TIC

TALENTO TECH

Misión 1

Arquitectura en la nube

Innovador

Tema 4: Buenas prácticas en arquitecturas nube

UTraining Entrenamiento en Innovación y Tecnología | UNIVERSIDAD DE ANTIOQUIA | Universidad de Caldas | ubicua Technology

Campista, llegó el momento de retar tus conocimientos y que los pongas aprueba a través de los diferentes recursos que encontraras en este espacio como son: conceptos, ejemplos, herramientas, actividades prácticas y retos, los cuales te ayudaran alcanzar los objetivos trazados en el nivel innovador.

Buenas prácticas en arquitecturas nube

Desarrollar una comprensión integral de las buenas prácticas en arquitecturas en la nube mediante el análisis y la aplicación de principios de diseño, seguridad, y optimización, con el fin de mejorar la eficiencia, escalabilidad y resiliencia de soluciones tecnológicas en entornos de computación en la nube.

Introducción a la seguridad en AWS

En esta lección, los estudiantes aprenderán sobre los fundamentos de la seguridad en AWS, incluyendo patrones de diseño, arquitecturas distribuidas y servicios específicos para la seguridad en la nube. La lección está diseñada para proporcionar una comprensión sólida de cómo proteger las aplicaciones y datos en AWS, así como las mejores prácticas para implementar medidas de seguridad eficaces.

INTRODUCCIÓN

En esta lección, aprenderás sobre los fundamentos de la seguridad en AWS, incluyendo patrones de diseño, arquitecturas distribuidas y servicios específicos para la seguridad en la nube.

CONCEPTOS BÁSICOS DE SEGURIDAD

- Seguridad en la nube vs. seguridad tradicional
- Principios de seguridad en AWS
- Responsabilidad compartida

PATRONES DE DISEÑO DE SEGURIDAD

- Seguridad en capas
- Principio de privilegio mínimo
- Defensa en profundidad

CASO DE ESTUDIO 1

- Descripción del problema
- Solución implementada
- Resultados obtenidos

CASO DE ESTUDIO 2

- Descripción del problema
- Solución implementada
- Resultados obtenidos

SERVICIOS DE SEGURIDAD EN AWS

- AWS IAM
- AWS KMS
- AWS CloudTrail
- AWS Shield

AWS IAM

- Gestión de identidades y accesos
- Roles y políticas
- Buenas prácticas

AWS KMS

- Gestión de claves

- Cifrado de datos
- Integración con otros servicios

AWS CLOUDTRAIL

- Auditoría y monitoreo
- Configuración básica
- Ejemplos prácticos

AWS SHIELD

- Protección contra DDoS
- Tipos de protección
- Configuración y uso

EVALUACIÓN Y REFLEXIÓN

- Evaluación formativa
- Discusión final
- Reflexión sobre la importancia de la seguridad en AWS

RESUMEN

- Conceptos básicos de seguridad en AWS
- Patrones de diseño de seguridad
- Servicios de seguridad en AWS
- Taller práctico y evaluación

Campista en esta lección, aprenderás sobre la seguridad en contenedores, un aspecto crucial para el despliegue de aplicaciones en la nube. Abordaremos los riesgos de seguridad asociados con los contenedores y las herramientas y técnicas para identificar y mitigar estos riesgos. La lección combinará teoría y práctica para asegurar una comprensión profunda del tema.

INTRODUCCIÓN A LA SEGURIDAD EN CONTENEDORES

La seguridad en contenedores es crucial para el despliegue de aplicaciones en la nube. Abordaremos los riesgos de seguridad y las herramientas para mitigarlos.

OBJETIVOS DE LA LECCIÓN

1. Identificar riesgos de seguridad en contenedores.
2. Utilizar herramientas para evaluar y mitigar riesgos.
3. Implementar buenas prácticas de seguridad.

RIESGOS DE SEGURIDAD EN CONTENEDORES

- Vulnerabilidades en imágenes de contenedores.
- Configuraciones inseguras.
- Acceso no autorizado.
- Falta de aislamiento entre contenedores.

EVALUACIÓN DE RIESGOS

Evaluar riesgos implica identificar vulnerabilidades y analizar su impacto. Utilizamos herramientas y técnicas específicas para esta tarea.

HERRAMIENTAS PARA EVALUAR RIESGOS

- Docker Bench for Security: Evalúa configuraciones de Docker.
- Clair: Analiza vulnerabilidades en imágenes de contenedores.

DOCKER BENCH FOR SECURITY

Docker Bench for Security es una herramienta que verifica configuraciones de seguridad en Docker, proporcionando recomendaciones para mejorar la seguridad.

CLAIR

Clair es una herramienta que analiza imágenes de contenedores en busca de vulnerabilidades conocidas, ayudando a mantener la seguridad de las aplicaciones.

BUENAS PRÁCTICAS DE SEGURIDAD

- Usar imágenes oficiales y actualizadas.
- Configurar políticas de red estrictas.
- Implementar autenticación y autorización.
- Monitorizar y actualizar contenedores regularmente.

CASOS DE ESTUDIO

Analizaremos casos reales donde se implementaron buenas prácticas de seguridad en contenedores, destacando lecciones aprendidas.

EVALUACIÓN Y REFLEXIÓN FINAL

- Cuestionario para evaluar comprensión.
- Discusión abierta para resolver dudas y reflexionar sobre lo aprendido.

RESUMEN

Hemos aprendido sobre los riesgos de seguridad en contenedores, herramientas para evaluarlos y cómo implementar buenas prácticas para mitigarlos.