

# Projeto de Infraestrutura de Servidores Distribuídos

## Introdução:

Este documento descreve o projeto de uma infraestrutura de servidores distribuídos, utilizando virtualização e contêineres, com foco em segurança, estabilidade, disponibilidade e integridade. O ambiente será configurado para hospedar sistemas e sites, seguindo as diretrizes da ISO 9001 para documentação e implementação.

## Objetivo:

O objetivo principal do projeto é a construção de uma infraestrutura robusta e escalável que atenda às necessidades de nossos sistemas e sites, garantindo alta disponibilidade e segurança.

## Escopo do Projeto:

O projeto abrange as seguintes etapas:

- **Planejamento:**
  - Definição dos requisitos e recursos necessários para o ambiente.
  - Criação de diagrama de arquitetura detalhado.
  - Escolha da plataforma de virtualização (VMware ou Blackbox).
  - Seleção de ferramentas de contêinerização (Docker, Kubernetes, etc.).
  - Definição de políticas de segurança e monitoramento.
- **Implementação:**
  - Configuração da plataforma de virtualização escolhida (VMware ou Blackbox).
  - Implantação dos servidores virtuais.
  - Instalação e configuração dos sistemas operacionais.
  - Implementação da plataforma de contêinerização.
  - Configuração de redes e serviços (DNS, firewall, etc.).
  - Implementação de medidas de segurança (antivírus, firewalls, etc.).
  - Configuração de ferramentas de monitoramento.
- **Testes e Documentação:**
  - Realização de testes de carga e performance.
  - Verificação da segurança e integridade do ambiente.
  - Documentação completa da infraestrutura e das configurações.
- **Manutenção:**
  - Monitoramento constante do ambiente.
  - Realização de backups regulares.
  - Atualização de sistemas operacionais e softwares.
  - Resolução de problemas e incidentes.

## Estrutura do Projeto:

A estrutura do projeto será organizada da seguinte forma:

- **Camada de Virtualização:**

- A plataforma de virtualização (VMware ou Blackbox) será utilizada para criar servidores virtuais que hospedarão os sistemas e serviços.
- A camada de virtualização oferece recursos de isolamento, gerenciamento de recursos e alta disponibilidade.

- **Camada de Containerização:**

- A plataforma de containerização (Docker, Kubernetes, etc.) será utilizada para encapsular as aplicações e suas dependências em contêineres.
- A camada de containerização permite a execução de diferentes aplicações em um mesmo servidor, garantindo portabilidade e escalabilidade.

- **Camada de Rede:**

- A rede será configurada para garantir a comunicação entre os servidores virtuais e a internet.
- A rede também deve garantir segurança e desempenho.

- **Camada de Segurança:**

- A segurança será implementada em várias camadas, incluindo firewalls, antivírus, autenticação de usuários e criptografia de dados.

- **Camada de Monitoramento:**

- O monitoramento será realizado através de ferramentas que coletam dados sobre o desempenho e funcionamento do ambiente.
- Os dados de monitoramento serão utilizados para identificar e solucionar problemas.

## **Modulos:**

O projeto será dividido em módulos, cada um com suas responsabilidades e metas:

- **Modulo de Virtualização:** Responsável pela configuração e gerenciamento da plataforma de virtualização.
- **Modulo de Containerização:** Responsável pela instalação e configuração da plataforma de containerização.
- **Modulo de Rede:** Responsável pela configuração da rede e dos serviços de rede.
- **Modulo de Segurança:** Responsável pela implementação das políticas de segurança.
- **Modulo de Monitoramento:** Responsável pela implementação do sistema de monitoramento.

## **Aplicações na Nuvem:**

O projeto pode ser implementado em plataformas de nuvem como VMware Cloud ou AWS.

## **Plataforma VMware:**

A plataforma VMware oferece recursos de virtualização, gerenciamento de recursos, alta disponibilidade e segurança. A escolha da plataforma VMware depende dos requisitos

específicos do projeto, como o nível de segurança e a necessidade de integração com outras soluções VMware.

### **Blackbox:**

A Blackbox é uma plataforma de virtualização open source que oferece recursos de gerenciamento de recursos e alta disponibilidade. A Blackbox é uma alternativa mais flexível e econômica em relação à VMware.

### **Considerações finais:**

O projeto de infraestrutura de servidores distribuídos é um processo complexo que exige planejamento e implementação cuidadosos. O sucesso do projeto dependerá da escolha das tecnologias adequadas, da qualidade da implementação e do monitoramento constante do ambiente.

### **Documentação:**

A documentação do projeto deve ser completa e detalhada, incluindo os seguintes tópicos:

- **Requisitos:** Descrição dos requisitos do projeto.
- **Arquitetura:** Diagrama de arquitetura detalhado.
- **Configurações:** Documentação de todas as configurações.
- **Procedimentos:** Documentação dos procedimentos operacionais.
- **Manutenção:** Descrição das atividades de manutenção.

A documentação deve ser organizada e facilmente acessível para que os usuários e administradores possam facilmente consultar as informações necessárias.

# **SEGURANÇA - PENTEST**

## **Segurança Básica**

- **Mantenha o sistema atualizado:** Use `apt update` e `apt upgrade` para garantir que você tenha as últimas versões de software e patches de segurança.
- **Use senhas fortes e gerenciador de senhas:** Evite senhas óbvias e gerencie suas senhas com um gerenciador confiável.
- **Ative o firewall:** Configure o firewall do seu servidor para bloquear o acesso não autorizado.
- **Desabilite os serviços desnecessários:** Se você não precisar de um serviço, desative-o para reduzir a superfície de ataque.
- **Crie um usuário com privilégios limitados:** Evite usar o usuário root para tarefas do dia a dia.
- **Mantenha o software atualizado:** Isso inclui aplicativos, bibliotecas e o sistema operacional.

- **Proteja sua rede:** Utilize um firewall, VPN e outros mecanismos de segurança para proteger sua rede.

## Segurança Avançada

- **Utilize um sistema de detecção de intrusões (IDS):** Isso pode ajudar a identificar e bloquear atividades maliciosas.
- **Implemente a autenticação multifator (MFA):** Adicione uma camada extra de segurança ao exigir mais do que apenas uma senha para acessar o servidor.
- **Crie backups regulares:** Os backups regulares ajudam a restaurar seus dados caso o servidor seja comprometido.
- **Monitoramento constante:** Monitore seu sistema em busca de atividades suspeitas e configurações desprotegidas.
- **Verifique logs regularmente:** Monitore os logs do sistema para identificar atividades suspeitas e erros.
- **Use criptografia:** Criptografe dados confidenciais em trânsito e em repouso.
- **Segurança de dados:** Implemente medidas para proteger a confidencialidade, integridade e disponibilidade dos dados.
- **Gerenciamento de acesso:** Implemente um sistema para controlar quem tem acesso a quais recursos e dados do servidor.
- **Segurança de aplicativos:** Utilize medidas para proteger seus aplicativos e serviços contra ataques.
- **Treinamento e conscientização:** Treine os usuários sobre as melhores práticas de segurança e como identificar e relatar ameaças.