System Access, Repositories, and Network Configuration

This work documents the configuration and validation of core Linux services required for secure access, reliable package management, and stable network functionality on a CentOS Stream–based system.

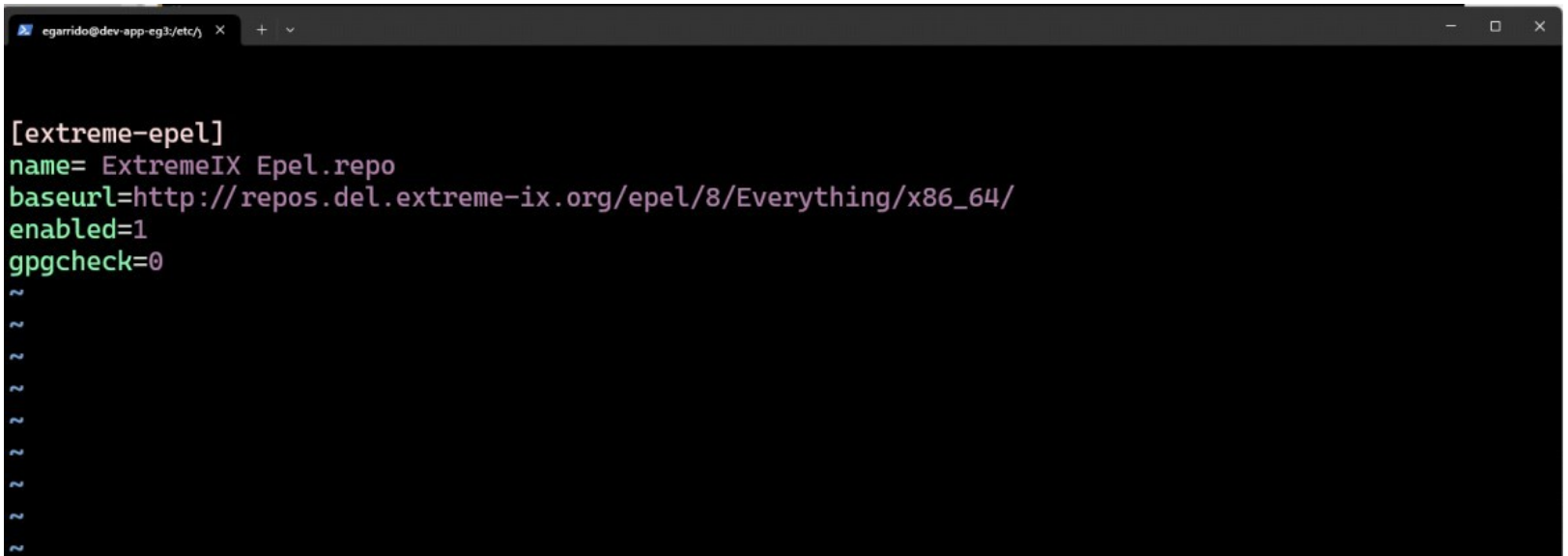
SSH access and firewall rules are verified to ensure secure and persistent remote connectivity. External repositories are added and validated, with connectivity checks confirming successful access to external mirrors and proper DNF repository loading. Package installation testing confirms repository health and dependency resolution.

Network configuration is finalized by validating DNS resolver settings managed by NetworkManager, including search domains and redundant name servers to ensure consistent hostname resolution across the environment.

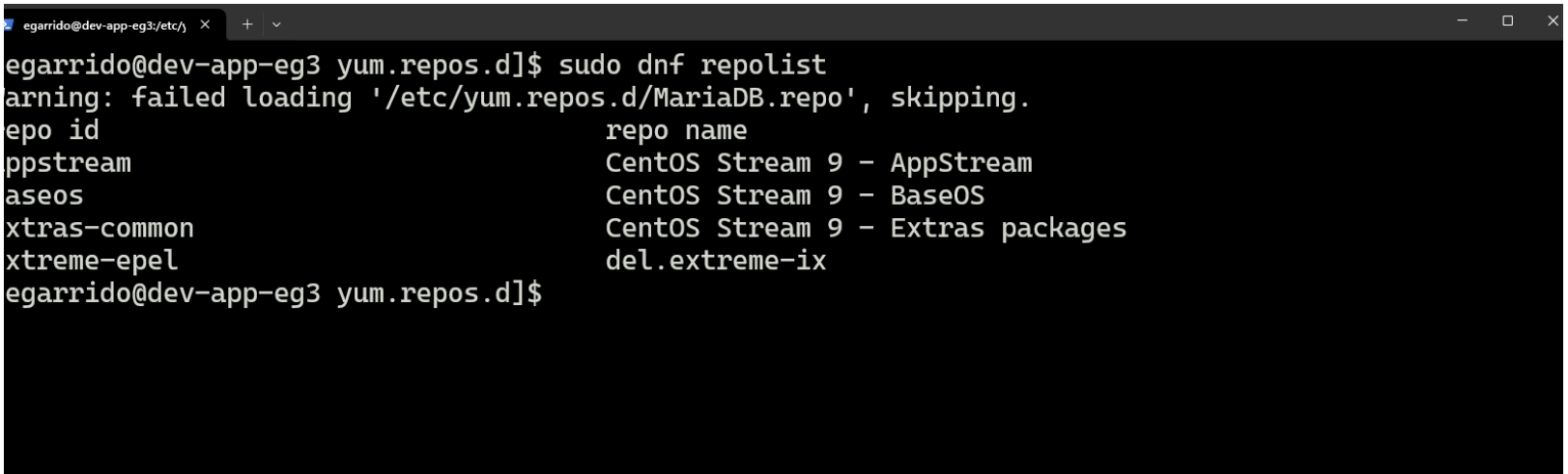
Result:

A production-ready system with secure remote access, functional package repositories, confirmed external connectivity, and reliable DNS resolution.

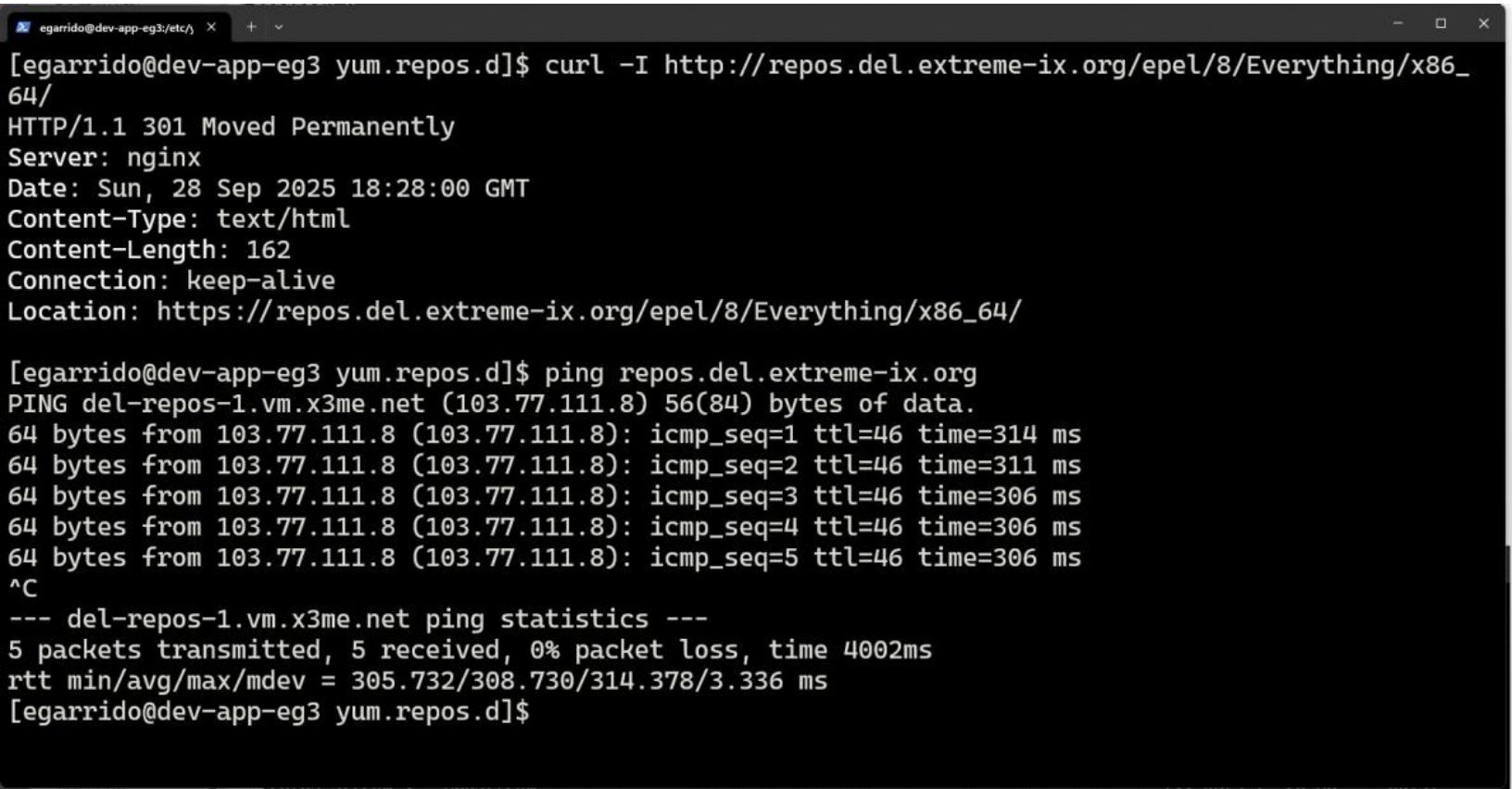
This configuration shows a custom EPEL repository definition being added to the system package manager. The repository is enabled and points to an external mirror providing additional packages not included in the default distribution repositories. This setup extends package availability for the system while maintaining compatibility with the underlying OS architecture.



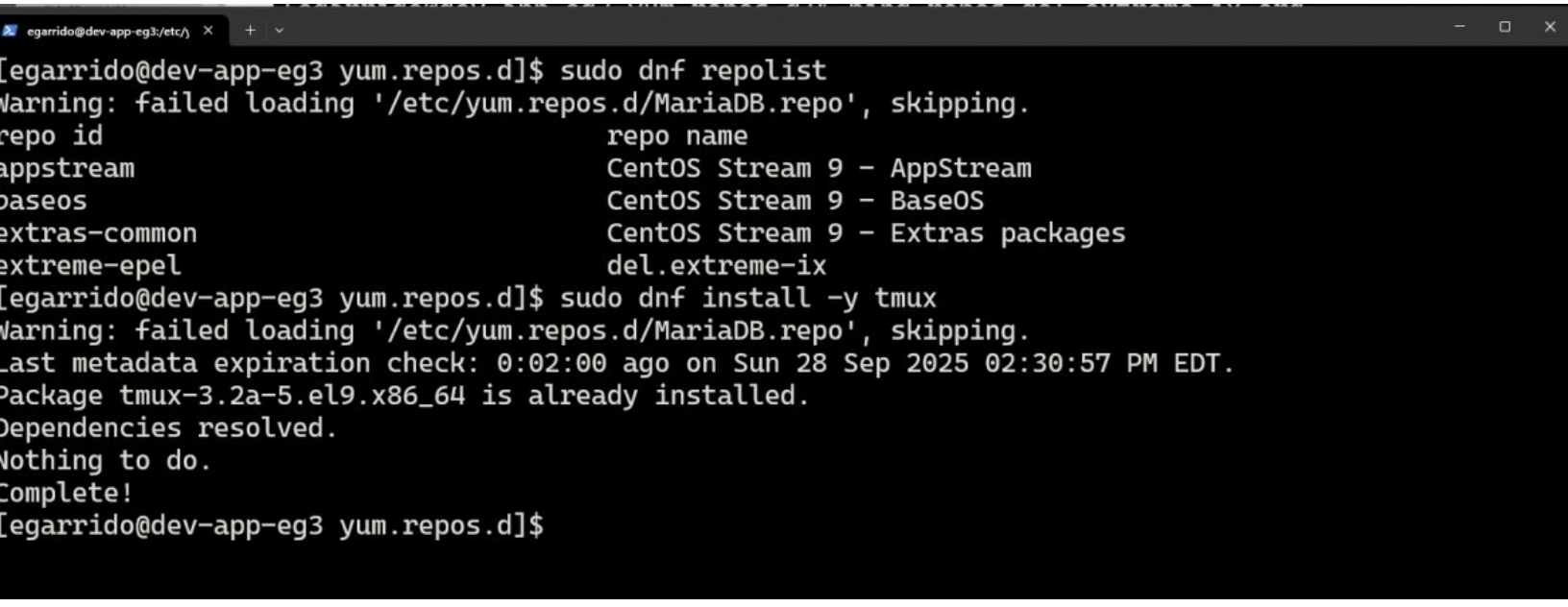
This output verifies the currently enabled DNF repositories on the system. The default CentOS Stream 9 repositories (BaseOS, AppStream, and Extras) are active, along with a custom external EPEL repository. The repository list confirms that the package manager is correctly recognizing and loading the configured repositories, ensuring access to both core system packages and extended software sources.



This step validates network connectivity and availability of the external EPEL repository source. An HTTP header check confirms the repository endpoint is reachable and properly redirects from HTTP to HTTPS, indicating correct server response and secure access. ICMP testing verifies consistent network connectivity to the repository host with zero packet loss, confirming that the system can reliably reach the external mirror for package retrieval.



This step verifies that the configured DNF repositories are accessible and functional by querying the active repository list and performing a package installation check. The output confirms that the system successfully recognizes the default CentOS Stream repositories along with the external EPEL source. A test installation of the tmux package confirms repository availability and dependency resolution, indicating that the package management configuration is working as expected.



This configuration shows the system DNS resolver settings generated by NetworkManager. A search domain is defined to support internal hostname resolution, and multiple name servers are configured to provide redundancy and reliable DNS lookup. This setup ensures consistent name resolution for services within the environment while allowing NetworkManager to maintain the configuration dynamically.

Summary

This work validates secure system access, repository availability, and network configuration on a CentOS Stream–based server. SSH access and firewall rules are confirmed to support secure remote connectivity. External repositories are added and verified, with connectivity checks and package installation confirming proper DNF functionality and dependency resolution. DNS resolver settings managed by NetworkManager are validated to ensure reliable internal and external name resolution.

Outcome:

A stable, production-ready system with secure access, functional package management, verified external connectivity, and consistent DNS resolution.