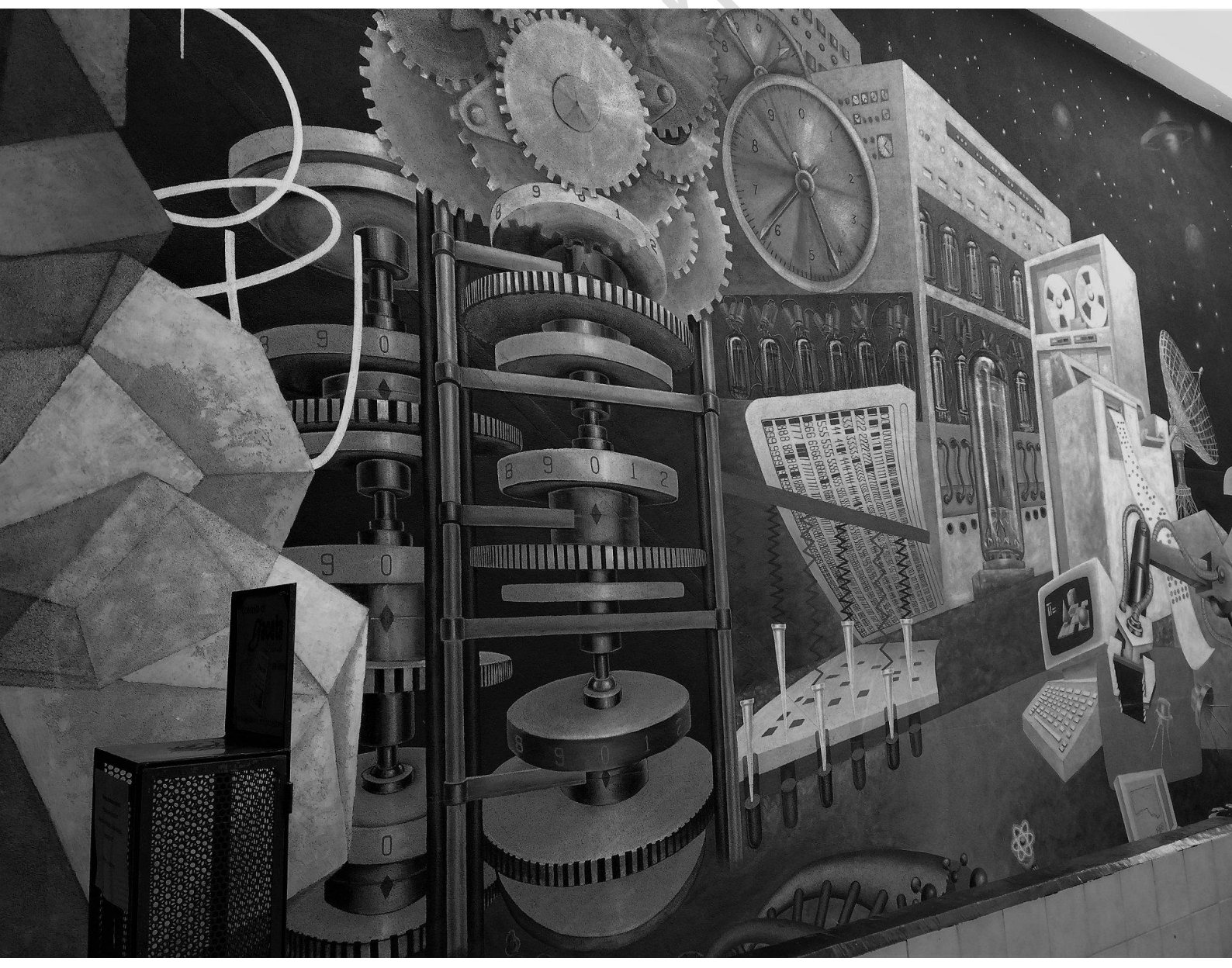

Diseño del proyecto de colaboración de la NUBE regional 2023

revisión



Contenido

Presentación:..... 3

Nube regional de la Red de Macrouiversidades 3

Objetivo..... 3

Alcance 3

Beneficios esperados 3

Retos. 4

Marco de referencia 4

Nube comunitaria 4

IaaS..... 4

Bóveda Digital..... 4

OpenStack..... 4

Desarrollo del Proyecto 5

Instituciones participantes..... 5

Hoja de ruta..... 5

Hitos 5

Cronograma de actividades..... 5

Grupo de trabajo..... 6

Servicios 7

Descripción técnica 8

Software 8

Descripción de los módulos..... 8

Topología:..... 10

Comunicación en red:..... 11

Disponibilidad de Infraestructura:..... 11

Avance del proyecto 13

Presentación:

La red de Macrouniversidades de América Latina y el Caribe es una organización que conjunta instituciones de rasgos específicos y de características comunes y es por ello que coinciden en requerimientos de cómputo y herramientas para la atención de sus comunidades y el desarrollo de sus actividades sustantivas.

Dentro de sus principales objetivos destacan los de:

- Establecer sistemas y mecanismos que permitan compartir la utilización de la infraestructura científico, tecnológica, de información y comunicación de las Instituciones Integrantes, e
- Incrementar el trabajo en redes académicas para propiciar proyectos conjuntos en la Región; así como definir y organizar programas de formación universitaria y de investigación.

Para el cumplimiento de estos objetivos, se realizó el “Taller de avances, reflexiones y perspectivas de la cooperación en TIC de las Macrouniversidades, efectuado el 8 de noviembre de 2022 y siendo anfitriona la Universidad Nacional de Colombia, donde, entre varios proyectos, se planteó la creación de una nube de cómputo regional para compartir recursos y servicios.

Como resultado de dicha actividad se integró un grupo de trabajo para establecer la propuesta de creación de la nube regional con la participación de la Universidad de Costa Rica (UCR), la Universidad de El Salvador (UES) y la Universidad Nacional Autónoma de México (UNAM).

Nube regional de la Red de Macrouniversidades

Objetivo

Establecer un esquema de colaboración para compartir servicios de nube que permitan a las Macrouniversidades de la región, extender sus capacidades de cómputo, almacenamiento y red.

Alcance

Las Macrouniversidades ofrecen un conjunto de recursos y servicios de nube privada en un modelo de infraestructura como servicio (IaaS) y Bóveda Virtual para que las instituciones integrantes de la Red accedan a estos recursos bajo criterios de asignación acordados, que les permitan contar con alternativas competitivas a las ofertas comerciales en un esquema de colaboración institucional.

Beneficios esperados

- Al contar con la colaboración de las Macrouniversidades se crean opciones de servicios de nube privada en infraestructura propia de las instituciones miembro de la red como una oferta más a las existentes en el mercado
- Se favorece el intercambio de experiencias en la administración y uso de esquemas de consumo de servicios de TIC basados en modelos de nube.
- Se cuenta con opciones para fortalecer los planes de recuperación ante desastres de los servicios críticos de las Macrouniversidades

Retos.

- Contar con infraestructura para colaborar en la conformación de la nube.
- Tener conectividad suficiente para los Centros de Datos que proporcionen el servicio.
- Establecer acuerdos normativos que regulen la integración y el uso del servicio.
- Contar con personal capacitado.

Marco de referencia

Nube comunitaria

Con base en la experiencia en la operación y construcción de nubes privadas, el grupo de desarrollo de la nube regional estableció la conveniencia de interconectar la infraestructura de cada institución, bajo un esquema de nube comunitaria. Esto es, la nube regional de las Macrouiversidades operará como un conjunto de recursos de las nubes privadas interconectadas a través de clientes seguros bajo el protocolo de redes virtuales privadas (VPN). La infraestructura que se interconectará en un inicio será de la UES y la UNAM.

IaaS

La Infraestructura como Servicio (IaaS) permite acceder a recursos de cómputo en un Centro de Datos, con la flexibilidad de solicitar las capacidades de procesamiento y almacenamiento adecuadas para el sistema o servicio de información que se requiera publicar. Es similar a los servidores físicos alojados en algún sitio con condiciones de operación que incrementan su disponibilidad y seguridad.

Bóveda Digital

Servicio para conservar en el largo plazo información de carácter institucional que no cambia o no lo hace frecuentemente, debido a sus características.

Es un recurso tecnológico para la preservación de datos digitales en cualquier formato, que no requieren ser consultados continuamente o tienen niveles mínimos de transacciones en períodos prolongados de tiempo. Se apoya en infraestructura para almacenamiento a largo plazo por medio de cintas magnéticas y un subsistema de lectura y escritura en disco duro.

OpenStack

OpenStack es una plataforma de tecnología open source que utiliza recursos virtuales agrupados para diseñar y gestionar nubes privadas y públicas.

OpenStack por sí solo no virtualiza los recursos, sino que los utiliza para diseñar nubes.

Openstack proporciona y orquesta los recursos necesarios para el cloud computing: una red, recursos agrupados, una interfaz de usuario, la capacidad de implementación y el control o la asignación de recursos de forma automática.

La arquitectura de OpenStack está constituida por una gran cantidad de proyectos open source.

Desarrollo del Proyecto

Esta sección describe el diseño y estrategia de implementación creada por el grupo de trabajo.

Instituciones participantes

Los trabajos iniciales se realizaron con la participación de tres universidades, la Universidad de Costa Rica, la Universidad del Salvador y la Universidad Nacional Autónoma de México.

La Universidad de Costa Rica colaborara en el diseño de la nube regional, además de asistir a cada una de las reuniones y su principal necesidad es contar con un respaldo de su información fuera de sitio.

La Universidad del Salvador colaborara con recursos humanos y hardware para montar el piloto de la nube regional.

La Universidad Nacional Autónoma de México participara con recursos humanos y hardware para el piloto de la nube regional, y fungira como gestor del proyecto.

Hoja de ruta

Hitos

- Definición de la plataforma de compartición de infraestructura (análisis para EGI Open Stack). Primer trimestre de 2023
- Definición y alcance de los servicios. Primer trimestre de 2023
- Elaboración del documento del diseño del proyecto de colaboración de compartición de servicios de nube. Segundo trimestre de 2023.
- Elaboración de lineamientos y políticas (generales y por servicio). Segundo y tercer trimestre de 2023.
- Elaboración de convenios de colaboración. Tercer trimestre de 2023
- Establecimiento de plan de capacitación. Cuarto trimestre de 2023.
- Elaboración de materiales de capacitación. Cuarto trimestre de 2023 y primero de 2024
- Establecimiento de la mesa de ayuda. Cuarto trimestre de 2023
- Infraestructura piloto operando. Primer trimestre de 2024
- Capacitación. Primer trimestre de 2024.
- Contar con 5 macrouiversidades con infraestructura compartida
- Contar con 10 macrouiversidades usuarias

Cronograma de actividades

| Hitos | Trimestres 2023 | | | | Trimestres 2024 | | | |
|---|-----------------|----|-----|----|-----------------|----|-----|----|
| | 1er | 2° | 3er | 4° | 1er | 2° | 3er | 4° |
| Definición de la plataforma de compartición de infraestructura (análisis para EGI Open Stack). | | | | | | | | |
| Definición y alcance de los servicios. | | | | | | | | |
| Elaboración del documento del diseño del proyecto de colaboración de compartición de servicios de nube. | | | | | | | | |
| Elaboración de lineamientos y políticas (generales y por servicio). | | | | | | | | |
| Elaboración de convenios de colaboración. | | | | | | | | |
| Establecimiento de plan de capacitación. | | | | | | | | |

| | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|
| Elaboración de materiales de capacitación. | | | | | | | | | |
| Establecimiento de la mesa de ayuda. | | | | | | | | | |
| Infraestructura piloto operando. | | | | | | | | | |
| Capacitación. | | | | | | | | | |
| Contar con 5 macrouniversidades con infraestructura compartida | | | | | | | | | |
| Contar con 10 macrouniversidades usuarias | | | | | | | | | |

Grupo de trabajo

A partir del Taller de Colombia, se estableció un grupo de trabajo con el personal de las instituciones que incluyó a quienes tomarían decisiones, quienes harían el desarrollo de la infraestructura base de la nube de cómputo, así como quienes realizarían la documentación del proyecto.

| Nombre | Rol | Atribuciones |
|----------------------------------|-------------------------|--|
| Mtra. Lourdes Velázquez Pastrana | Patrocinador | Toma de decisiones directivas |
| Ing Damian Morales | Líder técnico | Tomar decisiones técnicas |
| Ing. Javier Mejía | TécnicoS | Ejecutar trabajo técnico |
| Ing. Víctor Calles | TécnicoS | Ejecutar trabajo técnico |
| Mtro. Jesus Fernandez | TécnicoU Coordinador | Ejecutar trabajo técnico Coordinar reuniones Reportar avances (Documentar) |
| Ing. Pedro Bautista | TécnicoU | Ejecutar trabajo técnico |
| Ing. Wilfredo Fonseca | TécnicoCR | Colaboración técnica |

Con base en su formación, experiencia y responsabilidades al interior de sus instituciones, el grupo de trabajo se conformó como se indica en la siguiente matriz RACI

| | Patrocinador | Lider Técnico | TécnicoS | TécnicoU | TecnicoCR | Coordinador |
|---|--------------|---------------|----------|----------|-----------|-------------|
| Definición de la plataforma de compartición de infraestructura (análisis para EGI Open Stack). | I | A | C | C | C | I |
| Definición y alcance de los servicios. | I | A | C | C | C | C |
| Elaboración del documento del diseño del proyecto de colaboración de compartición de servicios de nube. | A | I | I | I | I | R |

| | | | | | | |
|---|---|---|---|---|---|---|
| Elaboración de lineamientos y políticas (generales y por servicio). | R | I | R | R | R | R |
| Elaboración de convenios de colaboración. | R | C | C | C | C | C |
| Establecimiento de plan de capacitación. | I | A | C | C | C | R |
| Elaboración de materiales de capacitación. | I | I | R | R | R | I |
| Establecimiento de la mesa de ayuda. | A | A | R | R | R | I |
| Infraestructura piloto operando. | I | I | R | R | I | I |
| Capacitación. | C | C | R | R | R | R |
| Contar con 5 macrouniversidades con infraestructura compartida | C | I | | | | I |
| Contar con 10 macrouniversidades usuarias | C | I | | | | I |

El equipo técnico ha establecido reunirse cada 15 días aproximadamente, dependiendo de la disponibilidad de los participantes y generó un grupo de Microsoft Teams con un repositorio documental en el drive de Google.

Además del grupo de trabajo técnico, se incluyeron los representantes de las áreas jurídicas respectivas para el desarrollo de los instrumentos legales que sustentarán la participación y colaboración de las universidades miembros de la Red de Macrouniversidades.

Servicios

Para el proyecto se estableció contar con dos zonas de disponibilidad inicialmente, una en la UES y otra en la UNAM configurados para ofrecer el servicios de IaaS. Esto, utilizando la infraestructura de cómputo disponible para ello en cada una de las instituciones, por lo que no hubo una ampliación de capacidades ni actualizaciones de versiones de software.

A partir de la experiencia del personal técnico de las mismas instituciones, que operan sus propias nubes de cómputo privadas, se concluyó ofrecer como servicios:

IaaS. Basado en la configuración de la nube privada de la UNAM, este servicio permitirá acceder a recursos de cómputo en la UES y la UNAM con la flexibilidad de solicitar las capacidades de procesamiento y almacenamiento adecuadas para el sistema o servicio de información que se requiera publicar por institución usuaria.

Bóveda digital. Ideal para guardar datos importantes y en caso de contingencia tenerlos disponibles.

Descripción técnica

Software

Para la elección del software se definieron las siguientes consideraciones.

- Software de uso libre para no generar costos de licenciamiento.
- Que tenga una comunidad o empresa que lo soporte.
- Que facilite la administración de la nube-regional y de todas las instituciones participantes

Con base en lo anterior se eligió el siguiente software para el desarrollo de la nube regional:

- Sistema operativo: Ubuntu o Debian
- Plataforma de IaaS: openstack
 - Módulo de autenticación: Keystone
 - Módulo de administración de almacenamiento: Cinder
 - Módulo de administración de red: Neutrón
 - Módulo de administración de imágenes: Glance
 - Portal de administración de tenant: Horizon
- Ceph: Administración de almacenamiento servidores físicos.
- Monitoreo del cluster STF (Service Telemetry Framework): Grafana y prometheus.
- Administración y automatización del cluster: Metal-as-a-Service (MaaS) y juju

Descripción de los módulos

Keystone proporciona la autenticación de clientes, detección de servicios y autorización multi-inquilino distribuida mediante la implementación de la API de identidad de OpenStack. Es compatible con LDAP, OAuth, OpenID Connect, SAML y SQL.

Cinder, es un servicio de almacenamiento de bloques para OpenStack. Virtualiza la gestión de dispositivos de almacenamiento en bloque y proporciona a los usuarios finales una API de autoservicio para solicitar y consumir esos recursos sin necesidad de saber dónde se implementa realmente su almacenamiento o en qué tipo de dispositivo.

Glance los servicios de imágenes incluyen la detección, el registro y la recuperación de imágenes de máquinas virtuales. Glance tiene una API RESTful que permite consultar metadatos de imágenes de máquinas virtuales, así como recuperar la imagen real. Las imágenes de VM disponibles a través de Glance se pueden almacenar en una variedad de ubicaciones, desde sistemas de archivos simples hasta sistemas de almacenamiento de objetos como el proyecto OpenStack Swift.

Horizon es la implementación de la empresa canonical del tablero de OpenStack, que es extensible y proporciona una interfaz de usuario basada en web para los servicios de OpenStack.

Neutron es un proyecto de OpenStack para proporcionar "redes como servicio" entre dispositivos de interfaz de red (p. ej., vNIC) administrados por otros servicios de Openstack (p. ej., nova).

Ceph es una plataforma de almacenamiento definido por software diseñada para las arquitecturas de nube privada. Se puede usar para proporcionar Ceph Object Storage y Ceph Block Device para plataformas de nube Ceph.

Grafana software el cual nos permite consultar, visualizar, alertar y comprender datos sin importar dónde estén almacenados. Con Grafana se pueden crear, explorar y compartir todos los datos a través de hermosos paneles flexibles.

Prometheus es un conjunto de herramientas de monitoreo y alertamiento de sistemas de código abierto creado originalmente en SoundCloud. Desde su creación en 2012, muchas empresas y organizaciones han adoptado Prometheus, y el proyecto cuenta con una comunidad de desarrolladores y usuarios muy activa. Ahora es un proyecto independiente de código abierto y se mantiene independientemente de cualquier empresa.

Maas nos permite automatizar la configuración de la infraestructura a través del autodescubrimiento de servidores y redes.

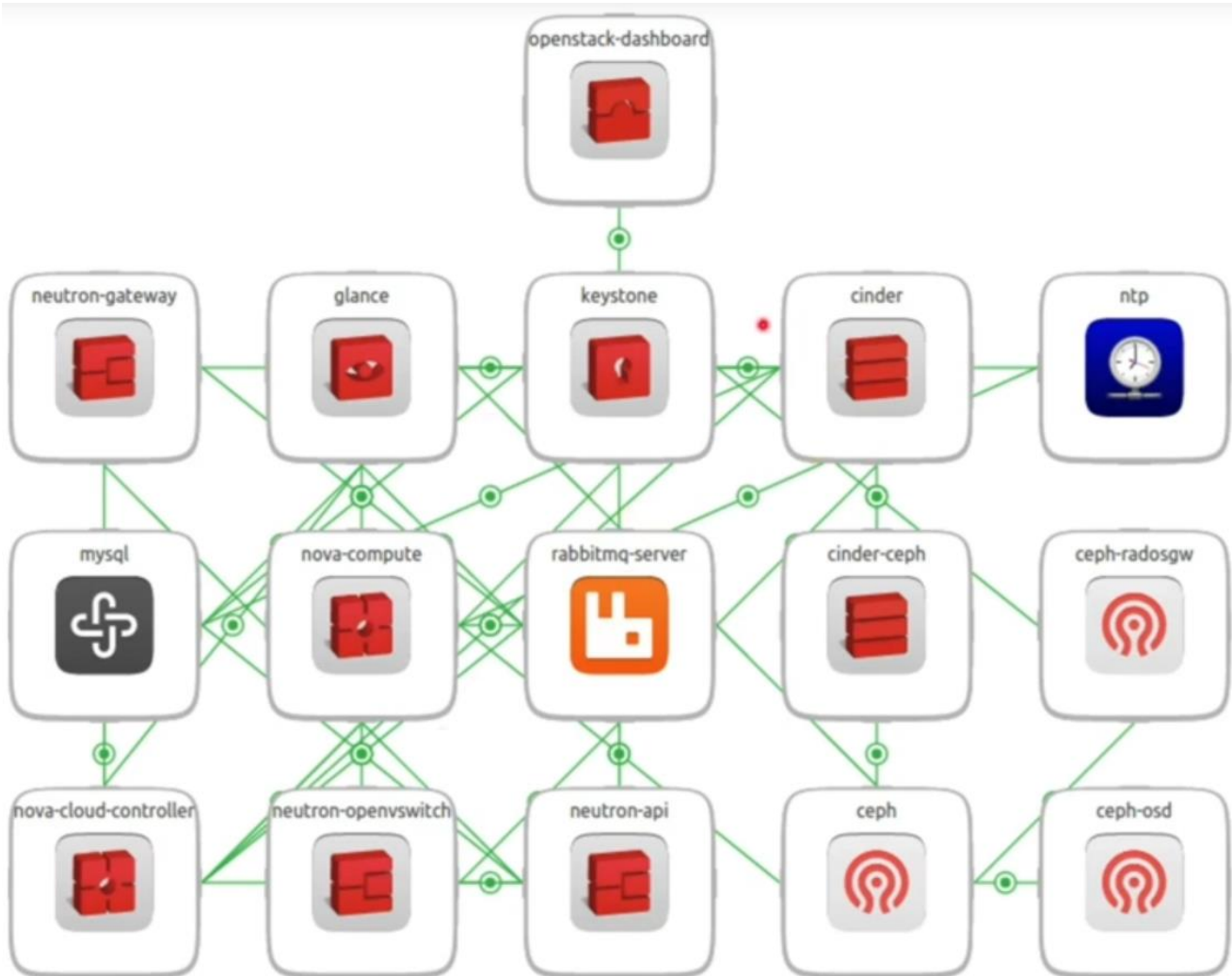
Metal as a Service (MAAS), tiene las siguientes características.

- Nube completa con servidores bajo demanda
- Operaciones remotas de clúster de borde
- Monitoreo y descubrimiento de infraestructura
- Integración de Ansible, Chef, Puppet, SALT, Juju
- Instalación súper rápida desde cero
- VMWare ESXi, Windows, CentOS, RHEL, Ubuntu
- Imágenes personalizadas con aplicaciones preinstaladas
- Configuración de red y disco
- DHCP, DNS, PXE, IPAM controlados por API
- API REST para el aprovisionamiento Autenticación de usuario LDAP
- Control de acceso basado en roles (RBAC)
- Pruebas y puesta en marcha de hardware

Juju es el marco de operación de código abierto que utiliza Charmed Operators, o 'Charms', para implementar infraestructura y aplicaciones en la nube y administrar sus operaciones desde el día 0 hasta el día 2. Con Juju, puede instalar, mantener, actualizar e integrar aplicaciones en clústeres y contenedores de Kubernetes , máquinas virtuales y máquinas bare metal, en nubes públicas o privadas. Tomando el control de un entorno híbrido.

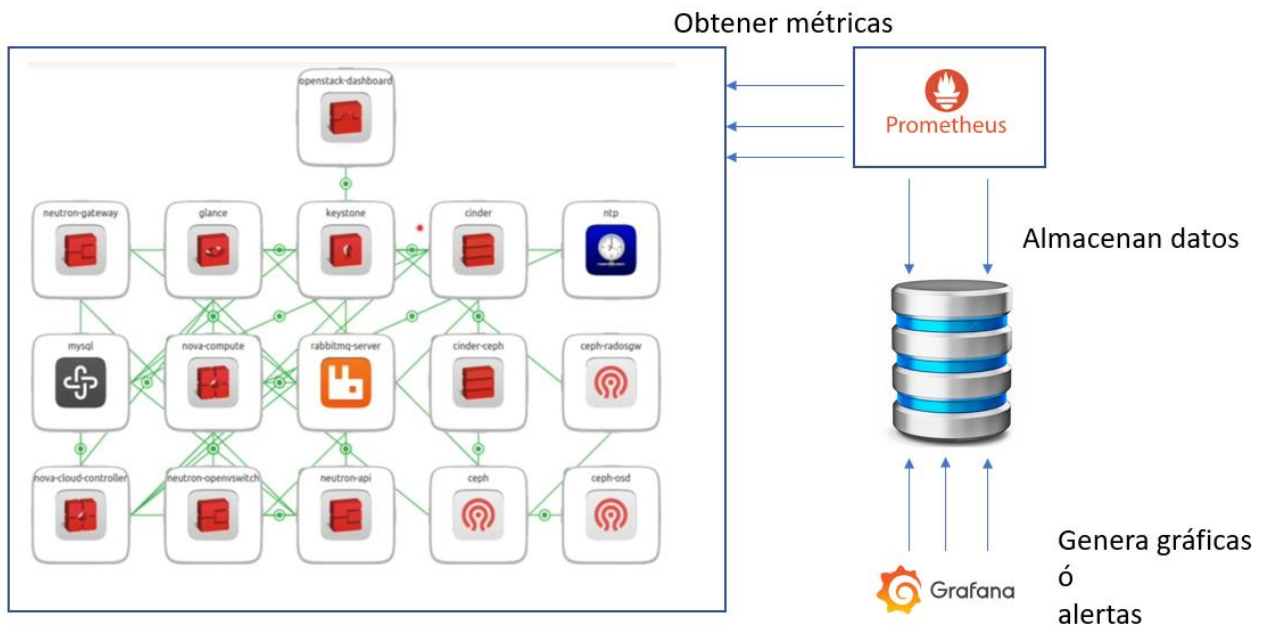
Topología:

Se iniciarán dos zonas de servicio; una en la UES y otra en la UNAM. La anexión de más instituciones se hará con la generación de zonas de servicios con el hardware proporcionado por la universidad anexada. Asimismo, el software seleccionado da la flexibilidad de replicar el sistema de autenticación en cada una de las zonas, a continuación se muestra el digrama mínimo de openstack para cada zona.



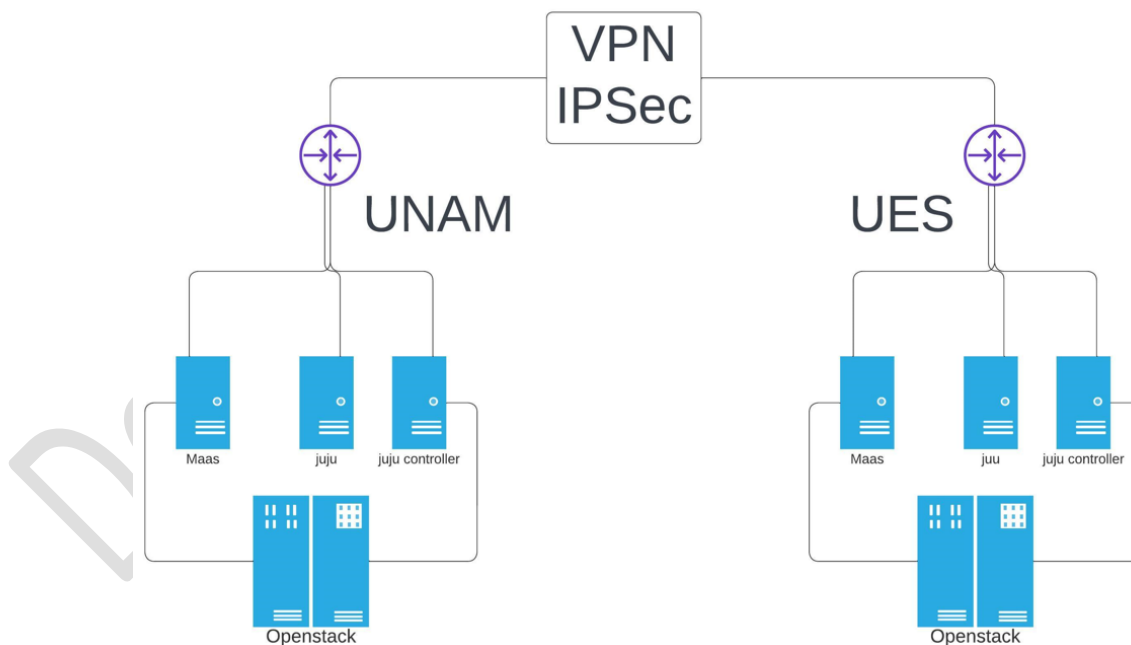
En caso de que una institución solo quiera participar con hardware, se explorara la posibilidad de que se administre su infraestructura de manera remota.

Monitoreo del servicio:



Comunicación en red:

Para realizar la replicación del módulo de autenticación entre las zonas, se usará una VPN (red privada virtual) con el protocolo de comunicación IPsec entre los nodos.



Disponibilidad de Infraestructura:

El desarrollo de la prueba piloto cada institución ha destinado infraestructura para la creación de las dos primeras zonas (nodos o clusters) de la nube regional.

Zona 1 Universidad de El Salvador

- 64VCPU con conectividad en 10GB
- Memoria RAM de 128GB
- Almacenamiento 16 discos de 1.92TB
- RAID 5 actualmente 3.84 TB usables.
- 15 Ips públicas
- Un segundo servidor (posiblemente) 80VCPU tarjeta 1GB y memoria de 128 GB mismo almacenamiento.

Zona 2 Universidad Nacional Autónoma de México

- 3 nodos físicos DELL R620 256 GB de RAM, 2 procesadores e5-2670 8 cores físicos por CPU,
- 2 tarjetas con dos puertos a 10Gb y una tarjeta de 4 puertos a 1GB y dos discos RAID 1 1TB.
- 2TB de almacenamiento base de la SAN
- IPs (falta verlo con el departamento de Redes de la DG TIC)

Avance del proyecto

| Producto | Institución | Fecha y porcentaje |
|---|-------------|--------------------|
| Instalación de MAAS | UNAM | 2023/09/19 100% |
| | UES | 2023/09/19 100% |
| Configuración de MAAS | UNAM | 2023/09/19 100% |
| | UES | 2023/09/19 100% |
| Instalación de juju | UNAM | 2023/09/19 100% |
| | UES | 2023/09/19 100% |
| Configuración de juju | UNAM | 2023/09/19 100% |
| | UES | 2023/09/19 100% |
| Instalación de servidores | UNAM | 2023/09/19 100% |
| | UES | 2023/09/19 100% |
| Instalación componentes de openstack | UNAM | 2023/09/19 100% |
| | UES | 2023/09/19 100% |
| Verificación de funcionalidad | UNAM | |
| | UES | 2023/09/19 100% |
| Pruebas de conectividad entre las zonas | UNAM | |
| | UES | 2023/09/19 100% |
| Replicación de componentes | UNAM | |
| | UES | |
| Verificación de replicación | UNAM | |
| | UES | |
| Pruebas finales | UNAM | |
| | UES | |

Actualmente se cuenta con una guía realizada por la UES con una configuración base, que tiene dos zonas de disponibilidad. Ellos ya validaron la funcionalidad y la conectividad entre estas dos zonas.

Esta configuración base, será replicada en la UNAM en las siguientes dos semanas, y teniendola operativa, se coordinara la configuración para unir las zonas de disponibilidad de la UES con las de la UNAM.

Documento en revisión