ONE PAGE SUMMARY

IT & Software › Kubernetes › Kubernetes Security

Introduction to Kubernetes Security

Secure your Kubernetes environment to protect your applications and data.

DEFINITION

> Kubernetes security involves protecting your container orchestration platform from threats and vulnerabilities. It ensures that your applications run safely and securely in a cloud-native environment.

KEY CONCEPTS

Role-Based Access Control (RBAC)

RBAC manages who can access and perform actions in a Kubernetes cluster based on roles.

Network Policies

Network policies control the traffic flow between pods, enhancing security by limiting communication.

Pod Security Policies

These policies define security conditions for pod creation, ensuring they meet specific security standards.

Secrets Management

Kubernetes secrets store sensitive information like passwords and API keys securely within the cluster.

Image Scanning

Scanning container images for vulnerabilities before deployment helps prevent security risks.

EXAMPLES

→ Implement RBAC to restrict user permissions.

→ Use network policies to isolate sensitive applications.

→ Store database credentials as Kubernetes secrets.

MEMORY TIPS

★ Remember 'RBAC' as 'Roles Bring Access Control'.

★ Think of 'Network Policies' as 'Traffic Rules for Pods'.

★ Associate 'Secrets Management' with 'Keeping Secrets Safe'.

COMMON MISTAKES

✗ Neglecting to update security patches regularly.

✗ Over-permitting user roles in RBAC.

✗ Ignoring the importance of image scanning.

QUICK RECAP

Kubernetes security is vital for protecting applications in a cluster. Key areas include RBAC, network policies, and secrets management. Always ensure to scan images and enforce security policies to maintain a secure environment.