EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico de Matamoros

“APLICACIONES WEB, EVOLUCIÓN, ARQUITECTURA Y PLANIFICACIÓN”

Actividad 1 – Programación WEB | GPO. B

RODRIGO TUDÓN VELÁZQUEZ

19260966

Docente

Ing. Celedonio Covarrubias Ávila

Ingeniería En Sistemas Computacionales

Grupo B | H. Matamoros, Tamaulipas.

Fecha De Entrega:

25 de febrero de 2023

Excelencia en Educación Tecnológica®

Tecnología es progreso®

Contenido

La computación en nube (cloud computing) puede verse como un nuevo estilo de computación en el cual los recursos, dinámicamente escalables y frecuentemente virtualizados, son provistos como servicios sobre Internet. La computación en nube se ha convertido en una tendencia tecnológica significativa y muchos expertos esperan que cambie los procesos y el mercado de las Tecnologías de la Información (IT).

5.1 Conceptos generales.

DEFINICIÓN

Según el Instituto Nacional de Normas y Tecnología (NIST: National Institute of Standards and Technology), la computación en nube es un modelo que permite, convenientemente, el acceso bajo demanda a redes ubicuas para compartir un conjunto configurable de recursos de computación (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden proveer y liberar rápidamente con un mínimo esfuerzo de administración o interacción del proveedor del servicio. Este modelo de nube está compuesto por cinco características esenciales, tres modelos de servicios y cuatro modelos de despliegue.

¿QUÉ SON LOS SERVICIOS EN LA NUBE?

Los servicios en la nube son servicios que se utilizan a través de Internet. Es decir, no están físicamente instalados en tu ordenador. Se trata de un nuevo paradigma que surgió con el advenimiento de la World Wide Web.

Antes de que apareciera la nube, todos los programas informáticos se instalaban en el ordenador. Los servicios en la nube son programas que se alojan en un servidor accesibles desde cualquier dispositivo conectado a Internet.

Las ventajas de este tipo de servicios son evidentes, ya que su uso no está restringido a un solo equipo informático y la seguridad, capacidad de almacenamiento y recursos de la nube son mayores que los de un ordenador.

5.2 TIPOS DE SERVICIOS EN LA NUBE.

Podemos agrupar los servicios de la nube en varias categorías:

Software as a Service (SaaS): Es el más utilizado, pues el software está alojado en servidores de los proveedores y el cliente accede a ellos a través del navegador web. Todo lo relacionado con mantenimiento, soporte y disponibilidad es manejado por el proveedor.

Platform as a Service (PaaS): En este tipo de servicios en la nube el proveedor ofrece acceso a un entorno basado en cloud en el cual los usuarios pueden crear y distribuir sus propias aplicaciones. El proveedor proporciona la infraestructura subyacente.

Infrastructure as a Service (IaaS): Un proveedor de servicios proporciona el software y las aplicaciones a través de Internet. Los usuarios se suscriben al software y acceden a él a través de la web o las APIs del proveedor.

Un usuario estándar normalmente utilizará solo SAAS.

EJEMPLOS DE SERVICIOS EN LA NUBE

En la actualidad todos usamos servicios en la nube, ya sea buscando algo en Google o leyendo nuestro correo de Gmail. Clinic Cloud es un buen ejemplo de servicio en la nube. Se trata de un programa de gestión online de clínicas que incluye el almacenamiento de historial médico en la nube. Se puede utilizar desde un ordenador, Tablet o Smartphone, siendo el único requisito tener conexión a Internet.

5.3 Patrones de diseño

PATRONES DE DISEÑO EN LA NUBE

Disponibilidad está relacionado al tiempo de actividad, con lo cual las aplicaciones en la nube deben diseñarse para poder brindar la mayor disponibilidad posible. Normalmente hay acuerdos de SLA con los proveedores de nube. Para poder verificar la disponibilidad es necesario diseñar:

PATRONES DE MONITOREO DE ESTADO/SALUD DE LOS PUNTOS DE ACCESO/ENTRADA

También conocido como (HEALTH MONITORING OF ENTRY POINTS PATTERN)

Para este caso es necesario implementar herramientas externas a las aplicaciones que controles la disponibilidad y emitan alertas o permitan responder a la disponibilidad. Normalmente dichas herramientas consultan los puntos de entrada de la aplicación y emiten un resultado de estado o realizan un análisis según el resultado para verificar el estado real.

Si no utilizamos herramientas externas podríamos programar servicios que cada cierto tiempo por ejemplo se conecten a la base de datos o intenten acceder a un servicio y con dichos resultados registrar lo que ha ocurrido además de enviar alertas a los subscriptores.

PATRONES DE BALANCEO DE CARGA CON COLAS DE TRABAJO

También conocido como (LOAD BALANCING WITH QUEUES PATTERN)

Para este caso es necesario balancear la carga de tareas de las aplicaciones para evitar cuellos de botella o interrupciones/saturación de los procesos. Normalmente se implementa una cola de procesos donde se cargan las tareas de la aplicación y se van tomando de la cola para ir ejecutándolas. Esto permite suavizar el procesamiento en los periodos de tiempo, evitar cuellos de botella y la caída de procesos o interrupción de servicios por sobrecarga. Por ejemplo, si tenemos un servicio que atiende consultas a la base de datos y lo consulta una cantidad excesiva de clientes, podríamos empezar a recibir timeouts para los distintos solicitantes, ya que en la carga y tiempo de procesamiento de los primeros comienza a saturar el servicio. De esta forma al implementar una cola de procesos podemos nivelar la carga de los procesos y responder a cada uno en forma secuencial. Cabe aclarar que se pueden utilizar distintos patrones y guías de colas de procesos para evitar problemas o mejorar la aplicación.

Esto implicaría por ejemplo patrones de mensajes asincrónicos, patrones de competencia de recursos, patrones que evitan estrangulamiento o cuellos de botella de la cola, patrones de servicios de mensajería, etc. Para este patrón también, si no utilizamos herramientas externas, podríamos desarrollar aplicaciones o servicios de cola que administren las tareas según las necesidades de la aplicación.

PATRÓN DE ESTRANGULAMIENTO

También conocido como (STRANGULATION PATTERN)

Este patrón es utilizado para evitar que el consumo de los recursos genere cuellos de botellas y permita que la aplicación siga funcionamiento correctamente aún cuando todos los recursos están en uso. Por ejemplo, puede ocurrir que en un momento de tiempo todos los usuarios accedan a un servicio particular y dispare los consumos de recursos al máximo permitido, en ese caso, para evitarlo se configuran límites de acceso por usuario, donde cuando se llega al límite se rechaza la comunicación y se le notifica al usuario que el servicio paso el límite o se lo pone en espera hasta que se libere la carga. Con esto evitamos la concurrencia absoluta y los usuarios que se conectan primero o antes del límite siguen teniendo una buena performance, sin problemas de uso. Para este patrón también, si no utilizamos herramientas externas, podríamos desarrollar aplicaciones o servicios o configuraciones que permitan por ejemplo para la situación antes dada el control de usuarios que acceden. Se podrían usar soluciones como estas o también colas de prioridad.

5.4 Estándares en servicios.

Es muy importante saber sobre los estándares en la nube cuando contratamos este servicio, debido a que se incluyen temas como privacidad, confidencialidad, ubicación, propiedad de los datos, uso no autorizado de los datos y los acuerdos de nivel de servicio. Los estándares para los servicios de Computación en la Nube, pueden ser divididos en dos clases: estándares prescriptivos y estándares evaluativos.

Los estándares prescriptivos se refieren a los estándares de comunicaciones, tales como los protocolos TCP, IP, SNMP, HTTP, entre otros. Por otra parte, los estándares evaluativos se refieren a estándares de calidad de los sistemas de Cloud Computing, los cuales se encargan de describir y evaluar los procedimientos seguidos en los procesos en general, como es el caso de la familia de estándares ISO 9000 y procedimientos específicos para seguridad de la información, como los de la familia ISO 27000.

Algunos aspectos de calidad de los proveedores de Servicios en la nube incluyen características medibles como: tiempo de actividad, rendimiento, disponibilidad, seguridad, privacidad, cumplimiento, servicio al cliente y portabilidad.

Se trata de los requisitos generales y los casos de uso de la computación en la nube; Infraestructura como Servicio (IaaS), la Red como un Servicio (NaaS) y el escritorio como servicio (DaaS); también la interconexión entre nubes, la gestión de extremo a extremo de los recursos y la infraestructura Cloud. Los retos en el entorno de los Servicios en la nube también describen las capacidades de protección que podrían mitigar estas amenazas y desafíos a la seguridad. A continuación mencionamos algunos de estos:

SAAS

En una solución SaaS, el proveedor es quien controla completamente la aplicación y su gestión. Por lo tanto, la gestión SaaS únicamente está relacionada con la administración de la propia aplicación. La infraestructura que da soporte a la aplicación es invisible al usuario, por lo que la gestión SaaS se centra en controlar los derechos de acceso a la aplicación y el modo en que los datos son almacenados y se realiza su copia de seguridad. Esas funciones son específicas de la aplicación, por lo que es improbable que la creación de estándares tenga un impacto significativo sobre las soluciones.

PAAS

En el caso de una solución PaaS (Platform as a Service), la nube brinda al usuario servidores, almacenamiento, sistemas operativos y aplicaciones de gestión como, por ejemplo, un sistema gestor de base de datos. Por lo tanto, podemos considerar que en PaaS el centro de datos es la nube y su gestión debería ser diferente a una solución SaaS. La gestión de la plataforma es altamente dependiente de los componentes que la conforman y del modo en que están organizados. Por ello, es probable que cada proveedor PaaS tenga un sistema de gestión diferente.

Una empresa que tenga dos o más proveedores PaaS, puede tener dos o más plataformas de servidores completamente diferentes, por ejemplo, una Windows y otra Linux.

IAAS

En el caso de una solución IaaS es más importante disponer de estándares. En los modelos IaaS no es necesario que el usuario cambie sus prácticas de gestión a nivel de aplicación y plataforma, pero sí necesita gestionar el modo en el que su proveedor cloud asigna los recursos, el almacenamiento y otras herramientas. Es habitual que una empresa tenga múltiples proveedores IaaS, más que en otros modelos cloud.

5.5 Plataformas tecnológicas.

AMAZON ELASTIC COMPUTE CLOUD (EC2)

Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad informática con tamaño modificable en la nube. Está diseñado para facilitar a los desarrolladores recursos informáticos escalables y basados en web. Amazon EC2 reduce el tiempo necesario para obtener y arrancar nuevas instancias de servidor en minutos, lo que permite escalar rápidamente la capacidad, ya sea aumentándola o reduciéndola, según cambien sus necesidades. Amazon EC2 cambia el modelo económico de la informática, al permitir pagar sólo por la capacidad que utiliza realmente. Amazon EC2 presenta un auténtico entorno informático virtual, que permite utilizar interfaces de servicio web para iniciar instancias con distintos sistemas operativos, cargarlas con su entorno de aplicaciones personalizadas, gestionar sus permisos de acceso a la red y ejecutar su imagen utilizando los sistemas que desee.

WINDOWS AZURE

Windows Azure es una plataforma de nube abierta y flexible que permite compilar, implementar y administrar aplicaciones rápidamente en una red global de centros de datos administrados por Microsoft. Puede compilar aplicaciones en cualquier lenguaje, herramienta o marco, permitiendo además integrar sus aplicaciones de nube públicas con el entorno de TI existente.

GOOGLE APP ENGINE

Google App Engine permite crear y alojar aplicaciones web en los mismos sistemas escalables con los que funcionan las aplicaciones de Google. Google App Engine ofrece procesos de desarrollo y de implementación rápidos, y una administración sencilla, sin necesidad de preocuparse por el hardware, las revisiones o las copias de seguridad y una ampliación sin esfuerzos. Las aplicaciones Google App Engine son fáciles de crear, fáciles de mantener y fáciles de escalar a medida que el tráfico y las necesidades de almacenamiento de datos crecen. Con App Engine no es necesario

mantener ningún servidor. Basta con cargar su aplicación y está ya se encontrará lista para servir a los usuarios.

RED HAT OPENSHIFT

OpenShift es la oferta de plataforma como servicio para Computación en la nube de Red Hat. En esta plataforma los desarrolladores de aplicaciones pueden construir, desplegar, probar y correr sus aplicaciones. Prporciona espacio en disco, recursos de CPU, memoria, conectividad de red y un servidor Apache o JBoss. Dependiendo del tipo de aplicación que se está construyendo, también proporciona acceso a una plantilla de sistema de archivos para esos tipos (por ejemplo PHP, Python y Ruby/Rails). También proporciona herramientas de desarrollo integradas para apoyar el ciclo de vida de las aplicaciones, incluyendo la integración de Eclipse, JBoss Developer Studio, Jenkins, Maven y GIT. OpenShift utiliza un ecosistema de código abierto para proporcionar servicios clave de la plataforma de aplicaciones móviles (Appcelerator), servicios NoSQL (MongoDB), servicios de SQL (PostgreSQL, MySQL), y más. JBoss proporciona una plataforma de middleware empresarial para aplicaciones Java, proporcionando apoyo para Java EE6 y servicios integrados tales como transacciones y mensajes, que son fundamentales para las aplicaciones empresariales.

5.6 Seguridad e interoperabilidad.

SEGURIDAD EN NUBE

La computación en la nube provee numerosas capacidades de almacenamiento y procesamiento de información en centros de datos de terceros; de este modo, cuando un usuario decide utilizar la nube, pierde la habilidad de tener acceso físico a sus datos; y como resultado, confía en que su proveedor de servicios prestará especial atención a la seguridad de su información. A pesar de hay muchos tipos de controles detrás de una arquitectura en la nube, usualmente se pueden encontrar en una de las siguientes categorías:

Controles disuasivos: están destinados a reducir los ataques en un sistema en la nube. Cumplen el propósito de alertar a los posibles atacantes que habrá consecuencias adversas hacia ellos si continúan con el ataque.

Controles preventivos: refuerzan el sistema contra incidentes, generalmente reduciendo o eliminando vulnerabilidades. Suministran autenticaciones fuertes de los usuarios de la nube, reduciendo la posibilidad de que usuarios no autorizados tengan acceso al sistema, y mejorando su identificación.

Controles de detección: están destinados a detector y reaccionar adecuadamente a cualquier incidente que ocurra. El monitoreo de la seguridad de red y del sistema, incluyen detección de intrusos y alistamientos de prevención, y son típicamente utilizados para detectar ataques en el sistema de la nube, y dar soporte a la infraestructura de comunicación.

Controles correctivos: reducen las consecuencias de un incidente, normalmente limitando el daño. Su efecto ocurre durante o después de un ataque. Por lo general están diseñados para reconstruir un sistema comprometido después de un ataque mediante copias de respaldo.

Generalmente se recomienda que los controles de seguridad en la nube sean seleccionados e implementados de acuerdo y en proporción a los riesgos, típicamente evaluando las amenazas, vulnerabilidades y sus impactos. Además, los proveedores de servicios y sus usuarios deben negociar términos acerca de responsabilidades, estipulando cómo deben resolverse los incidentes que involucren pérdida de datos o que comprometan los mismos.

CIFRADO DE DATOS EN LA NUBE

La seguridad de la computación en la nube se ha convertido en corto tiempo en asunto fundamental para los usuarios que emplean estas tecnologías, por la importancia que reviste la información que almacenan en Internet. La sincronización de archivos entre diferentes dispositivos y la nube constituye un proceso crítico vulnerable desde el punto de vista de la seguridad de la información, en donde el cifrado de datos parece ser una opción no despreciable para garantizar un alto nivel de protección. La mayoría de los proveedores de almacenamiento en la nube emplean algún nivel de encriptación de archivos sea del lado del servidor (para almacenar la información), o del cliente.

El cifrado del lado del servidor es el método que utilizan la mayoría de los servicios de almacenamiento de archivos en la nube. Se refiere a que la información llega al servidor sin cifrar, y allí es cifrada (normalmente con la contraseña del usuario). La transferencia de los archivos se realiza a través de una conexión segura (HTTPS/SSL). No obstante, existe la posibilidad de que, aunque la seguridad de los datos está garantizada, ante ataque externos, no así su privacidad, pues el administrador del servidor u otro atacante interno puede acceder a los datos y/o a las claves de cifrado.

El cifrado del lado del cliente, aunque menos empleando, consiste en encriptar los archivos antes de que salgan del dispositivo que se conecta a un servicio en la nube. Lo ideal, aunque no todas las aplicaciones lo cumplen, es que la contraseña nunca

salga del cliente, es decir, que los responsables del servicio en la nube solo almacenen y sincronicen datos, cuyo contenido no pueden descifrar. Su empleo trae aparejado como ventajas que la información del usuario es mucho más privada, pues solo en su dispositivo permanece descifrada, y ante cualquier alteración en el servidor o en la transferencia de archivos, solo se obtendrán datos encriptados, y nunca la información original. Como inconvenientes, tiene la particularidad de que, ante un olvido de su contraseña de seguridad, el usuario nunca tendrá acceso a la misma, además de verse afectada la interacción vía web con los archivos, por encontrarse cifrados en el servidor, y solo serán modificables desde el cliente.

La realidad es que la administración y el monitoreo de la seguridad en la nube es una tarea continua, y tanto clientes como proveedores de servicios necesitan trabajar, bajo la premisa de comprender que la protección de la información que intercambian es una tarea compartida. La seguridad en la nube se refiere a una amplia gama de políticas, tecnologías y formas de control, destinadas a proteger los datos, las aplicaciones y la infraestructura asociada a la computación en la nube. Existen varios problemas de seguridad asociados con la computación en la nube, sin embargo, es posible agruparlos en dos grandes categorías: aquellos a los que se enfrentan los proveedores (organizaciones que proveen software, plataformas o infraestructura como servicio a través de la nube) y problemas de seguridad enfrentados por los clientes (entidades y usuarios que utilizan la aplicación o almacenan información en la nube).

La responsabilidad es compartida, pues el proveedor debe asegurar que la infraestructura que ofrece sea segura y que la información de sus clientes estará a salvo, mientras que los usuarios, por su parte, deben tomar medidas para fortalecer su acceso, empleando eficientes métodos de autenticación. La arquitectura de seguridad en la nube es efectiva solo si se implementan defensas en los lugares correctos, reconociendo donde pueden aparecer determinados problemas, y estableciendo controles para resguardar cualquier debilidad y reducir el efecto de los ataques.

Conclusión

La computación en la nube ha surgido como un nuevo paradigma de computación que ofrece ventajas significativas en términos de accesibilidad, escalabilidad y recursos. Este modelo proporciona servicios y recursos informáticos a través de Internet, sin necesidad de instalaciones físicas en los dispositivos de los usuarios.

La computación en la nube se ha convertido en una tendencia tecnológica importante y se espera que tenga un impacto significativo en los procesos y el mercado de las Tecnologías de la Información. Se clasifica en tres categorías principales: Software as a Service (SaaS), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS), lo que permite a los usuarios acceder y utilizar aplicaciones, plataformas y recursos de infraestructura de manera conveniente y eficiente.

El diseño de la computación en la nube requiere considerar patrones específicos para garantizar la disponibilidad, el equilibrio de carga y evitar el estrangulamiento de recursos. Estos patrones aseguran un funcionamiento eficiente y confiable de las aplicaciones en la nube.

Es importante tener en cuenta los estándares en la nube al contratar servicios de computación en la nube, abordando aspectos como la privacidad, la confidencialidad, la ubicación y la propiedad de los datos, así como los acuerdos de nivel de servicio.

Existen diversas plataformas tecnológicas disponibles para la computación en la nube, como Amazon Elastic Compute Cloud (EC2), Windows Azure, Google App Engine y Red Hat OpenShift, que ofrecen capacidades informáticas escalables y flexibles para desarrollar, implementar y administrar aplicaciones de manera eficiente.

Bibliografía

TEMAS UNIDAD 5. (s/f-a). Neocities.org. Recuperado el 28 de mayo de 2023, de https://sanjuan17350317.neocities.org/Seguridad

TEMAS UNIDAD 5. (s/f-b). Neocities.org. Recuperado el 28 de mayo de 2023, de https://sanjuan17350317.neocities.org/Plataform

TEMAS UNIDAD 5. (s/f-c). Neocities.org. Recuperado el 28 de mayo de 2023, de https://sanjuan17350317.neocities.org/Estandar

TEMAS UNIDAD 5. (s/f-d). Neocities.org. Recuperado el 28 de mayo de 2023, de https://sanjuan17350317.neocities.org/Patrones

TEMAS UNIDAD 5. (s/f-e). Neocities.org. Recuperado el 28 de mayo de 2023, de https://sanjuan17350317.neocities.org/Concep

TEMAS UNIDAD 5. (s/f-f). Neocities.org. Recuperado el 28 de mayo de 2023, de https://sanjuan17350317.neocities.org