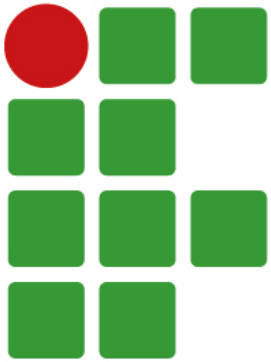


INSTITUTO FEDERAL
DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
São Paulo

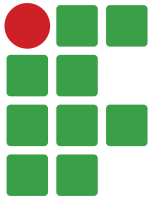
Monitoramento de Rede

Soluções implementadas na DTI

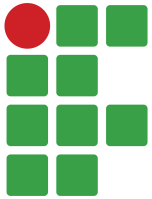
Geraldo Jr

CAOTI/DTI
IFSP

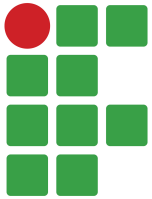
20/06/2023



Sumário

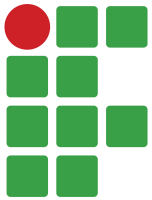


Sumário



Por quê monitorar?

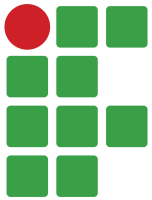
Benefícios:



Por quê monitorar?

Benefícios:

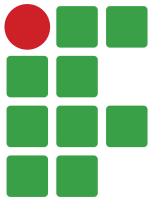
- Ajuda a diagnosticar problemas e prevenir falhas;



Por quê monitorar?

Benefícios:

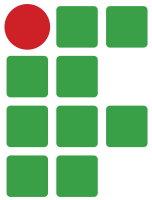
- Ajuda a diagnosticar problemas e prevenir falhas;
- Facilita na resolução de problemas (Troubleshoting);



Por quê monitorar?

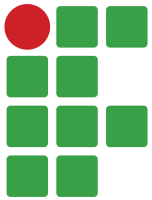
Benefícios:

- Ajuda a diagnosticar problemas e prevenir falhas;
- Facilita na resolução de problemas (Troubleshoting);
- É menos custoso.



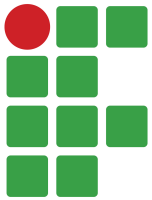
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)



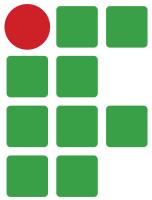
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais



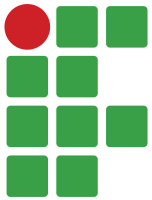
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM



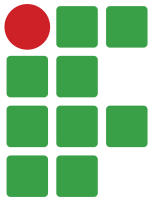
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM
  - Constantemente listado em Blacklist



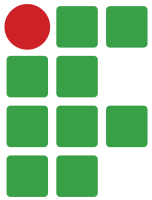
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM
  - Constantemente listado em Blacklist
  - Logs sem tratamento



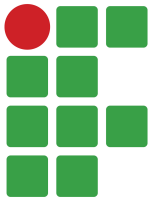
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM
  - Constantemente listado em Blacklist
  - Logs sem tratamento
- Analise dos logs



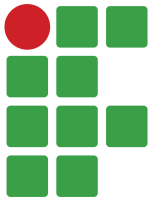
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM
  - Constantemente listado em Blacklist
  - Logs sem tratamento
- Analise dos logs
  - Transformar dados em informação (Elastic Stack)



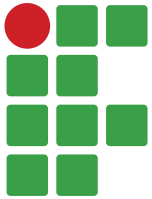
Estudo de caso 1 - Zimbra

- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM
  - Constantemente listado em Blacklist
  - Logs sem tratamento
- Analise dos logs
  - Transformar dados em informação (Elastic Stack)
  - ELK + Zabbix » Grafana



Estudo de caso 1 - Zimbra

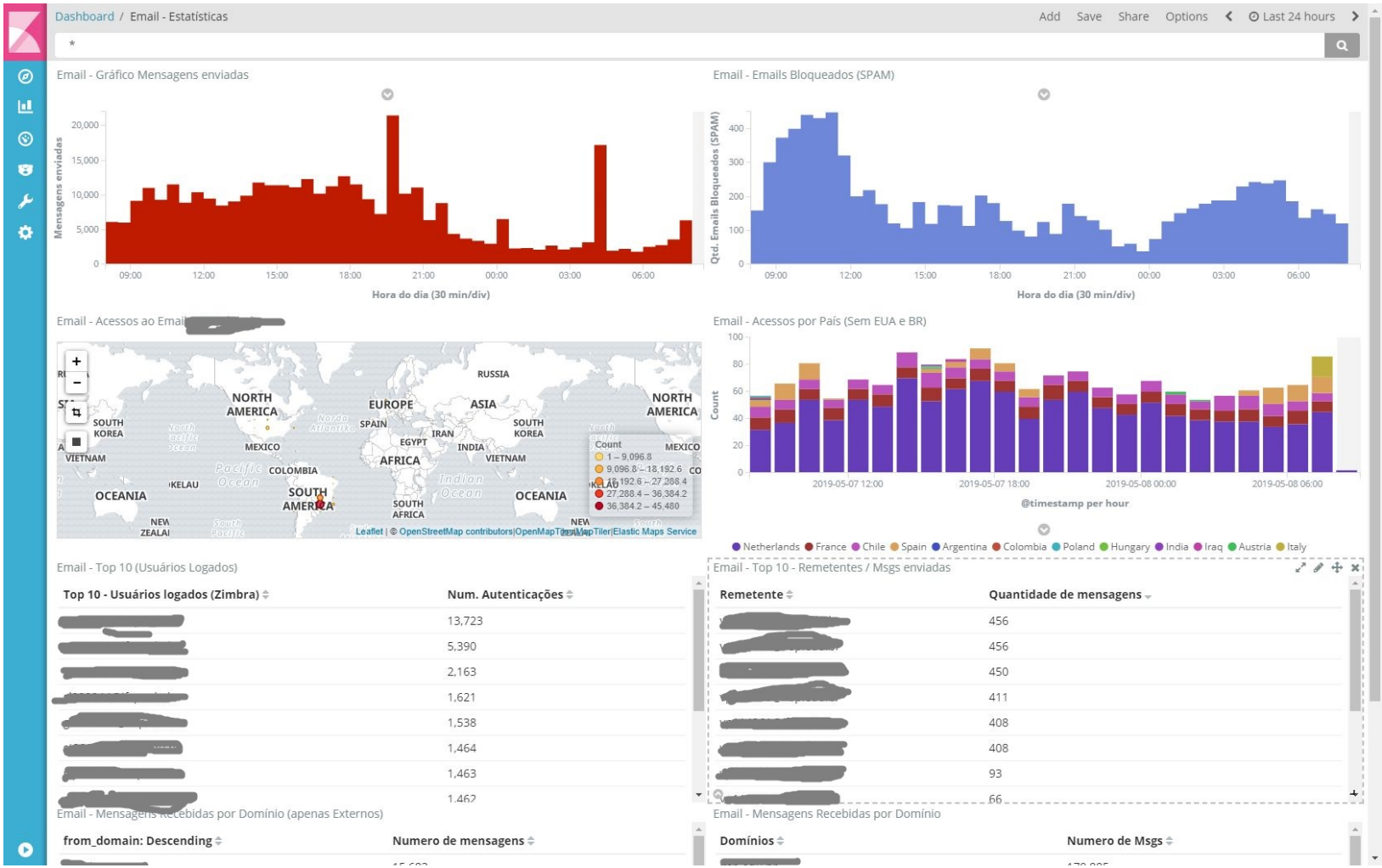
- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM
  - Constantemente listado em Blacklist
  - Logs sem tratamento
- Analise dos logs
  - Transformar dados em informação (Elastic Stack)
  - ELK + Zabbix » Grafana
  - Configuração de Blacklists > Diminuição de SPAM



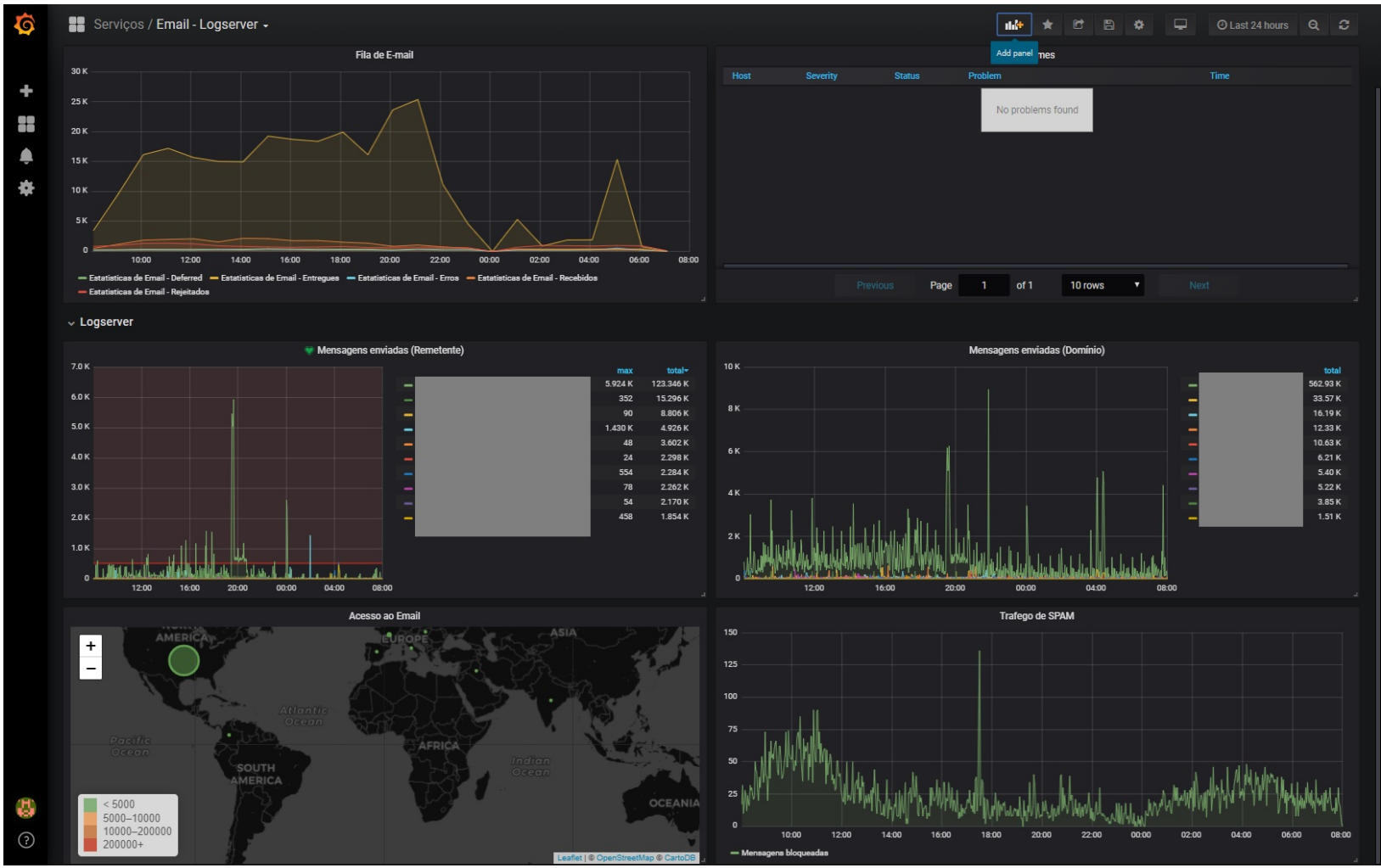
Estudo de caso 1 - Zimbra

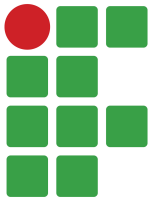
- Zimbra (E-mail Institucional até Jul/21)
  - Alto índice de comprometimento de credenciais
  - Alto índice de SPAM
  - Constantemente listado em Blacklist
  - Logs sem tratamento
- Analise dos logs
  - Transformar dados em informação (Elastic Stack)
  - ELK + Zabbix » Grafana
  - Configuração de Blacklists > Diminuição de SPAM
  - Monitoramento de filas > CBPolycid > Automação do Bloqueio de contas

Dashboard Kibana - Estatísticas do E-mail



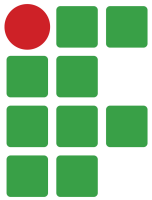
Dashboard Grafana - Estatísticas do E-mail





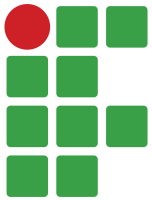
Estudo de caso 2 - Stonesoft

- Monitoramento de Firewall StoneSoft
  - Zabbix + Grafana: Centralização e compartilhamento de informações



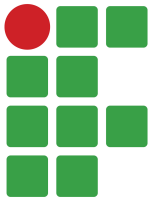
Estudo de caso 2 - Stonesoft

- Monitoramento de Firewall StoneSoft
  - Zabbix + Grafana: Centralização e compartilhamento de informações
    - Identificação de gargalos



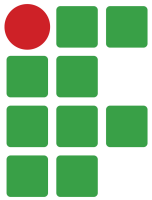
Estudo de caso 2 - Stonesoft

- Monitoramento de Firewall StoneSoft
  - Zabbix + Grafana: Centralização e compartilhamento de informações
    - Identificação de gargalos
    - Identificação de possíveis problemas de config



Estudo de caso 2 - Stonesoft

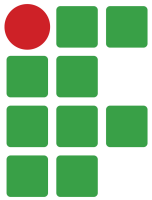
- Monitoramento de Firewall StoneSoft
  - Zabbix + Grafana: Centralização e compartilhamento de informações
    - Identificação de gargalos
    - Identificação de possíveis problemas de config
    - Auxilio na identificação de falhas



Estudo de caso 2 - Stonesoft

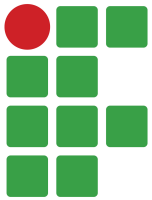
- Monitoramento de Firewall StoneSoft
  - Zabbix + Grafana: Centralização e compartilhamento de informações
    - Identificação de gargalos
    - Identificação de possíveis problemas de config
    - Auxilio na identificação de falhas
  - Dashboards do Stone: Detalhamento do tráfego

Dashboard Grafana - Stonesoft



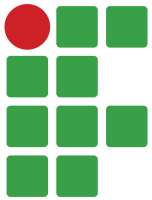
Estudo de caso 3 - HPE IMC

- NMS licenciado HPE / Aruba



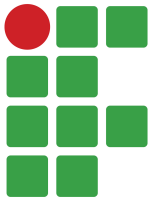
Estudo de caso 3 - HPE IMC

- NMS licenciado HPE / Aruba
- Gerencia de rede e elemento



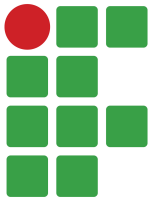
Estudo de caso 3 - HPE IMC

- NMS licenciado HPE / Aruba
- Gerencia de rede e elemento
- Compatível com HP, 3Com, Aruba entre outros



Estudo de caso 3 - HPE IMC

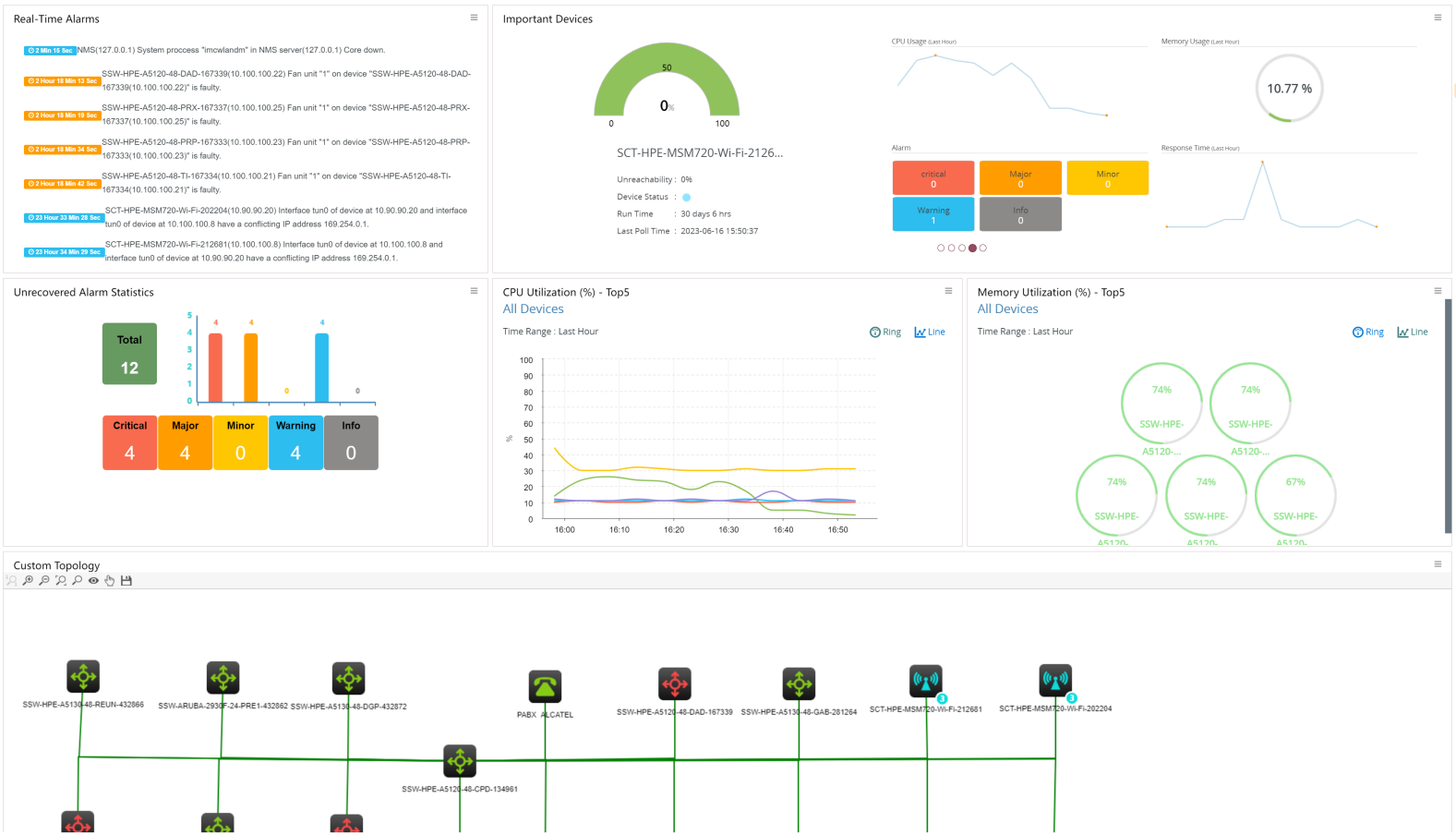
- NMS licenciado HPE / Aruba
- Gerencia de rede e elemento
- Compatível com HP, 3Com, Aruba entre outros
- SNMP, TELNET, SSH entre outros



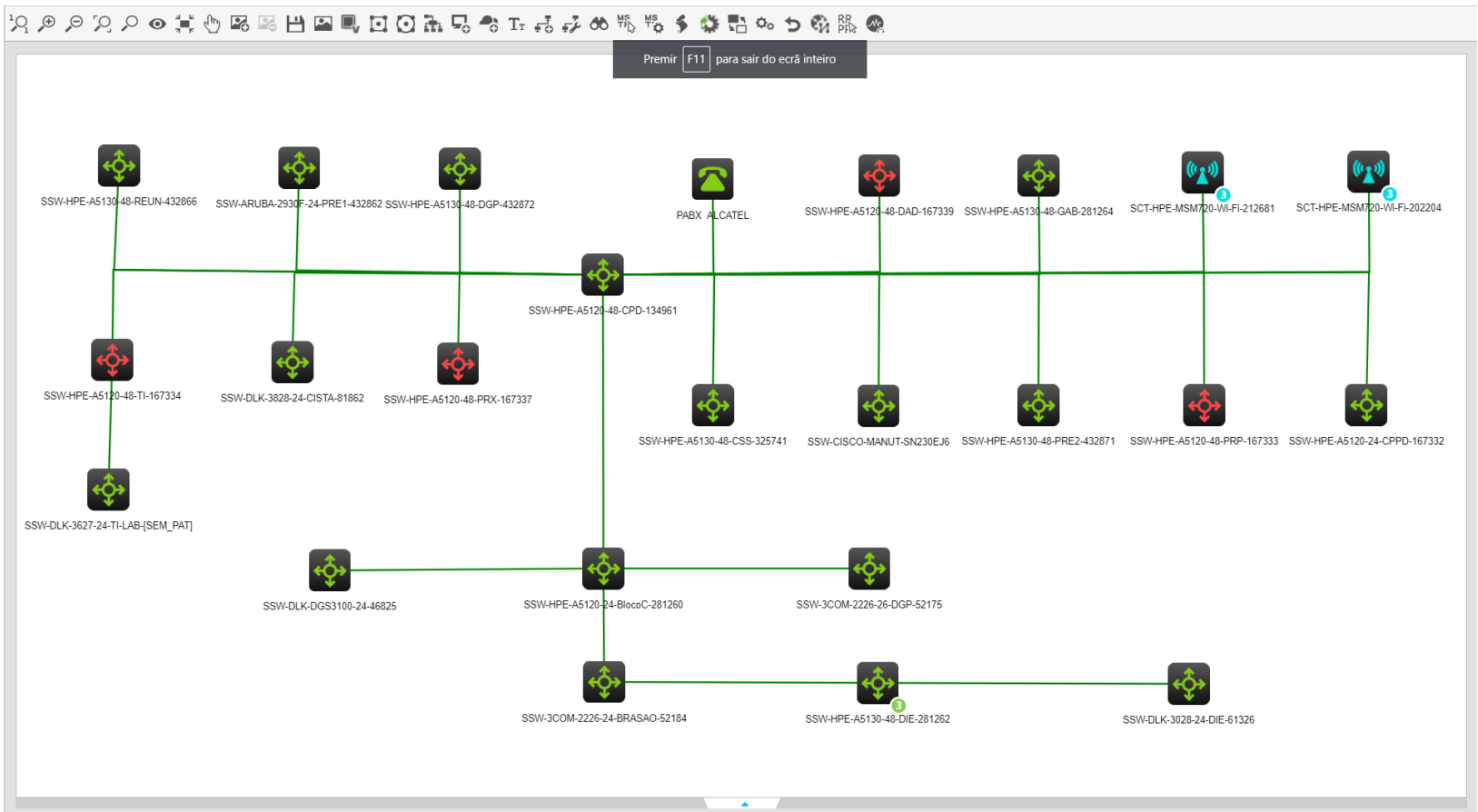
Estudo de caso 3 - HPE IMC

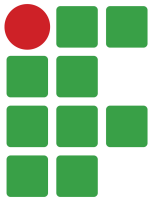
- NMS licenciado HPE / Aruba
- Gerencia de rede e elemento
- Compatível com HP, 3Com, Aruba entre outros
- SNMP, TELNET, SSH entre outros
- Instalação com muitos pré-requisitos

Dashboard HPE IMC



Dashboard HPE IMC





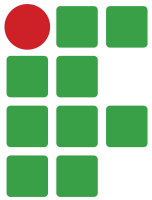
Qual ferramenta escolher?

a) Zabbix

b) ELK Stack

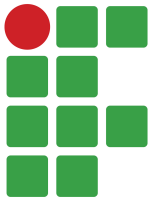
c) HPE IMC

d) Grafana Stack (Prometheus, Loki, Tempo, etc)



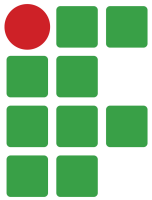
Bonus: The Dude - MikroTik

- Ferramenta de monitoramento de rede da MikroTik



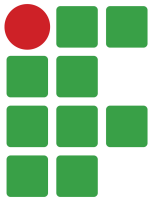
Bonus: The Dude - MikroTik

- Ferramenta de monitoramento de rede da MikroTik
- Descoberta automática de dispositivos



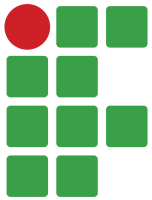
Bonus: The Dude - MikroTik

- Ferramenta de monitoramento de rede da MikroTik
- Descoberta automática de dispositivos
- Mapas de rede



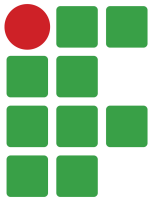
Bonus: The Dude - MikroTik

- Ferramenta de monitoramento de rede da MikroTik
- Descoberta automática de dispositivos
- Mapas de rede
- Monitoramento em tempo real



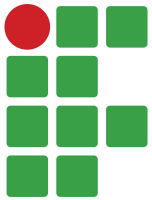
Bonus: The Dude - MikroTik

- Ferramenta de monitoramento de rede da MikroTik
- Descoberta automática de dispositivos
- Mapas de rede
- Monitoramento em tempo real
- Notificações por e-mail, SMS, etc.



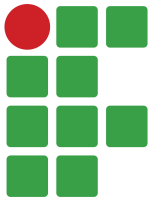
Bonus: The Dude - MikroTik

- Adequado para redes menores



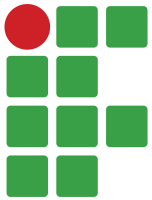
Bonus: The Dude - MikroTik

- Adequado para redes menores
- Operação em ambiente Mikrotik (RouterOS ou CHR)



Bonus: The Dude - MikroTik

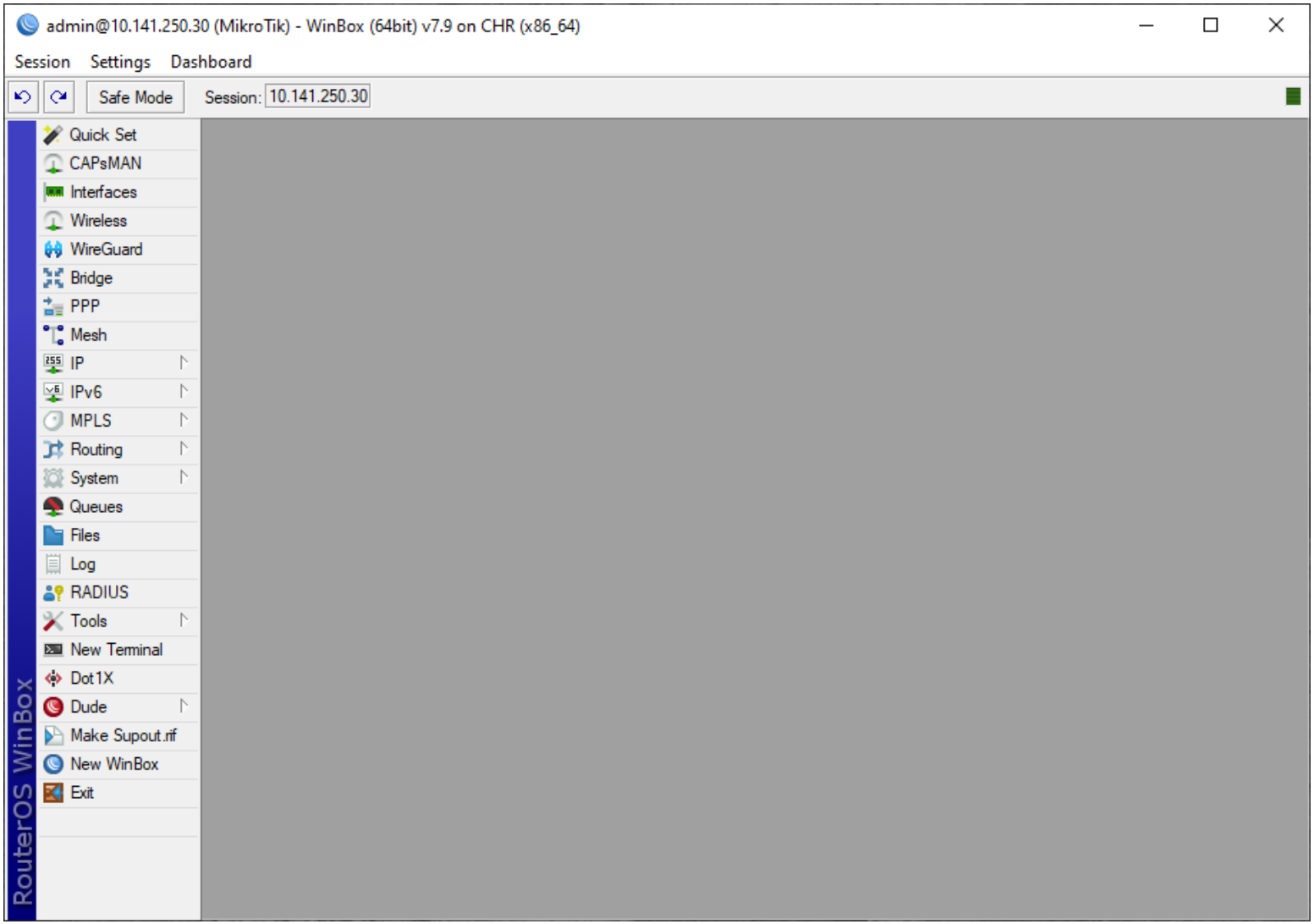
- Adequado para redes menores
- Operação em ambiente Mikrotik (RouterOS ou CHR)
- Interface gráfica intuitiva



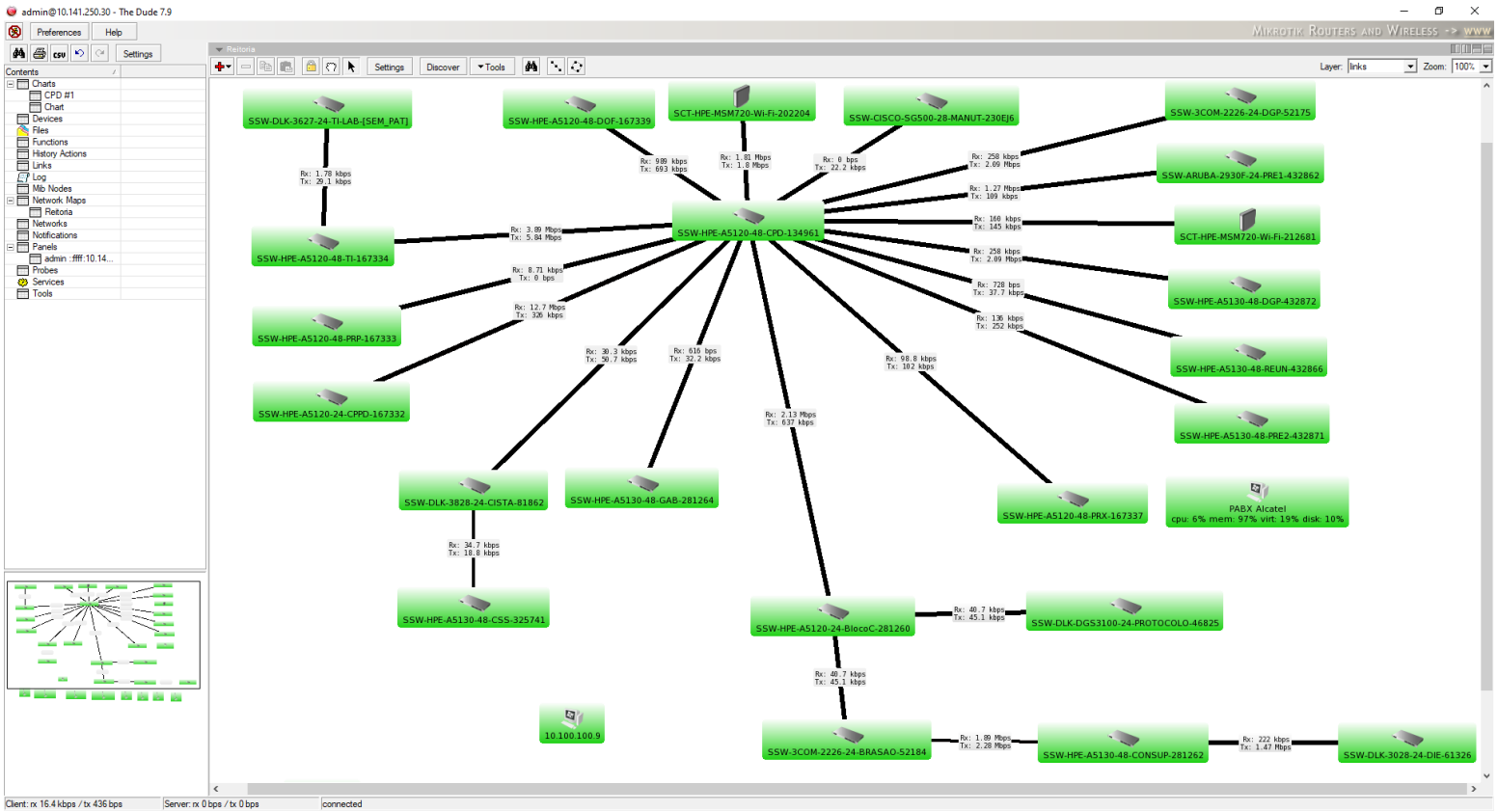
Bonus: The Dude - MikroTik

- Adequado para redes menores
- Operação em ambiente Mikrotik (RouterOS ou CHR)
- Interface gráfica intuitiva
- Mapeamento de rede

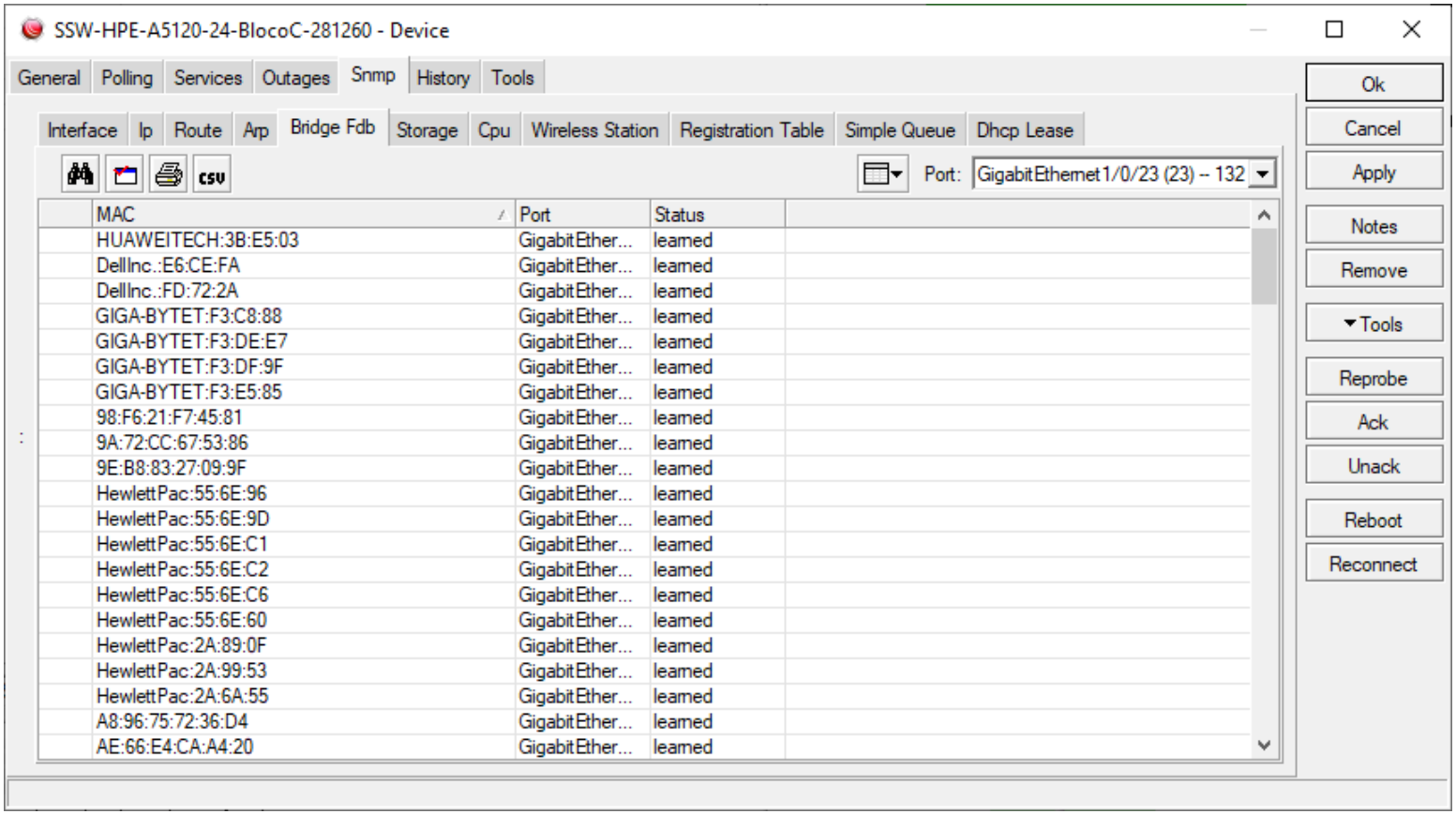
CHR - Configuração



Dude - Topologia

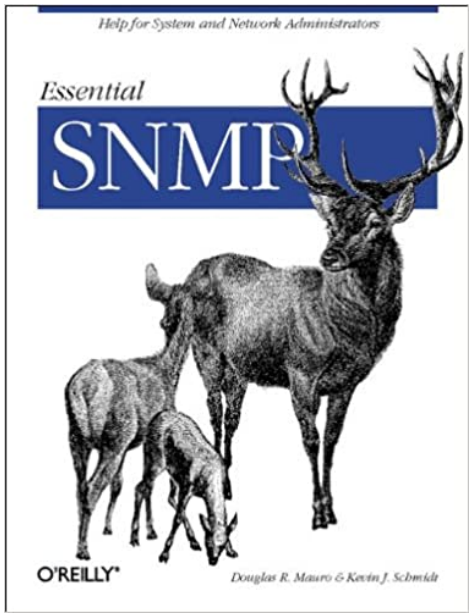


Dude - SNMP

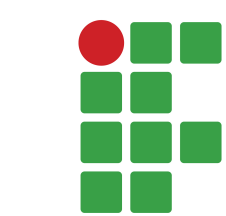


Perguntas?

Para saber mais...



`https://wiki.mikrotik.com/wiki/`



Até a próxima

Contato: geraldo.junior@ifsp.edu.br