Oracle VM Server for SPARC 3.6 and Oracle Solaris 11.4

Common Criteria Guide

Version 1.5

January 2024

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of Oracle VM Server for SPARC 3.6 and Oracle Solaris 11.4 and related information.

1.2 Audience

2 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed section 1.5.

1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1 Protection Profile Conformance

4 The Common Criteria evaluation was performed against the following requirements:

a) NIAP Protection Profile for Virtualization, Version 1.1 (Base_PP)

b) NIAP PP-Module for Server Virtualization, Version 1.1 (MOD_SV)

c) NIAP Functional Package for SSH, Version 1.0 (PKG_SSH)

d) NIAP Functional Package for TLS, Version 1.1 (PKG_TLS)

5 Protection Profiles are available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Hardware/Software

6 The TOE is Oracle VM Server for SPARC 3.6.2.0.57 and Oracle Solaris 11.4.57.0.1.144.3 with IDR 5391, running on the SPARC T8 hardware.

7 **NOTE:** VM Server for SPARC is an integrated part of Oracle Solaris.

1.3.3 Evaluated Functions

8 The following functions have been evaluated under Common Criteria:

a) **VM Hardware-based Isolation.** The TOE supports isolation mechanisms to constrain a Guest Virtual Machines (VM) direct access to physical devices.

b) **VM Resource Control.** The TOE enables control of Guest VM access to physical platform resources.

c) **VM Residual Information Clearing.** The TOE ensures that any previous information content in memory or physical disk storage is cleared prior to allocation to a Guest VM.

d) **VM Networking & Separation.** The TOE enables control of mechanisms used to transfer data between Guest VMs, including control of virtual networking components.

e) **VM User Interface.** The TOE indicates to users which VM if any has current input focus and supports unique identification of VMs.

f) **VS Integrity.** The TOE maintains integrity of the virtualization system (VS) critical components via measured boot and trusted software updates.

g) **VS Self Protection.** The TOE implements self-protection mechanisms including execution environment mitigations, hardware-assists, hypercall controls, isolation from VMs and controls for removable media.

h) **Protected Communications.** The TOE protects the integrity and confidentiality of communications with remote administrators and remote audit servers.

i) **Secure Administration.** The TOE enables secure management of its security functions, including:

   i) Administrator authentication with passwords

   ii) Configurable password policies

   iii) Role Based Access Control

   iv) Access banners

   v) Management of critical security functions and data

j) **System Monitoring.** The TOE generates audit records and stores them locally and is capable of sending records to a remote audit server. The TOE protects stored audit records and enables their review.

k) **Cryptographic Operations.** The TOE implements cryptographic operations in support if its security functions.

9 **NOTE:** No claims are made regarding any other security functionality.

1.3.4 Evaluation Assumptions

10 The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 1: Evaluation Assumptions

Assumption	Guidance
A.PLATFORM_INTEGRITY - The platform has not been compromised prior to installation of the Virtualization System.	No additional guidance.
A.PHYSICAL - Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.	Ensure that the TOE hardware is hosted in a physically secure environment, such as a locked server room.
A.TRUSTED_ADMIN - TOE Administrators are trusted to follow and apply all administrator guidance.	Ensure that administrators are competent, are able to follow the provided guidance.
A.COVERT_CHANNELS - If the TOE has covert storage or timing channels, then for all VMs executing on that TOE, it is assumed that relative to the IT assets to which they have access, those VMs will have assurance sufficient to outweigh the risk that they will violate the security policy of the TOE by using those covert channels.	The evaluation did not address covert channels.
A.NON_MALICIOUS_USER - The user of the VS is not wilfully negligent or hostile and uses the VS in compliance with the applied enterprise security policy and guidance. At the same time, malicious applications could act as the user, so requirements which confine malicious applications are still in scope.	The evaluation considered users to be non-hostile – additional controls should be employed if this is not the case.

1.4 Conventions

11 The following conventions are used in this guide:

a) `CLI Command <replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example:

Use the `cat <filename>` command to view the contents of a file

b) [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

c) **GUI => Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File => Save** to save the file.

d) [REFERENCE] *Section* – denotes a related document and section reference. For example:

Follow [ADMIN] *Configuring Users* to add a new user.

1.5 Virtualization Terminology

12 The following terms are explicitly noted to assist in correlating NIAP Protection Profile terminology with Oracle terminology:

a) **Logical Doman.** A Virtual Machine (VM).

b) **Guest Domain.** A Guest VM.

1.6 Additional Guides

13 This document supplements the following guides:

a) [OVM] - Oracle VM Server for SPARC 3.6 Documentation Library - https://docs.oracle.com/cd/E93612_01/

b) [T8LIB] – Oracle SPARC T8 information Library - https://docs.oracle.com/en/servers/sparc/t8/index.html

c) [Solaris] – Oracle Solaris 11.4 Information Library - https://docs.oracle.com/cd/E37838_01/

14 **NOTE:** The information in this guide supersedes related information in other documentation.

2 Secure Acceptance and Installation

2.1 Obtaining the TOE

15 The TOE software is installed on the TOE hardware and delivered to the customer by a commercial courier service with a package tracking system.

16 To obtain the CC evaluated version of the TOE software, if not already installed, customers may download the TOE software from the Oracle Software Delivery Cloud at https://edelivery.oracle.com.

17 To download the TOE:

1) Login to the edelivery website.
2) Search for “Oracle Solaris” and select the Oracle Solaris 11.4.0.0.0 download package.
3) Press the continue button.
4) Select the SPARC option and press continue.
5) Read and accept all license agreements.
6) Select “V979533-01.iso” and click download.

2.2 Installing the TOE

18 To install the T8 server hardware, follow the Setup and Installation instructions detailed in [T8LIB].

19 For Oracle Solaris, follow the instructions of Manually Installing an Oracle Solaris 11.4 System augmented by the configuration guidance in this document.

20 To achieve the evaluated configuration, the correct Support Repository Update (SRU) must be installed. Installation of SRU 57 is required to achieve the evaluated configuration. The ‘entire’ package version should be 11.4.57.0.1.144.3 with IDR 5391. See Applying Support Updates and Installing an IDR Custom Software Update and Understanding Oracle Solaris 11 Package Versioning for more information.

2.3 Verifying the TOE

21 Each TOE appliance shipment contains a packing list. The packing list is used by customers to verify their orders. The packing list contains the billing and shipping information for the order as well as the shipping carrier information, number of pieces in the shipment, estimated weight of the shipment, and the delivery number. The packing list also contains a line-by-line listing of the quantity of appliances, and their serial numbers for each appliance in the sales order.

22 To verify the TOE and SRU versions installed, use the `pkg info entire` command.

23 To verify the IDR installed, use the `pkg list -a | grep idr | grep 'i...$'` command.

24 To verify the OVM version, use the `ldm -V` command.

2.4 Updating the TOE

25 Upgrading to a new Oracle Solaris operating system release is done through the Oracle Solaris Image Packaging System (IPS) framework which provides tools to perform a number of tasks including:

a) List, search, install, restrict installation, update, and remove software packages.

b) List, add, and remove package publishers. Change publisher attributes such as search priority and stickiness. Set publisher properties such as signature policy.

c) Upgrade an image to a new operating system release.

d) Install additional application software

e) Create and publish packages.

f) Create boot environments and other images.

26 Oracle Solaris 11 software is distributed in IPS packages, stored in IPS package repositories from configured publishers. An IPS package is defined by a text file called a manifest. A package manifest describes package actions in a defined format of key/value pairs and possibly a data payload. Package actions include files, directories, links, drivers, dependencies, groups, users, and license information. Package actions represent the installable objects of a package. IPS packages are installed into Oracle Solaris 11 images.

27 Oracle Solaris operating system upgrade packages are downloaded from a configured publishers package repository.

28 Use the pkg publisher command to display information about package publishers configured for the Oracle Solaris 11 software image.

29 Use the pkg list -avf entire command to list the available packages. See *Displaying Package Contents and Descriptions* to see more on this command.

30 Use the pkg update command to upgrade the system. The (-v) option of the command can be used to see what packages and what versions of the packages will be updated, removed, and installed; and to diagnose problems with the software upgrades.

31 The pkg update command (in addition to other pkg commands) will also check for updates to installed applications (software packages).

32 The authorized administrator must be assigned the Software Installation rights profile in order to execute the pkg and beadm commands to install and update packages and manage boot environments.

33 Platform firmware updates are downloaded from the Oracle IPS support repository.

34 See Image Update Best Practices for additional information on manual update of the TOE.

3 Configuration Guidance

3.1 Services Configuration

35 The Oracle Solaris Service Management Facility (SMF) framework manages system and application services, including all critical system services essential to the working operation of the TOE. SMF ensures that essential system and application services run continuously even in the event of hardware or software failures.

36 **NOTE:** To perform tasks associated with network configuration, the authorized administrator must be assigned the Network Management Profile access rights. See Network Administration Cheatsheet for additional details of network configuration.

3.1.1 Time Server

37 Oracle Solaris supports the use of an NTP server to provide accurate time services, only the authorized administrator can configure the NTP server.

38 Copy the ntp.client file to use as a template for the ntp.conf file

39 Use the command cp ntp.client ntp.conf

40 Use the the pfedit command to edit the ntp.conf file with the name and address of the specific ntp server, and start the ntp daemon with the command

41 Use the command svcadm enable ntp

42 Additional information can be found here.

43 To ensure that an audit record is generated for changes to the ntp server configuration, a per-file auditing ACL is required. See Specifying Files or Directories to be Audited for more information.

3.2 Secure Administration

3.2.1 User Interfaces

44 The TOE provides the following user interfaces to access and manage its functions and data.

a) Command line interface — on the local console, used to administrator the system locally, including managing user accounts.

b) SSH interface — used to administer the TOE remotely. All commands including the SMF service stencils used to configure essential system and application services are accessible through SSH.

45 Users terminate a local interactive session by selecting the logout option on the TOE dashboard or by typing '*exit*' at the command line.

3.2.2 Admin/User authentication

46 The TOE ensures that all users must be authenticated before gaining access to its functions and data. The TOE maintains a local repository of user attributes which it uses to authenticate users. This repository includes the user information stored in the /etc/password and in the /etc/shadow files.

47 The useradd command is used to setup and manage user accounts. The useradd, userdel, passwd, and usermod commands provide options to configure user accounts settings that include username, userID number, passwords, role, group membership,

and home directory. The user password attribute is stored hashed in the /etc/shadow file. Only privileged accounts can read the /etc/shadow file. The RAD usermgr module can also be used to configure user accounts remotely via the RAD interface. See Setting Up and Managing User Accounts for more information.

48 Idle session timeouts should be configured by adding the following to the top of /etc/profile file:
readonly TMOUT=<time-in-seconds>
export TMOUT

(Note: the readonly command is used to make the variable TMOUT read only, therefore users cannot change the value of the variable once configured).

49 When users log in to the TOE, they must supply a username and passwords. The TOE verifies the username/password entered based on a SHA-256 hash comparison to the known user database and allow access only if the information match; access is denied if username/password entered is incorrect. The TOE leverages the Pluggable Authentication Module (PAM) authentication mechanism for user authentication. A user account can be disabled by locking the password.

50 The TOE uses public key and password for user authentication on the SSH interface. When users log into the SSH interface, the TOE will first do the public key check to allow the connection and then optionally verify the user password before allowing access. For more information on specifying public keys to permit in the AuthorizedKeysFile, see sshd(8).

3.2.3 Role-Based Access Controls

51 The TOE implements role-based access control to restrict access to its functions. A role defines a set of access rights assigned to a user. The TOE restricts management of its security functions to the authorized administrators. The root user is assigned all permissions. The table below identify the security functions that are accessible to authorized administrators and users.

Number	Function	Admin	User
1	Ability to update the Virtualization System	X	N
2	Ability to configure Administrator password policy	X	N
3	Ability to create, configure and delete VMs	X	N
4	Ability to set default initial VM configurations	X	N
5	Ability to configure virtual networks including VM	X	N
6	Ability to configure and manage the audit system and audit data	X	N
7	Ability to configure VM access to physical devices	X	N
8	Ability to configure inter-VM data sharing	X	N
9	Ability to configure removable media policy	X	N
10	Ability to configure the cryptographic functionality	X	N
11	Ability to change default authorization factors	X	N

Number	Function	Admin	User
12	Ability to enable/disable screen lock	N	N
13	Ability to configure screen lock inactivity timeout	N	N
14	Ability to configure remote connection inactivity timeout	X	N
15	Ability to configure lockout policy for unsuccessful authentication attempts	X	N
16	Ability to configure name/address of audit/logging server to which to send audit/logging records	X	N
17	Ability to configure name/address of network time server	X	N
18	Ability to configure banner	X	N
19	Ability to connect/disconnect removable devices to/from a VM	X	N
20	Ability to start a VM	X	N
21	Ability to stop/halt a VM	X	N
22	Ability to checkpoint a VM	N	N
23	Ability to suspend a VM	N	N
24	Ability to resume a VM	N	N

3.2.4 Management of Security Functions

52 The svc:/system/account-policy:default service provides the security policy configuration only when the config/etc_security_policyconf/disabled setting (within the account-policy:default service) is set to “FALSE”. Therefore, this service will override the /etc/security/policy.conf file to address user account attributes, Authentication Policy, password complexity and default RBAC settings. The following SMF properties should be set using this service:

rbac/default_authorizations — specifies the default set of authorizations granted to all users.

rbac/console_user_profiles — Specify an additional default set of profiles granted to the *console user* user.

password/crypt/default — Specify the default algorithm for new passwords. The Oracle Solaris default is the crypt_sha256 algorithm. Value should be a single numeric code for an algorithm chosen from the list in /etc/security/crypt.conf.

login_policy/lock_after_retries — Specifies whether a local account is locked after the count of failed logins for a user equals or exceeds the allowed number of retries as defined by login_policy/retries.in the account-policy:default service.

rbac/default_privileges and rbac/default_limit_privileges — specifies default privileges.

login/auto_unlock_time — Specifies the time after which an account lock for failed logins will be unlocked upon a valid password entry. The time may be specified as a number of minutes (m), hours (h), days (d), or weeks (w).

3.2.4.1 Authentication Failure

53 The account lockout policy is configured using the service svc:/system/account-policy:default and setting the property login_policy/lock_after_retries. The authorized administrator configured the number of failed attempts before the account is locked to be between 1 and 15. Per user account policy should be configured using the usermod or rolemod commands.

3.2.4.2 Password Management

54 The TOE enforces a password policy that defines the composition and complexity of passwords. The password policy is provided by the svc:/system/account-policy:default service only when the config/etc_default_passwd/disabled setting (within the account-policy:default service) is set to "FALSE". Therefore, this service will override the /etc/default/passwd file. The configurable passwords parameters set by the password policy includes password length, case sensitivity, use of numeric and special characters. For additional details see Password Parameters.

55 The passwd <user> command is used to change a user's password. To unlock a user account passwd -u is used. See the passwd Manpage for more information.

3.2.4.3 Audit Logging

56 The TOE audit services track auditable actions that occur on the system, keep a record of how the system is being used and provide tools to review and analyse the collected audit data. Captured in each audit record is information that identifies the type of audit event, what caused the event including the identity of the user that caused the event - where applicable, the time and date of the event, success or failure of the event, as well as other event specific information required by the ST.

57 The audit service, auditd, is enabled by default, however, in the evaluated configuration, at initial installation the default configuration must be modified to ensure that all audit parameters and auditable events required by the security requirements defined by the Oracle Solaris 11.4 ST are satisfied.

58 To configure and manage the audit functions the authorized administrator must be assigned the following rights profiles:

Audit configuration – required for configuring the parameters of the audit service and to run the auditconfig command.

Audit Control – required to run the audit command to start, refresh, stop the audit service or to enable/disable the audit service

Audit Review – required to view and analyse the audit records with the commands praudit and auditreduce, and to run the auditstat command.

root privilege is required to edit an audit configuration file.

59 The auditconfig command is used to specify the audit parameters for the TOE including:

Audit Class — classes of attributable events (events that can be attributed to a user) and non-attributable events (events that occurs at the kernel-interrupt level, not attributable to a user such as booting the system). The audit class definitions are specified in the audit_class system file, which is configured by the authorized administrator and which maps like auditable events to one or more audit classes.

Audit Policy — divides synchronous events (events that are associated with a process where the process can be stopped if events cannot be queued); and

asynchronous events (events that are not associated with a process such as initial system boot).

Audit plugin — places audit records from the queue to the appropriate file or repository.

Queue Control — defines the maximum message size.

60 The auditconfig subcommands are used to configure the classes of events to be audited. An audit flag character string can be used to Audit flags used as part of the audit

auditconfig -set* assigns a value to the parameter that is represented by the asterisk (*), such as –setflags, –setpolicy, or –setqctrl. To configure classes for non-attributable events, the auditconfig setnaflags subcommand is used. The audit flag character string specifies which audit classes are to be audited for a process.

auditconfig -conf configures kernel audit event to class mappings.

61 The following events are handled by the identified audit classes:

a) Startup and Shutdown of audit services – “frcp” (part of “cusa”)

b) Session authentication and termination – “lo” (part of “cusa”)

c) Privilege elevation – “pe” and “pm”

d) File operations – “fc”, “fr”, “fd”, “fw”, and “fm”

e) User and Group management events – “ua”

f) Audit and Log data access events – “fr”

g) Cryptographic verification of software – “pe”

h) Attempted application invocation with arguments – “ex”

i) System reboot, restart, or shutdown events – “frpc” (part of “cusa”)

j) Kernel module loading and unloading events – “as” (part of “cusa”)

k) Administrator and root-level access events – “lo”

62 For additional details on audit classes and the auditconfig subcommands see Audit_class and Configuring the Audit Service. Virtualization related audit events are part of the “as” class.

63 The audit policy determines the characteristics of the audit records for the local system. The TOE audit service includes several audit policy options that can be enabled in the TOE including the ahlt option which if enabled will stop the system when the audit queue is full, the cnt option which when enable, if audit storage is reaching capacity, will ensure that a warning is issued when one percent disk space remains, and the argv option which enables the capability of auditing the arguments to called binaries If audit records cannot be added to the audit trail because the audit queue is full, the cnt option will also ensure that the system tracks the number of dropped audit records. The auditconfig command is used to set the audit policy.

64 For additional information about audit policy see Understanding Audit Policy.

65 Audit plugins direct the audit records from the audit queue to a file or repository. The TOE includes 2 audit plugins which are configured using the auditconfig -setplugin command.

The audit_binfile plugin places binary audit records in /var/audit. This is the only plugin that is active by default. This plugin is also used to assign additional disk

space to the audit trail. For additional information see Configuring Audit Space for the Audit Trail and Audit Files.

To enable/disable the audit service, the authorized administrator must be assigned Audit Control rights profile.

Use the command pfbash ; audit -t to disable the audit service

Use the command audit -s to enable the audit service after it has been disabled

Use the command auditconfig -getcond to verify that the audit service is running

66 The praudit command is used to review the audit records in the audit trail.

67 Detailed audit messages for cryptographic verification of software can be retrieved using the pkg history command. More verbose information, including failure information, can be yielded by appending a timestamp to this command (eg. pkg history -l -t <timestamp>) See man pkg(1) for more information.

68 Per-file auditing ACLs can be used to track changes to files such as writes, deletes, and appends. See Specifying Files or Directories to be Audited for more information

69 To audit the enabling/disabling of the session timeout function, an additional directory should be created with an inheritable ACE to track file write, create, delete, append_data changes (eg. /etc/profile.timeout.d). A file can then be created within this directory that contains the TMOUT variable (containing the session timeout value). the /etc/profile file should then source the file contained within the /etc/profile.timeout.d to configure session timeout. This method would enable an auditing mechanism to track the enabling/disabling or configuration changes to session timeout functionality.

70 Note: log messages for configuring the local audit storage capacity are stored in the ZFS audit log which can be accessed via the zpool history -l command.

71 Audit record format can be found in [Solaris] under *Managing Auditing in Oracle* > *Auditing Reference* > *Audit Record Structure*.

3.2.4.4 Setting Audit Flags

72 To set system-wide audit flags, use the following commands/syntax:

- `auditconfig -setflags cusa,ex,fd,fw,fc,vs[other flags as needed]`
- `auditconfig -setnaflags cusa,ex,fd,fw,fc,vs[other flags as needed]`
- `auditconfig -setpolicy +argv`
- `svcadm refresh svc:/system/auditset:default`

73 To set per-user audit flags:

- `usermod -K audit_flags=[flag1,flag2,...,flagN] <username>`

74 To set per-file audit flags:

- `chmod A+everyone@:full_set:successful_access/failed_access/file_inherit:audit <filename>`

3.2.4.5 Enable Logging of the Virtualization System

75 To enable logging of the Virtualization System:

- Add the following line to `/etc/ /etc/security/audit_event`:

  ```
  40700:AUE_ldoms:ldoms administration:vs
  ```

- Add the following line to `/etc/security/audit_class`:

  ```
  0x10000000:vs:virtualization_software
  ```

- Run the following commands to ensure the ldmd service is configured for auditing:

  ```
  svccfg -s ldmd listprop
  svccfg -s ldmd setprop ldmd/audit = boolean: true
  svcadm restart ldmd
  ```

3.2.4.6 Syslog

76 The TOE must be configured to send logs to a remote syslog server over TLS. To configure the TOE use rsyslog, follow the instructions in Annex A: Syslog Configuration below. To configure the TOE to use TLS for this communication channel, follow the instructions in section 4.2.

3.2.5 Non-Essential Services

77 The following services should be uninstalled from the system using the pkg uninstall command to achieve the evaluated configuration and reduce attack surface:

a) CUPS print service on tcp port 515 (pkg uninstall cups)
Note: only applicable if the TOE is not also functioning as a print server.

b) System Web Interface on tcp port 6787 (pkg uninstall webui-server)

3.3 Cryptography

78 The TOE cryptographic framework provides two FIPS 140-2 validated cryptographic modules: a userland module which supplies cryptography for applications that run in user space and the kernel module which provides cryptography for kernel-level processes. The TOE OpenSSL FIPS 140-2 provider installed with the command pkg install openssl-fips-140.

79 The cryptoadm utility displays cryptographic provider information for a system, configures the mechanism policy for each provider, and installs or uninstalls a cryptographic provider. The cryptographic framework supports three types of providers: a user-level provider (a PKCS11 shared library), a kernel software provider (a loadable kernel software module), and a kernel hardware provider (a cryptographic hardware device).

80 FIPS mode is enabled in the evaluated configuration with the detailed steps and specific commands outlined in Running in FIPS 140-2 Mode on an Oracle Solaris 11.4 System:

81 The cryptographic engines described above are the only ones tested for use in the CC evaluation. Use of any other cryptographic engines were not tested and therefore are not included within the scope of the CC evaluation.

3.3.1 SSH

82 The TOE supports The OpenSSH daemon is linked to the OpenSSL FIPS 140-2 package in the TOE so it runs in FIPS mode. Additional sshd configuration can be done using the command line or by modifying the `sshd_config` file. See sshd for the correct syntax for configuring or modifying the following the cryptographic parameters with the following values:

a) Public Key Algorithms — ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384

b) Encryption Algorithms — aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc, aes128- gcm@openssh.com, aes256-gcm@openssh.com

c) MAC Algorithms — hmac-sha2-256, hmac-sha2-512, and implicit (when using @openssh.com encryption)

d) Key Exchange Methods — diffie-hellman-group14-sha256

e) ReKey Limit – not to exceed 3600 seconds or 1024 MB

f) AuthenticationMethods – publickey, password

83 Both Public key and Password authentication methods are supported in the evaluated configuration. All other authentication mechanisms should be disabled. Setting the AuthenticationMethods parameter in the `sshd_config` file as described above specifies this configuration.

84 SSH host keys must be generated using only RSA 2048, 3072 and ECDSA P-256, P-384 curves and must be protected in a ZFS encrypted dataset.

3.3.2 Entropy

85 To disable swrand, use the cryptoadm disable provider=swrand all command.

86 To increase the rng health check frequency to every 60 seconds, add the hc_seconds=60 parameter to the /etc/driver/drv/n2rng.conf file.

3.4 VM Server for SPARC Configuration

87 Oracle VM Server for SPARC (also known as LDom) is the server virtualization system that allows for the creation of multiple systems on a single physical SPARC server by partitioning system resources.

88 During the initial set up of an LDom server, a default domain is created called the Control Domain, which owns all the hardware available to the system (CPU, RAM, IO, etc.). The Control Domain instance should only be exposed on a dedicated management network. LDom requires ports TCP/6482 for Management and TCP/8101 for Migration services.

89 General administration and configuration guidance is provided at https://docs.oracle.com/cd/E93612_01/

3.4.1 Physical Platform Resource Control

90 Guest Domains are explicitly denied access to Integrated Lights Out Management (ILOM).

91 Guest Domain access to physical devices (including removable devices and media) is configured when it is created or edited by an administrator. See How to Create and Start a Guest Domain.

3.4.2 VM Separation

92 The TOE users virtual networking to allow communication between Guest Domains. See Using Virtual Networks.

3.4.3 VM User Interface

93 VMs are assigned a unique name when they are created. A VM cannot be created using an existing name. This name is displayed to users of the VM in the CLI, in which the VM is running.

3.4.4 Separation of Management and Operational Networks

94 Administrators can establish separate management and operational networks using physical and virtual networking. See Using Virtual Networks and Solaris Network Administration Cheatsheet for details on physical network configuration.

4 Annex A: Syslog Configuration

4.1 Syslog Setup

95 Ensure the system-log uses rsyslog by running the following commands:

- `svcadm disable svc:/system/system-log:default`
- `svcadm enable svc:/system/system-log:rsyslog`

96 Create the log destination files if they do not already exist:

- `touch /var/log/authlog`
- `touch /var/adm/auditlog`
- `chmod 640 /var/log/authlog`
- `chmod 640 /var/adm/auditlog`

97 Edit `/etc/rsyslog.d/example_rsyslog_config_file.conf` as follows:

- `auth.info;auth.debug /var/log/authlog`
- `audit.* /var/adm/auditlog`

4.2 TLS Configuration

98 Edit `/etc/rsyslog.d/example_rsyslog_tls_client_config_file.conf` as follows:

Configure the client Certs/Keys, the trusted CAs and CRLs

```
global(
      DefaultNetstreamDriverCAFile="/etc/certs/ca-
   certificates.crt"
      DefaultNetstreamDriverCRLFile="/etc/certs/crls/rsyslo
 g-crl.pem"
      )
```

99 Log entry format, with timestamp:

```
$template CustomFormat,"%timegenerated:::date-year%-
%timegenerated:::date-month%-%timegenerated:::date-day%
%timegenerated:::date-hour%:%timegenerated:::date-
minute%:%timegenerated:::date-second% %HOSTNAME%
%syslogtag%%msg%\n"
```

100 The action for all messages:

101 **Note**: The `StreamDriverPermittedPeers` option is used to set the reference identifier.

```
*.* action(
      type="omfwd"
      protocol="tcp"
      port="6514"
```

```
target="services.example.com"
StreamDriver="ossl"
StreamDriverMode="1"
StreamDriverAuthMode="x509/name"
StreamDriverPermittedPeers="services.example.com"
StreamDriver.CheckExtendedKeyPurpose="on"
Template="CustomFormat"
gnutlsPriorityString="
MinProtocol=TLSv1.2
MaxProtocol=TLSv1.2
CipherString=AES128-SHA:AES256-SHA:AES128-
SHA256:AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-
SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-
SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-
SHA384"
)
```

4.3 CRL Configuration

102 The administrator should ensure that the CRL for the remote rsyslog server is updated before the rsyslog service starts. This is not provided as a core feature of Oracle Solaris / Logical Domains platform because it is not always possible to determine where to retrieve the CRL from.

103 Assuming that the CRL is available over http without authentication then a simple SMF service that is run before rsyslog starts is provided below.

104 The site/rsyslog-crl service will go into the maintenance state on any errors (miss configured, no or invalid CRL) and prevent the start-up of the dependent svc:/system/system-log:rsyslog service. It will also cause an FMA alert to be raised for the administrator.

105 Create the following as /lib/svc/method/site-rsyslog-crl and make it executable:

```
--- BEGIN method script ---
#!/usr/bin/bash
. /lib/svc/share/smf_include.sh
. /lib/svc/share/smf_exit_codes.sh

CRL_URL=$(svcprop -p config/crl-url $SMF_FMRI)
crlfile=$(awk -F= '/DefaultNetstreamDriverCRLFile/ {print $2}'
\
     /etc/rsyslog.d/* | sed -e s/\"// -e s/\"$//)
if [ -z "$crlfile" ]; then
   smf_method_exit $SMF_EXIT_ERR_CONFIG no_config \
   "DefaultNetstreamDriverCRLFile not set in/etc/rsyslog.d/"
```

```
fi
download_file=$(mktemp)
/usr/bin/curl -s $CRL_URL -o ${download_file}
if [ $? -ne 0 ]; then
   smf_method_exit $SMF_EXIT_ERR_CONFIG no_crl \
   "Unable to download CRL from $CRL_URL"
fi
/usr/openssl/3/bin/openssl crl -noout -in ${download_file}
if [ $? -ne 0 ]; then
   smf_method_exit $SMF_EXIT_ERR_CONFIG invalid_crl \
   "Invalid CRL downloaded from $CRL_URL"
fi
mv ${download_file} $crlfile
--- END method script ---
```

106 Create the service manifest as /lib/svc/manifest/site/rsyslog-crl.xml.

```
--- BEGIN SMF manifest ---
<?xml version="1.0" ?>
<!DOCTYPE service_bundle
SYSTEM '/usr/share/lib/xml/dtd/service_bundle.dtd.1'>
<service_bundle name="site/rsyslog-crl" type="manifest">
   <service name="site/rsyslog-crl" version="1"
type="service">
         dependency name="networking" grouping="require_all"
         restart_on="none" type="service">
         <service_fmri value="svc:/milestone/name-services"/>
   </dependency>
         dependent name="rsyslog" grouping="require_all"
         restart_on="restart">
         <service_fmri value="svc:/system/system-
      log:rsyslog"/>
   </dependent>
   exec_method name="start" type="method" timeout_seconds="60"
         exec="/lib/svc/method/site-rsyslog-crl"/>
   <exec_method name="stop" type="method" timeout_seconds="60"
         exec=":true"/>
   <property_group name="startd" type="framework">
```

```
            <propval name="duration" type="astring"
          value="transient"/>
      </property_group>
      <instance name="default" enabled="false">
            <property_group name="config" type="application">
            <propval name="crl-url" type="astring" value=""/>
       </property_group>
</instance>
</service>
</service_bundle>
--- END SMF manifest ---
```

107 Import the service and set the location of the CRL and start the service:

- `svcadm restart -s manifest-import`
- `svccfg -s site/rsyslog-crl:default setprop config/crl-url="http://example.com/crl.pem"`
- `svccfg -s site/rsyslog-crl:default refresh`

108 Enable the service. This will cause rsyslog to restart. On reboot this service will run before svc:/system/system-log:rsyslog:

- `svcadm enable -s site/rsyslog-crl`