



TEST REPORT

Table of Contents

Prerequisites	1
Test reports.....	2
Tests common for virtu-ci1	2
Tests common_security for virtu-ci1	2
Tests hypervisorsecurity for virtu-ci1.....	5
Tests hypervisoriommu for virtu-ci1.....	6
Tests cluster for virtu-ci1	6
Tests hypervisor for virtu-ci1	8
Tests common for virtu-ci3	9
Tests common_security for virtu-ci3.....	9
Tests hypervisorsecurity for virtu-ci3.....	13
Tests hypervisoriommu for virtu-ci3	13
Tests cluster for virtu-ci3	14
Tests hypervisor for virtu-ci3	15
Tests common for virtu-ci2	16
Tests common_security for virtu-ci2	17
Tests hypervisorsecurity for virtu-ci2.....	20
Tests hypervisoriommu for virtu-ci2	20
Tests cluster for virtu-ci2	21
Tests hypervisor for virtu-ci2	22
Notes	24
About this documentation	25

Prerequisites

Test reports

Tests common for virtu-ci1

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

- number of tests: 9
- number of failures: 1

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-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	FAIL
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	FAIL
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	FAIL
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	FAIL
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	FAIL
SEAPATH-00099	su is denied	FAIL
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in login policy	FAIL
SEAPATH-00050	Linux kernel <i>hardening</i> : SECURITY_YAMA is enabled	PASS

Test ID	Tests	Results
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> : 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
SEAPATH-00050	Linux kernel <i>hardening</i> : 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)	FAIL
SEAPATH-00164	sudo requires password for group operator (operator)	PASS
SEAPATH-00165	sudo requires password for group maintenance-N1 (maint-n1)	PASS
SEAPATH-00166	sudo requires password for group maintenance-N3 (maint-n3)	PASS
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsyz)	PASS
SEAPATH-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	FAIL
SEAPATH-00105	/usr/bin/sudo has permissions 4750	FAIL
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/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	FAIL
SEAPATH-00172	Check kexec is disabled	FAIL
SEAPATH-00173	Check binfmt_misc is disabled	FAIL
SEAPATH-00082	/var/log is mounted on a separate partition	PASS

Test ID	Tests	Results
SEAPATH-00085	syslog-ng can not acquire new privileges	FAIL
SEAPATH-00086	syslog-ng capabilities are bounded	FAIL
SEAPATH-00087	syslog-ng system calls are filtered	FAIL
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-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	FAIL
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	FAIL
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	FAIL
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	FAIL
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	FAIL
SEAPATH-00099	su is denied	FAIL
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in <i>login</i> policy	FAIL
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> : 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
SEAPATH-00050	Linux kernel <i>hardening</i> : 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)	FAIL
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

Test ID	Tests	Results
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsyst)	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	FAIL
SEAPATH-00105	/usr/bin/sudo has permissions 4750	FAIL
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/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	FAIL
SEAPATH-00172	Check kexec is disabled	FAIL
SEAPATH-00173	Check binfmt_misc is disabled	FAIL
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	FAIL
SEAPATH-00086	syslog-ng capabilities are bounded	FAIL

- number of tests: 126
- number of failures: 34

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-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	FAIL
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	FAIL
SEAPATH-00013	admin has a password	FAIL

- number of tests: 17
- number of failures: 5

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	FAIL
SEAPATH-00130	ceph-mon system calls are filtered	FAIL
SEAPATH-00131	ceph-mgr system calls are filtered	FAIL
SEAPATH-00132	ceph-osd system calls are filtered	FAIL
SEAPATH-00120	corosync can not acquire new privileges	FAIL
SEAPATH-00121	corosync capabilities are bounded	FAIL
SEAPATH-00128	corosync system calls are filtered	FAIL
SEAPATH-00123	pacemaker can not acquire new privileges	FAIL

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

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

Tests hypervisor for virtu-ci1

Test ID	Tests	Results
SEAPATH-00044	Check /etc/syslog-ng/cert.d/clientcert.pem permissions	FAIL
SEAPATH-00045	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	FAIL
SEAPATH-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-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
SEAPATH-00050	Linux kernel <i>iommu</i> : DMAR_TABLE is enabled	PASS
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-00008	Slab merging is disabled on cmdline	PASS
SEAPATH-00009	Kernel Page Table Isolation is always enabled on cmdline	PASS

Test ID	Tests	Results
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	FAIL
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	FAIL
SEAPATH-00013	admin has a password	FAIL

- number of tests: 35
- number of failures: 7

Tests common for virtu-ci3

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

- number of tests: 9
- number of failures: 1

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	FAIL
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	FAIL
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	FAIL
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	FAIL
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	FAIL
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	FAIL
SEAPATH-00099	su is denied	FAIL
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in login policy	FAIL
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> : 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
SEAPATH-00050	Linux kernel <i>hardening</i> : 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)	FAIL
SEAPATH-00164	sudo requires password for group operator (operator)	PASS
SEAPATH-00165	sudo requires password for group maintenance-N1 (maint-n1)	PASS
SEAPATH-00166	sudo requires password for group maintenance-N3 (maint-n3)	PASS
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsyz)	PASS
SEAPATH-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	FAIL
SEAPATH-00105	/usr/bin/sudo has permissions 4750	FAIL
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/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	FAIL
SEAPATH-00172	Check kexec is disabled	FAIL
SEAPATH-00173	Check binfmt_misc is disabled	FAIL
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	FAIL
SEAPATH-00086	syslog-ng capabilities are bounded	FAIL
SEAPATH-00087	syslog-ng system calls are filtered	FAIL
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-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	FAIL
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	FAIL
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	FAIL
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	FAIL
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	FAIL
SEAPATH-00099	su is denied	FAIL
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in login policy	FAIL
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

Test ID	Tests	Results
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> : 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
SEAPATH-00050	Linux kernel <i>hardening</i> : 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)	FAIL
SEAPATH-00164	sudo requires password for group operator (operator)	PASS
SEAPATH-00165	sudo requires password for group maintenance-N1 (maint-n1)	PASS
SEAPATH-00166	sudo requires password for group maintenance-N3 (maint-n3)	PASS
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsyz)	PASS
SEAPATH-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	FAIL
SEAPATH-00105	/usr/bin/sudo has permissions 4750	FAIL
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/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	FAIL
SEAPATH-00172	Check kexec is disabled	FAIL
SEAPATH-00173	Check binfmt_misc is disabled	FAIL
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	FAIL
SEAPATH-00086	syslog-ng capabilities are bounded	FAIL

- number of tests: 126
- number of failures: 34

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	FAIL
SEAPATH-00034	/etc/gshadow does not include extra group	FAIL
SEAPATH-00008	Slab merging is disabled on cmdline	PASS
SEAPATH-00009	Kernel Page Table Isolation is always enabled on cmdline	PASS
SEAPATH-00010	SLUB redzoning and sanity checking enabled on cmdline	PASS
SEAPATH-00047	/etc/passwd is consistent	PASS
SEAPATH-00048	/etc/passwd does not include extra user	FAIL
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	FAIL
SEAPATH-00013	admin has a password	FAIL

- number of tests: 17
- number of failures: 5

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 <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-ci3

Test ID	Tests	Results
SEAPATH-00129	ceph-crash system calls are filtered	FAIL
SEAPATH-00130	ceph-mon system calls are filtered	FAIL
SEAPATH-00131	ceph-mgr system calls are filtered	FAIL
SEAPATH-00132	ceph-osd system calls are filtered	FAIL
SEAPATH-00120	corosync can not acquire new privileges	FAIL
SEAPATH-00121	corosync capabilities are bounded	FAIL
SEAPATH-00128	corosync system calls are filtered	FAIL
SEAPATH-00123	pacemaker can not acquire new privileges	FAIL
SEAPATH-00124	pacemaker capabilities are bounded	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL
SEAPATH-00134	pacemaker-based system calls are filtered	FAIL
SEAPATH-00135	pacemaker-fenced system calls are filtered	FAIL
SEAPATH-00136	pacemaker-execd system calls are filtered	FAIL
SEAPATH-00137	pacemaker-atrtd system calls are filtered	FAIL
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	FAIL
SEAPATH-00139	pacemaker-controld system calls are filtered	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL
SEAPATH-00134	pacemaker-based system calls are filtered	FAIL
SEAPATH-00135	pacemaker-fenced system calls are filtered	FAIL
SEAPATH-00136	pacemaker-execd system calls are filtered	FAIL
SEAPATH-00137	pacemaker-atrtd system calls are filtered	FAIL
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	FAIL
SEAPATH-00139	pacemaker-controld system calls are filtered	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL
SEAPATH-00134	pacemaker-based system calls are filtered	FAIL
SEAPATH-00135	pacemaker-fenced system calls are filtered	FAIL
SEAPATH-00136	pacemaker-execd system calls are filtered	FAIL
SEAPATH-00137	pacemaker-atrtd system calls are filtered	FAIL
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	FAIL
SEAPATH-00139	pacemaker-controld system calls are filtered	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL
SEAPATH-00134	pacemaker-based system calls are filtered	FAIL
SEAPATH-00135	pacemaker-fenced system calls are filtered	FAIL
SEAPATH-00136	pacemaker-execd system calls are filtered	FAIL
SEAPATH-00137	pacemaker-atrtd system calls are filtered	FAIL
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	FAIL
SEAPATH-00139	pacemaker-controld system calls are filtered	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL

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

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

Tests hypervisor for virtu-ci3

Test ID	Tests	Results
SEAPATH-00044	Check /etc/syslog-ng/cert.d/clientcert.pem permissions	FAIL
SEAPATH-00045	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	FAIL
SEAPATH-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-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

Test ID	Tests	Results
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
SEAPATH-00050	Linux kernel <i>iommu</i> : DMAR_TABLE is enabled	PASS
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-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	FAIL
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	FAIL
SEAPATH-00013	admin has a password	FAIL

- number of tests: 35
- number of failures: 7

Tests common for virtu-ci2

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

- number of tests: 9
- number of failures: 1

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	FAIL
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	FAIL
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	FAIL
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	FAIL
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	FAIL
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	FAIL
SEAPATH-00099	su is denied	FAIL
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in login policy	FAIL
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> : 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
SEAPATH-00050	Linux kernel <i>hardening</i> : 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)	FAIL
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 (adminsyzs)	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	FAIL
SEAPATH-00105	/usr/bin/sudo has permissions 4750	FAIL
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/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	FAIL
SEAPATH-00172	Check kexec is disabled	FAIL
SEAPATH-00173	Check binfmt_misc is disabled	FAIL
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	FAIL
SEAPATH-00086	syslog-ng capabilities are bounded	FAIL
SEAPATH-00087	syslog-ng system calls are filtered	FAIL
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-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	FAIL
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	FAIL
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	FAIL
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	FAIL
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS

Test ID	Tests	Results
SEAPATH-00098	password set to expire after 90 days	FAIL
SEAPATH-00099	su is denied	FAIL
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in <i>login</i> policy	FAIL
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> : 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
SEAPATH-00050	Linux kernel <i>hardening</i> : 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)	FAIL
SEAPATH-00164	sudo requires password for group operator (operator)	PASS
SEAPATH-00165	sudo requires password for group maintenance-N1 (maint-n1)	PASS
SEAPATH-00166	sudo requires password for group maintenance-N3 (maint-n3)	PASS
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsyz)	PASS
SEAPATH-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	FAIL
SEAPATH-00105	/usr/bin/sudo has permissions 4750	FAIL
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/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

Test ID	Tests	Results
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	FAIL
SEAPATH-00172	Check kexec is disabled	FAIL
SEAPATH-00173	Check binfmt_misc is disabled	FAIL
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	FAIL
SEAPATH-00086	syslog-ng capabilities are bounded	FAIL

- number of tests: 126
- number of failures: 34

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	FAIL
SEAPATH-00034	/etc/gshadow does not include extra group	FAIL
SEAPATH-00008	Slab merging is disabled on cmdline	PASS
SEAPATH-00009	Kernel Page Table Isolation is always enabled on cmdline	PASS
SEAPATH-00010	SLUB redzoning and sanity checking enabled on cmdline	PASS
SEAPATH-00047	/etc/passwd is consistent	PASS
SEAPATH-00048	/etc/passwd does not include extra user	FAIL
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	FAIL
SEAPATH-00013	admin has a password	FAIL

- number of tests: 17
- number of failures: 5

Tests hypervisoriommu for virtu-ci2

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

Test ID	Tests	Results
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-ci2

Test ID	Tests	Results
SEAPATH-00129	ceph-crash system calls are filtered	FAIL
SEAPATH-00130	ceph-mon system calls are filtered	FAIL
SEAPATH-00131	ceph-mgr system calls are filtered	FAIL
SEAPATH-00132	ceph-osd system calls are filtered	FAIL
SEAPATH-00120	corosync can not acquire new privileges	FAIL
SEAPATH-00121	corosync capabilities are bounded	FAIL
SEAPATH-00128	corosync system calls are filtered	FAIL
SEAPATH-00123	pacemaker can not acquire new privileges	FAIL
SEAPATH-00124	pacemaker capabilities are bounded	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL
SEAPATH-00134	pacemaker-based system calls are filtered	FAIL
SEAPATH-00135	pacemaker-fenced system calls are filtered	FAIL
SEAPATH-00136	pacemaker-execd system calls are filtered	FAIL
SEAPATH-00137	pacemaker-attd system calls are filtered	FAIL
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	FAIL
SEAPATH-00139	pacemaker-controld system calls are filtered	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL
SEAPATH-00134	pacemaker-based system calls are filtered	FAIL
SEAPATH-00135	pacemaker-fenced system calls are filtered	FAIL
SEAPATH-00136	pacemaker-execd system calls are filtered	FAIL
SEAPATH-00137	pacemaker-attd system calls are filtered	FAIL
SEAPATH-00138	pacemaker-schedulerd system calls are filtered	FAIL
SEAPATH-00139	pacemaker-controld system calls are filtered	FAIL
SEAPATH-00133	pacemakerd system calls are filtered	FAIL
SEAPATH-00134	pacemaker-based system calls are filtered	FAIL
SEAPATH-00135	pacemaker-fenced system calls are filtered	FAIL
SEAPATH-00136	pacemaker-execd system calls are filtered	FAIL

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

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

Tests hypervisor for virtu-ci2

Test ID	Tests	Results
SEAPATH-00044	Check /etc/syslog-ng/cert.d/clientcert.pem permissions	FAIL
SEAPATH-00045	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	FAIL
SEAPATH-00003	libvirtd service is running	PASS

Test ID	Tests	Results
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-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
SEAPATH-00050	Linux kernel <i>iommu</i> : DMAR_TABLE is enabled	PASS
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-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	FAIL
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	FAIL
SEAPATH-00013	admin has a password	FAIL

- number of tests: 35
- 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
```