



TEST REPORT SEAPATH DEBIAN

Receiver: SEAPATH

Contact: <seapath@savoirfairelinux>

21 February 2025, 21:16:03 UTC

Copyright © 2025 Savoir-faire Linux

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive license of Linus Torvalds, owner of the mark on a world-wide basis.

Table of Contents

| | |
|--|----|
| Test reports..... | 1 |
| Tests common for standalone..... | 1 |
| Tests common security for standalone..... | 1 |
| Tests hypervisor for standalone..... | 4 |
| Tests hypervisor iommu for standalone..... | 5 |
| Tests hypervisor security for standalone..... | 5 |
| Tests common for node3..... | 6 |
| Tests common security for node3..... | 6 |
| Tests hypervisor for node3..... | 9 |
| Tests hypervisor iommu for node3..... | 10 |
| Tests hypervisor security for node3..... | 10 |
| Tests common for node2..... | 10 |
| Tests common security for node2..... | 11 |
| Tests hypervisor for node2..... | 14 |
| Tests hypervisor iommu for node2..... | 14 |
| Tests hypervisor security for node2..... | 15 |
| Tests common for node1..... | 15 |
| Tests common security for node1..... | 16 |
| Tests hypervisor for node1..... | 19 |
| Tests hypervisor iommu for node1..... | 19 |
| Tests hypervisor security for node1..... | 20 |
| Tests cluster for ci121..... | 20 |
| Compliance Matrix..... | 23 |
| Matrix include/ANSSI-BP28-Recommandations-M.csv..... | 23 |
| Matrix include/ANSSI-BP28-Recommandations-MI.csv..... | 23 |
| Matrix include/ANSSI-BP28-Recommandations-MIR.csv..... | 24 |
| About this documentation..... | 26 |

Test reports

Tests common for standalone

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00078 | no paging error | PASS |
| SEAPATH-00079 | no rcu stall | PASS |
| SEAPATH-00080 | no backtraces | PASS |
| SEAPATH-00075 | kernel is PREEMPT RT | PASS |
| SEAPATH-00076 | kernel is realtime | PASS |
| SEAPATH-00081 | kernel is >= 4.19.106 | PASS |
| SEAPATH-00083 | syslog-ng service is running | PASS |
| SEAPATH-00084 | syslog-ng is configured to send log on network | PASS |

- number of tests: 8
- number of failures: 0

Tests common security for standalone

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00197 | Only wanted apt repositories configured: only use sources.list | PASS |
| SEAPATH-00197 | Only wanted apt repositories configured: do not add other repositories | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://ftp.fr.debian.org/debian bullseye main contrib non-free | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://security.debian.org/debian-security bullseye-security main contrib non-free | PASS |
| SEAPATH-00197 | Only official apt repositories configured: https://download.docker.com/linux/debian bullseye stable | PASS |
| SEAPATH-00197 | Only official apt repositories configured: https://artifacts.elastic.co/packages/8.x/apt stable main | PASS |
| SEAPATH-00198 | No unrecognized packages installed | PASS |
| SEAPATH-00215 | auditd service is active | PASS |
| SEAPATH-00216 | auditd is configured to output in syslog | PASS |
| SEAPATH-00217 | insmod call is logged | FAIL |
| SEAPATH-00217 | kmod call is logged | PASS |
| SEAPATH-00217 | modprobe call is logged | PASS |
| SEAPATH-00217 | rmmod call is logged | FAIL |
| SEAPATH-00218 | modification in /etc/ is logged | FAIL |
| SEAPATH-00219 | mount/umount call is logged | PASS |
| SEAPATH-00220 | ioperm call is logged | FAIL |
| SEAPATH-00220 | prctl call is logged | PASS |
| SEAPATH-00220 | ptrace call is logged | FAIL |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00221 | file deletion is logged | FAIL |
| SEAPATH-00222 | open monitoring is logged | PASS |
| SEAPATH-00222 | openat monitoring is logged | PASS |
| SEAPATH-00222 | unlink monitoring is logged | PASS |
| SEAPATH-00106 | Check /etc/shadow permissions | PASS |
| SEAPATH-00107 | Check /etc/passwd permissions | PASS |
| SEAPATH-00108 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |
| SEAPATH-00049 | Check /etc/ssh/ssh_host_ed25519_key permissions | PASS |
| SEAPATH-00090 | Check /etc/ssh/ssh_host_rsa_key permissions | PASS |
| SEAPATH-00192 | All files have a known owner and group | FAIL |
| SEAPATH-00193 | All directories writable by all users have the sticky bit | PASS |
| SEAPATH-00194 | All directories writable by all users are owned by root | PASS |
| SEAPATH-00195 | Ceph OSD are owned by ceph | PASS |
| SEAPATH-00196 | No unexpected file has setuid/setgid enabled | PASS |
| SEAPATH-00088 | root password was randomized at boot | PASS |
| SEAPATH-00089 | root password is randomized at each boot | PASS |
| SEAPATH-00091 | root password is encrypted with a crypto at least equivalent as sha512 | PASS |
| SEAPATH-00092 | bash timeout is set read-only to 300s | PASS |
| SEAPATH-00093 | sshd forbids setting environment variables | PASS |
| SEAPATH-00094 | sshd server time-out is set to 300s of client inactivity | PASS |
| SEAPATH-00095 | shadow encrypts passwords with SHA512 by default | PASS |
| SEAPATH-00096 | shadow encryption uses at least 65536 rounds | PASS |
| SEAPATH-00097 | pam password authentication uses sha512 with 65536 rounds or yescrypt | PASS |
| SEAPATH-00098 | password set to expire after 90 days | PASS |
| SEAPATH-00099 | 'su' is denied | PASS |
| SEAPATH-00100 | /etc/securetty is empty | PASS |
| SEAPATH-00101 | PAM securetty module is active in 'login' policy | PASS |
| SEAPATH-00202 | grub root superuser is set in /boot/grub/grub.cfg | PASS |
| SEAPATH-00203 | grub root superuser is password protected | PASS |
| SEAPATH-00204 | main menuentry is unrestricted in /boot/grub/grub.cfg | PASS |
| SEAPATH-00205 | TMPDIR env var is defined and readonly | PASS |
| SEAPATH-00206 | TMPDIR is set with 700 mode and root as owner and group | PASS |
| SEAPATH-00225 | Umask is set correctly set | PASS |
| SEAPATH-00227 | AppArmor processes are confined in enforce mode | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_YAMA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : DEBUG_WX is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_DMESG_RESTRICT is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : LEGACY_VSYSCALL_NONE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_RANDOM is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_HARDENED is enabled | PASS |

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00050 | Linux kernel 'hardening' : HARDENED_USERCOPY is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : FORTIFY_SOURCE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : PAGE_POISONING is enabled | PASS |
| SEAPATH-00170 | Wipe slab and page allocations enabled on cmdline | PASS |
| SEAPATH-00174 | Randomize kstack offset in on | PASS |
| SEAPATH-00175 | Disable slab usercopy fallback | PASS |
| SEAPATH-00201 | LSM Yama is enabled | PASS |
| SEAPATH-00210 | MCE is disabled | PASS |
| SEAPATH-00211 | rng_core.default_quality is set to 500 | PASS |
| SEAPATH-00226 | Test AppArmor is enabled | PASS |
| SEAPATH-00223 | All sockets are bound to an interface | PASS |
| SEAPATH-00224 | IPv6 is disabled | PASS |
| SEAPATH-00164 | sudo requires password for group operator (operator) | PASS |
| SEAPATH-00165 | sudo requires password for group maintenance-N1 (maint-n1) | PASS |
| SEAPATH-00166 | sudo requires password for group maintenance-N3 (maint-n3) | PASS |
| SEAPATH-00167 | sudo requires password for group administrator (admincluster) | PASS |
| SEAPATH-00168 | sudo requires password for group super-administrator (adminsyz) | PASS |
| SEAPATH-00103 | /usr/bin/sudo exists | PASS |
| SEAPATH-00104 | /usr/bin/sudo belongs to group privileged | PASS |
| SEAPATH-00105 | /usr/bin/sudo has permissions 4750 | PASS |
| SEAPATH-00148 | sudoers files include directive noexec | PASS |
| SEAPATH-00148 | sudoers files include directive requiretty | PASS |
| SEAPATH-00148 | sudoers files include directive use_pty | PASS |
| SEAPATH-00148 | sudoers files include directive umask=0027 | PASS |
| SEAPATH-00148 | sudoers files include directive ignore_dot | PASS |
| SEAPATH-00148 | sudoers files include directive env_reset | PASS |
| SEAPATH-00149 | sudo commands don't target privileged user | PASS |
| SEAPATH-00150 | all commands require authentication | PASS |
| SEAPATH-00152 | EXEC option is not used | PASS |
| SEAPATH-00153 | rules are not defined by negation | PASS |
| SEAPATH-00154 | sudo commands always specify arguments | PASS |
| SEAPATH-00154 | no user can run all commands as root | PASS |
| SEAPATH-00155 | sudo commands don't use wildcard * argument | PASS |
| SEAPATH-00156 | /etc/sudoers - /etc/sudoers is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/ceph-smartctl - /etc/sudoers.d/ceph-smartctl is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/00-security - /etc/sudoers.d/00-security is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00171 | Check coredumps are disabled | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00172 | Check kexec is disabled | PASS |
| SEAPATH-00173 | Check binfmt_misc is disabled | PASS |
| SEAPATH-00176 | Check kptr_restrict is set to 2 | PASS |
| SEAPATH-00177 | Check dmesg_restrict is set to 1 | PASS |
| SEAPATH-00178 | Check pid_max is set to 4194304 | PASS |
| SEAPATH-00179 | Check perf_cpu_time_max_percent is set to 1 | PASS |
| SEAPATH-00180 | Check perf_event_max_sample_rate is set to 1 | PASS |
| SEAPATH-00181 | Check perf_event_paranoid is set to 2 | PASS |
| SEAPATH-00182 | Check randomize_va_space is set to 2 | PASS |
| SEAPATH-00183 | Check sysrq is set to 0 | PASS |
| SEAPATH-00184 | Check unprivileged_bpf_disabled is set to 1 | PASS |
| SEAPATH-00185 | Check panic_on_oops is set to 1 | PASS |
| SEAPATH-00186 | Check kernel.yama.ptrace_scope is set to 2 | PASS |
| SEAPATH-00187 | Check suid_dumpable is set to 0 | PASS |
| SEAPATH-00188 | Check protected_fifos is set to 2 | PASS |
| SEAPATH-00189 | Check protected_regular is set to 2 | PASS |
| SEAPATH-00190 | Check protected_symlinks is set to 1 | PASS |
| SEAPATH-00191 | Check protected_hardlinks is set to 1 | PASS |
| SEAPATH-00082 | /var/log is mounted on a separate partition | PASS |
| SEAPATH-00085 | syslog-ng can not acquire new privileges | PASS |
| SEAPATH-00086 | syslog-ng capabilities are bounded | PASS |
| SEAPATH-00087 | syslog-ng system calls are filtered | PASS |
| SEAPATH-00199 | No systemd service failed | PASS |
| SEAPATH-00200 | No unrecognized service enabled | PASS |

- number of tests: 119
- number of failures: 8

Tests hypervisor for standalone

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00044 | Check /etc/syslog-ng/cert.d/clientcert.pem permissions | FAIL |
| SEAPATH-00045 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |
| SEAPATH-00035 | ovs-vswitchd service is running | PASS |
| SEAPATH-00035 | ovsdb-server service is running | PASS |
| SEAPATH-00038 | lspci 3.6.2+ is available | PASS |
| SEAPATH-00018 | KVM device available | PASS |
| SEAPATH-00019 | Qemu for x86-64 available | PASS |
| SEAPATH-00020 | Libvirtd service is running | PASS |
| SEAPATH-00021 | IPv4 NAT is available | PASS |

- number of tests: 9
- number of failures: 2

Tests hypervisor iommu for standalone

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00030 | iommu enabled in passthrough mode | PASS |
| SEAPATH-00031 | iommu is loaded | FAIL |
| SEAPATH-00032 | iommu is populated | FAIL |
| SEAPATH-00050 | Linux kernel 'iommu' : INTEL_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : AMD_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : IOMMU_IOVA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : DMAR_TABLE is enabled | PASS |

- number of tests: 7
- number of failures: 2

Tests hypervisor security for standalone

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00033 | /etc/group is consistent | PASS |
| SEAPATH-00033 | /etc/gshadow is consistent | PASS |
| SEAPATH-00034 | /etc/group does not include extra group | PASS |
| SEAPATH-00034 | /etc/gshadow does not include extra group | FAIL |
| SEAPATH-00008 | Slab merging is disabled on cmdline | PASS |
| SEAPATH-00009 | Kernel Page Table Isolation is always enabled on cmdline | PASS |
| SEAPATH-00010 | SLUB redzoning and sanity checking enabled on cmdline | PASS |
| SEAPATH-00207 | CPU has no known vulnerabilities | PASS |
| SEAPATH-00047 | /etc/passwd is consistent | PASS |
| SEAPATH-00048 | /etc/passwd does not include extra user | PASS |
| SEAPATH-00046 | /etc/shadow is consistent | PASS |
| SEAPATH-00015 | Vulnerabilities sysfs entry exist | PASS |
| SEAPATH-00017 | System is not vulnerable to : meltdown | PASS |
| SEAPATH-00017 | System is not vulnerable to : l1tf | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v1 | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v2 | PASS |

- number of tests: 16
- number of failures: 1

Tests common for node3

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00078 | no paging error | PASS |
| SEAPATH-00079 | no rcu stall | PASS |
| SEAPATH-00080 | no backtraces | PASS |
| SEAPATH-00075 | kernel is PREEMPT RT | PASS |
| SEAPATH-00076 | kernel is realtime | PASS |
| SEAPATH-00081 | kernel is >= 4.19.106 | PASS |
| SEAPATH-00083 | syslog-ng service is running | PASS |
| SEAPATH-00084 | syslog-ng is configured to send log on network | FAIL |

- number of tests: 8
- number of failures: 1

Tests common security for node3

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00197 | Only wanted apt repositories configured: only use sources.list | PASS |
| SEAPATH-00197 | Only wanted apt repositories configured: do not add other repositories | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://ftp.fr.debian.org/debian bookworm main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://security.debian.org/debian-security bookworm-security main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://ftp.fr.debian.org/debian bookworm-backports main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: https://artifacts.elastic.co/packages/8.x/apt stable main | PASS |
| SEAPATH-00198 | No unrecognized packages installed | PASS |
| SEAPATH-00215 | auditd service is active | PASS |
| SEAPATH-00216 | auditd is configured to output in syslog | PASS |
| SEAPATH-00217 | insmod call is logged | PASS |
| SEAPATH-00217 | kmod call is logged | PASS |
| SEAPATH-00217 | modprobe call is logged | PASS |
| SEAPATH-00217 | rmmod call is logged | PASS |
| SEAPATH-00218 | modification in /etc/ is logged | PASS |
| SEAPATH-00219 | mount/umount call is logged | PASS |
| SEAPATH-00220 | ioperm call is logged | PASS |
| SEAPATH-00220 | prctl call is logged | PASS |
| SEAPATH-00220 | ptrace call is logged | PASS |
| SEAPATH-00221 | file deletion is logged | PASS |
| SEAPATH-00222 | open monitoring is logged | PASS |
| SEAPATH-00222 | openat monitoring is logged | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00222 | unlink monitoring is logged | PASS |
| SEAPATH-00106 | Check /etc/shadow permissions | PASS |
| SEAPATH-00107 | Check /etc/passwd permissions | PASS |
| SEAPATH-00108 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |
| SEAPATH-00049 | Check /etc/ssh/ssh_host_ed25519_key permissions | PASS |
| SEAPATH-00090 | Check /etc/ssh/ssh_host_rsa_key permissions | PASS |
| SEAPATH-00192 | All files have a known owner and group | PASS |
| SEAPATH-00193 | All directories writable by all users have the sticky bit | PASS |
| SEAPATH-00194 | All directories writable by all users are owned by root | PASS |
| SEAPATH-00195 | Ceph OSD are owned by ceph | PASS |
| SEAPATH-00196 | No unexpected file has setuid/setgid enabled | PASS |
| SEAPATH-00088 | root password was randomized at boot | PASS |
| SEAPATH-00089 | root password is randomized at each boot | PASS |
| SEAPATH-00091 | root password is encrypted with a crypto at least equivalent as sha512 | PASS |
| SEAPATH-00092 | bash timeout is set read-only to 300s | PASS |
| SEAPATH-00093 | sshd forbids setting environment variables | PASS |
| SEAPATH-00094 | sshd server time-out is set to 300s of client inactivity | PASS |
| SEAPATH-00095 | shadow encrypts passwords with SHA512 by default | PASS |
| SEAPATH-00096 | shadow encryption uses at least 65536 rounds | PASS |
| SEAPATH-00097 | pam password authentication uses sha512 with 65536 rounds or yescrypt | PASS |
| SEAPATH-00098 | password set to expire after 90 days | PASS |
| SEAPATH-00099 | 'su' is denied | PASS |
| SEAPATH-00100 | /etc/securetty is empty | PASS |
| SEAPATH-00101 | PAM securetty module is active in 'login' policy | PASS |
| SEAPATH-00202 | grub root superuser is set in /boot/grub/grub.cfg | PASS |
| SEAPATH-00203 | grub root superuser is password protected | PASS |
| SEAPATH-00204 | main menuentry is unrestricted in /boot/grub/grub.cfg | PASS |
| SEAPATH-00205 | TMPDIR env var is defined and readonly | PASS |
| SEAPATH-00206 | TMPDIR is set with 700 mode and root as owner and group | PASS |
| SEAPATH-00225 | Umask is set correctly set | PASS |
| SEAPATH-00227 | AppArmor processes are confined in enforce mode | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_YAMA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : DEBUG_WX is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_DMESG_RESTRICT is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : LEGACY_VSYSCALL_NONE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_RANDOM is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_HARDENED is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : HARDENED_USERCOPY is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : FORTIFY_SOURCE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : PAGE_POISONING is enabled | PASS |

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00170 | Wipe slab and page allocations enabled on cmdline | PASS |
| SEAPATH-00174 | Randomize kstack offset in on | PASS |
| SEAPATH-00175 | Disable slab usercopy fallback | PASS |
| SEAPATH-00201 | LSM Yama is enabled | PASS |
| SEAPATH-00210 | MCE is disabled | PASS |
| SEAPATH-00211 | rng_core.default_quality is set to 500 | PASS |
| SEAPATH-00226 | Test AppArmor is enabled | PASS |
| SEAPATH-00223 | All sockets are bound to an interface | PASS |
| SEAPATH-00224 | IPv6 is disabled | PASS |
| SEAPATH-00164 | sudo requires password for group operator (operator) | PASS |
| SEAPATH-00165 | sudo requires password for group maintenance-N1 (maint-n1) | PASS |
| SEAPATH-00166 | sudo requires password for group maintenance-N3 (maint-n3) | PASS |
| SEAPATH-00167 | sudo requires password for group administrator (admincluster) | PASS |
| SEAPATH-00168 | sudo requires password for group super-administrator (adminsyst) | PASS |
| SEAPATH-00103 | /usr/bin/sudo exists | PASS |
| SEAPATH-00104 | /usr/bin/sudo belongs to group privileged | PASS |
| SEAPATH-00105 | /usr/bin/sudo has permissions 4750 | PASS |
| SEAPATH-00148 | sudoers files include directive noexec | PASS |
| SEAPATH-00148 | sudoers files include directive requiretty | PASS |
| SEAPATH-00148 | sudoers files include directive use_pty | PASS |
| SEAPATH-00148 | sudoers files include directive umask=0027 | PASS |
| SEAPATH-00148 | sudoers files include directive ignore_dot | PASS |
| SEAPATH-00148 | sudoers files include directive env_reset | PASS |
| SEAPATH-00149 | sudo commands don't target privileged user | PASS |
| SEAPATH-00150 | all commands require authentication | PASS |
| SEAPATH-00152 | EXEC option is not used | PASS |
| SEAPATH-00153 | rules are not defined by negation | PASS |
| SEAPATH-00154 | sudo commands always specify arguments | PASS |
| SEAPATH-00154 | no user can run all commands as root | PASS |
| SEAPATH-00155 | sudo commands don't use wildcard * argument | PASS |
| SEAPATH-00156 | /etc/sudoers - /etc/sudoers is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/ceph-smartctl - /etc/sudoers.d/ceph-smartctl is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/00-security - /etc/sudoers.d/00-security is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00171 | Check coredumps are disabled | PASS |
| SEAPATH-00172 | Check kexec is disabled | PASS |
| SEAPATH-00173 | Check binfmt_misc is disabled | PASS |
| SEAPATH-00176 | Check kptr_restrict is set to 2 | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00177 | Check dmesg_restrict is set to 1 | PASS |
| SEAPATH-00178 | Check pid_max is set to 4194304 | PASS |
| SEAPATH-00179 | Check perf_cpu_time_max_percent is set to 1 | PASS |
| SEAPATH-00180 | Check perf_event_max_sample_rate is set to 1 | PASS |
| SEAPATH-00181 | Check perf_event_paranoid is set to 2 | PASS |
| SEAPATH-00182 | Check randomize_va_space is set to 2 | PASS |
| SEAPATH-00183 | Check sysrq is set to 0 | PASS |
| SEAPATH-00184 | Check unprivileged_bpf_disabled is set to 1 | PASS |
| SEAPATH-00185 | Check panic_on_oops is set to 1 | PASS |
| SEAPATH-00186 | Check kernel.yama.ptrace_scope is set to 2 | PASS |
| SEAPATH-00187 | Check suid_dumpable is set to 0 | PASS |
| SEAPATH-00188 | Check protected_fifos is set to 2 | PASS |
| SEAPATH-00189 | Check protected_regular is set to 2 | PASS |
| SEAPATH-00190 | Check protected_symlinks is set to 1 | PASS |
| SEAPATH-00191 | Check protected_hardlinks is set to 1 | PASS |
| SEAPATH-00082 | /var/log is mounted on a separate partition | PASS |
| SEAPATH-00085 | syslog-ng can not acquire new privileges | PASS |
| SEAPATH-00086 | syslog-ng capabilities are bounded | PASS |
| SEAPATH-00087 | syslog-ng system calls are filtered | PASS |
| SEAPATH-00199 | No systemd service failed | PASS |
| SEAPATH-00200 | No unrecognized service enabled | PASS |

- number of tests: 119
- number of failures: 1

Tests hypervisor for node3

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00044 | Check /etc/syslog-ng/cert.d/clientcert.pem permissions | FAIL |
| SEAPATH-00045 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |
| SEAPATH-00035 | ovs-vswitchd service is running | PASS |
| SEAPATH-00035 | ovsdb-server service is running | PASS |
| SEAPATH-00038 | lspci 3.6.2+ is available | PASS |
| SEAPATH-00018 | KVM device available | PASS |
| SEAPATH-00019 | Qemu for x86-64 available | PASS |
| SEAPATH-00020 | Libvirtd service is running | PASS |
| SEAPATH-00021 | IPv4 NAT is available | PASS |

- number of tests: 9
- number of failures: 2

Tests hypervisor iommu for node3

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00030 | iommu enabled in passthrough mode | PASS |
| SEAPATH-00031 | iommu is loaded | FAIL |
| SEAPATH-00032 | iommu is populated | FAIL |
| SEAPATH-00050 | Linux kernel 'iommu' : INTEL_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : AMD_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : IOMMU_IOVA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : DMAR_TABLE is enabled | PASS |

- number of tests: 7
- number of failures: 2

Tests hypervisor security for node3

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00033 | /etc/group is consistent | PASS |
| SEAPATH-00033 | /etc/gshadow is consistent | PASS |
| SEAPATH-00034 | /etc/group does not include extra group | PASS |
| SEAPATH-00034 | /etc/gshadow does not include extra group | PASS |
| SEAPATH-00008 | Slab merging is disabled on cmdline | PASS |
| SEAPATH-00009 | Kernel Page Table Isolation is always enabled on cmdline | PASS |
| SEAPATH-00010 | SLUB redzoning and sanity checking enabled on cmdline | PASS |
| SEAPATH-00207 | CPU has no known vulnerabilities | PASS |
| SEAPATH-00047 | /etc/passwd is consistent | PASS |
| SEAPATH-00048 | /etc/passwd does not include extra user | PASS |
| SEAPATH-00046 | /etc/shadow is consistent | PASS |
| SEAPATH-00015 | Vulnerabilities sysfs entry exist | PASS |
| SEAPATH-00017 | System is not vulnerable to : meltdown | PASS |
| SEAPATH-00017 | System is not vulnerable to : l1tf | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v1 | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v2 | PASS |

- number of tests: 16
- number of failures: 0

Tests common for node2

| Test ID | Tests | Results |
|---------------|-----------------|---------|
| SEAPATH-00078 | no paging error | PASS |
| SEAPATH-00079 | no rcu stall | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00080 | no backtraces | PASS |
| SEAPATH-00075 | kernel is PREEMPT RT | PASS |
| SEAPATH-00076 | kernel is realtime | PASS |
| SEAPATH-00081 | kernel is >= 4.19.106 | PASS |
| SEAPATH-00083 | syslog-ng service is running | PASS |
| SEAPATH-00084 | syslog-ng is configured to send log on network | FAIL |

- number of tests: 8
- number of failures: 1

Tests common security for node2

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00197 | Only wanted apt repositories configured: only use sources.list | PASS |
| SEAPATH-00197 | Only wanted apt repositories configured: do not add other repositories | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://ftp.fr.debian.org/debian bookworm main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://security.debian.org/debian-security bookworm-security main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://ftp.fr.debian.org/debian bookworm-backports main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: https://artifacts.elastic.co/packages/8.x/apt stable main | PASS |
| SEAPATH-00198 | No unrecognized packages installed | PASS |
| SEAPATH-00215 | auditd service is active | PASS |
| SEAPATH-00216 | auditd is configured to output in syslog | PASS |
| SEAPATH-00217 | insmod call is logged | PASS |
| SEAPATH-00217 | kmod call is logged | PASS |
| SEAPATH-00217 | modprobe call is logged | PASS |
| SEAPATH-00217 | rmmod call is logged | PASS |
| SEAPATH-00218 | modification in /etc/ is logged | PASS |
| SEAPATH-00219 | mount/umount call is logged | PASS |
| SEAPATH-00220 | ioperm call is logged | PASS |
| SEAPATH-00220 | prctl call is logged | PASS |
| SEAPATH-00220 | ptrace call is logged | PASS |
| SEAPATH-00221 | file deletion is logged | PASS |
| SEAPATH-00222 | open monitoring is logged | PASS |
| SEAPATH-00222 | openat monitoring is logged | PASS |
| SEAPATH-00222 | unlink monitoring is logged | PASS |
| SEAPATH-00106 | Check /etc/shadow permissions | PASS |
| SEAPATH-00107 | Check /etc/passwd permissions | PASS |
| SEAPATH-00108 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00049 | Check /etc/ssh/ssh_host_ed25519_key permissions | PASS |
| SEAPATH-00090 | Check /etc/ssh/ssh_host_rsa_key permissions | PASS |
| SEAPATH-00192 | All files have a known owner and group | PASS |
| SEAPATH-00193 | All directories writable by all users have the sticky bit | PASS |
| SEAPATH-00194 | All directories writable by all users are owned by root | PASS |
| SEAPATH-00195 | Ceph OSD are owned by ceph | PASS |
| SEAPATH-00196 | No unexpected file has setuid/setgid enabled | PASS |
| SEAPATH-00088 | root password was randomized at boot | PASS |
| SEAPATH-00089 | root password is randomized at each boot | PASS |
| SEAPATH-00091 | root password is encrypted with a crypto at least equivalent as sha512 | PASS |
| SEAPATH-00092 | bash timeout is set read-only to 300s | PASS |
| SEAPATH-00093 | sshd forbids setting environment variables | PASS |
| SEAPATH-00094 | sshd server time-out is set to 300s of client inactivity | PASS |
| SEAPATH-00095 | shadow encrypts passwords with SHA512 by default | PASS |
| SEAPATH-00096 | shadow encryption uses at least 65536 rounds | PASS |
| SEAPATH-00097 | pam password authentication uses sha512 with 65536 rounds or yescrypt | PASS |
| SEAPATH-00098 | password set to expire after 90 days | PASS |
| SEAPATH-00099 | 'su' is denied | PASS |
| SEAPATH-00100 | /etc/securetty is empty | PASS |
| SEAPATH-00101 | PAM securetty module is active in 'login' policy | PASS |
| SEAPATH-00202 | grub root superuser is set in /boot/grub/grub.cfg | PASS |
| SEAPATH-00203 | grub root superuser is password protected | PASS |
| SEAPATH-00204 | main menuentry is unrestricted in /boot/grub/grub.cfg | PASS |
| SEAPATH-00205 | TMPDIR env var is defined and readonly | PASS |
| SEAPATH-00206 | TMPDIR is set with 700 mode and root as owner and group | PASS |
| SEAPATH-00225 | Umask is set correctly set | PASS |
| SEAPATH-00227 | AppArmor processes are confined in enforce mode | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_YAMA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : DEBUG_WX is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_DMESG_RESTRICT is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : LEGACY_VSYSCALL_NONE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_RANDOM is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_HARDENED is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : HARDENED_USERCOPY is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : FORTIFY_SOURCE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : PAGE_POISONING is enabled | PASS |
| SEAPATH-00170 | Wipe slab and page allocations enabled on cmdline | PASS |
| SEAPATH-00174 | Randomize kstack offset in on | PASS |
| SEAPATH-00175 | Disable slab usercopy fallback | PASS |
| SEAPATH-00201 | LSM Yama is enabled | PASS |

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00210 | MCE is disabled | PASS |
| SEAPATH-00211 | rng_core.default_quality is set to 500 | PASS |
| SEAPATH-00226 | Test AppArmor is enabled | PASS |
| SEAPATH-00223 | All sockets are bound to an interface | PASS |
| SEAPATH-00224 | IPv6 is disabled | PASS |
| SEAPATH-00164 | sudo requires password for group operator (operator) | PASS |
| SEAPATH-00165 | sudo requires password for group maintenance-N1 (maint-n1) | PASS |
| SEAPATH-00166 | sudo requires password for group maintenance-N3 (maint-n3) | PASS |
| SEAPATH-00167 | sudo requires password for group administrator (admincluster) | PASS |
| SEAPATH-00168 | sudo requires password for group super-administrator (adminsyst) | PASS |
| SEAPATH-00103 | /usr/bin/sudo exists | PASS |
| SEAPATH-00104 | /usr/bin/sudo belongs to group privileged | PASS |
| SEAPATH-00105 | /usr/bin/sudo has permissions 4750 | PASS |
| SEAPATH-00148 | sudoers files include directive noexec | PASS |
| SEAPATH-00148 | sudoers files include directive requiretty | PASS |
| SEAPATH-00148 | sudoers files include directive use_pty | PASS |
| SEAPATH-00148 | sudoers files include directive umask=0027 | PASS |
| SEAPATH-00148 | sudoers files include directive ignore_dot | PASS |
| SEAPATH-00148 | sudoers files include directive env_reset | PASS |
| SEAPATH-00149 | sudo commands don't target privileged user | PASS |
| SEAPATH-00150 | all commands require authentication | PASS |
| SEAPATH-00152 | EXEC option is not used | PASS |
| SEAPATH-00153 | rules are not defined by negation | PASS |
| SEAPATH-00154 | sudo commands always specify arguments | PASS |
| SEAPATH-00154 | no user can run all commands as root | PASS |
| SEAPATH-00155 | sudo commands don't use wildcard * argument | PASS |
| SEAPATH-00156 | /etc/sudoers - /etc/sudoers is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/ceph-smartctl - /etc/sudoers.d/ceph-smartctl is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/00-security - /etc/sudoers.d/00-security is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00171 | Check coredumps are disabled | PASS |
| SEAPATH-00172 | Check kexec is disabled | PASS |
| SEAPATH-00173 | Check binfmt_misc is disabled | PASS |
| SEAPATH-00176 | Check kptr_restrict is set to 2 | PASS |
| SEAPATH-00177 | Check dmesg_restrict is set to 1 | PASS |
| SEAPATH-00178 | Check pid_max is set to 4194304 | PASS |
| SEAPATH-00179 | Check perf_cpu_time_max_percent is set to 1 | PASS |
| SEAPATH-00180 | Check perf_event_max_sample_rate is set to 1 | PASS |

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00181 | Check perf_event_paranoid is set to 2 | PASS |
| SEAPATH-00182 | Check randomize_va_space is set to 2 | PASS |
| SEAPATH-00183 | Check sysrq is set to 0 | PASS |
| SEAPATH-00184 | Check unprivileged_bpf_disabled is set to 1 | PASS |
| SEAPATH-00185 | Check panic_on_oops is set to 1 | PASS |
| SEAPATH-00186 | Check kernel.yama.ptrace_scope is set to 2 | PASS |
| SEAPATH-00187 | Check suid_dumpable is set to 0 | PASS |
| SEAPATH-00188 | Check protected_fifos is set to 2 | PASS |
| SEAPATH-00189 | Check protected_regular is set to 2 | PASS |
| SEAPATH-00190 | Check protected_symlinks is set to 1 | PASS |
| SEAPATH-00191 | Check protected_hardlinks is set to 1 | PASS |
| SEAPATH-00082 | /var/log is mounted on a separate partition | PASS |
| SEAPATH-00085 | syslog-ng can not acquire new privileges | PASS |
| SEAPATH-00086 | syslog-ng capabilities are bounded | PASS |
| SEAPATH-00087 | syslog-ng system calls are filtered | PASS |
| SEAPATH-00199 | No systemd service failed | PASS |
| SEAPATH-00200 | No unrecognized service enabled | PASS |

- number of tests: 119
- number of failures: 1

Tests hypervisor for node2

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00044 | Check /etc/syslog-ng/cert.d/clientcert.pem permissions | FAIL |
| SEAPATH-00045 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |
| SEAPATH-00035 | ovs-vswitchd service is running | PASS |
| SEAPATH-00035 | ovsdb-server service is running | PASS |
| SEAPATH-00038 | lspci 3.6.2+ is available | PASS |
| SEAPATH-00018 | KVM device available | PASS |
| SEAPATH-00019 | Qemu for x86-64 available | PASS |
| SEAPATH-00020 | Libvirtd service is running | PASS |
| SEAPATH-00021 | IPv4 NAT is available | PASS |

- number of tests: 9
- number of failures: 2

Tests hypervisor iommu for node2

| Test ID | Tests | Results |
|---------------|-----------------------------------|---------|
| SEAPATH-00030 | iommu enabled in passthrough mode | PASS |

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00031 | iommu is loaded | FAIL |
| SEAPATH-00032 | iommu is populated | FAIL |
| SEAPATH-00050 | Linux kernel 'iommu' : INTEL_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : AMD_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : IOMMU_IOVA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : DMAR_TABLE is enabled | PASS |

- number of tests: 7
- number of failures: 2

Tests hypervisor security for node2

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00033 | /etc/group is consistent | PASS |
| SEAPATH-00033 | /etc/gshadow is consistent | PASS |
| SEAPATH-00034 | /etc/group does not include extra group | PASS |
| SEAPATH-00034 | /etc/gshadow does not include extra group | PASS |
| SEAPATH-00008 | Slab merging is disabled on cmdline | PASS |
| SEAPATH-00009 | Kernel Page Table Isolation is always enabled on cmdline | PASS |
| SEAPATH-00010 | SLUB redzoning and sanity checking enabled on cmdline | PASS |
| SEAPATH-00207 | CPU has no known vulnerabilities | PASS |
| SEAPATH-00047 | /etc/passwd is consistent | PASS |
| SEAPATH-00048 | /etc/passwd does not include extra user | PASS |
| SEAPATH-00046 | /etc/shadow is consistent | PASS |
| SEAPATH-00015 | Vulnerabilities sysfs entry exist | PASS |
| SEAPATH-00017 | System is not vulnerable to : meltdown | PASS |
| SEAPATH-00017 | System is not vulnerable to : l1tf | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v1 | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v2 | PASS |

- number of tests: 16
- number of failures: 0

Tests common for node1

| Test ID | Tests | Results |
|---------------|----------------------|---------|
| SEAPATH-00078 | no paging error | PASS |
| SEAPATH-00079 | no rcu stall | PASS |
| SEAPATH-00080 | no backtraces | PASS |
| SEAPATH-00075 | kernel is PREEMPT RT | PASS |
| SEAPATH-00076 | kernel is realtime | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00081 | kernel is >= 4.19.106 | PASS |
| SEAPATH-00083 | syslog-ng service is running | PASS |
| SEAPATH-00084 | syslog-ng is configured to send log on network | FAIL |

- number of tests: 8
- number of failures: 1

Tests common security for node1

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00197 | Only wanted apt repositories configured: only use sources.list | PASS |
| SEAPATH-00197 | Only wanted apt repositories configured: do not add other repositories | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://ftp.fr.debian.org/debian bookworm main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://security.debian.org/debian-security bookworm-security main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: http://ftp.fr.debian.org/debian bookworm-backports main contrib non-free non-free-firmware | PASS |
| SEAPATH-00197 | Only official apt repositories configured: https://artifacts.elastic.co/packages/8.x/apt stable main | PASS |
| SEAPATH-00198 | No unrecognized packages installed | PASS |
| SEAPATH-00215 | auditd service is active | PASS |
| SEAPATH-00216 | auditd is configured to output in syslog | PASS |
| SEAPATH-00217 | insmod call is logged | PASS |
| SEAPATH-00217 | kmod call is logged | PASS |
| SEAPATH-00217 | modprobe call is logged | PASS |
| SEAPATH-00217 | rmmod call is logged | PASS |
| SEAPATH-00218 | modification in /etc/ is logged | PASS |
| SEAPATH-00219 | mount/umount call is logged | PASS |
| SEAPATH-00220 | ioperm call is logged | PASS |
| SEAPATH-00220 | prctl call is logged | PASS |
| SEAPATH-00220 | ptrace call is logged | PASS |
| SEAPATH-00221 | file deletion is logged | PASS |
| SEAPATH-00222 | open monitoring is logged | PASS |
| SEAPATH-00222 | openat monitoring is logged | PASS |
| SEAPATH-00222 | unlink monitoring is logged | PASS |
| SEAPATH-00106 | Check /etc/shadow permissions | PASS |
| SEAPATH-00107 | Check /etc/passwd permissions | PASS |
| SEAPATH-00108 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |
| SEAPATH-00049 | Check /etc/ssh/ssh_host_ed25519_key permissions | PASS |
| SEAPATH-00090 | Check /etc/ssh/ssh_host_rsa_key permissions | PASS |
| SEAPATH-00192 | All files have a known owner and group | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00193 | All directories writable by all users have the sticky bit | PASS |
| SEAPATH-00194 | All directories writable by all users are owned by root | PASS |
| SEAPATH-00195 | Ceph OSD are owned by ceph | PASS |
| SEAPATH-00196 | No unexpected file has setuid/setgid enabled | PASS |
| SEAPATH-00088 | root password was randomized at boot | PASS |
| SEAPATH-00089 | root password is randomized at each boot | PASS |
| SEAPATH-00091 | root password is encrypted with a crypto at least equivalent as sha512 | PASS |
| SEAPATH-00092 | bash timeout is set read-only to 300s | PASS |
| SEAPATH-00093 | sshd forbids setting environment variables | PASS |
| SEAPATH-00094 | sshd server time-out is set to 300s of client inactivity | PASS |
| SEAPATH-00095 | shadow encrypts passwords with SHA512 by default | PASS |
| SEAPATH-00096 | shadow encryption uses at least 65536 rounds | PASS |
| SEAPATH-00097 | pam password authentication uses sha512 with 65536 rounds or yescrypt | PASS |
| SEAPATH-00098 | password set to expire after 90 days | PASS |
| SEAPATH-00099 | 'su' is denied | PASS |
| SEAPATH-00100 | /etc/securetty is empty | PASS |
| SEAPATH-00101 | PAM securetty module is active in 'login' policy | PASS |
| SEAPATH-00202 | grub root superuser is set in /boot/grub/grub.cfg | PASS |
| SEAPATH-00203 | grub root superuser is password protected | PASS |
| SEAPATH-00204 | main menuentry is unrestricted in /boot/grub/grub.cfg | PASS |
| SEAPATH-00205 | TMPDIR env var is defined and readonly | PASS |
| SEAPATH-00206 | TMPDIR is set with 700 mode and root as owner and group | PASS |
| SEAPATH-00225 | Umask is set correctly set | PASS |
| SEAPATH-00227 | AppArmor processes are confined in enforce mode | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_YAMA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : DEBUG_WX is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SECURITY_DMESG_RESTRICT is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : LEGACY_VSYSCALL_NONE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_RANDOM is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : SLAB_FREELIST_HARDENED is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : HARDENED_USERCOPY is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : FORTIFY_SOURCE is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'hardening' : PAGE_POISONING is enabled | PASS |
| SEAPATH-00170 | Wipe slab and page allocations enabled on cmdline | PASS |
| SEAPATH-00174 | Randomize kstack offset in on | PASS |
| SEAPATH-00175 | Disable slab usercopy fallback | PASS |
| SEAPATH-00201 | LSM Yama is enabled | PASS |
| SEAPATH-00210 | MCE is disabled | PASS |
| SEAPATH-00211 | rng_core.default_quality is set to 500 | PASS |
| SEAPATH-00226 | Test AppArmor is enabled | PASS |

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00223 | All sockets are bound to an interface | PASS |
| SEAPATH-00224 | IPv6 is disabled | PASS |
| SEAPATH-00164 | sudo requires password for group operator (operator) | PASS |
| SEAPATH-00165 | sudo requires password for group maintenance-N1 (maint-n1) | PASS |
| SEAPATH-00166 | sudo requires password for group maintenance-N3 (maint-n3) | PASS |
| SEAPATH-00167 | sudo requires password for group administrator (admincluster) | PASS |
| SEAPATH-00168 | sudo requires password for group super-administrator (adminsys) | PASS |
| SEAPATH-00103 | /usr/bin/sudo exists | PASS |
| SEAPATH-00104 | /usr/bin/sudo belongs to group privileged | PASS |
| SEAPATH-00105 | /usr/bin/sudo has permissions 4750 | PASS |
| SEAPATH-00148 | sudoers files include directive noexec | PASS |
| SEAPATH-00148 | sudoers files include directive requiretty | PASS |
| SEAPATH-00148 | sudoers files include directive use_ptty | PASS |
| SEAPATH-00148 | sudoers files include directive umask=0027 | PASS |
| SEAPATH-00148 | sudoers files include directive ignore_dot | PASS |
| SEAPATH-00148 | sudoers files include directive env_reset | PASS |
| SEAPATH-00149 | sudo commands don't target privileged user | PASS |
| SEAPATH-00150 | all commands require authentication | PASS |
| SEAPATH-00152 | EXEC option is not used | PASS |
| SEAPATH-00153 | rules are not defined by negation | PASS |
| SEAPATH-00154 | sudo commands always specify arguments | PASS |
| SEAPATH-00154 | no user can run all commands as root | PASS |
| SEAPATH-00155 | sudo commands don't use wildcard * argument | PASS |
| SEAPATH-00156 | /etc/sudoers - /etc/sudoers is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/ceph-smartctl - /etc/sudoers.d/ceph-smartctl is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00156 | /etc/sudoers.d/00-security - /etc/sudoers.d/00-security is owned by root:root with 0440 permissions | PASS |
| SEAPATH-00171 | Check coredumps are disabled | PASS |
| SEAPATH-00172 | Check kexec is disabled | PASS |
| SEAPATH-00173 | Check binfmt_misc is disabled | PASS |
| SEAPATH-00176 | Check kptr_restrict is set to 2 | PASS |
| SEAPATH-00177 | Check dmesg_restrict is set to 1 | PASS |
| SEAPATH-00178 | Check pid_max is set to 4194304 | PASS |
| SEAPATH-00179 | Check perf_cpu_time_max_percent is set to 1 | PASS |
| SEAPATH-00180 | Check perf_event_max_sample_rate is set to 1 | PASS |
| SEAPATH-00181 | Check perf_event_paranoid is set to 2 | PASS |
| SEAPATH-00182 | Check randomize_va_space is set to 2 | PASS |
| SEAPATH-00183 | Check sysrq is set to 0 | PASS |

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00184 | Check unprivileged_bpf_disabled is set to 1 | PASS |
| SEAPATH-00185 | Check panic_on_oops is set to 1 | PASS |
| SEAPATH-00186 | Check kernel.yama.ptrace_scope is set to 2 | PASS |
| SEAPATH-00187 | Check suid_dumpable is set to 0 | PASS |
| SEAPATH-00188 | Check protected_fifos is set to 2 | PASS |
| SEAPATH-00189 | Check protected_regular is set to 2 | PASS |
| SEAPATH-00190 | Check protected_symlinks is set to 1 | PASS |
| SEAPATH-00191 | Check protected_hardlinks is set to 1 | PASS |
| SEAPATH-00082 | /var/log is mounted on a separate partition | PASS |
| SEAPATH-00085 | syslog-ng can not acquire new privileges | PASS |
| SEAPATH-00086 | syslog-ng capabilities are bounded | PASS |
| SEAPATH-00087 | syslog-ng system calls are filtered | PASS |
| SEAPATH-00199 | No systemd service failed | PASS |
| SEAPATH-00200 | No unrecognized service enabled | PASS |

- number of tests: 119
- number of failures: 1

Tests hypervisor for node1

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00044 | Check /etc/syslog-ng/cert.d/clientcert.pem permissions | FAIL |
| SEAPATH-00045 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions | FAIL |
| SEAPATH-00035 | ovs-vswitchd service is running | PASS |
| SEAPATH-00035 | ovsdb-server service is running | PASS |
| SEAPATH-00038 | lspci 3.6.2+ is available | PASS |
| SEAPATH-00018 | KVM device available | PASS |
| SEAPATH-00019 | Qemu for x86-64 available | PASS |
| SEAPATH-00020 | Libvirtd service is running | PASS |
| SEAPATH-00021 | IPv4 NAT is available | PASS |

- number of tests: 9
- number of failures: 2

Tests hypervisor iommu for node1

| Test ID | Tests | Results |
|---------------|---|---------|
| SEAPATH-00030 | iommu enabled in passthrough mode | PASS |
| SEAPATH-00031 | iommu is loaded | FAIL |
| SEAPATH-00032 | iommu is populated | FAIL |
| SEAPATH-00050 | Linux kernel 'iommu' : INTEL_IOMMU is enabled | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00050 | Linux kernel 'iommu' : AMD_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : IOMMU_IOVA is enabled | PASS |
| SEAPATH-00050 | Linux kernel 'iommu' : DMAR_TABLE is enabled | PASS |

- number of tests: 7
- number of failures: 2

Tests hypervisor security for node1

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00033 | /etc/group is consistent | PASS |
| SEAPATH-00033 | /etc/gshadow is consistent | PASS |
| SEAPATH-00034 | /etc/group does not include extra group | PASS |
| SEAPATH-00034 | /etc/gshadow does not include extra group | PASS |
| SEAPATH-00008 | Slab merging is disabled on cmdline | PASS |
| SEAPATH-00009 | Kernel Page Table Isolation is always enabled on cmdline | PASS |
| SEAPATH-00010 | SLUB redzoning and sanity checking enabled on cmdline | PASS |
| SEAPATH-00207 | CPU has no known vulnerabilities | PASS |
| SEAPATH-00047 | /etc/passwd is consistent | PASS |
| SEAPATH-00048 | /etc/passwd does not include extra user | PASS |
| SEAPATH-00046 | /etc/shadow is consistent | PASS |
| SEAPATH-00015 | Vulnerabilities sysfs entry exist | PASS |
| SEAPATH-00017 | System is not vulnerable to : meltdown | PASS |
| SEAPATH-00017 | System is not vulnerable to : l1tf | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v1 | PASS |
| SEAPATH-00017 | System is not vulnerable to : spectre_v2 | PASS |

- number of tests: 16
- number of failures: 0

Tests cluster for ci121

| Test ID | Tests | Results |
|---------------|---------------------------------------|---------|
| SEAPATH-00051 | health is not error | PASS |
| SEAPATH-00052 | 3 monitors are configured | PASS |
| SEAPATH-00053 | 3 monitors are up | PASS |
| SEAPATH-00054 | at least 2 osds are configured and up | PASS |
| SEAPATH-00055 | a manager is active | PASS |
| SEAPATH-00119 | corosync service is running | PASS |
| SEAPATH-00122 | pacemaker service is running | PASS |
| SEAPATH-00063 | no OFFLINE node | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00064 | 3 nodes are configured | PASS |
| SEAPATH-00065 | list secrets | PASS |
| SEAPATH-00066 | define VM from a valid configuration | PASS |
| SEAPATH-00067 | define VM from a valid configuration | PASS |
| SEAPATH-00068 | list VM | PASS |
| SEAPATH-00069 | export VM configuration | PASS |
| SEAPATH-00070 | VM configuration has been export | PASS |
| SEAPATH-00071 | Test add VM | PASS |
| SEAPATH-00072 | Test stop VM | PASS |
| SEAPATH-00073 | Test start VM | PASS |
| SEAPATH-00074 | Test remove VM | PASS |
| SEAPATH-00306 | Test clone disk | PASS |
| SEAPATH-00307 | Test groups | PASS |
| SEAPATH-00308 | Test namespaces | PASS |
| SEAPATH-00309 | Test metadata | PASS |
| SEAPATH-00060 | Test snapshots | PASS |
| SEAPATH-00061 | Test snapshots rollback | PASS |
| SEAPATH-00062 | Test write rbd | PASS |
| SEAPATH-00129 | ceph-crash system calls are filtered | PASS |
| SEAPATH-00130 | ceph-mon system calls are filtered | PASS |
| SEAPATH-00131 | ceph-mgr system calls are filtered | PASS |
| SEAPATH-00132 | ceph-osd system calls are filtered | PASS |
| SEAPATH-00120 | corosync can not acquire new privileges | PASS |
| SEAPATH-00121 | corosync capabilities are bounded | PASS |
| SEAPATH-00128 | corosync system calls are filtered | PASS |
| SEAPATH-00123 | pacemaker can not acquire new privileges | PASS |
| SEAPATH-00124 | pacemaker capabilities are bounded | PASS |
| SEAPATH-00133 | pacemakerd system calls are filtered | PASS |
| SEAPATH-00134 | pacemaker-based system calls are filtered | PASS |
| SEAPATH-00135 | pacemaker-fenced system calls are filtered | PASS |
| SEAPATH-00136 | pacemaker-execd system calls are filtered | PASS |
| SEAPATH-00137 | pacemaker-attribd system calls are filtered | PASS |
| SEAPATH-00138 | pacemaker-schedulerd system calls are filtered | PASS |
| SEAPATH-00139 | pacemaker-controld system calls are filtered | PASS |
| SEAPATH-00133 | pacemakerd system calls are filtered | PASS |
| SEAPATH-00134 | pacemaker-based system calls are filtered | PASS |
| SEAPATH-00135 | pacemaker-fenced system calls are filtered | PASS |
| SEAPATH-00136 | pacemaker-execd system calls are filtered | PASS |
| SEAPATH-00137 | pacemaker-attribd system calls are filtered | PASS |
| SEAPATH-00138 | pacemaker-schedulerd system calls are filtered | PASS |

| Test ID | Tests | Results |
|---------------|--|---------|
| SEAPATH-00139 | pacemaker-controld system calls are filtered | PASS |
| SEAPATH-00133 | pacemakerd system calls are filtered | PASS |
| SEAPATH-00134 | pacemaker-based system calls are filtered | PASS |
| SEAPATH-00135 | pacemaker-fenced system calls are filtered | PASS |
| SEAPATH-00136 | pacemaker-execd system calls are filtered | PASS |
| SEAPATH-00137 | pacemaker-attribd system calls are filtered | PASS |
| SEAPATH-00138 | pacemaker-schedulerd system calls are filtered | PASS |
| SEAPATH-00139 | pacemaker-controld system calls are filtered | PASS |
| SEAPATH-00133 | pacemakerd system calls are filtered | PASS |
| SEAPATH-00134 | pacemaker-based system calls are filtered | PASS |
| SEAPATH-00135 | pacemaker-fenced system calls are filtered | PASS |
| SEAPATH-00136 | pacemaker-execd system calls are filtered | PASS |
| SEAPATH-00137 | pacemaker-attribd system calls are filtered | PASS |
| SEAPATH-00138 | pacemaker-schedulerd system calls are filtered | PASS |
| SEAPATH-00139 | pacemaker-controld system calls are filtered | PASS |
| SEAPATH-00133 | pacemakerd system calls are filtered | PASS |
| SEAPATH-00134 | pacemaker-based system calls are filtered | PASS |
| SEAPATH-00135 | pacemaker-fenced system calls are filtered | PASS |
| SEAPATH-00136 | pacemaker-execd system calls are filtered | PASS |
| SEAPATH-00137 | pacemaker-attribd system calls are filtered | PASS |
| SEAPATH-00138 | pacemaker-schedulerd system calls are filtered | PASS |
| SEAPATH-00139 | pacemaker-controld system calls are filtered | PASS |
| SEAPATH-00133 | pacemakerd system calls are filtered | PASS |
| SEAPATH-00134 | pacemaker-based system calls are filtered | PASS |
| SEAPATH-00135 | pacemaker-fenced system calls are filtered | PASS |
| SEAPATH-00136 | pacemaker-execd system calls are filtered | PASS |
| SEAPATH-00137 | pacemaker-attribd system calls are filtered | PASS |
| SEAPATH-00138 | pacemaker-schedulerd system calls are filtered | PASS |
| SEAPATH-00139 | pacemaker-controld system calls are filtered | PASS |
| SEAPATH-00133 | pacemakerd system calls are filtered | PASS |
| SEAPATH-00134 | pacemaker-based system calls are filtered | PASS |
| SEAPATH-00135 | pacemaker-fenced system calls are filtered | PASS |
| SEAPATH-00136 | pacemaker-execd system calls are filtered | PASS |
| SEAPATH-00137 | pacemaker-attribd system calls are filtered | PASS |
| SEAPATH-00138 | pacemaker-schedulerd system calls are filtered | PASS |
| SEAPATH-00139 | pacemaker-controld system calls are filtered | PASS |

- number of tests: 82
- number of failures: 0

Compliance Matrix

Matrix include/ANSSI-BP28-Recommandations-M.csv

| Requirement | Test id | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R30 | SEAPATH-00048 | PASS |
| ANSSI-BP28-R53 | SEAPATH-00192 | FAIL |
| ANSSI-BP28-R54 | SEAPATH-00193 | PASS |
| | SEAPATH-00194 | PASS |
| ANSSI-BP28-R56 | SEAPATH-00196 | PASS |
| ANSSI-BP28-R58 | SEAPATH-00198 | PASS |
| ANSSI-BP28-R59 | SEAPATH-00197 | PASS |
| ANSSI-BP28-R62 | SEAPATH-00200 | PASS |
| ANSSI-BP28-R68 | SEAPATH-00088 | PASS |
| | SEAPATH-00089 | PASS |
| | SEAPATH-00091 | PASS |
| | SEAPATH-00095 | PASS |
| | SEAPATH-00098 | PASS |
| | SEAPATH-00203 | PASS |
| ANSSI-BP28-R80 | SEAPATH-00223 | PASS |

Matrix include/ANSSI-BP28-Recommandations-MI.csv

| Requirement | Test id | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R11 | SEAPATH-00186 | PASS |
| | SEAPATH-00201 | PASS |
| ANSSI-BP28-R12 | SEAPATH-00173 | PASS |
| ANSSI-BP28-R13 | SEAPATH-00224 | PASS |
| ANSSI-BP28-R14 | SEAPATH-00187 | PASS |
| | SEAPATH-00188 | PASS |
| | SEAPATH-00189 | PASS |
| | SEAPATH-00190 | PASS |
| | SEAPATH-00191 | PASS |
| ANSSI-BP28-R32 | SEAPATH-00092 | PASS |
| ANSSI-BP28-R34 | SEAPATH-00046 | PASS |
| ANSSI-BP28-R39 | SEAPATH-00148 | PASS |
| ANSSI-BP28-R40 | SEAPATH-00149 | PASS |
| ANSSI-BP28-R42 | SEAPATH-00153 | PASS |
| ANSSI-BP28-R43 | SEAPATH-00154 | PASS |
| | SEAPATH-00155 | PASS |
| ANSSI-BP28-R5 | SEAPATH-00203 | PASS |

| Requirement | Test id | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R55 | SEAPATH-00205 | PASS |
| | SEAPATH-00206 | PASS |
| ANSSI-BP28-R79 | SEAPATH-00085 | PASS |
| | SEAPATH-00086 | PASS |
| | SEAPATH-00087 | PASS |
| | SEAPATH-00120 | PASS |
| | SEAPATH-00121 | PASS |
| | SEAPATH-00123 | PASS |
| | SEAPATH-00124 | PASS |
| | SEAPATH-00128 | PASS |
| | SEAPATH-00129 | PASS |
| | SEAPATH-00130 | PASS |
| | SEAPATH-00131 | PASS |
| | SEAPATH-00132 | PASS |
| | SEAPATH-00133 | PASS |
| | SEAPATH-00134 | PASS |
| | SEAPATH-00135 | PASS |
| | SEAPATH-00136 | PASS |
| | SEAPATH-00137 | PASS |
| | SEAPATH-00138 | PASS |
| ANSSI-BP28-R8 | SEAPATH-00207 | PASS |
| ANSSI-BP28-R9 | SEAPATH-00176 | PASS |
| | SEAPATH-00177 | PASS |
| | SEAPATH-00178 | PASS |
| | SEAPATH-00179 | PASS |
| | SEAPATH-00180 | PASS |
| | SEAPATH-00181 | PASS |
| | SEAPATH-00182 | PASS |
| | SEAPATH-00183 | PASS |
| | SEAPATH-00184 | PASS |
| | SEAPATH-00185 | PASS |

Matrix include/ANSSI-BP28-Recommandations-MIR.csv

| Requirement | Test id | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R36 | SEAPATH-00148 | PASS |
| | SEAPATH-00225 | PASS |
| ANSSI-BP28-R37 | SEAPATH-00226 | PASS |
| ANSSI-BP28-R38 | SEAPATH-00104 | PASS |

| Requirement | Test id | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R45 | SEAPATH-00226 | PASS |
| | SEAPATH-00227 | PASS |
| ANSSI-BP28-R64 | SEAPATH-00085 | PASS |
| | SEAPATH-00086 | PASS |
| | SEAPATH-00120 | PASS |
| | SEAPATH-00121 | PASS |
| | SEAPATH-00123 | PASS |
| | SEAPATH-00124 | PASS |
| ANSSI-BP28-R65 | SEAPATH-00087 | PASS |
| | SEAPATH-00128 | PASS |
| | SEAPATH-00129 | PASS |
| | SEAPATH-00130 | PASS |
| | SEAPATH-00131 | PASS |
| | SEAPATH-00132 | PASS |
| | SEAPATH-00133 | PASS |
| | SEAPATH-00134 | PASS |
| | SEAPATH-00135 | PASS |
| | SEAPATH-00136 | PASS |
| | SEAPATH-00137 | PASS |
| | SEAPATH-00138 | PASS |
| | SEAPATH-00139 | PASS |
| ANSSI-BP28-R71 | SEAPATH-00044 | FAIL |
| | SEAPATH-00045 | FAIL |
| | SEAPATH-00083 | PASS |
| | SEAPATH-00084 | FAIL |
| | SEAPATH-00108 | FAIL |
| ANSSI-BP28-R72 | SEAPATH-00199 | PASS |
| ANSSI-BP28-R73 | SEAPATH-00215 | PASS |
| | SEAPATH-00216 | PASS |

About this documentation

This documentation uses the AsciiDoc documentation generator. It is a convenient format that allows using plain-text formatted writing that can later be converted to various output formats such as HTML and PDF.

In order to generate an HTML version of this documentation, use the following command (the asciidoc package will need to be installed in your Linux distribution):

```
$ asciidoc test-report.adoc
```

This will result in a README.html file being generated in the current directory.

If you prefer a PDF version of the documentation instead, use the following command (the dlatex package will need to be installed on your Linux distribution):

```
$ asciidoctor-pdf test-report.adoc
```