NETSCOUT®

TestStream Management Software v5.3.0 on nGenius 3900 Series Switches

Common Criteria Guide

Version 1.3

April 2023

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Description
1.0	16 Feb 2023	Release for Certification
1.1	1 Mar 2023	Certification updates
1.2	31 Mar 2023	Address CB OR
1.3	14 Apr 2023	Address CB Comments

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 TestStream Management Software v5.3.0 on nGenius 3900 Series Switches with build 5.3.0.54 and related information.

2 This document has been developed as part of the NETSCOUT TestStream Management Software Common Criteria (CC) documentation suite. The scope of the security functions under evaluation is defined in the Security Target (ST) (Ref. [ST])

1.2 Audience

3 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

4 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

5 The Common Criteria evaluation was performed against the requirements of the Network Device collaborative Protection Profile (NDcPP) v2.2e available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Software and Hardware

6 The physical boundary of the TOE includes the NETSCOUT TestStream Management Software v5.3.0 on nGenius 3900 Series Switches as identified in [ST] sections 1.2 Table 1 and 2.4 Table 5.

7 NETSCOUT 3900 series switches includes a switch chassis and blade combination. The switch chassis component houses the blades and provides power. The blades run the TOE software and provide management and networking interfaces and services. In a multi-blade configuration, only one blade can assume the role of the active controller. The active controller manages all other blades in the switch.

1.3.3 Evaluated Functions

8 The following functions have been evaluated under Common Criteria:

a) **Protected Communications.** The TOE protects the integrity and confidentiality of communications as noted in [ST] section 2.2.

b) **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

vi) Protection of cryptographic keys and passwords

c) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates through published hashes.

d) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

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

f) **Cryptographic Operations.** The TOE implements a cryptographic module. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in [ST] Table 4.

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 Table 1 below should be followed to uphold these assumptions in the operational environment.

Table 1: Environment & Assumptions

Objective/Assumption	Guidance
A.PHYSICAL_ PROTECTION	Deploy TestStream and the nGenius switches in a physically secure environment with controlled access, such as a server room or data centre facility.
A.LIMITED_ FUNCTIONALITY	Ensure that the TOE only provides networking functionality as per its core function as outlined in [ST] and is not configured to provide other computing services or general purpose applications which are outside the scope of this document.
A.NO_THRU_ TRAFFIC_ PROTECTION	Ensure that traffic originating from, or destined to the TOE itself such as administrative traffic and audit data is protected by using secure protocols that leverage encryption and other secure mechanisms of operation.
A.TRUSTED_ ADMINISTRATOR	Ensure that administrators are trustworthy and competent by implementing background checks or similar vetting procedures, and providing any relevant or appropriate training.
A.REGULAR_ UPDATES	Ensure all relevant updates pertaining to the security and critical functionality of the TOE are applied in a timely and controlled fashion.
A.ADMIN_ CREDENTIALS_ SECURE	Ensure that any passwords or private keys used for the management or administration of the TOE are adequately protected or otherwise secured from theft and unauthorized access on the platform in which they are stored.

Objective/Assumption	Guidance
A.RESIDUAL_ INFORMATION	Ensure that any storage devices used by the TOE which may contain sensitive residual information are properly purged, destroyed, or otherwise protected from unauthorized access.

1.3.5 Exclusions

11 Only those functions identified in section 1.3.3 have been evaluated. No other claims regarding functionality of the TOE have been made and are otherwise outside the scope of this evaluation.

12 The management features to modify and monitor the layer 1 fabric with applications in test labs, customer support labs, and other environments are outside of the scope of the evaluated security functions.

13 Logging in using the 'root' account is not allowed in the evaluated configuration.

1.4 Conventions

14 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

15 Table 2 lists the relevant reference documents which are available with this CC Guide.

Table 2: Related Documents

Reference	Document
[ST]	NETSCOUT TestStream Management Software 5.3.0 Security Target, v1.3
[ADMIN]	NETSCOUT TestStream Management Software 5.3.0 Administrator Guide, 733-1696 Rev. A

Reference	Document
[ADDENDUM]	NETSCOUT TestStream Management Software 5.3.0 Common Criteria Addendum Rev 4.10

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

2 Secure Acceptance and Update

2.1 Obtaining the TOE

17 The TOE appliance will be delivered via commercial courier. The following checks should be performed upon receipt. If any of the checks fail, the device should be returned to NETSCOUT.

a) Verify the correct device has been delivered by checking that information on all packing slips, labels, and paperwork match.

b) Inspect all packaging to confirm there are no signs of physical tampering, or damage caused while in transit.

18 Follow instructions at [ADMIN] *Updating TestStream Management Servers* and *Updating nGenius 3900 Series Switches* to obtain the TOE software or update to the current version.

2.2 Verifying the TOE

19 Follow instructions at [ADMIN] *About TestStream Management* to verify the current version of software installed on the TOE.

20 The TOE software is verified by means of a published hash as follows:

a) Download the installation package and SHA256 file from the MasterCare Portal

b) Compute a sha256 checksum of the installation package using the linux or windows commandline and confirm it matches the checksum contained in the downloaded SHA256 file.

21 Detailed instructions on the TOE verification procedures can be found in [ADMIN] *Downloading and Verifying the Upgrade/Installation Package* section.

2.3 Power-on Self-Tests

22 The TOE performs the following self-tests on startup to ensure the correct operation of cryptographic functions, CPU, BIOS, and firmware integrity:

a) Firmware integrity

b) Known answer tests

c) CPU and BIOS self tests

23 A failure of any of the above tests will result in the TOE not completing the boot up process. LED lights on the front of the device indicate an error state. Results of other self tests can be viewed in the log files.

2.4 Updating the TOE

24 Follow instructions at [ADMIN] *Updating TestStream Management Servers* and *Updating nGenius 3900 Series Switches* to update the TOE. Verification of the authenticity and integrity of the TOE software must be conducted prior to installation per the instructions above in section 2.2.

3 Configuration Guidance

25 This section contains the detailed configuration steps necessary to achieve the evaluated configuration. All steps in this section must be performed on the TOE to meet the requirements of this evaluation and the evaluated configuration.

26 A checklist outlining these configuration steps in order of execution can be found in *Annex A: Evaluated Configuration Checklist*.

3.1 Administration Interfaces

27 Only the following administration interfaces may be used:

a) **CLI / Console.** Directly connected via Rollover Console cable.

  i) Detailed usage steps can be found in [ADMIN] *CLI Access using an nGenius 3900 Series Blade Console Port* section.

b) **CLI / SSH (TestStream).** Remote access to the TestStream CLI interface via SSH for administration of TestStream features and functions.

  i) This interface is disabled by default and must first be enabled.

  ii) This interface only accepts TestStream CLI commands.

c) **CLI / SSH (Linux).** Remote access to the Linux CLI interface via SSH for management of the TOE security functions. This interface accepts normal Linux shell commands.

d) **GUI / HTTP(S).** Management client that can be started via a web page hosted by the TOE or via TestStream Launcher client application. The client application is available on the NETSCOUT support portal.

  i) Note: HTTPS is disabled by default.

  ii) Note: The client TLS/SSL Component must be installed before accessing the TOE via https. This component is available via the WebUI page, or the TestStream launcher application.

e) **REST API / HTTPS.** Provides programmatic access for administration of TestStream functionality.

  i) Note: This interface is disabled by default and is not required to manage the security functionality of the TOE.

3.2 Remote Access Configuration

28 The following administrative interfaces are disabled by default and must be manually enabled by an administrator:

a) **TestStream CLI (SSH)**

  i) Log in to the TestStream Controller via web page or launcher app and navigate to **Tools** > **Configure** > **Remote Access > CLI Access** and check the ‘***Enable SSH Port’*** box (default port is 22022). Click **OK.** Port 22022 should now be open.

ii) Check the ‘***Terminate if idle time exceeds’*** box and enter a time value in minutes.

iii) Detailed usage steps can be found in [ADMIN] sections *SSH Access Support on TestStream Management* and *CLI Access – SSH.*

b) **GUI (HTTPS)**

i) Log in to the TestStream Controller via web page or launcher app and navigate to **Tools** > **Configure** > **Remote Access > Web Access** and check the ‘***Enable HTTPS Port’*** box (default port is 443). Click **OK.** Port 443 should now be open and GUI accessible.

ii) Check the ‘***Terminate if idle time exceeds’*** box and enter a time value in minutes.

iii) The GUI can also connect to the sever via the Java applet using TLS. Log in to the TestStream Controller via the web page or launcher app and navigate to **Tools > Configure > Remote Access > Web Access** and check the ‘***Enable Client TLS***’ box. Click ‘**OK**’.

iv) Detailed usage steps can be found in [ADMIN] section *Installing and Starting the TestStream Management Client.*

c) **REST API**

i) Log in to the TestStream Controller via web page or launcher app and navigate to **Tools** > **Configure** > **Remote Access > REST API Access** and check the ‘***Enable HTTPS Port’*** box (default port is 8443). Click **OK.** Port 8443 should now be open.

ii) Check the ‘***Terminate if idle time exceeds’*** box and enter a time value in minutes.

iii) Detailed usage steps can be found in [ADMIN] section *NETSCOUT TestStream Rest API.*

d) **Linux CLI (SSH).**

i) The idle timeout interval for the Linux shell interface on port 22 can be configured via the ‘LINUX_SHELL_IDLE_TIMEOUT’ line in the ‘/etc/teststream/teststream.conf’ file.

29 The following administrative interfaces are enabled by default and must be manually disabled by an administrator by logging in to the TestStream Controller via the web page or launcher app, navigating to **Tools > Configure > Remote Access > Web Access** and unchecking the following:

a) TestStream CLI via telnet (TCP port 53058)

b) Management WebUI via HTTP (TCP port 80)

3.3 Installation

30 Follow the instructions described in section 2.2 above, which are augmented by the configuration steps in the following sections.

31 Detailed information regarding steps for the sections below can be found in [ADDENDUM].

32 All steps in this document are to be executed as the Linux ‘tsadmin’ user over SSH/port 22 unless otherwise stated or implied in the step instructions.

3.3.1 Installing a Blade

33 Blades installed into slots 1 and 2 are controllers. Only one blade can assume the role of the active controller and the other takes the role of standby controller. The active controller manages all other blades in the switch including the standby controller.

34 When installing a blade, the following steps are recommended:

a) Verify hostname.

  i) It is recommended that all blades in the same switch use the same hostname. To set or change the hostname, see section 3.3.1.1

b) Verify FIPS is enabled.

  i) To enable FIPS, see section 3.3.1.3

3.3.1.1 Set the Hostname

35 To set the hostname, use the script ts-hostname.sh. To verify the hostname, run the Linux command ‘***hostname***’at the shell prompt.

36 See [ADDENDUM] section ‘*Set the Hostname’* for detailed instructions.

3.3.1.2 Verify FIPS is Enabled

37 To verify that FIPS is enabled, use the *ts-security-mode.sh* script with the ‘ *-s* ‘ option. The console output will indicate either *‘Security mode is disabled’* or ‘*Security mode is enabled’*

38 See [ADDENDUM] section ‘*Verify FIPS is enabled’* for detailed instructions.

3.3.1.3 Enable FIPS Mode

39 To enable FIPS mode, stop the TestStream SW with the *sudo /HorizON/shutdown.sh* command and then use the *ts-security-mode.sh* script with the ‘ *-e* ‘ option. When enabling security mode, the following changes are made:

a) Bootloader is updated to pass the fips=1 argument to the kernel

b) Users ‘root’ and ‘onpath’ passwords are reset. See section 3.5 for more information.

c) SSH root login is disabled.

40 After executing the *ts-security-mode.sh* script the blade must be rebooted via the ‘`sudo shutdown –r now’` command.

41 See [ADDENDUM] section ‘*Enable FIPS’* for detailed instructions. Refer to Section 3.3.1.2 for steps on verifying FIPS mode is enabled.

3.4 Cryptography

42 Enable FIPS mode is enabled per instructions in section 3.3.1.3.

3.5 Default Passwords

43 The TOE is initially configured with default password values. The administrator shall change these default values where applicable to comply with standard security best practices and conform to the evaluated configuration. Failure to change these default values puts the security of the TOE at risk and violates the evaluated configuration.

44 The following passwords have default values that shall be changed by the administrator:

a) **Administrator.** Default TestStream management account. See [ADMIN] section *SSH Access Support on TestStream Management* for more information.

b) **Tsadmin.** Account for most maintenance and management activities. See [ADMIN] section *SSH Access Support on TestStream Management* for more information. The *'./ts-linux-password-update.sh'* script can be used to change the password of tsadmin.

c) **Root.** Account for system maintenance. See [ADMIN] section *SSH Access Support on TestStream Management* for more information
Note: SSH root login is disabled when FIPS mode is enabled.

d) **Onpath.** Account for communications between the Java Client and the TestStream server and cannot be interactively logged into.

45 Instructions for resetting 'root' user passwords can be found in [ADMIN] section *Changing SSH System Access Passwords.*

3.6 Administrator Authentication

46 Complex passwords must be enabled per [ADMIN] Section '*Change Security Policy'* and shall:

a) Contain at least one lowercase character;

b) Contain at least one uppercase character;

c) Contain at least one digit; and

d) Contain at least one special character (from those listed below).

47 The minimum length for administrator passwords is configurable to between 1 and 30 case sensitive characters and include only the following special characters: @ # $ % ^ & + = _ ! * - .

48 The maximum length for administrator passwords is 95 characters.

49 Instructions for configuring the lockout threshold for unsuccessful login attempts can be found in [ADMIN] section '*User Accounts'* subsection '*Change Security Policy'.*

50 More information on unlocking user accounts and resetting passwords can also be found in [ADMIN] section '*User Accounts'.*

51 Unlocking user accounts via the TestStream CLI can be achieved by using the '*reset password <user>'* command.

3.6.1 Account Lockout

52 Failed authentication attempt thresholds can be configured by logging into the TestStream controller and navigating to **Tools** > **User Accounts** > **Security Policy**

and entering the desired threshold in the "***Invalid Password Threshold***" section. Click 'Save'.

3.7 Setting Time

53 The use of NTP is not claimed and has not been evaluated. The setting of time on the TOE can been accomplished by following instructions in [ADMIN] section Set Server Date/Time.

54 Audit logs should show the correct timestamp data and running the 'date' command should return the current date and time.

3.8 Audit Log Offloading

55 By default, logs are stored locally on the TOE. 'Log-audit' is a package for securely offloading audit logs to a syslog endpoint in compliance with Common Criteria requirements.

56 Syslog traffic is transmitted by the TOE over an SSHv2 connection to the syslog endpoint and supports ECDSA public keys, and AES 128 and 256 bit encryption.

57 To properly configure syslog offloading, you will need a system running TestStream 5.2.0 or later and a Centos 7 machine to collect the logs, referred to hereafter as the "syslog collector". There may be other platforms that these scripts work on, but these instructions were only tested on CentOS 7. It should be verified that the 'openssh' version on the syslog collector is version 7.4 (2017) or later and rsyslogd is installed.

58 Detailed instructions on configuring syslog remote log offloading, security parameters for the SSHv2 tunnel, and specific requirements for the syslog collector itself per the steps below can be found in [ADDENDUM] section *'Log Offloading'*. Additional information on log offloading functionality can be found in Section 3.8 subsections, and [ST] Section 6.1.3.

3.8.1 TestStream Server Setup

59 Refer to [ADDENDUM] section *'Log Offloading'* for the location of the directory containing the files required for setup, as well as detailed steps for the following:

a) Set the hostname for the TestStream server. See section 3.8.1.1

b) Install the *ts-audit-tunnel* service. See section 3.8.1.2 Service Setup

c) Generate the audit tunnel keys. See section 3.8.1.3 Audit Tunnel Keys

d) Setup the syslog collector. See section 3.8.2 Syslog Collector Setup

e) After setting up the syslog collector, configure the log audit forwarding parameters. See section 3.8.2.1 Forwarding Parameters Setup

f) In the TestStream GUI, enable syslog forwarding to IP address **127.0.0.1** port **514** (do not enable TLS) using facility **'local7'**.

3.8.1.1 Set Hostname

60 Set the hostname for the TestStream server. It is recommended to use the switch name (for embedded servers). See section 3.3.1.1 for detailed steps.

3.8.1.2 Service Setup

61 To install the log offloading service, use the *ts-audit-tunnel-service-setup.sh* script with the '*-i* ' option. Optionally, use the option *'-r '* to update the standby server/controller.

62 The service can be manually restarted by using the following command: '*sudo /etc/init.d/ts-audit-tunnel restart'*

63 See [ADDENDUM] section '*Service Setup'* for detailed instructions.

3.8.1.3 Audit Tunnel Keys

64 Security keys must be generated for use by the audit tunnel service in order to protect the syslog traffic in transit. To generate security keys for the audit tunnel service, use the script *ts-audit-tunnel-keys.sh*.

65 See [ADDENDUM] section '*Audit Tunnel Keys'* for detailed instructions.

3.8.2 Syslog Collector Setup

66 Refer to [ADDENDUM] section '*Syslog Collector Setup'* for detailed instructions.

3.8.2.1 Forwarding Parameters Setup

67 To configure the audit tunnel service, use the script *ts-audit-tunnel-config.sh.*

68 See [ADDENDUM] section '*Forwarding Parameters Setup'* for detailed instructions.

3.9 Certificate Store

69 The certificate store handles certificate authority certificates and user certificates (leaf certificates). Once a CA or user (leaf) certificate is installed, the OCSP configuration must be updated.

70 Certificate validation is performed when certificates such as CA's and device-level certificates are loaded into the TOE. All certificates imported onto the TOE are validated against several characteristics. The SAN IP.1 field must contain an IP address parameter. For server certificates, 'serverAuth' must be present in the extendedKeyUsage extension.

71 See [ST] section 6.3.6 for more detailed information.

3.9.1 Certificate Authority

3.9.1.1 Install Certificate

72 To install a CA certificate, use the *./ts-certificate-ca-install.sh* script.

73 See [ADDENDUM] section '*Install Certificate'* for detailed instructions.

3.9.1.2 List Certificates

74 To list the installed CA certificates, use the *./ts-certificate-ca-list.sh* script.

75 See [ADDENDUM] section '*List Certificates*' for detailed instructions.

3.9.1.3 Remove Certificates

76 To Remove an installed CA certificate, use the *./ts-certificate-ca-remove.sh* script. The filename of the CA certificate to be remove must be passed as an argument.

77 See [ADDENDUM] section ‘*Remove Certificate’* for detailed instructions.

3.9.2 User Certificates

3.9.2.1 Generate Self-Signed Certificates

78 To generate a user or leaf certificate, use the ./ts-certificate-user-generate.sh script.

79 Create a copy of the file ts_cert.conf.sample and customize it for the desired values and use with the ‘-f ‘ option.

80 See [ADDENDUM] section ‘*Generate Self-signed Certificate’* for detailed instructions.

3.9.2.2 Generate a Certificate Signing Request

81 To generate certificate signing requests, use the *./ts-certificate-use-csr.sh* script.

82 Create a copy of the file ts_cert.conf.sample and customize it for the desired values and use with the ‘-f ‘ option.

83 See [ADDENDUM] section ‘*Generate a Certificate Signing Request’* for detailed instructions.

3.9.2.3 Install User Certificate

84 Once a user certificate is generated, install it using the *./ts-certificate-user-install.sh* script. Besides specifying the private key file and the certificate file, the service must be specified too. In a TestStream system, the following services need certificates:

a) httpd

b) stunnel

85 See [ADDENDUM] section ‘*Install Certificate’* for detailed instructions.

Note: For changes to stunnel certificates to take place, the blade must be rebooted. Instructions on rebooting the blade can be found in [ADMIN] Appendix A.

3.9.2.4 Display Certificates

86 To display the X509 certificate, use the *./ts-certificate-user-display.sh* script. This script displays the X509 fields of all the certificates that belong to the certificate chain ordered from issuer(s) down to leaf certificates.

87 See [ADDENDUM] section ‘*Display Certificates’* for detailed instructions.

3.9.2.5 Sample Cert Configuration File

88 Contents of the sample certificate configuration file can be found in [ADDENDUM] section *‘Sample Cert Configuration File’.*

3.10 OCSP Service

89 All certificate revocation checking is performed via OCSP. Intermediate CA and leaf certificates are checked at load time and then hourly following successful loading. More detailed information can be found in [ST] section 6.3.6.

3.10.1 OCSP Service Installation

90 To install the OCSP service, use the *./ts-ocsp-service-setup.sh* script with the *‘-i ‘* option.

91 See [ADDENDUM] section ‘*OCSP Service Installation’* for detailed instructions.

3.10.2 OCSP Service Configuration

92 To configure the OCSP service, use the *./ts-ocsp-config.sh* script.

93 See [ADDENDUM] section ‘*OCSP Service Configuration’* for detailed instructions.

3.10.3 OCSP Status

94 To check the OCSP service and certificate status, use the *./ts-ocsp-status.sh* script.

95 See [ADDENDUM] section ‘*OCSP Status’* for detailed instructions.

3.10.4 OCSP On Demand Check

96 To check the validity of a certificate using OCSP, use the *./ts-ocsp.sh* script with the *‘-o ‘* option.

97 See [ADDENDUM] section ‘*OCSP On Demand Check’* for detailed instructions.

3.11 SSH Utilities

98 The SSH Daemon provides access to many features and configurations on the TOE. For a list of configurable features, refer to [ADDENDUM] section *‘Utilities’*.

3.11.1 Public Key Authentication

99 The TOE supports public key authentication via the Linux SSH/CLI interface. Authorized user public keys can be managed as the ‘tsadmin’ user by using the ‘*ts-sshd-authorized-keys.sh [options(-u <username> -a <key>)]’* script.

3.11.2 Banner Configuration

100 The banner displayed by the SSH interface can be modified by the ‘tsadmin’ user using the ‘*ts-ssh-edit-banner.sh’* script.

101 See [ADDENDUM] section *‘SSH Daemon Banner’* for detailed instructions.

4 Annex A: Evaluated Configuration Checklist

102 The following configuration tasks must be performed on the TOE to achieve the evaluated configuration:

a) **Obtaining and Verifying the TOE.**

   i) When obtaining the TOE, all steps described in Section 2.1 shall be performed to ensure the secure acceptance and receipt of the TOE by the customer.

   ii) All self-tests described in Section 2.3 are performed by the TOE during the startup process which shall be observed by the administrator to ensure no errors or failures occur.

   iii) Next, all steps described in Section 2.2 shall be followed to ensure the correct software versions are downloaded and/or installed.

b) **Configure Remote Access.**

   i) All steps for each interface described in Section 3.2 shall be performed to ensure availability of secure connections.

c) **Configure Hostname.**

   i) All steps in Section 3.3.1.1 shall be performed to ensure a unique and meaningful hostname is configured on the TOE.

d) **Enable FIPS Mode.**

   i) All steps in Section 3.3.1.3 shall be performed to ensure the TOE is correctly operating in FIPS mode.

e) **Change Default Passwords.**

   i) All default passwords described in Section 3.5 shall be changed to ensure unique passwords are configured for administrative interfaces.

f) **Configure Complex Passwords.**

   i) All steps in Section 3.6 shall be performed to ensure strong passwords are required to secure administrative interfaces.

g) **Configure Time.**

   i) All steps in Section 3.7 shall be performed to ensure the correct time is configured for accurate time related functions.

h) **Configure Log Offloading.**

   i) All steps in Section 3.8.1.2 shall be performed to ensure the log offloading service is installed and enabled.

   ii) All steps in Section 3.8.1.3 shall be performed to ensure that keys are generated for the audit tunnel/log offloading service.

i) **Configure Syslog Collector.**

   i) All steps in Section 3.8.2 shall be performed to ensure audit records are received by the remote audit log collector.

   ii) All steps in Section 3.8.2.1 shall be performed to ensure forwarding parameters for the audit tunnel are configured properly.

   iii) Audit logs should now be received by the remote audit log collector.

j) **Configure Certificates.**

   i) All steps in Section 3.9.1.1 shall be performed to ensure certificates are installed correctly.

   ii) All steps in Section 3.9.2.2 shall be performed to ensure certificate signing requests are generated correctly.

   iii) All steps in Section 3.9.2.3 shall be performed to ensure user certificates are installed correctly.

   iv) Installed certificates can be viewed by performing the steps listed in Section 3.9.2.4.

k) **Configure OCSP.**

   i) All steps in Section 3.10.1 shall be performed to ensure the OCSP service is correctly installed.

   ii) All steps in Section 3.10.2 shall be performed to ensure the OCSP service is correctly configured.

   iii) All steps in Section 3.10.3 shall be performed to ensure the OCSP service status is nominal.

l) **Configure SSH Utilities.**

   i) All steps in Section 3.11.1 shall be performed to ensure authorized user public keys are configured.

   ii) All steps in Section 3.11.2 shall be performed to ensure a unique and meaningful banner message is displayed at SSH login.

5 Annex B: Log Reference

5.1 Format

103 Each audit record includes the following fields:

a) Date/Timestamp

b) Event type

c) Subject identity

d) Event outcome (success/failure)

5.2 Events

104 The TOE generates the following log events.

Table 3: Audit Events

Requirement	Auditable Events	Additional Audit Record Contents	Log
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	Apr 17 21:47:41 HorizON : 09:47:41PM 04/17/21 HorizON: [TS][SSH] USER1 Logon Logon failed 3 time! Account has been locked. IP [172.16.200.38]
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	06:07:16PM 03/30/21 SSH testadmin Logon Successful logon from IP [10.100.1.168], Id [2]
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	06:08:28PM 03/30/21 SSH TESTADMIN Logon Local logon failed! Invalid UserId/Password, IP [10.100.1.168]
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.	Jan 14 21:29:02 HorizON sudo: root : TTY=unknown ; PWD=/mnt/app1/HorizON_5.2.0.38/SystemFiles ; USER=root ; COMMAND=/mnt/app1/HorizON_5.2.0.38/SystemFiles//update_fpga.py -f /mnt/app1/HorizON_5.2.0.38/SystemFiles//fpga_db.txt
FMT_SMF.1	All management activities of TSF data.	None.	Apr 9 23:14:10 HorizON: 11:14:10PM 04/09/21 HorizON: [TS][API] administrator Revise System Parameters Client enabled TLS: FALSE => TRUE

Requirement	Auditable Events	Additional Audit Record Contents	Log
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	Jan 14 21:29:02 HorizON update_flash.py: 291 INFO: Flash upgrade successful. Jan 14 21:30:26 HorizON logger: [TS] INFO: System updated - snmp 5.7.3
FPT_STM_EXT.1	Discontinuous changes to time- either Administrator actuated or changed via an automated process.(Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	10:25:19PM 03/26/21 API administrator Set Server Date/Time Server date and time set to 22:25:19 03/26/2021
FTA_SSL_EXT.1(if "lock the session" is selected)	Any attempts at unlocking of an interactive session.	None.	n/a – Not selected
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.	05:25:30PM 03/29/21 SYSTEM SysAdm Terminate SERIAL Session Session for user "administrator" on 127.0.0.1, Id [3], terminated due to inactivity > 1 minutes.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	05:50:20PM 03/29/21 SYSTEM SysAdm Terminate SSH Session Session for user "administrator" on 10.100.1.168, Id [3], terminated due to inactivity > 1 minutes.
FTA_SSL.4	The termination of an interactive session.	None.	05:54:13PM 03/29/21 SYSTEM SysAdm Logoff administrator is now logged off.

Requirement	Auditable Events	Additional Audit Record Contents	Log
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	04:01:09AM 04/14/21 HorizON: [TS] (root:ts-audit-tunnel-config.sh) ts-audit-tunnel started successfully. Connection status: Connected to 10.100.1.168
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.	Apr 14 03:30:11 HorizON: 03:30:11AM 04/14/21 HorizON: [TS][SSH] administrator Logon Successful logon from IP [10.100.1.168], Id [6]
FCS_HTTPS_EXT.1	Failure to establish a HTTPS session.	Reason for failure.	2022-11-01T17:57:23-04:00 HorizoN httpd(rest): [Tue Nov 01 17:57:23.251988 2022] [ssl:info] [pid 9305] [client 10.100.1.205:49038] AH01964: Connection to child 1 established (server localhost.localdomain:8443) 2022-11-01T17:57:23-04:00 HorizoN httpd(rest): [Tue Nov 01 17:57:23.252333 2022] [ssl:debug] [pid 9305] ssl_engine_kernel.c(2427): [client 10.100.1.205:49038] AH02645: Server name not provided via TLS extension (using default/first virtual host) 2022-11-01T17:57:23-04:00 HorizoN httpd(rest): [Tue Nov 01 17:57:23.252548 2022] [ssl:info] [pid 9305] [client 10.100.1.205:49038] AH02008: SSL library error 1 in handshake (server localhost.localdomain:8443) 2022-11-01T17:57:23-04:00 HorizoN httpd(rest): [Tue Nov 01 17:57:23.252733 2022] [ssl:info] [pid 9305] SSL Library Error: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate?

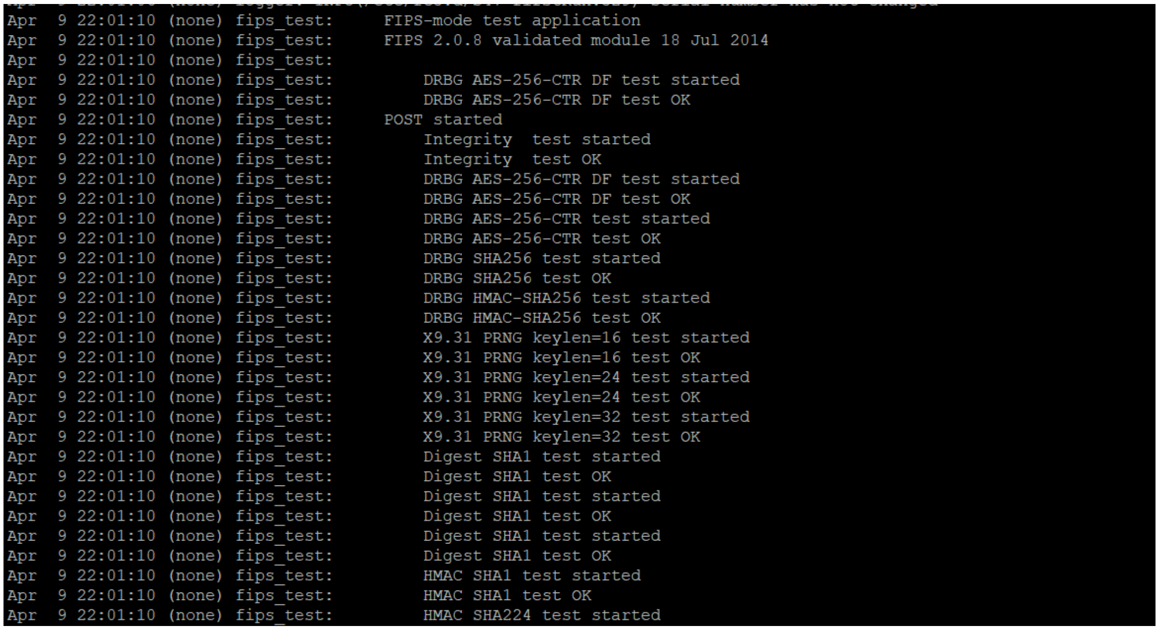
Requirement	Auditable Events	Additional Audit Record Contents	Log
			2022-11-01T17:57:23-04:00 HorizoN httpd(rest): [Tue Nov 01 17:57:23.252779 2022] [ssl:info] [pid 9305] [client 10.100.1.205:49038] AH01998: Connection closed to child 1 with abortive shutdown (server localhost.localdomain:8443)
FCS_SSHC_EXT.1	Failure to establish an SSH session.	Reason for failure.	Jan 18 23:15:02 HorizON sshd[13013]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.200.26 Jan 18 23:15:03 HorizON sshd[13013]: debug1: PAM: password authentication failed for an illegal user: User not known to the underlying authentication module Jan 18 23:15:03 HorizON sshd[13013]: Failed password for invalid user admin6 from 172.16.200.26 port 1324 ssh2
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.	Apr 12 18:40:15 HorizON sshd[10847]: ssh_dispatch_run_fatal: Connection from user tsadmin 10.100.1.168 port 54626: message authentication code incorrect
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	2022-11-01T17:59:24-04:00 HorizoN httpd(web): [Tue Nov 01 17:59:24.850706 2022] [ssl:info] [pid 24863] [client 10.100.1.205:45616] AH01964: Connection to child 5 established (server localhost.localdomain:443) 2022-11-01T17:59:24-04:00 HorizoN httpd(web): [Tue Nov 01 17:59:24.851049 2022] [ssl:debug] [pid 24863] ssl_engine_kernel.c(2427): [client 10.100.1.205:45616] AH02645: Server name not provided via TLS extension (using default/first virtual host) 2022-11-01T17:59:24-04:00 HorizoN httpd(web): [Tue Nov 01

Requirement	Auditable Events	Additional Audit Record Contents	Log
			17:59:24.851265 2022] [ssl:info] [pid 24863] [client 10.100.1.205:45616] AH02008: SSL library error 1 in handshake (server localhost.localdomain:443) 2022-11-01T17:59:24-04:00 HorizoN httpd(web): [Tue Nov 01 17:59:24.851445 2022] [ssl:info] [pid 24863] SSL Library Error: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate? 2022-11-01T17:59:24-04:00 HorizoN httpd(web): [Tue Nov 01 17:59:24.851491 2022] [ssl:info] [pid 24863] [client 10.100.1.205:45616] AH01998: Connection closed to child 5 with abortive shutdown (server localhost.localdomain:443)
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store.	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	2022-08-25T15:51:42.200905-04:00 centsyslog.example.com 03:52:07PM 08/25/22 HorizON: [TS] Failed to validate the certificate chain for new Trusted CA import, certificate sha256 hash = 810bab8c1fdee7fd986dfb79e870146d316f0503ee6e9453d9d573ad5b81118f, by tsadmin. 2022-10-28T12:16:34.630728-04:00 centsyslog.example.com 04:16:48PM 10/28/22 HorizON: [TS] (root:ts-certificate-ca-install.sh) script run by tsadmin, invoked with args [ca-ecdsa.cert.pem], pid=6827, shell=/bin/sh. 2022-10-28T12:16:34.984484-04:00 centsyslog.example.com 04:16:48PM 10/28/22 HorizON: [TS] Successfully imported certificate, with certificate ID (public key hash): 1b6099532a74fa2194b438d9ecebcc8db78ef3f18941ec9a8bd5df405341e221, by tsadmin. 2022-10-28T12:16:35.042976-04:00 centsyslog.example.com 04:16:48PM 10/28/22 HorizON: [TS] Trusted CA

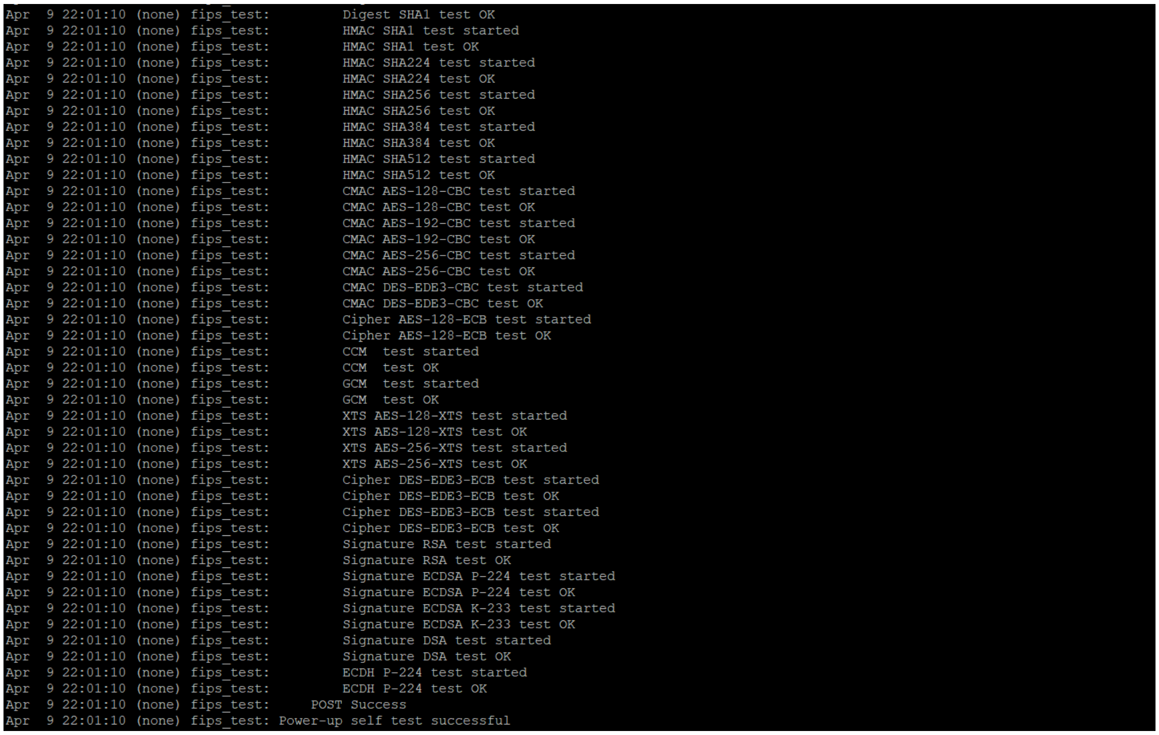
Requirement	Auditable Events	Additional Audit Record Contents	Log
			imported, 1 certificate(s) imported, by tsadmin. 2022-10-28T12:18:21.352702-04:00 centsyslog.example.com 04:18:35PM 10/28/22 HorizON: [TS] (root:ts-certificate-user-install.sh) script run by tsadmin, invoked with args [-k ecdsa_secp384r1.key.pem -c ecdsa_secp384r1.cert.pem -s stunnel], pid=8756, shell=/bin/sh. 2022-10-28T12:18:21.518163-04:00 centsyslog.example.com 04:18:35PM 10/28/22 HorizON: [TS] Certificate Chain verification failed, try importing valid trust certificates using ts-certificate-ca-install.sh Error message: ecdsa_secp384r1.cert.pem: C = CA, ST = ON, L = Ottawa, O = Lightship Security, OU = CC Testing, CN = 10.120.1.10error 7 at 0 depth lookup:certificate signature failure , by tsadmin.

5.2.1 FPT_TST_EXT.1 TSF Testing

105 The following log entries should be generated as a result of TOE cryptographic self-tests:



```
Apr  9 22:01:10 (none) fips_test:     FIPS-mode test application
Apr  9 22:01:10 (none) fips_test:     FIPS 2.0.8 validated module 18 Jul 2014
Apr  9 22:01:10 (none) fips_test:
Apr  9 22:01:10 (none) fips_test:         DRBG AES-256-CTR DF test started
Apr  9 22:01:10 (none) fips_test:         DRBG AES-256-CTR DF test OK
Apr  9 22:01:10 (none) fips_test:     POST started
Apr  9 22:01:10 (none) fips_test:         Integrity  test started
Apr  9 22:01:10 (none) fips_test:         Integrity  test OK
Apr  9 22:01:10 (none) fips_test:         DRBG AES-256-CTR DF test started
Apr  9 22:01:10 (none) fips_test:         DRBG AES-256-CTR DF test OK
Apr  9 22:01:10 (none) fips_test:         DRBG AES-256-CTR test started
Apr  9 22:01:10 (none) fips_test:         DRBG AES-256-CTR test OK
Apr  9 22:01:10 (none) fips_test:         DRBG SHA256 test started
Apr  9 22:01:10 (none) fips_test:         DRBG SHA256 test OK
Apr  9 22:01:10 (none) fips_test:         DRBG HMAC-SHA256 test started
Apr  9 22:01:10 (none) fips_test:         DRBG HMAC-SHA256 test OK
Apr  9 22:01:10 (none) fips_test:         X9.31 PRNG keylen=16 test started
Apr  9 22:01:10 (none) fips_test:         X9.31 PRNG keylen=16 test OK
Apr  9 22:01:10 (none) fips_test:         X9.31 PRNG keylen=24 test started
Apr  9 22:01:10 (none) fips_test:         X9.31 PRNG keylen=24 test OK
Apr  9 22:01:10 (none) fips_test:         X9.31 PRNG keylen=32 test started
Apr  9 22:01:10 (none) fips_test:         X9.31 PRNG keylen=32 test OK
Apr  9 22:01:10 (none) fips_test:         Digest SHA1 test started
Apr  9 22:01:10 (none) fips_test:         Digest SHA1 test OK
Apr  9 22:01:10 (none) fips_test:         Digest SHA1 test started
Apr  9 22:01:10 (none) fips_test:         Digest SHA1 test OK
Apr  9 22:01:10 (none) fips_test:         Digest SHA1 test started
Apr  9 22:01:10 (none) fips_test:         Digest SHA1 test OK
Apr  9 22:01:10 (none) fips_test:         HMAC SHA1 test started
Apr  9 22:01:10 (none) fips_test:         HMAC SHA1 test OK
Apr  9 22:01:10 (none) fips_test:         HMAC SHA224 test started
```



```
Apr  9 22:01:10 (none) fips_test:         Digest SHA1 test OK
Apr  9 22:01:10 (none) fips_test:         HMAC SHA1 test started
Apr  9 22:01:10 (none) fips_test:         HMAC SHA1 test OK
Apr  9 22:01:10 (none) fips_test:         HMAC SHA224 test started
Apr  9 22:01:10 (none) fips_test:         HMAC SHA224 test OK
Apr  9 22:01:10 (none) fips_test:         HMAC SHA256 test started
Apr  9 22:01:10 (none) fips_test:         HMAC SHA256 test OK
Apr  9 22:01:10 (none) fips_test:         HMAC SHA384 test started
Apr  9 22:01:10 (none) fips_test:         HMAC SHA384 test OK
Apr  9 22:01:10 (none) fips_test:         HMAC SHA512 test started
Apr  9 22:01:10 (none) fips_test:         HMAC SHA512 test OK
Apr  9 22:01:10 (none) fips_test:         CMAC AES-128-CBC test started
Apr  9 22:01:10 (none) fips_test:         CMAC AES-128-CBC test OK
Apr  9 22:01:10 (none) fips_test:         CMAC AES-192-CBC test started
Apr  9 22:01:10 (none) fips_test:         CMAC AES-192-CBC test OK
Apr  9 22:01:10 (none) fips_test:         CMAC AES-256-CBC test started
Apr  9 22:01:10 (none) fips_test:         CMAC AES-256-CBC test OK
Apr  9 22:01:10 (none) fips_test:         CMAC DES-EDE3-CBC test started
Apr  9 22:01:10 (none) fips_test:         CMAC DES-EDE3-CBC test OK
Apr  9 22:01:10 (none) fips_test:         Cipher AES-128-ECB test started
Apr  9 22:01:10 (none) fips_test:         Cipher AES-128-ECB test OK
Apr  9 22:01:10 (none) fips_test:         CCM  test started
Apr  9 22:01:10 (none) fips_test:         CCM  test OK
Apr  9 22:01:10 (none) fips_test:         GCM  test started
Apr  9 22:01:10 (none) fips_test:         GCM  test OK
Apr  9 22:01:10 (none) fips_test:         XTS AES-128-XTS test started
Apr  9 22:01:10 (none) fips_test:         XTS AES-128-XTS test OK
Apr  9 22:01:10 (none) fips_test:         XTS AES-256-XTS test started
Apr  9 22:01:10 (none) fips_test:         XTS AES-256-XTS test OK
Apr  9 22:01:10 (none) fips_test:         Cipher DES-EDE3-ECB test started
Apr  9 22:01:10 (none) fips_test:         Cipher DES-EDE3-ECB test OK
Apr  9 22:01:10 (none) fips_test:         Cipher DES-EDE3-ECB test started
Apr  9 22:01:10 (none) fips_test:         Cipher DES-EDE3-ECB test OK
Apr  9 22:01:10 (none) fips_test:         Signature RSA test started
Apr  9 22:01:10 (none) fips_test:         Signature RSA test OK
Apr  9 22:01:10 (none) fips_test:         Signature ECDSA P-224 test started
Apr  9 22:01:10 (none) fips_test:         Signature ECDSA P-224 test OK
Apr  9 22:01:10 (none) fips_test:         Signature ECDSA K-233 test started
Apr  9 22:01:10 (none) fips_test:         Signature ECDSA K-233 test OK
Apr  9 22:01:10 (none) fips_test:         Signature DSA test started
Apr  9 22:01:10 (none) fips_test:         Signature DSA test OK
Apr  9 22:01:10 (none) fips_test:         ECDH P-224 test started
Apr  9 22:01:10 (none) fips_test:         ECDH P-224 test OK
Apr  9 22:01:10 (none) fips_test:     POST Success
Apr  9 22:01:10 (none) fips_test: Power-up self test successful
```

106 The following log entries should be generated as a result of TOE software integrity self-tests:

```
SW Integrity test executed on Tue Sep 21 23:19:02 UTC 2021
-----------------------------
Directory: /HorizON/Server
UCSMgmt: OK
Directory: /HorizON/Server
UDBServ: OK
Directory: /HorizON/Server
autossh: OK
Directory: /HorizON/Server
horizONsshd: OK
Directory: /HorizON/Server
horizONtelnet: OK
Directory: /usr/bin
fips_test_suite: OK
Directory: /usr/bin
httpd: OK
Directory: /usr/bin
openssl: OK
Directory: /usr/lib
libcrypto.so.1.0.0: OK
Directory: /usr/lib
libssl.so.1.0.0: OK
Directory: /usr/modules
mod_ssl.so: OK
Directory: /usr/sbin
sshd: OK
```