LinSentry

SANITIZED SAMPLE REPORT

Linux Diagnostic Report

ATTENTION

Generated	2026-09-08 20:59:25 CEST
Hostname	server01.example.com
Report identifier	LS-SAMPLE-0001

Representative LinSentry Community report. Hostnames, identifiers, paths, interface names, and other infrastructure-specific details have been anonymized.

Contents

1. Executive Summary

Operating system	Ubuntu 24.04.4 LTS
Kernel	6.8.0–138–generic
Architecture	amd64
Privileges	Administrator
Report output	Available
Total assessment duration	6.929056977s

What to review first

Warning: DNS resolution	DNS resolution failed for the test hostname.
Warning: SSH root login policy	SSH root login appears enabled.
Warning: SSH password authentication	SSH password authentication appears enabled.
Warning: Website issue: webmail.example.com	The HTTPS listener did not present a valid certificate for the selected domain.
Website result	18/19 websites healthy; 1 require attention; 0 critical
Website coverage	Complete within configured limits
Mail assessment	LIMITED – Basic mail service checks completed; domain–level and endpoint diagnostics are not inclu
Primary MTA	postfix
Queue messages	0
Database assessment	HEALTHY – Community includes basic database runtime, service, listener, and socket checks.
Database instances	2

2. Immediate Priorities

Warning: DNS resolution	DNS resolution failed for the test hostname.
Warning: SSH root login policy	SSH root login appears enabled.
Warning: SSH password authentication	SSH password authentication appears enabled.
Warning: Website issue: `webmail.example.com`	The HTTPS listener did not present a valid certificate for the selected domain.

3. Host Health, Containers, and Exposure

Overall report status	ATTENTION
Diagnostic engine status	ATTENTION
Checks run	27
Passed	17
Warnings	3
Critical	0
Unavailable	0
Diagnostic-engine duration	2.191987946s

Category Summary

System resources	PASS, 2 check(s), No key issue
Storage	PASS, 1 check(s), No key issue
Services	PASS, 1 check(s), No key issue
Packages	PASS, 1 check(s), No key issue
Network	WARNING, 3 check(s), DNS resolution failed for the test hostname.
Time	PASS, 1 check(s), No key issue
SSH	WARNING, 7 check(s), SSH root login appears enabled.
Firewall	PASS, 3 check(s), No key issue
Exposure	PASS, 2 check(s), No key issue
Containers	PASS, 6 check(s), No key issue

3.1 SSH, Firewall and Network Exposure

SSH – SSH service	PASS: SSH service appears active. Evidence: service state: active systemctl is-active ssh/sshd; failure is not treated as proof of absence.
SSH – SSH listeners	INFORMATION: SSH has at least one public or wildcard listener. Evidence: SSH listener: tcp 0.0.0.0:22 scope: wildcard category: ssh owner: sshd Parsed from ss/netstat output.; SSH listener: tcp :::22 scope: wildcard category: ssh owner: sshd Parsed from ss/netstat output.
SSH – SSH root login policy	WARNING: SSH root login appears enabled. Evidence: permitrootlogin: yes sshd -T
SSH – SSH password authentication	WARNING: SSH password authentication appears enabled. Evidence: passwordauthentication: yes sshd -T
SSH – SSH empty-password policy	PASS: SSH empty passwords does not appear enabled. Evidence: permitemptypasswords: no sshd -T

SSH – SSH configuration permissions	PASS: SSH server configuration permissions did not show group/world–writable files. Evidence: config permissions: /etc/ssh/sshd_config 0644 SSH server configuration metadata only; file content is not exposed.
SSH – SSH configuration ambiguity	PASS: No conflicting SSH directives were detected in the primary configuration file.
Firewall – Firewall tooling	PASS: Supported host firewall tooling was detected: ufw, nftables, iptables. Evidence: tools: ufw, nftables, iptables Supported tooling detection uses read–only commands.
Firewall – Firewall state	INFORMATION: Firewall state is ambiguous from supported tooling. LinSentry did not confirm active firewall enforcement from supported tooling. Evidence: state: inactive ufw status verbose
Firewall – Firewall default policy	PASS: Firewall default inbound policy appears restrictive. This is configuration evidence; active firewall enforcement must be confirmed separately. Evidence: default inbound: drop ufw status verbose
Network – Listening ports	INFORMATION: 157 listening TCP/UDP socket(s) were observed. Evidence: listener: tcp *:106 scope: wildcard category: unknown owner: xinetd Scope and category are conservative classifications from socket listing.; listener: tcp *:21 scope: wildcard category: unknown owner: xinetd Scope and category are conservative classifications from socket listing.; listener: tcp *:33535 scope: wildcard category: unknown owner: service-runner Scope and category are conservative classifications from socket listing.
Network – Basic exposure	INFORMATION: Public administrative or database listeners were observed; firewall protection was not fully evaluated. Evidence: public listener: tcp 0.0.0.0:22 scope: wildcard category: ssh owner: sshd Public/wildcard administrative or database service exposure requires review.; public listener: tcp :::22 scope: wildcard category: ssh owner: sshd Public/wildcard administrative or database service exposure requires review.
Public administrative/database listeners	tcp 0.0.0.0:22 scope: wildcard category: ssh owner: sshd; tcp :::22 scope: wildcard category: ssh owner: sshd

Resource Summary

CPU and load / Load 1m	0.29
CPU and load / 15–minute load per CPU	0.07
Memory and swap / Available memory	33.0%
Memory and swap / Swap used percent	0.0%
Filesystems and storage / Highest filesystem usage	39.5%
Filesystems and storage / Worst inode percent	6.0%

Containers

Container runtime detection	PASS – Docker detected and accessible.

Docker daemon health	PASS – Docker daemon is responding.
Docker client/server compatibility	PASS – Docker client/server metadata was collected.
Container state	PASS – Container states appear healthy.
Podman detection	SKIPPED – Podman was not detected.
containerd detection	INFORMATION – containerd was detected; Docker–managed containerd is not treated as a conflict.

4. Package and Update Posture

Package manager	APT/dpkg
Package database	Healthy
Metadata refreshed	Not checked in Community
Available updates	Not checked in Community
Security updates	Not checked in Community
Reboot required	Not checked in Community
Automatic updates	Not checked in Community
Plesk updates	Not checked in Community

5. Website Portfolio

Conclusion	18/19 websites healthy; 1 attention; 0 critical; 0 limited
Public checks	19 tested, 0 omitted
Inventory	19 of 19 hosted domains checked
Coverage	Basic website inventory and public HTTP/TLS evidence only

6. Mail Overview

Mail assessment	LIMITED – Basic mail service checks completed; domain–level and endpoint diagnostics are not included in Community.
Reason	Basic mail service checks completed; domain–level and endpoint diagnostics are not included in Community.
Primary MTA	postfix
MTA state	active
Mail domains	0 total, 0 mail–enabled
Queue	0 message(s), oldest deferred 0s
Endpoint testing	0 attempted, 0 completed, 0 not configured, 0 skipped
Endpoint failures	0 DNS, 0 refused, 0 timeout, 0 TLS, 0 protocol
Unique IP/port combinations	Unavailable; hostname/port sessions retained
Hostname/port combinations tested	0
Terminal TLS failures	0
TLS handshake observations	0
TLS related endpoint sessions	0
TLS posture	not checked
DNS authentication	pass

Service Posture

Port 25	pass
Port 587	not configured; implicit TLS submission is available on 465
Port 465	pass
Port 143	pass
Port 993	pass
Port 110	pass
Port 995	pass
Filtering	pass: spamd
Antivirus	could not be confirmed

Basic Mail Coverage

Runtime detection	Complete
Service assessment	Complete
Queue assessment	Skipped
Mail–log access	Skipped

7. Databases

Conclusion	2/2 database instance(s) healthy; 0 attention; 0 critical; 0 limited
Status reason	Community includes basic database runtime, service, listener, and socket checks.
Instances discovered	2
Instances checked	2

Database Instances

mariadb / mariadb	Active Yes | Listeners 1 | Sockets 2 | Overall HEALTHY
postgresql / postgresql	Active Yes | Listeners 2 | Sockets 1 | Overall HEALTHY

8. System Information

Product version	0.9.4
Edition	LinSentry Community
Commit	sample-build
Build date	2026-09-08T13:40:58Z
Report schema	1.0
Inspection mode	Read-only; LinSentry did not modify system configuration, files, services, packages, containers, firewall rules, users, or accounts.
Generated UTC	2026-09-08 18:59:25 UTC
Generated local	2026-09-08 20:59:25 CEST
Hostname	server01.example.com
Username	root
Effective UID	0
Root status	true
OS	linux
Distribution ID	ubuntu
Distribution family	debian
Distribution version	24.04.4 LTS (Noble Numbat)
Init system	systemd
Virtualization	unknown

Permission Assessment

Running as root	Yes
Privileged checks	Not limited by privileges
Reports writable	Yes
Selected directory	/home/admin
Write-test created file	Yes
Write-test wrote data	Yes
Write-test cleanup	Yes

Findings

DNS resolution

WARNING / OPEN

DNS resolution failed for the test hostname.

Recommendation: Review resolver configuration and local stub resolver status.

SSH root login policy

WARNING / OPEN

SSH root login appears enabled.

Recommendation: Review SSH authentication policy before changing configuration. LinSentry did not modify SSH settings.

SSH password authentication

WARNING / OPEN

SSH password authentication appears enabled.

Recommendation: Review SSH authentication policy before changing configuration. LinSentry did not modify SSH settings.

Website issue: webmail.example.com

WARNING / OPEN

The HTTPS listener did not present a valid certificate for the selected domain.

Recommendation: Review certificate assignment and chain state; LinSentry does not renew certificates.

Memory and swap

INFORMATION / OBSERVED

Memory availability is healthy. No swap is configured.

SSH listeners

INFORMATION / OBSERVED

SSH has at least one public or wildcard listener.

Firewall state

INFORMATION / OBSERVED

Firewall state is ambiguous from supported tooling.

Listening ports

INFORMATION / OBSERVED

157 listening TCP/UDP socket(s) were observed.

Basic exposure

INFORMATION / OBSERVED

Public administrative or database listeners were observed; firewall protection was not fully evaluated.

containerd detection

INFORMATION / OBSERVED

containerd was detected; Docker–managed containerd is not treated as a conflict.

Mail assessment coverage is limited

INFORMATION / OBSERVED

Some mail diagnostics were omitted, inaccessible, or unsupported under configured safety limits.

Recommendation: Review mail coverage before treating untested domains or endpoints as healthy.

Database assessment coverage is limited

INFORMATION / OBSERVED

Some database diagnostics were unavailable, unsupported, skipped, or permission–limited.

Recommendation: Review database coverage before treating untested services as healthy.

Running with administrator privileges

SUCCESS / OK

LinSentry is running with administrator privileges.

Report output is available

SUCCESS / OK

A report directory passed a real write test.

9. Detailed Diagnostic Appendix

CPU and load

PASS | 208.591µs

CPU load appears healthy.

logical_cpus	2
load_1m	0.29
load_15m_per_cpu	0.07
uptime_seconds	1672478
runnable_processes	2
processes_total	719

- /proc/loadavg: 1m 0.29, 5m 0.22, 15m 0.13, runnable/total 2/719 – 15–minute load is normalized by logical CPU count. Runnable/total process counts are current /proc/loadavg state.
- CPU pressure: some avg10=0.78 avg60=0.68 avg300=0.61 total=14635625256 – Pressure stall information from /proc/pressure/cpu.

Memory and swap

INFORMATION | 196.909µs

Memory availability is healthy. No swap is configured.

mem_total	3.8 GiB
mem_available_percent	33.0%
swap_used_percent	0.0%

- /proc/meminfo: MemAvailable 33.0%, Swap used 0.0% – Linux page cache is not treated as wasted memory.
- Memory pressure: some avg10=0.00 avg60=0.00 avg300=0.00 total=120559923 – Pressure stall information.

Filesystems and storage

PASS | 625.384µs

Filesystem capacity and inode usage appear healthy.

filesystems_checked	20
worst_capacity_percent	39.5%
worst_inode_percent	6.0%

- /: ext4 39.5% used, inodes 6.0% – Mounted filesystem statistics from statfs.
- /boot: ext4 13.2% used, inodes 1.0% – Mounted filesystem statistics from statfs.
- /boot/efi: vfat 5.8% used, inodes 0.0% – Mounted filesystem statistics from statfs.

Failed services

PASS | 14.740375ms

No failed systemd services were detected.

failed_units	0

- systemd state: running – systemctl is–system–running

Package–manager health

PASS | 72.648355ms

dpkg package configuration audit did not report issues.

- dpkg ––audit: – Read–only package configuration audit.

Network configuration

PASS | 1.659874ms

Local network configuration appears healthy.

non_loopback_interfaces	14
active_interfaces	14
nameservers	1

- interface: ens6 up|broadcast|multicast|running addresses=2 – MAC addresses are intentionally omitted.
- interface: vpn0 up|pointtopoint|multicast|running addresses=3 – MAC addresses are intentionally omitted.
- interface: br-example01 up|broadcast|multicast|running addresses=2 – MAC addresses are intentionally omitted.

- interface: br-example02 up|broadcast|multicast|running addresses=2 – MAC addresses are intentionally omitted.
- interface: docker0 up|broadcast|multicast|running addresses=2 – MAC addresses are intentionally omitted.
- interface: br-example03 up|broadcast|multicast addresses=1 – MAC addresses are intentionally omitted.
- interface: br-example04 up|broadcast|multicast|running addresses=2 – MAC addresses are intentionally omitted.
- interface: veth-example up|broadcast|multicast|running addresses=1 – MAC addresses are intentionally omitted.
- Additional evidence was omitted after 8 entries.

External connectivity

PASS | 22.490003ms

External TCP connectivity was confirmed.

- TCP connectivity: 1.1.1.1:443 – Connection to port 443 succeeded; no HTTP request was sent.
- TCP connectivity: 8.8.8.8:443 – Connection to port 443 succeeded; no HTTP request was sent.

DNS resolution

WARNING | 3.926607ms

DNS resolution failed for the test hostname.

nameservers	1
resolution_ms	3 ms
returned_addresses	0

- nameserver: 127.0.0.53 – Parsed from resolver configuration.

Clock synchronization

PASS | 200.553889ms

Clock synchronization appears active.

- UTC time: 2026-09-08T18:59:25Z – Local system clock.
- timedatectl: Europe/Madrid yes – Machine-readable synchronization properties.

SSH service

PASS | 13.931316ms

SSH service appears active.

- service state: active – systemctl is-active ssh/sshd; failure is not treated as proof of absence.

SSH listeners

INFORMATION | 129.858076ms

SSH has at least one public or wildcard listener.

ssh_listeners	2

- SSH listener: tcp 0.0.0.0:22 scope: wildcard category: ssh owner: sshd – Parsed from ss/netstat output.
- SSH listener: tcp :::22 scope: wildcard category: ssh owner: sshd – Parsed from ss/netstat output.

SSH root login policy

WARNING | 25.744669ms

SSH root login appears enabled.

- permitrootlogin: yes – sshd -T

SSH password authentication

WARNING | 30.918245ms

SSH password authentication appears enabled.

- passwordauthentication: yes – sshd -T

SSH empty-password policy

PASS | 20.271121ms

SSH empty passwords does not appear enabled.

- permitemptypasswords: no – sshd -T

SSH configuration permissions

PASS | 24.035µs

SSH server configuration permissions did not show group/world–writable files.

- config permissions: /etc/ssh/sshd_config 0644 – SSH server configuration metadata only; file content is not exposed.

SSH configuration ambiguity

PASS | 647.725µs

No conflicting SSH directives were detected in the primary configuration file.

Firewall tooling

PASS | 3.467µs

Supported host firewall tooling was detected: ufw, nftables, iptables.

- tools: ufw, nftables, iptables – Supported tooling detection uses read–only commands.

Firewall state

INFORMATION | 1.222µs

Firewall state is ambiguous from supported tooling.

- state: inactive – ufw status verbose

Firewall default policy

PASS | 1.373µs

Firewall default inbound policy appears restrictive.

- default inbound: drop – ufw status verbose

Listening ports

INFORMATION | 91.522105ms

157 listening TCP/UDP socket(s) were observed.

listeners_private	25
listeners	157
listeners_wildcard	40
listeners_public	11
listeners_loopback	26
listeners_unknown	55

- listener: tcp *:106 scope: wildcard category: unknown owner: xinetd – Scope and category are conservative classifications from socket listing.
- listener: tcp *:21 scope: wildcard category: unknown owner: xinetd – Scope and category are conservative classifications from socket listing.
- listener: tcp *:33535 scope: wildcard category: unknown owner: service-runner – Scope and category are conservative classifications from socket listing.
- listener: tcp *:34947 scope: wildcard category: unknown owner: service-runner – Scope and category are conservative classifications from socket listing.
- listener: tcp *:38959 scope: wildcard category: unknown owner: service-runner – Scope and category are conservative classifications from socket listing.
- listener: tcp *:40507 scope: wildcard category: unknown owner: service-runner – Scope and category are conservative classifications from socket listing.
- listener: tcp *:42345 scope: wildcard category: unknown owner: service-runner – Scope and category are conservative classifications from socket listing.
- listener: tcp *:42735 scope: wildcard category: unknown owner: service-runner – Scope and category are conservative classifications from socket listing.
- Additional evidence was omitted after 8 entries.

Basic exposure

INFORMATION | 366.909377ms

Public administrative or database listeners were observed; firewall protection was not fully evaluated.

- public listener: tcp 0.0.0.0:22 scope: wildcard category: ssh owner: sshd – Public/wildcard administrative or database service exposure requires review.
- public listener: tcp :::22 scope: wildcard category: ssh owner: sshd – Public/wildcard administrative or database service exposure requires review.

Container runtime detection

PASS | 1.342µs

Docker detected and accessible.

- Docker CLI: /usr/bin/docker – Docker version 29.8.0, build 88096ef
- socket: Known Docker socket –
- containerd: /usr/bin/containerd –

Docker daemon health

PASS | 7.364µs

Docker daemon is responding.

images	66
running_containers	7
total_containers	7

- Docker socket access: Available – Access to the Docker socket provides administrative control over the host.
- Storage driver: overlay2 –
- Logging driver: json–file –
- Docker root: /var/lib/docker –

Docker client/server compatibility

PASS | 682ns

Docker client/server metadata was collected.

- Server version: 29.8.0 –
- API version: 1.56 –
- Architecture: x86_64 –

Container state

PASS | 2.434µs

Container states appear healthy.

containers	7
running_containers	7
restarting_containers	0
dead_containers	0

Podman detection

SKIPPED | 330ns

Podman was not detected.

containerd detection

INFORMATION | 401ns

containerd was detected; Docker–managed containerd is not treated as a conflict.

- containerd: containerd containerd v2.3.4 db8809540e1a7a9da5d518876894933ff55692ab –

10. Coverage and Limitations

Linux system checks	Complete when diagnostics ran
Container checks	See container section
Package database health	Complete
Available–update inventory	Not checked in Community
Security classification	Not checked in Community
Metadata freshness	Not checked in Community
Repository posture	Not checked in Community
Restriction/hold posture	Not checked in Community
Automatic–update posture	Not checked in Community
Reboot requirement	Not checked in Community
Plesk update posture	Not checked in Community
Website inventory coverage	19 of 19 domains
Public HTTP/TLS coverage	19 tested, 0 omitted
Mail runtime detection	Complete
Mail service assessment	Complete
Mail–domain inventory	0 of 0
MX assessments	0 of 0
SPF assessments	0 of 0
DKIM assessments	0 configured selectors
DMARC assessments	0 of 0
Mail endpoint hostnames tested	0 of 0
Queue assessment	Not checked in Community
Quota assessment	Not checked in Community
Mail–log access	Not checked in Community
Mail coverage note	Community includes basic mail runtime, service, and listener checks; domain–level diagnostics are not performed in Community.
Database runtime detection	Complete
Database service assessment	Complete
Database listener assessment	Complete
Database status collection	Not checked in Community
Database log access	Not checked in Community
Database backup assessment	Not checked in Community
Database instances discovered	2

Database instances checked	2
Database coverage note	Community includes basic database runtime, service, listener, and socket checks.

11. Methodology

Safety	Diagnostics are read–only. LinSentry does not read customer database table contents, send SMTP DATA, authenticate to mailbox protocols, or modify queues, DNS, services, Plesk, or database configuration.
Scope	Protocol checks use standard ports and bounded timeouts. Reputation and end–to–end delivery are not verified through external services.
Environment detection duration	191.559µs
Plesk detection duration	722ns
Report–directory selection duration	3.207037ms
Core Linux diagnostic duration	2.192005689s
Package diagnostic duration	2.177039731s
Container diagnostic duration	208.865351ms
Website diagnostic duration	1.265037922s
Mail diagnostic duration	1.781406101s
Database diagnostic duration	1.475196013s
Report model assembly duration	3.077494ms
Total assessment duration	6.929056977s
PDF rendering duration	34.445162ms