



INGENIERÍA Y PROCESOS INDUSTRIALES

#

MÓDULO III

DESARROLLO TI

INFRAESTRUCTURA, AUTOMATIZACIÓN Y DESARROLLO



ÍNDICE

INTRODUCCIÓN	4
AUTOMATIZACIÓN DE LA INFRAESTRUCTURA CON CISCO.....	5
Soluciones de automatización de Cisco.....	5
DEVOPS Y SER.....	7
DevOps.....	7
SRE (Site Reliability Engineering).....	8
SCRIPTS DE AUTOMATIZACIÓN BÁSICA.....	9
Herramientas básicas para la automatización.....	10
Automatización de la nube.....	11
HERRAMIENTAS DE AUTOMATIZACIÓN	11
Como nos ayuda la automatización	11
INFRAESTRUCTURA COMO CÓDIGO.....	15
GitOps: infraestructura moderna como código.....	15
AUTOMATIZACIÓN DE PRUEBAS	16
Prueba de redes definidas por software (SDN, Software Defined Networks)	17
SIMULACIÓN DE RED	18
Componentes VIRT y flujo de trabajo	18
INTRODUCCIÓN A LAS PLATAFORMAS DE CISCO	19
SDK DE CISCO	21
COMPRENSIÓN DE LA PROGRAMABILIDAD DE LA RED Y LOS MODELOS DE DISPOSITIVOS	22
¿Qué es un modelo de datos?	23
ADMINISTRACIÓN DE RED DE CISCO (CISCO NETWORK MANAGEMENT)	24
Cisco IOS XE	25
ADMINISTRACIÓN DE CÓMPUTOS DE CISCO.....	26
Cisco UCS Manager	26
Cisco Intersight.....	27
Cisco HyperFlex	27
Cisco ACI (Application Centric Infrastructure)	27

#





PLATAFORMAS DE COLABORACIÓN DE CISCO	28
PLATAFORMAS DE SEGURIDAD DE CISCO	30
CIERRE	32
BIBLIOGRAFÍA.....	33



INTRODUCCIÓN

La infraestructura, la automatización y el desarrollo son elementos fundamentales en el ámbito de la tecnología y la informática. En un entorno empresarial, la infraestructura se refiere a la base tecnológica necesaria para soportar los sistemas, aplicaciones y servicios de una organización.

La infraestructura puede incluir componentes físicos, como servidores, dispositivos de red, almacenamiento y centros de datos, así como componentes lógicos, como sistemas operativos, software de virtualización y herramientas de gestión de red. Una infraestructura sólida y confiable es crucial para garantizar el funcionamiento eficiente de los sistemas y mantener la continuidad del negocio.

La automatización se refiere a la implementación de procesos y tareas que se ejecutan automáticamente, sin intervención humana directa. Esto implica el uso de herramientas, scripts y software especializado para realizar tareas repetitivas, optimizar el tiempo y los recursos, minimizar errores humanos. La automatización puede abarcar diferentes áreas, como la gestión de configuraciones, la implementación de aplicaciones, monitorización de sistemas y la gestión de la infraestructura.

El desarrollo se refiere al proceso de creación, mejora y mantenimiento de aplicaciones y software. Esto implica el diseño, la programación, las pruebas y la implementación de soluciones tecnológicas que satisfacen las necesidades y objetivos de una organización. El desarrollo de software puede involucrar diferentes metodologías y enfoques, como el desarrollo ágil, la entrega continua, para garantizar una implementación eficiente y una evolución constante de las aplicaciones.

La combinación de infraestructura, automatización y desarrollo es esencial para lograr una infraestructura de TI eficiente y escalable.



AUTOMATIZACIÓN DE LA INFRAESTRUCTURA CON CISCO

La automatización de la infraestructura se refiere a la implementación de tecnologías y procesos que permiten controlar y gestionar de forma programática los recursos de infraestructura en un entorno de TI. En lugar de realizar tareas manuales y repetitivas, la automatización utiliza herramientas y scripts para realizar acciones de forma automatizada, eficiente y precisa.

La infraestructura en un entorno de TI abarca una amplia gama de componentes, como servidores, redes, almacenamiento, sistemas operativos, bases de datos, aplicaciones y servicios. La automatización de la infraestructura permite gestionar y configurar estos componentes de manera coherente, ágil y escalable.

Las herramientas en esta área incluyen Ansible, Puppet y Chef. Para la automatización con la infraestructura Cisco, las plataformas pueden integrarse con esas herramientas comunes o proporcionar acceso directo a la API a la infraestructura programable.

SOLUCIONES DE AUTOMATIZACIÓN DE CISCO

Cisco ofrece una variedad de soluciones de automatización para ayudar a las organizaciones a gestionar y operar su infraestructura de red y servicios de TI de manera más eficiente. Estas soluciones están diseñadas para simplificar las tareas de administración, configuración y monitoreo, y permiten a las empresas adaptarse rápidamente a los cambios y desafíos del entorno tecnológico.

Walk: La automatización de solo lectura, también conocida como "walk", se refiere a un proceso automatizado utilizado en el ámbito de las redes y la administración de dispositivos. En este contexto, "walk" se refiere a la capacidad de recorrer de forma sistemática y recopilar información de múltiples dispositivos de red, como routers, switches o firewalls, sin realizar ninguna modificación en la configuración o el estado de los dispositivos.

El objetivo principal de la automatización de solo lectura es obtener datos y métricas relevantes de los dispositivos de red para el monitoreo, la generación de informes y el análisis. Al automatizar el proceso de recopilación de información, se ahorra tiempo y se evita la necesidad de acceder manualmente a cada dispositivo de forma individual.

Correr (Run): La acción de "correr" o "run" en el contexto de la automatización se refiere a activar directivas o políticas predefinidas y proporcionar capacidades de autoservicio en varios dominios o entornos. Esta forma de automatización permite implementar y ejecutar de manera rápida y eficiente acciones y procesos sin la intervención manual continua.

Al correr una directiva, se ejecutan una serie de tareas y acciones automatizadas para lograr un resultado específico. Estas directivas suelen estar configuradas previamente y se pueden aplicar a diferentes áreas o dominios, como redes, seguridad, infraestructura, nubes, entre otros.

La idea central de correr directivas es permitir que los usuarios o administradores realicen cambios o desplieguen servicios de forma autónoma, sin tener que depender de una intervención manual constante. Esto proporciona un mayor nivel de autonomía y agilidad, y permite a las organizaciones responder rápidamente a las demandas cambiantes del negocio.

La automatización de directivas puede realizarse a través de herramientas y plataformas de automatización, como sistemas de orquestación, software de gestión de configuraciones, sistemas de administración de políticas, entre otros. Estas herramientas permiten definir, programar y ejecutar directivas de manera eficiente, y proporcionan interfaces de autoservicio para que los usuarios o administradores puedan activar directivas según sea necesario.

Volar (Fly): Implementar aplicaciones, configuraciones de red y mucho más a través de CI/CD. La acción de "volar" o "fly" en el contexto de la automatización se refiere a implementar aplicaciones, configuraciones de red y otros elementos a través de CI/CD (Continuous Integration/Continuous Deployment) o integración continua/despliegue continuo. Esta forma de automatización permite una entrega rápida y frecuente de software y cambios de configuración en entornos de desarrollo, prueba y producción.



Al "volar" con CI/CD, se establece un flujo de trabajo automatizado que involucra la integración continua de código, la construcción de aplicaciones, las pruebas automatizadas y el despliegue automatizado en los diferentes entornos. Este enfoque proporciona una forma ágil y eficiente de implementar cambios, mejoras y nuevas funcionalidades en los sistemas.

DEVOPS Y SER

DevOps y SRE (Site Reliability Engineering) son dos enfoques relacionados pero distintos para la gestión y operación de sistemas y aplicaciones. A continuación, se presenta una breve introducción a ambos conceptos:

DEVOPS

DevOps es una metodología o filosofía de trabajo que busca la colaboración estrecha entre los equipos de desarrollo de software y los equipos de operaciones de tecnología (IT Operations). Su objetivo principal es lograr una entrega rápida y confiable de software, así como mejorar la colaboración, la comunicación y la eficiencia en todo el ciclo de vida de desarrollo y despliegue de aplicaciones.

En un entorno DevOps, los desarrolladores y los profesionales de operaciones trabajan en conjunto, compartiendo responsabilidades y utilizando herramientas y prácticas comunes. Esto implica la adopción de técnicas como la integración continua (CI), la entrega continua (CD) y la automatización de pruebas y despliegues. Además, se fomenta la cultura de mejora continua, la retroalimentación constante y la capacidad de respuesta rápida a los cambios y requisitos del negocio.



SRE (SITE RELIABILITY ENGINEERING)

SRE, por otro lado, es un enfoque específico para garantizar la confiabilidad y disponibilidad de los sistemas y servicios en producción. El término fue acuñado por Google y se refiere a una disciplina que combina aspectos de desarrollo de software y operaciones de infraestructura.

Los profesionales de SRE aplican principios de ingeniería de software para diseñar, construir y operar sistemas escalables y confiables. Su objetivo principal es minimizar el tiempo de inactividad y maximizar la eficiencia operativa a través de la automatización, la monitorización y el diseño de arquitecturas resistentes a fallos.

A diferencia de DevOps, SRE se enfoca específicamente en la confiabilidad y el rendimiento de los sistemas en producción. Los equipos de SRE se centran en establecer objetivos de nivel de servicio (SLOs) y acuerdos de nivel de servicio (SLAs) para garantizar la calidad y la disponibilidad del servicio.

FIGURA No. 1

Tabla Comparativa

Característica	Dev(Desarrollo)	Ops(Operaciones)
Se preocupa por:	Aplicaciones personalizadas y cómo funcionan	Aplicaciones y cómo se ejecutan, además de Infraestructura (históricamente, hardware), SO, red, servicios básicos, disponibilidad, seguridad, escalamiento y mantenimiento
El negocio trata como:	Centro de beneficios: demanda recursos	Centro de costos: proporciona y contabiliza los recursos
Participa en la rotación de guardia:	Ocasionalmente (y se altera solo cuando los problemas se escalan a desarrollo)	Regularmente (punto de lanza)
Rendimiento medido:	De forma abstracta (incluidas métricas erróneas, como líneas de código/día)	Concretamente (cumplimiento de SLA, problemas resueltos)
Habilidades Necesarias:	Más profundo que amplio: lenguajes, API, arquitectura, herramientas, proceso, "frontend", "backend", etc.	Más amplio que profundo: Configuración, administración, SO, CLIs/API de administración específicos del fabricante, shell, automatización, base de datos, seguridad, etc.
Agilidad requerida:	¡Mucho! Muévase rápido, innove, rompa cosas, arregle más tarde.	¡No tanto! Las inversiones deben estar ampliamente justificadas, gestionadas las expectativas. Las escalas de tiempo largas son normales. Más seguro decir no que sí.

<https://contenthub.netacad.com/devnet/7.2.2>



SCRIPTS DE AUTOMATIZACIÓN BÁSICA

Los scripts de automatización básica son programas escritos en un lenguaje de scripting, como Python, Bash, PowerShell, entre otros, que se utilizan para automatizar tareas repetitivas y mejorar la eficiencia en la administración y gestión de sistemas y aplicaciones.

Estos scripts son secuencias de comandos o instrucciones que se ejecutan en un orden determinado para realizar una serie de acciones. Pueden interactuar con el sistema operativo, acceder a bases de datos, manipular archivos, enviar solicitudes a través de la red, entre otras funciones, dependiendo del propósito y la necesidad de automatización.

Existen varias herramientas de automatización potentes disponibles en el mercado que pueden ayudar a simplificar y agilizar los procesos de automatización.

Estas son algunas de las herramientas más populares:

Ansible: Ansible es una herramienta de automatización de infraestructura de código abierto que permite la configuración y administración de sistemas de forma sencilla. Utiliza un lenguaje declarativo y no requiere agentes en los nodos de destino. Ansible permite automatizar tareas como la configuración de servidores, el despliegue de aplicaciones y la gestión de configuraciones.

Puppet: Puppet es una herramienta de automatización de infraestructura que se enfoca en la configuración y gestión de sistemas a gran escala. Permite definir y mantener la configuración de los sistemas de manera centralizada, lo que facilita la escalabilidad y la consistencia en entornos complejos.

Chef: Chef es una plataforma de automatización que utiliza un enfoque basado en la infraestructura como código. Permite definir la configuración de los sistemas en forma de recetas y roles, y luego aplicar y gestionar esa configuración de manera centralizada. Chef es ampliamente utilizado para automatizar la configuración de servidores y el despliegue de aplicaciones.



Jenkins: Jenkins es una herramienta de automatización de integración continua y entrega continua (CI/CD). Permite la automatización de tareas como la compilación de código, las pruebas automatizadas, el despliegue y la notificación de resultados. Jenkins facilita la colaboración entre equipos de desarrollo y operaciones, y ayuda a acelerar el ciclo de entrega de software.

Terraform: Terraform es una herramienta de automatización de infraestructura que permite definir y desplegar la infraestructura como código. Con Terraform, se pueden describir y gestionar recursos de infraestructura en proveedores de nube y plataformas locales, lo que facilita la creación y gestión de entornos de manera reproducible.

SaltStack: SaltStack es una herramienta de automatización y gestión de configuraciones que utiliza un enfoque basado en eventos. Permite la automatización de tareas de configuración, la gestión de sistemas y la orquestación de infraestructura de forma escalable y eficiente.

Pero las herramientas aún no resuelven todos los problemas de implementación y configuración.

Es por eso que cada herramienta de automatización tiene una o más funciones que ejecutan comandos y scripts básicos en destinos y devuelven resultados. Por ejemplo, en Ansible, estas funciones incluyen **command**, **shell** y **raw**.

HERRAMIENTAS BÁSICAS PARA LA AUTOMATIZACIÓN

Existen varias herramientas básicas que puedes utilizar para la automatización de scripts. Estas herramientas facilitan la ejecución y programación de scripts, así como la gestión de dependencias y la programación de tareas.

A continuación, se mencionan algunas herramientas populares:

Bash (Unix Shell): Bash es una shell de Unix ampliamente utilizada que permite la automatización de tareas a través de scripts. Es una mejora del shell original de Unix, conocido como el shell Bourne, y se ha convertido en uno de los shells más ampliamente utilizados en sistemas basados en Unix. Es



especialmente útil en entornos Linux y Unix, y ofrece una amplia gama de funciones y utilidades para la automatización de tareas en línea de comandos.

Bash proporciona una interfaz de línea de comandos (CLI) que permite a los usuarios interactuar con el sistema operativo ejecutando comandos. También es un lenguaje de scripting versátil que permite la creación de scripts para automatizar tareas y realizar operaciones más complejas.

AUTOMATIZACIÓN DE LA NUBE

a automatización de la nube se refiere al uso de herramientas, scripts y procesos automatizados para administrar y gestionar las tareas y recursos en entornos de nube, como Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) u otras plataformas de nube.

HERRAMIENTAS DE AUTOMATIZACIÓN

Existen varias herramientas de automatización disponibles que se utilizan para agilizar y simplificar los procesos de desarrollo, despliegue y administración de aplicaciones y sistemas.

COMO NOS AYUDA LA AUTOMATIZACIÓN

Las herramientas de automatización tienen como objetivo principal agilizar y simplificar los procesos manuales y repetitivos en el desarrollo, despliegue y administración de sistemas y aplicaciones. Al utilizar estas herramientas, obtenemos varios beneficios:

Simplificar y estandarizar: Las herramientas de automatización "envuelven" las utilidades del sistema operativo y las funciones API para simplificar y estandarizar el acceso. Al "envolver" estas utilidades y funciones, las herramientas de automatización proporcionan una interfaz más fácil de usar y una abstracción de nivel superior para interactuar con el sistema.

Esto significa que no es necesario realizar comandos o llamadas API complicadas y de bajo nivel para realizar ciertas tareas. En su lugar, las herramientas de automatización ofrecen una capa de



abstracción que simplifica la interacción y proporciona comandos o funciones más intuitivas y fáciles de entender.

Al simplificar el acceso y la interacción con las utilidades del sistema operativo y las funciones API, las herramientas de automatización permiten que los usuarios realicen tareas de manera más eficiente y sin necesidad de conocimientos especializados en programación o administración de sistemas.

Además, estas herramientas ayudan a estandarizar los procesos y las prácticas en toda la organización. Al proporcionar una interfaz común y predefinida, se garantiza que las tareas se realicen de la misma manera en diferentes entornos y por diferentes usuarios. Esto facilita la colaboración, mejora la consistencia y reduce la posibilidad de errores. A menudo, también establecen valores predeterminados inteligentes que aceleran la redacción y las pruebas de código. Hacen que el código centrado en herramientas sea menos detallado y más fácil de entender que los scripts.

Acelere el desarrollo con funciones listas para usar: Las herramientas de automatización suelen proporcionar una funcionalidad muy potente para acelerar el desarrollo. Estas funciones predefinidas y potentes permiten a los desarrolladores aprovechar la funcionalidad existente sin tener que desarrollarla desde cero, lo que ahorra tiempo y esfuerzo.

Facilitar la reutilización, segregar las preocupaciones, promover la seguridad: Las herramientas de automatización modernas se esfuerzan por ser "basadas en datos" con el objetivo de facilitar la reutilización, segregar las preocupaciones y promover la seguridad.

- Facilitar la reutilización: Las herramientas de automatización modernas están diseñadas para permitir la reutilización de componentes y recursos. Esto significa que se pueden crear bloques de automatización que aborden tareas comunes y luego utilizarlos en diferentes contextos y proyectos. Al reutilizar estos bloques, se ahorra tiempo y esfuerzo, y se fomenta la consistencia en el enfoque de automatización.

- Segregar las preocupaciones: Las herramientas de automatización buscan separar las preocupaciones y modularizar los componentes de automatización. Esto significa que se pueden gestionar diferentes aspectos de un sistema de manera independiente, como la configuración, el despliegue, la monitorización, etc. Al tener una separación clara de las preocupaciones, se facilita la gestión y el mantenimiento de los diferentes componentes y se mejora la escalabilidad y flexibilidad del sistema.
- Promover la seguridad: Las herramientas de automatización modernas ponen un fuerte enfoque en la seguridad de los procesos y sistemas automatizados. Proporcionan funcionalidades y características para gestionar y controlar el acceso, cifrar datos sensibles, auditar las acciones realizadas y detectar posibles vulnerabilidades o amenazas. Además, facilitan la implementación de mejores prácticas de seguridad en el proceso de automatización, lo que contribuye a proteger los sistemas y datos de forma más efectiva.

Al adoptar un enfoque basado en datos, las herramientas de automatización modernas se benefician de la capacidad de recopilar y utilizar datos para optimizar y mejorar los procesos automatizados. Esto implica la recolección de métricas, la generación de informes, el análisis de datos y la toma de decisiones basadas en datos para optimizar la eficiencia, identificar problemas y mejorar continuamente los flujos de trabajo automatizados.

Realizar descubrimiento y administrar inventario: Las herramientas de automatización suelen realizar el descubrimiento y la administración del inventario de dispositivos en un entorno de TI. Estas herramientas recopilan información relevante sobre los dispositivos presentes en la red, como servidores, routers, switches, firewalls, dispositivos de almacenamiento, entre otros.

El descubrimiento de dispositivos implica identificar y registrar todos los dispositivos activos en la red, incluyendo su dirección IP, nombre, sistema operativo, puertos abiertos, servicios disponibles, entre otros detalles. Esto proporciona una visibilidad completa de la infraestructura de red y ayuda a mantener un inventario actualizado de los dispositivos existentes.

La administración del inventario implica mantener una base de datos actualizada con la información recopilada durante el descubrimiento de dispositivos. Esta base de datos puede incluir detalles



como el fabricante del dispositivo, el número de serie, la fecha de adquisición, la ubicación física, las configuraciones, las versiones de firmware o software, entre otros datos relevantes.

Gestión de escala: Una de las ventajas de las herramientas de automatización es su capacidad para gestionar la escala en los entornos de TI. Estas herramientas pueden funcionar tanto en modo local como en entornos distribuidos, lo que les permite adaptarse a las necesidades de diferentes tamaños y complejidades de infraestructura.

Involucrar a la comunidad: La mayoría de las herramientas populares están disponibles en versiones básicas de código abierto, lo que ayuda a la comunidad a acelerar el desarrollo y a encontrar y corregir errores.

- **Desarrollo colaborativo:** Las herramientas de código abierto fomentan la colaboración entre desarrolladores de todo el mundo. La comunidad puede contribuir con código, solucionar problemas, proponer mejoras y colaborar en el desarrollo continuo del software. Esta colaboración permite un rápido avance en la funcionalidad y la resolución de problemas, ya que se aprovechan los conocimientos y la experiencia colectiva de la comunidad.
- **Compartir conocimientos y recursos:** La comunidad de usuarios de estas herramientas comparte conocimientos, tutoriales, guías y recursos en línea. Esto facilita el aprendizaje y la adopción de las herramientas, ya que los nuevos usuarios pueden acceder a documentación detallada, casos de uso y ejemplos prácticos proporcionados por otros miembros de la comunidad. También se suelen organizar conferencias, encuentros y grupos de usuarios donde se comparten experiencias y conocimientos.
- **Personalización y contribución de complementos:** Las herramientas de código abierto suelen permitir la personalización y la creación de complementos por parte de la comunidad. Esto significa que los usuarios pueden adaptar las herramientas a sus necesidades específicas, desarrollar extensiones o módulos adicionales y compartirlos con otros miembros de la comunidad. De esta manera, se promueve la creación de soluciones personalizadas y se amplía la funcionalidad de las herramientas existentes.
- **Retroalimentación y soporte:** La comunidad brinda un valioso soporte y retroalimentación a los usuarios. Los miembros de la comunidad pueden responder preguntas, ofrecer soluciones a



problemas comunes, proporcionar asesoramiento técnico y compartir mejores prácticas. Esta retroalimentación y soporte comunitario crea un ambiente de colaboración y ayuda mutua, donde los usuarios pueden obtener ayuda y orientación en el uso de las herramientas.

Los usuarios de estas herramientas también comparten manuales de implementación, manifiestos, recetas y mucho más. Estos están diseñados para su uso con la herramienta, se pueden distribuir a través de GitHub y otros repositorios públicos, y en repositorios mantenidos por proveedores de herramientas como Ansible Galaxy.

INFRAESTRUCTURA COMO CÓDIGO

En el contexto de DevOps, el concepto de inmutabilidad se refiere a mantener los sistemas y la infraestructura completamente como código, sin realizar modificaciones o configuraciones manuales directamente en los recursos. En lugar de realizar cambios manuales, se actualiza y despliega nueva infraestructura mediante la creación de una nueva versión del código que describe dicha infraestructura.

La inmutabilidad se basa en el principio de tratar los recursos de infraestructura como elementos desechables y fácilmente reemplazables. En lugar de modificar directamente una instancia o servidor existente, se crea una nueva instancia con la configuración y las actualizaciones deseadas y se despliega en lugar de la anterior.

GITOPS: INFRAESTRUCTURA MODERNA COMO CÓDIGO.

GitOps es un enfoque moderno para la gestión de la infraestructura y las operaciones en el que se utiliza Git como fuente única de verdad para la configuración y el estado de la infraestructura. En GitOps, toda la infraestructura se describe y gestiona como código, y los cambios en la infraestructura se realizan a través de actualizaciones del repositorio Git.

En el contexto de GitOps, la infraestructura como código se combina con los principios y las prácticas de Git para permitir un control y una gestión eficientes de la infraestructura.

Los beneficios de GitOps incluyen una mayor automatización, control de versiones, consistencia, escalabilidad y colaboración en el proceso de gestión de la infraestructura. Al utilizar Git como fuente única de verdad, se facilita la colaboración entre equipos, se mejora la trazabilidad y se promueve una forma más segura y eficiente de gestionar y desplegar la infraestructura.

FIGURA No. 2

Operaciones por solicitud de extracción



<https://contenthub.netacad.com/devnet/7.5.1>

AUTOMATIZACIÓN DE PRUEBAS

La automatización de pruebas es el proceso de utilizar herramientas y tecnologías para realizar pruebas de forma automatizada en lugar de realizarlas manualmente. Consiste en desarrollar scripts o programas que ejecutan una serie de acciones y verificaciones en una aplicación o sistema para determinar si funciona correctamente y cumple con los requisitos establecidos.

Prueba de desafíos de infraestructura: Las herramientas de automatización como Ansible, Puppet, Chef y otras solucionan parte del problema convirtiendo la infraestructura en código, los desafíos relacionados con la infraestructura a través de la automatización de la configuración y la gestión de los sistemas. Estas herramientas permiten definir y administrar la infraestructura como código, lo que facilita la implementación, la configuración y la supervisión de los recursos de infraestructura de manera consistente y escalable.



las herramientas de automatización como Ansible, Puppet, Chef y otras abordan los desafíos de la infraestructura al permitir la configuración y gestión automatizada de los sistemas. Proporcionan configuraciones consistentes, aprovisionamiento rápido, escalabilidad, gestión centralizada, mantenimiento eficiente y funciones de auditoría para la infraestructura, lo que ayuda a mejorar la eficiencia, la consistencia y la seguridad en el entorno de infraestructura.

PRUEBA DE REDES DEFINIDAS POR SOFTWARE (SDN, SOFTWARE DEFINED NETWORKS)

Las pruebas de redes definidas por software (SDN) se centran en verificar y validar el correcto funcionamiento de las redes que utilizan esta tecnología. SDN es un enfoque de redes que separa el plano de control del plano de datos, lo que permite una mayor flexibilidad, programabilidad y automatización en la gestión de redes.

Algunos aspectos clave de las pruebas de SDN incluyen:

Compatibilidad con controladores SDN: Los controladores SDN son componentes clave en una arquitectura SDN. Las pruebas deben garantizar la compatibilidad entre los controladores SDN utilizados y los dispositivos de red gestionados por ellos. Se deben verificar aspectos como la configuración correcta, el enrutamiento, la seguridad y la interoperabilidad entre el controlador y los dispositivos de red.

Validación de políticas de red: En SDN, las políticas de red se definen y se implementan de manera centralizada a través del controlador. Las pruebas deben asegurarse de que las políticas de red se implementen correctamente y que se apliquen las reglas de enrutamiento, seguridad y calidad de servicio (QoS) definidas.

Orquestación y automatización: SDN permite una mayor automatización y orquestación en la gestión de redes. Las pruebas deben verificar la capacidad de automatización de la red, incluida la capacidad de implementar cambios en la configuración de manera rápida y eficiente, así como la capacidad de orquestar la conectividad entre diferentes dispositivos y servicios de red.

Resiliencia y escalabilidad: Las pruebas deben evaluar la capacidad de la red SDN para manejar una carga de tráfico creciente y para recuperarse de fallos de manera eficiente. Esto incluye verificar la capacidad de conmutación y enrutamiento dinámico, la capacidad de redundancia y la capacidad de recuperación ante fallos de dispositivos o enlaces.

Seguridad: Las pruebas de SDN deben incluir la validación de los mecanismos de seguridad implementados en la red. Esto incluye la autenticación de dispositivos y usuarios, el cifrado de datos, la segmentación de red y la detección y prevención de intrusiones.

SIMULACIÓN DE RED

La simulación de red es una técnica utilizada para emular y probar el funcionamiento de una red en un entorno virtual. Permite a los profesionales de redes crear escenarios realistas y reproducibles sin afectar la red de producción. Una de las herramientas populares utilizadas para la simulación de redes es Cisco Virtual Internet Routing Lab (VIRL).

VIRL es una plataforma de simulación y emulación de redes desarrollada por Cisco. Proporciona una solución virtualizada para diseñar, probar y validar redes complejas.

COMPONENTES VIRL Y FLUJO DE TRABAJO

Cisco Virtual Internet Routing Lab (VIRL) consta de varios componentes clave que permiten la simulación y emulación de redes. Estos componentes se combinan en un flujo de trabajo para diseñar, configurar, simular y probar redes virtuales. VIRL proporciona una CLI local para la administración de sistemas, una interfaz REST para la integración con la automatización y una interfaz de usuario potente que ofrece un entorno gráfico completo para crear y configurar topologías de simulación.

VIRL utiliza imágenes de dispositivos de red, una topología virtual y herramientas de configuración y gestión para permitir la simulación y prueba de redes virtuales. El flujo de trabajo típico implica



diseñar la topología, configurar los dispositivos, realizar simulaciones y pruebas, optimizar la configuración y documentar los resultados. Esto facilita el diseño y la validación de configuraciones de red antes de implementarlas en un entorno de producción.

INTRODUCCIÓN A LAS PLATAFORMAS DE CISCO

Cisco tiene una larga historia como empresa de equipos de red y proveedor de hardware. Esas ofertas están ahora disponibles como oportunidades de automatización.

Cisco es una empresa líder en el campo de las tecnologías de la información y las comunicaciones. Ofrece una amplia gama de soluciones y plataformas para ayudar a las organizaciones a construir, gestionar y asegurar sus redes y sistemas.

Las plataformas de Cisco abarcan diferentes áreas, desde redes empresariales hasta seguridad, colaboración, centro de datos, servicios en la nube e Internet de las cosas (IoT).

Explorar las categorías de la tecnología de Cisco

Cisco ofrece una amplia gama de tecnologías en diversas categorías para abordar las necesidades de conectividad, seguridad, colaboración y gestión en entornos empresariales.

Para ayudar a clasificar todas las ofertas de desarrolladores de Cisco, DevNet crea centros de desarrollo para cada grupo tecnológico, y esos centros de desarrollo son una forma conveniente de agrupar tecnologías.

Networking: Cisco es ampliamente reconocido por sus soluciones de networking, que incluyen enrutadores (routers), conmutadores (switches) y puntos de acceso inalámbricos. Estas tecnologías permiten la conectividad de redes locales (LAN), redes de área amplia (WAN) y redes inalámbricas, brindando un rendimiento confiable y seguro.

Seguridad: Cisco ofrece una amplia gama de soluciones de seguridad para proteger las redes y los sistemas empresariales contra amenazas y ataques cibernéticos. Esto incluye firewalls, sistemas de



prevención de intrusiones (IPS), soluciones de seguridad de endpoints, VPNs y herramientas de gestión de seguridad.

Colaboración: Cisco proporciona tecnologías de colaboración para facilitar la comunicación y la colaboración entre los empleados. Esto incluye plataformas de comunicación unificada, como Cisco Unified Communications Manager, herramientas de videoconferencia, aplicaciones de mensajería y colaboración en equipo.

Data Center: Cisco ofrece soluciones para la construcción y gestión de centros de datos eficientes y escalables. Esto incluye tecnologías de virtualización, servidores, almacenamiento, redes definidas por software (SDN) y gestión de la nube.

Cloud Services: Cisco ofrece servicios en la nube que permiten a las organizaciones aprovechar la flexibilidad y la escalabilidad de la nube. Esto incluye servicios de colaboración en la nube, como Cisco Webex, soluciones de seguridad en la nube, como Cisco Umbrella, y servicios de gestión de redes en la nube, como Cisco Meraki.

Internet of Things (IoT): Cisco proporciona tecnologías para habilitar y gestionar la conectividad de dispositivos en el Internet de las cosas. Esto incluye soluciones para la conectividad de dispositivos, la recopilación y análisis de datos, la seguridad de IoT y la gestión de dispositivos.

Analytics: Cisco ofrece soluciones de análisis de datos para obtener información valiosa de las redes, los sistemas y las aplicaciones. Esto incluye herramientas de monitoreo y análisis de red, análisis de datos en tiempo real, análisis de seguridad y análisis predictivo.

Estas categorías representan solo una parte de la amplia cartera de tecnologías de Cisco. La empresa continúa innovando y desarrollando nuevas soluciones para abordar los desafíos emergentes en el ámbito de la tecnología empresarial. Las tecnologías de Cisco están diseñadas para brindar rendimiento, confiabilidad y seguridad, ayudando a las organizaciones a impulsar la transformación digital y lograr sus objetivos comerciales.



SDK DE CISCO

SDK es la sigla en inglés de "Software Development Kit", que se traduce al español como "Kit de Desarrollo de Software". Un SDK es un conjunto de herramientas, bibliotecas, documentación y ejemplos de código que permiten a los desarrolladores crear aplicaciones y software para una plataforma o sistema específico.

Un SDK proporciona a los desarrolladores las herramientas necesarias para aprovechar las funcionalidades y características de una plataforma determinada. Por lo general, un SDK incluye un conjunto de APIs (Interfaces de Programación de Aplicaciones) que permiten a los desarrolladores interactuar con el sistema subyacente y utilizar sus servicios.

El objetivo principal de un SDK es facilitar el desarrollo de aplicaciones al proporcionar a los desarrolladores un conjunto de recursos y herramientas predefinidas. Esto incluye bibliotecas de funciones, controladores de dispositivo, emuladores, depuradores, compiladores y otros componentes necesarios para desarrollar software de manera eficiente y compatible con la plataforma objetivo.

Los SDK son ampliamente utilizados en el desarrollo de software para diversas plataformas, como sistemas operativos, frameworks de desarrollo web y móvil, plataformas de juegos, API de servicios en la nube, entre otros. Al utilizar un SDK, los desarrolladores pueden acelerar el proceso de desarrollo al tener acceso a herramientas y componentes listos para usar, evitando tener que crear todo desde cero.



COMPRENSIÓN DE LA PROGRAMABILIDAD DE LA RED Y LOS MODELOS DE DISPOSITIVOS

La programabilidad de la red se refiere a la capacidad de las redes de comunicación para ser controladas y gestionadas mediante software y programación. En lugar de depender exclusivamente de configuraciones manuales y estáticas, la programabilidad permite a los administradores de red controlar y adaptar la red a través de código y automatización.

Un aspecto fundamental de la programabilidad de la red es el uso de modelos de dispositivos. Un modelo de dispositivo es una representación abstracta y estructurada de un dispositivo de red, que describe sus características, funcionalidades y comportamiento. Los modelos de dispositivos se basan en estándares como el lenguaje YANG (Yet Another Next Generation), que proporciona una forma de describir la estructura de datos y las operaciones soportadas por los dispositivos de red.

Los modelos de dispositivos permiten la interoperabilidad y la comunicación entre diferentes componentes de la red, como controladores, orquestadores y dispositivos de red físicos o virtuales. Estos modelos proporcionan una forma común de describir y programar la configuración y el comportamiento de los dispositivos de red, lo que facilita la automatización y la gestión centralizada de la red.

La programabilidad de la red y los modelos de dispositivos permiten a los administradores de red realizar tareas como la configuración automatizada de dispositivos, la gestión de políticas de red, la monitorización y el análisis de la red, entre otros. Al programar la red, los administradores pueden adaptar rápidamente la infraestructura de red a las necesidades cambiantes del negocio, mejorar la eficiencia operativa y reducir los errores humanos.

¿QUÉ ES UN MODELO DE DATOS?

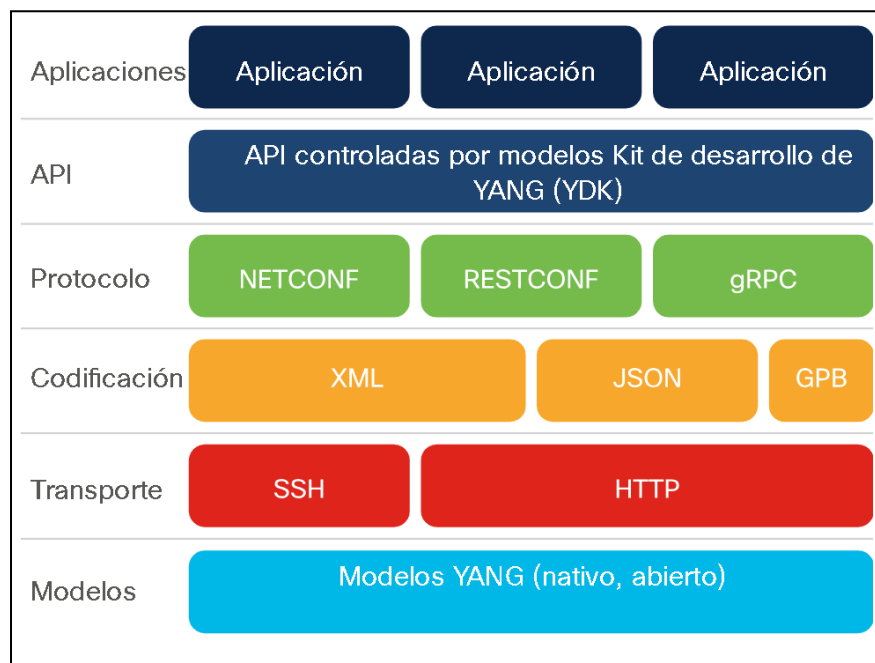
Un modelo de datos es una representación estructurada y organizada de la información que se utiliza para describir cómo se almacenan, se manipulan y se acceden a los datos en un sistema. Es un concepto fundamental en la gestión de bases de datos y en el diseño de sistemas de información.

Un modelo de datos define la estructura, las relaciones y las restricciones de los datos dentro de un sistema. Proporciona un marco conceptual y una notación específica para representar y comprender los datos y sus interrelaciones. Además, un modelo de datos establece reglas y convenciones para el almacenamiento y la manipulación de los datos.

Existen diferentes tipos de modelos de datos, cada uno con su propia notación y enfoque de representación

FIGURA No. 3

Pila de Programabilidad Basada en Modelos



<https://contenthub.netacad.com/devnet/8.3.1>



ADMINISTRACIÓN DE RED DE CISCO (CISCO NETWORK MANAGEMENT)

Cisco tiene una larga historia de inventar y apoyar soluciones de red, tanto en hardware como en software. Desde el comienzo de las redes informáticas, la configuración de red se centró en un conjunto de tareas de dispositivo por dispositivo, manual y, a menudo, complejo. Este enfoque no planteaba un gran problema con algunos dispositivos de red, pero la configuración y el mantenimiento de cientos o incluso miles de dispositivos en una red se hace casi imposible.

Además, a medida que aumenta la escala, los cambios implementados por los humanos tienen una mayor probabilidad de mal configuraciones. Los errores podrían ser errores tipográficos simples, aplicar un nuevo cambio en el dispositivo incorrecto o incluso perder un dispositivo por completo. La ejecución de tareas repetitivas que exigen un alto grado de coherencia, desafortunadamente, siempre introduce un riesgo de error. Y la cantidad de cambios que hacen los seres humanos aumenta cada vez más, ya que hay más exigencias del negocio para implementar más aplicaciones a una velocidad más rápida que nunca.

La administración de redes de Cisco se refiere al conjunto de actividades y procesos necesarios para gestionar y mantener eficientemente las redes que utilizan equipos y tecnologías de Cisco. Cisco Systems es una reconocida empresa de telecomunicaciones que ofrece una amplia gama de productos y soluciones para redes, desde dispositivos de red como routers y switches hasta tecnologías avanzadas como redes definidas por software (SDN) y virtualización.

La administración de redes de Cisco implica la configuración, el monitoreo, la seguridad y la optimización de las redes que utilizan equipos y tecnologías de Cisco. La administración eficaz de estas redes es fundamental para garantizar un rendimiento óptimo, una alta disponibilidad y una seguridad robusta de las comunicaciones y los servicios en la infraestructura de red.



CISCO IOS XE

IOS significa "Sistema Operativo de Internetwork". IOS era el sistema operativo original para los routers de Cisco Systems y los switches de red Cisco. IOS XE es la plataforma programable de próxima generación. Con IOS XE, tiene acceso a interfaces programables, consistentes y basadas en estándares, modelos de datos estándar para configuración, implementación y reversión, así como a la integración de servicios con la red

Cisco IOS XE (Extreme Edge) es una versión del sistema operativo Cisco IOS que se utiliza en routers y switch de la serie Cisco Catalyst 9000. Es una evolución del tradicional Cisco IOS, diseñado para brindar mayor flexibilidad, escalabilidad y capacidad de administración en entornos de red empresariales.

Algunas de las características y ventajas clave de Cisco IOS XE incluyen:

1. Modularidad: Cisco IOS XE está basado en una arquitectura modular que permite la ejecución de múltiples procesos independientes. Esto proporciona una mayor estabilidad y resiliencia, ya que un problema en un proceso no afectará a otros, y permite la actualización o agregado de funcionalidades de manera más fácil y rápida.
2. Separación de plano de control y plano de datos: Cisco IOS XE separa el plano de control (donde se ejecutan los protocolos de enrutamiento y configuración) del plano de datos (donde se reenvía el tráfico). Esta separación permite una mayor flexibilidad en la configuración y administración de la red, así como una mayor capacidad de escalamiento y resiliencia.
3. Virtualización de funciones de red: Cisco IOS XE permite la virtualización de funciones de red (Network Function Virtualization, NFV), lo que significa que se pueden ejecutar aplicaciones y servicios de red en forma de máquinas virtuales en los dispositivos. Esto simplifica la implementación y gestión de servicios de red, como firewalls, routers virtuales y controladores de redes definidas por software (SDN).
4. Programabilidad y automatización: Cisco IOS XE ofrece capacidades de programabilidad y automatización a través de interfaces de programación de aplicaciones (API) y herramientas



de desarrollo. Esto permite la personalización y automatización de la configuración y gestión de la red, facilitando la integración con herramientas de automatización y orquestación.

5. Seguridad avanzada: Cisco IOS XE incorpora características de seguridad avanzadas para proteger la red y los datos. Esto incluye capacidades de encriptación, autenticación de usuarios, protección contra amenazas cibernéticas y políticas de seguridad granulares.
6. Gestión simplificada: Cisco IOS XE se integra con herramientas de gestión de red, como Cisco DNA Center y Cisco Prime Infrastructure, que ofrecen una gestión centralizada y simplificada de la red. Estas herramientas permiten la configuración, monitoreo y solución de problemas de manera eficiente.

ADMINISTRACIÓN DE CÓMPUTOS DE CISCO

La administración de cómputos de Cisco se refiere a las soluciones y herramientas proporcionadas por Cisco para gestionar y administrar eficientemente los recursos de cómputo en entornos empresariales. Estas soluciones se centran en la administración de servidores, sistemas operativos, aplicaciones y cargas de trabajo, con el objetivo de optimizar el rendimiento, la disponibilidad y la seguridad de los recursos de cómputo.

Cisco ofrece varias soluciones de administración de cómputo, que incluyen:

CISCO UCS MANAGER

Es una herramienta de gestión centralizada para la infraestructura de computación unificada (Unified Computing System, UCS) de Cisco. Permite la administración y configuración de servidores, redes y almacenamiento en un entorno unificado, simplificando las operaciones y mejorando la eficiencia.

La Computación Unificada de Cisco se basa en el sistema Cisco Unified Computing System (UCS), el cual consiste en servidores blade, infraestructura de red y almacenamiento conectados a través de una arquitectura unificada. UCS se diferencia de las soluciones tradicionales de servidores en su enfoque integrado y centralizado, que permite una mayor flexibilidad, escalabilidad y rendimiento.



CISCO INTERSIGHT

Es una plataforma de administración basada en la nube que brinda una gestión simplificada y automatizada de la infraestructura de cómputo de Cisco. Proporciona capacidades de monitoreo, análisis, configuración y actualización de manera centralizada, lo que facilita la administración de grandes entornos y la implementación de políticas consistentes.

Cisco Intersight se basa en un modelo de administración basado en políticas, lo que significa que las operaciones y configuraciones se definen a través de políticas predefinidas y se aplican de manera consistente a través de la infraestructura. Esto simplifica la administración y permite una configuración rápida y uniforme de los recursos de TI.

CISCO HYPERFLEX

Cisco HyperFlex es una solución de infraestructura híper convergente (HCI) desarrollada por Cisco. Combina computación, almacenamiento y redes en una plataforma integrada y escalable, que está diseñada para simplificar la implementación y administración de infraestructuras de TI.

HyperFlex se basa en una arquitectura de software definida que utiliza servidores x86, almacenamiento definido por software y una red definida por software para proporcionar una infraestructura convergente. Esto significa que todos los componentes necesarios para el funcionamiento de una infraestructura de TI, como servidores, almacenamiento y redes, se combinan en un único sistema integrado.

Cisco ACI (Application Centric Infrastructure)

Cisco ACI (Application Centric Infrastructure) es una arquitectura de red definida por software (SDN) que se utiliza para proporcionar una infraestructura de red altamente automatizada y centrada en las aplicaciones. ACI se basa en un enfoque de políticas, lo que significa que las políticas de red se definen de manera centralizada y se aplican de forma consistente en toda la infraestructura, lo que



simplifica la administración y mejora la flexibilidad y la escalabilidad y la seguridad, y proporcionar una mayor visibilidad y control sobre los recursos de cómputo.

Algunos beneficios de Cisco ACI incluyen la simplificación de la administración de redes, la automatización de tareas, la mejora de la visibilidad y el control de la red, la reducción de los costos operativos y la capacidad de respuesta rápida a las necesidades de las aplicaciones.

PLATAFORMAS DE COLABORACIÓN DE CISCO

Cisco ofrece varias plataformas de colaboración que permiten a las organizaciones mejorar la comunicación y la colaboración entre sus equipos. Algunas de las plataformas de colaboración más populares de Cisco son las siguientes:

1. Cisco Webex: Webex es una plataforma de colaboración en línea que ofrece una amplia gama de herramientas, como reuniones virtuales, llamadas de voz y video, mensajería instantánea, compartición de pantalla y colaboración en tiempo real en documentos. Webex permite a los equipos trabajar juntos de manera efectiva, independientemente de su ubicación geográfica.

Algunas características y beneficios de Cisco Webex son:

- Reuniones virtuales: Permite realizar reuniones en línea con video y audio de alta calidad, compartición de pantalla, anotaciones y grabación de reuniones. Los participantes pueden unirse a través de enlaces de invitación o mediante la marcación de números de teléfono.
- Conferencias web: Permite realizar presentaciones en línea con capacidades de compartición de diapositivas, encuestas interactivas, chat en vivo y sesiones de preguntas y respuestas. Es una herramienta útil para realizar seminarios web, eventos en línea y capacitaciones virtuales.
- Mensajería instantánea y colaboración: Ofrece una plataforma de mensajería instantánea para una comunicación rápida y efectiva entre equipos de trabajo. Los usuarios pueden



enviar mensajes individuales o en grupos, compartir archivos y colaborar en tiempo real en proyectos.

- **Compartición de pantalla y colaboración en tiempo real:** Permite compartir la pantalla de forma segura durante las reuniones, lo que facilita la colaboración en documentos, presentaciones y aplicaciones. También ofrece herramientas interactivas, como pizarras virtuales y anotaciones, para una colaboración efectiva.
 - **Integración con otras herramientas y aplicaciones:** Webex se integra con una variedad de herramientas de productividad y aplicaciones de terceros, como Microsoft Office, Google Workspace y Salesforce. Esto facilita la colaboración y la realización de tareas dentro de un entorno de trabajo familiar.
 - **Seguridad y cumplimiento normativo:** Webex ofrece medidas de seguridad avanzadas, como cifrado de extremo a extremo, autenticación de usuarios, controles de acceso y cumplimiento normativo para proteger la confidencialidad de las reuniones y los datos compartidos.
2. **Cisco Jabber:** Cisco Jabber es una aplicación de comunicación empresarial que ofrece servicios de mensajería instantánea, llamadas de voz y video, y colaboración en tiempo real. Permite a los usuarios conectarse y comunicarse de manera efectiva y segura, tanto dentro como fuera de la organización, a través de diferentes dispositivos, como computadoras, teléfonos móviles y tablet.
 3. **Cisco Spark:** Cisco Spark, que ahora se conoce como Cisco Webex Teams, es una plataforma de colaboración en equipo basada en la nube. Proporciona un conjunto completo de herramientas de comunicación y colaboración que permiten a los equipos trabajar juntos de manera eficiente, sin importar su ubicación geográfica.

Cisco Spark (Cisco Webex Teams) es una plataforma de colaboración en equipo basada en la nube que proporciona herramientas de mensajería instantánea, llamadas de voz y video, compartición de archivos y colaboración en tiempo real. Permite a los equipos trabajar juntos de manera efectiva y productiva, mejorando la comunicación y la colaboración en el entorno empresarial.



4. Cisco TelePresence: es una solución de videoconferencia de alta gama que ofrece una experiencia de reunión virtual similar a estar presente físicamente en la sala. Esta tecnología utiliza equipos de videoconferencia de alta definición, pantallas grandes, audio de alta calidad y una interfaz fácil de usar para proporcionar una comunicación en tiempo real.

Con Cisco TelePresence, los usuarios pueden realizar videoconferencias de alta calidad con participantes ubicados en diferentes lugares geográficos. Los equipos de TelePresence están diseñados para brindar una experiencia visual realista, con imágenes nítidas y colores vivos, lo que facilita la comunicación efectiva y la colaboración en equipo.

La solución de TelePresence de Cisco incluye una variedad de equipos y configuraciones para adaptarse a diferentes entornos, desde pequeñas salas de reuniones hasta grandes salas de conferencias. Estos equipos pueden integrarse con otros sistemas de videoconferencia y plataformas de colaboración, lo que permite una interoperabilidad fluida con socios comerciales y clientes que utilizan diferentes soluciones de comunicación.

Estas plataformas de colaboración de Cisco ofrecen una variedad de herramientas y funcionalidades para mejorar la comunicación, la colaboración y la productividad de los equipos. Permiten a los usuarios conectarse y trabajar juntos de manera efectiva, sin importar la distancia física, lo que es especialmente útil en entornos empresariales distribuidos o con equipos remotos. Además, Cisco ofrece integraciones con otras herramientas y servicios populares, lo que permite una experiencia de colaboración más fluida y personalizable.

PLATAFORMAS DE SEGURIDAD DE CISCO

Cisco ofrece una amplia gama de plataformas de seguridad que ayudan a proteger las redes, los datos y las aplicaciones de las organizaciones. Algunas de las principales plataformas de seguridad de Cisco son:

1. Cisco Firepower Next-Generation Firewall (NGFW): Proporciona una seguridad integral para redes empresariales, ofreciendo funciones de firewall, prevención de intrusiones, control de aplicaciones y visibilidad avanzada del tráfico de red.
2. Cisco Advanced Malware Protection (AMP): Ofrece una protección avanzada contra malware y amenazas persistentes avanzadas (APT). Utiliza análisis de comportamiento y técnicas de aprendizaje automático para detectar y bloquear el malware en tiempo real.



3. Cisco Identity Services Engine (ISE): Es una plataforma de seguridad de acceso a la red que permite aplicar políticas de acceso basadas en identidades de usuarios y dispositivos. Proporciona autenticación, autorización y control de acceso a la red de manera centralizada.
4. Cisco Email Security: Proporciona protección contra amenazas de correo electrónico, como phishing, spam y malware. Utiliza técnicas avanzadas de detección para identificar y bloquear correos electrónicos maliciosos.
5. Cisco Umbrella: Es una solución de seguridad en la nube que protege a los usuarios contra amenazas en Internet, bloqueando el acceso a sitios web maliciosos y evitando la comunicación con servidores de comando y control.
6. Cisco SecureX: Es una plataforma de seguridad integrada que permite a las organizaciones gestionar y analizar de forma centralizada la seguridad en varios productos y servicios de Cisco. Proporciona visibilidad y control de amenazas, así como la capacidad de respuesta rápida a incidentes de seguridad.

Estas son solo algunas de las plataformas de seguridad ofrecidas por Cisco. La compañía también ofrece soluciones adicionales como seguridad en la nube, protección de endpoints, seguridad de aplicaciones, seguridad en la nube híbrida y más. Estas plataformas ayudan a las organizaciones a proteger sus activos digitales y garantizar la seguridad de sus redes y datos en un entorno cada vez más amenazante.



CIERRE

En conclusión, la infraestructura, la automatización y el desarrollo son aspectos fundamentales en el ámbito de las tecnologías de la información y las comunicaciones. La gestión eficiente de la infraestructura de redes, sistemas y aplicaciones es crucial para garantizar el funcionamiento fluido de las organizaciones.

La automatización juega un papel clave en la simplificación y estandarización de tareas, acelerando el desarrollo de software y facilitando la gestión de la infraestructura. Las herramientas de automatización permiten la implementación ágil, la configuración eficiente y la supervisión continua de los sistemas, lo que conduce a una mayor eficiencia operativa y ahorro de tiempo.

Por otro lado, el desarrollo de software se ha convertido en una parte fundamental de la transformación digital. La adopción de prácticas ágiles y DevOps ha permitido una entrega más rápida y confiable de software, promoviendo la colaboración entre equipos de desarrollo y operaciones.

En conjunto, la infraestructura, la automatización y el desarrollo se complementan para mejorar la eficiencia, la seguridad y la escalabilidad de los sistemas de TI. La implementación de tecnologías de Cisco, como la automatización de redes, la programabilidad y las plataformas de colaboración y seguridad, puede ayudar a las organizaciones a alcanzar estos objetivos y adaptarse a un entorno empresarial cada vez más dinámico y exigente.

BIBLIOGRAFÍA

- Bruno, A. A., & Jordan, S. (2017). CCDA 200-310 official cert guide. Indianápolis, IN: Cisco Press.nes sobre comunicación visual, Ediciones Infinito.
<https://elibro.net/es/lc/ipchile/titulos/78883>
- Indianápolis, IN: Cisco Press.nes sobre comunicación visual, Ediciones infinito.
<https://www.buscalibre.cl/libro-cisco-certified-devnet-associate-devasc-200-901-official-cert-guide-libro-en-ingles/9780136642961/p/53518764>
- Jackson, C; Gooley, J; Iliesiu, A; Malegaonkar, A (2020). DEVASC 200-901 official cert guide.



INGENIERÍA Y PROCESOS INDUSTRIALES

#

FIN DE MÓDULO

