

**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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

1 Monitoramento de Rede

- Por quê monitorar?

2 Exemplo de sistemas em uso na DTI

- Estudo de caso
- Qual ferramenta escolher?
- Bonus: Uma opção SOHO

3 Duvidas



Sumário

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

1 Monitoramento de Rede

■ Por quê monitorar?

2 Exemplo de sistemas em uso na DTI

■ Estudo de caso

■ Qual ferramenta escolher?

■ Bonus: Uma opção SOHO

3 Duvidas



Por quê monitorar?

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

Benefícios:



Por quê monitorar?

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

Benefícios:

- Ajuda a diagnosticar problemas e prevenir falhas;



Por quê monitorar?

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas

Benefícios:

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



Por quê monitorar?

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

Benefícios:

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



Estudo de caso 1 - Zimbra

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Estudo de caso 1 - Zimbra

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Estudo de caso 1 - Zimbra

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Estudo de caso 1 - Zimbra

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

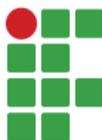
Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

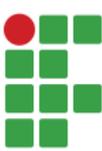
Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

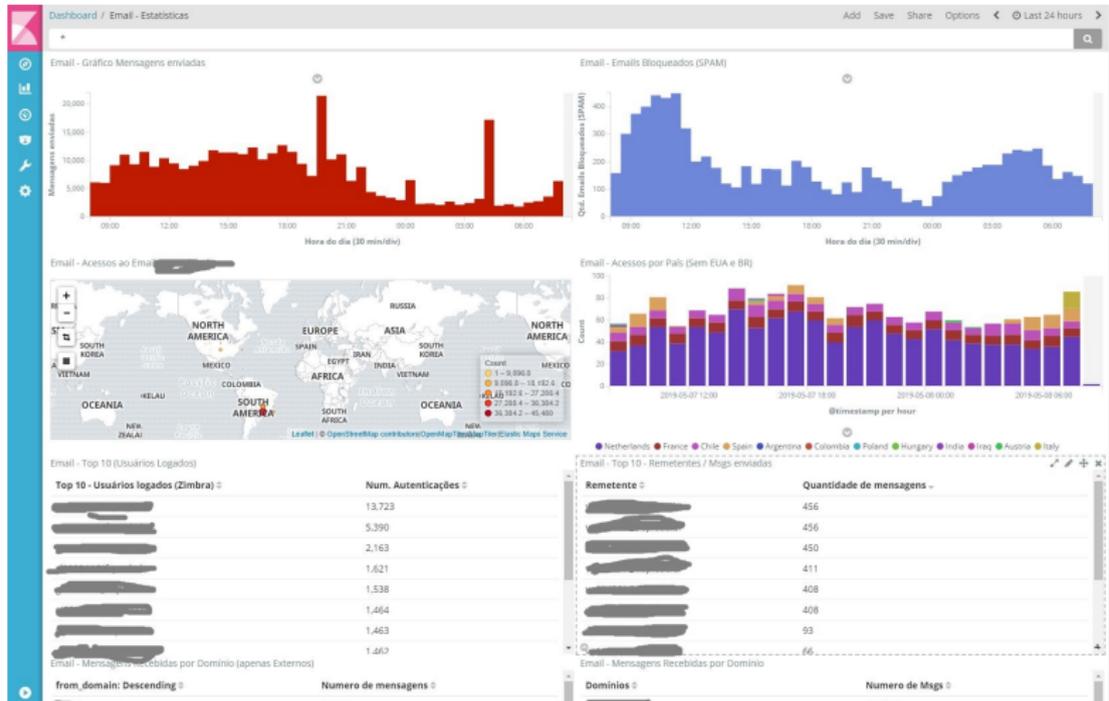
Exemplo de sistemas em uso na DTI

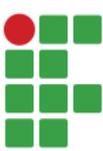
Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas





Dashboard Grafana - Estatísticas do E-mail

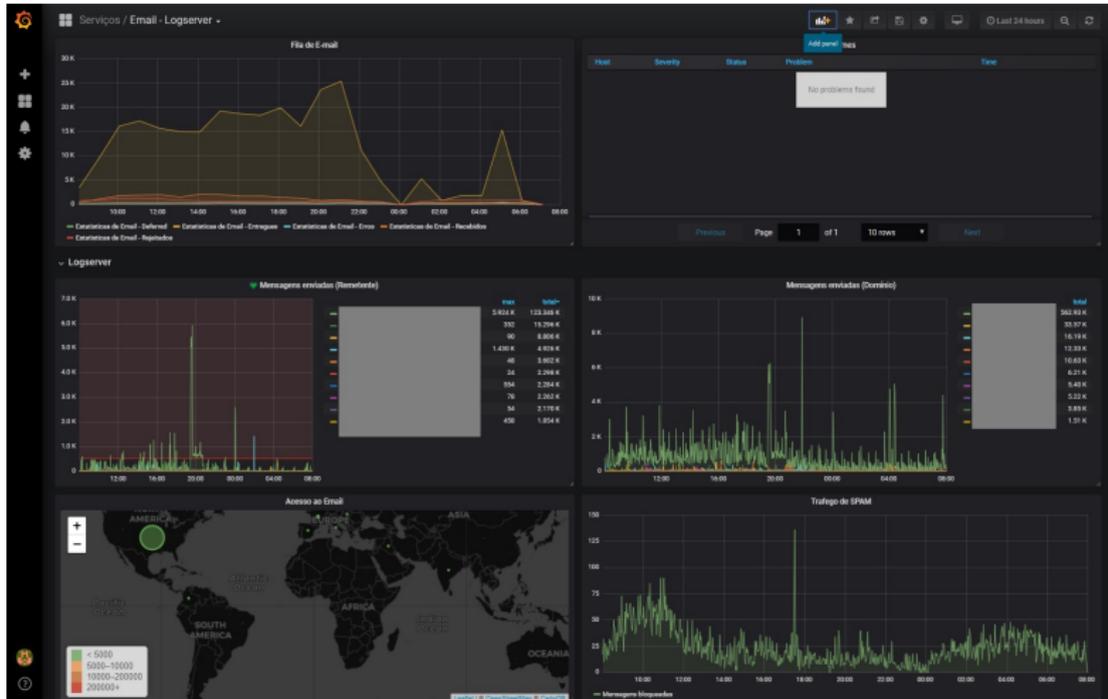
Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso
Qual ferramenta escolher?
Bonus: Uma opção SOHO

Duvidas





Estudo de caso 2 - Stonesoft

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- Monitoramento de Firewall StoneSoft

- Zabbix + Grafana: Centralização e compartilhamento de informações



Estudo de caso 2 - Stonesoft

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

■ Monitoramento de Firewall StoneSoft

■ Zabbix + Grafana: Centralização e compartilhamento de informações

- Identificação de gargalos



Estudo de caso 2 - Stonesoft

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

■ 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 Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

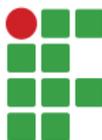
Bonus: Uma opção SOHO

Duvidas

■ 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 Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

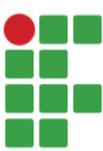
Duvidas

■ 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas





Estudo de caso 3 - HPE IMC

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- NMS licenciado HPE / Aruba



Estudo de caso 3 - HPE IMC

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Estudo de caso 3 - HPE IMC

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Estudo de caso 3 - HPE IMC

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

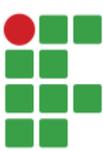
Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

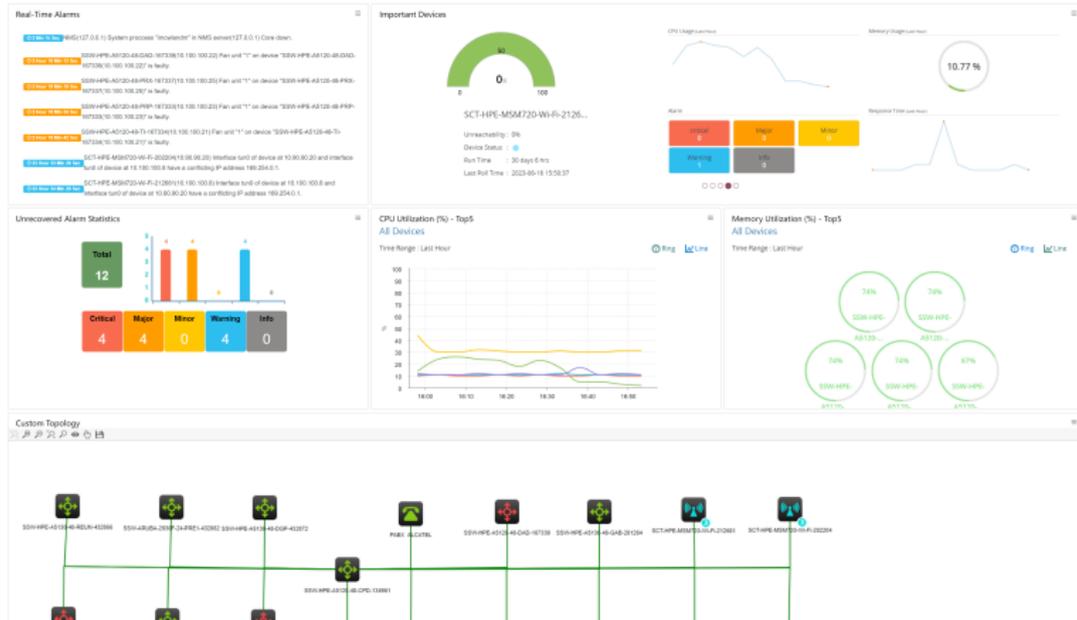
Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas





Dashboard HPE IMC

Monitoramento de Rede

Por quê monitorar?

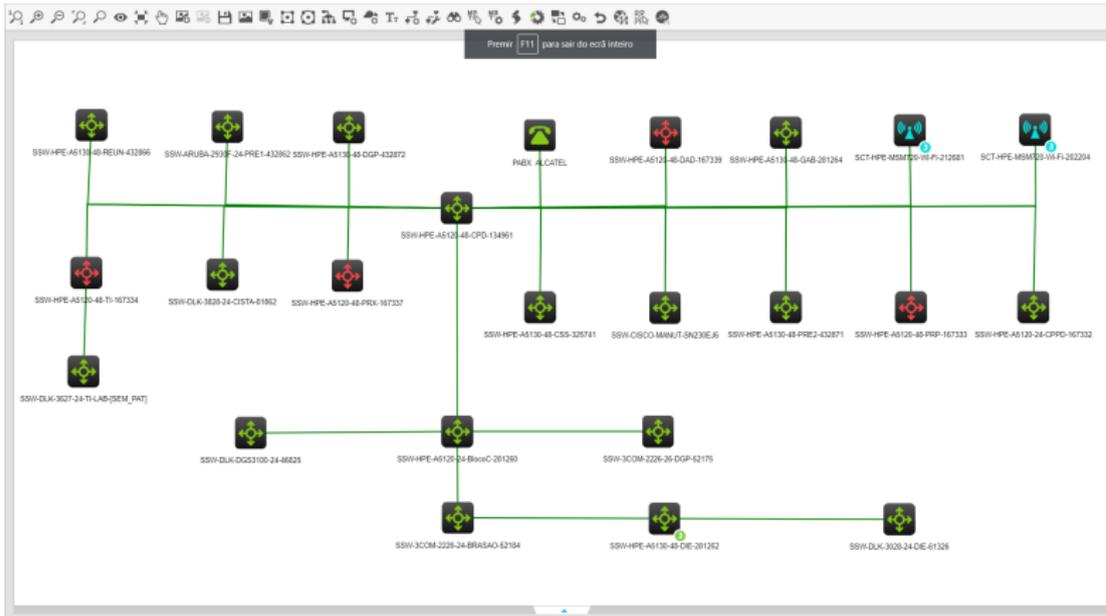
Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas





Qual ferramenta escolher?

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- a) Zabbix
- b) ELK Stack
- c) HPE IMC
- d) Grafana Stack (Prometheus, Loki, Tempo, etc)



Bonus: The Dude - MikroTik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- Ferramenta de monitoramento de rede da MikroTik



Bonus: The Dude - MikroTik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Bonus: The Dude - MikroTik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Bonus: The Dude - MikroTik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

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



Bonus: The Dude - MikroTik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- 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

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

- Adequado para redes menores



Bonus: The Dude - MikroTik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas

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



Bonus: The Dude - Mikrotik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas

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



Bonus: The Dude - Mikrotik

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

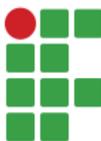
Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas

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



CHR - Configuração

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

admin@10.141.250.30 (MikroTik) - WinBox (64bit) v7.9 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 10.141.250.30

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- WireGuard
- Bridge
- PPP
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System
- Queues
- Files
- Log
- RADIUS
- Tools
- New Terminal
- Dot1X
- Dude
- Make Supout.rtf
- New WinBox
- Exit

RouterOS WinBox



Dude - Topologia

Monitoramento de Rede

Por quê monitorar?

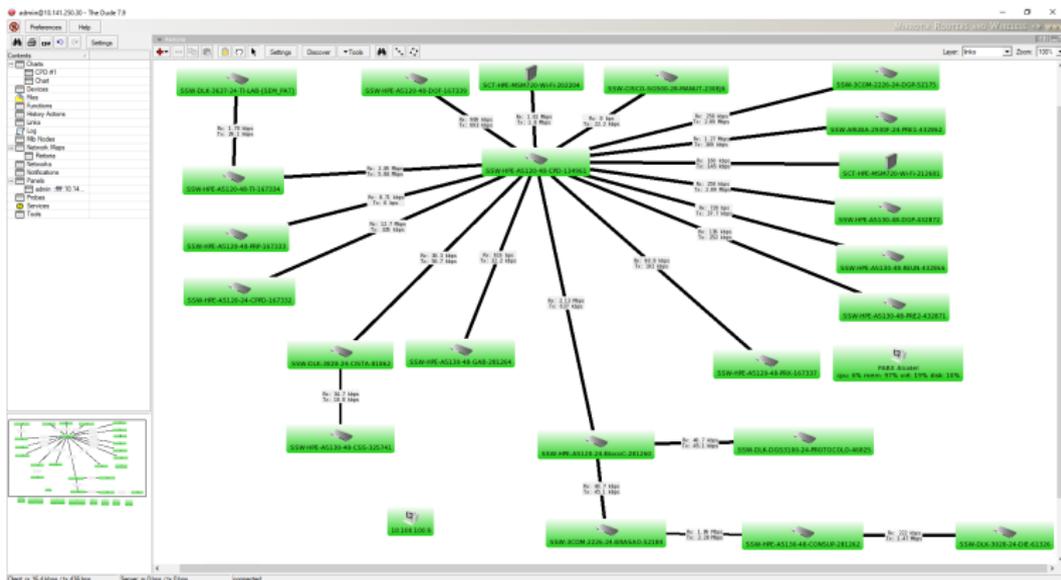
Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas





Dude - SNMP

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas

SSW-HPE-A5120-24-BlocoC-281260 - Device

General Polling Services Outages Snmp History Tools

Interface Ip Route Ap Bridge Fdb Storage Cpu Wireless Station Registration Table Simple Queue Dhcp Lease

Port: GigabitEthernet1/0/23 (23) - 132

MAC	Port	Status
HUAWEITECH:3B:E5:03	GigabitEther...	learned
Dellinc.:E6:CE:FA	GigabitEther...	learned
Dellinc.:FD:72:2A	GigabitEther...	learned
GIGA-BYTET:F3:C8:88	GigabitEther...	learned
GIGA-BYTET:F3:DE:E7	GigabitEther...	learned
GIGA-BYTET:F3:DF:9F	GigabitEther...	learned
GIGA-BYTET:F3:E5:85	GigabitEther...	learned
98:F6:21:F7:45:81	GigabitEther...	learned
9A:72:CC:67:53:86	GigabitEther...	learned
9E:88:83:27:09:9F	GigabitEther...	learned
HewlettPac:55:6E:96	GigabitEther...	learned
HewlettPac:55:6E:9D	GigabitEther...	learned
HewlettPac:55:6E:C1	GigabitEther...	learned
HewlettPac:55:6E:C2	GigabitEther...	learned
HewlettPac:55:6E:C6	GigabitEther...	learned
HewlettPac:55:6E:60	GigabitEther...	learned
HewlettPac:2A:89:0F	GigabitEther...	learned
HewlettPac:2A:99:53	GigabitEther...	learned
HewlettPac:2A:6A:55	GigabitEther...	learned
A8:96:75:72:36:D4	GigabitEther...	learned
AE:66:E4:CA:A4:20	GigabitEther...	learned

Ok
Cancel
Apply
Notes
Remove
Tools
Reprobe
Ack
Unack
Reboot
Reconnect



Perguntas?

Monitoramento de Rede

Por quê monitorar?

Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Duvidas





Para saber mais...

Monitoramento de Rede

Por quê monitorar?

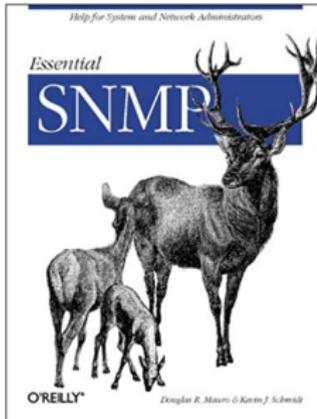
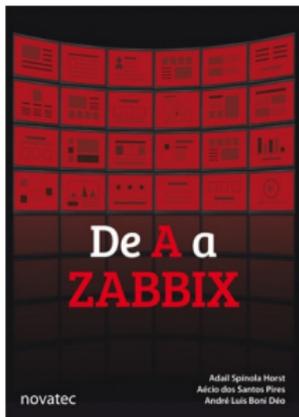
Exemplo de sistemas em uso na DTI

Estudo de caso

Qual ferramenta escolher?

Bonus: Uma opção SOHO

Dúvidas



<https://wiki.mikrotik.com/wiki/>

