Rhel Certification

Objectives

Objectives

Study points

Study points for the exam

RHCSA exam candidates should be able to accomplish the tasks below without assistance. These have been grouped into several categories.

Understand and use essential tools

- Access a shell prompt and issue commands with correct syntax
- Use input-output redirection (>, >>, |, 2>, etc.)
- Use grep and regular expressions to analyze text
- Access remote systems using SSH
- Log in and switch users in multiuser targets
- Archive, compress, unpack, and uncompress files using tar, gzip, and bzip2
- Create and edit text files
- Create, delete, copy, and move files and directories
- Create hard and soft links
- List, set, and change standard ugo/rwx permissions
- Locate, read, and use system documentation including man, info, and files in /usr/share/doc

Manage software

- Configure access to RPM repositories
- Install and remove RPM software packages
- Configure access to Flatpak repositories
- Install and remove Flatpak software packages

Create simple shell scripts

- Conditionally execute code (use of: if, test, [], etc.)
- Use Looping constructs (for, etc.) to process file, command line input
- Process script inputs ($1, $2, etc.)
- Processing output of shell commands within a script

Operate running systems

- Boot, reboot, and shut down a system normally

- Boot systems into different targets manually
- Interrupt the boot process in order to gain access to a system
- Identify CPU/memory intensive processes and kill processes
- Adjust process scheduling
- Manage tuning profiles
- Locate and interpret system log files and journals
- Preserve system journals
- Start, stop, and check the status of network services
- Securely transfer files between systems

Configure local storage

- List, create, delete partitions on GPT disks
- Create and remove physical volumes
- Assign physical volumes to volume groups
- Create and delete logical volumes
- Configure systems to mount file systems at boot by universally unique ID (UUID) or label
- Add new partitions and logical volumes, and swap to a system non-destructively

Create and configure file systems

- Create, mount, unmount, and use VFAT, ext4, and xfs file systems
- Mount and unmount network file systems using NFS
- Configure autofs
- Extend existing logical volumes
- Diagnose and correct file permission problems

Deploy, configure, and maintain systems

- Schedule tasks using at cron and systemd timer units
- Start and stop services and configure services to start automatically at boot
- Configure systems to boot into a specific target automatically
- Configure time service clients
- Install and update software packages from Red Hat Content Delivery Network, a remote repository, or from the local file system
- Modify the system bootloader

Manage basic networking

- Configure IPv4 and IPv6 addresses
- Configure hostname resolution
- Configure network services to start automatically at boot
- Restrict network access using firewalld and firewall-cmd

Manage users and groups

- Create, delete, and modify local user accounts
- Change passwords and adjust password aging for local user accounts
- Create, delete, and modify local groups and group memberships
- Configure privileged access

Manage security

- Configure firewall settings using firewall-cmd/firewalld
- Manage default file permissions
- Configure key-based authentication for SSH
- Set enforcing and permissive modes for SELinux
- List and identify SELinux file and process context
- Restore default file contexts
- Manage SELinux port labels
- Use boolean settings to modify system SELinux settings

As with all Red Hat performance-based exams, configurations must persist after reboot without intervention.

Objectives

Good training link

https://www.devopstraininginstitute.com/blog/how-to-configure-rhel-10-repositories-after-installation

Link contents

How to Configure RHEL 10 Repositories After Installation

Configuring repositories in RHEL 10 after installation is a critical step for ensuring smooth package management, updates, and security patches. This guide explains how to set up official, third-party, and custom repositories for Red Hat Enterprise Linux 10. By following the right configuration process, users can enable faster installations, apply system updates, and integrate tools efficiently. The article also covers troubleshooting common repository issues and maintaining long-term stability in enterprise environments. Designed for beginners and IT professionals alike, this step-by-step approach simplifies repository management and prepares your RHEL 10 system for long-term success.

How to Configure RHEL 10 Repositories After Installation

Table of Contents

Why Configure Repositories After Installation?

Ensuring Immediate System Readiness

Right after installation, a fresh RHEL 10 system may not expose every repository your workloads require, especially across **BaseOS**, **AppStream**, and any specialized add-ons. Configuring repositories immediately guarantees your administrators can install packages, pull updates, and remediate vulnerabilities without delay. It reduces friction in onboarding, aligns development and operations teams on approved sources, and ensures your automation pipelines behave consistently. When repositories are set correctly on day one, environments remain predictable, compliance teams are happier, and engineers aren’t forced into risky one-off downloads that bypass enterprise controls or violate carefully designed governance expectations.

Maintaining Security and Patch Velocity

Security posture depends on timely updates. Proper repository configuration unlocks a steady stream of signed, verified packages from trusted sources, so patch cycles remain fast and predictable. With **dnf** pulling from authenticated repos, you avoid shadow dependencies and unsafe mirrors. Moreover, aligning repos with entitlement scopes prevents accidental exposure to unsupported software. Centralized control over where updates originate allows security teams to audit provenance, measure patch latency, and enforce guardrails. In practice, it means fewer emergency change windows, reduced attack surface, and dependable remediation when vendor advisories land or threat intelligence demands urgent patch rollouts.

Achieving Compliance and Supportability

Many organizations operate under frameworks where provenance, change control, and supportability are non-negotiable. By registering with **subscription-manager** and enabling official repositories, you prove entitlement, maintain compliance, and guarantee access to vendor assistance. Should incidents arise, Red Hat support expects reproducible states backed by supported channels. Proper repository hygiene provides that, minimizing finger-pointing or unsupported configurations. It also enables consistent auditing, since every package and update follows a traceable route. Ultimately, compliance isn’t only about paperwork; it’s a daily practice. Correct repositories transform compliance from a burden into a stable, reliable operating rhythm for teams and systems.

Reducing Operational Friction and Drift

Repository misconfiguration is a common cause of environment drift, where two “identical” servers behave differently. By codifying repository settings from the start, you simplify image builds, golden templates, and configuration management. Teams can pin versions, set priorities, and ensure deterministic upgrades, reducing surprises in testing or production. When CI/CD pipelines run predictable **dnf** transactions, deployments are faster and rollbacks clearer. Moreover, consistent repos streamline collaboration between security, platform, and application teams. Instead of arguing about sources, everyone focuses on delivering features. Less friction across disciplines translates into fewer outages, cleaner incidents, and higher development velocity across portfolios.

What Are RHEL 10 Repositories and How Do They Work?

BaseOS vs AppStream: Complementary Foundations

The **BaseOS** repository delivers the stable core: kernel, core libraries, and essential tooling curated for enterprise reliability. **AppStream** supplies user-space applications and multiple versions via modules, letting teams choose streams that match application lifecycles. Together, they separate the operating system’s bedrock from evolving developer stacks. This division reduces risk while enabling choice. Administrators can lock a module stream for predictability, then advance deliberately. Understanding the distinction helps plan upgrades, validate dependencies, and keep production reproducible. In RHEL 10, these repositories continue reinforcing a balanced model: predictable stability partnered with controlled innovation choices for application teams.

Modularity, Metadata, and Dependency Resolution

Repositories aren’t just file lists; they include metadata that guides **dnf** in resolving dependencies, conflicts, and streams. Modularity allows selecting a supported version of languages or databases without unsafe side-loading. Repository metadata includes checksums, changelogs, and signatures so clients validate integrity during transactions. When **dnf** processes requests, it cross-references repository metadata to construct a coherent plan. This keeps upgrades sane as ecosystems evolve. Without such structure, administrators would juggle fragile dependency trees manually. RHEL 10’s approach simplifies that complexity, balancing convenience with control, paying dividends in stability, repeatability, and confidence during routine maintenance or major refreshes.

GPG Signatures and Trust Chains

Every reputable repository ships packages signed with a **GPG** key. Your client imports the public key and verifies signatures at install and update time, rejecting anything suspicious. This practice establishes a trust chain: you trust the key, the key validates the package, and **dnf** enforces the outcome. Avoid disabling GPG checks; shortcuts invite risk. Instead, rotate keys as needed, document procedures, and store keys securely. Clear key management ensures provenance remains strong. If teams must add third-party repos, insist on GPG validation, revocation awareness, and incident playbooks. Confidence in signatures translates directly into safer, audit-ready production systems.

CDN, Mirroring, and Performance Considerations

Official Red Hat content typically arrives through a global **CDN**, minimizing latency and boosting reliability. Enterprises may additionally maintain internal mirrors to reduce egress costs, protect air-gapped zones, or assure deterministic content. Mirroring introduces operational responsibilities: syncing schedules, bandwidth sizing, and storage governance. Done well, it accelerates patch cadence and avoids external bottlenecks. Pair mirrors with caching, regional placement, and monitoring for throughput and failures. The performance gains are real, but alignment with change windows matters. Treat mirrors as critical infrastructure, with capacity planning, disaster recovery considerations, and well-documented runbooks that platform teams can trust daily.

How to Enable Official RHEL 10 Repositories?

Register the System with Subscription-Manager

Begin by registering the host using **subscription-manager register** and authenticating against your Red Hat account. This step ties the machine to entitlements, enabling access to supported content. If automated, ensure secrets are handled securely through vaults or identity providers. After registration, verify status with **subscription-manager status** so troubleshooting starts from truth. For templated images or autoscaling nodes, bake registration steps into provisioning workflows. The overarching goal is repeatability and compliance: every system should assert entitlement consistently, align with corporate policy, and be ready to consume official repositories without manual exceptions or brittle post-install rituals in production.

Attach Entitlements and Enable Required Repos

Attach a subscription with **subscription-manager attach** or **--auto-attach**, then enable repositories deliberately using **subscription-manager repos --enable=**. Focus on **rhel-10-baseos-rpms** and **rhel-10-appstream-rpms** first, adding others only as justified. Resist enabling everything; less is more for stability. If multiple teams depend on distinct stacks, consider profiles that toggle per-role repositories consistently. Document the mapping so auditors and teammates understand intent. After changes, run **dnf clean all** and **dnf makecache** to refresh metadata, then confirm with **dnf repolist**. These simple verifications catch typos, entitlement drift, and network misrouting before they become puzzling incident tickets.

Verify Connectivity, Proxies, and Certificates

Enterprise networks often introduce proxies, TLS inspection, or route constraints. Configure **dnf.conf** with proxy settings when required, and validate outbound access using **curl** to repository endpoints. Certificate pinning or custom CA chains may be necessary; distribute trust stores through configuration management. If endpoints are egress-filtered, coordinate firewall rules well before maintenance windows. Collect logs from **/var/log/dnf.log** and subscription-manager to speed root-cause analysis. Proactive alignment with networking and security teams prevents surprises. When repositories are business-critical, consider synthetic checks that alert teams if resolution fails, so patching cycles don’t stall quietly behind a misconfigured proxy or expired certificate.

Automate with Ansible and Golden Images

Manual steps don’t scale. Capture repository registration, enablement, and verification in **Ansible** roles or cloud-init scripts. Golden images should include tested repository states, post-provision idempotent checks, and guardrails preventing drift. Add validation tasks that run **dnf repolist**, confirm GPG keys, and enforce desired **dnf.conf** directives. For multi-region fleets, parameterize mirror URLs and priorities. The investment pays off quickly: on-boarding servers is faster, rollbacks are predictable, and compliance reviews become straightforward. Automation also reduces human error, which remains a frequent source of subtle, costly repository defects that only surface during high-pressure release weekends or emergency patch nights.

Where Should You Configure Local or Offline Mirrors?

Deciding When a Mirror Makes Sense

Local mirrors shine when bandwidth is constrained, egress is expensive, or clusters reside in isolated networks. Mirrors also help enforce deterministic content, since you control

synchronization frequency and retention. Evaluate update cadence, scale, and regulatory constraints first. If teams frequently build images or patch large fleets, mirrors markedly reduce external dependencies. Air-gapped environments essentially require mirrors or removable-media repositories. Weigh operational complexity honestly: mirroring introduces jobs, monitoring, and storage overhead. When thoughtfully designed, mirrors bolster speed and resilience, providing a controlled bridge between official content and the unique realities of enterprise connectivity, capacity planning, and governance.

Building and Syncing the Mirror

Implement mirroring with tools that synchronize RPMs and metadata from upstream sources on schedules aligned with change windows. Throttle transfers to avoid saturating links, and perform integrity checks after sync jobs. Retain recent versions prudently; excessive hoarding inflates storage costs. Keep logs for auditing and troubleshooting sync anomalies. Where possible, stage updates in a quarantine area, promote after validation, and document the promotion path. This pipeline prevents surprises and supports rollback if regressions appear. The mirror itself becomes a mini supply chain, so treat it with the same rigor you apply to code repositories: versioning, approvals, and clear ownership.

Serving Content Reliably and Securely

Expose mirrored content through **HTTPS** using hardened web servers, strict TLS policies, and organization-trusted certificates. Restrict access via network segmentation and identity-aware controls if appropriate. Monitor availability and latency, and set alerts for failed syncs or disk pressure. Apply least-privilege to service accounts that manage repository files. If multiple sites consume the mirror, consider geo-distributed replicas with health-based routing. Security teams should periodically penetration-test the mirror surface. Remember, a repository is a software supply chain gateway; compromise here cascades into every dependent system. Stability, visibility, and strong authentication should be first-class design goals, not afterthoughts.

Pointing Clients and Validating Behavior

On clients, create **.repo** definitions under **/etc/yum.repos.d/** pointing to the mirror’s baseurl, add correct **gpgkey** locations, and disable conflicting external repos. Run **dnf clean all** and **dnf makecache** to refresh metadata, then verify with **dnf repolist** and test installs. Observe transaction logs to ensure packages resolve from the mirror, not the internet. Pin priorities so internal sources win. Finally, document the client bootstrap so new nodes reliably adopt the mirror configuration. Clear validation steps help catch subtle issues like stale metadata, wrong key paths, or misaligned priorities that otherwise emerge only during time-critical maintenance windows.

How to Add EPEL and Trusted Third-Party Repositories?

Evaluating External Sources with Policy

Before enabling any external repository, establish a policy that defines acceptable sources, review criteria, and security expectations. Require **GPG** signatures, published SBOMs when available, and transparent vulnerability disclosures. Favor communities with track records of stewardship, timely updates, and reproducible builds. Consider legal licensing implications, export controls, and data residency rules. Keep a register of approved external repositories, their intended use cases, and assigned owners. A small governance investment prevents sprawling, ad-hoc additions that later undermine reliability. When debates arise, let evidence and policy drive decisions, not convenience. It protects platform integrity and avoids costly cleanup efforts later.

Enabling EPEL for Additional Tooling

The **EPEL** repository is a popular, community-maintained source offering well-curated packages not present in official channels. Enable it by installing the EPEL release package appropriate for RHEL 10, importing keys, and confirming with **dnf repolist**. Treat EPEL as additive: use it when justified, avoid blanket installations, and document exceptions. In regulated settings, test updates in a staging environment before promotion. EPEL increases flexibility for developers, but production guidelines should still apply: pin versions where necessary, track changes, and watch for overlap with vendor packages. As with any external source, thoughtful enablement preserves stability alongside greater capability.

Vendor Repositories and Supported Integrations

Some commercial software vendors provide dedicated repositories for their agents, drivers, or management tooling. Prefer these over repackaged variants because support channels align with them. Import vendor **GPG** keys, examine update cadence, and map repos to environments. If a vendor publishes both stable and preview channels, keep preview restricted to labs. Where agents are security-sensitive, validate signatures and checksum policies explicitly. Capture vendor repository configuration in infrastructure-as-code so upgrades don’t drift. When incidents occur, demonstrating that you used the vendor’s certified repository accelerates triage, avoids finger-pointing, and keeps remediation efficient under time pressure.

Pinning, Priorities, and Conflict Avoidance

Conflicts arise when multiple repositories provide the same package. Use **priority** settings in repo files or **dnf** plugins to ensure preferred sources win. Consider **exclude** lists to prevent unwanted

replacements, and use modular streams to lock versions where flexibility exists. In complex estates, publish a matrix documenting which repositories own which packages. This clarity shortens incident calls and reduces accidental regressions. When something must change, write a change request describing impacts and rollback plans. Over time, disciplined pinning eliminates ambiguity, so deployments behave consistently regardless of who executes them or which cluster receives the rollout first.

Managing, Prioritizing, and Disabling Repositories Safely

Listing and Inspecting Repository State

Begin management by listing current state with **dnf repolist** and **dnf repolist all**. These commands distinguish enabled, disabled, and available repositories so drift becomes visible. Export inventories regularly for audits. On change, capture before-and-after diffs so reviewers understand intent. Inspect **/etc/yum.repos.d/** for stray files, verify each entry’s **baseurl** and **gpgkey**, and confirm priorities. Many incidents hide in small typos. Building muscle memory around inspection reduces mean time to recovery. When everything is documented, you empower on-call engineers to act confidently, even if they didn’t design the repository layout originally.

Temporarily Enabling or Disabling for Tasks

Sometimes you need a specific repository only during targeted maintenance. Use **--enablerepo** or **--disablerepo** flags with **dnf** to scope changes to a single transaction. This maintains global hygiene while granting necessary flexibility. After the task, global policy remains intact. Resist permanent changes for short-lived needs; surprises accumulate quickly at scale. If repeated tasks require the same exceptions, encode them as an approved pattern with documentation and guardrails. Principle of least privilege applies to repository exposure too: give processes only what they need, for only as long as they need it, then revert predictably.

Cleaning Metadata and Resolving Staleness

Stale metadata triggers confusing dependency errors and failed upgrades. Clear caches with **dnf clean all**, then rebuild with **dnf makecache**. Automate these steps in maintenance windows or post-enablement workflows. If errors persist, compare client timestamps against mirrors, and check for clock drift that breaks TLS. Consider structured rollouts: stage, validate, then proceed. Document recurrence thresholds that prompt deeper investigation. Healthy metadata pipelines are foundational; they prevent frustrating, late-night incidents where nothing installs, logs are noisy, and confidence evaporates. Treat freshness as a reliability objective that deserves monitoring,

ownership, and timely remediation like any other production signal.

Auditing, Version Pinning, and Documentation

Strong repository practices include periodic audits verifying enabled lists, priorities, and key validity. For critical packages, pin versions or module streams to stabilize behavior across environments. Maintain a living document summarizing repository strategy, ownership, and change rationale. Include incident postmortems to capture lessons. This cultural discipline deters ad-hoc tweaks that cause drift. When auditors arrive or teammates rotate, your estate remains understandable. Version pinning, clear runbooks, and simple diagrams turn repository configuration from an art into a repeatable practice. The payoff is calmer releases, faster onboarding, and fewer ambiguities during escalations, when clear answers matter most.

Informative Table: Repository Types, Scope, Pros, Cons, Tips

At-a-Glance Comparison of Common Repository Options

This table summarizes typical repository choices in RHEL 10 estates, highlighting origin, intended scope, representative contents, advantages, limitations, and practical tips. Use it during design reviews to justify enablement decisions, during incidents to spot conflict sources, and during audits to explain why certain repositories are present while others remain intentionally disabled for safety.

Repository	Origin	Examples	Advantages	Limitations / Tips
BaseOS	Red Hat	Kernel, core utils	Enterprise-grade stability; supported	Foundational only; avoid mixing with unstable sources
AppStream	Red Hat	Languages, databases	Modular streams; choice of versions	Choose streams carefully; standardize across teams
EPEL	Fedora Project	Utilities, tools	Expands capability; active community	Not vendor-supported; test before broad enablement
Vendor Repo	Software vendor	Agents, drivers	Aligned support; timely fixes	Prefer stable channels; validate keys and cadence

Repository	Origin	Examples	Advantages	Limitations / Tips
Internal Mirror	Your org	Curated RPM sets	Deterministic; low egress	Requires ops runbooks; monitor sync health
Testing/Preview	Vendor or community	Pre-release builds	Early features; validation	Not production; isolate to labs and pilots
Custom App Repo	Your org	In-house packages	Compliance control; speed	Document ownership; enforce signing and reviews

Security Hardening for RHEL 10 Repositories

TLS Everywhere and Trusted Proxies

Enforce **HTTPS** on all repository endpoints, including internal mirrors. Harden ciphers, disable legacy protocols, and use certificates from your enterprise trust chain. If egress proxies perform TLS inspection, coordinate certificate distribution and pinning policy. Monitor certificate expiration proactively. Document proxy bypass for patch windows should inspection fail. Security and reliability aren’t adversaries; they’re peers. The goal is encrypted, observable, dependable delivery of packages from origin to host. Avoid plain HTTP entirely. Where legacy tooling lingers, plan remediation. A secure transport layer dramatically reduces interception risks and unlocks confident automation across heterogeneous fleets and geographic boundaries.

GPG Key Lifecycle and Rotation

Treat **GPG** keys as critical secrets with lifecycles: creation, distribution, rotation, and revocation. Store public keys in controlled repositories, validate fingerprints during onboarding, and alert on unexpected key changes. For internal repos, implement signing in CI pipelines so artifacts are trusted by default. Practice key rotation in non-production first, documenting every step. When incidents occur, revocation procedures should be rehearsed, not improvised. Clear ownership and renewal calendars prevent last-minute scrambles. Robust key hygiene is a cornerstone of supply chain security; it reassures auditors and preserves the integrity of installations when pressure is highest.

SELinux Contexts and File Permissions

For on-prem mirrors, ensure repository paths, web roots, and staging areas carry correct **SELinux** contexts and POSIX permissions. A subtle mismatch can break serving or allow unintended writes. Use **restorecon** and policies aligned with your web server. Restrict write access to service accounts, enforce immutable flags on published trees when practical, and maintain separate staging paths. Integrate permission checks into sync jobs. This discipline blocks accidental corruption and raises the bar against tampering. When combined with versioned promotions, SELinux and least-privilege policies build a resilient perimeter around your internal software supply chain surfaces.

Observability, Alerts, and Incident Readiness

Instrument mirrors and clients with telemetry: success rates, latency, error codes, cache hit ratios, and sync durations. Send alerts when **dnf** transactions fail unusually or when mirrors lag beyond thresholds. Keep a runbook covering common failure modes: certificate expiry, DNS drift, proxy outages, and disk pressure. Practice game-days to validate readiness. During incidents, fast, credible signals shorten recovery. Pair metrics with logs from **/var/log/dnf.log** and web servers to correlate symptoms. Observability turns repository health from a guess into a managed SLO, allowing teams to act decisively instead of hunting in the dark during critical windows.

Conclusion

Final Thoughts and Next Steps

Repository configuration in RHEL 10 blends security, performance, and governance into a single practice that shapes everything from patch velocity to developer autonomy. By registering with **subscription-manager**, enabling only necessary repositories, and using internal mirrors wisely, teams reduce drift and boost confidence. Pair that with strong **GPG** policies, TLS everywhere, and clear priorities to avoid conflicts. Encode the strategy in automation, validate with observability, and document the why behind each decision. Do this well, and updates stop being stressful events and become routine. Your systems stay resilient, your audits stay calm, and your engineers stay productive.

Frequently Asked Questions (FAQs)

What is the practical difference between BaseOS and AppStream in RHEL 10?

BaseOS provides core, highly stable operating system packages, while **AppStream** delivers user-space software and modular streams offering multiple supported versions. BaseOS underpins reliability; AppStream enables controlled choice. Together, they separate foundational stability from flexible application stacks, simplifying upgrades, dependency management, and long-term lifecycle planning across environments.

Why should I avoid disabling GPG checks when installing packages?

Disabling **GPG** checks removes cryptographic verification that packages come from trusted sources and remain unaltered. It may temporarily “fix” an install but creates dangerous exposure. The safer route is importing the correct keys, validating fingerprints, and correcting repository configuration so security and reliability remain intact during transactions.

How do I confirm which repositories are currently enabled on a host?

Use **dnf repolist** to show enabled repositories and **dnf repolist all** for a complete view. Review entries under **/etc/yum.repos.d/** and confirm each **baseurl**, **gpgkey**, and priority. Exporting these results regularly supports audits, detects drift early, and gives on-call engineers fast context during incidents.

What steps help troubleshoot “Cannot find a valid baseurl” errors?

Validate network connectivity, DNS resolution, and proxy settings; test endpoints with **curl**. Confirm repository URLs, entitlement status in **subscription-manager**, and certificate trust chains. Clear caches using **dnf clean all**, rebuild with **dnf makecache**, then recheck. Many cases trace to typos, stale metadata, or proxy misconfigurations.

When is it appropriate to introduce a local mirror into the architecture?

Introduce mirrors for bandwidth savings, air-gapped environments, or deterministic content needs. They reduce external dependencies and speed patching for large fleets. Balance benefits against operational overhead: synchronization jobs, storage, monitoring, and promotions. Well-run mirrors improve reliability, but they require ownership, documentation, and thoughtful integration with change windows.

How should I evaluate whether a third-party repository is trustworthy?

Require **GPG** signatures, transparent maintenance history, timely updates, clear licensing, and reliable documentation. Favor communities or vendors with established governance and predictable release processes. Pilot in non-production, monitor for regressions, and document approval. A lightweight policy prevents ad-hoc enablement that later undermines stability or compliance goals.

What is the recommended way to enable EPEL on RHEL 10?

Install the appropriate EPEL release package for RHEL 10, import its **GPG** key, then verify presence with **dnf repolist**. Use EPEL selectively, documenting intended packages and environments. Test updates in staging before production, and avoid blanket installs. Treat EPEL as additive flexibility, not a replacement for vendor channels.

Can I prioritize internal mirrors over external repositories in resolution?

Yes. Configure repository **priority** values so internal mirrors outrank external sources. You can also use **exclude** directives to block unwanted replacements. Confirm behavior by inspecting transaction output and logs. Clear priorities reduce conflicts, minimize surprises, and ensure packages consistently originate from the sources your policy intends.

How do I temporarily use a repository for a single operation only?

Use **dnf** flags such as **--enablerepo** or **--disablerepo** to scope changes to one transaction. This approach grants situational flexibility without altering global configuration. It’s ideal for exceptional maintenance tasks. After completion, global policy remains intact, respecting least privilege and preventing gradual sprawl of persistent exceptions.

What signals indicate stale metadata is causing installation failures?

Repeated dependency resolution errors, missing packages you expect, or inconsistent results across similar hosts are clues. Flush caches with **dnf clean all**, rebuild with **dnf makecache**, and

compare timestamps. If issues persist, inspect mirror health, clock drift, and proxy behavior. Healthy metadata pipelines keep transactions predictable.

How do I enable optional repositories in a supported manner?

Attach entitlements with **subscription-manager**, then enable targeted repos using **subscription-manager repos --enable=**. Avoid enabling broad sets indiscriminately. Document purpose and owners for each repository, refresh caches, and validate with **dnf repolist**. Scoped enablement preserves stability and makes later audits faster and more transparent.

Why does subscription-manager remain central to enterprise support?

subscription-manager proves entitlement, aligns repository access with licensed content, and simplifies support interactions. When incidents occur, support teams rely on reproducible, compliant configurations. Centralized control reduces drift, clarifies provenance, and keeps estates audit-ready. It’s a cornerstone of predictable, supportable operations in regulated or scaled environments.

Can I configure local repositories for fully offline RHEL 10 hosts?

Yes. Mirror required content onto secure storage, serve it internally over hardened **HTTPS**, or provide removable-media repositories. Create client **.repo** files pointing to those sources, import matching keys, and validate transactions. Offline workflows demand rigorous processes for sync, promotion, and documentation to preserve integrity.

What benefits do custom internal repositories provide teams?

Custom repos centralize in-house packages, enforce signing, and streamline rollout of organization-specific tooling. They reduce internet dependency, accelerate deployments, and keep compliance tidy. Ownership is clear, promotion paths are documented, and incident response is faster because provenance is unambiguous. It’s a pragmatic foundation for enterprise software delivery.

How should I approach persistent repository configuration errors?

Work methodically: validate URLs, entitlements, proxies, and certificates; clear caches; compare behavior across a healthy reference host. Inspect logs, then reduce variables by disabling nonessential repos temporarily. If necessary, rebuild **.repo** files from known-good templates. Methodical isolation shortens time to resolution and avoids speculative changes.

What is EPEL’s role relative to official Red Hat channels?

EPEL adds community-maintained packages that complement, not replace, Red Hat repositories. It’s valuable for tools absent from vendor channels. Treat EPEL as optional, test thoroughly, and document usage boundaries. When vendor support is essential, prefer official repositories or vendor-provided repos aligned with contractual support obligations.

Is it safe to disable repositories I no longer need?

Yes, disabling reduces attack surface and conflict risk. Use **subscription-manager repos --disable** or set **enabled=0** in repo files. Document rationale, confirm no dependencies remain, and clean caches. Periodic pruning helps estates stay understandable, compliant, and efficient, especially during audits and platform migrations.

Why is GPG key hygiene emphasized so strongly?

GPG keys prove package authenticity. Strong hygiene—verified fingerprints, secure storage, rotation, and revocation—prevents tampering from masquerading as legitimate updates. Skipping checks trades short-term convenience for high risk. Treat keys like crown jewels: guard them, audit them, and practice rotation so emergency responses are smooth.

How do repositories influence patch management success rates?

Repositories define the universe of eligible updates and their trust guarantees. Clean, prioritized, and monitored repos produce predictable, high-success patch cycles. Misconfigured or conflicting sources yield failures, regressions, and firefighting. Investing in repository discipline pays compounding dividends across every maintenance window your organization executes.

What ongoing practices keep repository management healthy?

Audit enabled repos, verify keys, enforce priorities, and monitor sync health. Automate registration and validation, pin critical versions, and document exceptions. Combine observability with incident playbooks and runbooks. Above all, favor simplicity: fewer, clearer repositories outperform sprawling, ad-hoc collections in stability, security, and operational clarity.

Networking

Networking

Network info from google

n Red Hat Enterprise Linux (RHEL) 10, manage basic networking primarily using nmcli (command-line) or nmtui (text interface) to control NetworkManager. Key changes include the removal of `ifcfg` file support, favoring key files in `/etc/NetworkManager/system-connections/`. The `dhclient` tool is also replaced by an internal DHCP client.

Key Networking Commands and Tasks (RHEL 10)

- **View Network Status:**
  - `ip a`: View IP addresses and interface status.
  - `nmcli device status`: Check device states.
  - `nmcli connection show`: List active network profiles.
- **Configure Networking (DHCP):**
  - `nmtui`: Open the text-based user interface to edit connections.
  - `nmcli con add type ethernet con-name <name> ifname <interface>`: Create a new DHCP connection.
- **Configure Static IP:**
  - `nmcli con mod <connection> ipv4.addresses <ip/mask> ipv4.gateway <gateway> ipv4.method manual`: Sets static IP.
  - `nmcli con mod <connection> ipv4.dns "8.8.8.8"`: Sets DNS servers.
  - `nmcli con up <connection>`: Apply changes.
- **Troubleshooting:**
  - `ping <host>`: Test connectivity.
  - `ip route`: View routing table.
  - `nmcli dev connect <interface>`: Reconnect an interface.
- **Hostname:**
  - `hostnamectl set-hostname <new_name>`: Change the system hostname.

RHEL 10 fully deprecates the older `/etc/sysconfig/network-scripts/` format. Always use `nmcli` or `nmtui` to ensure configurations are properly saved in the new key file format.

Reh Hat docs on networking

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10/html/configuring_and_managing_networking/index

Configuring an Ethernet connection by using nmcli

2.1. Configuring an Ethernet connection by using nmcli

Copy link

If you connect a host to the network over Ethernet, you can manage the connection's settings on the command line by using the `nmcli` utility.

Prerequisites

- A physical or virtual Ethernet Network Interface Controller (NIC) exists in the server's configuration.

Procedure

1. List the NetworkManager connection profiles:

```
# nmcli connection show
NAME                UUID                                  TYPE      DEVICE
Wired connection 1  a5eb6490-cc20-3668-81f8-0314a27f3f75  ethernet  enp1s0
```

   By default, NetworkManager creates a profile for each NIC in the host. If you plan to connect this NIC only to a specific network, adapt the automatically-created profile. If you plan to connect this NIC to networks with different settings, create individual profiles for each network.
2. If you want to create an additional connection profile, enter:

```
# nmcli connection add con-name <connection-name> ifname <device-name> type ethernet
```

   Skip this step to modify an existing profile.
3. Optional: Rename the connection profile:

```
# nmcli connection modify "Wired connection 1" connection.id "Internal-LAN"
```

On hosts with multiple profiles, a meaningful name makes it easier to identify the purpose of a profile.

4. Display the current settings of the connection profile:

```
# nmcli connection show Internal-LAN
...
connection.interface-name:     enp1s0
connection.autoconnect:        yes
ipv4.method:                   auto
ipv6.method:                   auto
...
```

5. Configure the IPv4 settings:
   - To use DHCP, enter:

     ```
     # nmcli connection modify Internal-LAN ipv4.method auto
     ```

     Skip this step if `ipv4.method` is already set to `auto` (default).
   - To set a static IPv4 address, network mask, default gateway, DNS servers, and search domain, enter:

     ```
     # nmcli connection modify Internal-LAN ipv4.method manual ipv4.addresses 192.0.2.1/24 ipv4.gateway 192.0.2.254 ipv4.dns 192.0.2.200 ipv4.dns-search example.com
     ```

6. Configure the IPv6 settings:
   - To use stateless address autoconfiguration (SLAAC), enter:

     ```
     # nmcli connection modify Internal-LAN ipv6.method auto
     ```

     Skip this step if `ipv6.method` is already set to `auto` (default).
   - To set a static IPv6 address, network mask, default gateway, DNS servers, and search domain, enter:

     ```
     # nmcli connection modify Internal-LAN ipv6.method manual ipv6.addresses 2001:db8:1::fffe/64 ipv6.gateway 2001:db8:1::fffe ipv6.dns 2001:db8:1::ffbb ipv6.dns-search example.com
     ```

7. To customize other settings in the profile, use the following command:

```
# nmcli connection modify <connection-name> <setting> <value>
```

Enclose values with spaces or semicolons in quotes.

For details about which settings you can modify, see the `nm-settings(5)` man page on your system.

8. Activate the profile:

```
# nmcli connection up Internal-LAN
```

Verification

1. Display the IP settings of the NIC:

```
# ip address show enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 52:54:00:17:b8:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.1/24 brd 192.0.2.255 scope global noprefixroute enp1s0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:1::fffe/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
```

2. Display the IPv4 default gateway:

```
# ip route show default
default via 192.0.2.254 dev enp1s0 proto static metric 102
```

3. Display the IPv6 default gateway:

```
# ip -6 route show default
default via 2001:db8:1::fffe dev enp1s0 proto static metric 102 pref medium
```

4. Display the DNS settings:

```
# cat /etc/resolv.conf
search example.com
nameserver 192.0.2.200
nameserver 2001:db8:1::ffbb
```

If multiple connection profiles are active at the same time, the order of `nameserver` entries depend on the DNS priority values in these profiles and the connection types.

5. Use the `ping` utility to verify that this host can send packets to other hosts:

```
# ping <host-name-or-IP-address>
```

Troubleshooting

- Verify that the network cable is plugged-in to the host and a switch.

- Check whether the link failure exists only on this host or also on other hosts connected to the same switch.
- Verify that the network cable and the network interface are working as expected. Perform hardware diagnosis steps and replace defective cables and network interface cards.
- If the configuration on the disk does not match the configuration on the device, starting or restarting NetworkManager creates an in-memory connection that reflects the configuration of the device. For further details and how to avoid this problem, see the Red Hat Knowledgebase solution NetworkManager duplicates a connection after restart of NetworkManager service.

Configuring an Ethernet connection by using nmtui

If you connect a host to an Ethernet network, you can manage the connection's settings in a text-based user interface. Use the `nmtui` application to create new profiles and to update existing ones on a host without a graphical interface.

Note

In `nmtui`:

- Navigate by using the cursor keys.
- Press a button by selecting it and hitting `Enter`.
- Select and clear checkboxes by using `Space`.
- To return to the previous screen, use `ESC`.

Prerequisites

- A physical or virtual Ethernet Network Interface Controller (NIC) exists in the server's configuration.

Procedure

1. If you do not know the network device name you want to use in the connection, display the available devices:

```
# nmcli device status
DEVICE     TYPE      STATE                   CONNECTION
enp1s0     ethernet  unavailable             --
...
```

2. Start `nmtui`:

```
# nmtui
```

3. Select **Edit a connection**, and press `Enter`.
4. Choose whether to add a new connection profile or to modify an existing one:
   - To create a new profile:
     1. Press **Add**.

2. Select **Ethernet** from the list of network types, and press `Enter`.

- To modify an existing profile, select the profile from the list, and press `Enter`.

5. Optional: Update the name of the connection profile.
   On hosts with multiple profiles, a meaningful name makes it easier to identify the purpose of a profile.
6. If you create a new connection profile, enter the network device name into the **Device** field.
7. Depending on your environment, configure the IP address settings in the `IPv4 configuration` and `IPv6 configuration` areas accordingly. For this, press the button next to these areas, and select:
   - **Disabled**, if this connection does not require an IP address.
   - **Automatic**, if a DHCP server dynamically assigns an IP address to this NIC.
   - **Manual**, if the network requires static IP address settings. In this case, you must fill further fields:
     1. Press **Show** next to the protocol you want to configure to display additional fields.
     2. Press **Add** next to **Addresses**, and enter the IP address and the subnet mask in Classless Inter-Domain Routing (CIDR) format.
        If you do not specify a subnet mask, NetworkManager sets a `/32` subnet mask for IPv4 addresses and `/64` for IPv6 addresses.
     3. Enter the address of the default gateway.
     4. Press **Add** next to **DNS servers**, and enter the DNS server address.
     5. Press **Add** next to **Search domains**, and enter the DNS search domain.

   Figure 2.1. Example of an Ethernet connection with static IP address settings
   Static IP address settings in `nmtui`
8. Press **OK** to create and automatically activate the new connection.
9. Press **Back** to return to the main menu.
10. Select **Quit**, and press `Enter` to close the `nmtui` application.

Verification

1. Display the IP settings of the NIC:

```
# ip address show enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 52:54:00:17:b8:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.1/24 brd 192.0.2.255 scope global noprefixroute enp1s0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:1::fffe/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
```

2. Display the IPv4 default gateway:

```
# ip route show default
default via 192.0.2.254 dev enp1s0 proto static metric 102
```

3. Display the IPv6 default gateway:

```
# ip -6 route show default
default via 2001:db8:1::fffe dev enp1s0 proto static metric 102 pref medium
```

4. Display the DNS settings:

```
# cat /etc/resolv.conf
search example.com
nameserver 192.0.2.200
nameserver 2001:db8:1::ffbb
```

   If multiple connection profiles are active at the same time, the order of `nameserver` entries depend on the DNS priority values in these profiles and the connection types.

5. Use the `ping` utility to verify that this host can send packets to other hosts:

```
# ping <host-name-or-IP-address>
```

Troubleshooting

- Verify that the network cable is plugged-in to the host and a switch.
- Check whether the link failure exists only on this host or also on other hosts connected to the same switch.
- Verify that the network cable and the network interface are working as expected. Perform hardware diagnosis steps and replace defective cables and network interface cards.
- If the configuration on the disk does not match the configuration on the device, starting or restarting NetworkManager creates an in-memory connection that reflects the configuration of the device. For further details and how to avoid this problem, see the Red Hat Knowledgebase solution NetworkManager duplicates a connection after restart of NetworkManager service.

Configuring an Ethernet connection by using control-center

Copy link

If you connect a host to the network over Ethernet, you can manage the connection's settings with a graphical interface by using the GNOME Settings menu.

Note that `control-center` does not support as many configuration options as the `nmcli` utility.

Prerequisites

- A physical or virtual Ethernet Network Interface Controller (NIC) exists in the server's configuration.
- GNOME is installed.

Procedure

1. Press the Super key, enter `Settings`, and press `Enter`.
2. Select **Network** in the navigation on the left.
3. Choose whether to add a new connection profile or to modify an existing one:
    - To create a new profile, click the + button next to the **Ethernet** entry.
    - To modify an existing profile, click the gear icon next to the profile entry.
4. Optional: On the **Identity** tab, update the name of the connection profile.
   On hosts with multiple profiles, a meaningful name makes it easier to identify the purpose of a profile.
5. Depending on your environment, configure the IP address settings on the **IPv4** and **IPv6** tabs accordingly:
    - To use DHCP or IPv6 stateless address autoconfiguration (SLAAC), select `Automatic (DHCP)` as method (default).
    - To set a static IP address, network mask, default gateway, DNS servers, and search domain, select `Manual` as method, and fill the fields on the tabs:
      Static IP address settings in `control-center`

6. Depending on whether you add or modify a connection profile, click the Add or Apply button to save the connection.
   The GNOME `control-center` automatically activates the connection.

Verification

1. Display the IP settings of the NIC:

```
# ip address show enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 52:54:00:17:b8:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.1/24 brd 192.0.2.255 scope global noprefixroute enp1s0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:1::fffe/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
```

2. Display the IPv4 default gateway:

```
# ip route show default
default via 192.0.2.254 dev enp1s0 proto static metric 102
```

3. Display the IPv6 default gateway:

```
# ip -6 route show default
default via 2001:db8:1::fffe dev enp1s0 proto static metric 102 pref medium
```

4. Display the DNS settings:

```
# cat /etc/resolv.conf
search example.com
nameserver 192.0.2.200
nameserver 2001:db8:1::ffbb
```

   If multiple connection profiles are active at the same time, the order of `nameserver` entries depend on the DNS priority values in these profiles and the connection types.
5. Use the `ping` utility to verify that this host can send packets to other hosts:

```
# ping <host-name-or-IP-address>
```

Troubleshooting steps

- Verify that the network cable is plugged-in to the host and a switch.
- Check whether the link failure exists only on this host or also on other hosts connected to the same switch.

- Verify that the network cable and the network interface are working as expected. Perform hardware diagnosis steps and replace defective cables and network interface cards.
- If the configuration on the disk does not match the configuration on the device, starting or restarting NetworkManager creates an in-memory connection that reflects the configuration of the device. For further details and how to avoid this problem, see the Red Hat Knowledgebase solution NetworkManager duplicates a connection after restart of NetworkManager service.

Configuring an Ethernet connection with a static IP address by using nmstatectl with an interface name

You can use the declarative Nmstate API to configure an Ethernet connection with static IP addresses, gateways, and DNS settings, and assign them to a specified interface name. Nmstate ensures that the result matches the configuration file or rolls back the changes.

Prerequisites

- A physical or virtual Ethernet Network Interface Controller (NIC) exists in the server's configuration.
- The `nmstate` package is installed.

Procedure

1. Create a YAML file, for example `~/create-ethernet-profile.yml`, with the following content:

```
---
interfaces:
- name: enp1s0
  type: ethernet
  state: up
  ipv4:
    enabled: true
    address:
    - ip: 192.0.2.1
      prefix-length: 24
    dhcp: false
  ipv6:
    enabled: true
```

```
    address:
    - ip: 2001:db8:1::1
      prefix-length: 64
    autoconf: false
    dhcp: false
routes:
  config:
  - destination: 0.0.0.0/0
    next-hop-address: 192.0.2.254
    next-hop-interface: enp1s0
  - destination: ::/0
    next-hop-address: 2001:db8:1::fffe
    next-hop-interface: enp1s0
dns-resolver:
  config:
    search:
    - example.com
    server:
    - 192.0.2.200
    - 2001:db8:1::ffbb
```

These settings define an Ethernet connection profile for the `enp1s0` device with the following settings:

- A static IPv4 address - `192.0.2.1` with the `/24` subnet mask
- A static IPv6 address - `2001:db8:1::1` with the `/64` subnet mask
- An IPv4 default gateway - `192.0.2.254`
- An IPv6 default gateway - `2001:db8:1::fffe`
- An IPv4 DNS server - `192.0.2.200`
- An IPv6 DNS server - `2001:db8:1::ffbb`
- A DNS search domain - `example.com`

2. Optional: You can define the `identifier: mac-address` and `mac-address: <mac_address>` properties in the `interfaces` property to identify the network interface card by its MAC address instead of its name, for example:

```
---
interfaces:
- name: <profile_name>
  type: ethernet
  identifier: mac-address
  mac-address: <mac_address>
  ...
```

3. Apply the settings to the system:

```
# nmstatectl apply ~/create-ethernet-profile.yml
```

Verification

1. Display the current state in YAML format:

```
# nmstatectl show enp1s0
```

2. Display the IP settings of the NIC:

```
# ip address show enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 52:54:00:17:b8:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.1/24 brd 192.0.2.255 scope global noprefixroute enp1s0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:1::fffe/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
```

3. Display the IPv4 default gateway:

```
# ip route show default
default via 192.0.2.254 dev enp1s0 proto static metric 102
```

4. Display the IPv6 default gateway:

```
# ip -6 route show default
default via 2001:db8:1::fffe dev enp1s0 proto static metric 102 pref medium
```

5. Display the DNS settings:

```
# cat /etc/resolv.conf
search example.com
nameserver 192.0.2.200
nameserver 2001:db8:1::ffbb
```

   If multiple connection profiles are active at the same time, the order of `nameserver` entries depend on the DNS priority values in these profiles and the connection types.

6. Use the `ping` utility to verify that this host can send packets to other hosts:

```
# ping <host-name-or-IP-address>
```