

openNetAudit

Guilherme Ladvocat

RNP

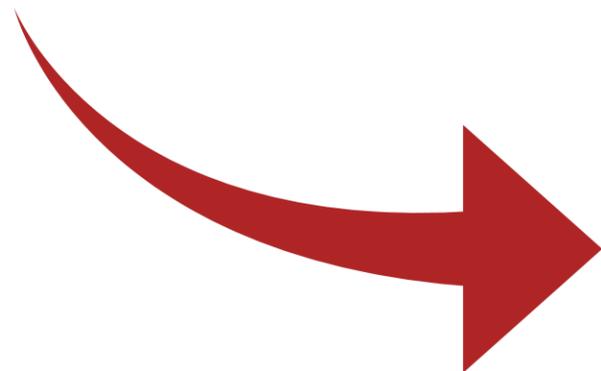
02/12/2021

Cenário

- Diversos fabricantes;
- Quantidade de equipamentos a serem gerenciados;
- Modelos sem suporte a tecnologias de automação mais modernas (Netconf, Restconf, YANG);
- Configurações default deficientes em segurança.

Cenário

- Diversos fabricantes;
- Quantidade de equipamentos a serem gerenciados;
- Modelos sem suporte a tecnologias de automação mais modernas (Netconf, Restconf, YANG);
- Configurações default deficientes em segurança.



DevOps

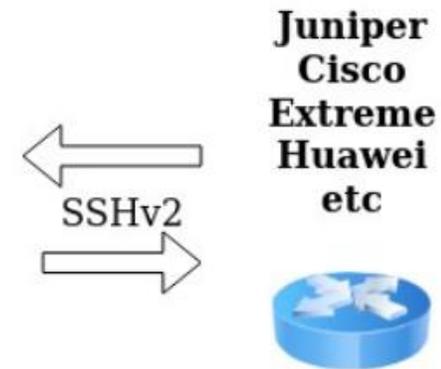
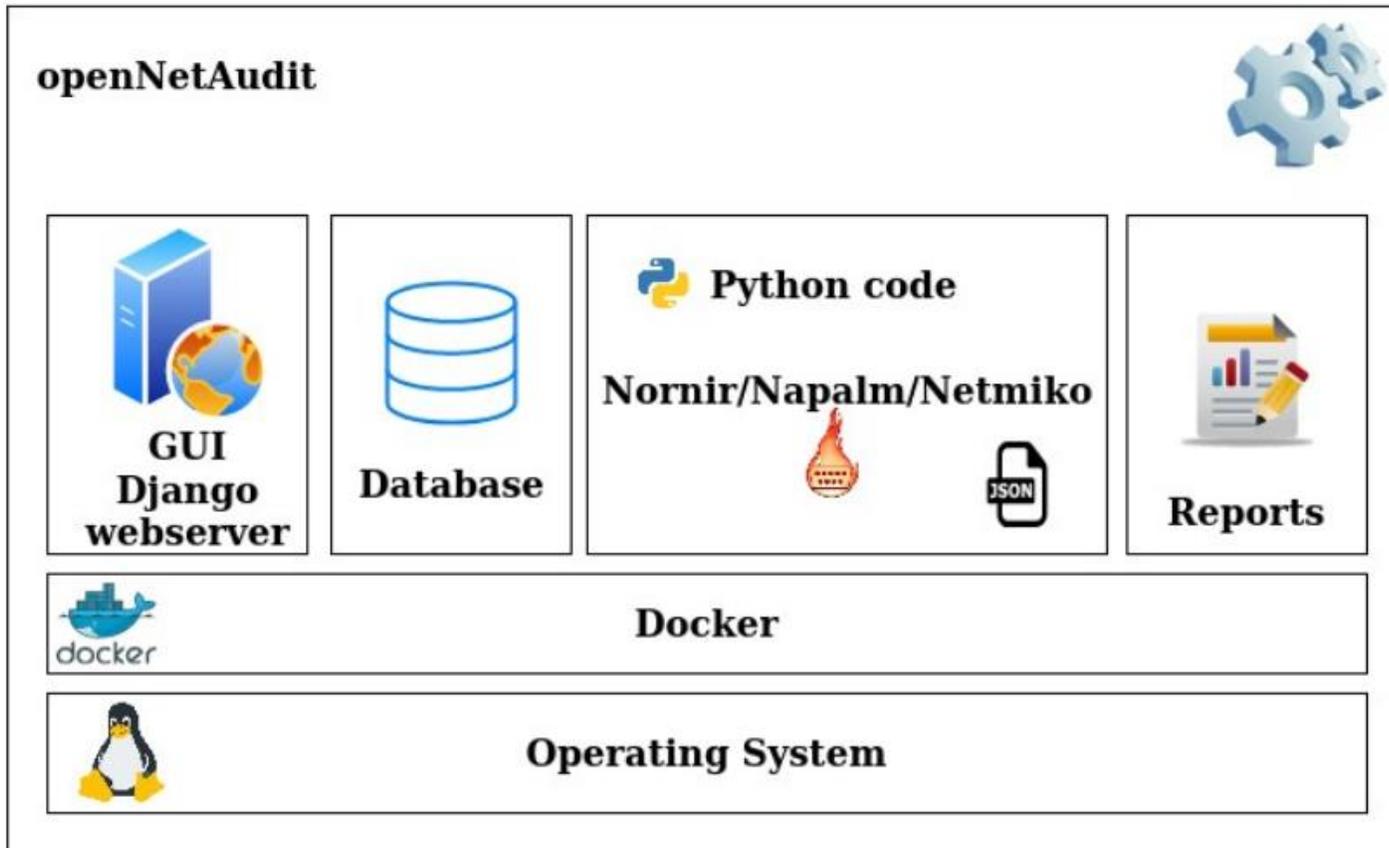
Objetivos

- Automatizar checagens de forma escalável e flexível
- Suportar múltiplos fabricantes
- Gerar relatórios de acompanhamento
- Padronizar configurações mínimas
- Melhorar a segurança da rede com a aplicação de boas práticas de configuração.

Histórico

- 2019: Produto mínimo viável;
 - 2020: Submissão de um roadmap evolutivo ao programa Frida do Lacnic;
 - 2021: Conclusão do ciclo de desenvolvimento e lançamento da v1.0.
-
- Desenvolvido pela Gerência de Operações da RNP e apoiado pela Gerência de Sistemas, CAIS e PoPs
 - Desenvolvedores:
 - Guilherme Ladvocat
 - Thiago Siqueira

Arquitetura



openNetAudit - MVP

- Suporte aos fabricantes Juniper e Extreme;
- Checagens baseadas no Guia de Configuração Segura;
- Interface web mínima;
- Base de dados simples;
- Relatórios simples, apenas armazenando logs e arquivos csv.

openNetAudit - MVP



[Página Inicial](#) [Devices PoP](#) [Executar auditoria](#) [Relatórios](#) [Logout](#)

Olá **admin!**

Base de devices e versões recomendadas

Cadastre ou veja a lista de **devices** cadastrados.

[Cadastrar Device](#)

[Vá para Lista](#)

Cadastro devices dos PoPs

Página para cadastro de devices dos **PoPs**

[Cadastro devices PoPs](#)

Executar auditoria

Executa auditoria

[Executar auditoria](#)



MINISTÉRIO DO
TURISMO

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA,
INOVAÇÕES E COMUNICAÇÕES





Selecione o PoP para cadastro de device

PoP

AC ▾

[Cadastro](#) [Upload csv](#)

Lista de devices dos PoPs

PoP

AC ▾

[Listar](#)

Selecione o PoP para commit de configuração

PoP

AC ▾

[Commit](#)



PoP

AC ▾

Selecione o tipo de device

Device list [CPE Juniper ▾](#)

Username:

Password:

[Executar](#)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
	host	vendor	model	os_version	rec_os_version	os_is_equal_to_rec	loopback_fw_ipv4	fw_ipv4_last_term_discard	loopback_fw_ipv6	fw_ipv6_last_term_discard	rpf_check_enabled	telnet_enabled	ssh2_enabled	web_admin_enabled	root_login_enabled	route_passive	
1	host	Juniper	J2320	12.1X44-D45.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
2	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
3	host	Juniper	SRX240H2	12.3X48-D30.7	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False	
4	host	Juniper	SRX240H2	12.3X48-D85.1	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False	
5	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
6	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False	
7	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False	
8	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False	
9	host	Juniper	SRX240H2	12.3X48-D30.7	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False	
10	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False	
11	host	Juniper	SRX240H2	12.3X48-D85.1	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False	
12	host	Juniper	J2350	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
13	host	Juniper	SRX240H2	12.1X46-D40.2	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False	
14	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
15	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
16	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
17	host	Juniper	SRX240H2	12.3X48-D85.1	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False	
18	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False	
19	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
20	host	Juniper	J2350	10.2R4.10	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
21	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
22	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False	
23	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False	
24	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
25	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
26	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
27	host	Juniper	J2350	10.2R4.8	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
28	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False	
29	host	Juniper	SRX340	15.1X49-D150.2	18.4R3-S2	False	True	True	True	True	False	False	True	False	False	False	
30	host	Juniper	SRX220H	12.1X46-D67	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False	
31	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
32	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False	
33	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False	
34	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False	
35	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	False	True	False	False	False	True	False	False	False	
36	host	Juniper	J2350	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
37	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False	
38	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False	
39	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False	
40																	
41	Legenda:																
42	os_is_equal_to_rec = True																
43	loopback_fw_ipv4 = True																
44	fw_ipv4_last_term_discard = True																
45	loopback_fw_ipv6 = True																
46	loopback_fw_ipv6_last_term_discard = True																
47	rpf_check_enabled = True																
48	telnet_enabled = False																
49	web_admin_enabled = False																
50																	

Roadmap – Principais evoluções

- Reformulação total do sistema;
- Organização hierárquica (Device/Site/Group);
- Módulo de auditoria reescrito:
 - Possibilita o cadastro de checagens customizadas;
 - Classificação de severidade dos testes;
 - Concatenação de regras.
- Adição de suporte a novos fabricantes (Cisco, Huawei, Mikrotik);
- Armazenamento de resultados em JSON;
- Relatórios mais amigáveis;
- Tracking de vulnerabilidades.

Demonstração



Site Info

Number of Hosts: 26

Hosts Without Issues: 1

Hosts With Issues: 25

Number of Issues: 136

Top 5

Hosts with more issues

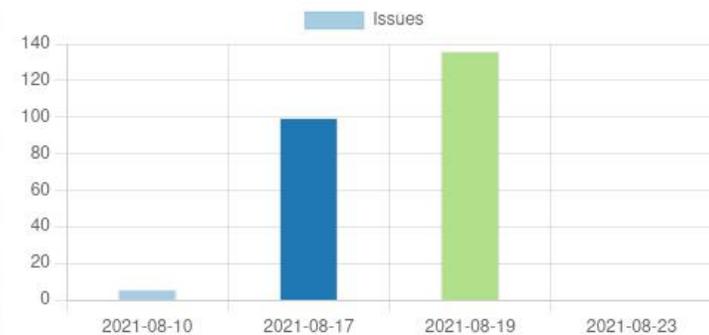
1. IFS-Laranjeiras	12
2. IFS-Ribellana	11
3. IFS-Lagarto	11
4. IFS-Poco_Redonda	11
5. IFS-Propria	11

Docs

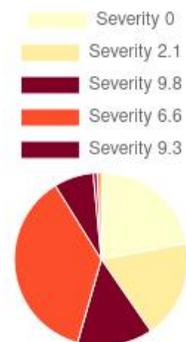
Documentation for OpenNetAudit, along with tutorials and guides, are available online.

[Documentation](#)

Issues History



Issues



Device List

List of devices from site: LAB

Select All <input type="checkbox"/>	Id	Name	Description	Type	IP : ssh_port		
<input type="checkbox"/>	1	Huawei-Secure	Secure	huawei	10.1.0.80:22	Edit	Delete
<input type="checkbox"/>	2	Huawei-Insecure	Insecure	huawei	10.1.0.85:22	Edit	Delete
<input type="checkbox"/>	3	Juniper-vsrx	VSRX	juniper	10.1.0.107:22	Edit	Delete
<input type="checkbox"/>	4	Cisco	V1000	cisco_ios	10.1.0.250:22	Edit	Delete
<input type="checkbox"/>	5	Mikrotik-Secure	Secure	mikrotik	10.1.0.150:2222	Edit	Delete
<input type="checkbox"/>	6	Mikrotik-Insecure	Insecure	mikrotik	10.1.0.155:22	Edit	Delete
<input type="checkbox"/>	7	Extreme-Secure	Secure	extreme	10.1.0.100:22	Edit	Delete
<input type="checkbox"/>	8	Extreme-Insecure	Insecure	extreme	10.1.0.90:22	Edit	Delete

Delete all Selected

Device Report

Info

Device: Cisco

IP: 10.1.0.250

Manufacturer: Cisco_ios

Last Audit: May 4, 2021

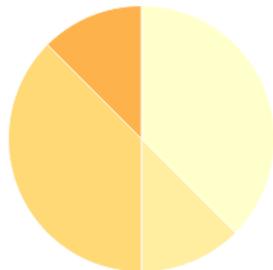
Status: Successful

Issues: 8

Recommended OS: True

Issues

Severity 1 Severity 3
Severity 4 Severity 5



Last Audit

Test	Description	Severity	Value
logging	OK	undefined	Logging service is enabled.
service.pad	OK	undefined	Service pad is disabled.
source_route	OK	undefined	IP Source Route service is disabled.
snmp_default_communities	NOK	5	SNMP default communities are present. Please delete them.
password_encryption	OK	undefined	Service password encryption disabled.
gratuitous_arp	NOK	3	Gratuitous ARP service is enabled
cdp	OK	undefined	CDP is disabled
http	OK	undefined	Web management is disabled
enable_secret	OK	undefined	Enable secret is applied. OK!
finger	NOK	4	IP Finger is enabled. Please disable it.
dhcp	NOK	1	DHCP service is enabled.
urpf	NOK	4	uRPF is disabled. Apply uRPF to the LAN interface.
telnet	OK	undefined	Telnet is disabled.
bootp	NOK	1	Bootp service is enabled.
ssh_parameters	NOK	4	SSH parameters like timeout and retries are not configured.

Audit Result

Number of hosts	Hosts with issues	Hosts without issues	Number of issues
1	1	0	8

Site	Host	Host Name	Ip	Model	OS	Os Recommended	SN	Status	Timestamp	Manufacturer
LAB	Cisco	Cisco-Lab	10.1.0.250	CSR1000V	16.6.5	True	91YV0PLMQW6	Successful	2021-05-04 13:58:05.281095	Cisco

Host	Test	Value	Severity	Description	Solution
Cisco	logging	OK	undefined	Logging service is enabled.	
Cisco	service.pad	OK	undefined	Service pad is disabled.	
Cisco	source_route	OK	undefined	IP Source Route service is disabled.	
Cisco	snmp_default_communities	NOK	5	SNMP default communities are present. Please delete them.	no snmp-server community private no snmp-server community public
Cisco	password_encryption	OK	undefined	Service password encryption disabled.	
Cisco	gratuitous_arp	NOK	3	Gratuitous ARP service is enabled	no ip gratuitous-arps
Cisco	cdp	OK	undefined	CDP is disabled	
Cisco	http	OK	undefined	Web management is disabled	
Cisco	enable_secret	OK	undefined	Enable secret is applied. OK!	
Cisco	finger	NOK	4	IP Finger is enabled. Please disable it.	no ip finger

[Gitlab => https://git.rnp.br/guilherme.ladvocat/opennetaudit](https://git.rnp.br/guilherme.ladvocat/opennetaudit)

[Docs => https://netaudit.rnp.br](https://netaudit.rnp.br)

[E-mail => guilherme.ladvocat@rnp.br](mailto:guilherme.ladvocat@rnp.br)

Obrigado!