PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

V16 Funkčný PoC

KPB5 – Realizácia riešenia

typ – dokumentácia

mesiac odovzdania – M22

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1. **ELK Stack** 3
2. **Shuffle** 3
3. **Wazuh** 3
4. **Greenbone Community edition** 7
5. **OpenCTI** 9
6. **MISP** 9
7. **GLPI** 10
8. **NetBox** 12
9. **DFIR IRIS – oblasť: Ticketing** 12
10. **DFIR IRIS – oblasť: Evidencia, správa incidentov** ..... Chyba! Záložka nie je definovaná.
11. **Kibana (ELK)** 12
12. **Wiki.js** 13

BRAIN:IT

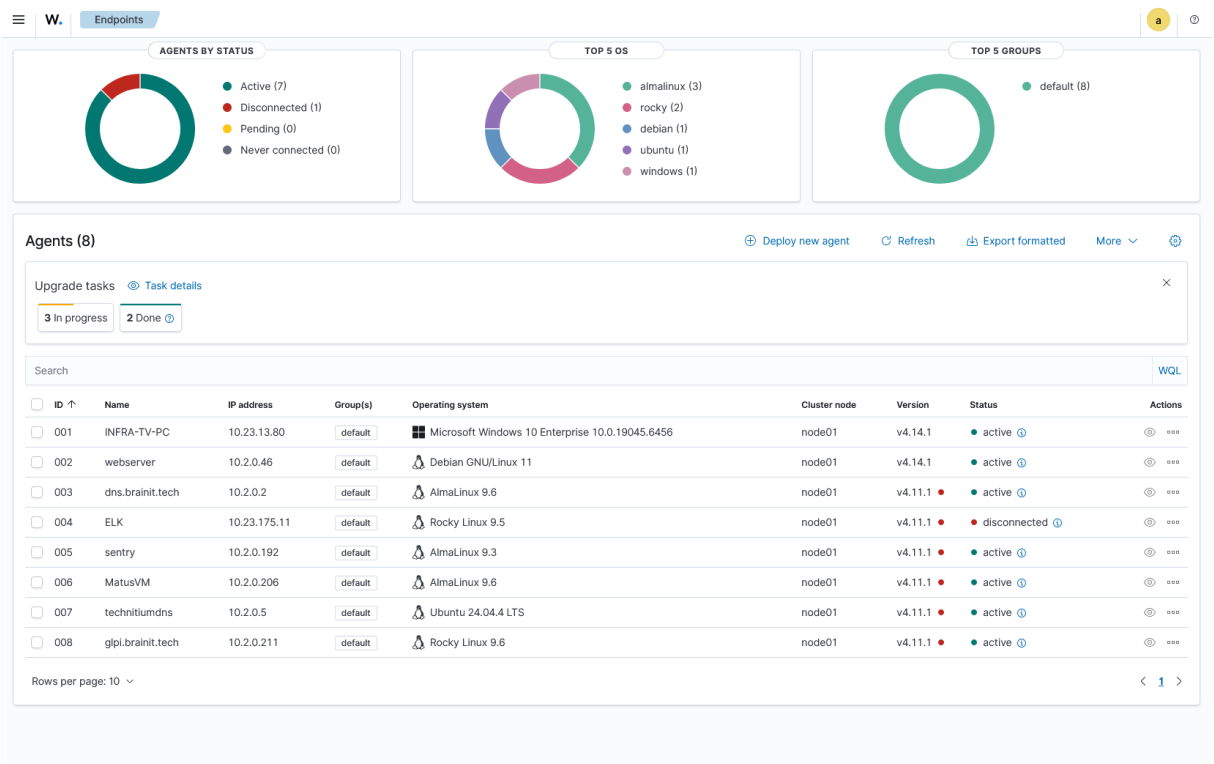
FRI

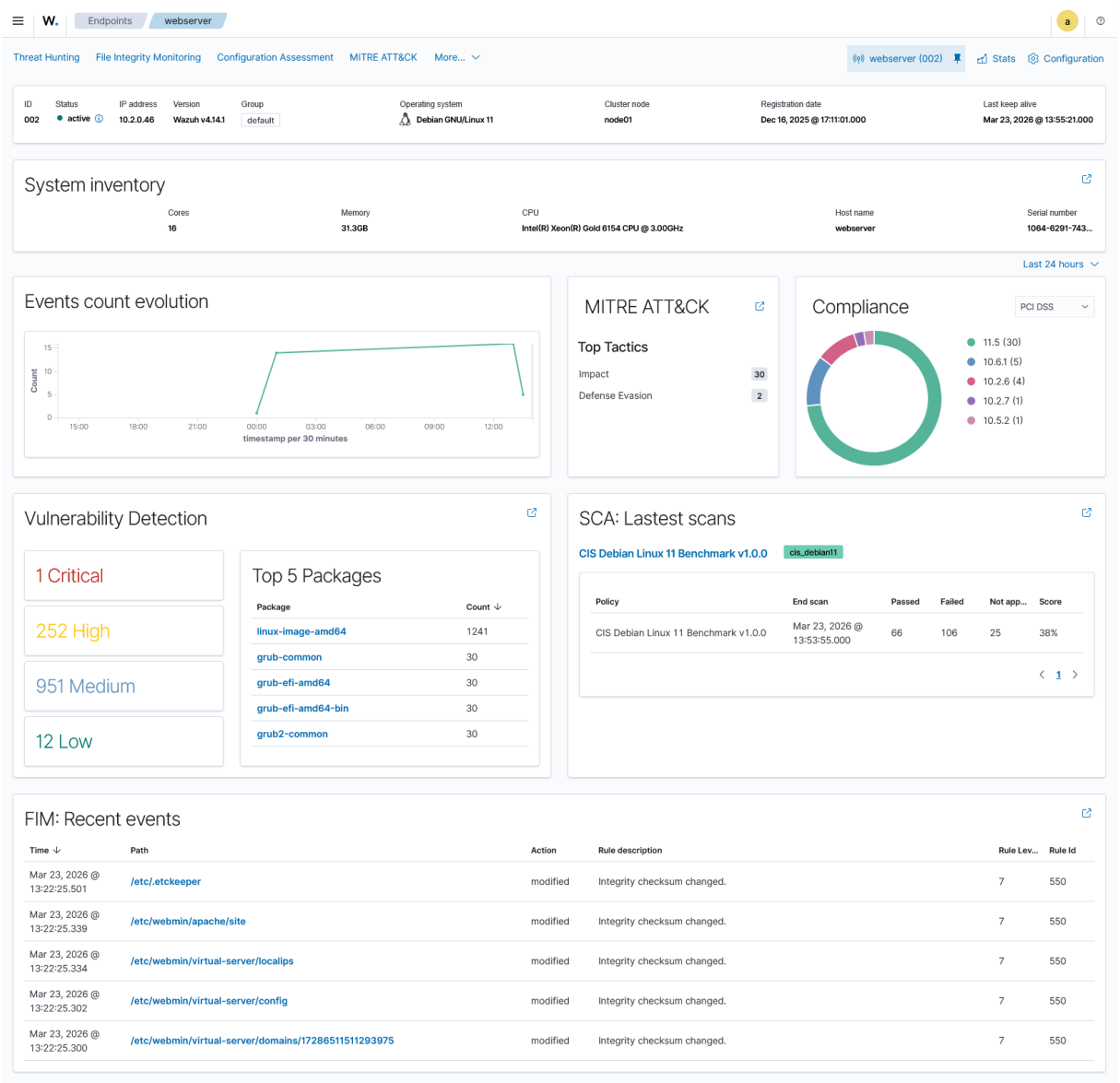
1. ELK STACK

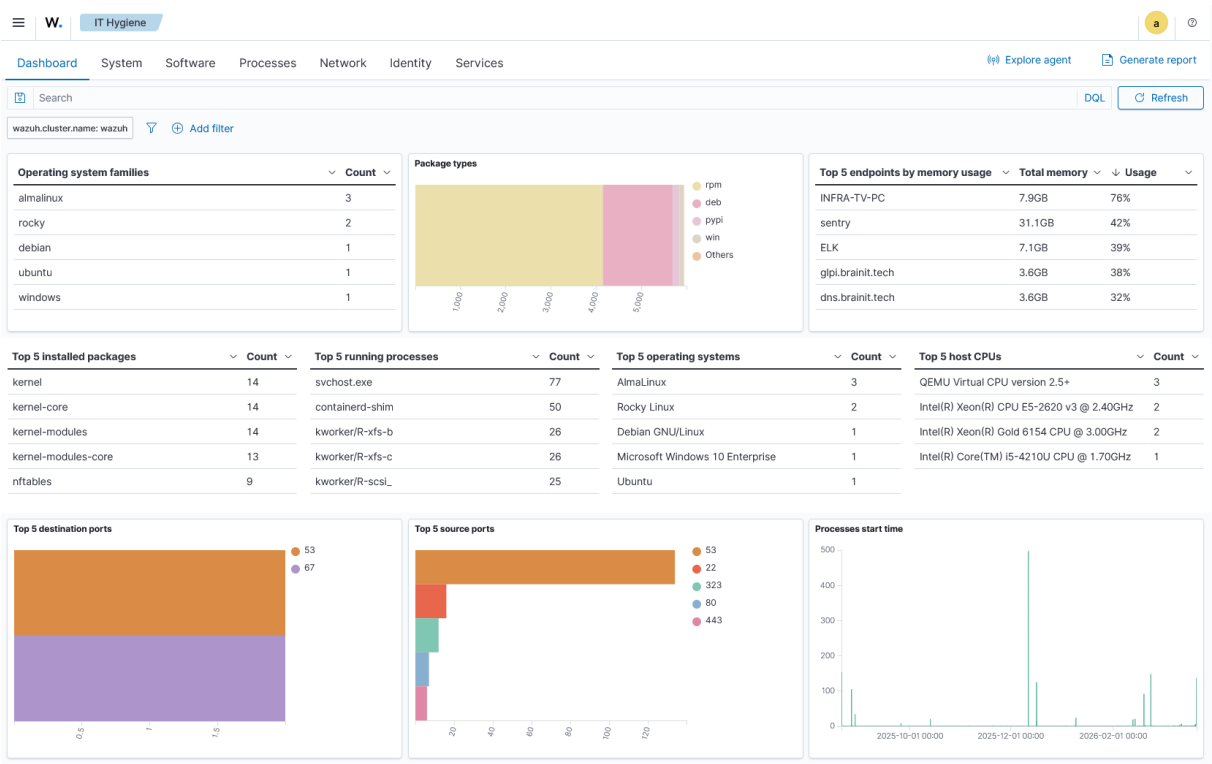
test

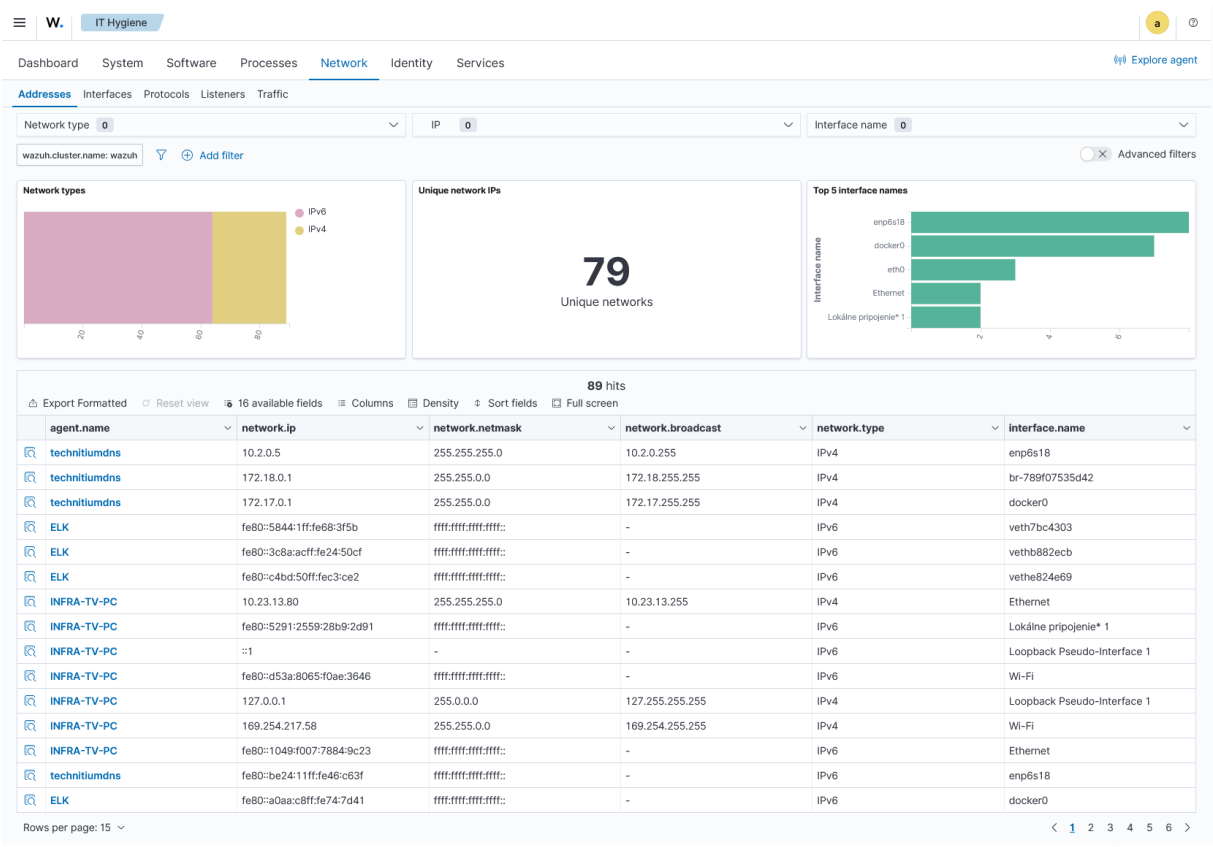
2. SHUFFLE

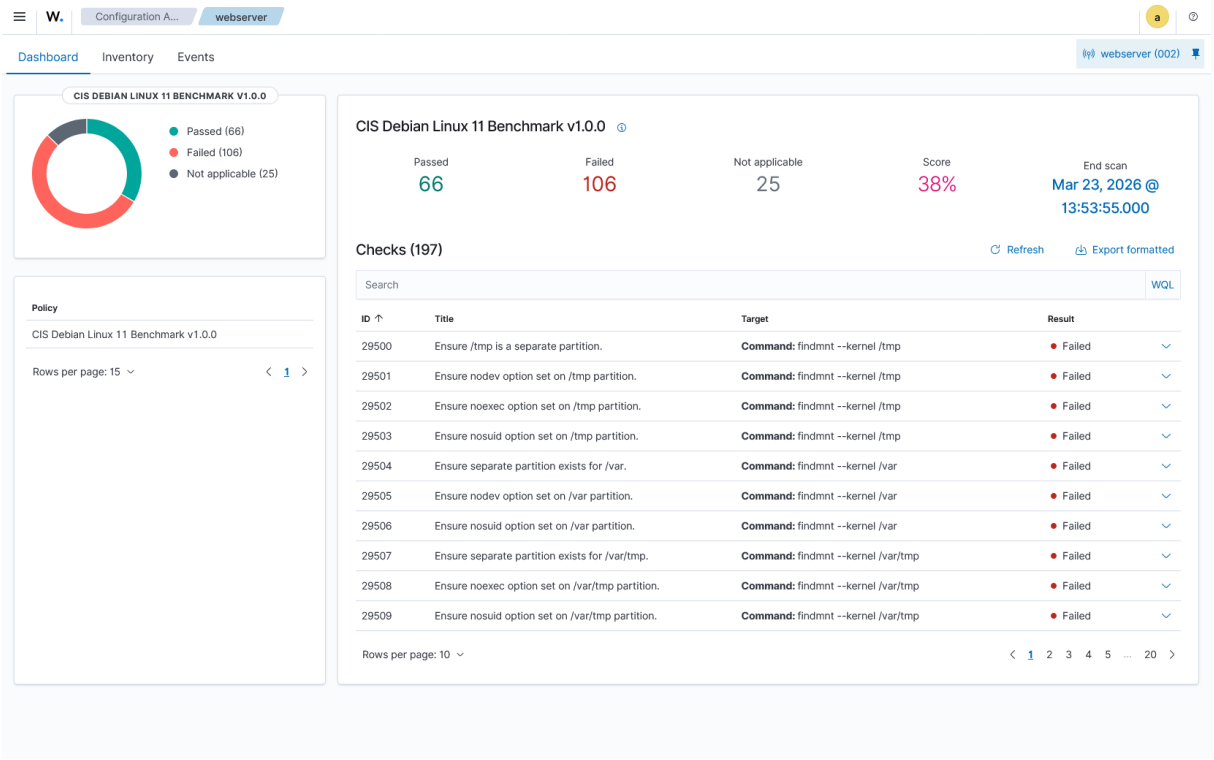
3. WAZUH



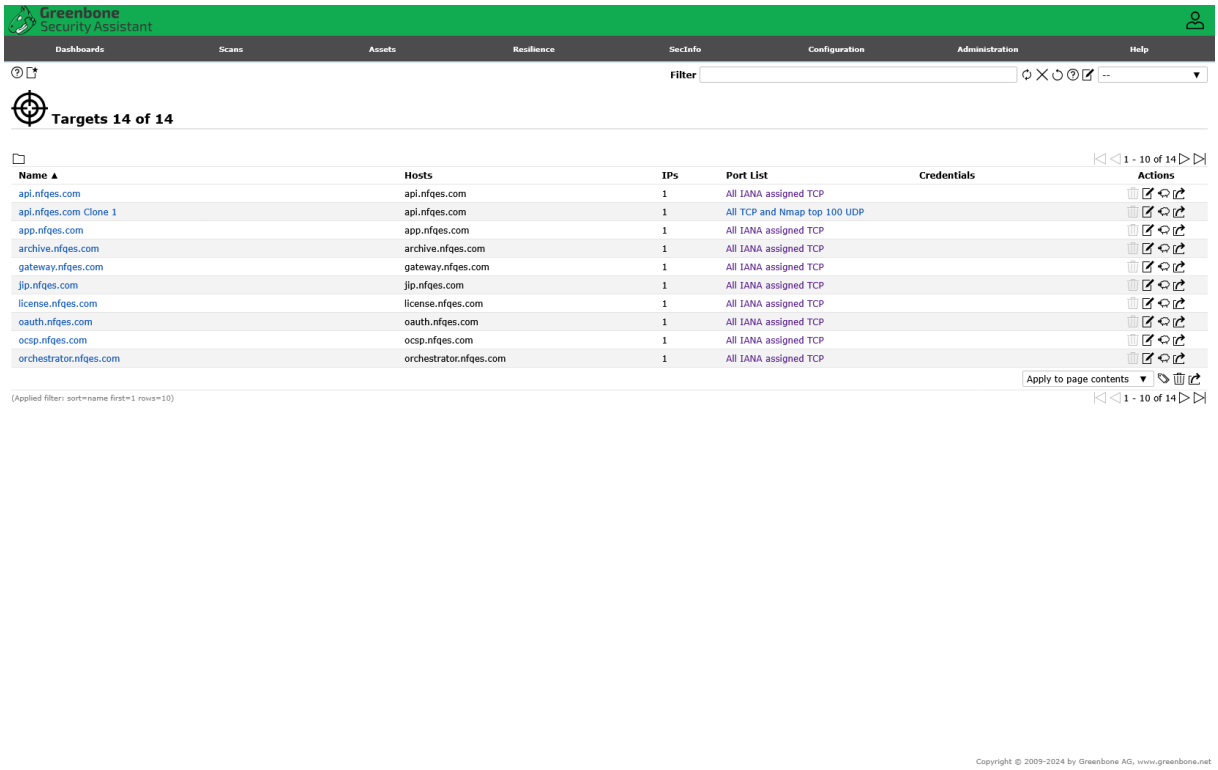

W.
Endpoints
webserver
Threat Hunting
File Integrity Monitoring
Configuration Assessment
MITRE ATT&CK
More...
webserver (002)
Stats
Configuration
ID 002
Status active
IP address 10.2.0.46
Version Wazuh v4.14.1
Group default
Operating system Debian GNU/Linux 11
Cluster node node01
Registration date Dec 16, 2025 @ 17:11:01.000
Last keep alive Mar 23, 2026 @ 13:55:21.000
System inventory
Cores 16
Memory 31.3GB
CPU Intel(R) Xeon(R) Gold 6154 CPU @ 3.00GHz
Host name webserver
Serial number 1064-6291-743...
Last 24 hours
Events count evolution
Count
timestamp per 30 minutes
MITRE ATT&CK
Top Tactics
Impact 30
Defense Evasion 2
Compliance
PCI DSS
11.5 (30)
10.6.1 (5)
10.2.6 (4)
10.2.7 (1)
10.5.2 (1)
Vulnerability Detection
1 Critical
252 High
951 Medium
12 Low
Top 5 Packages
Package
Count
linux-image-amd64 1241
grub-common 30
grub-efi-amd64 30
grub-efi-amd64-bin 30
grub2-common 30
SCA: Lastest scans
CIS Debian Linux 11 Benchmark v1.0.0
cis_debian11
Policy
End scan
Passed
Failed
Not app...
Score
CIS Debian Linux 11 Benchmark v1.0.0
Mar 23, 2026 @ 13:53:55.000
66
106
25
38%
FIM: Recent events
Time
Path
Action
Rule description
Rule Lev...
Rule Id
Mar 23, 2026 @ 13:22:25.501 /etc/.etckeeper modified Integrity checksum changed. 7 550
Mar 23, 2026 @ 13:22:25.339 /etc/webmin/apache/site modified Integrity checksum changed. 7 550
Mar 23, 2026 @ 13:22:25.334 /etc/webmin/virtual-server/localips modified Integrity checksum changed. 7 550
Mar 23, 2026 @ 13:22:25.302 /etc/webmin/virtual-server/config modified Integrity checksum changed. 7 550
Mar 23, 2026 @ 13:22:25.300 /etc/webmin/virtual-server/domains/17286511511293975 modified Integrity checksum changed. 7 550

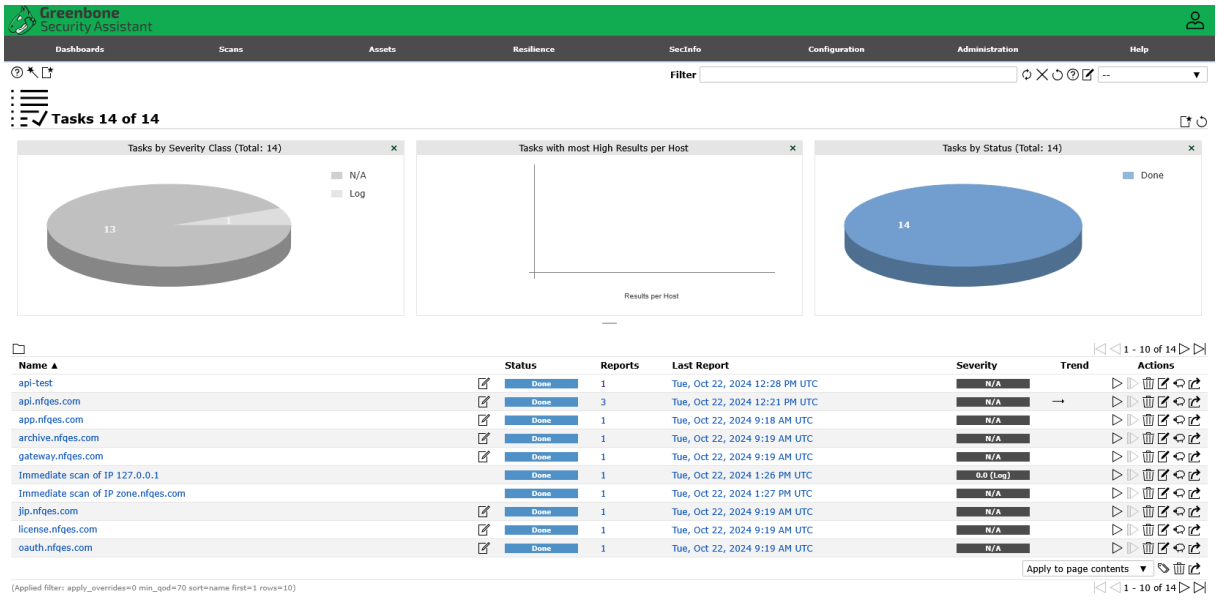

W.
IT Hygiene
a
Dashboard
System
Software
Processes
Network
Identity
Services
Explore agent
Generate report
Search
DQL
Refresh
wazuh.cluster.name: wazuh
Add filter
Operating system families
Count
almalinux 3
rocky 2
debian 1
ubuntu 1
windows 1
Package types
rpm
deb
pypi
win
Others
1,000
2,000
3,000
4,000
5,000
Top 5 endpoints by memory usage
Total memory
Usage
INFRA-TV-PC 7.9GB 76%
sentry 31.1GB 42%
ELK 7.1GB 39%
glpi.brainit.tech 3.6GB 38%
dns.brainit.tech 3.6GB 32%
Top 5 installed packages
Count
kernel 14
kernel-core 14
kernel-modules 14
kernel-modules-core 13
nftables 9
Top 5 running processes
Count
svchost.exe 77
containerd-shim 50
kworker/R-xfs-b 26
kworker/R-xfs-c 26
kworker/R-scsi_ 25
Top 5 operating systems
Count
AlmaLinux 3
Rocky Linux 2
Debian GNU/Linux 1
Microsoft Windows 10 Enterprise 1
Ubuntu 1
Top 5 host CPUs
Count
QEMU Virtual CPU version 2.5+ 3
Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz 2
Intel(R) Xeon(R) Gold 6154 CPU @ 3.00GHz 2
Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 1
Top 5 destination ports
53
67
0.5
1
1.5
Top 5 source ports
53
22
323
80
443
20
40
60
80
100
120
Processes start time
500
400
300
200
100
0
2025-10-01 00:00
2025-12-01 00:00
2026-02-01 00:00

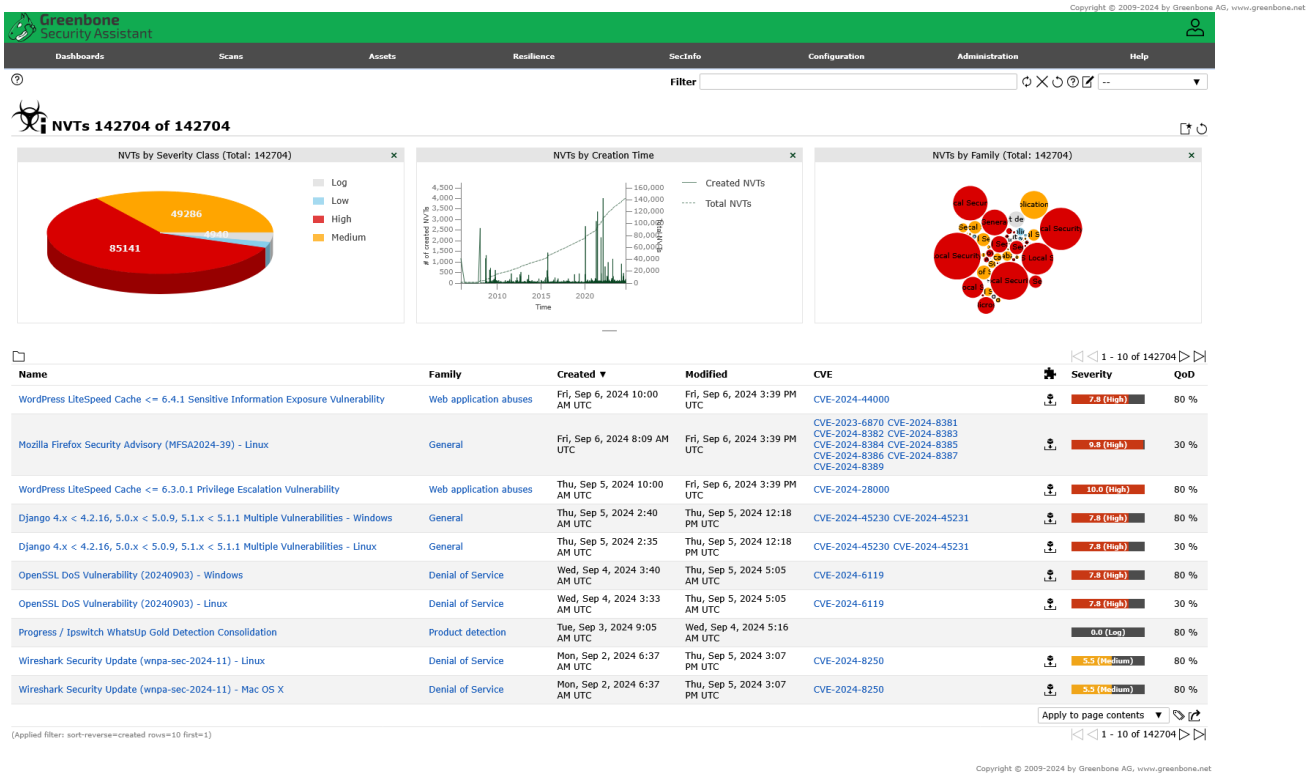

IT Hygiene
Dashboard
System
Software
Processes
Network
Identity
Services
Explore agent
Addresses
Interfaces
Protocols
Listeners
Traffic
Network type
IP
Interface name
wazuh.cluster.name: wazuh
Add filter
Advanced filters
Network types
IPv6
IPv4
Unique network IPs
79
Unique networks
Top 5 interface names
enp6s18
docker0
eth0
Ethernet
Lokálne pripojenie* 1
Interface name
89 hits
Export Formatted
Reset view
16 available fields
Columns
Density
Sort fields
Full screen
agent.name
network.ip
network.netmask
network.broadcast
network.type
interface.name
technitiumdns 10.2.0.5 255.255.255.0 10.2.0.255 IPv4 enp6s18
technitiumdns 172.18.0.1 255.255.0.0 172.18.255.255 IPv4 br-789f07535d42
technitiumdns 172.17.0.1 255.255.0.0 172.17.255.255 IPv4 docker0
ELK fe80::5844:1ff:fe68:3f5b ffff:ffff:ffff:ffff:: - IPv6 veth7bc4303
ELK fe80::3c8a:acff:fe24:50cf ffff:ffff:ffff:ffff:: - IPv6 vethb882ecb
ELK fe80::c4bd:50ff:fec3:ce2 ffff:ffff:ffff:ffff:: - IPv6 vethe824e69
INFRA-TV-PC 10.23.13.80 255.255.255.0 10.23.13.255 IPv4 Ethernet
INFRA-TV-PC fe80::5291:2559:28b9:2d91 ffff:ffff:ffff:ffff:: - IPv6 Lokálne pripojenie* 1
INFRA-TV-PC ::1 - - IPv6 Loopback Pseudo-Interface 1
INFRA-TV-PC fe80::d53a:8065:f0ae:3646 ffff:ffff:ffff:ffff:: - IPv6 Wi-Fi
INFRA-TV-PC 127.0.0.1 255.0.0.0 127.255.255.255 IPv4 Loopback Pseudo-Interface 1
INFRA-TV-PC 169.254.217.58 255.255.0.0 169.254.255.255 IPv4 Wi-Fi
INFRA-TV-PC fe80::1049:f007:7884:9c23 ffff:ffff:ffff:ffff:: - IPv6 Ethernet
technitiumdns fe80::be24:11ff:fe46:c63f ffff:ffff:ffff:ffff:: - IPv6 enp6s18
ELK fe80::a0aa:c8ff:fe74:7d41 ffff:ffff:ffff:ffff:: - IPv6 docker0
Rows per page: 15

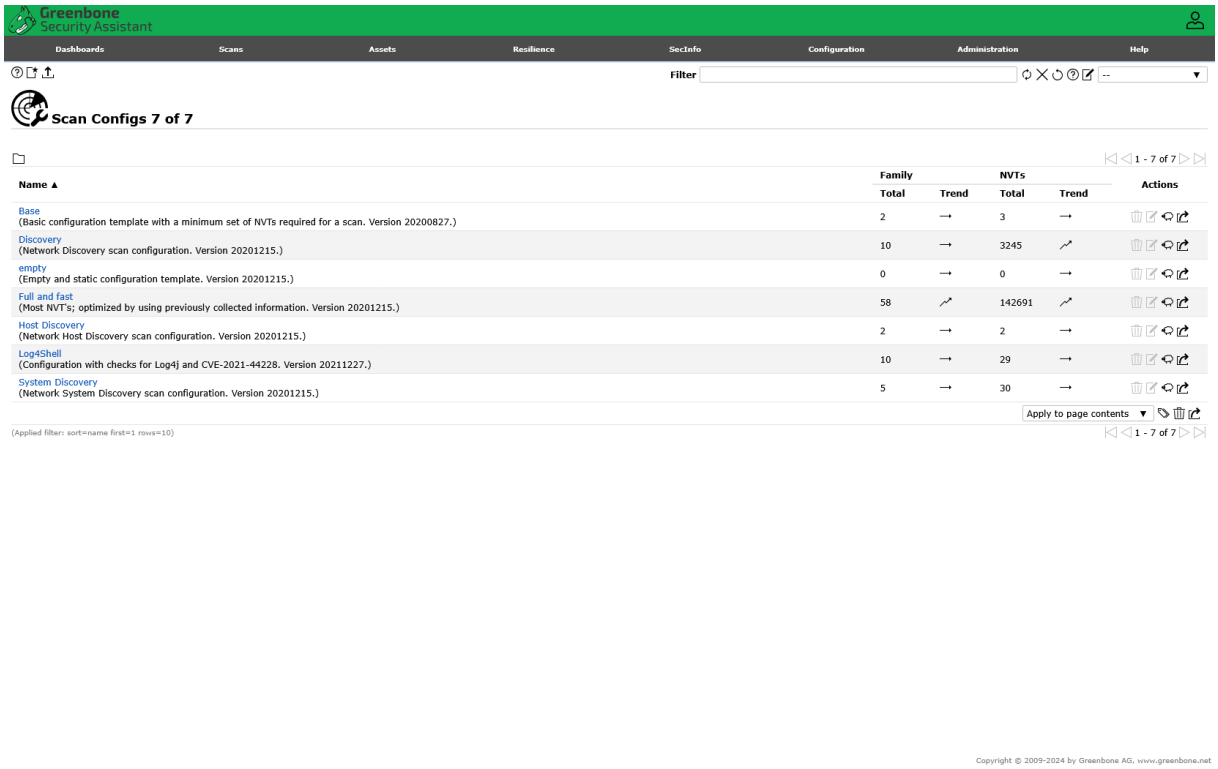

Configuration A...
webserver
Dashboard
Inventory
Events
webserver (002)
CIS DEBIAN LINUX 11 BENCHMARK V1.0.0
Passed (66)
Failed (106)
Not applicable (25)
CIS Debian Linux 11 Benchmark v1.0.0
Passed
66
Failed
106
Not applicable
25
Score
38%
End scan
Mar 23, 2026 @ 13:53:55.000
Checks (197)
Refresh
Export formatted
Search
WQL
Policy
CIS Debian Linux 11 Benchmark v1.0.0
ID
Title
Target
Result
29500 Ensure /tmp is a separate partition. Command: findmnt --kernel /tmp Failed
29501 Ensure nodev option set on /tmp partition. Command: findmnt --kernel /tmp Failed
29502 Ensure noexec option set on /tmp partition. Command: findmnt --kernel /tmp Failed
29503 Ensure nosuid option set on /tmp partition. Command: findmnt --kernel /tmp Failed
29504 Ensure separate partition exists for /var. Command: findmnt --kernel /var Failed
29505 Ensure nodev option set on /var partition. Command: findmnt --kernel /var Failed
29506 Ensure nosuid option set on /var partition. Command: findmnt --kernel /var Failed
29507 Ensure separate partition exists for /var/tmp. Command: findmnt --kernel /var/tmp Failed
29508 Ensure noexec option set on /var/tmp partition. Command: findmnt --kernel /var/tmp Failed
29509 Ensure nosuid option set on /var/tmp partition. Command: findmnt --kernel /var/tmp Failed
Rows per page: 10

4. GREENBONE COMMUNITY EDITION




Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tasks 14 of 14
Tasks by Severity Class (Total: 14)
N/A
Log
13
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 14)
Done
14
1 - 10 of 14
Name ▲
Status
Reports
Last Report
Severity
Trend
Actions
api-test
Done
1
Tue, Oct 22, 2024 12:28 PM UTC
N/A
api.nfqes.com
Done
3
Tue, Oct 22, 2024 12:21 PM UTC
N/A
app.nfqes.com
Done
1
Tue, Oct 22, 2024 9:18 AM UTC
N/A
archive.nfqes.com
Done
1
Tue, Oct 22, 2024 9:19 AM UTC
N/A
gateway.nfqes.com
Done
1
Tue, Oct 22, 2024 9:19 AM UTC
N/A
Immediate scan of IP 127.0.0.1
Done
1
Tue, Oct 22, 2024 1:26 PM UTC
0.0 (Log)
Immediate scan of IP zone.nfqes.com
Done
1
Tue, Oct 22, 2024 1:27 PM UTC
N/A
jip.nfqes.com
Done
1
Tue, Oct 22, 2024 9:19 AM UTC
N/A
license.nfqes.com
Done
1
Tue, Oct 22, 2024 9:19 AM UTC
N/A
oauth.nfqes.com
Done
1
Tue, Oct 22, 2024 9:19 AM UTC
N/A
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
1 - 10 of 14

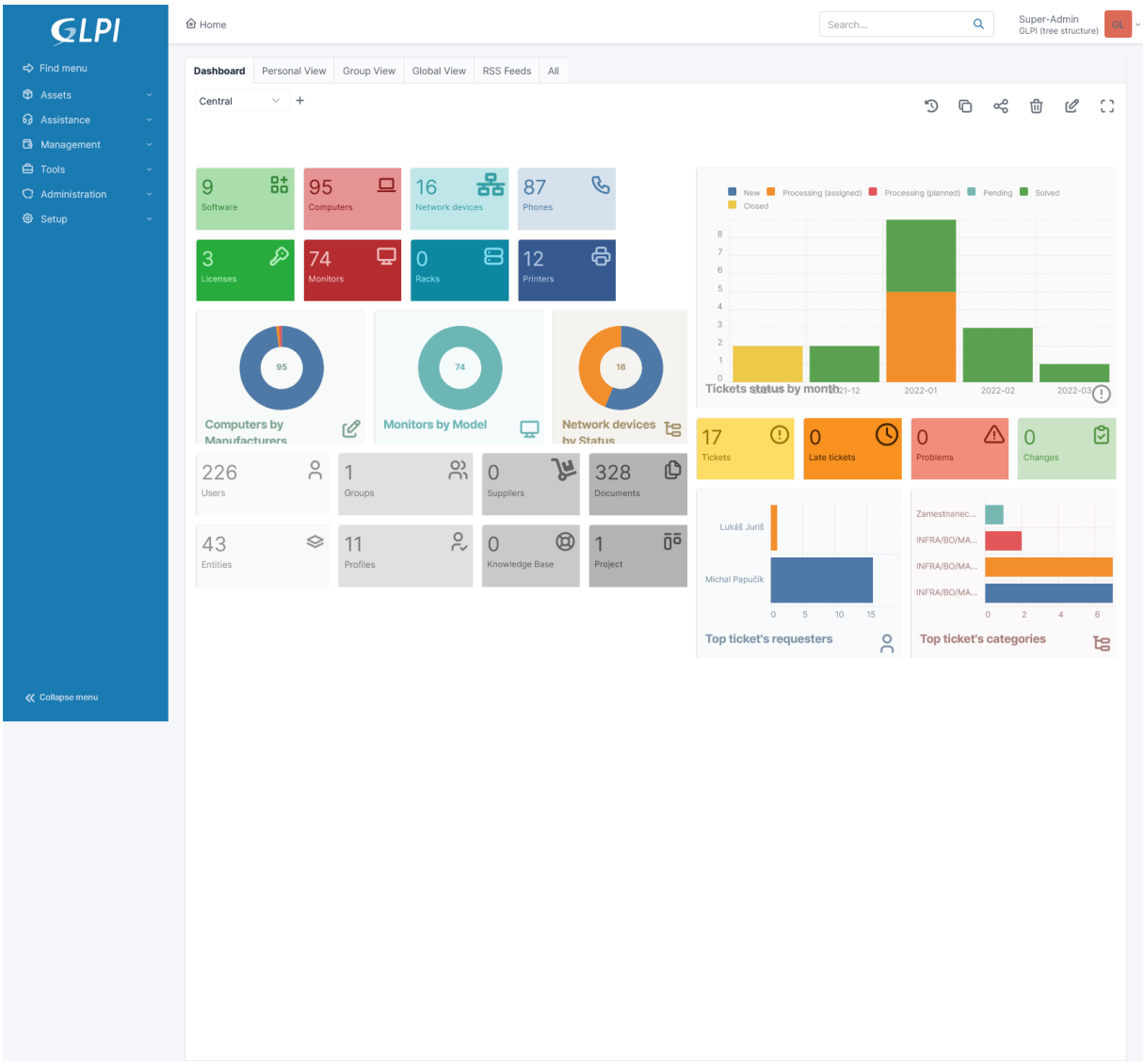

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
NVTs 142704 of 142704
NVTs by Severity Class (Total: 142704)
Log
Low
High
Medium
49286
85141
NVTs by Creation Time
Created NVTs
Total NVTs
# of created NVTs
# of total NVTs
Time
NVTs by Family (Total: 142704)
1 - 10 of 142704
Name
Family
Created ▼
Modified
CVE
Severity
QoD
WordPress LiteSpeed Cache <= 6.4.1 Sensitive Information Exposure Vulnerability
Web application abuses
Fri, Sep 6, 2024 10:00 AM UTC
Fri, Sep 6, 2024 3:39 PM UTC
CVE-2024-44000
7.8 (High)
80 %
Mozilla Firefox Security Advisory (MFSA2024-39) - Linux
General
Fri, Sep 6, 2024 8:09 AM UTC
Fri, Sep 6, 2024 3:39 PM UTC
CVE-2023-6870 CVE-2024-8381 CVE-2024-8382 CVE-2024-8383 CVE-2024-8384 CVE-2024-8385 CVE-2024-8386 CVE-2024-8387 CVE-2024-8389
9.8 (High)
30 %
WordPress LiteSpeed Cache <= 6.3.0.1 Privilege Escalation Vulnerability
Web application abuses
Thu, Sep 5, 2024 10:00 AM UTC
Fri, Sep 6, 2024 3:39 PM UTC
CVE-2024-28000
10.0 (High)
80 %
Django 4.x < 4.2.16, 5.0.x < 5.0.9, 5.1.x < 5.1.1 Multiple Vulnerabilities - Windows
General
Thu, Sep 5, 2024 2:40 AM UTC
Thu, Sep 5, 2024 12:18 PM UTC
CVE-2024-45230 CVE-2024-45231
7.8 (High)
80 %
Django 4.x < 4.2.16, 5.0.x < 5.0.9, 5.1.x < 5.1.1 Multiple Vulnerabilities - Linux
General
Thu, Sep 5, 2024 2:35 AM UTC
Thu, Sep 5, 2024 12:18 PM UTC
CVE-2024-45230 CVE-2024-45231
7.8 (High)
30 %
OpenSSL DoS Vulnerability (20240903) - Windows
Denial of Service
Wed, Sep 4, 2024 3:40 AM UTC
Thu, Sep 5, 2024 5:05 AM UTC
CVE-2024-6119
7.8 (High)
80 %
OpenSSL DoS Vulnerability (20240903) - Linux
Denial of Service
Wed, Sep 4, 2024 3:33 AM UTC
Thu, Sep 5, 2024 5:05 AM UTC
CVE-2024-6119
7.8 (High)
30 %
Progress / Ipswitch WhatsUp Gold Detection Consolidation
Product detection
Tue, Sep 3, 2024 9:05 AM UTC
Wed, Sep 4, 2024 5:16 AM UTC
0.0 (Log)
80 %
Wireshark Security Update (wnpa-sec-2024-11) - Linux
Denial of Service
Mon, Sep 2, 2024 6:37 AM UTC
Thu, Sep 5, 2024 3:07 PM UTC
CVE-2024-8250
5.5 (Medium)
80 %
Wireshark Security Update (wnpa-sec-2024-11) - Mac OS X
Denial of Service
Mon, Sep 2, 2024 6:37 AM UTC
Thu, Sep 5, 2024 3:07 PM UTC
CVE-2024-8250
5.5 (Medium)
80 %
Apply to page contents
(Applied filter: sort-reverse=created rows=10 first=1)
1 - 10 of 142704
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

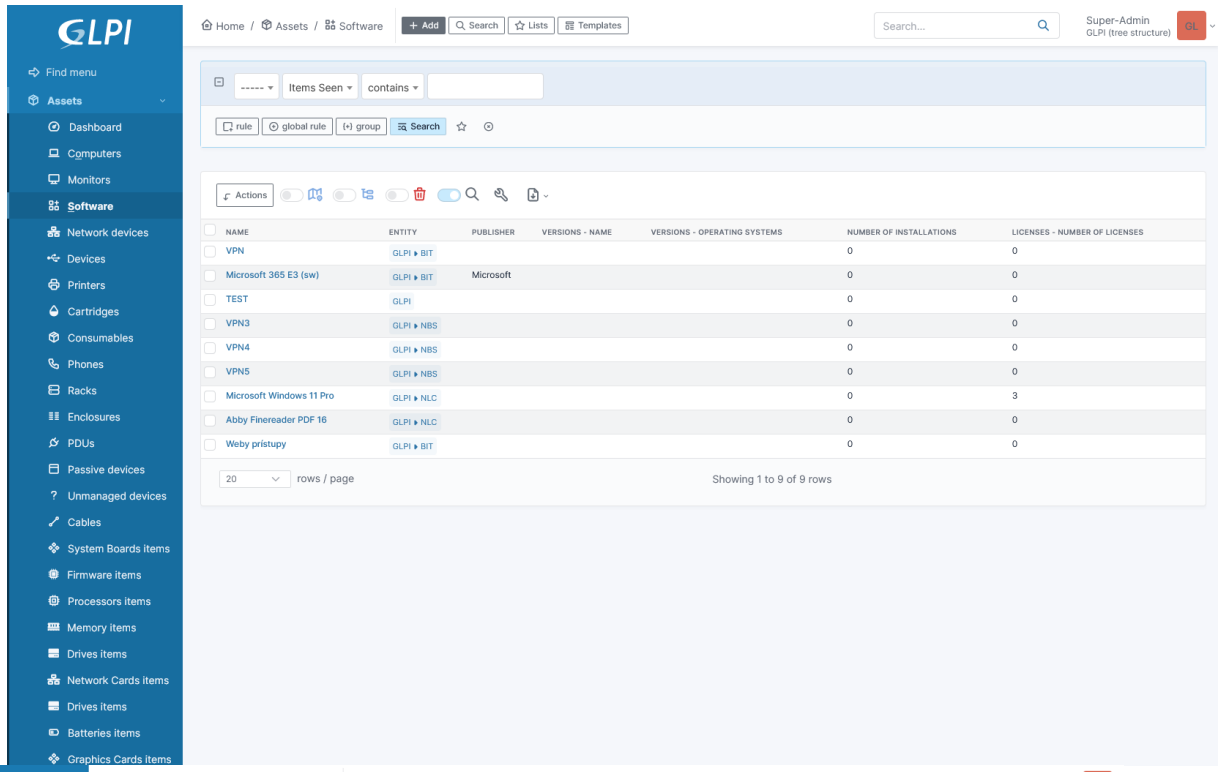


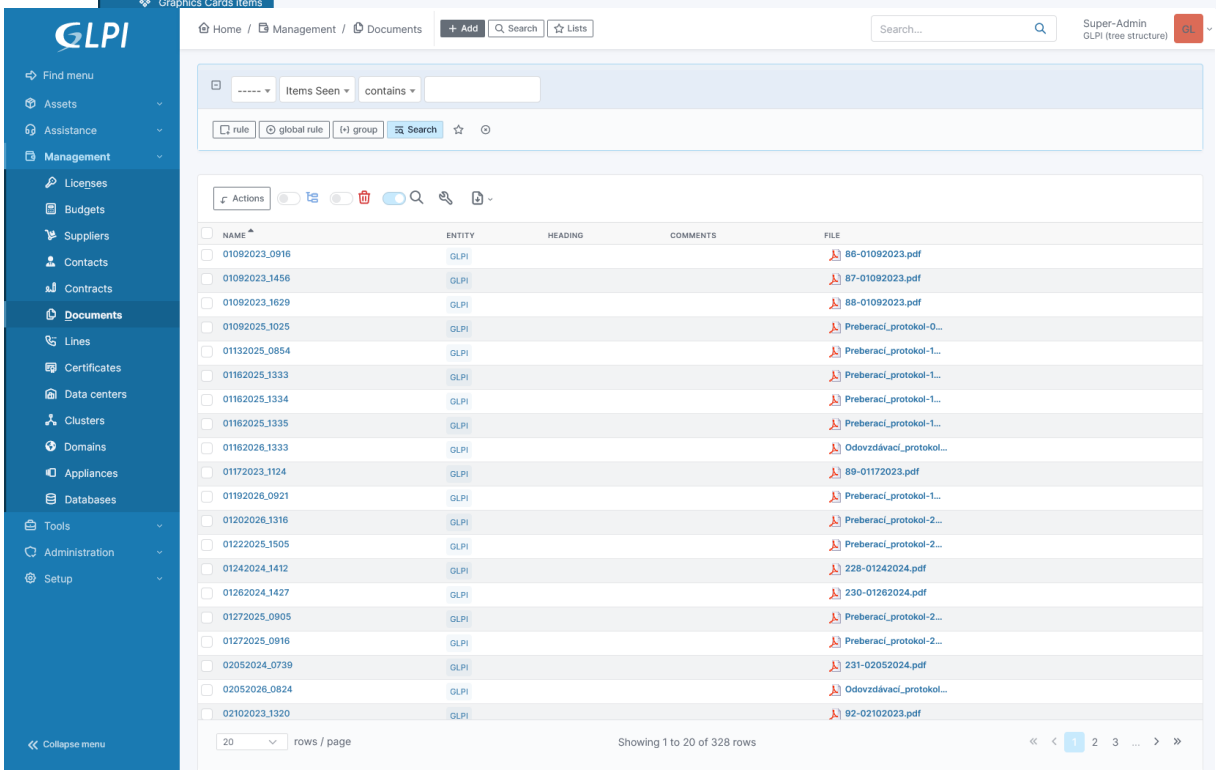
5. OPENCTI

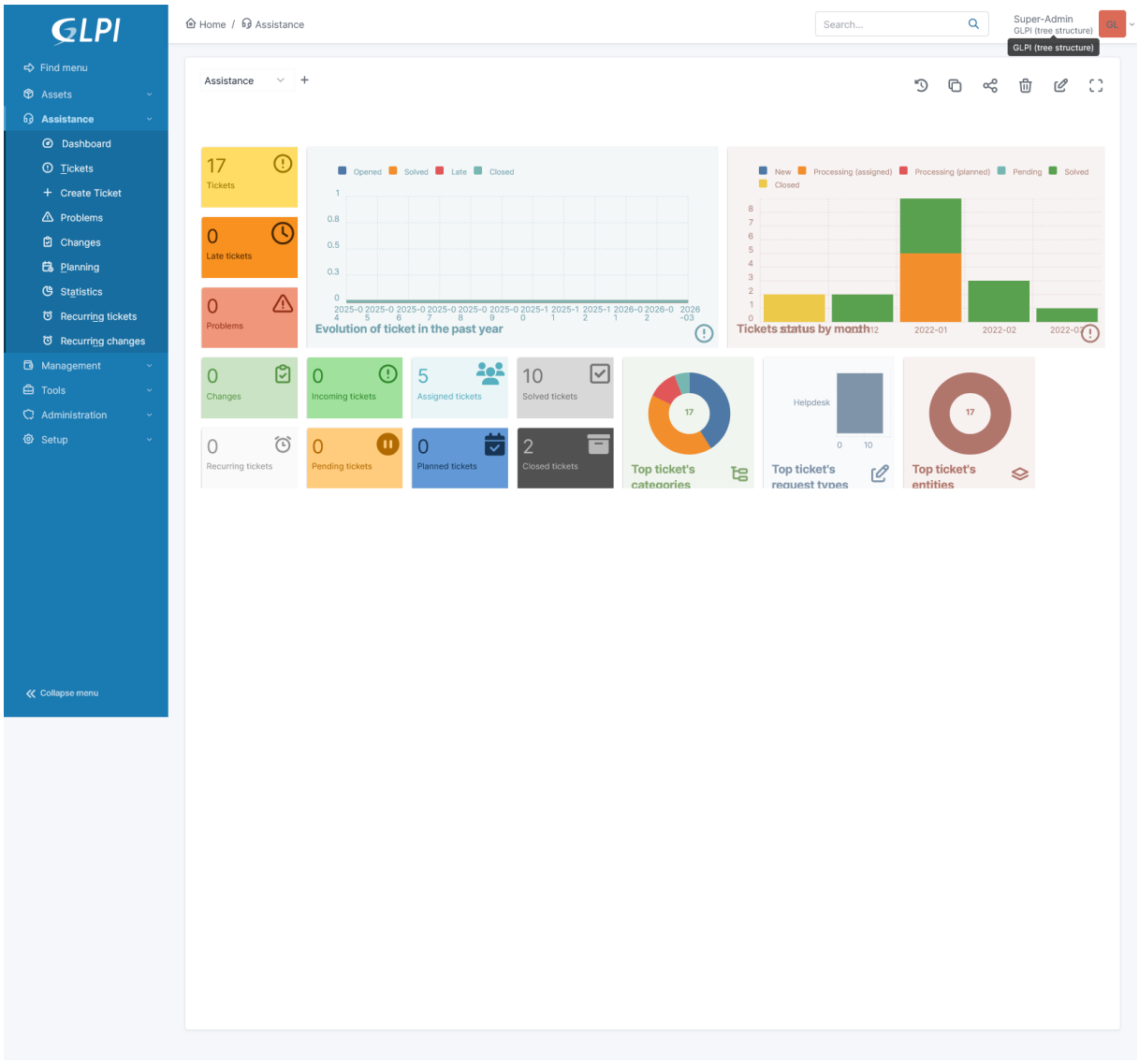
6. MISP

7. GLPI


GLPI
Home
Search...
Super-Admin
GLPI (tree structure)
Find menu
Assets
Assistance
Management
Tools
Administration
Setup
Collapse menu
Dashboard
Personal View
Group View
Global View
RSS Feeds
All
Central
9 Software
95 Computers
16 Network devices
87 Phones
3 Licenses
74 Monitors
0 Racks
12 Printers
Computers by Manufacturers
Monitors by Model
Network devices by Status
New
Processing (assigned)
Processing (planned)
Pending
Solved
Closed
Tickets status by month
2021-12
2022-01
2022-02
2022-03
17 Tickets
0 Late tickets
0 Problems
0 Changes
226 Users
1 Groups
0 Suppliers
328 Documents
43 Entities
11 Profiles
0 Knowledge Base
1 Project
Lukáš Juriš
Michal Papučík
Top ticket's requesters
Zamestnanec...
INFRA/BO/MA...
INFRA/BO/MA...
INFRA/BO/MA...
Top ticket's categories


GLPI
Home / Assets / Software
Add
Search
Lists
Templates
Search...
Super-Admin
GLPI (tree structure)
Find menu
Assets
Dashboard
Computers
Monitors
Software
Network devices
Devices
Printers
Cartridges
Consumables
Phones
Racks
Enclosures
PDUs
Passive devices
Unmanaged devices
Cables
System Boards items
Firmware items
Processors items
Memory items
Drives items
Network Cards items
Drives items
Batteries items
Graphics Cards items
Items Seen
contains
rule
global rule
group
Search
Actions
NAME
ENTITY
PUBLISHER
VERSIONS - NAME
VERSIONS - OPERATING SYSTEMS
NUMBER OF INSTALLATIONS
LICENSES - NUMBER OF LICENSES
VPN
Microsoft 365 E3 (sw)
Microsoft
TEST
VPN3
VPN4
VPN5
Microsoft Windows 11 Pro
Abby Finereader PDF 16
Weby prístupy
20
rows / page
Showing 1 to 9 of 9 rows


GLPI
Home / Management / Documents
Add
Search
Lists
Search...
Super-Admin
GLPI (tree structure)
Find menu
Assets
Assistance
Management
Licenses
Budgets
Suppliers
Contacts
Contracts
Documents
Lines
Certificates
Data centers
Clusters
Domains
Appliances
Databases
Tools
Administration
Setup
Collapse menu
Items Seen
contains
rule
global rule
group
Search
Actions
NAME
ENTITY
HEADING
COMMENTS
FILE
01092023_0916
01092023_1456
01092023_1629
01092025_1025
01132025_0854
01162025_1333
01162025_1334
01162025_1335
01162026_1333
01172023_1124
01192026_0921
01202026_1316
01222025_1505
01242024_1412
01262024_1427
01272025_0905
01272025_0916
02052024_0739
02052026_0824
02102023_1320
86-01092023.pdf
87-01092023.pdf
88-01092023.pdf
89-01172023.pdf
228-01242024.pdf
230-01262024.pdf
231-02052024.pdf
92-02102023.pdf
20
rows / page
Showing 1 to 20 of 328 rows

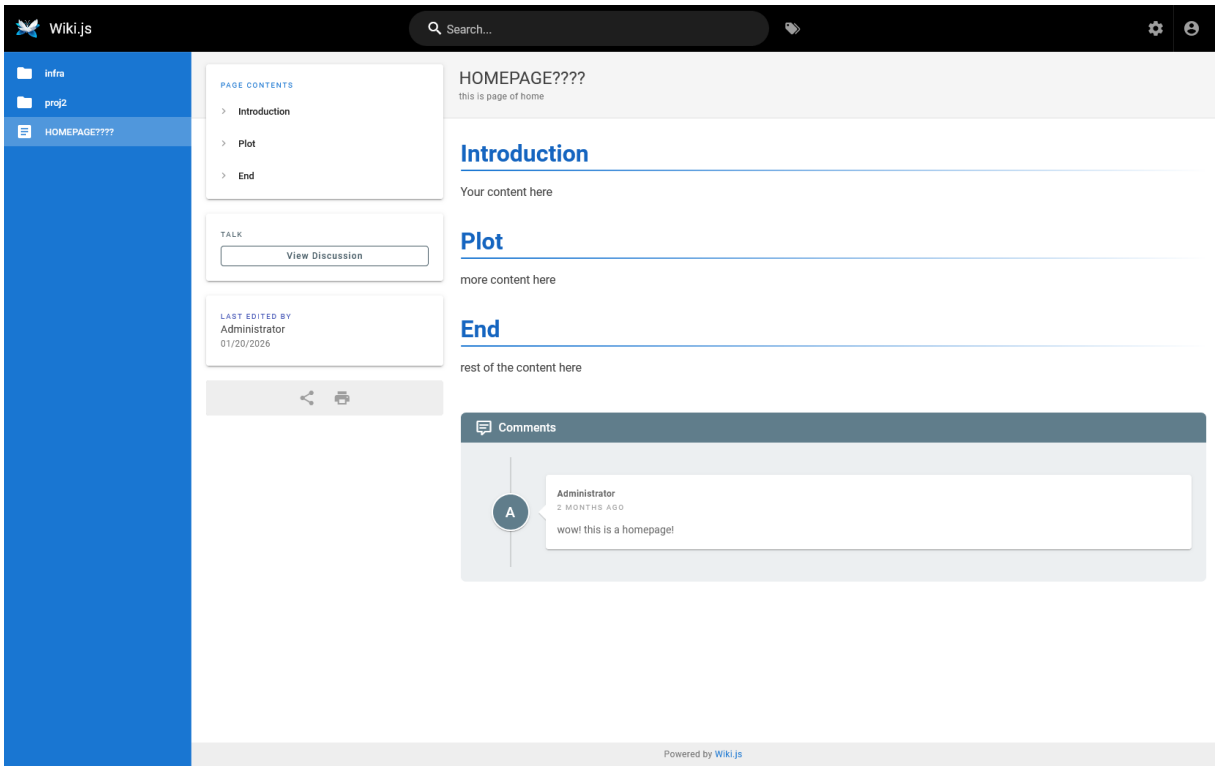


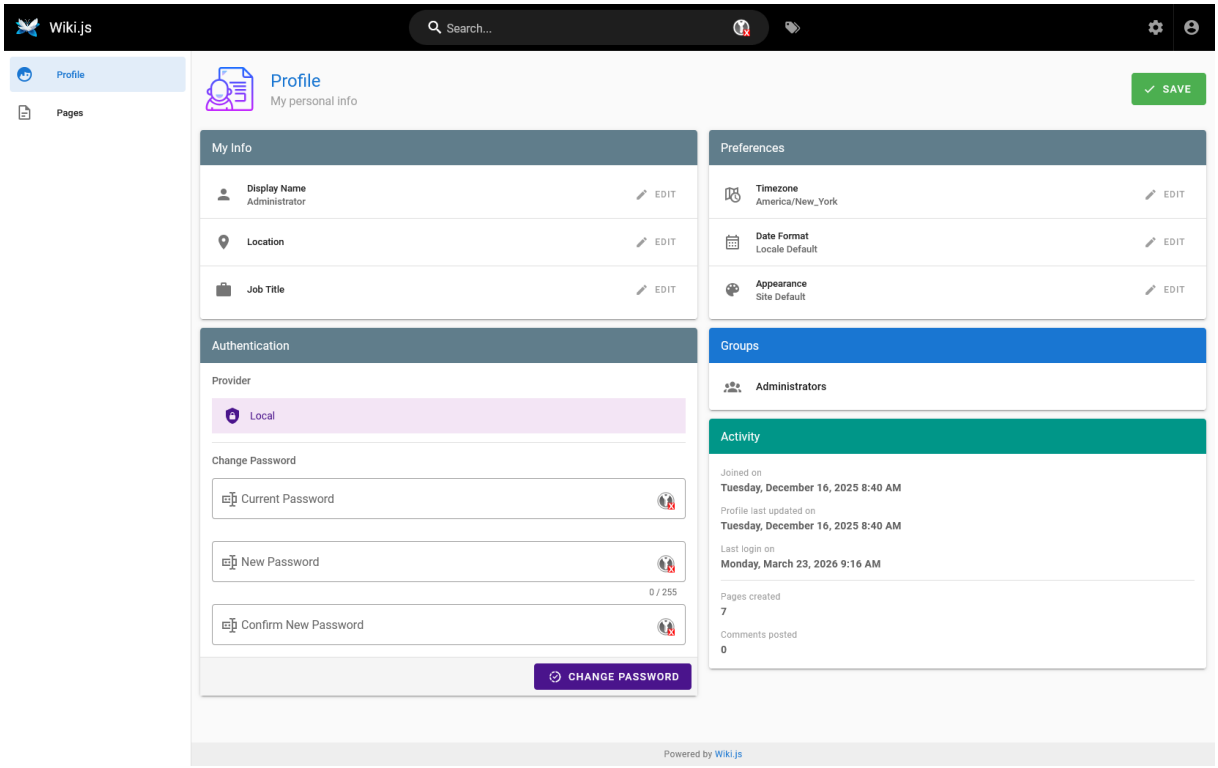
8. NETBOX

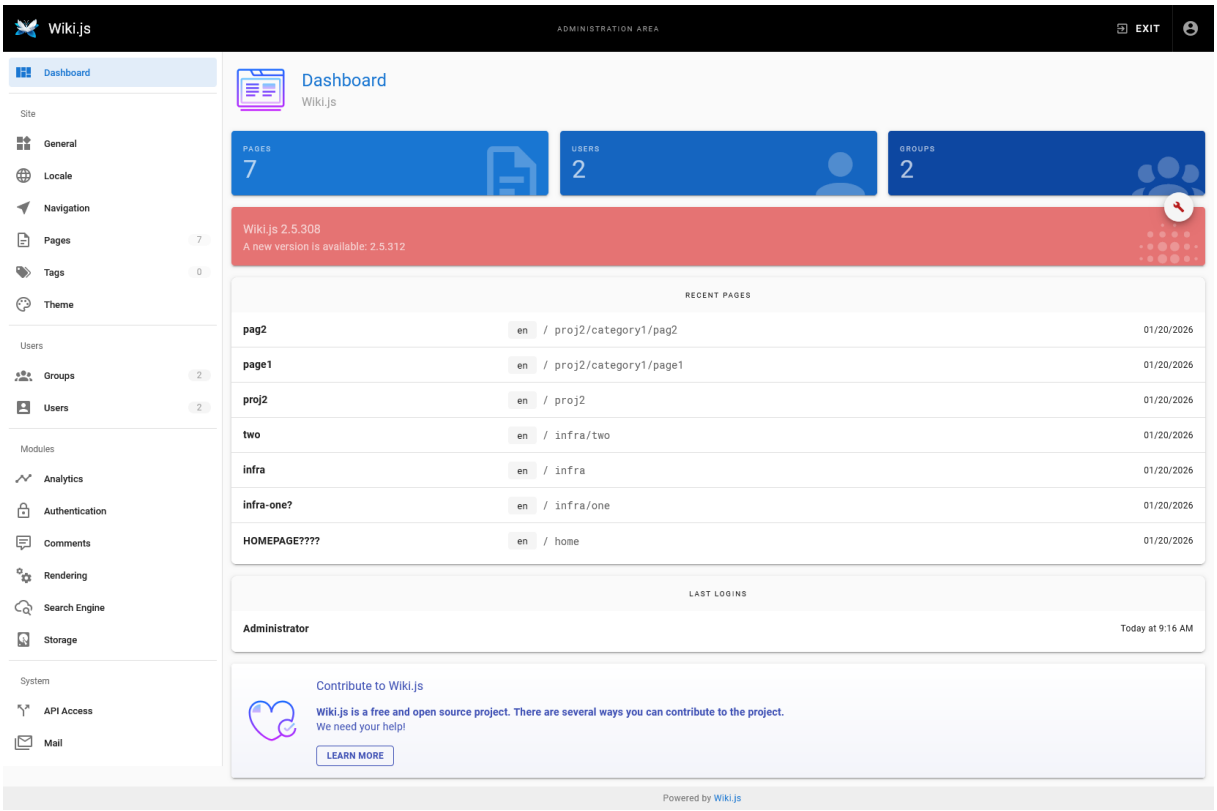
9. DFIR IRIS

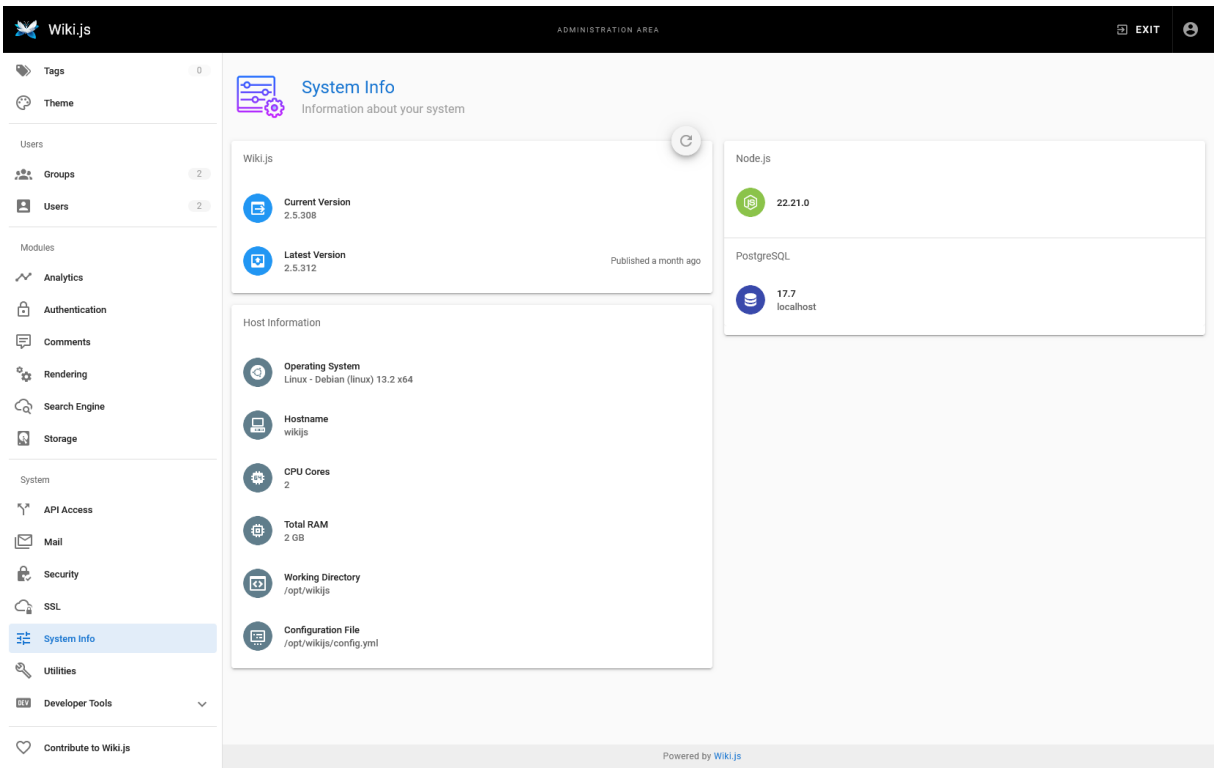
10. KIBANA (ELK)

11. WIKI.JS


Wiki.js
Search...
infra
proj2
HOMEPAGE????
PAGE CONTENTS
Introduction
Plot
End
TALK
View Discussion
LAST EDITED BY
Administrator
01/20/2026
HOMEPAGE????
this is page of home
Introduction
Your content here
Plot
more content here
End
rest of the content here
Comments
A
Administrator
2 MONTHS AGO
wow! this is a homepage!
Powered by Wiki.js


Wiki.js
Search...
Profile
Pages
Profile
My personal info
SAVE
My Info
Display Name
Administrator
EDIT
Location
EDIT
Job Title
EDIT
Preferences
Timezone
America/New_York
EDIT
Date Format
Locale Default
EDIT
Appearance
Site Default
EDIT
Authentication
Provider
Local
Change Password
Current Password
New Password
0 / 255
Confirm New Password
CHANGE PASSWORD
Groups
Administrators
Activity
Joined on
Tuesday, December 16, 2025 8:40 AM
Profile last updated on
Tuesday, December 16, 2025 8:40 AM
Last login on
Monday, March 23, 2026 9:16 AM
Pages created
7
Comments posted
0
Powered by Wiki.js





Plus v zvyšnej dokumentácii je aj nejaký screen z nastavenia emailov alebo čosi také myslím...