Enterprise Linux Host Hardening and Automation Readiness

This project documents the standardized configuration and security hardening of multiple Linux hosts across development, performance, and staging environments in an enterprise-style infrastructure.

All systems are deployed on vSphere and run CentOS Stream 9, with operating system versions verified prior to configuration. Hostnames, networking, and system identity are aligned to ensure consistency with centralized services and automation tooling.

A major focus of this work is secure remote access. SSH is hardened on every host by disabling direct root login, enforcing strict authentication controls, and validating daemon configuration after each change. Password and key-based authentication behavior is explicitly reviewed to align with organizational security standards.

Network access is further restricted using firewalld. Default SSH services and broad port rules are removed, and access is constrained using targeted rules that allow administrative connectivity only from trusted network ranges. These controls are applied consistently across application, performance, stage web, and automation hosts, demonstrating repeatable security enforcement.

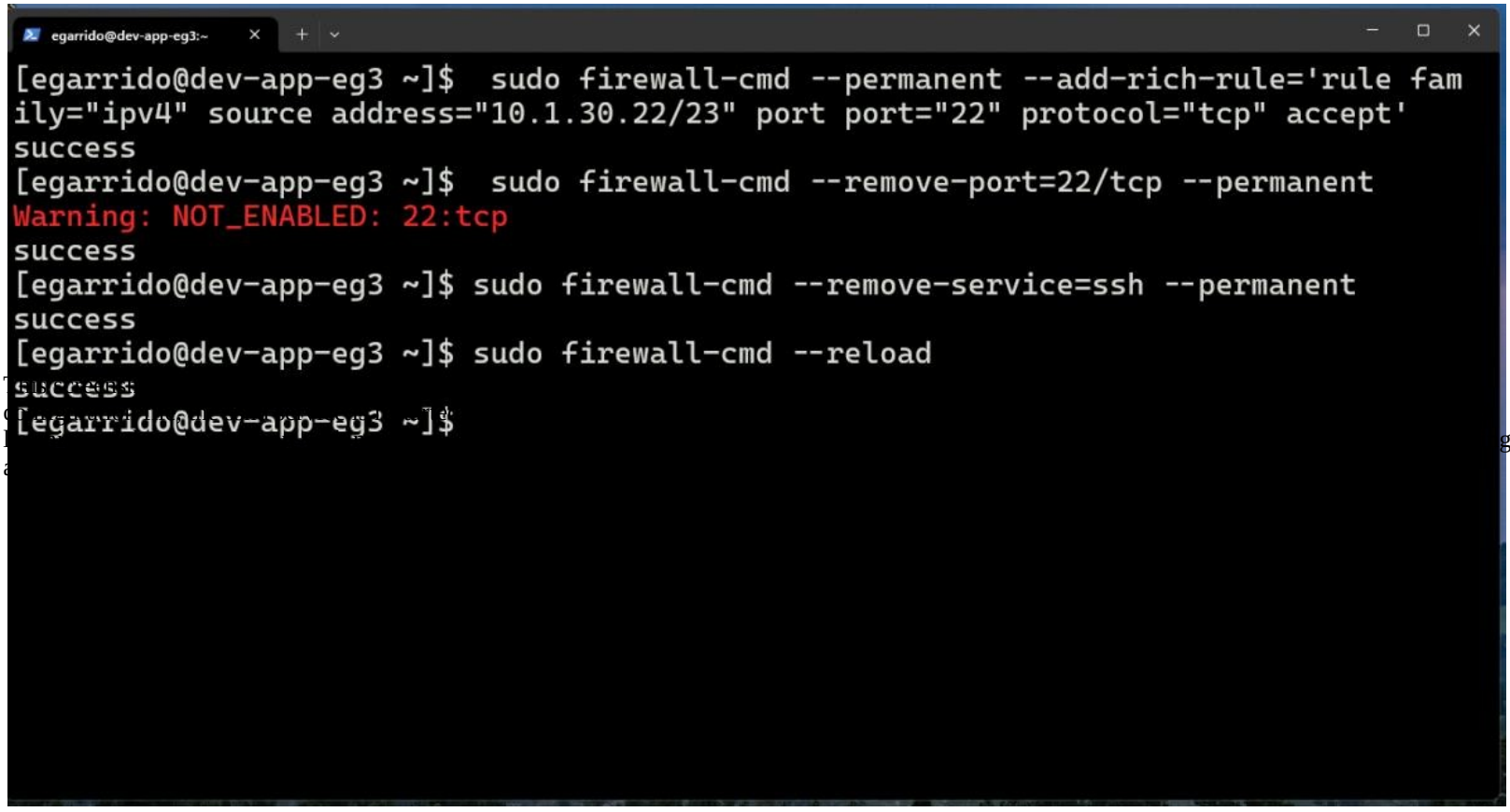
To support automation, SSH key-based trust is established bidirectionally between hosts, enabling passwordless access where appropriate. Host key conflicts and trust issues are identified, corrected, and validated to ensure reliable remote execution.

Connectivity and readiness for automation are verified using Ansible, confirming that all hardened hosts remain reachable and correctly configured for managed operations.

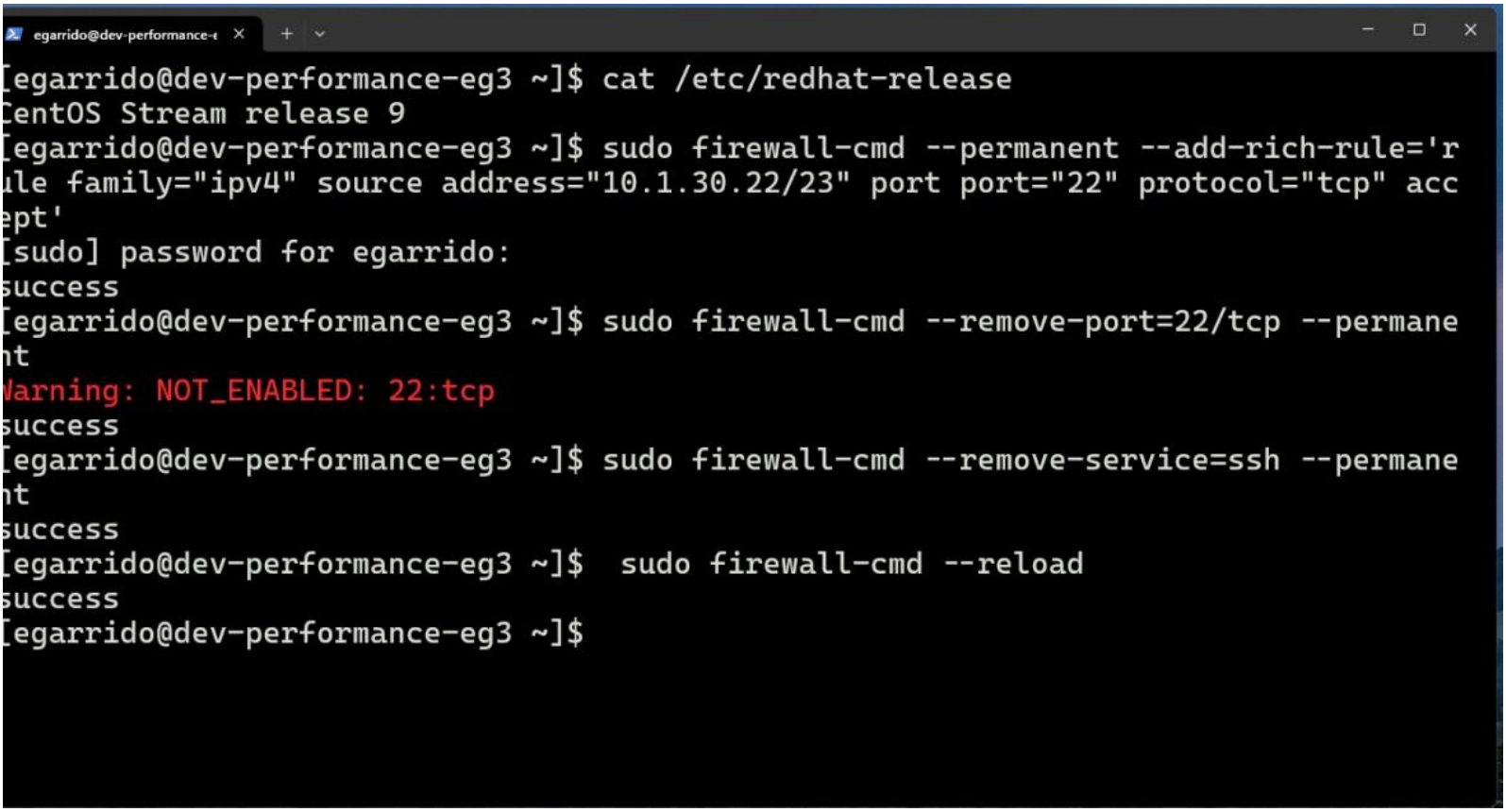
Security & Sanitization Notice

All IP addresses, hostnames, usernames, network ranges, timestamps, and environment-specific identifiers shown in screenshots, command output, and configuration files have been sanitized or obfuscated. No production credentials or sensitive infrastructure data are exposed in this repository.

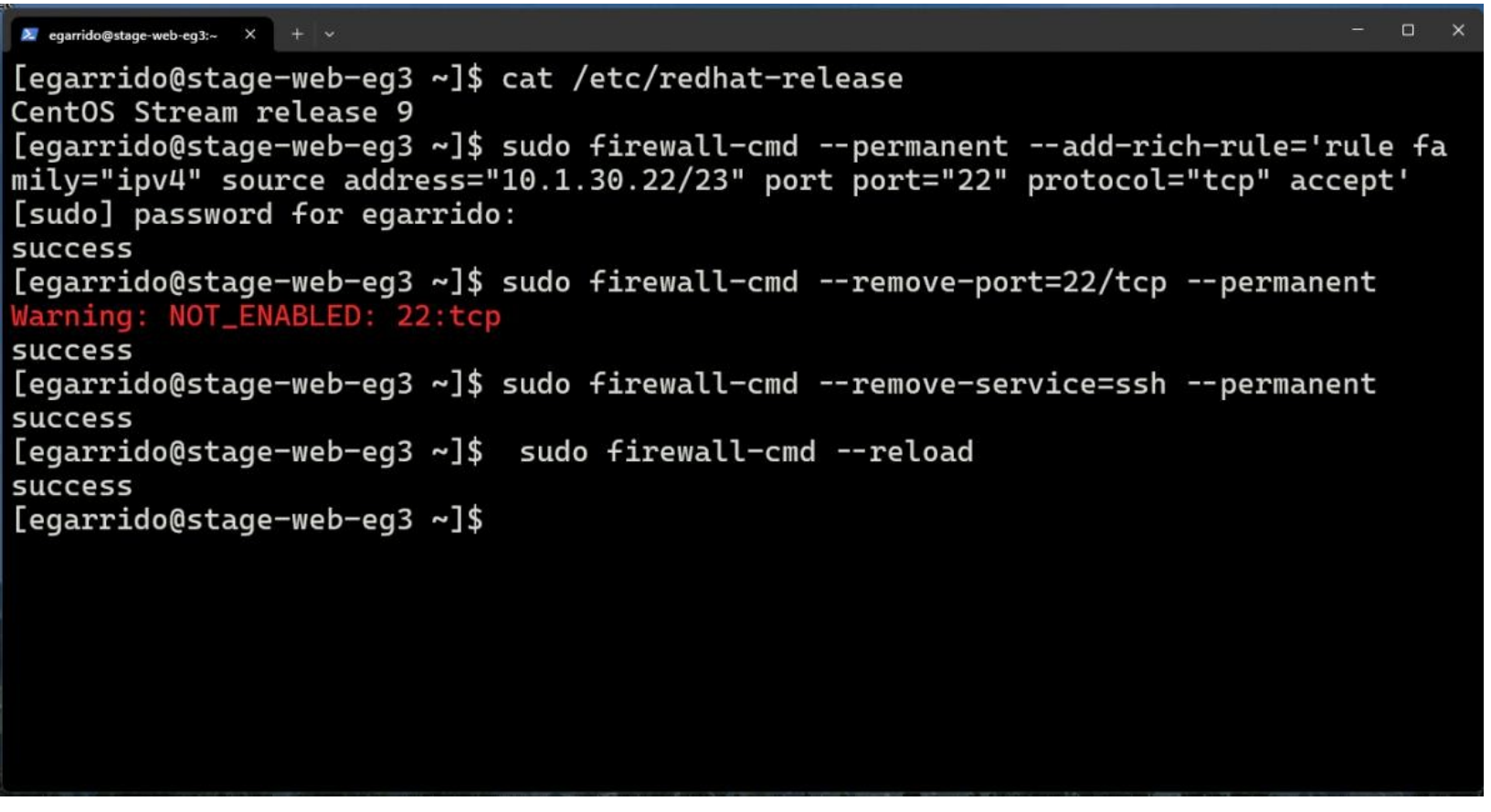
This screenshot shows firewalld hardening and SSH access restriction on the application server. A rich rule is added to permanently allow SSH (TCP port 22) only from a specific trusted subnet, replacing broad access. Default SSH service and open port rules are then removed to eliminate unrestricted exposure, and the firewall configuration is reloaded to apply the changes. This enforces least-privilege network access while maintaining required administrative connectivity



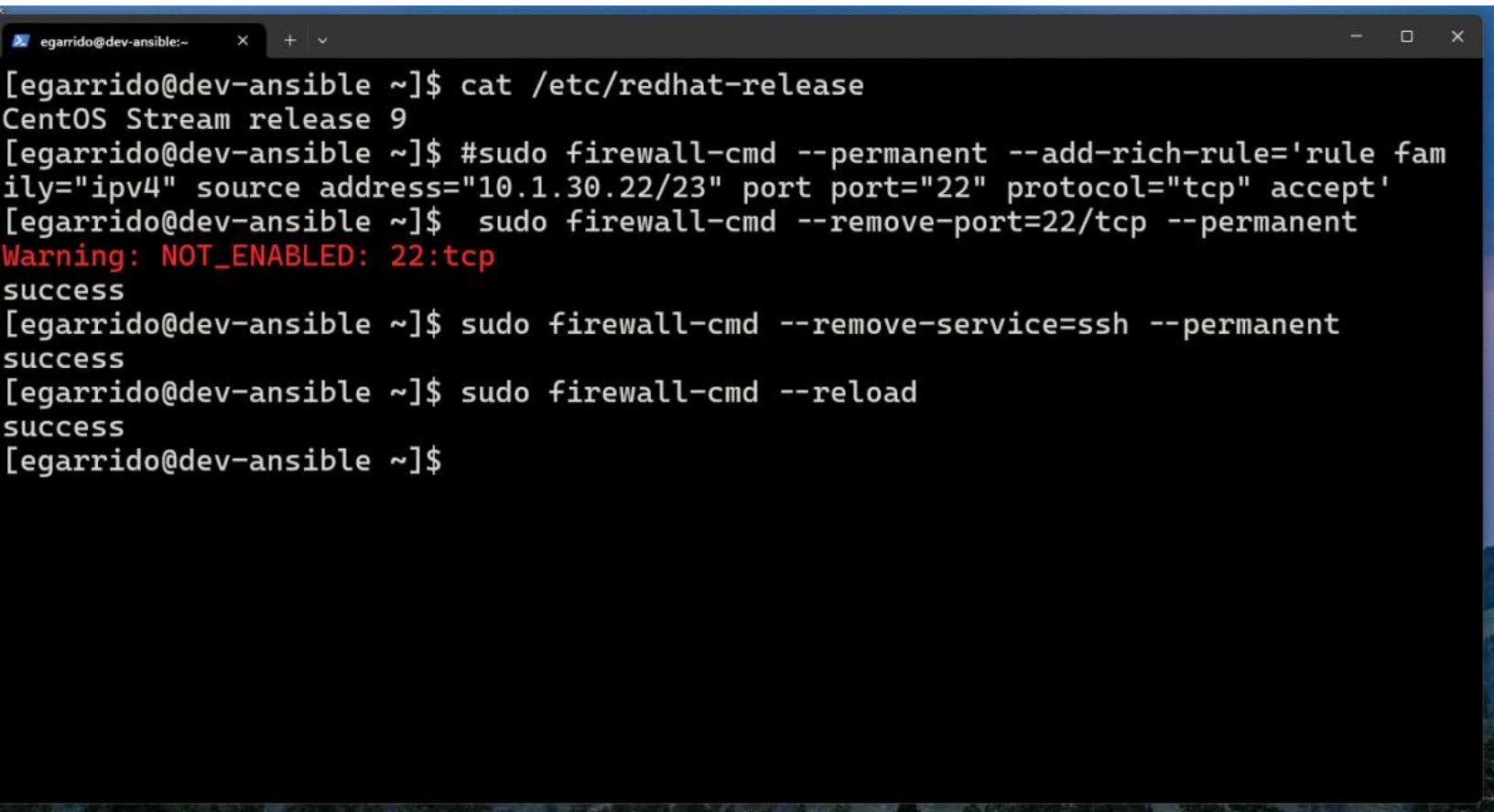
This screenshot demonstrates firewalld hardening and OS verification on the performance server. The operating system is first confirmed as CentOS Stream 9, after which firewall rules are tightened to restrict SSH access. A permanent rich rule is added to allow TCP port 22 only from a trusted subnet, while the default open SSH service and generic port rule are removed. The firewall is then reloaded to apply the changes, enforcing least-privilege network access while preserving required administrative connectivity.



This screenshot shows OS verification and firewall hardening on the stage web server. The operating system is confirmed as CentOS Stream 9, after which firewall rules are tightened using firewalld. A permanent rich rule is added to allow SSH access only from a trusted subnet, while the default SSH service and generic port rule are removed. The firewall configuration is then reloaded to apply the changes, enforcing restricted, least-privilege SSH access while maintaining required administrative connectivity



This screenshot shows OS verification and firewall rule cleanup on the Ansible control host. The system is confirmed to be running CentOS Stream 9, and the firewall configuration is adjusted to remove broad SSH exposure by deleting the default SSH service and generic port 22 rules. The firewall is then reloaded to apply the changes, aligning access control with a least-privilege security model for automation infrastructure.



Summary

This project demonstrates consistent security hardening and automation preparation across multiple Linux hosts in development, performance, and staging environments. Systems running CentOS Stream 9 are verified, SSH access is hardened, firewall rules are tightened to restrict access to trusted sources, and secure key-based authentication is validated. Ansible connectivity is confirmed after hardening to ensure all hosts remain manageable. All IP addresses, hostnames, usernames, and environment-specific details shown are sanitized for security purposes.