re_S21_A1_SL6_backend

Entrega no AVA

Nome: _____ Turma: _____

Título da atividade: Gerenciando configurações e segredos em ambientes corporativos

Contexto

A gestão de segredos é essencial para proteger informações sensíveis, como senhas, tokens de acesso, chaves de API e certificados. Ferramentas como HashiCorp Vault, AWS Secrets Manager e Azure Key Vault oferecem soluções para armazenar, gerenciar e acessar segredos de maneira segura. Entre as opções disponíveis, destacam-se:

- **HashiCorp Vault:** poderosa ferramenta para armazenar e acessar segredos. Suporta controle de acesso baseado em políticas, geração dinâmica de credenciais e auditoria de acessos;
- **AWS Secrets Manager:** solução integrada ao ecossistema AWS para gerenciar segredos em aplicações em nuvem;
- **Azure Key Vault:** ideal para ambientes baseados em Microsoft Azure, com suporte a gerenciamento de certificados e segredos.

Gerenciar configurações em ambientes de produção envolve armazenar variáveis sensíveis e específicas do ambiente (ex.: URLs de banco de dados ou *endpoints* de APIs). É recomendado separar configurações do código usando arquivos de configuração, serviços dedicados ou sistemas de gestão de configurações. Algumas boas práticas incluem:

- **separação por ambiente:** configurações distintas para desenvolvimento, homologação e produção;

- **centralização:** uso de ferramentas como ConfigMaps no Kubernetes ou AWS Parameter Store;
- **auditoria e controle:** registro de todas as alterações para evitar configurações incorretas.

Exemplos práticos

- Uma aplicação precisa acessar diferentes APIs em ambientes de homologação e produção. A solução é armazenar os *endpoints* em variáveis de ambiente ou em um serviço de gestão de segredos, acessando-os dinamicamente com base no ambiente configurado.
- Tokens de API usados para autenticação com provedores externos são armazenados no Vault, garantindo acesso apenas para serviços autorizados.

Roteiro da atividade

Vocês receberam um e-mail do gestor de segurança informando:

"Temos enfrentado dificuldades em gerenciar tokens de acesso em nossos sistemas e já tivemos problemas de exposição em repositórios. Precisamos de uma estratégia para proteger esses segredos e gerenciar configurações em produção. Vocês podem propor um plano?"

Situação fictícia produzida pela SEDUC-SP.

Redijam um plano detalhado abordando:

1. Ferramentas recomendadas e justificativas para sua escolha.
2. Boas práticas para gestão de configurações em produção.
3. Estratégias para implementar a separação de segredos por ambiente.

Após redigirem o plano, respondam:

1. Quais ferramentas recomendariam para gerenciar segredos e por quê?
2. Como garantiriam que as configurações estão seguras em produção?
3. Por que é importante separar segredos por ambiente?
4. Como documentar e manter a gestão de segredos acessível à equipe?