QA Agent Report

Target: 192.168.1.150 | Generated: 2026-02-19 03:12:11

QA Validation Summary

Total QA Validated	6
Safe	6
Unsafe	0
Regressions Detected	0

Per-Finding QA Details

ID	Title	Safe	Reason	Regression	Recommendation	Side Effects	Services Affected	Duration
openscap_012	Ensure PAM Enforces Password Requirements - Minimum Different Characters	SAFE	All critical services (sshd, auditd, firewalld) are active and the system remains accessible. The PAM password policy remediation applied (setting difok = 8) has not caused any service outages or critical failures. The system is functionally intact.	No	Approve	—	—	18.3s
openscap_014	Ensure PAM Enforces Password Requirements - Maximum Consecutive Repeating Characters from Same Character Class	SAFE	Validation completed: SSH daemon is active and listening on port 22, sshd, auditd, and firewalld services are all running. No critical service failures or accessibility issues detected after the remediation.	No	Approve	—	—	23.1s
openscap_015	Ensure PAM Enforces Password Requirements - Minimum Different Categories	SAFE	Validation completed. All critical services (sshd, auditd, firewalld) are active and SSH is listening on port 22. No adverse side effects observed from the PAM password policy remediation.	No	Approve	—	—	23.4s

ID	Title	Safe	Reason	Regression	Recommendation	Side Effects	Services Affected	Duration
openscap_017	Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	SAFE	Validation complete: sshd, auditd, and firewalld are all active; SSH daemon is listening on port 22; ucredit correctly set to -1; no critical service failures observed. System remains functional post-remediation.	No	Approve	—	—	42.4s
openscap_021	Configure Multiple DNS Servers in /etc/resolv.conf	SAFE	Validation completed: sshd, auditd, and firewalld are all active; SSH connectivity test succeeded, confirming system accessibility. No critical services are down and no major side effects observed. The remediation is safe for production.\x0a	No	Approve	—	—	30.2s
openscap_025	Ensure Chrony is only configured with the server directive	SAFE	Validation completed: SSH daemon is active and listening on port 22, auditd and firewalld services are running. System remains accessible and no critical services are down. The remediation modified /etc/chrony.conf but did not break any essential functionality. Therefore, the system is considered safe.	No	Approve	—	—	37.0s