



TEST REPORT

Table of Contents

Prerequisites	1
Test reports.....	2
Tests common_security for virtu-ci1	2
Tests hypervisorsecurity for virtu-ci1	6
Tests hypervisoriommu for virtu-ci1	7
Tests cluster for virtu-ci1	7
Notes	10
About this documentation	11

Prerequisites

Test reports

Tests common_security for virtu-ci1

Test ID	Tests	Results
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-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-00050	Linux kernel <i>hardening</i> : SECURITY_YAMA is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : DEBUG_WX is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : SECURITY_DMESG_RESTRICT is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : RETPOLINE is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : LEGACY_VSYSCALL_NONE is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : STATIC_USERMODEHELPER is enabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : USERFAULTFD is disabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : X86_VSYSCALL_EMULATION is disabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : MODIFY_LDT_SYSCALL is disabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : DEVMEM is disabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : USELIB is disabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : PROC_KCORE is disabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : KALLSYMS is disabled	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : SLAB_FREELIST_RANDOM is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : SLAB_FREELIST_HARDENED is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : HARDENED_USERCOPY is enabled	PASS
SEAPATH-00050	Linux kernel <i>hardening</i> : FORTIFY_SOURCE is enabled	PASS

Test ID	Tests	Results
SEAPATH-00050	Linux kernel <i>hardening</i> : PAGE_POISONING is enabled	PASS
SEAPATH-00050	Linux kernel <i>gcc_plugins</i> : GCC_PLUGIN_LATENT_ENTROPY is enabled	FAIL
SEAPATH-00050	Linux kernel <i>gcc_plugins</i> : GCC_PLUGIN_RANDSTRUCT is enabled	FAIL
SEAPATH-00050	Linux kernel <i>gcc_plugins</i> : GCC_PLUGIN_STRUCTLEAK_BYREF_ALL is enabled	FAIL
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-00158	sudo policy is installed for group operator (operator)	FAIL
SEAPATH-00159	sudo policy is installed for group maintenance-N1 (maint-n1)	FAIL
SEAPATH-00160	sudo policy is installed for group maintenance-N3 (maint-n3)	FAIL
SEAPATH-00161	sudo policy is installed for group cluster administrator (admincluster)	FAIL
SEAPATH-00162	sudo policy is installed for group system administrator (adminsys)	FAIL
SEAPATH-00163	sudo policy is installed for group ansible (ansible)	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-00169	sudo requires password for group ansible (ansible)	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-00143	/etc/sudoers include noexec directive	FAIL
SEAPATH-00144	/etc/sudoers include requiretty directive	FAIL
SEAPATH-00145	/etc/sudoers include use_pty directive	FAIL
SEAPATH-00146	/etc/sudoers include umask=0027 directive	FAIL
SEAPATH-00147	/etc/sudoers include ignore_dot directive	FAIL
SEAPATH-00148	/etc/sudoers include env_reset directive	PASS
SEAPATH-00149	/etc/sudoers include passwd_timeout=1 directive	FAIL
SEAPATH-00150	/etc/sudoers all commands require authentication	PASS
SEAPATH-00151	/etc/sudoers no rule target root user	FAIL
SEAPATH-00152	/etc/sudoers EXEC option is not used	PASS
SEAPATH-00153	/etc/sudoers rules are not defined by negation	PASS
SEAPATH-00154	/etc/sudoers commands are not specified without arguments	PASS
SEAPATH-00155	/etc/sudoers no command is specified with wildcard argument	PASS
SEAPATH-00156	/etc/sudoers /etc/sudoers is owned by root:root with 0440 permissions	PASS
SEAPATH-00150	/etc/sudoers.d/virtu all commands require authentication	PASS
SEAPATH-00151	/etc/sudoers.d/virtu no rule target root user	PASS
SEAPATH-00152	/etc/sudoers.d/virtu EXEC option is not used	PASS
SEAPATH-00153	/etc/sudoers.d/virtu rules are not defined by negation	PASS

Test ID	Tests	Results
SEAPATH-00154	/etc/sudoers.d/virtu commands are not specified without arguments	PASS
SEAPATH-00155	/etc/sudoers.d/virtu no command is specified with wildcard argument	PASS
SEAPATH-00156	/etc/sudoers.d/virtu /etc/sudoers.d/virtu is owned by root:root with 0440 permissions	PASS
SEAPATH-00150	/etc/sudoers.d/Debian-snmp all commands require authentication	PASS
SEAPATH-00151	/etc/sudoers.d/Debian-snmp no rule target root user	PASS
SEAPATH-00152	/etc/sudoers.d/Debian-snmp EXEC option is not used	PASS
SEAPATH-00153	/etc/sudoers.d/Debian-snmp rules are not defined by negation	PASS
SEAPATH-00154	/etc/sudoers.d/Debian-snmp commands are not specified without arguments	PASS
SEAPATH-00155	/etc/sudoers.d/Debian-snmp no command is specified with wildcard argument	PASS
SEAPATH-00156	/etc/sudoers.d/Debian-snmp /etc/sudoers.d/Debian-snmp is owned by root:root with 0440 permissions	PASS
SEAPATH-00150	/etc/sudoers.d/ceph-osd-smartctl all commands require authentication	PASS
SEAPATH-00151	/etc/sudoers.d/ceph-osd-smartctl no rule target root user	PASS
SEAPATH-00152	/etc/sudoers.d/ceph-osd-smartctl EXEC option is not used	PASS
SEAPATH-00153	/etc/sudoers.d/ceph-osd-smartctl rules are not defined by negation	PASS
SEAPATH-00154	/etc/sudoers.d/ceph-osd-smartctl commands are not specified without arguments	PASS
SEAPATH-00155	/etc/sudoers.d/ceph-osd-smartctl no command is specified with wildcard argument	PASS
SEAPATH-00156	/etc/sudoers.d/ceph-osd-smartctl /etc/sudoers.d/ceph-osd-smartctl is owned by root:root with 0440 permissions	PASS
SEAPATH-00150	/etc/sudoers.d/ansible all commands require authentication	PASS
SEAPATH-00151	/etc/sudoers.d/ansible no rule target root user	PASS
SEAPATH-00152	/etc/sudoers.d/ansible EXEC option is not used	PASS
SEAPATH-00153	/etc/sudoers.d/ansible rules are not defined by negation	PASS
SEAPATH-00154	/etc/sudoers.d/ansible commands are not specified without arguments	PASS
SEAPATH-00155	/etc/sudoers.d/ansible no command is specified with wildcard argument	PASS
SEAPATH-00156	/etc/sudoers.d/ansible /etc/sudoers.d/ansible is owned by root:root with 0440 permissions	PASS
SEAPATH-00150	/etc/sudoers.d/admin all commands require authentication	PASS
SEAPATH-00151	/etc/sudoers.d/admin no rule target root user	PASS
SEAPATH-00152	/etc/sudoers.d/admin EXEC option is not used	PASS
SEAPATH-00153	/etc/sudoers.d/admin rules are not defined by negation	PASS
SEAPATH-00154	/etc/sudoers.d/admin commands are not specified without arguments	PASS
SEAPATH-00155	/etc/sudoers.d/admin no command is specified with wildcard argument	PASS
SEAPATH-00156	/etc/sudoers.d/admin /etc/sudoers.d/admin is owned by root:root with 0440 permissions	PASS
SEAPATH-00109	panicreboot kernel.panic is set properly	PASS
SEAPATH-00109	schedrt kernel.sched_rt_runtime_us is set properly	PASS
SEAPATH-00109	schedrt kernel.printk is set properly	PASS
SEAPATH-00109	schedrt kernel.printk_devkmsg is set properly	PASS
SEAPATH-00109	ceph-osd fs.aio-max-nr is set properly	PASS
SEAPATH-00109	ceph-osd kernel.pid_max is set properly	PASS
SEAPATH-00109	coredump kernel.core_pattern is set properly	PASS
SEAPATH-00109	kexec kernel.kexec_load_disabled is set properly	PASS

Test ID	Tests	Results
SEAPATH-00109	sysctl-hardening dev.tty.ldisc_autoload is set properly	PASS
SEAPATH-00109	sysctl-hardening fs.protected_fifos is set properly	PASS
SEAPATH-00109	sysctl-hardening fs.protected_regular is set properly	PASS
SEAPATH-00109	sysctl-hardening fs.protected_hardlinks is set properly	PASS
SEAPATH-00109	sysctl-hardening fs.protected_symlinks is set properly	PASS
SEAPATH-00109	sysctl-hardening fs.suid_dumpable is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.dmesg_restrict is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.kptr_restrict is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.perf_event_paranoid is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.randomize_va_space is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.sysrq is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.unprivileged_bpf_disabled is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.yama.ptrace_scope is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.perf_event_max_sample_rate is set properly	PASS
SEAPATH-00109	sysctl-hardening kernel.perf_cpu_time_max_percent is set properly	PASS
SEAPATH-00109	sysctl-hardening vm.mmap_min_addr is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.all.accept_redirects is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.all.accept_source_route is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.all.log_martians is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.all.rp_filter is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.all.secure_redirects is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.all.send_redirects is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.all.shared_media is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.default.accept_redirects is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.default.accept_source_route is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.default.log_martians is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.default.rp_filter is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.default.secure_redirects is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.default.send_redirects is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.conf.default.shared_media is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.icmp_echo_ignore_broadcasts is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.icmp_ignore_bogus_error_responses is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.tcp_invalid_ratelimit is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.tcp_max_syn_backlog is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.tcp_rfc1337 is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.tcp_syn_retries is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.tcp_synack_retries is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.tcp_syncookies is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.tcp_timestamps is set properly	PASS
SEAPATH-00109	sysctl-network net.ipv4.ip_local_port_range is set properly	PASS

Test ID	Tests	Results
SEAPATH-00109	sysctl-network net.ipv4.tcp_challenge_ack_limit is set properly	PASS
SEAPATH-00109	sysctl-network net.netfilter.nf_conntrack_tcp_loose is set properly	PASS
SEAPATH-00109	ceph-tuning fs.aio-max-nr is set properly	PASS
SEAPATH-00109	ceph-tuning fs.file-max is set properly	PASS
SEAPATH-00109	ceph-tuning vm.zone_reclaim_mode is set properly	PASS
SEAPATH-00109	ceph-tuning vm.swappiness is set properly	PASS
SEAPATH-00109	ceph-tuning vm.min_free_kbytes is set properly	PASS
SEAPATH-00171	Check coredumps are disabled	PASS
SEAPATH-00172	Check kexec is disabled	PASS
SEAPATH-00173	Check binfmt_misc is disabled	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

- number of tests: 114
- number of failures: 24

Tests hypervisorsecurity for virtu-ci1

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	FAIL
SEAPATH-00034	/etc/gshadow does not include extra group	FAIL
SEAPATH-00006	Audit subsystem is disabled on cmdline	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-00004	libvirtd can not acquire new privileges	FAIL
SEAPATH-00005	libvirtd capabilities are bounded	FAIL
SEAPATH-00125	libvirtd system calls are filtered	FAIL
SEAPATH-00039	openvswitch user is created and locked	FAIL
SEAPATH-00040	openvswitch user is part of hugepages group	FAIL
SEAPATH-00041	openvswitch user is part of vfio-net group	FAIL
SEAPATH-00042	ovs-vswitchd is running as user openvswitch	FAIL
SEAPATH-00043	ovsdb-server is running as user openvswitch	FAIL
SEAPATH-00126	ovs-vswitchd system calls are filtered	PASS
SEAPATH-00127	ovsdb-server system calls are filtered	PASS
SEAPATH-00047	/etc/passwd is consistent	PASS
SEAPATH-00048	/etc/passwd does not include extra user	FAIL

Test ID	Tests	Results
SEAPATH-00046	/etc/shadow is consistent	FAIL
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
SEAPATH-00012	admin user exists	PASS
SEAPATH-00013	admin has a password	PASS
SEAPATH-00014	admin is sudoers	PASS

- number of tests: 29
- number of failures: 14

Tests hypervisoriommu for virtu-ci1

Test ID	Tests	Results
SEAPATH-00030	iommu enabled in passthrough mode	PASS
SEAPATH-00031	iommu is loaded	PASS
SEAPATH-00032	iommu is populated	PASS
SEAPATH-00050	Linux kernel <i>iommu</i> : INTEL_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel <i>iommu</i> : AMD_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel <i>iommu</i> : AMD_IOMMU_V2 is enabled	PASS
SEAPATH-00050	Linux kernel <i>iommu</i> : IOMMU_IOVA is enabled	PASS

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

Tests cluster for virtu-ci1

Test ID	Tests	Results
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

Test ID	Tests	Results
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-attd system calls are filtered	PASS
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	PASS

- number of tests: 58
- number of failures: 0

Notes

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 main.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 dblatex package will need to be installed on your Linux distribution):

```
$ asciidoctor-pdf main.adoc
```