RHEL Security Baseline

Highest impact security improvements for Our Visitors

Concetti Systems

2026-05-16

Contents

Concetti Systems RHEL Security Baseline

Highest impact security improvements for Our Visitors

Provided by

Concetti Systems

Infrastructure security and reliability, explained clearly and implemented carefully.

Report date: 2026-05-16

Concetti IT Consulting Ltd
Strovolos - Cyprus
https://concetti.systems – contact@concetti.systems

1 RHEL Security Baseline

1.1 Introduction

This document contains a focused selection of hardening recommendations for **Our Visitors**.

The goal is not to apply every possible security setting blindly. The goal is to reduce unnecessary operational and security risk while keeping the environment working.

The recommendations in this report were selected because they are relevant to the assessed systems, provide meaningful risk reduction, and can be implemented with acceptable operational impact.

1.2 Scope

- Customer: Our Visitors
- Systems assessed: Example RHEL servers
- Platform in scope: RHEL
- Versions in scope: RHEL 7 / 8 / 9 / 10
- Assessment method: Example report built from selected controls
- Report date: 2026-05-16

1.3 Important note

Not every hardening recommendation applies to every system. Some recommendations may be intentionally excluded because they conflict with application requirements, vendor support conditions, operational constraints, or accepted business risk.

Where a recommendation should not be implemented immediately, the text explains why and what should be validated first.

1.4 Ownership and reuse

This report was prepared by **Concetti Systems** for **Our Visitors**. It may be used internally by Our Visitors for the systems in scope.

The recommendations are context-specific. Reuse outside this scope should be reviewed before implementation.

1.5 Overview of recommendations

The following recommendations are included in this document:

- WHAT IT LOOKS LIKE (what-it-looks-like)
- Disable direct root login via SSH (SSH-01-ROOT-LOGIN)
- Disable unused filesystem types (FS-01-UNUSED-TYPES)
- Restrict core dumps (CORE-01-RESTRICT-DUMPS)
- Disable IP forwarding (NET-02-IP-FORWARDING)

2 Detailed recommendations

The following sections describe each recommendation in detail. For each item, you will find a short explanation of what it means, why it matters, and how it can be implemented safely.

2.1 WHAT IT LOOKS LIKE

Applies to: All Plaforms
Risk reduction: Low
Disruption risk: Low
Effort: Low

2.1.1 Example recommendation — Identity and access control

In a full report, this section explains the purpose of the control, why it matters, when it should not be applied blindly, and how implementation can be validated safely.

The customer-specific version includes platform-specific commands, configuration paths, expected values, and operational notes.

2.1.2 What does it mean?

Thank you for downloading this example report. When we work with you you will not just get a thick report with gaps in your system hardening. You get a personalized report with a clear explanation of how to execute. Or you can have us do the work for you.

This page is only an example to get you familiar with the report format you can expect. The Concetti Systems approach will provide you with workable chunks of tasks, tailored for the needs of your organization.

2.1.3 Why should you want this?

Hardening is meant to decrease your attack surface, or in plain English: reduce the entries that an attacker could use to compromise your system.

Such attacks aren't always malicious, but can also come from your own team or systems that, unwillingly, don't act in the most secure way.

In any case whatever is protected well, cannot easily be broken.

2.1.4 Operational prerequisite

In this section you will find what to do to securely implement the hardening we recommend and sometimes how to back out and roll back if there should be such a need.

2.1.5 Impact

Your system will change. That is a good thing. But you may see that some bad practices that have become a regular part of your workflow don't behave the same anymore. While this new behavior is intended, you may encounter issues if you rely on the current behavior.

2.1.6 How to implement

The texts before this section are meant for an audience that doesn't necessarily have a technical background.

From here on you will find step by step instructions for engineers. They are written so that a junior engineer can follow them.

2.1.7 How to verify

This section is an engineer level instruction to see if the changes have been applied correctly.

2.2 SSH-01-ROOT-LOGIN — Disable direct root login via SSH

Applies to: RHEL 7 / 8 / 9 / 10
Risk reduction: High
Disruption risk: Medium
Effort: Low

2.2.1 What does it mean?

Some systems allow administrators to log in directly as the `root` user over SSH.

2.2.2 Why should you want this?

In a hypothetical attack, an exposed SSH service can be targeted using stolen credentials, guessed passwords, or misplaced private keys.

If direct root login is allowed, there is no extra step between access and full system control.

If direct root login is used, access is shared and not individually attributable. When someone leaves the organization, all systems where the root password is known must be updated immediately. In practice, this is rarely done consistently, which increases long-term risk.

2.2.3 Operational prerequisite

Ensure that at least one administrative user with sudo privileges can log in successfully.

2.2.4 Impact

After applying this change, direct SSH login as `root` will no longer work.

Automation and procedures relying on root login must use a non-root account with sudo.

2.2.5 How to implement

Open /etc/ssh/sshd_config
Set: PermitRootLogin no
Restart SSH service

2.2.6 How to verify

Run: sshd -T | grep permitrootlogin

Expected: permitrootlogin no

2.3 FS-01-UNUSED-TYPES — Disable unused filesystem types

Applies to: RHEL 7 / 8 / 9 / 10
Risk reduction: Medium
Disruption risk: Low
Effort: Low

2.3.1 What does it mean?

Linux supports many different filesystem types, but most systems only use a limited set.

Unused filesystem support increases the available attack surface.

2.3.2 Why should you want this?

In a hypothetical case, a crafted filesystem image could be used to exploit unused drivers.

By disabling unused filesystem types, the number of potential attack paths is reduced.

2.3.3 Operational prerequisite

Confirm which filesystem types are required for system operation, backups, or container workflows.

2.3.4 Impact

After applying this change, disabled filesystem types can no longer be mounted.

Workflows relying on those filesystem types will fail.

2.3.5 How to implement

Open /etc/modprobe.d/disable-filesystems.conf
Add entries such as:

```
install cramfs /bin/true
install freevxfs /bin/true
install jffs2 /bin/true
install hfs /bin/true
install hfsplus /bin/true
install squashfs /bin/true
install udf /bin/true
```

Unload modules if currently active.

2.3.6 How to verify

Run: lsmod | grep

Expected: no output

2.4 CORE-01-RESTRICT-DUMPS — Restrict core dumps

Applies to: RHEL 7 / 8 / 9 / 10
Risk reduction: Medium
Disruption risk: Medium
Effort: Low

2.4.1 What does it mean?

Core dumps are memory snapshots of crashed processes. They may contain sensitive data.

2.4.2 Why should you want this?

In a hypothetical case, a core dump may contain passwords, encryption keys, tokens, or application data.

If accessible, it becomes a data leak.

2.4.3 Operational prerequisite

Confirm that core dumps are not required for active debugging or vendor-supported troubleshooting.

2.4.4 How to implement

Open /etc/security/limits.conf
Add: * hard core 0

2.4.5 How to verify

Run: ulimit -c
Expected: 0

2.5 NET-02-IP-FORWARDING — Disable IP forwarding

Applies to: RHEL 7 / 8 / 9 / 10
Risk reduction: Medium
Disruption risk: Medium
Effort: Low

2.5.1 What does it mean?

IP forwarding allows a system to route traffic between networks.

2.5.2 Why should you want this?

In a hypothetical case, a system unintentionally acts as a router, bypassing network controls and exposing internal systems.

2.5.3 Operational prerequisite

Confirm that the system is not intended to act as a router, gateway, or network device.

2.5.4 Impact

After applying this change, the system will no longer forward traffic between networks.

Applications relying on routing functionality will stop working.

2.5.5 How to implement

Open /etc/sysctl.conf
Set: net.ipv4.ip_forward = 0
Apply settings

2.5.6 How to verify

Run: sysctl net.ipv4.ip_forward

Expected: net.ipv4.ip_forward = 0

3 Conclusion

Based on the systems reviewed the recommendations in this document are intended to reduce unnecessary risk while maintaining the stability of the current environment.

Each item has been selected based on its relevance and potential impact. Not all possible hardening measures have been included, as some changes require further validation or may introduce operational constraints.

If needed, these recommendations can be extended or refined in a next phase, depending on the desired level of security and operational requirements.

Concetti Systems

