Automatização de Hardening Linux

Usando Ansible

SOBRE

- Cleriston Freitas
- Formado em Sistemas de Informação e especialização em Segurança da Informação
- Analista de Redes em um Data Center Privado
- Entusiasta em Segurança da Informação
- Co-Founder do HackBahia

AGENDA

1. O que é Hardening?
2. Problemas ao fazer os procedimentos de forma manual
3. O que é Ansible
4. Arquitetura Básica do Ansible
5. Executando o Ansible (vídeo)
6. Dicas

O QUE É HARDENING

- Técnica para o fortalecimento da segurança da informação em Servidores e Serviços;
- Redução dos Riscos;
- Aplicar diretivas de segurança;
- Tratamento de ameaças;
- Aplicável em qualquer tipo de sistema operacional, sistemas e serviços;

O QUE É HARDENING (cont..)

Técnicas Básicas de Hardening em Sistemas Linux:

- Manter o sistema sempre atualizado;
- Desinstalar softwares desnecessários;
- Desabilitar o usuário root;
- Gerenciamento de privilégios;
- Desabilitar protocolos não seguros;
- Configurar Firewall local;
- Uso de Criptografia;
- SELinux e AppArmor.

PROCEDIMENTOS MANUAIS

- Gasto maior do tempo;
- Procedimentos não padronizado;
- Menos produtividade;
- Aumento dos custos;
- Maior probabilidade de erros;
- Menos tempo para o café.


QUERO
CAFÉ

O QUE É ANSIBLE

Características:

- Ferramenta de automação;
- Open Source;
- Escrita em Python;
- Mantida pela Red Hat;
- Utiliza a linguagem YAML (Chave Valor);
- Sem Agentes;
- Idempotente;
- Curva de aprendizado.

O QUE É ANSIBLE

Benefícios do Ansible:

- Melhor uso do tempo;
- Maior produtividade;
- Redução de custos;
- Redução dos erros;
- Mais tempo para o Café

ARQUITETURA DO ANSIBLE

- Inventário

```
[webservers]
192.168.35.140
192.168.35.150

[datacache]
192.168.45.45

[appservers]
192.168.100.1
192.168.100.2

[dbservers]
172.35.0.10
```

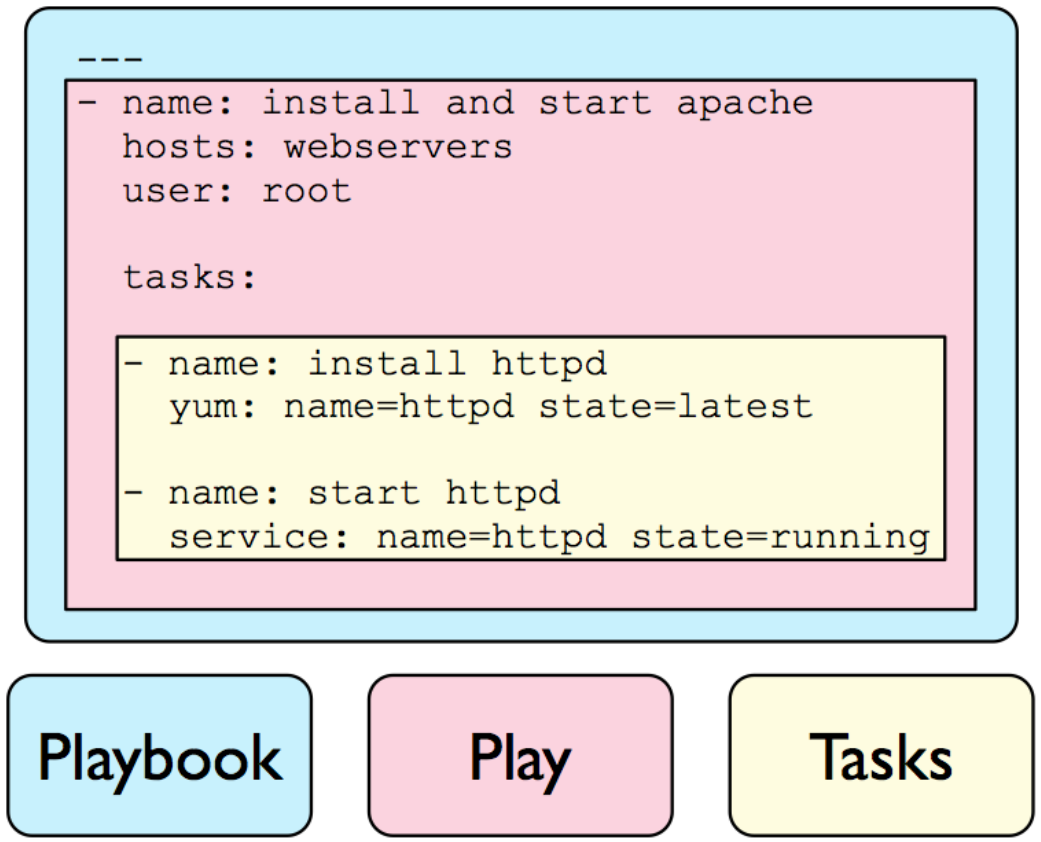
ARQUITETURA DO ANSIBLE

- Roles

```
ansible@ansibleserver:~$ tree
.
└── ensi
    ├── hosts
    ├── playbook.yml
    └── roles
        └── hardening_ubuntu
            ├── defaults
            ├── files
            ├── handlers
            │   └── main.yml
            ├── meta
            ├── tasks
            │   ├── firewall.yml
            │   ├── login_root.yml
            │   ├── main.yml
            │   ├── remover_pacotes.yml
            │   ├── ssh.yml
            │   └── updates.yml
            ├── templates
            └── vars
```

ARQUITETURA DO ANSIBLE

- Playbooks e Tasks

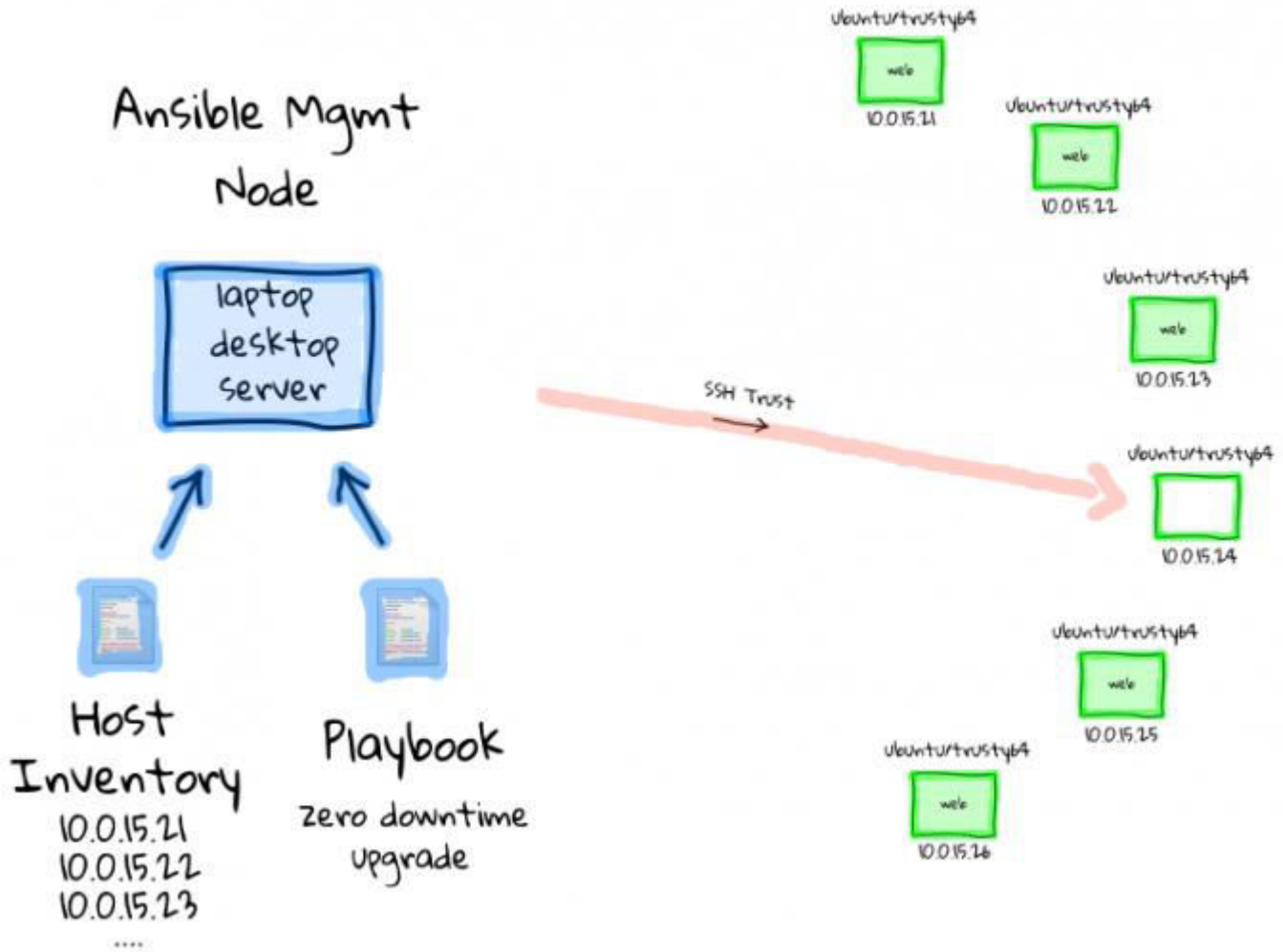


- Módulos

Module Index

- All modules
- Cloud modules
- Clustering modules
- Commands modules
- Crypto modules
- Database modules
- Files modules
- Identity modules
- Inventory modules
- Messaging modules
- Monitoring modules
- Net Tools modules
- Network modules
- Notification modules
- Packaging modules
- Remote Management modules
- Source Control modules
- Storage modules
- System modules
- Utilities modules
- Web Infrastructure modules
- Windows modules

ARQUITETURA DO ANSIBLE



EXECUANDO O ANSIBLE

DICAS

- Framework CIS
- Documentação do Ansible
- Ansible-Galaxy

DUVIDAS??