Infraestrutura Como Código com Terraform, AWS, Azure e Databricks

Segurança e Compliance

Ao trabalhar com Infraestrutura como Código (IaC), é essencial abordar questões de segurança e conformidade para garantir que a infraestrutura seja configurada corretamente e esteja em conformidade com as políticas e regulamentações aplicáveis. Aqui estão alguns cuidados e práticas recomendadas para considerar:

Princípio do menor privilégio: Garanta que os usuários e sistemas tenham acesso apenas aos recursos de que precisam para executar suas funções. Isso ajuda a limitar a exposição a possíveis ameaças e reduzir o impacto de violações de segurança.

Gerenciamento de chaves e senhas: Armazene e gerencie chaves e senhas, como chaves de API, credenciais de banco de dados e certificados, de forma segura e centralizada, usando ferramentas de gerenciamento como HashiCorp Vault, AWS Secrets Manager ou Azure Key Vault.

Rastreabilidade e auditoria: Mantenha um histórico detalhado das mudanças na infraestrutura e na configuração, incluindo informações sobre quem fez a mudança, quando e por quê. Isso facilita a identificação e a solução de problemas, além de atender aos requisitos de conformidade e auditoria.

Análise estática de código e verificação de conformidade: Use ferramentas de análise estática de código e verificação de conformidade para validar a configuração da infraestrutura e garantir que ela esteja em conformidade com as políticas e regulamentações aplicáveis. Exemplos de tais ferramentas incluem Checkov, Terrascan e Open Policy Agent (OPA).

Testes automatizados de segurança: Integre testes de segurança automatizados no pipeline CI/CD, incluindo varreduras de vulnerabilidades, testes de penetração e avaliações de conformidade, para identificar e corrigir problemas de segurança antes que a infraestrutura seja implantada em produção.

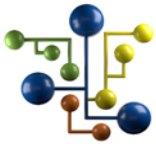
Segurança em camadas: Adote uma abordagem em camadas para a segurança da infraestrutura, incluindo firewalls, redes isoladas, segmentação de rede, criptografia de dados em repouso e em trânsito, e autenticação multifator (MFA) para acesso a recursos críticos.

Monitoramento e alerta contínuos: Monitore a infraestrutura e a configuração em tempo real, colete registros de eventos e gere alertas com base em desvios do estado desejado, atividades suspeitas ou violações de políticas.

Atualizações e patches: Mantenha a infraestrutura atualizada com patches de segurança e atualizações de software para proteger contra vulnerabilidades conhecidas e emergentes.

Capacitação e conscientização: Eduque os desenvolvedores e operadores sobre as melhores práticas de segurança e conformidade ao trabalhar com IaC, e promova uma cultura de responsabilidade compartilhada pela segurança.

Ao seguir essas práticas recomendadas, as equipes podem abordar proativamente questões de segurança e conformidade ao trabalhar com IaC, minimizar o risco de violações de segurança e garantir a conformidade com políticas e regulamentações aplicáveis.



Equipe DSA

Muito Obrigado!
Continue Trilhando Uma Excelente Jornada de Aprendizagem.