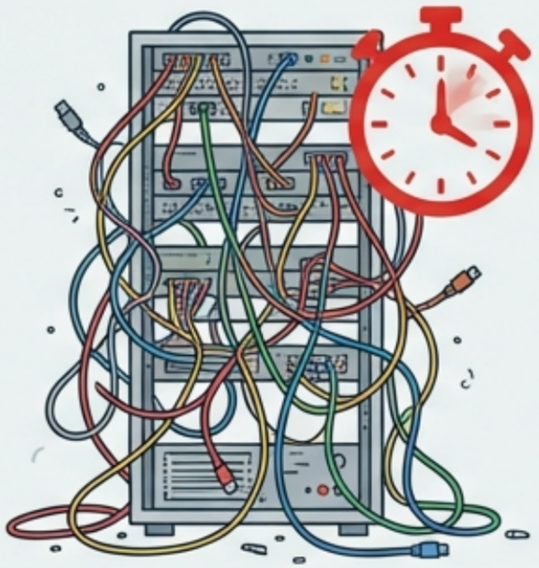
Ubuntu Hardening
(Edição Systemd)

Automação de Segurança e
Conformidade para Servidores.

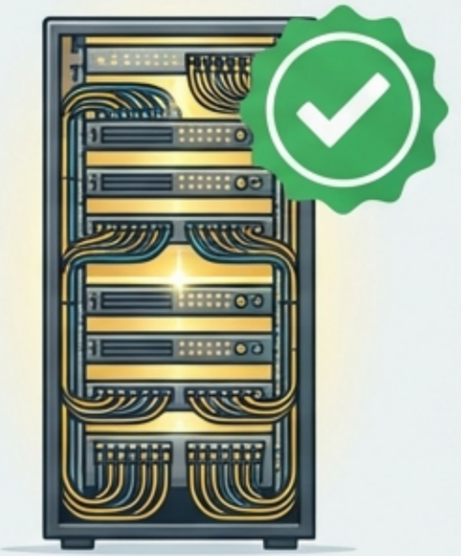
Transformando instalações padrão em Imagens Douradas

Antes



Horas de trabalho manual
hors de trabalho manual suscetível a
erros humanos.

Depois



Uma linha de base de segurança (baseline)
rigorosa implementada em segundos,
baseada nas recomendações do CIS
(Center for Internet Security).

Por que adotar esta automação em sua infraestrutura

Redução da Superfície de Ataque.
(Desativa módulos desnecessários como Bluetooth e Firewire).

Conformidade em Segundos.
(Aplica controles do benchmark CIS instantaneamente).

Proteção Ativa.
(Configura nativamente UFW, PSAD, Auditd e AIDE).

Facilidade de Auditoria.
(Inclui bateria de testes Bats para validação).

Uma arquitetura robusta baseada em cinco frentes

Kernel

Hardening de rede via sysctl e restrição de módulos (DCCP, SCTP).

Acesso

SSH restrito, bloqueio de conta root, regras de firewall via UFW.

Auditoria

Auditoria completa de chamadas de sistema com Auditd e monitoramento de logs.

Arquivos

Verificação de integridade sistemática com AIDE e debsums.

Identidade

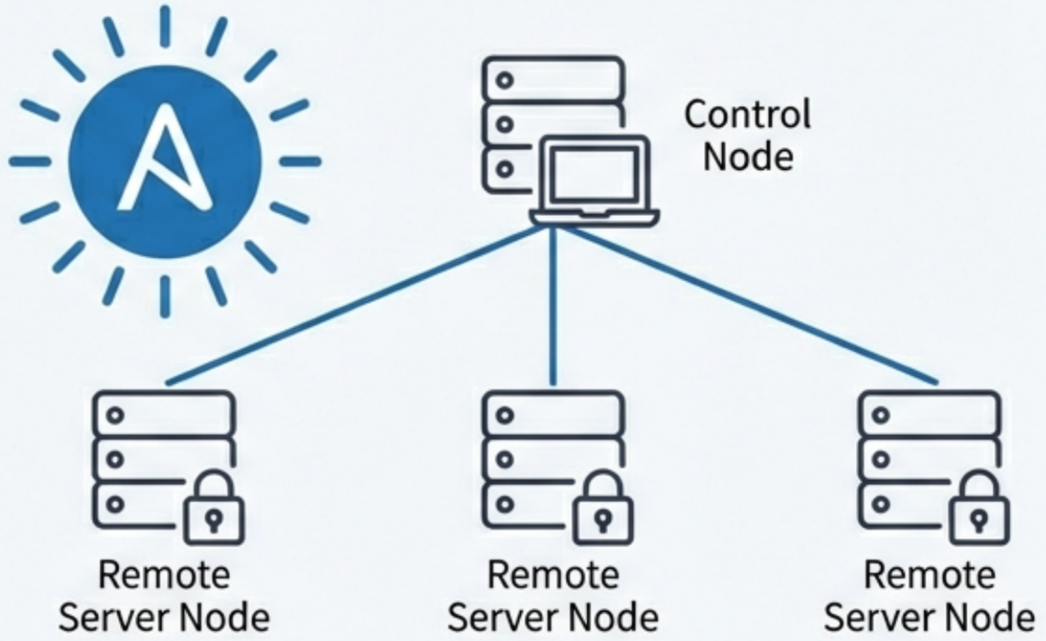
Políticas de senhas fortes e limpeza de usuários desnecessários.

O pipeline de transformação de segurança (Fase 1)

Finalizando a blindagem do servidor (Fase 2)

Implantação em escala via Ansible

Perfeito para preparar servidores remotos do zero.
O playbook realiza o update do sistema, instala o SSH e aplica todo o hardening de forma padronizada.




```
cd ansible/
ansible-playbook -i inventory.ini site.yml
```

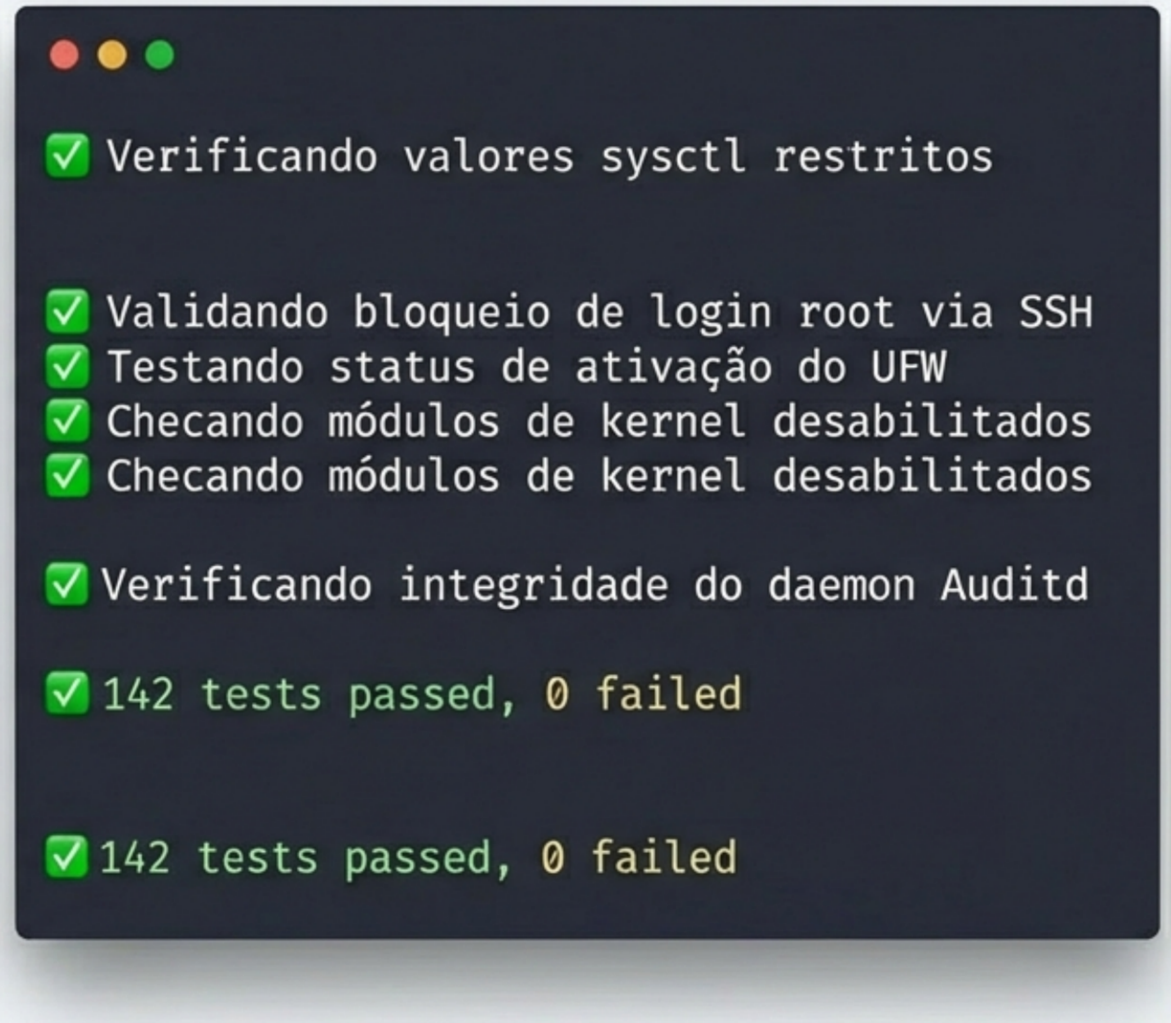
Construindo imagens Golden em containers Docker

Crie containers Ubuntu já endurecidos nativamente, prontos para receber e isolar as aplicações da sua empresa com a máxima segurança.

```
# Na raiz do projeto:
docker-compose build
```

Validação contínua com testes automatizados

A segurança não termina na instalação. Após a reinicialização, o framework de testes Bats é utilizado para validar centenas de configurações individuais, garantindo que o servidor permaneça em estrita conformidade.



Implementando a linha de base em quatro passos

1

Instalação Limpa.

(Requer Ubuntu Server Minimized 22.04 ou 24.04).

2

Instalar Dependências.

(Preparo inicial do sistema).

3

Download & Config.

(Clonar o repositório e ajustar parâmetros).

4

Execução.

(Rodar o script e reiniciar).

Atenção aos parâmetros críticos de operação

Não Idempotente

O script principal não é idempotente. Teste sempre de forma isolada em um ambiente de homologação antes de aplicar em servidores de produção.

Configuração Obrigatória

Segurança por design. Você deve obrigatoriamente atualizar a variável CHANGEME no arquivo ubuntu.cfg. Caso contrário, o script abortará a execução por segurança.

Explore a documentação e colabore

Acesse detalhes profundos, referências técnicas e guias passo a passo em nosso portal interativo (rode mkdocs serve).

Encontrou algo estranho ou quer sugerir uma melhoria? O projeto é open-source. Sinta-se à vontade para abrir uma Issue ou enviar um Pull Request no GitHub.