CAPITULO 7 – EVOLUCION DE LA RED



INTERNET DE LAS COSAS

IoT conecta los objetos inteligentes a Internet. Conecta dispositivos informáticos tradicionales y dispositivos no tradicionales.

Pilares del sistema de IoT

Usa el concepto de pilares para identificar los elementos fundamentales.

Específicamente, el sistema de loT identifica los seis pilares tecnológicos

Descripción:

• CONECTIVIDAD DE REDES.

Identifica los dispositivos que pueden usarse para proporcionar conectividad de IoT a muchas industrias y aplicaciones diferentes.

• COMPUTACIÓN DE LA NIEBLA.

Permite que las terminales, como los medidores inteligentes, los sensores industriales, las máquinas robóticas y demás, se conecten a un sistema local integrado de computación, redes y almacenamiento.

SEGURIDAD

Ofrece soluciones escalables de ciberseguridad que permiten que la organización pueda detectar, contener y corregir con rapidez y eficacia los ataques para minimizar el daño.

• ANÁLISIS DE DATOS

IoT puede conectar millones de dispositivos capaces de crear exabytes de datos cada día. Para proporcionar valor, estos datos se deben procesar y transformar rápidamente en inteligencia procesable.

ADMINISTRACIÓN Y AUTOMATIZACIÓN

Se pueden personalizar para usarse en industrias específicas a fin de obtener un nivel mejorado de seguridad, control y soporte

HABILITACIÓN DE APLICACIÓN
 Proporciona la infraestructura de alojamiento y movilidad de aplicaciones entre la nube y la computación en la niebla

NUBE

La computación en la nube implica una gran cantidad de computadoras conectadas a través de una red que puede estar ubicada físicamente cualquier lugar.

Servicios de la nube

Los servicios en la nube están disponibles en una variedad de opciones diseñadas para cumplir con los requisitos del cliente.

Descripción

Software como servicio (SaaS):

El proveedor de la nube es responsable del acceso a los servicios, como correo electrónico

Plataforma como servicio (PaaS):

El proveedor de la nube es responsable del acceso a las herramientas y los servicios de desarrollo que se usan para proporcionar las aplicaciones.

Infraestructura como servicio (laaS):

El proveedor de la nube es responsable del acceso a los equipos de la red, los servicios de red virtual izados y el soporte de infraestructura de la red.

Modelos de nube:

Nubes públicas: Los servicios pueden ser gratuitos u ofrecerse en el formato de pago según el uso, como el pago de almacenamiento en línea.

Nubes privadas: Se puede configurar una nube privada utilizando la red privada de la organización, si bien el armado y el mantenimiento pueden ser costosos.

Nubes híbridas: En una nube híbrida, las personas podrían tener grados de acceso a diversos servicios según los derechos de acceso de los usuarios.

Nubes comunitarias: Una nube comunitaria se crea para el uso exclusivo de una comunidad específica.

VIRTUALIZACION

La virtualización de servidores saca provecho de los recursos inactivos y consolida el número de servidores requeridos.

Ventajas de la virtualización:

Menos cantidad de equipos necesarios: La virtualización permite la consolidación de servidores, lo que reduce la cantidad necesaria de servidores físicos, dispositivos de red e infraestructura de soporte.

Menor consumo de energía: La consolidación de servidores reduce los costos mensuales de alimentación y refrigeración. El consumo reducido ayuda a las empresas a alcanzar una huella de carbono más pequeña.

Menos espacio necesario: La consolidación de servidores con virtualización reduce la huella total del centro de datos. Menos servidores, dispositivos de red y racks reducen la cantidad de espacio de piso requerido.

Hipervisor tipo 2:

Los hipervisores de tipo 2 son muy populares entre los consumidores y en las organizaciones que experimentan con la virtualización. Los más comunes de tipo 2 incluyen:

- Virtual PC
- VMware Workstation

Hipervisor tipo 1:

El Hipervisor está instalado directamente en el hardware. Los hipervisores de tipo 1 se usan generalmente en los servidores empresariales y los dispositivos de redes para centros de datos.

Los hipervisores de tipo 1 mejoran la escalabilidad, el rendimiento y la solidez.

PROGRAMACION DE REDES

Plano de control

Plano de control:

Suele considerarse el cerebro del dispositivo. Se utiliza para tomar decisiones de reenvío. El plano de control contiene los mecanismos de reenvío de ruta de capa 2 y capa 3, como las tablas de vecinos de protocolo de routing y las tablas de topología, las tablas de routing IPv4 e IPv6, STP, y la tabla ARP. La información que se envía al plano de control es procesada por la CPU.

Plano de datos:

Plano de datos: También conocido como plano de reenvío, este plano suele ser la estructura de switch que conecta lo varios puertos de red de un dispositivo. El plano de datos de cada dispositivo se utiliza para reenviar los flujos de tráfico. Los routers y los switches utilizan la información del plano de control para reenviar el tráfico entrante desde la interfaz de egreso correspondiente.

Virtualización de red:

Se han desarrollado dos arquitecturas de red principales para admitir la virtualización de la red:

- Redes definidas por software (SDN): una arquitectura de red definida por software que virtualiza la red.
- Infraestructura centrada en aplicaciones (ACI) de Cisco: Solución de hardware diseñada específicamente para integrar la computación en la nube con la administración de centros de datos.

CONTROLADORES

El controlador de SDN define los flujos de datos que ocurren en el flujo de datos de las SDN. Un flujo es una secuencia de paquetes que atraviesan una red que comparten un conjunto de valores de campo del encabezado.

Arquitectura ACI

Es una arquitectura de red de centro de datos desarrollada por Insieme y adquirida por Cisco en 2013.

Cisco ACI es una solución de hardware diseñada específicamente para integrar la computación en la nube con la administración de centros de datos. En un nivel alto, el elemento de políticas de la red se elimina del plano de datos. Esto simplifica el modo en que se crean redes del centro de datos.

Componentes de ACI

Perfil de aplicación de red (ANP): Un ANP es una colección de grupos de terminales (EPG) con sus conexiones y las políticas que definen dichas conexiones. Los EPG que se muestran en la figura, como VLAN, servicios web y aplicaciones, son solo ejemplos. Un ANP es con frecuencia mucho más complejo.

Controlador de infraestructura de política de aplicación (APIC): El APIC es un controlador centralizado de software que administra y opera una estructura agrupada ACI escalable. Está diseñado para la programabilidad y la administración centralizada.

Nexus: Estos switches proporcionan una estructura de switching con reconocimiento de aplicaciones y operan con un APIC para administrar la infraestructura virtual y física de la red.

TIPOS DE SDN

SDN basado en dispositivos: En este tipo de SDN, los dispositivos se programan con aplicaciones que se ejecutan en el mismo dispositivo o en un servidor de la red.

Permite que los programadores creen aplicaciones utilizando C y a Java con Python para integrar e interactuar con los dispositivos Cisco.

SDN basado en controlador: Este tipo de SDN usa un controlador centralizado que tiene conocimiento de todos los dispositivos de la red

Las aplicaciones pueden interactuar con el controlador responsable de administrar los dispositivos y de manipular los flujos de tráfico en la red

SDN basado en políticas: Este tipo de SDN es parecido al SDN basado en controlador, ya que un controlador centralizado tiene una vista de todos los dispositivos de la red

El SDN basado en políticas incluye una capa de políticas adicional que funciona a un nivel de abstracción mayor. Usa aplicaciones incorporadas que automatizan las tareas de configuración avanzadas mediante un flujo de trabajo guiado y una GUI fácil de usar. No se necesitan conocimientos de programación.

YANET ISLAS YAÑEZ ITI 91 APLICACION DE TELECOMUNICACINES