TEST REPORT

Table of Contents

Prerequisites

Test reports

Tests common for virtu-ci1

Test ID	Tests	Results
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* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : LEGACY_VSYSCALL_NONE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : STATIC_USERMODEHELPER is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USERFAULTFD is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : X86_VSYSCALL_EMULATION is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : MODIFY_LDT_SYSCALL is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : DEVMEM is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USELIB is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KEXEC is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : BINFMT_MISC is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : ALLOW_DEV_COREDUMP is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : PROC_KCORE is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KALLSYMS is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : SLUB_DEBUG_ON is enabled	FAIL
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* : SLUB_DEBUG_ON is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : HARDENED_USERCOPY is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : HARDENED_USERCOPY_FALLBACK is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : FORTIFY_SOURCE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : PAGE_POISONING is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RANDOMIZE_KSTACK_OFFSET_DEFAULT is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : INIT_ON_ALLOC_DEFAULT_ON is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : INIT_ON_FREE_DEFAULT_ON is enabled	FAIL
SEAPATH-00050	Linux kernel *misc* : EFI_PARTITION is enabled	PASS
SEAPATH-00050	Linux kernel *reporting* : EDAC is enabled	PASS
SEAPATH-00050	Linux kernel *usb* : USB_OHCI_HCD is enabled	FAIL
SEAPATH-00050	Linux kernel *usb* : USB_EHCI_HCD is enabled	FAIL
SEAPATH-00050	Linux kernel *usb* : USB_XHCI_HCD is enabled	FAIL
SEAPATH-00078	no paging error	PASS
SEAPATH-00079	no rcu stall	PASS
SEAPATH-00080	no backtraces	PASS

Test ID	Tests	Results
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: 42
- number of failures: 19

Tests future_common_security for virtu-ci1

Test ID	Tests	Results
SEAPATH-00050	Linux kernel *hardening* : STATIC_USERMODEHELPER is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USERFAULTFD is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : X86_VSYSCALL_EMULATION is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : MODIFY_LDT_SYSCALL is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : DEVMEM is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USELIB is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : PROC_KCORE is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KALLSYMS is disabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_LATENT_ENTROPY is enabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_RANDSTRUCT is enabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_STRUCTLEAK_BYREF_ALL is enabled	FAIL
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-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-00149	/etc/sudoers include passwd_timeout=1 directive	FAIL
SEAPATH-00151	/etc/sudoers no rule target root user	FAIL

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

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	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00176	All files have a known owner and group	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 cryto 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 *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* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE 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-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

Test ID	Tests	Results
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-00148	/etc/sudoers include env_reset directive	PASS
SEAPATH-00150	/etc/sudoers all commands require authentication	PASS
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/ansible all commands require authentication	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/virtu all commands require authentication	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
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-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/admin all commands require authentication	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-00150	/etc/sudoers.d/ceph-osd-smartctl all commands require authentication	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

Test ID	Tests	Results
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-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
SEAPATH-00087	syslog-ng system calls are filtered	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	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00176	All files have a known owner and group	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 cryto 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 *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* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE 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

Test ID	Tests	Results
SEAPATH-00174	Randomize kstack offset in on	PASS
SEAPATH-00175	Disable slab usercopy fallback	PASS
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-00148	/etc/sudoers include env_reset directive	PASS
SEAPATH-00150	/etc/sudoers all commands require authentication	PASS
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/ansible all commands require authentication	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/virtu all commands require authentication	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
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-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/admin all commands require authentication	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

Test ID	Tests	Results
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-00150	/etc/sudoers.d/ceph-osd-smartctl all commands require authentication	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-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: 174
- number of failures: 0

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	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-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
SEAPATH-00012	admin user exists	PASS
SEAPATH-00013	admin has a password	PASS

- number of tests: 17
- number of failures: 0

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 *iommu* : INTEL_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : AMD_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : AMD_IOMMU_V2 is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : 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
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-attrd 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

Test ID	Tests	Results
SEAPATH-00137	pacemaker-attrd 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-attrd 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-attrd 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-attrd 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-attrd 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-attrd system calls are filtered	PASS
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	PASS

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

Tests hypervisor for virtu-ci1

Test ID	Tests	Results
SEAPATH-00027	auditd is inactive	PASS
SEAPATH-00044	Check /etc/syslog-ng/cert.d/clientcert.pem permissions	FAIL
SEAPATH-00045	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	PASS
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_GRE is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_VXLAN is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_GENEVE is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : TRIM_UNUSED_KSYMS is disabled	PASS
SEAPATH-00050	Linux kernel *ovs* : NET_IPGRE is enabled	FAIL
SEAPATH-00050	Linux kernel *dpdk* : UIO is enabled	FAIL
SEAPATH-00050	Linux kernel *dpdk* : VFIO_PCI is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : IGB is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : TIGON3 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : R8169 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : E1000 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : E1000E is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : X86_PKG_TEMP_THERMAL is enabled	FAIL
SEAPATH-00050	Linux kernel *ceph* : AIO is enabled	PASS
SEAPATH-00050	Linux kernel *ceph* : TMPFS is enabled	PASS
SEAPATH-00050	Linux kernel *ceph* : MD is enabled	PASS
SEAPATH-00050	Linux kernel *kvm* : KVM is enabled	FAIL
SEAPATH-00050	Linux kernel *kvm* : KVM_INTEL is enabled	FAIL
SEAPATH-00050	Linux kernel *kvm* : KVM_VFIO is enabled	PASS
SEAPATH-00007	SMT is activated	PASS
SEAPATH-00003	libvirtd service is running	PASS
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
SEAPATH-00023	SPICE protocol is not installed	FAIL
SEAPATH-00006	Audit subsystem is disabled on cmdline	FAIL
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

Test ID	Tests	Results
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-00023	SPICE protocol is not installed	FAIL
SEAPATH-00030	iommu enabled in passthrough mode	PASS
SEAPATH-00031	iommu is loaded	PASS
SEAPATH-00032	iommu is populated	PASS
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* : AMD_IOMMU_V2 is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : IOMMU_IOVA is enabled	PASS

- number of tests: 53
- number of failures: 27

Tests hypervisorreadonly for virtu-ci1

Test ID	Tests	Results
SEAPATH-00140	rootfs is readonly mounted	PASS
SEAPATH-00141	/etc is mounted as overlayfs	FAIL
SEAPATH-00141	/home is mounted as overlayfs	FAIL
SEAPATH-00141	/usr/lib/python3.8/site-packages/*pycache* is mounted as overlayfs	FAIL
SEAPATH-00141	/var/cache is mounted as overlayfs	FAIL
SEAPATH-00141	/var/lib is mounted as overlayfs	FAIL
SEAPATH-00141	/var/spool is mounted as overlayfs	FAIL
SEAPATH-00142	Kernel OVERLAY_FS is set	FAIL
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-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

Test ID	Tests	Results
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

- number of tests: 25
- number of failures: 7

Tests common for virtu-ci3

Test ID	Tests	Results
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* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : LEGACY_VSYSCALL_NONE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : STATIC_USERMODEHELPER is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USERFAULTFD is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : X86_VSYSCALL_EMULATION is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : MODIFY_LDT_SYSCALL is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : DEVMEM is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USELIB is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KEXEC is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : BINFMT_MISC is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : ALLOW_DEV_COREDUMP is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : PROC_KCORE is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KALLSYMS is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : SLUB_DEBUG_ON is enabled	FAIL
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* : SLUB_DEBUG_ON is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : HARDENED_USERCOPY is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : HARDENED_USERCOPY_FALLBACK is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : FORTIFY_SOURCE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : PAGE_POISONING is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RANDOMIZE_KSTACK_OFFSET_DEFAULT is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : INIT_ON_ALLOC_DEFAULT_ON is enabled	PASS

Test ID	Tests	Results
SEAPATH-00050	Linux kernel *hardening* : INIT_ON_FREE_DEFAULT_ON is enabled	FAIL
SEAPATH-00050	Linux kernel *misc* : EFI_PARTITION is enabled	PASS
SEAPATH-00050	Linux kernel *reporting* : EDAC is enabled	PASS
SEAPATH-00050	Linux kernel *usb* : USB_OHCI_HCD is enabled	FAIL
SEAPATH-00050	Linux kernel *usb* : USB_EHCI_HCD is enabled	FAIL
SEAPATH-00050	Linux kernel *usb* : USB_XHCI_HCD is enabled	FAIL
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: 42
- number of failures: 19

Tests future_common_security for virtu-ci3

Test ID	Tests	Results
SEAPATH-00050	Linux kernel *hardening* : STATIC_USERMODEHELPER is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USERFAULTFD is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : X86_VSYSCALL_EMULATION is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : MODIFY_LDT_SYSCALL is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : DEVMEM is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USELIB is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : PROC_KCORE is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KALLSYMS is disabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_LATENT_ENTROPY is enabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_RANDSTRUCT is enabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_STRUCTLEAK_BYREF_ALL is enabled	FAIL
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-00143	/etc/sudoers include noexec directive	FAIL
SEAPATH-00144	/etc/sudoers include requiretty directive	FAIL
SEAPATH-00145	/etc/sudoers include use_pty directive	FAIL

Test ID	Tests	Results
SEAPATH-00146	/etc/sudoers include umask=0027 directive	FAIL
SEAPATH-00147	/etc/sudoers include ignore_dot directive	FAIL
SEAPATH-00149	/etc/sudoers include passwd_timeout=1 directive	FAIL
SEAPATH-00151	/etc/sudoers no rule target root user	FAIL

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

Tests common_security for virtu-ci3

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	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00176	All files have a known owner and group	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 cryto 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 *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* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE 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

Test ID	Tests	Results
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-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-00148	/etc/sudoers include env_reset directive	PASS
SEAPATH-00150	/etc/sudoers all commands require authentication	PASS
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/admin all commands require authentication	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-00150	/etc/sudoers.d/virtu all commands require authentication	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
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-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/ansible all commands require authentication	PASS

Test ID	Tests	Results
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/ceph-osd-smartctl all commands require authentication	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-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
SEAPATH-00087	syslog-ng system calls are filtered	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	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00176	All files have a known owner and group	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 cryto 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 *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

Test ID	Tests	Results
SEAPATH-00050	Linux kernel *hardening* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE 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-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-00148	/etc/sudoers include env_reset directive	PASS
SEAPATH-00150	/etc/sudoers all commands require authentication	PASS
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/admin all commands require authentication	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-00150	/etc/sudoers.d/virtu all commands require authentication	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
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

Test ID	Tests	Results
SEAPATH-00150	/etc/sudoers.d/Debian-snmp all commands require authentication	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/ansible all commands require authentication	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/ceph-osd-smartctl all commands require authentication	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-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: 174
- number of failures: 0

Tests hypervisorsecurity for virtu-ci3

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

Test ID	Tests	Results
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
SEAPATH-00012	admin user exists	PASS
SEAPATH-00013	admin has a password	PASS

- number of tests: 17
- number of failures: 0

Tests hypervisoriommu for virtu-ci3

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 *iommu* : INTEL_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : AMD_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : AMD_IOMMU_V2 is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : IOMMU_IOVA is enabled	PASS

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

Tests cluster for virtu-ci3

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

Test ID	Tests	Results
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-attrd 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-attrd 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-attrd 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-attrd 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-attrd 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

Test ID	Tests	Results
SEAPATH-00137	pacemaker-attrd 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-attrd system calls are filtered	PASS
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	PASS

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

Tests hypervisor for virtu-ci3

Test ID	Tests	Results
SEAPATH-00027	auditd is inactive	PASS
SEAPATH-00044	Check /etc/syslog-ng/cert.d/clientcert.pem permissions	FAIL
SEAPATH-00045	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	PASS
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_GRE is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_VXLAN is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_GENEVE is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : TRIM_UNUSED_KSYMS is disabled	PASS
SEAPATH-00050	Linux kernel *ovs* : NET_IPGRE is enabled	FAIL
SEAPATH-00050	Linux kernel *dpdk* : UIO is enabled	FAIL
SEAPATH-00050	Linux kernel *dpdk* : VFIO_PCI is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : IGB is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : TIGON3 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : R8169 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : E1000 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : E1000E is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : X86_PKG_TEMP_THERMAL is enabled	FAIL
SEAPATH-00050	Linux kernel *ceph* : AIO is enabled	PASS
SEAPATH-00050	Linux kernel *ceph* : TMPFS is enabled	PASS
SEAPATH-00050	Linux kernel *ceph* : MD is enabled	PASS
SEAPATH-00050	Linux kernel *kvm* : KVM is enabled	FAIL
SEAPATH-00050	Linux kernel *kvm* : KVM_INTEL is enabled	FAIL
SEAPATH-00050	Linux kernel *kvm* : KVM_VFIO is enabled	PASS
SEAPATH-00007	SMT is activated	PASS

Test ID	Tests	Results
SEAPATH-00003	libvirtd service is running	PASS
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
SEAPATH-00023	SPICE protocol is not installed	FAIL
SEAPATH-00006	Audit subsystem is disabled on cmdline	FAIL
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-00023	SPICE protocol is not installed	FAIL
SEAPATH-00030	iommu enabled in passthrough mode	PASS
SEAPATH-00031	iommu is loaded	PASS
SEAPATH-00032	iommu is populated	PASS
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* : AMD_IOMMU_V2 is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : IOMMU_IOVA is enabled	PASS

- number of tests: 53
- number of failures: 27

Tests hypervisorreadonly for virtu-ci3

Test ID	Tests	Results
SEAPATH-00140	rootfs is readonly mounted	PASS
SEAPATH-00141	/etc is mounted as overlayfs	FAIL
SEAPATH-00141	/home is mounted as overlayfs	FAIL
SEAPATH-00141	/usr/lib/python3.8/site-packages/*pycache* is mounted as overlayfs	FAIL
SEAPATH-00141	/var/cache is mounted as overlayfs	FAIL

Test ID	Tests	Results
SEAPATH-00141	/var/lib is mounted as overlayfs	FAIL
SEAPATH-00141	/var/spool is mounted as overlayfs	FAIL
SEAPATH-00142	Kernel OVERLAY_FS is set	FAIL
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-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
SEAPATH-00012	admin user exists	PASS
SEAPATH-00013	admin has a password	PASS

- number of tests: 25
- number of failures: 7

Tests cluster for cluster

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	2 osds are configured and up	FAIL
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
SEAPATH-00064	3 nodes are configured	PASS
SEAPATH-00065	list secrets	PASS
SEAPATH-00066	define VM from a valid configuration	PASS
	Running "test 1 -ne 0" returns success	PASS
SEAPATH-00068	list VM	PASS

Test ID	Tests	Results
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-00056	Test clone disk	PASS
SEAPATH-00057	Test groups	PASS
SEAPATH-00058	Test namespaces	PASS
SEAPATH-00059	Test metadata	PASS
SEAPATH-00060	Test snapshots	FAIL
SEAPATH-00061	Test snapshots rollback	FAIL
SEAPATH-00062	Test write rbd	FAIL
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-attrd 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-attrd 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

Test ID	Tests	Results
SEAPATH-00137	pacemaker-attrd 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-attrd 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-attrd 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-attrd 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-attrd system calls are filtered	PASS
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	PASS

- number of tests: 82
- number of failures: 4

Tests common for virtu-ci2

Test ID	Tests	Results
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

Test ID	Tests	Results
SEAPATH-00050	Linux kernel *hardening* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : LEGACY_VSYSCALL_NONE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : STATIC_USERMODEHELPER is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USERFAULTFD is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : X86_VSYSCALL_EMULATION is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : MODIFY_LDT_SYSCALL is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : DEVMEM is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USELIB is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KEXEC is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : BINFMT_MISC is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : ALLOW_DEV_COREDUMP is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : PROC_KCORE is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KALLSYMS is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : SLUB_DEBUG_ON is enabled	FAIL
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* : SLUB_DEBUG_ON is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : HARDENED_USERCOPY is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : HARDENED_USERCOPY_FALLBACK is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : FORTIFY_SOURCE is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : PAGE_POISONING is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RANDOMIZE_KSTACK_OFFSET_DEFAULT is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : INIT_ON_ALLOC_DEFAULT_ON is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : INIT_ON_FREE_DEFAULT_ON is enabled	FAIL
SEAPATH-00050	Linux kernel *misc* : EFI_PARTITION is enabled	PASS
SEAPATH-00050	Linux kernel *reporting* : EDAC is enabled	PASS
SEAPATH-00050	Linux kernel *usb* : USB_OHCI_HCD is enabled	FAIL
SEAPATH-00050	Linux kernel *usb* : USB_EHCI_HCD is enabled	FAIL
SEAPATH-00050	Linux kernel *usb* : USB_XHCI_HCD is enabled	FAIL
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: 42

- number of failures: 19

Tests future_common_security for virtu-ci2

Test ID	Tests	Results
SEAPATH-00050	Linux kernel *hardening* : STATIC_USERMODEHELPER is enabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USERFAULTFD is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : X86_VSYSCALL_EMULATION is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : MODIFY_LDT_SYSCALL is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : DEVMEM is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : USELIB is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : PROC_KCORE is disabled	FAIL
SEAPATH-00050	Linux kernel *hardening* : KALLSYMS is disabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_LATENT_ENTROPY is enabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_RANDSTRUCT is enabled	FAIL
SEAPATH-00050	Linux kernel *gcc_plugins* : GCC_PLUGIN_STRUCTLEAK_BYREF_ALL is enabled	FAIL
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-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-00149	/etc/sudoers include passwd_timeout=1 directive	FAIL
SEAPATH-00151	/etc/sudoers no rule target root user	FAIL

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

Tests common_security for virtu-ci2

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	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00176	All files have a known owner and group	PASS

Test ID	Tests	Results
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 cryto 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 *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* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE 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-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-00148	/etc/sudoers include env_reset directive	PASS
SEAPATH-00150	/etc/sudoers all commands require authentication	PASS
SEAPATH-00152	/etc/sudoers EXEC option is not used	PASS

Test ID	Tests	Results
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/Debian-snmp all commands require authentication	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/ansible all commands require authentication	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-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-00150	/etc/sudoers.d/ceph-osd-smartctl all commands require authentication	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/virtu all commands require authentication	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
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-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

Test ID	Tests	Results
SEAPATH-00086	syslog-ng capabilities are bounded	PASS
SEAPATH-00087	syslog-ng system calls are filtered	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	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00176	All files have a known owner and group	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 cryto 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 *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* : PAGE_TABLE_ISOLATION is enabled	PASS
SEAPATH-00050	Linux kernel *hardening* : RETPOLINE 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-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

Test ID	Tests	Results
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-00148	/etc/sudoers include env_reset directive	PASS
SEAPATH-00150	/etc/sudoers all commands require authentication	PASS
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/Debian-snmp all commands require authentication	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/ansible all commands require authentication	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-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-00150	/etc/sudoers.d/ceph-osd-smartctl all commands require authentication	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/virtu all commands require authentication	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-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: 174
- number of failures: 0

Tests hypervisorsecurity for virtu-ci2

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-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
SEAPATH-00012	admin user exists	PASS
SEAPATH-00013	admin has a password	PASS

- number of tests: 17
- number of failures: 0

Tests hypervisoriommu for virtu-ci2

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 *iommu* : INTEL_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : AMD_IOMMU is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : AMD_IOMMU_V2 is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : IOMMU_IOVA is enabled	PASS

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

Tests cluster for virtu-ci2

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
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-attrd 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-attrd 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

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

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

Tests hypervisor for virtu-ci2

Test ID	Tests	Results
SEAPATH-00027	auditd is inactive	PASS
SEAPATH-00044	Check /etc/syslog-ng/cert.d/clientcert.pem permissions	FAIL
SEAPATH-00045	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	PASS
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_GRE is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_VXLAN is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : OPENVSWITCH_GENEVE is enabled	FAIL
SEAPATH-00050	Linux kernel *ovs* : TRIM_UNUSED_KSYMS is disabled	PASS
SEAPATH-00050	Linux kernel *ovs* : NET_IPGRE is enabled	FAIL
SEAPATH-00050	Linux kernel *dpdk* : UIO is enabled	FAIL
SEAPATH-00050	Linux kernel *dpdk* : VFIO_PCI is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : IGB is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : TIGON3 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : R8169 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : E1000 is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : E1000E is enabled	FAIL
SEAPATH-00050	Linux kernel *hardware* : X86_PKG_TEMP_THERMAL is enabled	FAIL
SEAPATH-00050	Linux kernel *ceph* : AIO is enabled	PASS
SEAPATH-00050	Linux kernel *ceph* : TMPFS is enabled	PASS
SEAPATH-00050	Linux kernel *ceph* : MD is enabled	PASS
SEAPATH-00050	Linux kernel *kvm* : KVM is enabled	FAIL
SEAPATH-00050	Linux kernel *kvm* : KVM_INTEL is enabled	FAIL
SEAPATH-00050	Linux kernel *kvm* : KVM_VFIO is enabled	PASS
SEAPATH-00007	SMT is activated	PASS
SEAPATH-00003	libvirtd service is running	PASS
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
SEAPATH-00023	SPICE protocol is not installed	FAIL
SEAPATH-00006	Audit subsystem is disabled on cmdline	FAIL
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

Test ID	Tests	Results
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-00023	SPICE protocol is not installed	FAIL
SEAPATH-00030	iommu enabled in passthrough mode	PASS
SEAPATH-00031	iommu is loaded	PASS
SEAPATH-00032	iommu is populated	PASS
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* : AMD_IOMMU_V2 is enabled	PASS
SEAPATH-00050	Linux kernel *iommu* : IOMMU_IOVA is enabled	PASS

- number of tests: 53
- number of failures: 27

Tests hypervisorreadonly for virtu-ci2

Test ID	Tests	Results
SEAPATH-00140	rootfs is readonly mounted	PASS
SEAPATH-00141	/etc is mounted as overlayfs	FAIL
SEAPATH-00141	/home is mounted as overlayfs	FAIL
SEAPATH-00141	/usr/lib/python3.8/site-packages/*pycache* is mounted as overlayfs	FAIL
SEAPATH-00141	/var/cache is mounted as overlayfs	FAIL
SEAPATH-00141	/var/lib is mounted as overlayfs	FAIL
SEAPATH-00141	/var/spool is mounted as overlayfs	FAIL
SEAPATH-00142	Kernel OVERLAY_FS is set	FAIL
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-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

Test ID	Tests	Results
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

- number of tests: 25
- number of failures: 7

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
```