



# TEST REPORT SEAPATH YOCTO

Receiver: SEAPATH

Contact: <[seapath@savoirfairelinux.com](mailto:seapath@savoirfairelinux.com)>

16 December 2024, 09:33:40 CET

Copyright © 2024 Savoir-faire Linux

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

# Table of Contents

|   |    |
|---|----|
| 1. List of supported equipment .....                                | 1  |
| 2. Introduction .....   | 2  |
| 3. Testing Setup .....  | 3  |
| 3.1. Setup Information .....  | 3  |
| 3.2. System Capabilities .....                                      | 3  |
| 3.3. Hardening & ANSSI-BP28 Compliance .....                        | 3  |
| 3.4. Virtual Machine Deployment .....                               | 4  |
| 3.5. IEC61850 Sampled Value Latency Testing .....                   | 4  |
| 4. SFL .....  | 5  |
| 4.1. SEAPATH CI .....   | 5  |
| 4.1.1. Setup Information .....                                      | 5  |
| 4.1.2. System Capabilities and Hardening .....                      | 10 |
| Tests common security for yoctoCI .....                             | 10 |
| Tests hypervisor functionality for yoctoCI .....                    | 17 |
| Tests hypervisor security for yoctoCI .....                         | 18 |
| Tests update for yoctoCI .....                                      | 19 |
| 4.1.3. ANSSI-BP28 Compliance .....                                  | 20 |
| Matrix include/ANSSI-BP28-M-Recommendations.csv for yoctoCI .....   | 20 |
| Matrix include/ANSSI-BP28-MI-Recommendations.csv for yoctoCI .....  | 20 |
| Matrix include/ANSSI-BP28-MIE-Recommendations.csv for yoctoCI ..... | 22 |
| 4.1.4. Virtual Machine Deployment .....                             | 24 |
| Tests common security for guest0 .....                              | 24 |
| Tests common security for guest1 .....                              | 30 |
| 4.1.5. Real-time testing (Cyclictest) .....                         | 37 |
| Hypervisor .....  | 37 |
| Virtual Machines .....  | 38 |
| 4.1.6. IEC61850 Sampled Value Latency Testing .....                 | 39 |
| VM guest0 .....   | 39 |
| 5. About this documentation .....                                   | 40 |

# Chapter 1. List of supported equipment

- SFL
  - [SEAPATH CI](#)

# Chapter 2. Introduction

The purpose of this document is to certify the correct operation of the open source real-time operating system for virtualizing IEDs: SEAPATH, a project under the governance of the Linux Foundation Energy.

A series of tests has been carried out on a range of equipment from several vendors, in order to certify SEAPATH on them. Certified in virtualization functions, security, real-time functionality and network latency of IEC61850 Sampled Values.

# Chapter 3. Testing Setup

## 3.1. Setup Information

- Retrieve system information:
  - Kernel version and configuration
  - Boot options
  - CPU information
  - Memory information
  - Network interfaces

## 3.2. System Capabilities

- Virtualization:
  - Check processor support for hardware virtualization technologies (Intel VT-x or AMD-V)
  - Ensure hardware virtualization is enabled in UEFI settings
  - Verify KVM kernel module is enabled
- Network:
  - Ensure network drivers are operational
  - Verify SEAPATH's network infrastructure tools, such as OpenVSwitch, are operational
- Real-time:
  - Employ Cyclictest to measure real-time system latency:
    - Run on isolated CPUs
    - Determine worst-case latencies
- Clustering:
  - If the machine is part of a cluster
- Update:
  - Ensure that the system is upgradable using SWUpdate

## 3.3. Hardening & ANSSI-BP28 Compliance

- Launch SEAPATH cybersecurity tests
- Verify compliance with ANSSI-BP28 requirements
- Complete lists of requirements on SEAPATH [on the wiki](#).

## 3.4. Virtual Machine Deployment

- Deploy and test two VMs:
  - One real-time and isolated
  - One non-real-time and non-isolated
- Use VMs for:
  - Real-time (cyclic test)
  - SV IEC61850 packet network latency tests

## 3.5. IEC61850 Sampled Value Latency Testing

- Perform SV IEC61850 packet network latency tests
- Compute latency between publisher and VM userspace.



# Chapter 4. SFL

## 4.1. SEAPATH CI

### 4.1.1. Setup Information

- **kernel version:** Linux-6.1.112-rt43-mainline-rt-x86\_64-with-glibc2.39 #1 SMP PREEMPT\_RT Mon Oct 14 00:55:35 UTC 2024
- **boot options:** BOOT\_IMAGE=/bzImage root=PARTUUID=f0e7a87d-3891-4f89-80aa-dcf009f71d2d efiruntime rootwait console=ttyS0,115200 console=tty0 audit=0 slab\_nomerge slub\_debug=ZF rootfstype=ext4 page\_poison=on spec\_store\_bypass\_disable=auto mds=full,nosmt mce=0 page\_alloc.shuffle=1 rng\_core.default\_quality=500 init=/sbin/init.sh default\_hugepagesz=1G hugepagesz=1G skew\_tick=1 rcutree.kthread\_prio=10 kvm.halt\_poll\_ns=0 isolcpus=4-N nohz\_full=4-N rcu\_nocbs=4-N
- **CPU architecture:** x86\_64
- **Number of physical CPUs:** 8
- **RAM:** 65588860 kB
- **Network interfaces:**
  - **Interface Name:** lo
  - **Capabilities:**
    - *Speed:* Unknown
    - *Duplex:* Unknown
    - *Auto-negotiation:* Unknown
    - *Hardware PTP:* Not supported
  - **Interface Name:** enp5s0
  - **Capabilities:**
    - *Speed:* Unknown!
    - *Duplex:* Unknown! (255)
    - *Auto-negotiation:* on
    - *Hardware PTP:* Supported
  - **Interface Name:** enp6s0
  - **Capabilities:**
    - *Speed:* Unknown!
    - *Duplex:* Unknown! (255)
    - *Auto-negotiation:* on
    - *Hardware PTP:* Supported
  - **Interface Name:** enp7s0

- **Capabilities:**
  - *Speed*: Unknown!
  - *Duplex*: Unknown! (255)
  - *Auto-negotiation*: on
  - *Hardware PTP*: Supported

◦ **Interface Name:** enp8s0

- **Capabilities:**
  - *Speed*: Unknown!
  - *Duplex*: Unknown! (255)
  - *Auto-negotiation*: on
  - *Hardware PTP*: Supported

◦ **Interface Name:** enp1s0

- **Capabilities:**
  - *Speed*: 100Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: on
  - *Hardware PTP*: Supported

◦ **Interface Name:** enp2s0

- **Capabilities:**
  - *Speed*: 1000Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: on
  - *Hardware PTP*: Supported

◦ **Interface Name:** enp3s0

- **Capabilities:**
  - *Speed*: 1000Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: on
  - *Hardware PTP*: Supported

◦ **Interface Name:** enp4s0

- **Capabilities:**
  - *Speed*: Unknown!
  - *Duplex*: Unknown! (255)
  - *Auto-negotiation*: on
  - *Hardware PTP*: Supported



- **Interface Name:** gre0
- **Capabilities:**
  - *Speed:* Unknown
  - *Duplex:* Unknown
  - *Auto-negotiation:* Unknown
  - *Hardware PTP:* Not supported
- **Interface Name:** gretap0
- **Capabilities:**
  - *Speed:* Unknown
  - *Duplex:* Unknown
  - *Auto-negotiation:* Unknown
  - *Hardware PTP:* Not supported
- **Interface Name:** erspan0
- **Capabilities:**
  - *Speed:* Unknown
  - *Duplex:* Unknown
  - *Auto-negotiation:* Unknown
  - *Hardware PTP:* Not supported
- **Interface Name:** sit0
- **Capabilities:**
  - *Speed:* Unknown
  - *Duplex:* Unknown
  - *Auto-negotiation:* Unknown
  - *Hardware PTP:* Not supported
- **Interface Name:** ovs-system
- **Capabilities:**
  - *Speed:* Unknown
  - *Duplex:* Unknown
  - *Auto-negotiation:* Unknown
  - *Hardware PTP:* Not supported
- **Interface Name:** obr0
- **Capabilities:**
  - *Speed:* Unknown
  - *Duplex:* Unknown
  - *Auto-negotiation:* Unknown

- *Hardware PTP*: Not supported
- **Interface Name:** obr0P0
- **Capabilities:**
  - *Speed*: 10Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: off
  - *Hardware PTP*: Not supported
- **Interface Name:** obr0P1
- **Capabilities:**
  - *Speed*: 10Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: off
  - *Hardware PTP*: Not supported
- **Interface Name:** obr0P2
- **Capabilities:**
  - *Speed*: 10Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: off
  - *Hardware PTP*: Not supported
- **Interface Name:** obr0P3
- **Capabilities:**
  - *Speed*: 10Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: off
  - *Hardware PTP*: Not supported
- **Interface Name:** obr0P4
- **Capabilities:**
  - *Speed*: 10Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: off
  - *Hardware PTP*: Not supported
- **Interface Name:** br0
- **Capabilities:**
  - *Speed*: 100Mb/s
  - *Duplex*: Unknown! (255)

- *Auto-negotiation*: off
- *Hardware PTP*: Not supported
- **Interface Name**: enp1s0.33
- **Capabilities**:
  - *Speed*: 100Mb/s
  - *Duplex*: Full
  - *Auto-negotiation*: on
  - *Hardware PTP*: Supported
- **Interface Name**: virbr0
- **Capabilities**:
  - *Speed*: Unknown!
  - *Duplex*: Unknown! (255)
  - *Auto-negotiation*: off
  - *Hardware PTP*: Not supported

## 4.1.2. System Capabilities and Hardening

### Tests common security for yoctoCI

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00106 | Check /etc/passwd permissions                                 | PASS    |
| SEAPATH-00107 | Check /etc/shadow permissions                                 | PASS    |
| SEAPATH-00108 | Check /etc/syslog-ng/ca.d/cacert.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-00193 | All directories writable by all users have the sticky bit     | PASS    |
| SEAPATH-00194 | All directories writable by all users are owned by root       | PASS    |
| SEAPATH-00195 | Ceph OSD are owned by ceph                                    | PASS    |
| SEAPATH-00011 | Only polyinstantiated dirs in /tmp                            | PASS    |
| SEAPATH-00196 | No unexpected file has setuid/setgid enabled                  | PASS    |
| SEAPATH-00200 | Check for files with no user or 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 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     | 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-00157 | PATH env. variable is correctly set                           | 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' : STATIC_USERMODEHELPER is enabled   | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : USERFAULTFD is disabled            | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : X86_VSYSCALL_EMULATION is disabled | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : MODIFY_LDT_SYSCALL is disabled     | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : DEVMEM is disabled                 | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : USELIB is disabled                 | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00050 | Linux kernel 'hardening' : KEXEC is disabled                            | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : BINfmt_MISC is disabled                      | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : ALLOW_DEV_COREDUMP is disabled               | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : PROC_KCORE is disabled                       | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : KALLSYMS is disabled                         | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : SLUB_DEBUG_ON 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' : SLUB_DEBUG_ON 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-00050 | Linux kernel 'hardening' : SHUFFLE_PAGE_ALLOCATOR is enabled            | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : RANDOMIZE_KSTACK_OFFSET_DEFAULT is enabled   | PASS    |
| 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           | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : CC_HAS_AUTO_VAR_INIT_ZERO is enabled         | PASS    |
| SEAPATH-00050 | Linux kernel 'gcc_plugins' : GCC_PLUGIN_LATENT_ENTROPY is enabled       | PASS    |
| SEAPATH-00050 | Linux kernel 'gcc_plugins' : GCC_PLUGIN_RANDSTRUCT is enabled           | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : slab_nomerge is enabled                     | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : slub_debug is ZF                            | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : page_poison is on                           | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : spec_store_bypass_disable is auto           | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : mds is full,nosmt                           | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : mce is 0                                    | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : page_alloc.shuffle is 1                     | PASS    |
| SEAPATH-00008 | Linux cmdline 'hardening' : rng_core.default_quality is 500             | PASS    |
| SEAPATH-00158 | sudo policy is installed for group operator (operator)                  | PASS    |
| SEAPATH-00159 | sudo policy is installed for group maintenance-N1 (maint-n1)            | PASS    |
| SEAPATH-00160 | sudo policy is installed for group maintenance-N3 (maint-n3)            | PASS    |
| SEAPATH-00161 | sudo policy is installed for group cluster administrator (admincluster) | PASS    |
| SEAPATH-00162 | sudo policy is installed for group system administrator (adminsys)      | 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-00029 | pam namespaces configured for login                                     | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00037 | /tmp namespaces configured  | PASS    |
| SEAPATH-00036 | private /tmp configured for ssh   | PASS    |
| SEAPATH-00103 | /usr/bin/sudo exists  | PASS    |
| SEAPATH-00104 | /usr/bin/sudo belongs to group privileged   | PASS    |
| SEAPATH-00105 | /usr/bin/sudo has permissions 4750  | PASS    |
| SEAPATH-00143 | /etc/sudoers include noexec directive   | PASS    |
| SEAPATH-00144 | /etc/sudoers include requiretty directive   | PASS    |
| SEAPATH-00145 | /etc/sudoers include use_pty directive  | PASS    |
| SEAPATH-00146 | /etc/sudoers include umask=0027 directive   | PASS    |
| SEAPATH-00147 | /etc/sudoers include ignore_dot directive   | PASS    |
| SEAPATH-00148 | /etc/sudoers include env_reset directive  | PASS    |
| SEAPATH-00149 | /etc/sudoers include passwd_timeout=1 directive   | PASS    |
| SEAPATH-00150 | /etc/sudoers - all commands require authentication  | PASS    |
| SEAPATH-00151 | /etc/sudoers - no rule target root user   | 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/operator - all commands require authentication                                 | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/operator - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/operator - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/operator - rules are not defined by negation                                   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/operator - commands are not specified without arguments                        | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/operator - no command is specified with wildcard argument                      | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/operator - /etc/sudoers.d/operator is owned by root:root with 0440 permissions | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/ansible - all commands require authentication                                  | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/ansible - no rule target root user   | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/ansible - EXEC option is not used  | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/ansible - rules are not defined by negation                                    | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/ansible - commands are not specified without arguments                         | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/ansible - no command is specified with wildcard argument                       | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/ansible - /etc/sudoers.d/ansible is owned by root:root with 0440 permissions   | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/maint-n3 - all commands require authentication                                 | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/maint-n3 - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/maint-n3 - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/maint-n3 - rules are not defined by negation                                   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/maint-n3 - commands are not specified without arguments                        | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/maint-n3 - no command is specified with wildcard argument                      | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00156 | /etc/sudoers.d/maint-n3 - /etc/sudoers.d/maint-n3 is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/maint-n1 - all commands require authentication   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/maint-n1 - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/maint-n1 - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/maint-n1 - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/maint-n1 - commands are not specified without arguments                                | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/maint-n1 - no command is specified with wildcard argument                              | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/maint-n1 - /etc/sudoers.d/maint-n1 is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/admincluster - all commands require authentication                                     | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/admincluster - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/admincluster - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/admincluster - rules are not defined by negation                                       | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/admincluster - commands are not specified without arguments                            | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/admincluster - no command is specified with wildcard argument                          | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/admincluster - /etc/sudoers.d/admincluster is owned by root:root with 0440 permissions | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/cockpit - all commands require authentication  | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/cockpit - no rule target root user   | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/cockpit - EXEC option is not used  | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/cockpit - rules are not defined by negation  | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/cockpit - commands are not specified without arguments                                 | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/cockpit - no command is specified with wildcard argument                               | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/cockpit - /etc/sudoers.d/cockpit is owned by root:root with 0440 permissions           | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/emergadmin - all commands require authentication                                       | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/emergadmin - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/emergadmin - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/emergadmin - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/emergadmin - commands are not specified without arguments                              | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/emergadmin - no command is specified with wildcard argument                            | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/emergadmin - /etc/sudoers.d/emergadmin is owned by root:root with 0440 permissions     | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/snmp - all commands require authentication   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/snmp - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/snmp - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/snmp - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/snmp - commands are not specified without arguments                                    | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/snmp - no command is specified with wildcard argument                                  | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/snmp - /etc/sudoers.d/snmp is owned by root:root with 0440 permissions                 | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00150 | /etc/sudoers.d/admin - all commands require authentication  | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/admin - no rule target root user   | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/admin - EXEC option is not used  | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/admin - rules are not defined by negation  | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/admin - commands are not specified without arguments                               | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/admin - no command is specified with wildcard argument                             | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions           | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/privileged - all commands require authentication                                   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/privileged - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/privileged - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/privileged - rules are not defined by negation                                     | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/privileged - commands are not specified without arguments                          | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/privileged - no command is specified with wildcard argument                        | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/privileged - /etc/sudoers.d/privileged is owned by root:root with 0440 permissions | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/adminsys - all commands require authentication                                     | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/adminsys - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/adminsys - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/adminsys - rules are not defined by negation                                       | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/adminsys - commands are not specified without arguments                            | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/adminsys - no command is specified with wildcard argument                          | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/adminsys - /etc/sudoers.d/adminsys is owned by root:root with 0440 permissions     | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.modules_disabled is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - dev.tty.ldisc_autoload is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_fifos is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_regular is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_hardlinks is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_symlinks is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.suid_dumpable is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.dmesg_restrict is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.kptr_restrict is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_event_paranoid is set properly                                     | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.randomize_va_space is set properly                                      | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.sysrq is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.unprivileged_bpf_disabled is set properly                               | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.yama.ptrace_scope is set properly                                       | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_event_max_sample_rate is set properly                              | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_cpu_time_max_percent is set properly                               | PASS    |
| SEAPATH-00109 | sysctl-hardening - vm.mmap_min_addr is set properly   | PASS    |



| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00109 | sysctl-hardening - kernel.pid_max is set properly                           | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.panic_on_oops is set properly                     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.accept_redirects is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.accept_source_route is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.log_martians is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.rp_filter is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.secure_redirects is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.send_redirects is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.shared_media is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.accept_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.accept_source_route is set properly  | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.log_martians is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.rp_filter is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.secure_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.send_redirects is set properly       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.shared_media is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.icmp_echo_ignore_broadcasts is set properly       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.icmp_ignore_bogus_error_responses is set properly | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_invalid_ratelimit is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_max_syn_backlog is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_rfc1337 is set properly                       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_syn_retries is set properly                   | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_synack_retries is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_syncookies is set properly                    | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_timestamps is set properly                    | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.ip_local_port_range is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_challenge_ack_limit is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra_defrtr is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra_pinfo is set properly          | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_redirects is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_source_route is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.autoconf is set properly                 | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.dad_transmits is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.forwarding is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.max_addresses is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.router_solicitations is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.use_tempaddr is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra_defrtr is set properly     | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra_pinfo is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_source_route is set properly  | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.autoconf is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.dad_transmits is set properly        | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.forwarding is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.max_addresses is set properly        | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.router_solicitations is set properly | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.use_tempaddr is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.netfilter.nf_conntrack_max is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.netfilter.nf_conntrack_tcp_loose is set properly       | PASS    |
| SEAPATH-00176 | Check kptr_restrict is set to 2   | PASS    |
| SEAPATH-00177 | Check dmesg_restrict is set to 1  | PASS    |
| SEAPATH-00178 | Check pid_max is set to 4194304   | PASS    |
| SEAPATH-00179 | Check perf_cpu_time_max_percent is set to 1                                 | PASS    |
| SEAPATH-00180 | Check perf_event_max_sample_rate is set to 1                                | PASS    |
| SEAPATH-00181 | Check perf_event_paranoid is set to 3                                       | PASS    |
| SEAPATH-00182 | Check randomize_va_space is set to 2  | PASS    |
| SEAPATH-00183 | Check sysrq is set to 0   | PASS    |
| SEAPATH-00184 | Check unprivileged_bpf_disabled is set to 1                                 | PASS    |
| SEAPATH-00185 | Check panic_on_oops is set to 1   | PASS    |
| SEAPATH-00186 | Check kernel.yama.ptrace_scope is set to 2                                  | PASS    |
| SEAPATH-00187 | Check suid_dumpable is set to 0   | PASS    |
| SEAPATH-00188 | Check protected_fifos is set to 2   | PASS    |
| SEAPATH-00189 | Check protected_regular is set to 2   | PASS    |
| SEAPATH-00190 | Check protected_symlinks is set to 1  | PASS    |
| SEAPATH-00191 | Check protected_hardlinks is set to 1                                       | PASS    |
| SEAPATH-00192 | Check modules_disabled is set to 1  | PASS    |
| SEAPATH-00082 | /var/log is mounted on a separate partition                                 | PASS    |
| SEAPATH-00085 | syslog-ng can not acquire new privileges                                    | PASS    |
| SEAPATH-00086 | syslog-ng capabilities are bounded  | PASS    |
| SEAPATH-00087 | syslog-ng system calls are filtered   | PASS    |
| SEAPATH-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                                | PASS    |
| SEAPATH-00050 | Linux kernel 'usb' : USB_EHCI_HCD is enabled                                | PASS    |
| SEAPATH-00050 | Linux kernel 'usb' : USB_XHCI_HCD is enabled                                | PASS    |
| SEAPATH-00171 | no RT throttling triggered  | PASS    |
| SEAPATH-00078 | no paging error   | PASS    |
| SEAPATH-00079 | no rcu stall  | PASS    |

| Test ID       | Tests                                 | Results |
|---------------|---------------------------------------|---------|
| SEAPATH-00080 | no backtraces                         | PASS    |
| SEAPATH-00075 | kernel is PREEMPT RT                  | PASS    |
| SEAPATH-00076 | kernel is realtime                    | PASS    |
| SEAPATH-00081 | kernel is >= 4.19.106                 | PASS    |
| SEAPATH-00083 | syslog-ng service is running          | PASS    |
| SEAPATH-00084 | /var/log/syslog is used as log target | PASS    |
| SEAPATH-00102 | no systemd services have failed       | PASS    |
| SEAPATH-00170 | no systemd syntax warning             | PASS    |

- number of tests: 210
- number of failures: 0

### Tests hypervisor functionality for yoctoCI

| Test ID       | Tests  | Results |
|---------------|--|---------|
| SEAPATH-00027 | auditd is inactive                                     | PASS    |
| SEAPATH-00024 | ceph is installed                                      | PASS    |
| SEAPATH-00025 | LVM is installed                                       | PASS    |
| SEAPATH-00026 | At least 2 disks detected                              | PASS    |
| SEAPATH-00028 | Current CPU supports 'no-execute'                      | PASS    |
| SEAPATH-00028 | Current CPU supports 'Intel virtualization'            | PASS    |
| SEAPATH-00028 | Current CPU supports 'hugepages'                       | PASS    |
| SEAPATH-00028 | Current CPU supports '64bit'                           | PASS    |
| SEAPATH-00044 | Check /etc/syslog-ng/cert.d/clientcert.pem permissions | PASS    |
| SEAPATH-00045 | Check /etc/syslog-ng/cert.d/clientkey.pem permissions  | 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 '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    |
| SEAPATH-00050 | Linux kernel 'iommu' : DMAR_TABLE is enabled           | PASS    |
| SEAPATH-00050 | Linux kernel 'ovs' : OPENVSWITCH is enabled            | PASS    |
| SEAPATH-00050 | Linux kernel 'ovs' : OPENVSWITCH_GRE is enabled        | PASS    |
| SEAPATH-00050 | Linux kernel 'ovs' : OPENVSWITCH_VXLAN is enabled      | PASS    |
| SEAPATH-00050 | Linux kernel 'ovs' : OPENVSWITCH_GENEVE is enabled     | PASS    |
| SEAPATH-00050 | Linux kernel 'ovs' : TRIM_UNUSED_KSYMS is disabled     | PASS    |
| SEAPATH-00050 | Linux kernel 'ovs' : NET_IPGRE is enabled              | PASS    |
| SEAPATH-00050 | Linux kernel 'dpdk' : UIO is enabled                   | PASS    |
| SEAPATH-00050 | Linux kernel 'dpdk' : VFIO_PCI is enabled              | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00050 | Linux kernel 'hardware' : IGB is enabled                          | PASS    |
| SEAPATH-00050 | Linux kernel 'hardware' : TIGON3 is enabled                       | PASS    |
| SEAPATH-00050 | Linux kernel 'hardware' : R8169 is enabled                        | PASS    |
| SEAPATH-00050 | Linux kernel 'hardware' : E1000 is enabled                        | PASS    |
| SEAPATH-00050 | Linux kernel 'hardware' : E1000E is enabled                       | PASS    |
| SEAPATH-00050 | Linux kernel 'hardware' : X86_PKG_TEMP_THERMAL is enabled         | PASS    |
| 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                               | PASS    |
| SEAPATH-00050 | Linux kernel 'kvm' : KVM_INTEL is enabled                         | PASS    |
| SEAPATH-00050 | Linux kernel 'kvm' : KVM_VFIO is enabled                          | PASS    |
| SEAPATH-00003 | libvirtd service is running                                       | PASS    |
| SEAPATH-00035 | openvswitch service is running                                    | PASS    |
| SEAPATH-00038 | lspci 3.6.2+ is available   | PASS    |
| SEAPATH-00140 | rootfs is readonly mounted  | PASS    |
| SEAPATH-00141 | /etc is mounted as overlayfs                                      | PASS    |
| SEAPATH-00141 | /home is mounted as overlayfs                                     | PASS    |
| SEAPATH-00141 | /usr/lib/python3.12/site-packages/pycache is mounted as overlayfs | PASS    |
| SEAPATH-00141 | /var/cache is mounted as overlayfs                                | PASS    |
| SEAPATH-00141 | /var/lib is mounted as overlayfs                                  | PASS    |
| SEAPATH-00141 | /var/spool is mounted as overlayfs                                | PASS    |
| SEAPATH-00142 | Kernel OVERLAY_FS is set  | 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-00022 | IPv6 NAT is available   | PASS    |

- number of tests: 54
- number of failures: 0

### Tests hypervisor security for yoctoCI

| Test ID       | Tests  | Results |
|---------------|--|---------|
| SEAPATH-00033 | /etc/group is consistent                                       | PASS    |
| SEAPATH-00034 | /etc/group does not include extra group                        | PASS    |
| SEAPATH-00006 | Audit subsystem is disabled on cmdline                         | PASS    |
| SEAPATH-00009 | Kernel Page Table Isolation is enabled on kernel configuration | PASS    |
| SEAPATH-00004 | libvirtd can not acquire new privileges                        | PASS    |
| SEAPATH-00005 | libvirtd capabilities are bounded                              | PASS    |

| Test ID       | Tests                                       | Results |
|---------------|---|---------|
| SEAPATH-00125 | libvirtd system calls are filtered          | PASS    |
| SEAPATH-00039 | openvswitch user is created and locked      | PASS    |
| SEAPATH-00040 | openvswitch user is part of hugepages group | PASS    |
| SEAPATH-00041 | openvswitch user is part of vfio-net group  | PASS    |
| SEAPATH-00042 | ovs-vswitchd is running as user openvswitch | PASS    |
| SEAPATH-00043 | ovsdb-server is running as user openvswitch | PASS    |
| SEAPATH-00126 | ovs-vswitchd system calls are filtered      | PASS    |
| SEAPATH-00127 | ovsdb-server system calls are filtered      | PASS    |
| SEAPATH-00047 | /etc/passwd is consistent                   | PASS    |
| SEAPATH-00048 | /etc/passwd does not include extra user     | 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    |
| SEAPATH-00014 | admin is sudoers                            | PASS    |
| SEAPATH-00023 | SPICE protocol is not installed             | PASS    |

- number of tests: 25
- number of failures: 0

### Tests update for yoctoCI

| Test ID       | Tests  | Results |
|---------------|--|---------|
| SEAPATH-00007 | grub password is set                               | PASS    |
| SEAPATH-00077 | boot partition is only readable by root            | PASS    |
| SEAPATH-00115 | /dev/upgradable_bootloader exists                  | PASS    |
| SEAPATH-00116 | /dev/upgradable_rootfs exists                      | PASS    |
| SEAPATH-00117 | /dev/upgradable_bootloader points to inactive bank | PASS    |
| SEAPATH-00118 | /dev/upgradable_rootfs points to inactive bank     | PASS    |

- number of tests: 6
- number of failures: 0

### 4.1.3. ANSSI-BP28 Compliance

Matrix include/ANSSI-BP28-M-Recommendations.csv for yoctoCI

| Requirement    | Test id       | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R30 | SEAPATH-00033 | PASS   |
|                | SEAPATH-00034 | PASS   |
|                | SEAPATH-00046 | PASS   |
|                | SEAPATH-00047 | PASS   |
|                | SEAPATH-00048 | PASS   |
| ANSSI-BP28-R31 | SEAPATH-00088 | PASS   |
|                | SEAPATH-00089 | PASS   |
|                | SEAPATH-00091 | PASS   |
| ANSSI-BP28-R53 | SEAPATH-00200 | PASS   |
| ANSSI-BP28-R54 | SEAPATH-00193 | PASS   |
|                | SEAPATH-00194 | PASS   |
|                | SEAPATH-00195 | PASS   |
| ANSSI-BP28-R68 | SEAPATH-00091 | PASS   |
|                | SEAPATH-00095 | PASS   |
|                | SEAPATH-00096 | PASS   |
|                | SEAPATH-00097 | PASS   |
| ANSSI-BP28-R80 | SEAPATH-00003 | PASS   |
|                | SEAPATH-00020 | PASS   |
|                | SEAPATH-00035 | PASS   |
|                | SEAPATH-00083 | PASS   |
|                | SEAPATH-00125 | PASS   |
|                | SEAPATH-00126 | PASS   |
|                | SEAPATH-00127 | PASS   |

Matrix include/ANSSI-BP28-MI-Recommendations.csv for yoctoCI

| Requirement    | Test id       | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R1  | SEAPATH-00015 | PASS   |
|                | SEAPATH-00017 | PASS   |
|                | SEAPATH-00028 | PASS   |
|                | SEAPATH-00030 | PASS   |
|                | SEAPATH-00031 | PASS   |
|                | SEAPATH-00032 | PASS   |
|                | SEAPATH-00050 | PASS   |
| ANSSI-BP28-R11 | SEAPATH-00050 | PASS   |
|                | SEAPATH-00109 | PASS   |
|                | SEAPATH-00186 | PASS   |
| ANSSI-BP28-R12 | SEAPATH-00109 | PASS   |

| Requirement    | Test id       | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R13 | SEAPATH-00109 | PASS   |
| ANSSI-BP28-R14 | SEAPATH-00109 | PASS   |
|                | SEAPATH-00187 | PASS   |
|                | SEAPATH-00188 | PASS   |
|                | SEAPATH-00189 | PASS   |
|                | SEAPATH-00190 | PASS   |
|                | SEAPATH-00191 | PASS   |
| ANSSI-BP28-R28 | SEAPATH-00082 | PASS   |
|                | SEAPATH-00140 | PASS   |
|                | SEAPATH-00141 | PASS   |
| ANSSI-BP28-R32 | SEAPATH-00092 | PASS   |
|                | SEAPATH-00094 | PASS   |
| ANSSI-BP28-R34 | SEAPATH-00033 | PASS   |
|                | SEAPATH-00034 | PASS   |
|                | SEAPATH-00046 | PASS   |
|                | SEAPATH-00047 | PASS   |
|                | SEAPATH-00048 | PASS   |
| ANSSI-BP28-R35 | SEAPATH-00033 | PASS   |
|                | SEAPATH-00034 | PASS   |
|                | SEAPATH-00039 | PASS   |
|                | SEAPATH-00046 | PASS   |
|                | SEAPATH-00047 | PASS   |
|                | SEAPATH-00048 | PASS   |
| ANSSI-BP28-R39 | SEAPATH-00143 | PASS   |
|                | SEAPATH-00144 | PASS   |
|                | SEAPATH-00145 | PASS   |
|                | SEAPATH-00146 | PASS   |
|                | SEAPATH-00147 | PASS   |
|                | SEAPATH-00148 | PASS   |
| ANSSI-BP28-R40 | SEAPATH-00151 | PASS   |
| ANSSI-BP28-R42 | SEAPATH-00153 | PASS   |
| ANSSI-BP28-R43 | SEAPATH-00154 | PASS   |
|                | SEAPATH-00155 | PASS   |
| ANSSI-BP28-R44 | SEAPATH-00156 | PASS   |
| ANSSI-BP28-R5  | SEAPATH-00007 | PASS   |

| Requirement    | Test id       | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R50 | SEAPATH-00044 | PASS   |
|                | SEAPATH-00045 | PASS   |
|                | SEAPATH-00049 | PASS   |
|                | SEAPATH-00090 | PASS   |
|                | SEAPATH-00106 | PASS   |
|                | SEAPATH-00107 | PASS   |
|                | SEAPATH-00108 | PASS   |
|                | SEAPATH-00156 | PASS   |
| ANSSI-BP28-R52 | SEAPATH-00040 | PASS   |
|                | SEAPATH-00041 | PASS   |
| ANSSI-BP28-R55 | SEAPATH-00011 | PASS   |
|                | SEAPATH-00029 | PASS   |
|                | SEAPATH-00036 | PASS   |
|                | SEAPATH-00037 | PASS   |
| ANSSI-BP28-R79 | SEAPATH-00004 | PASS   |
|                | SEAPATH-00005 | PASS   |
|                | SEAPATH-00023 | PASS   |
|                | SEAPATH-00085 | PASS   |
|                | SEAPATH-00086 | PASS   |
| ANSSI-BP28-R8  | SEAPATH-00008 | PASS   |
|                | SEAPATH-00050 | PASS   |
| ANSSI-BP28-R9  | SEAPATH-00109 | PASS   |
|                | SEAPATH-00176 | PASS   |
|                | SEAPATH-00177 | PASS   |
|                | SEAPATH-00178 | PASS   |
|                | SEAPATH-00179 | PASS   |
|                | SEAPATH-00180 | PASS   |
|                | SEAPATH-00181 | PASS   |
|                | SEAPATH-00182 | PASS   |
|                | SEAPATH-00183 | PASS   |
|                | SEAPATH-00184 | PASS   |
|                | SEAPATH-00185 | PASS   |

Matrix include/ANSSI-BP28-MIE-Recommendations.csv for yoctoCI

| Requirement    | Test id       | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R10 | SEAPATH-00109 | PASS   |
|                | SEAPATH-00192 | PASS   |
| ANSSI-BP28-R29 | SEAPATH-00077 | PASS   |
| ANSSI-BP28-R36 | SEAPATH-00146 | PASS   |



| Requirement    | Test id       | Status |
|----------------|---------------|--------|
| ANSSI-BP28-R37 | SEAPATH-00005 | PASS   |
|                | SEAPATH-00084 | PASS   |
|                | SEAPATH-00085 | PASS   |
|                | SEAPATH-00086 | PASS   |
|                | SEAPATH-00125 | PASS   |
|                | SEAPATH-00126 | PASS   |
|                | SEAPATH-00127 | PASS   |
| ANSSI-BP28-R38 | SEAPATH-00104 | PASS   |
| ANSSI-BP28-R41 | SEAPATH-00152 | PASS   |
| ANSSI-BP28-R56 | SEAPATH-00196 | PASS   |
| ANSSI-BP28-R64 | SEAPATH-00004 | PASS   |
|                | SEAPATH-00005 | PASS   |
|                | SEAPATH-00085 | PASS   |
|                | SEAPATH-00086 | PASS   |
| ANSSI-BP28-R7  | SEAPATH-00030 | PASS   |
|                | SEAPATH-00031 | PASS   |
|                | SEAPATH-00032 | PASS   |
|                | SEAPATH-00050 | PASS   |
| ANSSI-BP28-R71 | SEAPATH-00082 | PASS   |
|                | SEAPATH-00083 | PASS   |
|                | SEAPATH-00084 | PASS   |
|                | SEAPATH-00102 | PASS   |
| ANSSI-BP28-R78 | SEAPATH-00039 | PASS   |
|                | SEAPATH-00040 | PASS   |
|                | SEAPATH-00041 | PASS   |
|                | SEAPATH-00042 | PASS   |
|                | SEAPATH-00043 | PASS   |
|                | SEAPATH-00085 | PASS   |
|                | SEAPATH-00086 | PASS   |

## 4.1.4. Virtual Machine Deployment

### Tests common security for guest0

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00106 | Check /etc/passwd permissions                                 | PASS    |
| SEAPATH-00107 | Check /etc/shadow permissions                                 | PASS    |
| SEAPATH-00108 | Check /etc/syslog-ng/ca.d/cacert.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-00193 | All directories writable by all users have the sticky bit     | PASS    |
| SEAPATH-00194 | All directories writable by all users are owned by root       | PASS    |
| SEAPATH-00195 | Ceph OSD are owned by ceph                                    | PASS    |
| SEAPATH-00088 | root password was randomized at boot                          | PASS    |
| SEAPATH-00089 | root password is randomized at each boot                      | PASS    |
| SEAPATH-00091 | root password is encrypted 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     | 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-00157 | PATH env. variable is correctly set                           | 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' : STATIC_USERMODEHELPER is enabled   | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : USERFAULTFD is disabled            | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : X86_VSYSCALL_EMULATION is disabled | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : MODIFY_LDT_SYSCALL is disabled     | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : DEVMEM is disabled                 | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : USELIB is disabled                 | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : KEXEC is disabled                  | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : BINFORMAT_MISC is disabled         | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : ALLOW_DEV_COREDUMP is disabled     | PASS    |

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

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00156 | /etc/sudoers.d/operator - /etc/sudoers.d/operator is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/admincluster - all commands require authentication                                     | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/admincluster - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/admincluster - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/admincluster - rules are not defined by negation                                       | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/admincluster - commands are not specified without arguments                            | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/admincluster - no command is specified with wildcard argument                          | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/admincluster - /etc/sudoers.d/admincluster is owned by root:root with 0440 permissions | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/adminsys - all commands require authentication   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/adminsys - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/adminsys - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/adminsys - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/adminsys - commands are not specified without arguments                                | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/adminsys - no command is specified with wildcard argument                              | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/adminsys - /etc/sudoers.d/adminsys is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/maint-n3 - all commands require authentication   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/maint-n3 - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/maint-n3 - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/maint-n3 - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/maint-n3 - commands are not specified without arguments                                | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/maint-n3 - no command is specified with wildcard argument                              | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/maint-n3 - /etc/sudoers.d/maint-n3 is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/emergadmin - all commands require authentication                                       | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/emergadmin - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/emergadmin - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/emergadmin - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/emergadmin - commands are not specified without arguments                              | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/emergadmin - no command is specified with wildcard argument                            | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/emergadmin - /etc/sudoers.d/emergadmin is owned by root:root with 0440 permissions     | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.modules_disabled is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - dev.tty.ldisc_autoload is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_fifos is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_regular is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_hardlinks is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_symlinks is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.suid_dumpable is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.dmesg_restrict is set properly  | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00109 | sysctl-hardening - kernel.kptr_restrict is set properly                     | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_event_paranoid is set properly               | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.randomize_va_space is set properly                | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.sysrq is set properly                             | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.unprivileged_bpf_disabled is set properly         | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.yama.ptrace_scope is set properly                 | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_event_max_sample_rate is set properly        | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_cpu_time_max_percent is set properly         | PASS    |
| SEAPATH-00109 | sysctl-hardening - vm.mmap_min_addr is set properly                         | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.pid_max is set properly                           | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.panic_on_oops is set properly                     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.accept_redirects is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.accept_source_route is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.log_martians is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.rp_filter is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.secure_redirects is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.send_redirects is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.shared_media is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.accept_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.accept_source_route is set properly  | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.log_martians is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.rp_filter is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.secure_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.send_redirects is set properly       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.shared_media is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.icmp_echo_ignore_broadcasts is set properly       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.icmp_ignore_bogus_error_responses is set properly | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_invalid_ratelimit is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_max_syn_backlog is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_rfc1337 is set properly                       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_syn_retries is set properly                   | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_synack_retries is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_syncookies is set properly                    | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_timestamps is set properly                    | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.ip_local_port_range is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_challenge_ack_limit is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra_defrtr is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra_pinfo is set properly          | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_redirects is set properly         | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_source_route is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.autoconf is set properly                 | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.dad_transmits is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.forwarding is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.max_addresses is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.router_solicitations is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.use_tempaddr is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra_defrtr is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra_pinfo is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_source_route is set properly  | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.autoconf is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.dad_transmits is set properly        | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.forwarding is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.max_addresses is set properly        | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.router_solicitations is set properly | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.use_tempaddr is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.netfilter.nf_conntrack_max is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.netfilter.nf_conntrack_tcp_loose is set properly       | PASS    |
| SEAPATH-00176 | Check kpтр_restrict is set to 2   | PASS    |
| SEAPATH-00177 | Check dmesg_restrict is set to 1  | PASS    |
| SEAPATH-00178 | Check pid_max is set to 4194304   | PASS    |
| SEAPATH-00179 | Check perf_cpu_time_max_percent is set to 1                                 | PASS    |
| SEAPATH-00180 | Check perf_event_max_sample_rate is set to 1                                | PASS    |
| SEAPATH-00181 | Check perf_event_paranoid is set to 3                                       | PASS    |
| SEAPATH-00182 | Check randomize_va_space is set to 2  | PASS    |
| SEAPATH-00183 | Check sysrq is set to 0   | PASS    |
| SEAPATH-00184 | Check unprivileged_bpf_disabled is set to 1                                 | PASS    |
| SEAPATH-00185 | Check panic_on_oops is set to 1   | PASS    |
| SEAPATH-00186 | Check kernel.yama.ptrace_scope is set to 2                                  | PASS    |
| SEAPATH-00187 | Check suid_dumpable is set to 0   | PASS    |
| SEAPATH-00188 | Check protected_fifos is set to 2   | PASS    |
| SEAPATH-00189 | Check protected_regular is set to 2   | PASS    |
| SEAPATH-00190 | Check protected_symlinks is set to 1  | PASS    |
| SEAPATH-00191 | Check protected_hardlinks is set to 1                                       | PASS    |
| SEAPATH-00192 | Check modules_disabled is set to 1  | PASS    |
| SEAPATH-00082 | /var/log is mounted on a separate partition                                 | PASS    |
| SEAPATH-00085 | syslog-ng can not acquire new privileges                                    | PASS    |
| SEAPATH-00086 | syslog-ng capabilities are bounded  | PASS    |



| Test ID       | Tests  | Results |
|---------------|--|---------|
| SEAPATH-00087 | syslog-ng system calls are filtered            | PASS    |
| 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   | PASS    |
| SEAPATH-00050 | Linux kernel 'usb' : USB_EHCI_HCD is enabled   | PASS    |
| SEAPATH-00050 | Linux kernel 'usb' : USB_XHCI_HCD is enabled   | PASS    |
| SEAPATH-00171 | no RT throttling triggered                     | PASS    |
| 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 | /var/log/syslog is used as log target          | PASS    |
| SEAPATH-00102 | no systemd services have failed                | PASS    |
| SEAPATH-00170 | no systemd syntax warning                      | PASS    |

- number of tests: 181
- number of failures: 0

### Tests common security for guest1

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00106 | Check /etc/passwd permissions                             | PASS    |
| SEAPATH-00107 | Check /etc/shadow permissions                             | PASS    |
| SEAPATH-00108 | Check /etc/syslog-ng/ca.d/cacert.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-00193 | All directories writable by all users have the sticky bit | PASS    |
| SEAPATH-00194 | All directories writable by all users are owned by root   | PASS    |
| SEAPATH-00195 | Ceph OSD are owned by ceph                                | PASS    |
| SEAPATH-00088 | root password was randomized at boot                      | PASS    |
| SEAPATH-00089 | root password is randomized at each boot                  | PASS    |
| SEAPATH-00091 | root password is encrypted 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 | PASS    |



| Test ID       | Tests   | Results |
|---------------|---|---------|
| 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-00157 | PATH env. variable is correctly set                                     | 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' : STATIC_USERMODEHELPER is enabled             | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : USERFAULTFD is disabled                      | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : X86_VSYSCALL_EMULATION is disabled           | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : MODIFY_LDT_SYSCALL is disabled               | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : DEVMEM is disabled                           | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : USELIB is disabled                           | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : KEXEC is disabled                            | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : BINFORMAT_MISC is disabled                   | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : ALLOW_DEV_COREDUMP is disabled               | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : PROC_KCORE is disabled                       | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : KALLSYMS is disabled                         | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : SLUB_DEBUG_ON 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' : SLUB_DEBUG_ON 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-00050 | Linux kernel 'hardening' : RANDOMIZE_KSTACK_OFFSET_DEFAULT is enabled   | PASS    |
| 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           | PASS    |
| SEAPATH-00050 | Linux kernel 'hardening' : CC_HAS_AUTO_VAR_INIT_ZERO is enabled         | PASS    |
| SEAPATH-00050 | Linux kernel 'gcc_plugins' : GCC_PLUGIN_LATENT_ENTROPY is enabled       | PASS    |
| SEAPATH-00050 | Linux kernel 'gcc_plugins' : GCC_PLUGIN_RANDSTRUCT is enabled           | PASS    |
| SEAPATH-00158 | sudo policy is installed for group operator (operator)                  | PASS    |
| SEAPATH-00159 | sudo policy is installed for group maintenance-N1 (maint-n1)            | PASS    |
| SEAPATH-00160 | sudo policy is installed for group maintenance-N3 (maint-n3)            | PASS    |
| SEAPATH-00161 | sudo policy is installed for group cluster administrator (admincluster) | PASS    |
| SEAPATH-00162 | sudo policy is installed for group system administrator (adminsys)      | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| 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 (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   | PASS    |
| SEAPATH-00105 | /usr/bin/sudo has permissions 4750  | PASS    |
| SEAPATH-00143 | /etc/sudoers include noexec directive   | PASS    |
| SEAPATH-00144 | /etc/sudoers include requiretty directive   | PASS    |
| SEAPATH-00145 | /etc/sudoers include use_pty directive  | PASS    |
| SEAPATH-00146 | /etc/sudoers include umask=0027 directive   | PASS    |
| SEAPATH-00147 | /etc/sudoers include ignore_dot directive   | PASS    |
| SEAPATH-00148 | /etc/sudoers include env_reset directive  | PASS    |
| SEAPATH-00149 | /etc/sudoers include passwd_timeout=1 directive   | PASS    |
| SEAPATH-00150 | /etc/sudoers - all commands require authentication  | PASS    |
| SEAPATH-00151 | /etc/sudoers - no rule target root user   | 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-00151 | /etc/sudoers.d/ansible - no rule target root user   | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/ansible - EXEC option is not used  | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/ansible - rules are not defined by negation                                  | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/ansible - commands are not specified without arguments                       | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/ansible - no command is specified with wildcard argument                     | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/ansible - /etc/sudoers.d/ansible is owned by root:root with 0440 permissions | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/admin - all commands require authentication                                  | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/admin - no rule target root user   | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/admin - EXEC option is not used  | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/admin - rules are not defined by negation                                    | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/admin - commands are not specified without arguments                         | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/admin - no command is specified with wildcard argument                       | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions     | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/maint-n1 - all commands require authentication                               | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00151 | /etc/sudoers.d/maint-n1 - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/maint-n1 - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/maint-n1 - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/maint-n1 - commands are not specified without arguments                                | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/maint-n1 - no command is specified with wildcard argument                              | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/maint-n1 - /etc/sudoers.d/maint-n1 is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/privileged - all commands require authentication                                       | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/privileged - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/privileged - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/privileged - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/privileged - commands are not specified without arguments                              | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/privileged - no command is specified with wildcard argument                            | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/privileged - /etc/sudoers.d/privileged is owned by root:root with 0440 permissions     | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/operator - all commands require authentication   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/operator - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/operator - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/operator - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/operator - commands are not specified without arguments                                | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/operator - no command is specified with wildcard argument                              | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/operator - /etc/sudoers.d/operator is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/admincluster - all commands require authentication                                     | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/admincluster - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/admincluster - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/admincluster - rules are not defined by negation                                       | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/admincluster - commands are not specified without arguments                            | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/admincluster - no command is specified with wildcard argument                          | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/admincluster - /etc/sudoers.d/admincluster is owned by root:root with 0440 permissions | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/adminsys - all commands require authentication   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/adminsys - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/adminsys - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/adminsys - rules are not defined by negation   | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/adminsys - commands are not specified without arguments                                | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/adminsys - no command is specified with wildcard argument                              | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/adminsys - /etc/sudoers.d/adminsys is owned by root:root with 0440 permissions         | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/maint-n3 - all commands require authentication   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/maint-n3 - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/maint-n3 - EXEC option is not used   | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00153 | /etc/sudoers.d/maint-n3 - rules are not defined by negation                                       | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/maint-n3 - commands are not specified without arguments                            | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/maint-n3 - no command is specified with wildcard argument                          | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/maint-n3 - /etc/sudoers.d/maint-n3 is owned by root:root with 0440 permissions     | PASS    |
| SEAPATH-00150 | /etc/sudoers.d/emergadmin - all commands require authentication                                   | PASS    |
| SEAPATH-00151 | /etc/sudoers.d/emergadmin - no rule target root user  | PASS    |
| SEAPATH-00152 | /etc/sudoers.d/emergadmin - EXEC option is not used   | PASS    |
| SEAPATH-00153 | /etc/sudoers.d/emergadmin - rules are not defined by negation                                     | PASS    |
| SEAPATH-00154 | /etc/sudoers.d/emergadmin - commands are not specified without arguments                          | PASS    |
| SEAPATH-00155 | /etc/sudoers.d/emergadmin - no command is specified with wildcard argument                        | PASS    |
| SEAPATH-00156 | /etc/sudoers.d/emergadmin - /etc/sudoers.d/emergadmin is owned by root:root with 0440 permissions | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.modules_disabled is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - dev.tty.ldisc_autoload is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_fifos is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_regular is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_hardlinks is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.protected_symlinks is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - fs.suid_dumpable is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.dmesg_restrict is set properly  | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.kptr_restrict is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_event_paranoid is set properly                                     | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.randomize_va_space is set properly                                      | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.sysrq is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.unprivileged_bpf_disabled is set properly                               | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.yama.ptrace_scope is set properly                                       | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_event_max_sample_rate is set properly                              | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.perf_cpu_time_max_percent is set properly                               | PASS    |
| SEAPATH-00109 | sysctl-hardening - vm.mmap_min_addr is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.pid_max is set properly   | PASS    |
| SEAPATH-00109 | sysctl-hardening - kernel.panic_on_oops is set properly   | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.accept_redirects is set properly                               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.accept_source_route is set properly                            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.log_martians is set properly                                   | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.rp_filter is set properly                                      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.secure_redirects is set properly                               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.send_redirects is set properly                                 | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.all.shared_media is set properly                                   | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.accept_redirects is set properly                           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.accept_source_route is set properly                        | PASS    |

| Test ID       | Tests   | Results |
|---------------|---|---------|
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.log_martians is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.rp_filter is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.secure_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.send_redirects is set properly       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.conf.default.shared_media is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.icmp_echo_ignore_broadcasts is set properly       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.icmp_ignore_bogus_error_responses is set properly | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_invalid_ratelimit is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_max_syn_backlog is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_rfc1337 is set properly                       | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_syn_retries is set properly                   | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_synack_retries is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_syncookies is set properly                    | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_timestamps is set properly                    | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.ip_local_port_range is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv4.tcp_challenge_ack_limit is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra is set properly                | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra_defrtr is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_ra_pinfo is set properly          | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_redirects is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.accept_source_route is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.autoconf is set properly                 | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.dad_transmits is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.forwarding is set properly               | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.max_addresses is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.router_solicitations is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.all.use_tempaddr is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra is set properly            | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra_defrtr is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_ra_pinfo is set properly      | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_redirects is set properly     | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.accept_source_route is set properly  | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.autoconf is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.dad_transmits is set properly        | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.forwarding is set properly           | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.max_addresses is set properly        | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.router_solicitations is set properly | PASS    |
| SEAPATH-00109 | sysctl-network - net.ipv6.conf.default.use_tempaddr is set properly         | PASS    |
| SEAPATH-00109 | sysctl-network - net.netfilter.nf_conntrack_max is set properly             | PASS    |
| SEAPATH-00109 | sysctl-network - net.netfilter.nf_conntrack_tcp_loose is set properly       | PASS    |

| Test ID       | Tests  | Results |
|---------------|--|---------|
| SEAPATH-00176 | Check kptr_restrict is set to 2                | PASS    |
| SEAPATH-00177 | Check dmesg_restrict is set to 1               | PASS    |
| SEAPATH-00178 | Check pid_max is set to 4194304                | PASS    |
| SEAPATH-00179 | Check perf_cpu_time_max_percent is set to 1    | PASS    |
| SEAPATH-00180 | Check perf_event_max_sample_rate is set to 1   | PASS    |
| SEAPATH-00181 | Check perf_event_paranoid is set to 3          | PASS    |
| SEAPATH-00182 | Check randomize_va_space is set to 2           | PASS    |
| SEAPATH-00183 | Check sysrq is set to 0                        | PASS    |
| SEAPATH-00184 | Check unprivileged_bpf_disabled is set to 1    | PASS    |
| SEAPATH-00185 | Check panic_on_oops is set to 1                | PASS    |
| SEAPATH-00186 | Check kernel.yama.ptrace_scope is set to 2     | PASS    |
| SEAPATH-00187 | Check suid_dumpable is set to 0                | PASS    |
| SEAPATH-00188 | Check protected_fifos is set to 2              | PASS    |
| SEAPATH-00189 | Check protected_regular is set to 2            | PASS    |
| SEAPATH-00190 | Check protected_symlinks is set to 1           | PASS    |
| SEAPATH-00191 | Check protected_hardlinks is set to 1          | PASS    |
| SEAPATH-00192 | Check modules_disabled is set to 1             | PASS    |
| SEAPATH-00082 | /var/log is mounted on a separate partition    | PASS    |
| SEAPATH-00085 | syslog-ng can not acquire new privileges       | PASS    |
| SEAPATH-00086 | syslog-ng capabilities are bounded             | PASS    |
| SEAPATH-00087 | syslog-ng system calls are filtered            | PASS    |
| SEAPATH-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   | PASS    |
| SEAPATH-00050 | Linux kernel 'usb' : USB_EHCI_HCD is enabled   | PASS    |
| SEAPATH-00050 | Linux kernel 'usb' : USB_XHCI_HCD is enabled   | PASS    |
| SEAPATH-00171 | no RT throttling triggered                     | PASS    |
| 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 | /var/log/syslog is used as log target          | PASS    |
| SEAPATH-00102 | no systemd services have failed                | PASS    |
| SEAPATH-00170 | no systemd syntax warning                      | PASS    |

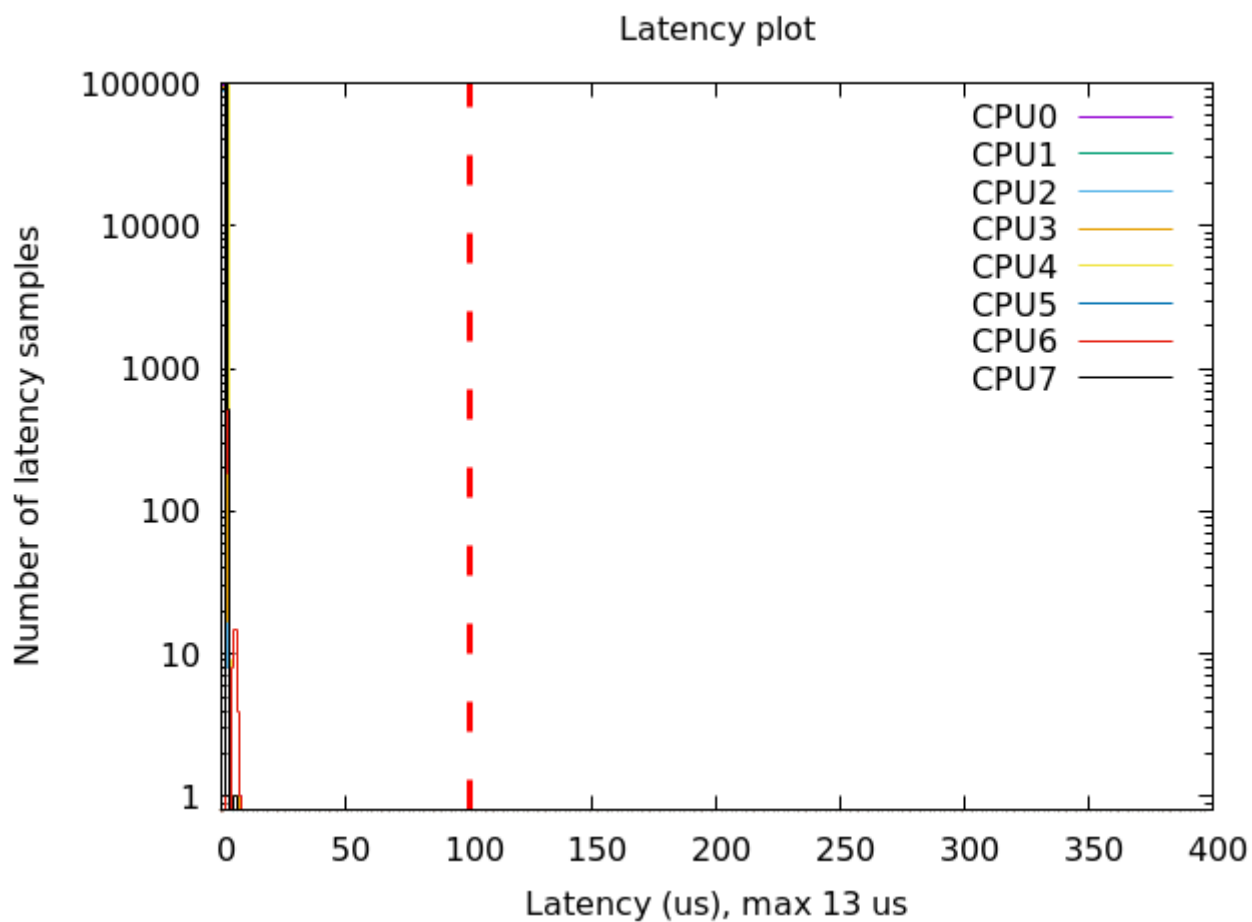
- number of tests: 181
- number of failures: 0

### 4.1.5. Real-time testing (Cyclictest)

The following command is launched:

```
cyclictest -l10000 -m -Sp90 -i200 -h400 -q
```

#### Hypervisor

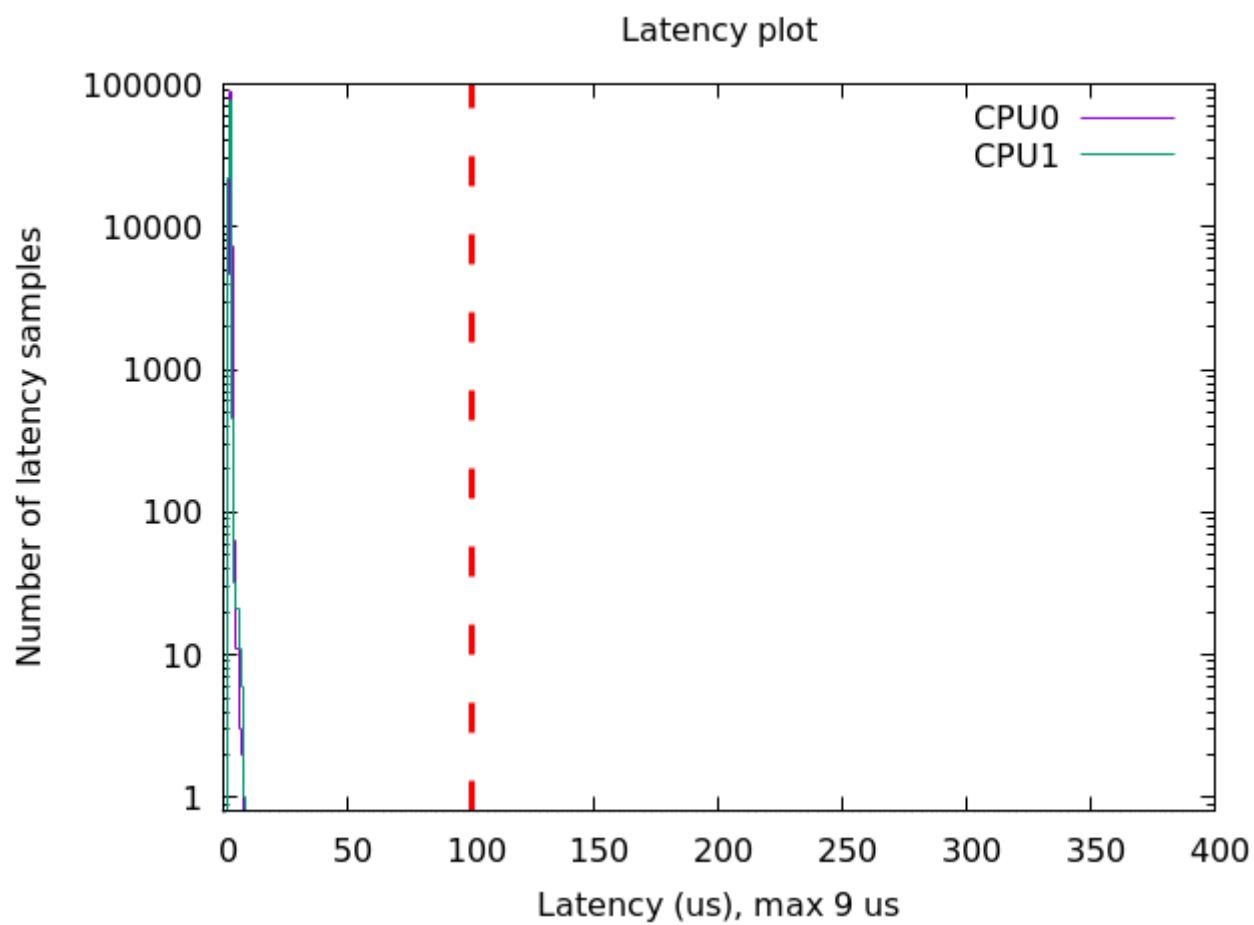


Max latency < 100 us

PASS

## Virtual Machines

Guest 0



Max latency < 100 us

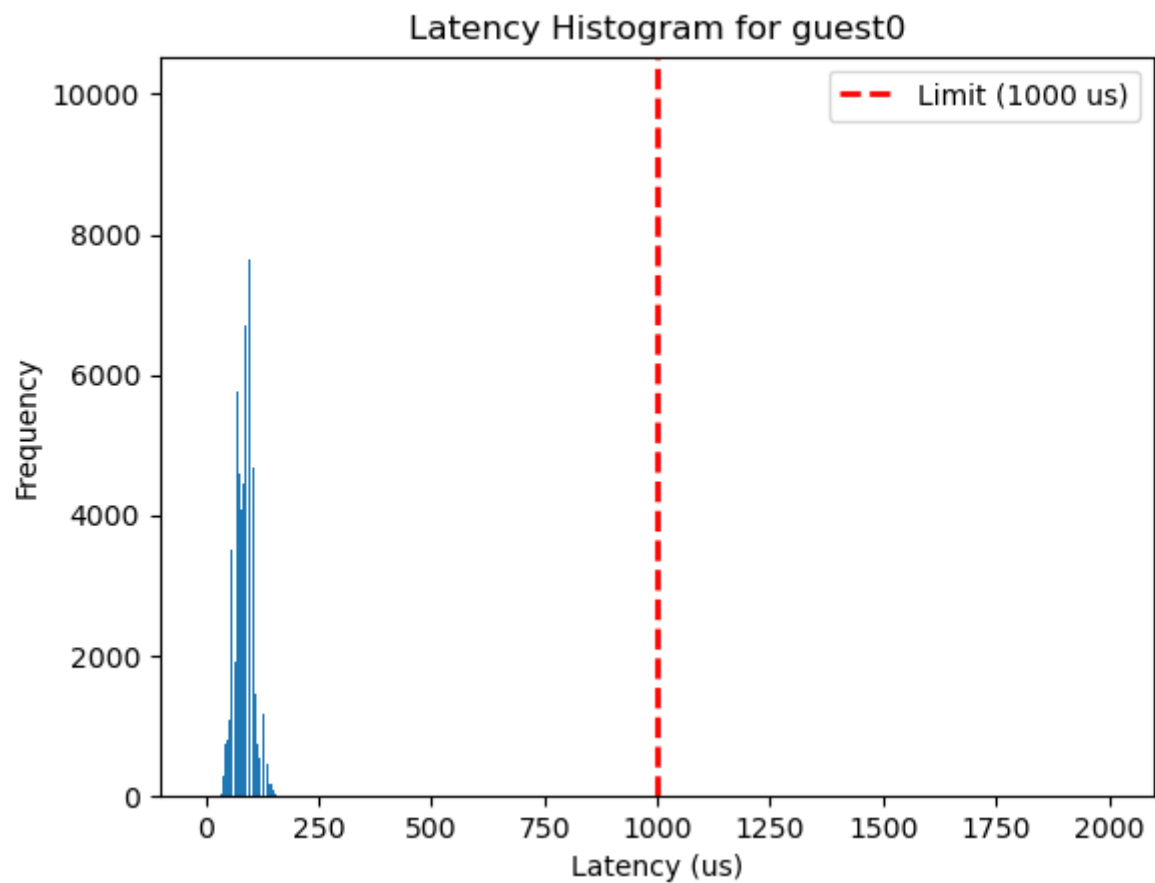
PASS



4.1.6. IEC61850 Sampled Value Latency Testing

VM guest0

| Number of IEC61850 Sampled Value | Minimum latency | Maximum latency | Average latency |
|----------------------------------|-----------------|-----------------|-----------------|
| 8                                | 31 us           | 160 us          | 87.0 us         |



|                       |      |
|-----------------------|------|
| Max latency < 1000 us | PASS |
|-----------------------|------|

# Chapter 5. About this documentation

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

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

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

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

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

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