

IMPLEMENTACIÓN DE UNA NUBE PRIVADA EN EL ITCV

Gamaliel Martínez Ibarra¹

Resumen—Actualmente el cómputo en nube es una herramienta que proporciona elasticidad y optimización de recursos computacionales a las organizaciones. Para una organización, implementar una nube privada conlleva al control y manejo de datos, sin embargo la administración de ésta recae sobre la organización. Para el Tecnológico de Cd. Victoria es importante administrar los recursos de hardware existentes de tal forma que se vean como un todo y distribuirlo en porciones adecuadas a las necesidades de los proyectos. La implementación de la nube privada en la institución tiene como objetivo no perder el acceso a los recursos aún si falla el internet. En este trabajo se propone un modelo de cómputo en nube privado que puede operar en sitios remotos mediante comunicaciones seguras. La implementación se realizó sobre máquinas virtuales dentro de un servidor físico y es capaz de brindar recursos de cómputo de acuerdo a la capacidad de los proyectos.

Palabras clave—cómputo en nube, automatización, orquestación, redes de computadoras.

Introducción

La implementación de cómputo en nube, en una institución no se puede tomar de forma trivial, existen requisitos en la documentación que al compararse con las características del equipo con el que se cuenta, que en forma teórica se pueden cumplir, sin embargo en la práctica existen detalles que pueden facilitar o complicar la implementación. Además es importante contar con una infraestructura de red adecuada, ya que el diseño de la red física impacta en la intercomunicación de las máquinas virtuales dentro de la nube.

En este trabajo se aborda la implementación de una nube escalable mediante el uso de la orquestación con el hardware disponible en el Instituto Tecnológico de Ciudad Victoria como una solución para explotar los recursos de cómputo que se encuentran distribuidos en el mismo y con el fin de construir las bases para dar soporte para las nuevas tecnologías como es Grandes Datos (Big Data) o el Internet de las cosas (Internet of Things).

Marco Teórico

Reseña del Cómputo en nube

En el ámbito de las tecnologías de la información y comunicación (TIC), las revistas y la publicidad han creado mucho contenido acerca del Cómputo en Nube, pero esto difiere ampliamente de lo que constituye en realidad el Cómputo en Nube (Coyne Larry et al. 2016) esto se debe a que los proveedores de servicios en la nube mezclan características de la nube con características propias, dificultando al usuario poderlas diferenciar.

El término "nube" proviene de una metáfora utilizada comúnmente en el mundo de las telecomunicaciones, en donde se utiliza el símbolo de una nube para representar un medio de transmisión que se presume disponible para transferir información sin tener que preocuparse de la infraestructura que lo soporte (López David, 2013). La idea de utilizar el símbolo de la nube en el mundo de las telecomunicaciones se extendió para ser utilizada en el Cómputo en nube, con la idea de facilitar el concepto a las personas no apegadas a dicha tecnología.

En primera instancia se puede relacionar al Cómputo en nube como un conjunto de tecnologías y servicios. Dicho conjunto, permite trabajar los recursos informáticos de una forma más eficiente, con altos niveles de automatización (Rountree Derrick y Castrillo Ileana, 2014).

Desarrollo

Actualmente existen varias herramientas que permiten implementar una nube en el Instituto Tecnológico de Ciudad Victoria de entre ellas se realizó un análisis para seleccionar el mejor conjunto que diera lugar a crear una nube orquestada. En relación al software para implementar nubes se identificaron las herramientas: OpenStack, Apache CloudStack, OpenNebula, Eucalyptus, según en (Omar Sefraoui et al, 2012) OpenStack representa la mejor opción, ya que tiene mejor soporte en los temas de instalación, almacenamiento, red, seguridad, escalabilidad y documentación. Con la finalidad de automatizar la instalación y configuración del sistema operativo se encontró el software Ubuntu MaaS. En el caso de las tecnologías para orquestación, se identificó: Chef, Puppet y JuJu.

Se optó por elegir a MaaS y JuJu porque su trabajo en conjunto logra la automatización y orquestación como un flujo continuo de trabajo, al contrario que las demás tecnologías en donde se tiene que crear un puente para conectar la automatización y orquestación. Finalmente, entre las tecnologías disponibles para realizar comunicaciones seguras se encuentran: OpenVPN, FreeSWAN, OpenSWAN, StrongSWAN. En este caso se eligió StrongSWAN

¹ Gamaliel Martínez Ibarra es Alumno de la Maestría en Sistemas Computacionales del TNM Instituto Tecnológico de Ciudad Victoria, Tamaulipas. gamamtz@gmail.com (autor corresponsal)

por que existe una comunidad activa que lo respalda y mantiene las actualizaciones tener actualizaciones. Con el conjunto de herramientas seleccionadas, se diseñó una arquitectura, la cual se describe en la siguiente sección.

Arquitectura Propuesta.

La arquitectura que se muestra en la figura 1 permite crear una nube que se pueda escalar utilizando equipo local o remoto. La arquitectura consta de 5 capas que se muestran en la figura 2, el bloque A representa la base para el resto. En la capa A se encuentra todo el soporte red, es decir, los protocolos de comunicación y seguridad, los dispositivos de red como conmutadores, enrutadores y puertas de enlaces. La capa B es la encargada del proceso de automatización, en esta capa se encuentran los servidores, los nodos y el software para llevar a cabo dicha tarea. La capa C realiza la instalación de openstack de forma orquestada, es decir, se apoya en la capa B para preparar el equipo y la capa C lleva el control de la instalación y de errores. El OpenStack es el controlador de la nube, este se encuentra en la capa D, éste ofrece la Infraestructura como Servicio, lo que permite a los usuarios de OpenStack (la nube) crear máquinas virtuales para sus proyectos, sin la intervención de un administrador. Y por último se encuentra la capa E, donde un usuario de la nube puede utilizar la misma orquestación de la capa C para instalar los servicios que requiera de forma orquestada. Las secciones A-E describen cada capa.

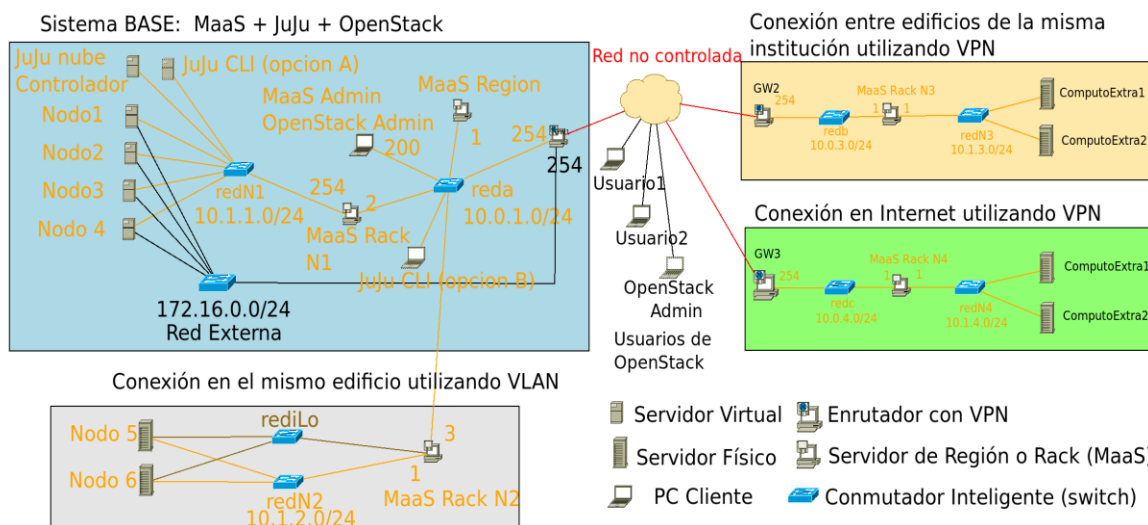


Figura 1. Arquitectura implementada.



Figura 2. Capas de la arquitectura propuesta.

A) Redes.

En esta capa se crearon los diagramas red para la comunicación interna entre los servidores, locales y remotos. La seguridad es administrada mediante la tecnología VLAN utilizando el estándar de la IEEE 802.1q, lo cual permite separar el tráfico de terceros del tráfico de la solución propuesta. Los servidores remotos utilizan el protocolo de comunicación VPN, que cifra el tráfico para ser utilizado en redes no controladas o no seguras. Esta capa también cuenta con el enrutado de las redes que se utilizarán para lograr comunicación entre los servidores locales y remotos. En la figura 3 se muestra un ejemplo de una VPN, en donde el tráfico del nodo A que va dirigido al nodo B (y viceversa) pasa a través del túnel (línea azul) seguro creado por las puertas de enlace que existen en cada red, el tráfico que no se dirige hacia al nodo B, se dirige hacia Internet (línea roja) para cualquiera de los dos nodos.

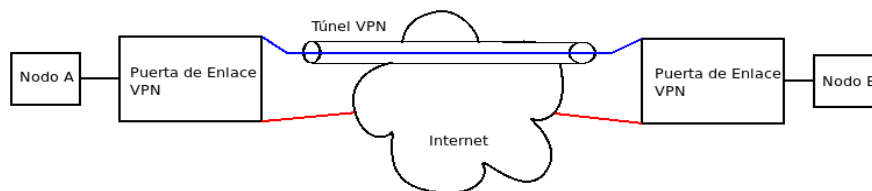


Figura 3. Concepto simple de VPN (StronSwan,2016).

B) Automatización en Hardware.

Capa cuya funcionalidad se centra en la automatización de la instalación y configuración del sistema operativo en los nodos. Para ello se instaló el software Ubuntu Metal as a Service (MaaS), este software se divide en dos partes, el controlador de región y el controlador de rack como se muestra en la figura 4, el controlador de región tiene a su cargo uno o varios controladores de rack, que se encarga de la interfaz WEB, de la API para integrarse con otras aplicaciones y guarda el estado (encendida, apagada, con error, en despliegue) de los nodos. El controlador de rack es quien se comunica directamente con el nodo a configurar, este contiene las herramientas necesarias para el encendido, instalación y configuración del nodo(Ubuntu MaaS,2017). También es el encargado de encender el nodo de cómputo, pero para realizar dicha acción es necesario de una tecnología adicional que permita el encendido remoto cuando el nodo se encuentre apagado, las tecnologías a utilizadas son: Intel Active Management Technology (AMT) y Hewlett Packard Integrated Lights-Out (HP iLO) las cuales son un hardware que se encuentra integrado en la tarjeta madre del nodo pero trabaja de forma independiente, permitiéndole el control y encendido remoto incluso cuando la tarjeta madre no responda.

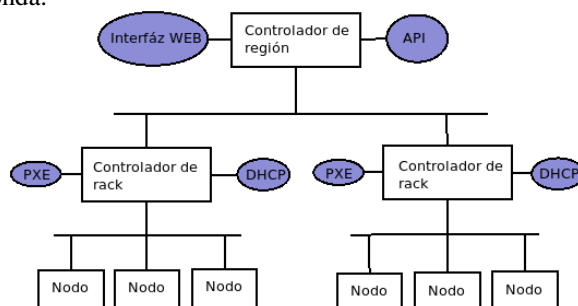


Figura 4. Concepto de Ubuntu MaaS (Ubuntu MaaS,2017).

C) Orquestación de nube.

Esta capa tiene la funcionalidad de orquestar el software de la nube, para esto se utiliza el software Ubuntu JuJu, este se encarga de instalar, configurar, vigilar el software que se le indique. Para ello se utiliza un formato llamado charm, que contiene todas las instrucciones para realizar la instalación y configuración del software. Además tiene la capacidad de ajustar parámetros para personalizar la instalación. El software MaaS se encarga de encender el servidor, instalar el sistema operativo y configurarlo, una vez que esté listo el proceso, le pasa el control a JuJu el cual instala el software de acuerdo a los requerimientos del charm. Durante la implementación se tomó un charm existente de OpenStack y se modificó a las necesidades. En la figura 5 se muestra el diagrama entre JuJu y MaaS, el cliente JuJu es la línea de comandos (CLI) y en él se configura el API key del MaaS, para inicializar el controlador JuJu, este paso solo se realiza una vez, por este motivo la conexión entre el cliente JuJu y el MaaS Región se encuentra en línea punteada. Después de este paso la interacción siempre se realiza con el controlador JuJu, que puede ser mediante el CLI o la interfaz WEB. Cuando se le envía una receta al controlador JuJu este se comunica con la API del MaaS Región solicitando los recursos computacionales que están previamente indicados en la receta, el MaaS Región se encarga de suministrar el equipo encendiéndolo y configurando los nodos disponibles, una vez terminado el proceso pasa el control al controlador JuJu para que este instale y configure el software indicado en la receta. Al final se notifica al cliente que el software se ha instalado(Ubuntu JuJu,2017).

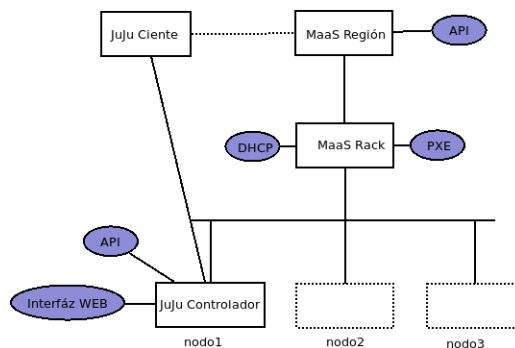


Figura 5. Concepto de JuJu + MaaS(Ubuntu JuJu,2017).

D) Nube.

La capa nube es la encargada de administrar los recursos de hardware disponibles mediante una infraestructura en la que se dividen las tareas en las siguientes áreas: Controlador, encargado de comunicarse con las demás áreas y asignar los trabajos que realizarán manteniendo un estado de los procesos. Almacenamiento, responsable de brindar los datos que se le sean solicitados o el almacenaje de ellos. Cómputo, consta de los servidores que ejecutarán las máquinas virtuales. Red, área que brinda los servicios de red para que las máquinas virtuales puedan comunicarse entre sí. En la figura 6 se muestra el concepto simple. En la nube se crean los proyectos y los usuarios que tendrán acceso a los recursos del hardware, en ella se encuentran as imágenes de los sistemas operativos que el usuario podrá utilizar para las máquinas virtuales, de esta forma el usuario cuenta con la libertad para desplegar máquinas virtuales de acuerdo a sus necesidades sin necesitar la intervención de un administrador(OpenStack, 2016).

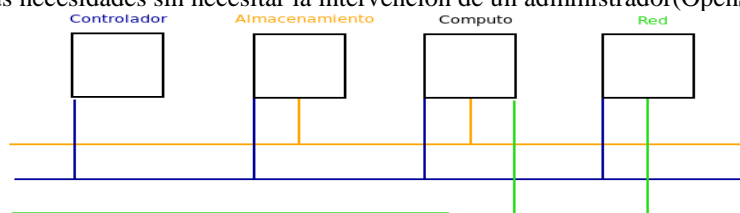


Figura 6. Concepto simple de nube(OpenStack, 2016).

E) Orquestación en nube.

En la última capa, se aprovecha la misma tecnología para instalar la nube, pero para el uso de los usuarios de la nube, en la figura 7 se muestra como se realizan las conexiones, y su funcionamiento es por ejemplo, el administrador puede crear un charm para un servidor web, entonces ese mismo charm puede subirlo para que esté disponible para los usuarios de la nube, entonces estos pueden utilizar el charm para proyectos propios y se evitan la tarea de la instalación y configuración del servidor web y se enfocan en sus investigaciones(Ubuntu JuJu, 2017).

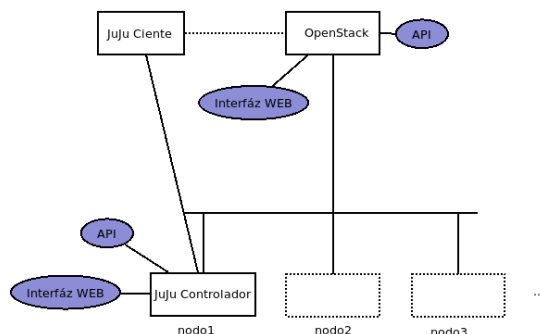


Figura 7. Concepto de JuJu y OpenStack (Ubunru JuJu,2017).

Resultados Experimentales

La nube implementada funciona de manera esperada, al indicar al orquestador escalar la nube en una unidad, este realiza el trabajo de comunicarse con MaaS y solicitar la activación de un nuevo nodo, cuando el nodo esta listo, el orquestador se encarga de instalar el software de la nube al nodo y configurarlo conectándolo a la nube actual. A continuación se muestran tres imágenes de los sistemas implementados (MaaS, JuJu y OpenStack), que se describen a continuación.

En la **figura 8** se muestran las máquinas registradas en MaaS, las máquinas JJClient y JJController son utilizadas para instalar JuJu, y para crear la nube. Las máquinas mario y novel-eft son equipos que sirven para probar la conexión VPN entre edificios. Las máquinas ML350G5 y ML350G6 permiten realizar la conexión en el mismo edificio utilizando VLAN. Finalmente, las máquinas rn1-nodo1 a rn1-nodo4 contienen el sistema base de la nube.

Deployed (11)	FQDN	MAC	Power	Status	Owner	Cores	RAM (GiB)	Disks	Storage (GiB)
<input type="checkbox"/>	JJClient.maas		Unknown	Ubuntu 16.04 LTS	msc	2	2.0	1	64.4
<input type="checkbox"/>	JJController.maas		Unknown	Ubuntu 16.04 LTS	msc	4	4.0	1	64.4
<input type="checkbox"/>	mario.maas		Unknown	Ubuntu 16.04 LTS	msc	12	128.0	2	4480.9
<input type="checkbox"/>	ML350G5.maas		On	Ubuntu 16.04 LTS	msc	8	7.0	2	2147.1
<input type="checkbox"/>	ML350G6.maas		On	Ubuntu 16.04 LTS	msc	4	12.0	2	800.0
<input type="checkbox"/>	novel-eft.maas		Unknown	Ubuntu 16.04 LTS	msc	40	128.0	2	1504.3
<input type="checkbox"/>	rn1-nodo1.maas		Unknown	Ubuntu 16.04 LTS	msc	4	8.0	2	123.5
<input type="checkbox"/>	rn1-nodo2.maas		Unknown	Ubuntu 16.04 LTS	msc	4	8.0	2	123.5
<input type="checkbox"/>	rn1-nodo3.maas		Unknown	Ubuntu 16.04 LTS	msc	4	8.0	2	123.5

Figura 8. Nodos Utilizados en Ubuntu MaaS.

En la **figura 9** se muestra la interfaz gráfica de JuJu, se puede ver una columna a la izquierda en esta se listan los módulos instalados y su cantidad, en el cuadro derecho se muestra un diagrama con las conexiones entre los módulos. En la **figura 10** se muestra el resumen de las máquinas registradas con el módulo compute de OpenStack, en la parte superior se presenta el uso de la cantidad de unidades de procesamiento virtuales (VCPU), la memoria RAM y el almacenamiento. En el recuadro inferior se desglosa la información anterior, ahí se puede apreciar que el nodo mario cuenta con once instancias, es decir, máquinas virtuales, y se puede ver que el nodo ya casi se encuentra en su límite de procesadores virtuales, aunque el límite no es mostrado se puede calcular si se observa el valor en VCPU (total) el cual muestra la cantidad de núcleos que puede utilizar el nodo y se multiplica por dos, dando un total de veinticuatro. En VCPU (usadas) se muestra un valor de veintidós, quedando solo dos núcleos disponibles a utilizar, si bien, en el nodo aun dispone de memoria RAM y almacenamiento, la creación de dos máquinas virtuales más con una necesidad de 4 núcleos virtuales, fueron creadas en el nodo novel-eft, debido a la poca capacidad disponible de procesadores virtuales en mario.

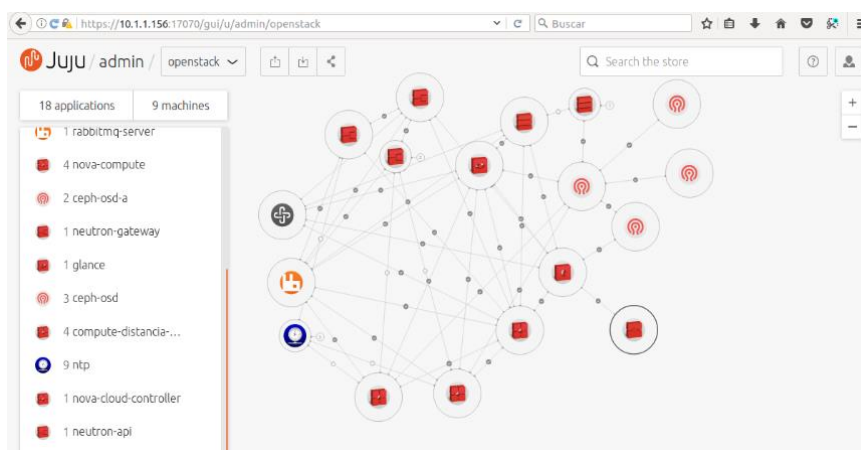


Figura 9. Nodos Receta (Charm) utilizado en Ubuntu JuJu.

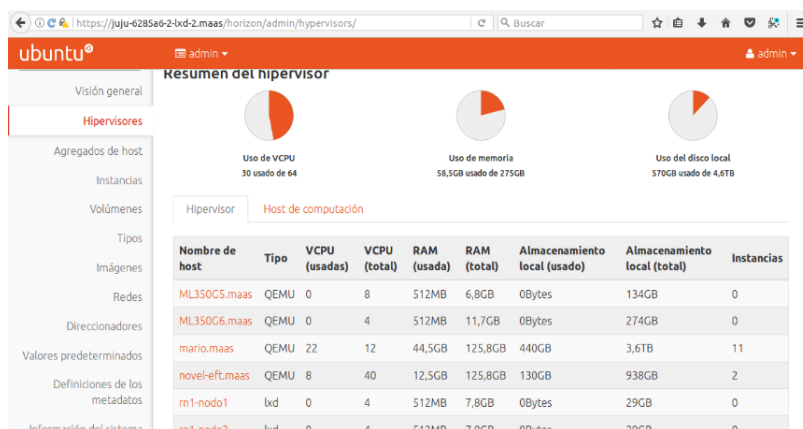


Figura 10. Muestra de los nodos utilizados en OpenStack.

Conclusiones y trabajos futuros

Una forma de aprovechar los recursos de cómputo que se encuentran distribuidos en el Instituto Tecnológico de Ciudad Victoria es mediante el uso de cómputo en nube y al hacerlo de una forma orquestada se obtienen los beneficios como la automatización y el ahorro de tiempo de las tareas repetitivas, la centralización de la configuración en donde se controla la escalabilidad y el mantenimiento de las actualizaciones del software.

Al utilizar la VPN para conectar sitios remotos, se pierde la capacidad de utilizar VLAN, esto es debido a que la VPN no envía tráfico a nivel de VLAN. Este error no es reconocido por el MaaS debido a que no reconoce la existencia una VPN. Aunque en la interfaz del MaaS aparece la opción para reconocer a la VPN, en la práctica no funciona. Como trabajo futuro se recomienda el uso de las Redes Privadas Virtuales Extendidas (VXLAN) ya que son una alternativa reciente para superar las limitaciones de la VPN.

Referencias

Rountree Derrick y Castrillo Ileana. The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice. Syngres is an imprint of Elsevier, 2014.

David López. La “computación en la nube” o “cloud computing” examinada desde el ordenamiento jurídico español. En: Revista de Derecho de la Pontificia Universidad Católica de Valparaíso (2013).

Larry Coyne, Tiberiu Hajas, Magnus Hallback, Mikael Lindström y Christopher Vollmar. IBM Private, Public, and Hybrid Cloud Storage Solutions. IBM. Abr. De 2016.

Omar Sefraoui, Mohammed Assaoui y Mohsine Eleuldj. OpenStack: Toward an Open-Source Solution for Cloud Computing. International Journal of Computer Applications. Oct. De 2012.

StrongSWAN (2016). Documentación oficial, <https://wiki.strongswan.org/projects/strongswan/wiki/IntroductionTostrongSwan>, último acceso: febrero 2018.

Ubuntu Metal as a Service (2017). Documentación oficial, <https://docs.maas.io/2.1/en/>, último acceso: marzo 2018.

Ubuntu JuJu (2017). Documentación oficial, <https://docs.juju charms.com/2.0/en/introducing-2>, último acceso: junio 2018.

OpenStack (2016). Documentación oficial, <https://docs.openstack.org/mitaka/>, último acceso: agosto 2018.