siguiente forma.

[ldap]

url = ldap://192.168.5.3

user = uid=admin,cn=users,cn=accounts,dc=identity,dc=net

password = admin

user_tree_dn = cn=users,cn=accounts,dc=identity,dc=net

user_objectclass = inetOrgPerson

user_id_attribute = uid

user_name_attribute = uid

user_mail_attribute = mail

user_pass_attribute =

user_allow_create = False

user_allow_update = False

user_allow_delete = False

tls_cacertfile = /usr/local/share/ca-certificates/ca-certificates.crt

[identity]

driver = ldap

Asignamos al usuario keystone como propietario del archivo, ejecutando la siguiente orden.

sudo chown keystone /etc/keystone/domains/keystone.proyecto.conf

A continuación, le brindamos acceso al usuario admin al dominio “proyecto”. Ejecutando la siguiente

Orden.

Información necesaria para ejecutar el comando.

IdDominio: openstack domain show proyecto

IdUsuarioAdmin: openstack user list --domain default | grep admin

IdRolAdmin: openstack role list

Asignando el acceso.

```
openstack role add --domain ID_DOMAIN --user ID_USER_ADMIN  
ID_ROLE_ADMIN
```

Cuando ya hayamos completado la configuración instalamos el complemento de apache para la comunicación con ldap y reiniciamos el servicio de apache, ejecutando la siguiente orden.

sudo apt install python3-ldappool

sudo service apache2 restart

Para verificar que tenemos acceso al servicio LDAP, podemos listar los usuarios, ejecutando la siguiente orden.

openstack user list --domain proyecto

Ahora asignaremos un rol (reader, admin, member) de openstack para los usuarios creados en openldap, ejecutando el siguiente comando.

```
openstack role add --user ID_USER --domain NAME_DOMAIN NAME_ROL
```

Es necesario también asignarle los permisos para un proyecto de openstack a los usuarios creados en openldap, ejecutando el siguiente comando.

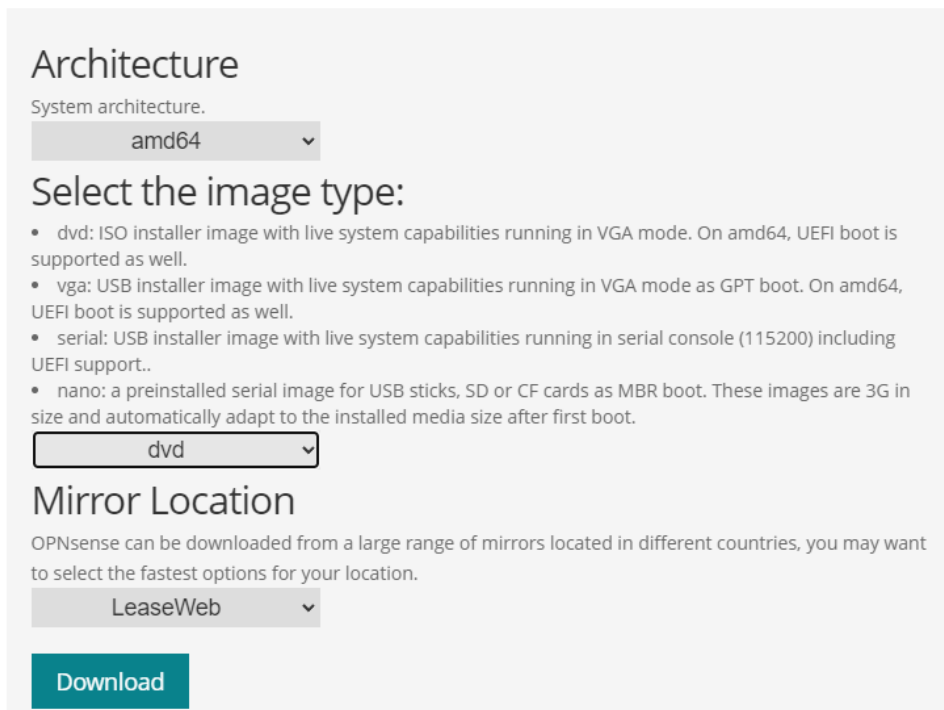
```
openstack role add --user ID_USER --project NAME_PROYECT NAME_ROL
```

Cuando hayamos completado la configuración de los permisos, los usuarios creados en openldap podrán iniciar sesión en el dashboard de Horizon, con el dominio “proyecto”.

5.3 Configuración del módulo de monitoreo

5.3.1 Instalación de OPNSense

Se accede al portal de descargas de OPNSense y se selecciona la arquitectura de la descarga, y el tipo de imagen DVD.



The screenshot shows a web form for downloading OPNSense. It has a title 'Architecture' and a subtitle 'System architecture.' Below this is a dropdown menu with 'amd64' selected. The next section is 'Select the image type:' followed by a bulleted list of options: 'dvd', 'vga', 'serial', and 'nano'. Below the list is another dropdown menu with 'dvd' selected. The next section is 'Mirror Location' with a subtitle 'OPNSense can be downloaded from a large range of mirrors located in different countries, you may want to select the fastest options for your location.' Below this is a dropdown menu with 'LeaseWeb' selected. At the bottom is a green 'Download' button.

Luego de completada la descarga se lanza una instancia con la imagen iso. En automático se procederá con el proceso de arranque y una vez completado se le enviará un mensaje por la terminal para el inicio de sesión. Las credenciales que debe usar para la instalación son, usuario: installer, contraseña: opnsense.

```
>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Sun Oct 13 23:12:08 UTC 2024

*** OPNsense.localdomain: OPNsense 24.7 ***

LAN (vtnet0)    -> v4: 192.168.1.1/24

HTTPS: sha256 56 D2 25 1E 25 2F 19 3F 45 6C D5 65 FB 9A D1 EE
              3C F6 9F 28 12 5B A9 69 0C BC BA 96 FC 11 F5 F1
SSH:   SHA256 iuXJM3IHg+M5w790EQwEk/GR4ao7JB03uTj4Ua953qA (ECDSA)
SSH:   SHA256 9iehurJpMUsvbSKY0un8aZKHKwLHvX040q/k4vQB53w (ED25519)
SSH:   SHA256 +lAa3ER/c71aDErm118+zT7k6AzulC0123DHXpfh0ng (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

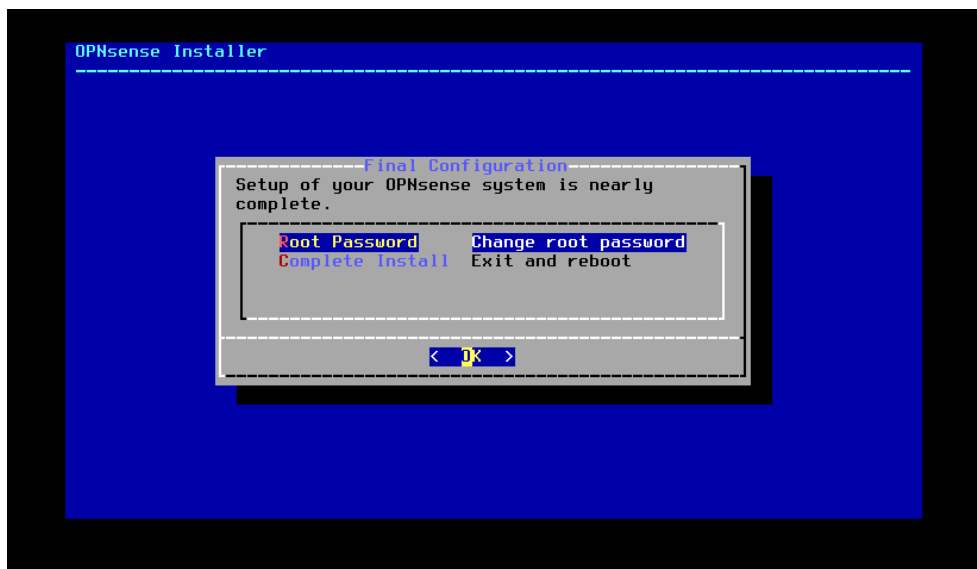
login: █
```

Se desplegará una ventana de bienvenida, y a continuación debe especificar el mapa de las teclas a utilizar, y seguido de eso debe especificar el tipo de instalación a realizar.





Una vez completado el proceso de instalación debe de establecer una contraseña para el usuario root, y reiniciar el sistema.



Cuando se haya completado el reinicio del sistema debe iniciar sesión para realizar la configuración de las interfaces de red. Para ello se configurarán dos, la de la red local (LAN) y la red pública (WAN). De no contar con las dos interfaces puede agregar las interfaces a la instancia y proceder con la configuración. Para ello debe seleccionar la opción 2.

Le preguntará que seleccione la interfaz de red para la red local y pública, además de que indique el tipo de enrutamiento si estático o dinámico.

```
|      Hello, this is OPNsense 24.7      |      @@@@@@@@@@@@@@@@@@
|                                          |      @@@@      @@@@
| Website:      https://opnsense.org/    |      @@@\\ \\   ///@@@
| Handbook:    https://docs.opnsense.org/ |      )))))))  ((((((
| Forums:      https://forum.opnsense.org/ |      @@@///   \\ \\@@@
| Code:        https://github.com/opnsense |      @@@@      @@@@
| Twitter:     https://twitter.com/opnsense |      @@@@@@@@@@@@@@@@@@
|-----|-----|
*** OPNsense.localdomain: OPNsense 24.7 ***

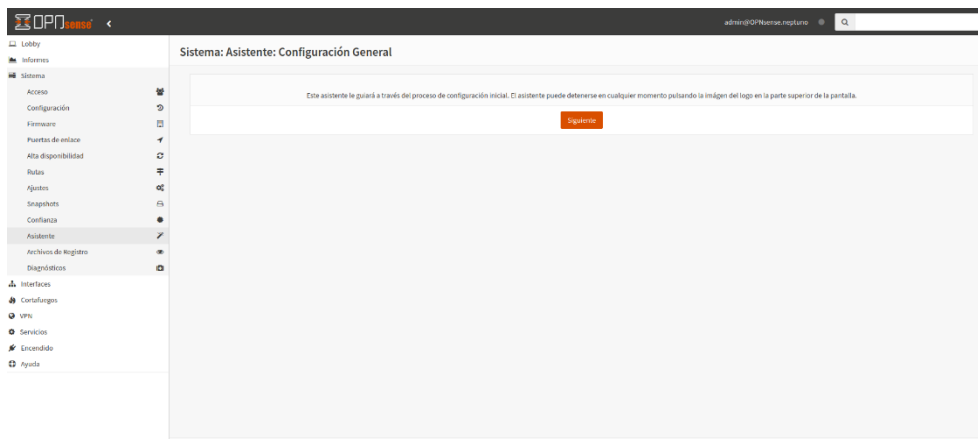
LAN (vtnet0)  -> v4: 192.168.1.1/24

HTTPS: sha256 56 D2 25 1E 25 2F 19 3F 45 6C D5 65 FB 9A D1 EE
          3C F6 9F 28 12 5B A9 69 0C BC BA 96 FC 11 F5 F1

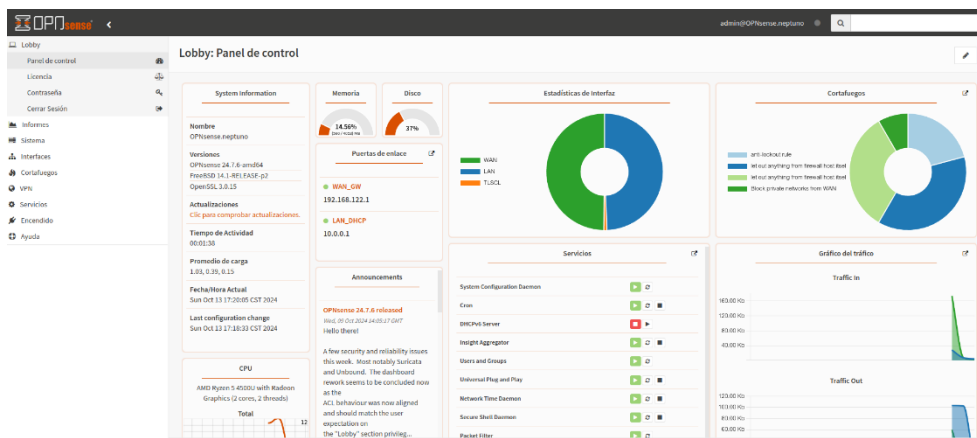
0) Logout                7) Ping host
1) Assign interfaces     8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system       12) Update from console
6) Reboot system          13) Restore a backup

Enter an option: █
```

Una vez completada la configuración se le presentarán las url para acceder al panel de control y completar la configuración de OPNsense. Para ello debe de iniciar sesión y proceder con la configuración. En el caso de la configuración de red se puede omitir porque se configuró previamente.



Una vez completada la configuración ya podremos hacer uso del panel de control para la administración de la red.



5.3.2 Integración de OPNsense con la VPN de Tailscale.

Para ello debemos de acceder desde la terminal como usuario root y seleccionar la opción 8 (Shell), con ello tendremos acceso a la terminal de la instancia. Lo primero debemos de descargar el árbol de ports con la siguiente instrucción.

opnsense-code ports

Una vez descargado el árbol de puertos, ejecute los siguientes pasos como root para instalar Tailscale.

cd /usr/ports/security/tailscale

make install

Cuando ya encuentre instalado podremos habilitar el servicio e iniciarlo. Además, podremos verificar su correcto funcionamiento verificando la versión instalada, ejecutando las siguientes instrucciones.

service tailscaled enable

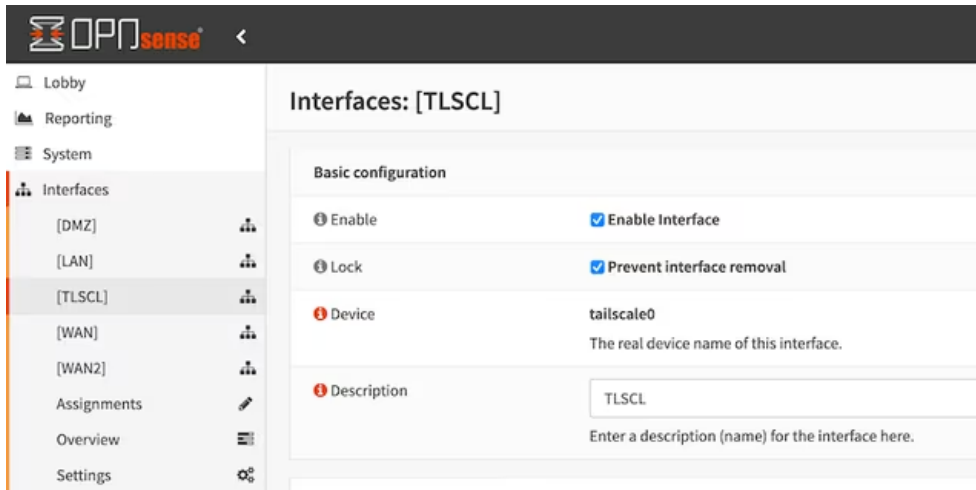
service tailscaled start

tailscale version

Luego de verificar la correcta instalación debemos agregar nuestra instancia de OPNsense a la red de Tailscale ejecutando la siguiente instrucción.

tailscale up

Luego de completado la conexión dentro del panel de control, en la opción de interfaces y asignaciones, ya podremos agregar la interfaz de Tailscale y habilitarla para el monitoreo.



6 CONECTAR REGIONES A LA REGIÓN PRINCIPAL

Primero debemos configurar las regiones, con base en la guía oficial de Openstack <https://docs.openstack.org/install-guide/>, para cual dispondremos de los siguientes nodos por región.

Cantidad	Nombre	Recursos
1	pc-controller-#{# de region}	4CPU, 8GB RAM, 50GB Almacenamiento
2	Compute-#{#}	4CPU, 8GB RAM, 50GB Almacenamiento

Con la siguiente configuración de red para cada nodo

Nodo	Interfaz de Red	IP
Controller	enp1s0	10.0.N.134

	enp7s0	192.168.N.2
	ztiv5nmu5h	100.N.N.N
Compute	enp1s0	10.0.N.13x
	enp7s0	192.168.N.x
	ztiv5nmu5h	100.N.N.N

6.1 Controller

Debe iniciar configurando el “Environment” como lo indica la guía oficial de openstack, debe asegurarse de colocar de forma correcta los hostnames, ip y nombres de cada región.

6.2 Nodos compute

Nos debemos guiar por la [Guía de instalación de Openstack](#), una vez finalizada procedemos a hacer la configuración necesaria para consumir el almacenamiento de Ceph.

6.3 Configurar nodos para consumir Ceph

En todos los nodos.

Creamos la carpeta para almacenar los archivos de configuración de Ceph.

```
sudo mkdir -p -m 755 /etc/ceph
```

Dentro de la carpeta agregamos los keyring configurados previamente en ceph.

```
sudo nano ceph.client.admin.keyring
```

```
[client.admin]
```

```
key = "Su clave"
```

```
caps mds = "allow *"
```

```
caps mgr = "allow *"
```

```
caps mon = "allow *"
```

```
caps osd = "allow *"
```

```
sudo nano ceph.client.cinder-backup.keyring
```

```
[client.cinder-backup]
```

```

    key = Su clave"
sudo nano ceph.client.cinder.keyring
[client.cinder]
    key = Su clave"
sudo nano ceph.client.glance.keyring
[client.glance]
    key = AQDF Ae5mwYQhOxAAiLqczdvvyvGJdVnYmTFjBg==

```

Instalaremos los paquetes de ceph

```
sudo apt install ceph-common
```

Probamos la configuración de ceph

```
sudo ceph -s
```

6.4 Configuración de Cinder.

Configuraremos Cinder en los nodos controller de las regiones.

Iniciamos creando la base de datos.

```
CREATE DATABASE region#_cinder;
```

Configure los usuarios que utilizaran la base de datos (reemplace # por el identificador de la región).

```

GRANT ALL PRIVILEGES ON cinder.* TO ' cinder_# '@'localhost' |
IDENTIFIED BY 'CINDER_DBPASS';
GRANT ALL PRIVILEGES ON cinder.* TO ' cinder_# '@'%' |
IDENTIFIED BY 'CINDER_DBPASS';

```

Ejecute las variables de entorno

```
. admin-openrc
```

Creamos el usuario de openstack

```
openstack user create --domain default --password-prompt cinder
```

Asignamos el rol de admin.

```
openstack role add --project service --user cinder admin
```

Creamos el servicio.

```
openstack service create --name cinderv3 |  
--description "OpenStack Block Storage" volumev3
```

Creamos los endpoints (reemplace # por el identificador de su región).

```
openstack endpoint create --region Region# | volumev3 public  
http://controller:8776/v3/%(project_id)s
```

```
openstack endpoint create --region Region# |  
volumev3 internal http://controller:8776/v3/%(project_id)s
```

```
openstack endpoint create --region RegionOne |
```

```
volumev3 admin http://controller:8776/v3/%(project_id)s
```

Instale los paquetes de cinder

```
sudo apt install cinder-api cinder-scheduler  
sudo apt install cinder-volume tgt
```

```
sudo apt install cinder-backup
```

Configure el siguiente archivo.

```
sudo nano /etc/cinder/cinder.conf
```

Agregaremos lo siguiente en el archivo de configuración.

```
[DEFAULT]  
rootwrap_config = /etc/cinder/rootwrap.conf  
api_paste_config = /etc/cinder/api-paste.ini  
iscsi_helper = lioadm  
volume_name_template = volume-%s  
volume_group = cinder-volumes
```

```
verbose = True
auth_strategy = keystone
state_path = /var/lib/cinder
lock_path = /var/lock/cinder
volumes_dir = /var/lib/cinder/volumes
enabled_backends = ceph
transport_url = rabbit://region#:RABBIT_PASS@100.79.203.120//region#
auth_strategy = keystone
my_ip = 10.0.N.134 #N es el identificador de la región (One, Two)
backup_driver = cinder.backup.drivers.ceph.CephBackupDriver
backup_ceph_user = cinder-backup
backup_ceph_conf = /etc/ceph/ceph.conf
backup_ceph_chunk_size = 134217728
backup_ceph_pool = backups
backup_ceph_stripe_unit = 0
backup_ceph_stripe_count = 0
restore_discard_excess_bytes = true
```

[database]

```
connection = mysql+pymysql://cinder: CINDER_DBPASS @100.123.47.17/cinder_#
#connection = sqlite:///var/lib/cinder/cinder.sqlite
```

[keystone_authtoken]

```
# ...
www_authenticate_uri = http://100.118.19.86:5000
auth_url = http://100.118.19.86:5000
memcached_servers = 100.91.68.101:11211
auth_type = password
project_domain_name = default
user_domain_name = default
project_name = service
username = cinder
password = CINDER_PASS
```

```
[oslo_concurrency]
```

```
lock_path = /var/lib/cinder/tmp
```

```
[ceph]
```

```
volume_driver = cinder.volume.drivers.rbd.RBDDriver
```

```
volume_clear = none
```

```
rbd_cluster_name = ceph
```

```
rbd_ceph_conf = /etc/ceph/ceph.conf
```

```
rbd_pool = volumes
```

```
rbd_user = cinder
```

```
rbd_secret_uuid = #uuid registrado en los nodos compute.
```

```
rbd_flatten_volume_from_snapshot = false
```

```
rbd_max_clone_depth = 5
```

```
rbd_store_chunk_size = 4
```

```
rados_connect_timeout = -1
```

Configuramos el nombre de la región en el archivo.

```
sudo nano /etc/nova/nova.conf
```

Creamos el siguiente archivo

```
sudo nano /etc/tgt/conf.d/cinder.conf
```

Agregamos lo siguiente

```
include /var/lib/cinder/volumes/*
```

Agregamos lo siguiente en [cinder].

```
[cinder]
```

```
os_region_name = RegionOne
```

Creamos un catálogo de objetos

```
openstack catalog show object-store
```

Reiniciamos los servicios

```
sudo service nova-api restart
```

```
sudo service tgt restart  
sudo service cinder-volume restart  
sudo service cinder-scheduler restart  
sudo service apache2 restart  
sudo service cinder-backup restart
```

6.5 Conectar regiones.

Una vez finalizada la configuración oficial de los nodos controller y compute se debe proceder con una copia de seguridad de los datos actuales de las instancias, para posteriormente migrarlos a las bases de datos de los servicios en el clúster de MariaDB, a su vez, debe tomar en cuenta que se debe crear una base de datos individual por región para cada servicio.

Una vez migradas las bases de datos, puede iniciar a modificar los archivos de configuración de los servicios de openstack. Con el propósito consumir los servicios preveidos por la región principal.

6.5.1 Glance

Iniciamos modificando los endpoint de la base de datos, y en este caso, el nombre de la base de datos se debe modificar para evitar posibles conflictos. Se sugiere agregar un prefijo “regionone_” antes del nombre de la base de datos. Se está consumiendo también el servicio de cache y los endpoints de autenticación apuntan al nodo keystone de la infraestructura.

Abrimos el archivo de configuración.

```
sudo nano /etc/glance/glance-api.conf
```

Modificamos las siguientes secciones.

```
[database]
```

```
connection = mysql+pymysql://glance:GLANCE_DBPASS@100.123.47.17/glance_#
```

```
[keystone_authtoken]
```

```
www_authenticate_uri = http://100.118.19.86:5000
```

```
auth_url = http://100.118.19.86:5000  
memcached_servers = 100.91.68.101:11211  
auth_type = password  
project_domain_name = Default  
user_domain_name = Default  
project_name = service  
username = glance  
password = GLANCE_PASS
```

```
[oslo_limit]
```

```
auth_url = http://100.118.19.86:5000  
auth_type = password  
user_domain_id = default  
username = glance  
system_scope = all  
password = GLANCE_PASS  
endpoint_id = af492800330346e694f30d7b9f606fb6 # su id real.  
region_name = RegionOne
```

6.5.2 Placement

De la igual forma que glance, es necesario apuntar la autenticación al nodo correspondiente, así como los servicios de base de datos deben apuntar a maxscale.

Debemos abrir el archivo de configuración.

```
sudo nano /etc/placement/placement.conf
```

Modificaremos las siguientes secciones

```
[keystone_authtoken]  
auth_url = http://100.118.19.86:5000/v3  
memcached_servers = 100.91.68.101:11211
```

```
[placement_database]  
connection =  
mysql+pymysql://placement:PLACEMENT_PASS@100.123.47.17/placement_#
```

6.5.3 Nova

Con respecto al servicio de nova, se deben configurar el nodo de autenticación principal, la base de datos y la cola de mensajes. Hay que tener en cuenta, es que si se cambia el nombre de la base de datos “nova” el nombre de la base de datos de célula “cell0” debe llevar el nuevo nombre de la base de datos nova, más el sufijo “_cell0”.

Modificaremos el archivo de configuración.

```
sudo nano /etc/nova/nova.conf
```

Modificamos las siguientes secciones:

```
[DEFAULT]  
transport_url = rabbit://region#:RABBIT_PASS@100.79.203.120//region#
```

```
[api_database]  
connection = mysql+pymysql://nova:NOVA_PASS@100.123.47.17/nova_#_api
```

```
[keystone_authtoken]  
www_authenticate_uri = http://100.118.19.86:5000/  
auth_url = http://100.118.19.86:5000/  
memcached_servers = 100.91.68.101:11211
```

```
[neutron]  
auth_url = http://100.118.19.86:5000
```

```
[placement]  
auth_url = http://100.118.19.86:5000/
```

```
[service_user]
```

```
auth_url = http://100.118.19.86:5000/
```

6.5.4 Neutron

Al igual que nova, neutron tiene las mismas configuraciones, lo que resulta fácil encontrar los puntos que se van a cambiar.

Abrimos el archivo de configuración.

```
sudo nano /etc/neutron/neutron.conf
```

Modificamos las siguientes secciones.

```
[DEFAULT]
```

```
transport_url = rabbit://region#:RABBIT_PASS@100.79.203.120//region#
```

```
[database]
```

```
connection = mysql+pymysql://nova:NOVA_PASS@100.123.47.17/nova_#_api
```

```
[keystone_authtoken]
```

```
www_authenticate_uri = http://100.118.19.86:5000/
```

```
auth_url = http://100.118.19.86:5000/
```

```
memcached_servers = 100.91.68.101:11211
```

```
[nova]
```

```
auth_url = http://100.118.19.86:5000
```

6.5.5 Horizon

En los archivos de configuración debe modificar las referencias a al servicio de autenticación.

```
sudo nano /etc/apache2/conf-available/openstack-dashboard.conf
```

Modificamos lo siguiente

```
CACHES = {  
    'default': {  
        'BACKEND': 'django.core.cache.backends.memcached.PyMemcacheCache',  
        'LOCATION': '100.91.68.101:11211',  
    },  
}  
OPENSTACK_HOST = "100.118.19.86"  
OPENSTACK_KEYSTONE_URL = "http://%s:5000/identity/v3"  
OPENSTACK_HOST
```

En este momento, se están consumiendo los servicios de la infraestructura.

7 CONFIGURACIÓN DEL SERVICIO DE PBX.

7.1 Instalación del servidor de Issabel en cada región.

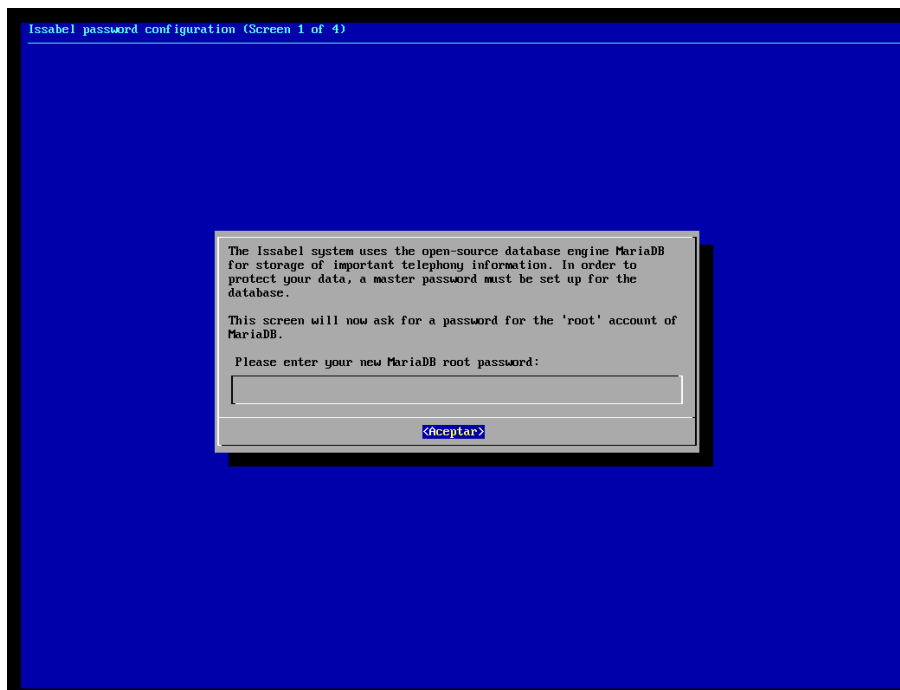
Primero debemos descargar la imagen iso desde el portal de Issabel. Una vez descargado procedemos a subir la imagen en cada región por medio del panel de administración de Openstack.

Cuando ya se haya subido la imagen, iniciamos una instancia seleccionando la imagen previamente subida y especificando los recursos que va a consumir la instancia.

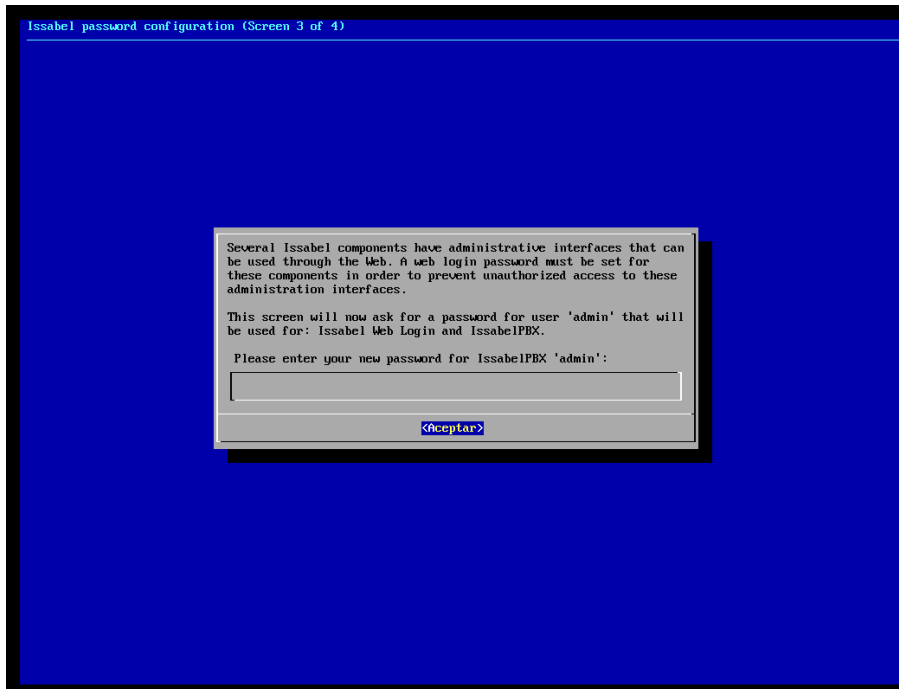
Una vez iniciada procedemos con la instalación de Issabel, debemos especificar la configuración del sistema operativo y hacemos el clic en el botón “Comenzar instalación” para continuar con la instalación.



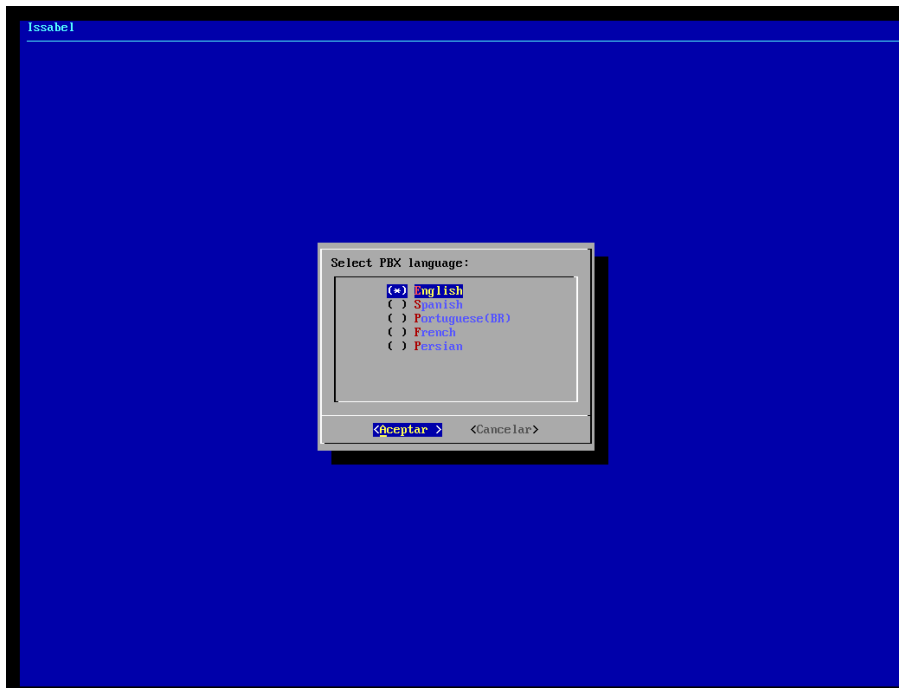
Una vez completada la instalación se nos solicitará que ingresemos la contraseña de la base de datos.



Así mismo debemos especificar la contraseña del administrador para acceder al panel de control de Issabel.



Luego de definir las credenciales se nos solicitará que seleccionemos el idioma que se utilizará en el panel de control de Isabbel.



Luego de haber completado esos pasos podremos iniciar sesión en la terminal y ya nos aparece la url a la que podemos acceder al panel de control del PBX.

```
Rocky Linux 8.8 (Green Obsidian)
Kernel 4.18.0-477.27.1.el8_8.x86_64 on an x86_64

issabel login: admin
Password:

 0 0 0 Issabel is a product meant to be configured through a web browser.
 0 0 0 Any changes made from within the command line may corrupt the system
 0 0 0 configuration and produce unexpected behavior; in addition, changes
 0    made to system files through here may be lost when doing an update.

To access your Issabel System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:

https://192.168.122.118

Your opportunity to give back: http://www.patreon.com/issabel

System load: 0.07 (1min) 0.25 (5min) 0.15 (15min)      Uptime: 5 min
Asterisk: OFFLINE
Memory: [====>-----] 12% 456/3921M
Usage on /: [=====>-----] 13% 4.3/25G
Swap usage: 0.0%
SSH logins: 1 open sessions
Processes: 168 total, 7 yours

[admin@issabel ~]$ _
```