Oracle Solaris 11.4

Common Criteria Guide

Version 1.3

January 2021

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 the 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 in Table 2.

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 requirements of the Protection Profile for General Purpose Operating Systems (PP_OS) v4.2.1, the Functional Package for Transport Layer Security (pkg_TLS) v1.1 and Extended Package for Secure Shell (EP_SSH) v1.0, all available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Software

5 The Target of Evaluation (TOE) is Oracle Solaris 11.4 Build: 11.4 SRU 26.0.1 with IDR 4534 v3. The package version of 'entire' is 11.4-11.4.26.0.1.75.4.

1.3.3 Evaluated Functions

6 The following functions have been evaluated under Common Criteria:

a) **Secure Administration.** The TOE enables secure management of its security functions, including:
   i) User authentication with passwords
   ii) Configurable password policies
   iii) Role Based Access Control
   iv) Management of security functions

b) **Protected Communications.** The TOE protects the integrity and confidentiality of communications as follows:
   i) **SSH.** The TOE implements an SSH server to protect communication with remote users and management servers.
   ii) **TLS.** The TOE includes the capability of implementing TLS clients that use TLS v1.2. to protect communication with a TLS server in its operational environment.

c) **Protected Storage.** The TOE implements storage encryption to protect sensitive data.

d) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates to itself and installed applications through digital signatures.

e) **Security Audit.** The TOE generates logs of security relevant events.

f) **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

g) **Self-Protection.** The TOE implements execution environment-based mitigations:

i) Address Space Layout Randomization

ii) Stack buffer overflow protection using stack canaries

h) **Cryptographic Operations.** The TOE implements cryptographic functions as described in section 3.4.

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

1.3.4 Evaluation Assumptions

8 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.

9

Table 1: Evaluation Assumptions

Assumption	Guidance
A.PLATFORM — The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.	Ensure that the host platform is trustworthy. (i.e. commercially available well-known platforms).
A.PROPER_USER — The user of the OS is not wilfully negligent or hostile and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.	Users will be provided operating guidance, are trusted to follow the provided guidance and operates the OS in compliance with applied enterprise security policy.
A.PROPER_ADMIN — The administrator of the OS is not careless, wilfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.	Ensure that administrators are competent, are able to follow the provided guidance, and will act in compliance with enterprise security policy.

1.4 Conventions

10 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 document and section reference from Table 2. For example:

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

1.5 Related Documents

11 This guide supplements the below documents which are available from the Oracle Solaris 11.4 Information Library https://docs.oracle.com/cd/E37838_01/

Table 2: Related Documents

Reference	Document
[INSTALL]	Manually Installing an Oracle Solaris 11.4 System
[ADMIN]	Introduction to Oracle Solaris 11.4 Administration
[GUIDE]	Guidance documents other than Installation guide or Administrator guide (e.g. Concept Guide, Security Guide, etc.) Configuring and Managing Network Components in Oracle Solaris 11.4 Oracle Solaris 11.4 Security and Hardening Guidelines

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

2 Secure Acceptance and Update

2.1 Obtaining the TOE

13 The TOE is obtained from the Oracle Software Delivery Cloud at https://edelivery.oracle.com

2.2 Verifying the TOE

14 Packages must be checked for signatures when installed. The pkg set-property signature-policy require-signatures command should be used to ensure all packages are signed and verified.

15 The pkg verify -v command is used to validate the software packages in the TOE image. The signatures of each package are validated based on the signature policy for the package publishers.

16 See Verifying boot and Elf Signature for description on verifying the TOE firmware.

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

18 To verify the IDR version use the pkg list -af "idr*" | egrep "i--$" command
Note: the first column is the name of the IDR while the second column is the version number. The ' i 'flag indicates 'installed'. Alternatively, the pkg info idr4534 command can be used to target the specific IDR package required for the CC evaluated configuration.

2.3 Power-on Self-Tests

19 The TOE implements the Verify boot process which includes a series of tests to validate the system hardware and software. For a full description of the power-on self-tests see Verification Sequence during System Boot and Booting and Shutdown Features in Oracle Solaris.

20 For X8 systems, the secure bootloader must be enabled via the bootadm install-bootloader -s command prior to enforcing UEFI Secure Boot mode. See Configure UEFI Secure Boot for more information.

2.4 Updating the TOE

21 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.

22 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.

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

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

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

26 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.

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

28 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.

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

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

2.4.1 Patch Management

31 To maintain a secure state, the TOE must be updated regularly. This should be accomplished through strict adherence to a mature patch management program that addresses all components of the TOE.

32 In addition to scheduled monthly updates from Oracle, the TOE contains third party components that must also be updated regularly. These third-party components may or may not adhere to the scheduled updates released by Oracle, therefore due diligence is required by the Administrator in monitoring for any pertinent update releases that affect the TOE and apply them accordingly.

33 Administrators of the TOE must stay informed of, and reference at least monthly, Oracle's critical patch updates, security alerts, and bulletins located at https://www.oracle.com/security-alerts/

34 A proper patch management strategy is necessary for the TOE and its third-party components to maintain the secure operation and state of the TOE, while ensuring the continued assurance of the TOE security functions.

3 Configuration Guidance

3.1 Installation

35 Follow the instructions of [INSTALL] augmented by the configuration steps in the following sections.

36 To achieve the evaluated configuration, the correct Support Repository Update (SRU) and Interim Diagnostic or Relief (IDR) must be installed. Installation of SRU 26.0.1 with IDR 4534 v3 (idr4534.3) is required to achieve the evaluated configuration. The 'entire' package version should be 11.4-11.4.26.0.1.75.4. See Applying Support Updates and Installing an IDR Custom Software Update and Understanding Oracle Solaris 11 Package Versioning for more information.

3.2 Services Configuration

37 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.

38 **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.

3.2.1 Firewall

39 Use the pfedit /etc/firewall/pf.conf to modify the firewall configuration file and add rules to restrict network traffic.

40 Note: the pf ruleset is not subject to standard auditing functions. To enable auditing of firewall rule changes, a per-file ACL on the rules file must be configured. See Specifying Files or Directories to be Audited for more information.

41 See Preparing to Configure the Oracle Solaris Firewall for additional details.

3.2.2 Domain Name System

42 To configure the DNS client service use the SMF dns/client service to enter the DNS information as follows:

a) Use svccfg -s dns/client setprop config/nameserver=net-address: <IP address>

b) Use svcadm refresh dns/client

c) Enable the dns client with the svcadm enable dns/client command

43 For additional information see Administering DNS.

3.2.3 Remote Management Server

44 The Remote Administration Daemon (RAD) provides programmable interfaces that enable administrators to configure and manage Oracle Solaris system components as described in Remote Administration Daemon.

45 RAD servers can configure and manage Oracle Solaris system components using C, Java, Python or the RAD REST API as described in Connecting to RAD.

46 The rad:remote service is disabled by default since the local RAD daemon is tunnelled through the existing SSH server to provide access.

47 Use of the RAD API must be performed over SSH as described in Connecting in Python to a RAD Instance by Using a URI.

3.2.4 Time Server

48 The TOE supports the use of an NTP server to provide accurate time services, only the authorized administrator can configure the NTP server.

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

50 Use the command cp ntp.client ntp.conf

51 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

52 Use the command svcadm enable ntp

53 Additional information can be found here.

54 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.

3.2.5 TLS Client

55 See section 3.4.2

3.3 Secure Administration

3.3.1 User Interfaces

56 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. The Remote Administration Daemon (RAD) also runs over SSH.

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

58 Remote Administrative sessions (RAD) can be terminated when the connection object is explicitly closed using the close API method, or automatically when the connection object is destroyed (dependent on binding language type).

3.3.2 Admin/User authentication

59 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.

60 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.

61 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).

62 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.

63 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).

3.3.3 Role-Based Access Controls

64 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.

Management Function	Administrator	User
Enable/disable [session timeout]	X	
Configure [session] inactivity timeout	X	
Configure local audit storage capacity	X	
Configure minimum number of lowercase characters in password	X	
Configure minimum password Length	X	
Configure minimum number of special characters in password	X	
Configure minimum number of numeric characters in password	X	
Configure minimum number of uppercase characters in password	X	

Management Function	Administrator	User
Configure lockout policy for unsuccessful authentication attempts through [limiting number of attempts during a time period]	X	
Configure host-based firewall	X	
Configure name/address of directory server with which to bind	X	
Configure name/address of audit/logging server to which to send audit/logging records	X	
Configure audit rules	X	
Configure name/address of network time server	X	

3.3.4 Management of Security Functions

65 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).

3.3.4.1 Authentication Failure

66 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.

3.3.4.2 Session Locking/Termination

67 See Section 3.3.2.

3.3.4.3 Password Management

68 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.

69 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.

3.3.4.4 Setting Time

70 See Section on Time Server above.

3.3.4.5 Access Control – Files & Directories

71 The user file-creation mode mask (umask) is used to assign file permissions for files and folders that have been newly created. See Modifying Login Environment Variables for more information.

72 *Note:* when using the SMF to configure a umask, leading zeros must not be used (eg. To set a umask normally by using 077, simply set as 77 in SMF)

73 The default umask is provided by the svc:/system/account-policy:default service only when the config/etc_default_login/disabled setting (within the account-policy:default service) is set to “FALSE”. Therefore, this service will override the /etc/default/login file.

3.3.4.6 Audit Logging

74 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.

75 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.

76 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.

77 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.

78 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.

79 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”

80 For additional details on audit classes and the auditconfig subcommands see Audit_class and Configuring the Audit Service.

81 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.

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

83 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.

The audit_syslog plugin handles delivery of audit records to the syslog logs. The logs are stored in a location specified in the /etc/syslog.conf file.

The audit_remote plugin sends the binary audit trail to an ARS in the same format as the audit_binfile plugin writes to the local 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

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

85 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.

86 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

87 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.

88 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.

3.3.5 LDOM Management

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

90 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.

3.3.6 Non-Essential Services

91 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)

3.4 Cryptography

92 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.

93 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).

94 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:

95 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.

3.4.1 SSH

96 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-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512

d) Key Exchange Methods — diffie-hellman-group14-sha1

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

97 Password authentication method is supported.

98 RAD clients use SSH to protect communication to a specified server. The users $HOME/.ssh/authorized_keys database is used to manage the public keys used for authentication.

99 SSH host keys must be generated using only RSA 2048, 3072 and ECDSA P-256, P-384, and P-521 curves and must be protected in a ZFS encrypted dataset.

3.4.2 TLS

100 The TOE can provide secure communication with a TLS server, and is capable of implementing a TLS 1.2 client that uses the following cipher suites:

a) TLS_RSA_WITH_AES_128_CBC_SHA

b) TLS_RSA_WITH_AES_256_CBC_SHA

c) TLS_RSA_WITH_AES_128_CBC_SHA256

d) TLS_RSA_WITH_AES_256_CBC_SHA256

e) TLS_RSA_WITH_AES_128_GCM_SHA256

f) TLS_RSA_WITH_AES_256_GCM_SHA384

g) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

h) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

i) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

j) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

101 Reference identifiers can be set using the following:
X509_VERIFY_PARAM_set1_host
X509_VERIFY_PARAM_add1_host
X509_VERIFY_PARAM_set1_ip
X509_VERIFY_PARAM_set1_ip_asc

See X509_VERIFY (3openssl) for more information
For details on the OpenSSL API see 1openssl and 3openssl manpages for more information. Specific details on API calls and exposed structures can be found in the headers located in /usr/include/openssl.

102 All cryptographic parameters are configured by default as part of enabling FIPS mode in the BE. The cryptoadm utility is used to view the cryptographic parameters. . The pktool utility is used to generate and manage public key objects including X509v3 certificates, passwords, and keystores.

3.5 Protected Storage

3.5.1 FCS_STO_EXT.1

103 The /etc/shadow file stores hashed passwords. See Where User Account and Group Information Is Stored for configuration details on how the TOE handles protected user account and group information.

104 Storage pools and specific filesystems can be encrypted using the zfs command. Data is encrypted using AES with key lengths of 128 and 256 in both GCM and CCM operation modes. See Encrypting ZFS File Systems for more information.

105 For greater security, raw AES keys should be stored externally from the TOE, such as on protected removable media or on a remote key management server via KMIP.

4 Annex A: Log Reference

4.1 Format

106 For description of each field in an audit record see Displaying Audit Records Definition. See also Configuring the Format of Audit Records and Where they are stored.

4.2 Events

107 The TOE generates the following log events.

Table 3: Audit Records

Audit Event	Audit Records example
Start-up of the audit functions	header,54,2,audit service started,na,10.19.14.10,2020-10-23 14:04:23.267-07:00,return,success,0,zone,global
Shut-down of the audit functions	file,2020-10-23 14:03:12.000-07:00, header,54,2,audit service terminated,na,10.19.14.10,2020-10-23 14:03:12.524-07:00,return,success,0,zone,global file,2020-10-23 14:03:12.000-07:00,
Authentication Events	
Admin login	header,95,2,login - ssh,,10.19.14.10,2020-10-23 09:01:59.132-07:00,subject,root,root,root,root,root,11142,3232473395,0 0 10.19.14.3,return,success,0,zone,global
Admin logout	header,95,2,logout,,10.19.14.10,2020-10-23 09:01:59.610-07:00,subject,root,root,root,root,root,11142,3232473395,0 0 10.19.14.3,return,success,0,zone,global
User login	header,107,2,login - ssh,,fe80::210:e0ff:febb:b9c2,2020-10-20 13:34:02.212-07:00,subject,user1,user1,staff,user1,staff,4074,1608522511,0 0 10.100.1.3,return,success,0,zone,global
User failed login	header,95,2,login - local,fe,sca15-t82-03,2020-10-08 13:59:16.743-07:00,subject,user1,user1,staff,user1,staff,3990,1403746252,0 0 sca15-t82-03,return,failure,Authentication failed,zone,global

Audit Event	Audit Records example
User logout	header,107,2,logout,,fe80::210:e0ff:febb:b9c2,2020-10-20 13:35:02.292-07:00,subject,user1,user1,staff,user1,staff,4074,1608522511,0 0 10.100.1.3,return,success,0,zone,global
Privilege or Role Escalation Events	
Use of 'su' or 'sudo' command	header,95,2,su,,sca15-t82-03,2020-10-08 14:14:41.292-07:00,subject,user1,user2,staff,user2,staff,4173,3199832535,158 5 10.100.1.130,return,success,0,zone,global … header,148,2,privileged execution,,sca15-t82-03,2020-10-08 14:15:14.097-07:00,path,/usr/bin/su,path,/,exec_args,2,su,user2,use of privilege,successful use of priv,sys_res_config,subject,user1,root,staff,user1,staff,4173,3199832535,158 5 10.100.1.130,return,success,0,zone,global
Use of 'setuid' or 'setgid' command	header,162,2,bind(2),sp,10.19.14.10,2020-10-23 19:13:45.570-07:00,argument,1,0x3,so,socket,0x001a,0x0002,0x0000,2700::,0x0000,::,subject,user1,root,staff,user1,staff,14032,1525041035,158 1 172.16.200.14,use of privilege,successful use of priv,net_privaddr,return,success,0,zone,global
System reboot, restart	header,95,2,reboot(8),,10.19.14.10,2020-10-24 01:54:43.457-04:00,subject,root,root,root,root,root,1370,3823973100,0 0 10.19.14.10,return,success,0,zone,global
System shutdown	header,100,2,init(8),,10.19.14.10,2020-10-24 01:59:19.926-04:00,subject,root,root,root,root,root,1348,1197124405,0 0 10.19.14.10,text,0,return,success,0,zone,global
Kernel module loading (success/ Failure)	header,157,2,modctl(2) - load module,,10.19.14.10,2020-10-23 23:32:28.915-07:00,path,/platform/sun4v/kernel /kernel /usr/kernel,path,/drv/sparcv9/dump,subject,root,root,root,root,root,1450,1700342744,158 1 172.16.200.14,return,success,0,zone,global
	header,165,2,modctl(2) - load module,fp:fe,10.19.14.10,2020-10-23 23:31:45.189-07:00,path,/platform/sun4v/kernel /kernel /usr/kernel,path,/drv/sparcv9/dump,subject,user1,user1,staff,user1,staff,1447,1559527537,158 2 172.16.200.14,use of privilege,failed use of priv,ALL,return,failure: Not owner,-1,zone,global
Kernel module unloading	header,117,2,modctl(2) - unload module,sp,10.19.14.10,2020-10-23 23:30:56.221-07:00,argument,1,0xc4,id,subject,root,root,root,root,root,1444,1700342744,158 1 172.16.200.14,use of privilege,successful use of priv,sys_config,return,success,0,zone,global

Audit Event	Audit Records example
(success/ Failure)	
	header,117,2,modctl(2) - unload module,fp:fe,10.19.14.10,2020-10-24 02:28:07.049-04:00,argument,1,0xc4,id,subject,112,112,staff,112,staff,1440,1559527537,158 2 172.16.200.14,use of privilege,failed use of priv,sys_config,return,failure: Not owner,-1,zone,global
Attempted application invocation with arguments (success/ Failure e.g. due to software restriction policy)	header,175,2,execve(2),,10.19.14.10,2020-10-23 21:53:11.373-07:00,path,/tmp/true,attribute,100555,root,root,16374,737529256,184467440737 09551615,exec_args,5,/tmp/true,these,are,my,arguments,subject,user1,user1,staff,user1,staff,14947,276572979,158 1 172.16.200.14,return,success,0,zone,global
	header,158,2,execve(2),fp:fe,10.19.14.10,2020-10-23 21:57:18.482-07:00,path,/tmp/true,attribute,100444,root,root,16374,737529256,184467440737 09551615,subject,user1,user1,staff,user1,staff,14969,276572979,158 1 172.16.200.14,use of privilege,failed use of priv,file_dac_execute,return,failure: Permission denied,-1,zone,global
Cryptographic verification of software (success/failure)	Operation: install Outcome: Succeeded Reason: None Client: pkg Version: b'3beb69dcf209' User: root (0) … Start Time: 2020-10-24T23:32:52 End Time: 2020-10-24T23:36:43
	Operation: install Outcome: Failed Reason: Unknown Client: pkg Version: b'3beb69dcf209' User: root (0) Boot Env.: 11.4.24.75.2-IDR4534 … Start Time: 2020-10-24T23:30:27

Audit Event	Audit Records example
	End Time: 2020-10-24T23:31:06 … pkg.client.api_errors.RequiredSignaturePolicyException: The policy for solaris requires signatures to be present but no signature was found in pkg://solaris/service/security/stunnel@5.35,11.4-11.4.24.0.1.75.1:20200703T190124Z.
Audit and log data access events (success/failure)	header,181,2,open(2) - read,ace,10.19.14.10,2020-10-30 13:35:27.592-07:00,path,/var/audit/20201027005741.not_terminated.sca15-t82-03,attribute,100640,root,root,259,32,18446744073709551615,subject,root,root,root,root,root,4028,1853536638,158 1 10.100.1.149,return,success,3,zone,global
	header,199,2,open(2) - read,fp:fe,10.19.14.10,2020-10-22 09:40:15.039-07:00,path,/var/audit/20201022021104.20201022021117.sca15-t82-03,attribute,100640,root,root,259,10,18446744073709551615,subject,user1,user1,staff,user1,staff,8575,3215090104,158 2 10.100.1.102,use of privilege,failed use of priv,file_dac_read,return,failure: Permission denied,-1,zone,global
User and Group Management events – add (successful/unsuccessful)	header,218,2,add new user login to the system,,10.19.14.10,2020-10-26 09:56:43.915-07:00,subject,root,root,root,root,root,7640,825136418,0 0 10.19.14.3,text,repository = files,user,115,user4,group,10,staff,text,gecos = ,text,homedir = /export/home/local/user3,text,shell = /usr/bin/bash,return,success,0,zone,global
	header,125,2,add new user login to the system,fe,10.19.14.10,2020-10-28 21:14:53.742-07:00,subject,root,root,root,root,root,3194,494638983,158 1 172.16.200.14,text,repository = files,user,0,,return,failure,Invalid ID,zone,global
User and Group Management events – delete (successful/unsuccessful)	header,131,2,delete user's login from the system,,10.19.14.10,2020-10-28 21:20:35.733-07:00,subject,root,root,root,root,root,3214,494638983,158 1 172.16.200.14,text,repository = files,user,114,user10,return,success,0,zone,global
	header,185,2,delete group from the system,fe,10.19.14.10,2020-10-28 21:59:09.145-07:00,subject,root,root,root,root,root,3331,494638983,158 1 172.16.200.14,text,repository = files,group,101,group10,use of authorization,solaris.group.manage,solaris.group.assign/group10,return,failure,Program failure,zone,global

Audit Event	Audit Records example
User and Group Management events – modify (successful/unsuccessful)	header,152,2,modify user's login information on the system,,10.19.14.10,2020-10-26 10:05:22.966-07:00,subject,root,root,root,root,root,7673,2803366339,158 1 172.16.200.14,text,repository = files,user,0,,text,new audit_flags = no:no,return,success,0,zone,global
	header,125,2,modify user's login information on the system,fe,10.19.14.10,2020-10-28 21:37:09.612-07:00,subject,root,root,staff,user1,staff,3248,494638983,158 1 172.16.200.14,text,repository = files,user,0,,return,failure,authorization failed,zone,global
User and Group Management events – disable (successful/unsuccessful)	header,215,2,lock account,,10.19.14.10,2020-10-26 10:28:01.568-07:00,subject,root,root,sys,root,root,7809,2803366339,158 1 172.16.200.14,text,repository = files,user,113,user2,text,old password status = PS,text,new password status = LK,use of authorization,solaris.account.setpolicy,return,success,0,zone,global
	header,215,2,lock account,fe,10.19.14.10,2020-10-26 10:23:05.549-07:00,subject,user1,root,sys,user1,staff,7744,927587763,158 2 172.16.200.14,text,repository = files,user,113,user2,text,old password status = PS,text,new password status = PS,use of authorization,solaris.account.setpolicy,return,failure,authorization failed,zone,global
User and Group Management events – enable (successful/unsuccessful)	header,215,2,unlock account,,10.19.14.10,2020-10-26 10:28:05.937-07:00,subject,root,root,sys,root,root,7810,2803366339,158 1 172.16.200.14,text,repository = files,user,113,user2,text,old password status = LK,text,new password status = PS,use of authorization,solaris.account.setpolicy,return,success,0,zone,global
	header,215,2,unlock account,fe,10.19.14.10,2020-10-26 10:23:08.022-07:00,subject,user1,root,sys,user1,staff,7745,927587763,158 2 172.16.200.14,text,repository = files,user,113,user2,text,old password status = PS,text,new password status = PS,use of authorization,solaris.account.setpolicy,return,failure,authorization failed,zone,global
User and Group Managem	header,133,2,passwd,,10.19.14.10,2020-10-26 10:28:14.847-07:00,subject,root,root,sys,root,root,7811,2803366339,158 1

Audit Event	Audit Records example
ent events – credential changes (successful/unsuccessful)	172.16.200.14,user,113,user2,use of authorization,solaris.passwd.assign,return,success,0,zone,global
	header,108,2,passwd,fe,10.19.14.10,2020-10-26 10:23:10.605-07:00,subject,user1,root,sys,user1,staff,7746,927587763,158 2 172.16.200.14,user,113,user2,return,failure,Permission denied,zone,global
File and object events (successful/unsuccessful) attempt to - Create	header,187,2,open(2) - write,creat,trunc,,10.19.14.10,2020-10-22 11:01:09.773-07:00,path,/..../var/share/user/112/webui/preferences/solaris.json.lock ,attribute,100600,user1,staff,259,251,18446744073709551615,subject,user1,user1,staff,user1,staff,9105,611625539,0 0 10.19.14.10,return,success,6,zone ,global
File and object events (successful/unsuccessful) attempt to - Access	header,199,2,open(2) - read,fp:fe,10.19.14.10,2020-10-22 09:40:15.039-07:00,path,/var/audit/20201020205257.20201020210151.sca15-t82-03,attribute,100640,root,root,259,8,18446744073709551615,subject,user1,user1,staff,user1,staff,8575,3215090104,158 2 10.100.1.102,use of privilege,failed use of priv,file_dac_read,return,failure: Permission denied,-1,zone,global
File and object events (successful/unsuccessful) attempt to - Delete	header,141,2,unlink(2),,10.19.14.10,2020-10-22 10:48:05.603-07:00,path,/tmp/4ad9rt_1,attribute,100600,user1,staff,16374,720350848,18446744073709551615,subject,user1,user1,staff,user1,staff,9078,1403979187,0 0 10.19.14.10,return,success,0,zone,global
File and object events (successful/unsuccessful) attempt to - Modify	header,169,2,open(2) - write,,fe80::210:e0ff:febb:b9c2,2020-10-20 14:02:26.473-07:00,path,/devices/pseudo/log@0:conslog,attribute,20666,root,sys,16379,61865988,506806140928,subject,user1,root,root,root,root,4335,3762893713,0 0 10.100.1.3,return,success,8,zone,global

Audit Event	Audit Records example
File and object events (successful/unsuccessful) attempt to – Modify permissions	header,184,2,chmod(2),sp,10.19.14.10,2020-10-22 11:05:00.037-07:00,argument,2,0x1c0,new file mode,path,/var/share/user/112,attribute,40700,user1,staff,259,279,18446744073709551615,subject,user1,root,staff,root,staff,9146,727154527,0 0 10.19.14.10,use of privilege,successful use of priv,file_owner,return,success,0,zone,global
Administrator or root-level access events (Success/failure)	*Refer to messages for authentication events and privilege escalation events above for administrative-level roles and accounts such as root.*
Use of Privilege/Special Rights Events	
Enable/disable session timeout	header,160,2,open(2) - write,ace,fe80::210:e0ff:febb:b9c2,2020-10-20 13:11:12.137-07:00,path,/etc/profile.timeout,attribute,100600,root,root,259,3293803,18446744073709551615,subject,root,root,root,root,root,3994,2800923958,158 2 10.100.1.3,return,success,3,zone,global (See Section 3.3.4.6, paragraph 81 for more information)
Configure session inactivity timeout	header,160,2,open(2) - write,ace,fe80::210:e0ff:febb:b9c2,2020-10-20 13:11:12.137-07:00,path,/etc/profile.timeout,attribute,100600,root,root,259,3293803,18446744073709551615,subject,root,root,root,root,root,3994,2800923958,158 2 10.100.1.3,return,success,3,zone,global
Configure local audit storage capacity	header,188,2,privileged execution,,fe80::210:e0ff:febb:b9c2,2020-10-20 13:58:45.830-07:00,path,/usr/sbin/zfs,path,/var/audit,exec_args,4,zfs,set,quota=10K,rpool/audit,use of privilege,successful use of priv,sys_config,subject,root,root,root,root,root,4233,2800923958,158 2 10.100.1.3,return,success,0,zone,global
Configure minimum password length	header,223,2,create service instance property,,fe80::210:e0ff:febb:b9c2,2020-10-21 11:16:11.412-07:00,subject,root,root,root,root,root,4606,28903747,158 1 10.100.1.189,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/password/complexity/passlength,text,c,text,"15",return,success,0,zone,global

Audit Event	Audit Records example
Configure minimum number of special characters in password	header,223,2,create service instance property,,fe80::210:e0ff:febb:b9c2,2020-10-21 12:15:48.424-07:00,subject,root,root,root,root,root,4720,28903747,158 1 10.100.1.189,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/password/complexity/min_special,text,c,text,"2",return,success,0,zone,global
Configure minimum number of numeric characters in password	header,221,2,create service instance property,,fe80::210:e0ff:febb:b9c2,2020-10-21 12:25:24.938-07:00,subject,root,root,root,root,root,4758,28903747,158 1 10.100.1.189,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/password/complexity/min_digit,text,c,text,"2",return,success,0,zone,global
Configure minimum number of uppercase characters in password	header,221,2,create service instance property,,fe80::210:e0ff:febb:b9c2,2020-10-21 12:35:14.938-07:00,subject,root,root,root,root,root,4784,28903747,158 1 10.100.1.189,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/password/complexity/min_upper,text,c,text,"2",return,success,0,zone,global
Configure minimum number of lowercase characters in password	header,221,2,create service instance property,,fe80::210:e0ff:febb:b9c2,2020-10-21 12:46:49.463-07:00,subject,root,root,root,root,root,4807,28903747,158 1 10.100.1.189,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/password/complexity/min_lower,text,c,text,"2",return,success,0,zone,global
Configure lockout policy for unsuccessful authentication attempts through [limiting number of attempts during a time period]	header,200,2,change service instance property,,sca15-t82-03,2020-10-08 13:54:07.521-07:00,subject,root,root,root,root,root,3897,18709946,158 2 10.100.1.130,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/login_policy/retries,text,c,text,"5",return,success,0,zone,global header,213,2,change service instance property,,sca15-t82-03,2020-10-08 13:54:14.522-07:00,subject,root,root,root,root,root,3898,18709946,158 2 10.100.1.130,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/login_policy/lock_after_retries,text,s,text,"yes",return,success,0,zone,global header,210,2,create service instance property,,sca15-t82-03,2020-10-08 14:28:29.304-07:00,subject,root,root,root,root,root,4260,18709946,158 2 10.100.1.130,use of authorization,solaris.smf.modify,fmri,svc:/system/account-policy:default/:properties/login_policy/auto_unlock_time,text,s,text,"1m",return,success,0,zone,global
Configure host-	header,190,2,persistently enable service instance,,fe80::210:e0ff:febb:b9c2,2020-10-21 13:26:18.676-07:00,subject,root,root,root,root,root,4977,3779883095,158 5

Audit Event	Audit Records example
based firewall	10.100.1.189,use of authorization,solaris.smf.modify,fmri,svc:/network/firewall:default/:properties/general/enabled,return,success,0,zone,global header,209,2,change service instance property,,10.19.14.10,2020-10-23 12:18:01.751-07:00,subject,root,root,root,root,root,12272,932677216,0 0 10.19.14.3,use of authorization,solaris.smf.modify,fmri,svc:/network/firewall:default/:properties/firewall/rules,text,s,text,"/etc/firewall/pf.conf",return,success,0,zone,global header,200,2,refresh service instance,,fe80::210:e0ff:febb:b9c2,2020-10-21 13:26:18.684-07:00,subject,root,root,root,root,root,4978,3779883095,158 5 10.100.1.189,use of authorization,solaris.smf.modify,fmri,svc:/network/firewall:default/:properties/restarter_actions/refresh,return,success,0,zone,global
Configure audit rules	header,196,2,change service instance property,,10.19.14.10,2020-10-22 10:04:16.984-07:00,subject,root,root,root,root,root,8814,2481428998,158 1 10.100.1.102,use of authorization,solaris.smf.modify,fmri,svc:/system/auditd:default/:properties/preselection/flags,text,s,text,"cusa,fd",return,success,0,zone,global header,155,2,auditon(2) - set default user preselection mask,sp,10.19.14.10,2020-10-22 10:04:16.984-07:00,argument,2,0x2000750a0,as_success,argument,2,0x2000750a0,as_failure,subject,root,root,root,root,root,8814,2481428998,158 1 10.100.1.102,use of privilege,successful use of priv,sys_audit,return,success,21,zone,global header,198,2,change service instance property,,10.19.14.10,2020-10-22 10:04:21.063-07:00,subject,root,root,root,root,root,8815,2481428998,158 1 10.100.1.102,use of authorization,solaris.smf.modify,fmri,svc:/system/auditd:default/:properties/preselection/naflags,text,s,text,"cusa,fd",return,success,0,zone,global header,155,2,auditon(2) - set kernel mask,sp,10.19.14.10,2020-10-22 10:04:21.063-07:00,argument,2,0x2000750a0,as_success,argument,2,0x2000750a0,as_failure,subject,root,root,root,root,root,8815,2481428998,158 1 10.100.1.102,use of privilege,successful use of priv,sys_audit,return,success,4,zone,global
Configure name/address of network time server	header,121,2,open(2) - write,creat,trunc,fp:fe,10.19.14.10,2020-10-22 10:37:05.017-07:00,path,/etc/inet/ntp.conf,subject,user1,user1,staff,user1,staff,9065,3295230268,158 1 10.100.1.102,use of privilege,failed use of priv,ALL,return,failure: Permission denied,-1,zone,global

Audit Event	Audit Records example
Configure name/address of directory server with which to bind	header,182,2,privileged execution,,10.19.14.10,2020-10-22 09:28:08.746-07:00,path,/usr/sbin/ldapclient,path,/root,exec_args,3,ldapclient,mod,10.19.14.3,use of privilege,successful use of priv,file_dac_write,subject,root,root,root,root,root,8310,1979871805,0 0 10.19.14.10,return,success,0,zone,ldapclient
Configure name/address of audit/logging server to which to send audit/logging records	header,201,2,change service instance property,,10.19.14.10,2020-10-22 09:52:12.675-07:00,subject,root,root,root,root,root,8778,3147870781,158 2 10.100.1.102,use of authorization,solaris.smf.modify,fmri,svc:/system/auditd:default/:properties/audit_remote/p_hosts,text,s,text,"10.19.14.2",return,success,0,zone,global