NETSCOUT nGeniusOne with InfiniStreamNG v6.3.3

Common Criteria Guide

Version 1.20

April 2024

Document prepared by

Lightship Security

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 NETSCOUT nGeniusOne with InfiniStreamNG v6.3.3 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 3.

1.3 Terminology

Table 1: Terminology

Term	Definition
AA	Authenticator Address
CC	Common Criteria
EAL	Evaluation Assurance Level
LAN	Local Area Network
NDcPP	collaborative Protection Profile for Network Devices
NDcPP-SD	collaborative Protection Profile for Network Devices Supporting Document
NG1	nGeniusONE
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

1.4 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/

1.4.1 Protection Profile Conformance

4 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

1.4.2 Evaluated Software and Hardware

5 The Target of Evaluation (TOE) is a distributed network device that consists of a nGeniusOne v6.3.3 server and InfiniStream v6.3.3 appliance added to the server.

Model	CPU
nGenius (OS: Linux 3.10)	
NETSCOUT nGeniusOne Enhanced Appliance	Intel® Xeon® Gold 6142 (Skylake)
NETSCOUT nGeniusOne Standard Appliance	Intel® Xeon® Gold 6132 (Skylake)
NETSCOUT nGeniusOne Appliance	Intel® Xeon® Silver 4110 (Skylake)
InfiniStreamNG (OS: Linux 3.10)	
NETSCOUT 1410J	Intel® Xeon® Silver 4110 (Skylake)
NETSCOUT 2410J	
NETSCOUT 2695J	Intel® Xeon® Gold 6126 (Skylake)
NETSCOUT 4795J	
NETSCOUT 6695J	
NETSCOUT 9795J	
NETSCOUT 4895J	Intel® Xeon® Gold 6152 (Skylake)
NETSCOUT 9802J	
NETSCOUT 9807J	
NETSCOUT 9895J	
NETSCOUT 690J	Intel Atom® Processor C3955 (Denverton)

1.4.3 Evaluated Functions

6 The following functions have been evaluated under Common Criteria:

a) **Protected Communications.** The TOE provides secure communication channels:

i) **CLI.** Administrative CLI via direct serial connection or remote SSH.

ii) **GUI/Web API.** Administrative nGeniusONE web GUI via HTTPS.

iii) **Syslog.** Transmission of logs to the syslog server via SSH.

iv) **OCSP Responder.** X.509v3 certificate revocation checking via OCSP.

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

i) Administrator authentication with passwords

ii) Configurable password policies

iii) 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 using a published hash mechanism.

d) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and can send 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 cryptographic algorithms used in the above functions have been validated for correct implementation.

7 **NOTE:** No claims are made regarding any other security functionality. Only the cryptographic engines configured in this guide were tested and can be used in the evaluated configuration. No other cryptographic engines were tested or can be used.

1.4.4 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.

Table 2: Evaluation Assumptions

Assumption	Guidance
Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Ensure that the device is hosted in a physically secure environment, such as a locked server room.
There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Do not install other software on the device hardware.
The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by	The Common Criteria evaluation focused on the management plane of the device.

Assumption	Guidance
other security and assurance measures in the operational environment.	
Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Ensure that administrators are trustworthy – e.g. implement background checks or similar controls.
The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Apply updates regularly according to your organization’s policies.
The Administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators should take care to not disclose credentials and ensure private keys are stored securely.
The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	Administrators should sanitize the device before disposal or transfer out of the organization’s control.

1.5 Conventions

9 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 3. For example:

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

1.6 Related Documents

10 This guide supplements the below documents which are available from https://my.netscout.com/mcp/Pages/Doc_Landing.aspx

Table 3: Related Documents

Reference	Document
[INSTALL]	NETSCOUT Server Administrator Guide Release Version 6.3.3 Doc ID 733-1661, Rev. I/ July 2022 nGeniusONE Configuration Essentials for Administrators Release Version 6.3.3 Doc ID 733-1665, Rev. A / November 2021
[USER]	InfiniStreamNG Certified/Hardware Appliance Administrator Guide, v6.3.3 733-1638 Rev. D July 18, 2022

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

2 Secure Acceptance and Update

2.1 Obtaining the TOE

12 The TOE is delivered via commercial courier. Perform the following checks upon receipt (return the device if either of the checks fail):

a) Confirm that the correct device has been delivered

b) Inspect the packaging to confirm that there are no signs of tampering

13 InfiniStream is installed via the CLI. The nGeniusONE appliance is installed from the base NETSCOUT restore installation. Follow the instructions detailed in the nGeniusONE v6.3 Server Administrator Guide (733-1354 Rev. A) at [INSTALL] to complete the installation.

2.2 Verifying the TOE

14 Refer [USER] *Verify the Software Version* section of *InfiniStreamNG Certified/Hardware Appliance Administrator Guide, v6.3* for a description on how to query the currently active version.

2.3 Power-on Self-Tests

15 On start-up, the system will run a series of self-tests:

a) **POST.** The system runs Power-On diagnostic Self-Test (POST) every time it starts until disabled.

b) **FIPS Self-tests.** The TOE checks the integrity of the system files at the startup.

16 Any failure of the POST test writes a diagnostic code to the console (an LCD K/V/M or a terminal connected to the serial port) and sounds a beep code on the system speaker. Depending on the severity of the error, the boot-up may halt.

a) If an error occurs, power down the system, check all cables and retry the power on sequence.

b) If a hardware error persists, record the error codes or symptoms, and if possible, take a screen shot of the errors. Contact NETSCOUT Customer Support for assistance.

17 The TOE runs FIPS-Approved power-up self-tests (during power-up or reboot of the TOE) and conditional self-tests. If any of the self-tests fail to produce the expected outcome, failure of any of these tests will cause the module startup to fail and write a failure message to the appropriate log file.

18 All of the above errors result in a critical error state and an administrator must reboot the TOE to run the self tests again by using the appliance’s power button. Once the self-tests successfully pass, the appliance will start up successfully. The log messages displaying the error messages can then be viewed via the following:

a) Log in to the nGeniusONE server, either via SSH or locally via the serial port, and assume root privileges.

b) Navigate to the `/opt/` directory.

c) Make a new directory named `fipstest` and navigate into it:

```
mkdir fipstest
cd fipstest
```

d) Copy the FIPS test suite to this temporary directory, unpack it, copy it the indicated directory, and make it executable:

```
cp /opt/NetScout/rtm/bin/fips_test_suite.tar .
tar –xvf fips_test_suite.tar
cp fips_test_suite /opt/platform
chmod 550 /opt/platform/fips_test_suite
```

e) Enable rsyslog service so it will start on reboot.

```
systemctl enable rsyslog.service
```

f) Edit `rc.local:`

```
vi /etc/rc.d/rc.local
```

g) Add the following lines:

```
service rsyslog start
/opt/ngp/log-audit/local/ngp-log-audit.sh -t start
/opt/platform/fips_test_suite post|logger
```

h) Save and exit the file.

i) Add a script that can be run as a service on startup:

```
cd /opt/startupscript/
touch runfipstestsuite.sh
vi runfipstestsuite.sh
```

j) Add the following lines to the script

```
#!/usr/bin/bash
/opt/ngp/log-audit/local/ngp-log-audit.sh -t start
/opt/platform/fips_test_suite post|logger
```

k) Save and exit the file.

l) Enable execute for this new script:

```
chmod 744 ftptestsuiterun.sh
```

m) Create new Service file to run the script

```
cd /usr/lib/systemd/system
touch runfipstestsuite.service
```

n) Add following lines to runfipstestsuite.service:

```
[Unit]
Description=Runs /opt/startupscript/runfipstestsuite.sh
After=rsyslog.service
[Service]
ExecStart=/opt/startupscript/runfipstestsuite.sh
[Install]
WantedBy=multi-user.target
```

o) Add a link to this service in /etc/systemd/system

```
cd /etc/systemd/system
ln -s /usr/lib/systemd/system/runfipstestsuite.service
```

p) Enable the new service

```
systemctl enable runfipstestsuite.service
```

q) Reboot the server to invoke these changes:

```
reboot
```

2.4 Updating the TOE

19 Refer [USER] *Verify the Software Version* section of *InfiniStreamNG Certified/Hardware Appliance Administrator Guide, v6.3* for a description on how to query the currently active version.

20 To upgrade the NG1 perform a :

21

```
sudo /opt/NetScout/rtm/bin/cc_upgrade.sh /opt/nG1-6330-XXX-lin.bin
```

22 or

23

```
sudo ./nG1-6330-XXX-lin.bin
```

24 And for additional patches:

25

```
sudo /opt/NetScout/rtm/bin/cc_upgrade.sh /opt/ATSFX64_56W_56L_53_90069_02zg_208.bin
```

26 To upgrade the InfiniStream from the NG1, download the application installer file (is-6330-xxx-eth.bin or is-6330-xxx-eth-J.bin) to the `/opt/` directory on the nGeniusONE server using either manual or automatic methods. Next run:

27

```
sudo /opt/NetScout/rtm/bin/cc_upgrade.sh /opt/is-6330-XXX-eth.bin
```

a) On the InfiniStream device perform a `/opt/NetScout/rtm/bin/stop`

b) From the nGeniusONE console, perform the following steps:

   i) Launch **Device Configuration**.

   ii) On the **Devices** tab, installed InfiniStreamNG appliances are listed with their current status, name, IP address, model, version and build number. The Upgrade column indicates whether the appliance already has the latest version of software installed that is stored in the console server upgrade file repository (Up to date) or a higher version is available for remote upgrades (Upgrade).

   iii) select the appliance and click the **Upgrade** link in the Upgrade column.

   iv) In the **Device Software Packages** dialog box, select the appropriate installer file to use. The dialog box displays only those software packages appropriate to the type of selected appliance(s).

c) Once the install is complete use the backups user to restore any custom configuration changes made in the below sections.

28 Upgrade files for the nGeniusOne and InfiniStream are verified for authenticity manually by Administrators by checking the hash published by the vendor for each file.

29 To verify upgrade images perform the following procedures:

a) Access the system command-line as the backups user.

b) Navigate to the directory to which you copied the downloaded files.

c) Ensure the checksum files and binary are in this same directory.

d) Use the following command to generate a new checksum for the binary, and compare it to the downloaded checksum. `/usr/bin/sha256sum -c <sha checksum filename>`

30 Example of valid file output:

a)

```
[backups@host /opt/]# /usr/bin/sha256sum -c pm-6330-XXX-lin.sha256
pm-6330-XXX-lin.bin: OK
```

31 Example of invalid file output :

a)

```
[backups@host /opt/]# /usr/bin/sha256sum -c pm-6330-XXX-lin.sha256
pm-6330-XXX-lin.bin: FAILED
sha256sum: WARNING: 1 of 1 computed checksum did NOT match
```

32 If the validation fails, try downloading the files and re-validating them again. For repeated validation errors, contact Customer Support for assistance.

33 The nGeniusOne and InfiniStream TOE components may be updated in no particular order. All services should be stopped before upgrades are performed, allowing for no dependency on which component is updated first.

3 Configuration Guidance

3.1 Installation

34 NOTE: The commands given in the document must be prefixed with ‘sudo’ or ‘sudoedit’ when executing by user Backups after the initial installation and configuration of the TOE.

35 iDRAC interface is not in scope and should not be connected to the network.

36 Follow the instructions below to perform the first time installation steps with the “root” user.

37 nGeniusOne:

a) Download the version 6.3.3 image from NETSCOUT’s MasterCare site and place it in the /opt/ directory.

b) Run a `chmod +x ng1-6330-XXX-lin.bin`

c) Install the image by executing: `./ng1-6330-XXX-lin.bin`

d) Follow the prompts.

e) `Locale: <user defined Locale>`

f) `End User License Agreement: Press Enter and then Y when prompted`

g) `Installation Location: /opt/NetScout`

h) `Server Type: Standalone Server`

i) `Host Name / IP address: <user defined hostname and IP>`

j) `Web Server Port: 443`

k) `Web Server Protocol: HTTPS`

l) `Web User Account Name and Password: Administrator / <user defined password>`

m) Reboot the appliance to apply the changes.

n) Download the `ATSFX64_34W_54L_53_90058_02zg_208.bin` patch from NETSCOUT’s MasterCare site and place it in the /opt/ directory.

o) Run a `chmod +x ATSFX64_34W_54L_53_90058_02zg_208.bin`

p) Install the image by executing:
```
./ATSFX64_34W_54L_53_90058_02zg_208.bin
```

q) After running the bin installation files on the nGeniusONE, execute the `/opt/NetScout/rtm/bin/LicenseCL.sh` and follow the prompts to install the server license you received from NETSCOUT.

r) Put the web server on port 443
```
./websecure.sh -protocol HTTPS -port 443
```

The following message will appear:
```
This script will stop nG1 Server. Do you wish to continue
?: Y / N
```
Enter Y

s) Once finished, verify that all NETSCOUT processes are running:
```
/opt/NetScout/rtm/bin/PS
```

Open a web browser and navigate to the nGeniusONE server. The new URL will be https://<nG1_IP_address>. Verify that all processes and services are available.

t) Completing the security changes to the TOE via the nG1-STIG script file consists of two major steps: verifying the nGeniusONE Security bundle is in the correct directory and executing the script. Verify the STIG script is in the root directory (/) of the TOE.

u) Change to the root directory (/) of the TOE and expand the Security bundle. `tar –xvzf /nG1-STIG-<DD-MMM-YYYY>.tgz`

v) Execute the Security bundle script and complete the remaining compliance requirements manually. Once the script completes, a list of outstanding items to manually change are listed. `/opt/STIG/nG1-STIG.sh`

w) When the STIG script has completed modify the /etc/fstab file to appear as follows:

```
UUID=de1d7dc7-47f2-47d7-854d-0258988d03ef / ext4 noatime 1 1

UUID=b04baa5a-ec85-409e-b28e-3913cb302f33 /boot ext4 nosuid 1 2

UUID=3a8e951b-e5d8-4fa3-b0b7-ca08bd6635f8 /export/home ext4
defaults,nosuid 1 2

UUID=572ce51f-01a3-42d8-983b-4f03d8bd00e1 /opt xfs noatime 1 2

UUID=8087f57f-0e83-4407-9a64-1efb3e793070 /opt/NetScout/rtm/html ext4
noatime 1 2

UUID=9ea4d173-8eaa-47bb-869f-d5a9c8201c05 /tmp ext4 defaults 1 2

UUID=4fd472a1-df82-41dc-ae25-f553ff909a3a /var ext4 defaults 1 2

UUID=64ade394-eaaa-4432-a12f-37e113c87582 swap swap defaults 0 0

tmpfs /dev/shm tmpfs defaults 0 0

devpts /dev/pts devpts gid=5,mode=620 0 0

sysfs /sys sysfs defaults 0 0
```

x) For sudoers changes run : `/opt/NetScout/rtm/bin/appendNtctCmnds.sh`

y) Append the following to the end of the /etc/sudoers.d/backups file

```
backups ALL=(ALL) /opt/*.bin

backups ALL=(ALL) sudoedit /etc/pam.d/system-auth-local

backups ALL=(ALL) sudoedit /etc/pam.d/password-auth-local
```

z) Modify the `/opt/NetScout/rtm/bin/serverprivate.properties` file and append the following:

```
SSLHelper.verifyCertificatesCC=true
```

aa) Modify the `/opt/NetScout/rtm/bin/append_java.security` file

```
# securerandom.source=file:/dev/urandom

securerandom.source=file:/dev/random

securerandom.drbg.config=CTR_DRBG,AES-
256,256,pr_and_reseed,use_df

jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH
keySize < 768, EC keySize > 256, ECDH, SHA1, DHE, 3DES,
TLS_EMPTY_RENEGOTIATION_INFO_SCSV,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```

```
security.provider.1=org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider

security.provider.2=sun.security.provider.Sun

security.provider.3=sun.security.rsa.SunRsaSign

security.provider.4=sun.security.ec.SunEC

security.provider.5=com.sun.net.ssl.internal.ssl.Provider BCFIPS

security.provider.6=com.sun.crypto.provider.SunJCE

security.provider.7=sun.security.jgss.SunProvider

security.provider.8=com.sun.security.sasl.Provider

security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI

security.provider.10=sun.security.smartcardio.SunPCSC
```

bb) Add the following to the `/opt/NetScout/rtm/bin/httpd-ssl-custom.conf`

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256

SSLOpenSSLConfCmd Curves prime256v1
```

cc) Modify the `/etc/ssh/sshd_config` file and add the following below `KexAlgorithms:`

```
PubKeyAcceptedKeyTypes ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521

HostKeyAlgorithms ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521

RekeyLimit 512M 1h
```

dd) create the script `/opt/NetScout/rtm/bin/cc_upgrade.sh`

ee) Vi the script and add the following:

```
#!/bin/bash

. /var/adm/NetScout/nGeniusReg.properties


# script used when in Common Criteria configuration

# allows backups user to perform nG1 upgrades, install ATSF patches

# and copy IS bins to tftpboot directory for ISNG upgrades


# allow backups user to perform nG1 upgrades
```

```
if grep -q "nG1" <<< $1; then
    echo "nG1:   " $1
    /bin/chmod 770 $1
    $1 -DMIN_CHECK=true
fi

# allow backups user to run ATSF patch
if grep -q "ATSF" <<< $1; then
    echo "ATSF:   " $1
    /bin/chmod 770 $1
    $1
fi

# allow backups user to copy IS bin to tftpboot directory
if grep -q "is-" <<< $1; then
    echo $1
    /bin/cp $1  $PERFMGR_PATH/rtm/tftpboot
    /bin/chown ngenius:ngenius $PERFMGR_PATH/rtm/tftpboot/*
    /bin/chmod 750 $PERFMGR_PATH/rtm/tftpboot/*
Fi
```

ff) Save the file

gg) Execute the following:

```
chown ngenius:ngenius /opt/NetScout/rtm/bin/cc_upgrade.sh
chmod 750  /opt/NetScout/rtm/bin/cc_upgrade.sh
```

hh) Run the visudo command and add the highlighted text

Cmnd_Alias NTCT_CMDS = /opt/NetScout/rtm/bin/start, /opt/NetScout/rtm/bin/stop, /opt/NetScout/rtm/bin/webstart, /opt/NetScout/rtm/bin/webstop, /opt/NetScout/rtm/bin/PS, /opt/NetScout/rtm/bin/techsupp.sh norm, /opt/NetScout/rtm/bin/LicenseCL.sh, /opt/NetScout/rtm/bin/nGApplianceConfig.plx, /opt/NetScout/rtm/tools/nscertutil.sh, /bin/cat /opt/NetScout/rtm/pa/bin/decoderelease.properties, /opt/NetScout/rtm/bin/nstool.sh com.netscout.database.util.ServerTool, /bin/less /var/log/messages, /bin/less /var/log/dmesg, /bin/openssl x509 -in /opt/NetScout/apache/conf/ssl.crt/server.crt -text, /bin/sudoedit /opt/NetScout/rtm/bin/serverprivate.properties, /sbin/visudo, /bin/sudoedit /opt/NetScout/rtm/html/client.properties, /bin/sudoedit /opt/NetScout/rtm/html/umcclient.properties, /bin/sudoedit /etc/bashrc , /bin/sudoedit /etc/issue, /bin/sudoedit /etc/rsyslog.conf , /bin/sudoedit /etc/pam.d/password-auth-local, /bin/sudoedit /etc/security/pwquality.conf, /bin/sudoedit /opt/NetScout/rtm/bin/httpd-custom.conf, /bin/sudoedit /opt/NetScout/rtm/bin/httpd-ssl-custom.conf, /bin/sudoedit /opt/NetScout/rtm/bin/append_java.security, /bin/sudoedit /opt/NetScout/rtm/bin/dvtools.properties, /bin/sudoedit /etc/ssh/sshd_config, /bin/sudoedit /etc/rc.d/rc.local, /opt/ngp/log-audit/local/ngp-log-audit.sh, /opt/ngp/log-audit/local/ngp-audit-tunnel.sh, /bin/sudoedit

/opt/NetScout/rtm/bin/bootstrapconfig/masterconfig/ProcessMaster.xml, /opt/NetScout/rtm/bin/cc_upgrade.sh

ii) Save the file

jj) Add unlocker user:

```
useradd unlocker
passwd unlocker
```

kk) Create file `/etc/sudoers.d/unlocker` with this content

```
unlocker ALL=(ALL) /usr/sbin/faillock
```

ll) Disable NTP

```
systemctl stop ntpd
systemctl disable ntpd
```

mm) Disable Dell OpenManage Server Administrator service:

```
/opt/dell/srvadmin/sbin/srvadmin-services.sh disable
```

38 InfiniStream:

a) Download the version 6.3.3 image from NETSCOUT's MasterCare site and place it in the /opt/ directory.

b) Run a `chmod +x is-6330-XXX-eth-j.bin`

c) Install the image by executing: `./ is-6330-XXX-eth-j.bin`

d) Follow the prompts.

e) `Locale: <user defined Locale>`

f) `End User License Agreement: Press Enter and then Y when prompted`

g) The installation will then run and complete, and a reboot will be required to apply the changes. In order to configure the network interface run the *nGApplianceConfig.plx.*

h) Stop all of the NETSCOUT services and verify that none of the services are active. `isbin; ./stopall; PS`

i) Verify the security bundle is in the following directory of the TOE `/opt/platform/security/stig/STIG/.`

j) Change to the STIG directory of the TOE.

k) Execute the Security bundle script and complete the remaining compliance requirements manually. Once the script completes, a list of outstanding items to manually change are listed.

```
/opt/platform/security/stig/STIG/ISNG-STIG.sh
Confirm the system is a 6.3.3 64-bit (FC12) platform
[Y/y]: y
```

l) Modify the `/etc/ssh/sshd_config` file and add the following below `KexAlgorithms:`

```
PubKeyAcceptedKeyTypes ecdsa-sha2-nistp256, ecdsa-sha2-
nistp384, ecdsa-sha2-nistp521
```

```
HostKeyAlgorithms ecdsa-sha2-nistp256, ecdsa-sha2-
nistp384, ecdsa-sha2
```

```
RekeyLimit 512M 1h
```

39 For all devices run the following to enable and start the device firewall:

a) `systemctl enable iptables`

b) `systemctl start iptables`

40 Check that the firewall is running:

a) `systemctl status iptables`

41 Using root perform the following:

a) `usermod -a -G ngenius backups`

b) `chown backups:ngenius /home/backups`

c) `chmod 750 /home/backups`

d) `mkdir /home/ngenius`

e) `chown ngenius:ngenius /home/ngenius`

f) `chmod 750 /home/ngenius`

g) In /home/ngenius create create_key_and_csr.sh with this content and make it executable.

```
#!/bin/bash

/bin/openssl ecparam -genkey -out /home/ngenius/ssl.key -name
prime256v1
/bin/openssl req -new -key /home/ngenius/ssl.key -out
/home/ngenius/ssl.csr
chmod 660 /home/ngenius/ssl.csr
```

h) Execute `chmod +x /home/ngenius/create_key_and_csr.sh and chown ngenius:ngenius /home/ngenius/create_key_and_csr.sh`

i) In /home/ngenius create load_cert.sh with this content and make it executable.

```
#!/bin/bash

display_usage() {
       echo "This script must be run sudo as ngenius."
       echo -e "\nUsage: $0 <host_cert> <signing_cert>
[additional_signing_cert, ...] \n"
       }

if [  $# -lt 2 ]
then
    display_usage
     logger "$user executed load_cert.sh: certificate import
   failed, host certificate provided without signer"
    exit 1
```

```
fi

status=$(openssl x509 -in $2 -noout -text | grep "CA:TRUE")
if [ -z "$status" ]
then
    display_usage
    logger "$user executed load_cert.sh: certificate import failed, invalid CA file $2 provided"
    exit 1
fi

verified=$(openssl verify -CAfile $2 $1 | grep "OK")
if [ -z "$verified" ]
then
    display_usage
    logger "$user executed load_cert.sh: verification failed, $2 invalid issuer of $1"
    exit 1
fi

cp -p /opt/NetScout/config/is.pem "/opt/NetScout/config/is.pem.$$"
cat /home/ngenius/ssl.key > /opt/NetScout/config/is.pem

for ii in "$@"
do
    cat "$ii" >> /opt/NetScout/config/is.pem
done

logger "$user executed load_cert.sh: $1 successfully imported"
chmod 600 /opt/NetScout/config/is.pem
```

j) Execute `chmod +x /home/ngenius/load_cert.sh` and `chown ngenius:ngenius /home/ngenius/load_cert.sh`

k) add these lines to /etc/sudoers.d/backups

```
backups ALL=(ALL) sudoedit /etc/pam.d/system-auth-local
backups ALL=(ALL) sudoedit /etc/pam.d/password-auth-local
backups ALL=(ngenius) /home/ngenius/create_key_and_csr.sh
backups ALL=(ngenius) /home/ngenius/load_cert.sh
backups ALL=(ALL) /bin/ssh-keygen
backups ALL=(ALL) /bin/cat
backups ALL=(ALL) sudoedit /etc/bashrc
backups ALL=(ALL)sudoedit /etc/security/pwquality.conf
```

l) Add unlocker user:

```
useradd unlocker
passwd unlocker
```

m) Create file `/etc/sudoers.d/unlocker` with this content

```
unlocker ALL=(ALL) /usr/sbin/faillock
```

n) Disable NTP

```
systemctl stop ntpd
systemctl disable ntpd
```

42 There is a known issue with the version of rsyslog loaded on the TOE and may require routine maintenance via the root user to address as it is an out of scope issue. The “imstate” files may periodically need to be cleared from “/var/lib/rsyslog”.

43 Follow these steps to properly clear the imstate files:

a) Stop rsyslog

b) Stop server

c) Clear /var/lib/rsyslog/imstate files

d) Move NSWebxContent.out to a new file name

e) Restart server

f) Restart rsyslog

3.2 Cryptography

44 Following the instructions in section 3.1 above will create the administrative user “backups” and enable FIPS mode on both TOE components.

45 TOE components run the following tests on start-up:

a) POST or power on self-test: The POST memory test writes various data patterns into memory locations and reads them back to confirm that each memory location is functional. The test then interacts with every device in the machine looking for any failures. If any tests fail, the POST writes the failure indicator to the display and exits. When the POST ends successfully, the BIOS searches the various boot mechanisms (using the boot ordering maintained in ROM) for the operating system. The cryptographic POST consists of:

i) software integrity test: HMAC-SHA1 verification of the binary code comprising the module executable

ii) KATs (known answer tests) for cryptographic algorithms

iii) PCTs (pairwise consistency tests) for asymmetric key pairs: a conditional test that runs only when asymmetric keys are generated

iv) random bit and random number generator tests: (conditional tests that run only when random bits and random numbers are generated

46 All self-tests are performed by both TOE components at start-up.

47 InfiniStream self-tests can be executed with the following:

48
```
cd /opt/platform/security/fips
```

49
```
# sh netscout_fips_post.sh
```

50 In the event that a power on self-test fails, the boot process will terminate. The TOE component will need to be rebooted to attempt to clear the error. If the TOE component has been corrupted or the hardware has failed such that rebooting will not resolve the issue, a Security Administrator will need to contact NETSCOUT support.

3.3 Administration Interfaces

51 Only the following administration interfaces may be used:

52 nGeniusOne:

a) **Console.** See [INSTALL] *Accessing the Appliance OS* chapter *of NETSCOUT Server Administrator Guide* to connect using serial port.

   i) The inactivity period can be configured by modifying `TMOUT=X` where X is a time value in seconds, at the top of the `/etc/bashrc` similar to the following:

   ```
   TMOUT = X
   readonly TMOUT
   export TMOUT
   ```

   When the session has been idle for the configured inactivity period, the session is terminated and the administrator logged out.

   ii) The user can terminate a session by typing `logout` into the console.

   iii) Banner messages are displayed and can be configured as follows. Login via CLI, modify the “issue” file via “`sudoedit /etc/issue`”. The configured banner will appear at both the Serial and SSH CLI.

b) **HTTPS.** Web based Graphical User Interface via HTTPS.

   i) Refer [INSTALL] *Accessing the Appliance OS* chapter of *NETSCOUT Server Administrator Guide* to login to the web console as a System Administrator and perform the actions listed below.

   ii) User may use the **Logout** button to terminate the current Web Console session.

   iii) The session timeout can be configured via [INSTALL] *Modifying the client.properties File* chapter of *NETSCOUT Server Administrator Guide*.
   When the session has been idle for the configured session timeout value, the session is terminated and the administrator logged out.

   iv) The user lockout can be configured using the NG1 Web GUI, go to **User Management => Users => ☰ => Security Settings**. Modify the values under **Failed Login Attempts**, enable “Lock accounts if login fails too many times”, configure **Lock accounts after** value to set the consecutive failure threshold, and configure **Lock accounts for** value to set the lockout duration.

v) Web GUI Banner messages are supported and can be configured by following. Log in to the nGeniusONE server, either via SSH or locally via the serial CLI. Edit the “umcclient.properties” file

```
sudoedit
/opt/NetScout/rtm/html/umcclient.properties.
```

Enable the security message by locating the showConfirm variable and changing the default from false to true: `showConfirm=true.` (Optional) NETSCOUT provides default text, which you may also customize, if desired. To change the banner, modify the text for confirmTitle: `confirmTitle=NETSCOUT Security Message.`

To change the security message, modify the text for confirmMessage:

```
confirmMessage=USE OF THIS COMPUTER SYSTEM
CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES.
```

Save and exit the file.

vi) The TOE supports the addition of OCSP responder to configure and manage instructions on configuring certificates and generate signing requests.

c) **SSH.** See instructions for Console. Use an SSH client to connect to the device. The SSH client must be capable of negotiating with the following configurations:

i) Password-based or public key credentials.

ii) Encryption algorithm: AES128-CBC, AES256-CBC

iii) User public key for authentication: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521

iv) Host keys for authentication: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521

v) Data integrity: hmac-sha2-256, hmac-sha2-512

vi) Key agreement scheme: Diffie-Hellman-group14-sha1

53 InfiniStreamNG:

a) **Console.** See [USER] *Accessing the Appliance* chapter of *InfiniStreamNG Certified/Hardware Appliance Administrator Guide* to connect using serial port.

i) The inactivity period can be configured by modifying `TMOUT=X` where `X` is a time value in seconds, at the top of the `/etc/bashrc` similar to the following:

```
TMOUT = X
readonly TMOUT
export TMOUT
```

When the session has been idle for the configured inactivity period, the session is terminated and the administrator logged out.

ii) The user can terminate a session by typing `logout` into the console.

iii) Banner messages are displayed and can be configured as follows. Login via CLI, modify the “issue” file via “`sudoedit /etc/issue`”. The configured banner will appear at both the Serial and SSH CLI.

b) **SSH.** See instructions for Console. Use an SSH client to connect to the device. The SSH client must be capable of negotiating with the following configurations:

i) Password-based or public key credentials.

ii) Encryption algorithm: AES128-CTR, AES256-CTR

iii) User public key for authentication: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521

iv) Host keys for authentication: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521

v) Data integrity: hmac-sha2-256, hmac-sha2-512

vi) Key agreement scheme: Diffie-Hellman-group14-sha1

54 For both the NG1 and InfiniStream, Administrators should only connect using trusted host keys to mitigate the chance of man-in-the-middle attacks occurring. Administrators should also refrain from using the "." character or "-r" option if specifying directories on the target SSH server.

3.4 Default Passwords

55 **admin.** The default administrator account used to access the TOE. Follow the instructions at [USER] *Installing the InfiniStream Application* chapter of *InfiniStreamNG Certified/Hardware Appliance Administrator Guide, v6.3* to change the default password.

3.5 Setting Time

56 The TOE supports various time synchronization options**.** For manual time setting of all TOE components: `timedatectl set-time 'YYYY-MM-DD HH:MM:SS'`. Use the command without parameters to verify the time was changed: `timedatectl`.

3.6 Audit Logging

57 The Common Criteria evaluation confirmed that the log events listed at Annex A: Log Reference are generated by the TOE.

58 A syslog must be configured to store the logs as follows:

a) Navigate to /opt/ngp/log-audit/local/ and use the following commands.

Generate new SSH keys `./ngp-log-audit.sh -k`

Configure both TOE and remote syslog `./ngp-log-audit.sh -c -h (host name or IP) -u (remote user name) -r`

Complete local configuration `./ngp-log-audit.sh -c`

Check the status of the tunnel with the following:

```
./ngp-log-audit.sh -t status
```

If the tunnel is not running the following commands can be used to stop, start and restart the tunnel.

```
./ngp-log-audit.sh -t stop
./ngp-log-audit.sh -t start
./ngp-log-audit.sh -t restart
```

b) On the NG1, Add or Modify the `/opt/NetScout/rtm/bin/serverprivate.properties` file with the following

```
disable.ocsp=false
BaseEngineManager.ssl.protocol=TLSv1.2
log.syslog=true
syslogHost=127.0.0.1
syslogDestPort=514
```

c) Uncomment the following lines in `/opt/NetScout/rtm/bin/httpd-ssl-custom.conf:`

```
ErrorLog "/var/log/httpd/ssl_error_log"

TransferLog "/var/log/httpd/ssl_access_log"

CustomLog "/var/log/httpd/ssl_request_log" "%a %A %h %H
%l %m %s %t %u %U %{SSL_PROTOCOL}x %{SSL_CIPHER}x
\"%{Referer}i\" \"%{User-Agent}i\""
```

d) To increase the logging verbosity the following can be uncommented in the `/opt/NetScout/rtm/bin/httpd-custom.conf.` LogLevel can be changed from “warn” to “debug”.

```
ErrorLog "/var/log/httpd/error_log"

CustomLog "/var/log/httpd/access_log" combined

LogLevel debug
LogFormat "%a %A %h %H %l %m %s %t %u %U \"%{Referer}i\"
\"%{User-Agent}i\"" combined
```

e) In addition to the instructions above include the following in the NG1 `/etc/rsyslog.conf` file

```
$LocalHostName netscout5.catl.local
$template SecureFormat,"%timegenerated:1:10:date-rfc3339%
%timegenerated:12:19:date-rfc3339% %HOSTNAME% %syslogtag% %msg%\n”
$ActionFileDefaultTemplate SecureFormat
$ActionForwardDefaultTemplate RSYSLOG_ForwardFormat
```

```
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
$ModLoad imfile

$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local7

$InputRunFileMonitor
$InputFileName /var/log/messages
$InputFileTag tag_sys_msg:
$InputFileStateFile sys_msg
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/secure
$InputFileTag tag_sys_secure:
$InputFileStateFile sys_secure
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/NetScout/rtm/database/postgresql/pg_log/postgresql-*.log
$InputFileTag tag_postgres_log:
$InputFileStateFile postgres_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/httpd/ssl_request_log
$InputFileTag tag_ssl_request_log:
$InputFileStateFile ssl_request_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/httpd/ssl_access_log
$InputFileTag tag_ssl_access_log:
$InputFileStateFile ssl_access_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
```

```
$InputFileName /var/log/httpd/ssl_error_log
$InputFileTag tag_ssl_error_log:
$InputFileStateFile ssl_error_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/httpd/error_log
$InputFileTag tag_error_log:
$InputFileStateFile error_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/NetScout/rtm/log/NSWebxContent.out
$InputFileTag tag_NSWebxContent.out:
$InputFileStateFile NSWebxContent.out
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/NetScout/rtm/log/NSNG1Content.out
$InputFileTag tag_NSNG1Content.out:
$InputFileStateFile NSNG1Content.out
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/NetScout/rtm/log/NSCDMFlowLogger.out
$InputFileTag tag_NSCDMFlowLogger.out:
$InputFileStateFile NSCDMFlowLogger.out
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/NetScout/rtm/log/NSLogger.out
$InputFileTag tag_NSLogger.out:
$InputFileStateFile NSLogger.out
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/NetScout/apache/logs/error_log
$InputFileTag tag_apache_error_log:
$InputFileStateFile
```

```
$InputFileSeverity info

$InputFileFacility local7

$InputRunFileMonitor


$InputFileName /opt/NetScout/rtm/log/nscertutil.log

$InputFileTag tag_nscertutil:

$InputFileStateFile

$InputFileSeverity info

$InputFileFacility local7

$InputRunFileMonitor


$InputFileName /var/log/ngp/log-audit/audit-tunnel-error.txt

$InputFileTag ngp_error_audit_log:

$InputFileStateFile ngp_error_audit_log

$InputFileSeverity info

$InputFileFacility local7

$InputRunFileMonitor


# PostgreSQL messages for SYSLOG
:msg, contains, "WRITE" @@127.0.0.1:514
:msg, contains, "ERROR :" @@127.0.0.1:514
:msg, contains, "FATAL" @@127.0.0.1:514
:msg, contains, " connection " @@127.0.0.1:514
:msg, contains, " disconnection " @@127.0.0.1:514

# SSL Logging

:msg, contains, "ngp-audit-tunnel" @@127.0.0.1:514
:msg, contains, "Exception:" @@127.0.0.1:514
:msg, contains, "SSL Library Error" @@127.0.0.1:514
:msg, contains, "update handshake state" @@127.0.0.1:514
:msg, contains, "PKIX path validation failed"
:msg, contains, "Failed to parse" @@127.0.0.1:514
:msg, contains, "SSL Library Error" @@127.0.0.1:514
:msg, contains, "PKIX path validation failed"
:msg, contains, "Unsupported named group" @@127.0.0.1:514
:msg, contains, "Unsupported protocol version" @@127.0.0.1:514
:msg, contains, "cipher" @@127.0.0.1:514
:msg, contains, "signature" @@127.0.0.1:514
:msg, contains, "hostname wrong" @@127.0.0.1:514
:msg, contains, "SSL: error" @@127.0.0.1:514
:msg, contains, "fips.selftest" @@127.0.0.1:514
:msg, contains, "ocsp" @@127.0.0.1:514
:msg, contains, "OCSP" @@127.0.0.1:514
:msg, contains, "server.crt" @@127.0.0.1:514
:msg, contains, "server.key" @@127.0.0.1:514
:msg, contains, "ngp-audit-tunnel" @@127.0.0.1:514
:msg, contains, "User" @@127.0.0.1:514
:syslogtag, isequal, "tag_audit_log:" @@127.0.0.1:514
:syslogtag, isequal, "tag_sys_msg:" @@127.0.0.1:514
:syslogtag, isequal, "tag_sys_secure:" @@127.0.0.1:514
:syslogtag, isequal, "tag_ssl_request_log:" @@127.0.0.1:514
:syslogtag, isequal, "tag_ssl_access_log:" @@127.0.0.1:514
:syslogtag, isequal, "tag_postgres_log:" @@127.0.0.1:514
:syslogtag, isequal, "tag_error_log:" @@127.0.0.1:514
```

f) Uncomment the following:

```
#local7.*                                                /var/log/boot.log
```

g) include the following in the InfiniStream /etc/**rsyslog.conf** file

```
$LocalHostName infinistream

$template SecureFormat,"%timegenerated:1:10:date-rfc3339%
%timegenerated:12:19:date-rfc3339% %HOSTNAME% %syslogtag% %msg%\n”

$ActionFileDefaultTemplate SecureFormat
```

```
$ActionForwardDefaultTemplate RSYSLOG_ForwardFormat
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
$ModLoad imfile
$InputFileName /var/log/ipm/api/api.log
$InputFileTag tag_api_log:
$InputFileStateFile api_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/ipm/xms/xms.log
$InputFileTag tag_xms_log:
$InputFileStateFile xms_log
$InputFileSeverity info
$InputFileFacility local7

# Watch the install log
$InputRunFileMonitor
$InputFileName /var/log/ipm/appliance/appliance-install.log
$InputFileTag tag_appliance_log:
$InputFileStateFile appliance_install_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local7

$InputRunFileMonitor
$InputFileName /var/log/messages
$InputFileTag tag_sys_msg:
$InputFileStateFile sys_msg
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/secure
$InputFileTag tag_sys_secure:
$InputFileStateFile sys_secure
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
```

```
$inputRunFileMonitor
$InputFileName /var/log/ipm/appliance/appliance-upgrade-*.log
$InputFileTag tag_appliance_log:
$InputFileStateFile appliance_upgrade_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/nginx/localhost.error.log
$InputFileTag tag_nginx_err:
$InputFileStateFile nginx_err
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/ngp/ocsp/ocsp.log
$InputFileTag tag_ocsp_log:
$InputFileStateFile ocsp_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/ngp/query/audit.log
$InputFileTag ngp_query_audit_log:
$InputFileStateFile ngp_query_audit_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /var/log/ngp/log-audit/audit-tunnel-error.txt
$InputFileTag ngp_error_audit_log:
$InputFileStateFile ngp_error_audit_log
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor


:msg, contains, "audit" @@127.0.0.1:514
:msg, contains, "nGP.Admin" @@127.0.0.1:514
:msg, contains, "ngp-date" @@127.0.0.1:514
:msg, contains, "SSL: error" @@127.0.0.1:514
:msg, contains, "fips.selftest" @@127.0.0.1:514
:msg, contains, "ocsp" @@127.0.0.1:514
:msg, contains, "sshd" @@127.0.0.1:514
:syslogtag, isequal, "tag_audit_log:" @@127.0.0.1:514
```

```
:syslogtag, isequal, "tag_appliance_log:" @@127.0.0.1:514
:syslogtag, isequal, "tag_xms_log:" @@127.0.0.1:514
:syslogtag, isequal, "tag_sys_msg:" @@127.0.0.1:514
:syslogtag, isequal, "ngp_query_audit_log:" @@127.0.0.1:514
```

h) Uncomment the following:

```
#local7.*                                                /var/log/boot.log
```

59 Once these steps for both the nGeniusONE and InfiniStream devices has been performed restart the syslog service and check that the `ngp-audit-tunnel` is running:

```
./ngp-log-audit.sh -t restart
./ngp-log-audit.sh -t status
```

60 The audit records are securely sent to a remote audit server in the operational environment using SSH. Both TOE components transmit audit data to the remote audit server in real time.

61 To troubleshoot TLS audit failures use the commands:

62 `./ngp-log-audit.sh -t restart`

63 `./ngp-log-audit.sh -t status`

64 The TOE also stores logs locally. See [INSTALL] *Managing Activity Logs* chapter of *nGeniusONE v6.3 Configuration Essentials for Administrators* for details. The local audit record will drop new audit data if it exceeds the storage capacity.

3.7 Administrator Authentication

65 The TOE provides internal authentication mechanisms. Follow these instructions to configure the number of successive unsuccessful authentication attempts and period of inactivity.

66 nGeniusOne Web GUI:

a) Run the following commands to create a new certificate for the nGeniusOne:

```
openssl ecparam -genkey -out <filename>.key -name
prime256v1
openssl req -new -key <filename>.key -out <filename>.csr
```

b) Respond to the following prompts:

Country Name (2 letter code) [XX]:

State or Province Name (full name) []:

Locality Name (eg, city) [Default City]:

Organization Name (eg, company) [Default Company Ltd]:

Organizational Unit Name (eg, section) []:

Common Name (hostname) []:

Email Address []:

c) Submit the CSR to your Certificate Authority (CA) for signing. Once it is approved, download the signed certificate along with the root and intermediate certificates for the complete certificate chain.

d) Upload the certificates to the NG1 under `/opt/certs`

e) Add the root and intermediate CA's to the NG1 trust store using the following:
```
/opt/NetScout/rtm/tools/nscertutil.sh
```

f) For each select options [3] Add .crt certificate to the truststore

g) Provide the location of the certs when prompted
```
/opt/certs/<filename>.crt
```

h) Add the server certificate to the NG1 using the following:
```
/opt/NetScout/rtm/tools/nscertutil.sh
```

i) Select option [2] Import a .crt certificate

j) Provide the location of the cert and key when prompted:
```
/opt/certs/<filename>.crt
```
```
/opt/certs/<filename>.key
```

k) Edit the /opt/NetScout/rtm/bin/serverprivate.properties file as in this example:
```
sudoedit /opt/NetScout/rtm/bin/serverprivate.properties
```

l) Enable lockout capabilities, locate the following parameter and set it to true. If it is not in the file, add it.
```
serviceManager.userAccountLockup.enabled=true
```

m) To set the maximum lockout attempts, locate the following parameter and adjust it to the desired number of login attempts to be permitted, according to your security policy, until lockout should occur:
```
serviceManager.userAccount.maxLoginAttempts=6
```

n) To set the desired lockout duration, locate the following parameter and adjust it as desired. `serviceManager.userAccount.lockupPeriod=18000`

o) Save and exit the file.

p) Edit and uncomment the following line in `/opt/NetScout/apache/conf/extra/httpd-ssl.conf`:
```
Listen 443
```

q) Restart nGeniusONE application processes:
```
/opt/NetScout/rtm/bin/stop
/opt/NetScout/rtm/bin/start
```

67 nGeniusOne and InfiniStream SSH:

a) Navigate to the indicated directory:
```
cd /etc/pam.d
```

b) Make backup copies of the following two files, as indicated:
```
cp password-auth password-auth.bak
```
```
cp system-auth system-auth.bak
```

c) Edit the password-auth file:
```
sudoedit /etc/pam.d/password-auth-local
```

d) To configure lockout attempts and duration, locate and edit the line indicated below.
```
auth required pam_faillock.so preauth silent audit deny=3
unlock_time=600
```

Where: deny - allows you to set the value N (no. of attempts) after which the user account should be locked.
unlock_time - is the time in seconds for which the account should stay locked.

e) Save and exit the file.

f) Edit the system-auth file and perform the same edits.

g) Reboot the TOE to apply the changes:

h) Configure public key authentication by adding public keys to the `authorized_keys` file under with: `sudoedit /home/backups/.ssh/authorized_keys`

68 Any interface can be locked out except for the serial console. This ensures that administrator access can always be maintained. The "unlocker" user can use the `sudo faillock --user backups –reset` to maintain access to the backups user.

69 Follow instructions at [INSTALL] Configuration section of the *Viewing and Managing User Accounts* chapter of *nGeniusONE v6.3 Configuration Essentials for Administrators* to disable lockout mechanism.

70 Passwords can be composed of any combination of upper and lower case letters, numbers, and special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", ")".

71 The minimum password length is settable by the Administrator and can range from 5 to 255 characters. To configure the minimum password length for the Web GUI, refer to the [INSTALL] *Managing Passwords* chapter of *NETSCOUT Server Administrator Guide*. To configure the minimum password length for CLI users, modify the `/etc/security/pwquality.conf minlen` value.

3.8 Trusted Channel

72 The TOE implements a TLS client for the trusted channel with its components.

73 The TOE web GUI is accessed via an HTTPS connection using the TLS implementation described by FCS_TLSS_EXT.1. The TOE does not use HTTPS in a client capacity. The TOE's HTTPS protocol complies with RFC 2818.

74 RFC 2818 specifies HTTP over TLS. The majority of RFC 2818 is spent on discussing practices for validating endpoint identities and how connections must be setup and torn down. The TOE web GUI operates on an explicit port designed to natively speak TLS: it does not attempt STARTTLS or similar multi-protocol negotiation which is described in section 2.3 of RFC 2818.

75 When a connection is broken during registration, no plaintext is sent. The administrator must re-initiate the connection. TLS will be used when the connection is established.

76 When a connection is broken during an operational connection, no plaintext is sent. The reconnect re-initiates the TCP handshake and TLS handshake. TLS will be reused when the connection is re-established.

77 The TOE performs certificate validity checking for the TLS connection between TOE components. As part of the certificate validation checking, the TSF will validate certificate revocation status using an OCSP server in the Operational Environment. If the revocation status cannot be verified, the certificate will be rejected.

78 The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The NG1 component supports a minimum path length of three certificates for its own web UI server certificate. While the InfiniStream component supports a minimum path length of 2 certificates for inter-TOE communication. In addition, the certificate path is terminated in a trusted CA certificate, the basicConstraints extension is present, and the CA flag is set to TRUE for all CA certificates. Finally, the TOE ensures the extendedKeyUsage field includes the Server Authentication purpose (id-kp 1 with

OID 1.3.6.1.5.5.7.3.1) for server certificates used in TLS, or the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) for OCSP certificates used for OCSP. When the validity of a certificate cannot be established due to a failed connection to the OCSP responder, the certificate not be accepted, no Administrator override is possible. Each TOE component certificate supports the use of the SAN extension.

79 To support HTTPS/TLS connectivity for the web UI interface and the inter-TOE component communication, the TSF of all components provide the ability to generate a Certificate Request Message as specified by RFC 2986 so that its server certificate can be signed by a Certification Authority. The message includes public key, Common Name, Organization, Organizational Unit, and Country values. The certificate chain of the Certificate Response is validated by the TSF prior to being installed as the TOE's server certificate.

80 Instructions for the NG1 to support HTTPS over TLS can be found in [INSTALL] *6.6.4 Configuring SSL/TLS* of the *NETSCOUT Server Administrator Guide.*

81 Communication between TOE components can be disabled by either removing the entry for InfiniStream from the **Device Configuration =**> **Devices** in the NG1 Web GUI or by performing a `/opt/NetScout/rtm/bin/stop` on the InfiniStream device. Once the InfiniStream is removed from the device list the NG1 can no longer communicate with the InfiniStream.

82 The minimum configuration is the deployment of an NG1 and one InfiniStream. Multiple InfiniStreams can be deployed and maintain their own separate communication channels with the NG1 and external IT entities that comply with FPT_ITT.1 and FTP_ITC.1. The InfiniStreams do not communicate with each other.

83 The TOE components communicate with each other over HTTPS/TLS. The connection makes use of elliptic curve certificates and ciphersuites. To perform initial setup of this channel and supply it with the appropriate keys and algorithms, use the following instructions:

a) Run the following commands to create a new certificate for the InfiniStream:

```
sudo -u ngenius /home/ngenius/create_key_and_csr.sh
```

b) Respond to the following prompts:

Country Name (2 letter code) [XX]:

State or Province Name (full name) []:

Locality Name (eg, city) [Default City]:

Organization Name (eg, company) [Default Company Ltd]:

Organizational Unit Name (eg, section) []:

Common Name (hostname) []:

Email Address []:

c) The server certificate will requires a DNS either in the SAN or the CN field to match the configured reference identifier. IP addresses are not supported.

d) Submit the CSR to your Certificate Authority (CA) for signing. Once it is approved, download the signed certificate along with the root and any intermediate certificates for the complete certificate chain.

e) Upload the certificates and key obtained from your Certificate Authority to `/home/backups` and run `sudo -u ngenius /home/ngenius/load_cert.sh <host_cert> <signing_cert>`

f) Under the `/opt/NetScout/rtm/bin` perform a `./start`

g) Restrict access to the InfiniStream from NG1 with `./add_http_access_list.sh <NG1 IP>`

h) Call `./localconsole`

i) If the NG1 server IP address is not displayed in the row for Change Config Server Address, press **4**, then Enter to input the correct address.

j) Select the options to [5] Change Read Community and [6] Change Write Community and set these to Public

k) Press [11] and then [Enter] to Enter Command-line mode of the utility.

l) Run the following: `set access_list 1 <NG1 IP> 255.255.255.255 rw`

m) Verify the change you made has occurred: `get access_list`

n) Exit the command line utility: `exit`

o) Modify the `/opt/NetScout/rtm/bin/procmanager.env` with the following

```
export PROCMANAGER_DBGL=8
export CLEANUPENGINE_DBGL=8
export TFAENGINE_DBGL=8
export HTTPENGINE_DBGL=8
export COMMD_DBGL=8
export NS_HTTP_PATH=/opt/NetScout/www
export NS_SSL_CERT_FILE=/opt/NetScout/config/is.pem
export NS_SSL_CA_FILE=/opt/NetScout/config/is.pem
export NSPROCPORT=80
export NSPROCPORT_SECURED=443
export NS_PROCMANAGER_PORT=8080
export NS_PROCMANAGER_PORT_SECURED=8443
```

p) From the operating system command-line, restart the InfiniStream application software, to invoke it with the changes you made:

```
./stopall
./start
```

84 To establish the trusted channel between TOE components, complete the following instructions:

a) Import the InfiniStream Root CA into the NG1 trust store with the following:

   i) Copy the Root CA to the NG1 `/opt/certs` directory.

   ii) Execute `/opt/NetScout/rtm/tools/nscertutil.sh`

   iii) Choose option [3] Add a .crt certificate to the truststore

   iv) Enter the path of the Root CA `/opt/certs/<cert>.crt`

b) Using the NG1 Web GUI, go to **Device Configuration =**> **Devices.** Click **Add**.

c) Enter the following values:

Name: InfiniStream

Alias: (optional)

Address: <FQDN >

Description: (optional)

Device Type: InfiniStream

Communication Protocol: Automatic

Read and Write Community: PUBLIC, PUBLIC

HTTP/HTTPS Port: <default 8443>

d) Modify `/opt/NetScout/rtm/bin/append_java.security`

```
ocsp.enable=true
```

e) `/opt/NetScout/rtm/bin/serverprivate.properties`

`SSLHelper.verifyCertificatesCC=true` (enabled by default with this property)

f) Modify `/opt/NetScout/rtm/bin/bootstrapconfig/masterconfig/ProcessMaster.xml.` Uncomment the following 3 properties:

```
<!-- The following 3 properties are required for common criteria configuration -->
<Param name="-Dcom.sun.net.ssl.checkRevocation">true</Param >
<Param name="-Dcom.sun.security.enableAIAcaIssuers">true</Param>
<Param name="-Dorg.bouncycastle.pkix.disable_certpath">true</Param>
```

3.9 Starting and Stopping Services

85 The starting and stopping of services is restricted to Security Administrators. Use the following commands to start and stop services.

a) `/opt/NetScout/rtm/bin/start` - start all TOE services

b) `/opt/NetScout/rtm/bin/stop` - stop all TOE services

Annex A: Log Reference

3.10 Format

86 Each audit record includes the following fields:

a) Timestamp

b) Type (SERVICE_START, etc)

c) Message (including user if applicable and indication of success or failure)

87 Refer [USER] *Directing Log Messages to an External Server* section of *InfiniStreamNG Certified/Hardware Appliance Administrator Guide, v6.3.*

3.11 Events

88 The TOE generates the following log events.

Table 4: Audit Events

Requirement	Audit Events	Examples
FAU_GEN.1	Start-up and shutdown of the audit functions	NG1: 2021-03-08T15:55:11-05:00 NG1 tag_audit_log: type=SERVICE_START msg=audit(1615218909.175:3556183): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=sys tem_u:system_r:init_t:s0 msg='unit=ngp-audit-tunnel comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' 2021-03-08T15:55:11-05:00 NG1 tag_sys_msg: Mar 8 15:55:08 NG1 systemd: Stopped SSH tunnel for remote audit daemon. 2021-03-08T15:55:11-05:00 NG1 tag_sys_msg: Mar 8 15:55:08 NG1 systemd: Starting SSH tunnel for remote audit daemon... 2021-03-08T15:55:11-05:00 NG1 tag_sys_msg: Mar 8 15:55:08 NG1 ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 15:55:08 GMT 2021] INFO: Audit log forwarding tunnel starting ... 2021-03-08T15:55:11-05:00 NG1 tag_sys_msg: Mar 8 15:55:09 NG1 ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 15:55:09 GMT 2021] INFO: Audit log forwarding tunnel to 10.100.1.156 started. PID 5855 2021-03-08T15:55:11-05:00 NG1 tag_sys_msg: Mar 8 15:55:09 NG1 ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 15:55:09 GMT 2021] INFO: Audit log health monitor started.

Requirement	Audit Events	Examples
		Infinistream: 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream systemd: Starting SSH tunnel for remote audit daemon... 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 16:08:22 GMT 2021] INFO: Audit log forwarding tunnel starting ... 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 16:08:22 GMT 2021] INFO: Audit log forwarding tunnel to 10.100.1.156 started. PID 121594 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 16:08:22 GMT 2021] INFO: Audit log health monitor started. 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream systemd: Started SSH tunnel for remote audit daemon. 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream systemd: Stopping SSH tunnel for remote audit daemon... 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 16:08:22 GMT 2021] INFO: Audit log health monitor is stopped 2021-03-08T16:08:24-05:00 infinistream tag_sys_msg: Mar 8 16:08:22 infinistream ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 16:08:22 GMT 2021] INFO: Audit log forwarding tunnel is stopped
	Administrative login and logout	2021-03-08T16:29:25-05:00 NG1 tag_audit_log: type=USER_AUTH msg=audit(1615220962.787:3663588): pid=11056 uid=0 auid=4294967295 ses=4294967295 subj=sys tem_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_securetty,pam_faillock,pam_unix acct="backups" exe="/usr/bin/login " hostname=NG1.example.com addr=? terminal=ttyS1 res=success' Feb 8 21:17:48 127.0.0.1 tag_audit_log: type=USER_END msg=audit(1612819059.765:11388): pid=14029 uid=0 auid=0 ses=1056

Requirement	Audit Events	Examples
		msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits, pam_systemd,pam_unix,pam_lastlog acct="root" exe="/usr/sbin/sshd" hostname=172.16.200.22 addr=172.16.200.22 terminal=ssh res=success' 2021-03-08T19:38:15-05:00 NG1 tag_audit_log: type=USER_END msg=audit(1615232292.737:4207614): pid=22937 uid=0 auid=1001 ses=130 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits, pam_sy stemd,pam_unix,pam_lastlog,pam_lastlog acct="backups" exe="/usr/sbin/sshd" hostname=172.16.200.22 addr=172.16.200.22 terminal=ssh res=success'
	Changes to TSF data related to configuration changes	NG1 Serial 2021-03-08T17:07:10-05:00 NG1 tag_sys_msg: Mar 8 17:07:07 NG1 login: pam_faillock(login:auth): Consecutive login failures for user backups account temporarily lockedNG1 Web GUI NG1 SSH 2021-03-08T16:40:07-05:00 NG1 tag_sys_msg: Mar 8 16:40:06 NG1 sshd[16829]: error: maximum authentication attempts exceeded for backups from 172.16.200.22 port 55871 ssh2 [preauth] Infinistream Serial 2021-03-08T17:20:49-05:00 infinistream tag_sys_msg: Mar 8 17:20:40 infinistream login: pam_faillock(login:auth): Consecutive login failures for user backups account temporarily locked Infinistream SSH 2021-03-08T17:43:01-05:00 infinistream tag_sys_msg: Mar 8 17:42:56 infinistream sshd[133968]: pam_faillock(sshd:auth): Consecutive login failures for user backups account temporarily locked

Requirement	Audit Events	Examples
	Generating/import of, changing, or deleting of cryptographic keys	NG1: 2022-01-27 21:16:03 netscout program[2230]: Generating ssh tunnel keys 2022-01-27 21:16:03 netscout program[2230]: Generate new ssh tunnel keys: 2022-01-27 21:16:03 netscout program[2230]: Backup old keys 2022-01-27 21:16:03 netscout program[2230]: Generating new keys 2022-01-27 21:16:03 netscout program[2230]: Log-audit ssh tunnel keys created on 20220127160814. Infinistream: 2021-03-15T21:20:18-04:00 infinistream tag_sys_msg: Mar 15 21:20:11 infinistream nGP.Admin: File: [audit.key] shredded by root. 2021-03-15T21:20:18-04:00 infinistream tag_sys_msg: Mar 15 21:20:11 infinistream nGP.Admin: File: [audit.key.pub] shredded by root. 2021-03-15T21:20:18-04:00 infinistream tag_sys_msg: Mar 15 21:20:11 infinistream nGP.Admin: New ssh tunnel keys generated by root.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	This test is now performed as part of FIA_X509_EXT.1/Rev testing.
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Tue Jun 07 15:22:10 GMT 2022: 0,local,An internal error has occured., Details: Connect to 10.20.23.11:8080 [/10.20.23.11] failed: Connection refused (Connection refused); Tue Jun 07 14:53:50 GMT 2022: 0,local,Device is not reachable using SNMP, either SNMP is not supported or read/write community is incorrect., Details: 10.20.23.11/HTTPS, Severity: 3, Code: 8034 10.20.23.11/HTTPS, Severity: 3, Code: 8034
FCS_TLSS_EXT.1	Failure to establish a TLS Session	NG1: [Tue Jun 07 18:25:00.055124 2022] [ssl:info] [pid 7787:tid 139638555461376] SSL Library Error: error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown (SSL alert number 46) [Tue Apr 18 17:27:22.635878 2023] [ssl:info] [pid 168482:tid 139663620671232] SSL Library Error: error:1408F10B:SSL

Requirement	Audit Events	Examples
		routines:SSL3_GET_RECORD:wrong version number [Tue Apr 18 17:25:02.835244 2023] [ssl:info] [pid 168482:tid 139663637456640] SSL Library Error: error:1408F119:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac [Tue Apr 18 17:22:45.908744 2023] [ssl:info] [pid 168482:tid 139663645849344] SSL Library Error: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate? Infinistream: 2021-03-08T22:38:53-05:00 infinistream tag_sys_msg: Mar 8 22:38:51 infinistream procmanager[11049]: ERRDBG nsssl.cpp[645] pid:11049 - ThreadID:186205952 Connection ID: [10.100.1.156]:43798 Error: SSL_ERROR_SSL - a failure in the SSL library occurred 2021-03-08T22:38:53-05:00 infinistream tag_sys_msg: Mar 8 22:38:51 infinistream procmanager[11049]: ERRDBG nsssl.cpp[648] pid:11049 - error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher 2021-03-08T22:38:53-05:00 infinistream tag_sys_msg: Mar 8 22:38:51 infinistream procmanager[11049]: ERRDBG nsssl.cpp[460] pid:11049 - ThreadID:186205952 Connection ID: [10.100.1.156]:43798 Error in SSL Handshake. rc=-1 2021-03-08T22:38:53-05:00 infinistream tag_sys_msg: Mar 8 22:38:51 infinistream procmanager[11049]: INFDBG2 nsssl.cpp[534] pid:11049 - ThreadID:186205952 Connection ID: [10.100.1.156]:43798 SSL connection CLOSE [cipher = (NONE), version = TLSv1.2, mode = server]
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	NG1: Sent 1024*256 bytes over ssh, connection closed. 2021-02-22T18:25:08-05:00 NG1 tag_audit_log: type=CRYPTO_KEY_USER msg=audit(1614018307.688:10452): pid=23708 uid=0 auid=1001 ses=988 msg='op=destroy kind=session fp=? direction=both spid=23719 suid=1001 rport=41078 laddr=10.20.23.10 lport=22 exe="/usr/sbin/sshd" hostname=? addr=10.100.1.156 terminal=? res=success'

Requirement	Audit Events	Examples
		2021-02-22T18:25:08-05:00 NG1 tag_audit_log: type=USER_END msg=audit(1614018307.690:10453): pid=23708 uid=0 auid=1001 ses=988 msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_lastlog,pam_lastlog acct="backups" exe="/usr/sbin/sshd" hostname=10.100.1.156 addr=10.100.1.156 terminal=ssh res=success' Infinistream: Sent 1024*256 bytes over ssh, connection closed.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	NG1 local Success 2021-03-08T16:29:25-05:00 NG1 tag_audit_log: type=USER_AUTH msg=audit(1615220962.787:3663588): pid=11056 uid=0 auid=4294967295 ses=4294967295 subj=sys tem_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_securetty,pam_faillock,pam_unix acct="backups" exe="/usr/bin/login " hostname=NG1.example.com addr=? terminal=ttyS1 res=success' Failure 2021-03-08T16:15:34-05:00 NG1 tag_audit_log: type=USER_AUTH msg=audit(1615220130.383:3623848): pid=13734 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=? acct="backups" exe="/usr/bin/login" hostname=NG1.example.com addr=? terminal=ttyS1 res=failed' NG1 SSH success 2021-03-08T16:25:45-05:00 NG1 tag_audit_log: type=USER_AUTH msg=audit(1615220738.284:3658244): pid=13548 uid=0 auid=4294967295 ses=4294967295 subj=sys
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	

Requirement	Audit Events	Examples
		tem_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=success acct="backups" exe="/usr/sbin/sshd" hostname=? addr=172.16.200.22 terminal=ssh res=success' failure 2021-03-08T16:17:04-05:00 NG1 tag_audit_log: type=USER_AUTH msg=audit(1615220219.958:3625769): pid=11282 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=password acct="backups" exe="/usr/sbin/sshd" hostname=? addr=172.16.200.22 terminal=ssh res=failed' InfiniStream ssh Success 2021-03-08T16:40:06-05:00 infinistream tag_sys_msg: Mar 8 16:40:01 infinistream sshd[125729]: Connection from 172.16.200.22 port 55756 on 10.20.23.11 port 22 2021-03-08T16:40:06-05:00 infinistream tag_sys_msg: Mar 8 16:40:01 infinistream sshd[125729]: reprocess config line 54: Deprecated option RSAAuthentication 2021-03-08T16:40:06-05:00 infinistream tag_sys_msg: Mar 8 16:40:01 infinistream sshd[125729]: reprocess config line 59: Deprecated option RhostsRSAAuthentication 2021-03-08T16:40:06-05:00 infinistream tag_sys_msg: Mar 8 16:40:02 infinistream sshd[125729]: Accepted password for backups from 172.16.200.22 port 55756 ssh2 failure 2021-03-08T16:26:05-05:00 infinistream tag_sys_msg: Mar 8 16:25:55 infinistream sshd[123861]: Connection from 172.16.200.22 port 55561 on 10.20.23.11 port 22 2021-03-08T16:26:05-05:00 infinistream tag_sys_msg: Mar 8 16:25:56 infinistream sshd[123861]: reprocess config line 54: Deprecated option RSAAuthentication 2021-03-08T16:26:05-05:00 infinistream tag_sys_msg: Mar 8 16:25:56 infinistream sshd[123861]: reprocess config line 59: Deprecated option RhostsRSAAuthentication

Requirement	Audit Events	Examples
		2021-03-08T16:26:05-05:00 infinistream tag_sys_msg: Mar 8 16:25:57 infinistream unix_chkpwd[123868]: password check failed for user (backups) 2021-03-08T16:26:05-05:00 infinistream tag_sys_msg: Mar 8 16:25:57 infinistream sshd[123861]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.200.22 user=backups 2021-03-08T16:26:05-05:00 infinistream tag_sys_msg: Mar 8 16:25:59 infinistream sshd[123861]: Failed password for backups from 172.16.200.22 port 55561 ssh2 InfiniStream local: Success 2021-03-08T16:39:06-05:00 infinistream tag_sys_msg: Mar 8 16:39:00 infinistream systemd-logind: New session 107 of user backups. 2021-03-08T16:39:06-05:00 infinistream tag_sys_msg: Mar 8 16:39:00 infinistream login: pam_unix(login:session): session opened for user backups by LOGIN(uid=0) 2021-03-08T16:39:06-05:00 infinistream tag_sys_msg: Mar 8 16:39:00 infinistream login: DIALUP AT ttyS0 BY backups 2021-03-08T16:39:06-05:00 infinistream tag_sys_msg: Mar 8 16:39:00 infinistream login: LOGIN ON ttyS0 BY backups failure 2021-03-08T16:15:04-05:00 infinistream tag_sys_msg: Mar 8 16:14:56 infinistream unix_chkpwd[122428]: password check failed for user (backups) 2021-03-08T16:15:04-05:00 infinistream tag_sys_msg: Mar 8 16:14:56 infinistream login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=ttyS0 ruser= rhost= user=backups 2021-03-08T16:15:04-05:00 infinistream tag_sys_msg: Mar 8 16:14:59 infinistream login: FAILED LOGIN SESSION FROM ttyS0 FOR backups, Permission denied

Requirement	Audit Events	Examples
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Mon Jun 06 19:22:45 GMT 2022: 0,local,An internal error has occured., Details: PKIX path validation failed: java.security.cert.CertPathValidatorException: TrustAnchor found but certificate validation failed.; java.base/sun.security.ssl.Alert.createSSLException(Alert.java:131), Severity: 3, Code: 17 Mon Jun 06 19:22:45 GMT 2022: 0,local,An internal error has occured., Details: PKIX path validation failed: java.security.cert.CertPathValidatorException: TrustAnchor found but certificate validation failed.; java.base/sun.security.ssl.Alert.createSSLException(Alert.java:131), Severity: 3, Code: 17 javax.net.ssl.SSLHandshakeException: PKIX path validation failed: java.security.cert.CertPathValidatorException: TrustAnchor found but certificate validation failed. at java.base/sun.security.ssl.Alert.createSSLException(Alert.java:131) at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:349) at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:292) at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:287) at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.checkServerCerts(CertificateMessage.java:654) at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.onCertificate(CertificateMessage.java:473) at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.consume(CertificateMessage.java:369) at java.base/sun.security.ssl.SSLHandshake.consume(SSLHandshake.java:392) at java.base/sun.security.ssl.HandshakeContext.dispatch(HandshakeContext.java:443)

Requirement	Audit Events	Examples
		at java.base/sun.security.ssl.HandshakeContext.dispatch(HandshakeContext.java:421) at java.base/sun.security.ssl.TransportContext.dispatch(TransportContext.java:182) at java.base/sun.security.ssl.SSLTransport.decode(SSLTransport.java:172) at java.base/sun.security.ssl.SSLSocketImpl.decode(SSLSocketImpl.java:1426) at java.base/sun.security.ssl.SSLSocketImpl.readHandshakeRecord(SSLSocketImpl.java:1336) at java.base/sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:450) at java.base/sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:421) at org.apache.http.conn.ssl.SSLConnectionSocketFactory.createLayeredSocket(SSLConnectionSocketFactory.java:436) at org.apache.http.conn.ssl.SSLConnectionSocketFactory.connectSocket(SSLConnectionSocketFactory.java:384) at org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultHttpClientConnectionOperator.java:142) at org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHttpClientConnectionManager.java:374) at org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.java:393)
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate	NG1: Tue Jun 07 15:22:10 GMT 2022: 0,local,An internal error has occured., Details: PKIX path validation failed: java.security.cert.CertPathValidatorException: TrustAnchor found but certificate validation failed.;

Requirement	Audit Events	Examples
	Any addition, replacement or removal of trust anchors in the TOE's trust store	java.base/sun.security.ssl.Alert.createSSLException(Alert.java:131), Severity: 3, Code: 17 Tue Jun 07 15:22:10 GMT 2022: 0,local,An internal error has occured., Details: PKIX path validation failed: java.security.cert.CertPathValidatorException: TrustAnchor found but certificate validation failed.; java.base/sun.security.ssl.Alert.createSSLException(Alert.java:131), Severity: 3, Code: 17 Wed Jun 08 15:54:43 GMT 2022 Executing following command : /opt/NetScout/jre64/bin/keytool -import -file /opt/certs/test_ca.crt -alias NewTestCert -keystore /opt/NetScout/rtm/html/ngeniusclient.truststore -storepass ***** -noprompt /opt/certs/test_ca.crt Imported Wed Jun 08 18:10:02 GMT 2022 Executing following command : /opt/NetScout/jre64/bin/keytool -delete -storepass ***** -alias newtestcert -keystore /opt/NetScout/rtm/html/ngeniusclient.truststore newtestcert deleted Infinistream: 2022-06-07 07:19:02 infinistream procmanager[277189]: ERRDBG nsssl.cpp[648] pid:277189 - error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	See FCS_TLSC_EXT.1 NG1 and FCS_TLSS_EXT.1 Infinistream logs
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	Wed Apr 27 11:27:40 GMT 2022 decodeengine.version = Version 6.3.3 Build1093 Wed Apr 27 11:39:04 GMT 2022

Requirement	Audit Events	Examples
		Free Memory: 40564 kB Total Memory: 71680 kB 2 Command Line Args: 0: -m 1: CONSOLE java.class.path: /tmp/install.dir.10587/InstallerData /tmp/install.dir.10587/InstallerData/installer.zip ZGUtil.CLASS_PATH: /tmp/install.dir.10587/InstallerData /tmp/install.dir.10587/InstallerData/installer.zip sun.boot.class.path: <none specified> java.ext.dirs: <none specified> java.version == 11.0.13 (Java 1) java.vm.name == OpenJDK 64-Bit Server VM java.vm.vendor == Eclipse Adoptium java.vm.version == 11.0.13+8 java.vm.specification.name == Java Virtual Machine Specification java.vm.specification.vendor == Oracle Corporation java.vm.specification.version == 11 java.specification.name == Java Platform API Specification java.specification.vendor == Oracle Corporation java.specification.version == 11 java.vendor == Eclipse Adoptium

Requirement	Audit Events	Examples
		java.vendor.url == https://adoptium.net/ java.class.version == 55.0 java.library.path == /usr/java/packages/lib:/usr/lib64:/lib64:/lib:/usr/lib java.compiler == null java.home == /tmp/install.dir.10587/Linux/resource/jre java.io.tmpdir == /tmp os.name == Linux os.arch == amd64 os.version == 3.10.0-1062.18.1.el7.x86_64 path.separator == : file.separator == / file.encoding == UTF-8 user.name == root user.home == /root user.dir == /tmp/install.dir.10587 user.language == en user.region == null Installed Feature(s) Upgrade2 of nGeniusONE Install Begin: APRIL 27, 2022 11:17:05 AM GMT Install End: APRIL 27, 2022 11:39:03 AM GMT Installed by InstallAnywhere 19.0 Premier Build 6112 Infinistream: Mon Nov 08 08:06:22 GMT 2021 Free Memory: 87824 kB Total Memory: 188928 kB

Requirement	Audit Events	Examples
		4 Command Line Args: 0: -l 1: en 2: -m 3: CONSOLE java.class.path: /tmp/install.dir.12403/InstallerData /tmp/install.dir.12403/InstallerData/installer.zip ZGUtil.CLASS_PATH: /tmp/install.dir.12403/InstallerData /tmp/install.dir.12403/InstallerData/installer.zip sun.boot.class.path: /tmp/install.dir.12403/Linux/resource/jre/lib/resources.jar /tmp/install.dir.12403/Linux/resource/jre/lib/rt.jar /tmp/install.dir.12403/Linux/resource/jre/lib/sunrsasign.jar /tmp/install.dir.12403/Linux/resource/jre/lib/jsse.jar /tmp/install.dir.12403/Linux/resource/jre/lib/jce.jar /tmp/install.dir.12403/Linux/resource/jre/lib/charsets.jar /tmp/install.dir.12403/Linux/resource/jre/lib/jfr.jar /tmp/install.dir.12403/Linux/resource/jre/classes java.ext.dirs: /tmp/install.dir.12403/Linux/resource/jre/lib/ext /usr/java/packages/lib/ext java.version == 1.8.0_101 (Java 1) java.vm.name == Java HotSpot(TM) Server VM java.vm.vendor == Oracle Corporation

Requirement	Audit Events	Examples
		java.vm.version == 25.101-b13 java.vm.specification.name == Java Virtual Machine Specification java.specification.vendor == Oracle Corporation java.specification.version == 1.8 java.vendor == Oracle Corporation java.vendor.url == http://java.oracle.com/ java.class.version == 52.0 java.library.path == /usr/java/packages/lib/i386:/lib:/usr/lib java.compiler == null java.home == /tmp/install.dir.12403/Linux/resource/jre java.io.tmpdir == /tmp os.name == Linux os.arch == i386 os.version == 3.10.0-1127.13.1.el7.x86_64 path.separator == : file.separator == / file.encoding == UTF-8 user.name == root user.home == /root user.dir == /tmp/install.dir.12403 user.language == en user.region == null Installed Feature(s) RTM of nGenius InfiniStream Install Begin: NOVEMBER 8, 2021 8:01:02 PM GMT Install End: NOVEMBER 8, 2021 8:06:20 PM GMT Installed by InstallAnywhere 17.0 Premier Build 5158

Requirement	Audit Events	Examples
FMT_SMF.1	All management activities of TSF data.	NG1: 2022-06-08 18:23:25 netscout5.catl.local sudo: backups : TTY=pts/2 ; PWD=/home/backups ; USER=root ; COMMAND=/bin/vi /etc/issue 2022-06-08 18:30:42 netscout5.catl.local sudo: backups : TTY=pts/2 ; PWD=/home/backups ; USER=root ; COMMAND=/bin/vi .bashrc Infinistream: 2022-06-08 10:53:29 infinistream sudo: backups : command not allowed ; TTY=pts/2 ; PWD=/home/backups ; USER=root ; COMMAND=/bin/vi .bashrc
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	NG1: Tue May 09 02:47:39 EDT 2023 Free Memory: 28374 kB Total Memory: 65536 kB 2 Command Line Args: 0: -m 1: CONSOLE java.class.path: /tmp/install.dir.23754/InstallerData /tmp/install.dir.23754/InstallerData/installer.zip ZGUtil.CLASS_PATH: /tmp/install.dir.23754/InstallerData /tmp/install.dir.23754/InstallerData/installer.zip sun.boot.class.path: <none specified>

Requirement	Audit Events	Examples
		java.ext.dirs: <none specified> java.version == 11.0.18 (Java 1) java.vm.name == OpenJDK 64-Bit Server VM java.vm.vendor == Eclipse Adoptium java.vm.version == 11.0.18+10 java.vm.specification.name == Java Virtual Machine Specification java.vm.specification.vendor == Oracle Corporation java.vm.specification.version == 11 java.specification.name == Java Platform API Specification java.specification.vendor == Oracle Corporation java.specification.version == 11 java.vendor == Eclipse Adoptium java.vendor.url == https://adoptium.net/ java.class.version == 55.0 java.library.path == /usr/java/packages/lib:/usr/lib64:/lib64:/lib:/usr/lib java.compiler == null java.home == /tmp/install.dir.23754/Linux/resource/jre ...skipping... Execute Script/Batch file: SSD-21925-> check for string "HSTS" in httpd-ssl-custom.conf Status: SUCCESSFUL Modify Text File - Single File: /opt/NetScout/rtm/bin/httpd-ssl-custom.conf Status: SUCCESSFUL Execute Script/Batch file: SSD-22043-> check for string "SecureSitein httpd-custom.conf Status: SUCCESSFUL

Requirement	Audit Events	Examples
		Execute Script/Batch file: SSD-22235 execute the following script only during upgarde -Linux Status: SUCCESSFUL Execute Script/Batch file: SSD-18979 - execute the following script only during upgarde Status: SUCCESSFUL Modify Text File - Single File: New File /opt/NetScout/rtm/pmupgrade/installerstatus.log Status: SUCCESSFUL Execute Script/Batch file: Add Entries in /etc/sudoers Status: SUCCESSFUL Execute Script/Batch file: Modify nGeniusReg.properties - Linux Status: SUCCESSFUL Execute Script/Batch file: remove postgresql10-* and s2pm-*.rpm Status: SUCCESSFUL Execute Script/Batch file: remove .gitignore files after installation. Status: SUCCESSFUL Delete Folder: Source:infinidb Status: SUCCESSFUL InfiniStream:

Requirement	Audit Events	Examples
		2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: Removing nt3gd_0000:86:00.0 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: destroy: commencing total teardown 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: destroy: teardown of dmapool[0] 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: DMA pool statistics for NUMA 0: 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: Total DMA memory allocations : 0 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: Maximum simultaneous allocation: 0 B 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: destroy: teardown of dmapool[0] complete 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: destroy: teardown of dmapool[1] 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: DMA pool statistics for NUMA 1: 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: Total DMA memory allocations : 0 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: Maximum simultaneous allocation: 0 B 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: destroy: teardown of dmapool[1] complete

Requirement	Audit Events	Examples
		2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: ntdmapool: destroy: total teardown complete 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream kernel: nt3g: nt3gd: Napatech 3GD (3.19.1.6-9ff0b-NT) kernel component unloaded. 2021-03-09T00:54:43-05:00 infinistream tag_sys_msg: Mar 9 00:54:41 infinistream systemd: Reloading.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	NG1: Feb 8 23:50:05 127.0.0.1 tag_audit_log: type=SERVICE_STOP msg=audit(1612824736.019:11578): pid=1 uid=0 auid=4294967295 ses=4294967295 msg='unit=systemd-timedated comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' Feb 8 23:50:05 127.0.0.1 tag_audit_log: type=SERVICE_START msg=audit(1612824739.074:11579): pid=1 uid=0 auid=4294967295 ses=4294967295 msg='unit=systemd-timedated comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' Infinistream: 2021-03-08T17:05:36-05:00 infinistream tag_sys_msg: Mar 8 17:05:30 infinistream systemd-timedated: Changed local time to Mon Mar 8 17:05:30 2021
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	NG1: 2021-03-08T19:03:11-05:00 NG1 tag_audit_log: type=USER_END msg=audit(1615230184.159:4088398): pid=24411 uid=0 auid=1001 ses=123 subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_console,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_lastlog,pam_lastlog acct="backups" exe="/usr/bin/login" hostname=NG1.example.com addr=? terminal=ttyS1 res=success'

Requirement	Audit Events	Examples
		Infinistream: 2021-03-08T17:14:16-05:00 infinistream tag_sys_msg: Mar 8 17:14:10 infinistream bash[171695]: timed out waiting for input on /dev/ttyS0 (user backups): auto-logout 2021-03-08T17:14:16-05:00 infinistream tag_sys_msg: Mar 8 17:14:10 infinistream login: pam_unix(login:session): session closed for user backups
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	NG1: Jun 6 22:08:00 NG1.example.com nGenius User = ADMINISTRATOR IP Address = 172.16.200.30 Description = User session removed due to inactivity User ID: ADMINISTRATOR idle session timeout logged from Client IP: 172.16.200.30 Host Name: X.X.X.X SUCCESSFUL Feb 10 21:23:31 127.0.0.1 audispd: node=infinistream type=USER_END msg=audit(1612992211.266:19646422): pid=263057 uid=0 auid=0 ses=1230 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_lastlog acct="root" exe="/usr/sbin/sshd" hostname=172.16.200.22 addr=172.16.200.22 terminal=ssh res=success' Feb 10 22:46:01 127.0.0.1 tag_audit_log: type=USER_END msg=audit(1612997152.716:15255): pid=32651 uid=0 auid=0 ses=1425 msg='op=PAM:session_close gran tors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_lastlog acct="root" exe="/usr/sbin /sshd" hostname=X.X.X.X addr=X.X.X.X terminal=ssh res=success'
FTA_SSL.4	The termination of an interactive session.	NG1: 2021-03-08T19:22:34-05:00 NG1 tag_audit_log: type=USER_END msg=audit(1615231345.888:4156080): pid=14143

Requirement	Audit Events	Examples
		uid=0 auid=1001 ses=128 subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_console,pam_selinux,pam_namespace,pam_keyinit,pam_keyini t,pam_limits,pam_systemd,pam_unix,pam_lastlog,pam_lastlog acct="backups" exe="/usr/bin/login" hostname=NG1.example.com addr=? terminal=ttyS1 res=success' Infinistream: 2021-03-08T17:32:18-05:00 infinistream tag_sys_msg: Mar 8 17:32:13 infinistream login: pam_unix(login:session): session closed for user backups
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	NG1 : 2021-03-08T20:57:13-05:00 NG1 tag_sys_msg: Mar 8 20:57:04 NG1 ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 20:57:04 GMT 2021] ERROR: The log audit forwarding tunnel is not running, check ngp-log-audit and restart the service. Remote Host: 10.100.1.156 Infinistream: Mar 8 19:06:20 infinistream ngp-audit-tunnel.sh: [ngp-audit-tunnel Mon Mar 8 19:06:20 GMT 2021] ERROR: The log audit forwarding tunnel is not running, check ngp-log-audit and restart the service. Remote Host: 10.100.1.156
FTP_TRP.1/ Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	NG1: Jun 7 17:07:16 NG1.example.com nGenius User = ADMINISTRATOR IP Address = X.X.X.X Description = User logged in User logged in from Client IP: X.X.X.X Host Name: X.X.X.X Browser Details: [Browser] Firefox/101.0 [Application] Applet SUCCESSFUL Jun 6 20:30:45 NG1.example.com nGenius User = ADMINISTRATOR IP Address = X.X.X.X Description = User logged out User logged out from Client IP: X.X.X.X Host Name: X.X.X.X SUCCESSFUL Jun 6 20:31:18 NG1.example.com nGenius User = ADMINISTRATOR IP Address = X.X.X.X Description = User login failed User login failed for

Requirement	Audit Events	Examples
		User Name: ADMINISTRATOR Client IP: X.X.X.X Host Name: X.X.X.X SUCCESSFUL Feb 17 20:25:38 NG1 tag_audit_log: type=USER_AUTH msg=audit(1613593536.671:1958): pid=11571 uid=0 auid=4294967295 ses=4294967295 msg='op=success acct="backups" exe="/usr/sbin/sshd" hostname=? addr=X.X.X.X terminal=ssh res=success' type=USER_END msg=audit(1654622410.571:40449762): pid=23950 uid=0 auid=1001 ses=2247 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_lastlog,pam_lastlog acct="backups" exe="/usr/sbin/sshd" hostname=X.X.X.X addr=X.X.X.X terminal=ssh res=success' Feb 17 20:24:48 NG1 tag_audit_log: type=USER_AUTH msg=audit(1613593483.891:1939): pid=11259 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication grantors=? acct="backups" exe="/usr/sbin/sshd" hostname=X.X.X.X addr=X.X.X.X terminal=ssh res=failed' Infinistream: 2022-06-07 09:45:41 infinistream sshd[23966]: Accepted password for backups from X.X.X.X port 56557 ssh2 2022-06-07 09:45:41 infinistream sshd[23966]: pam_unix(sshd:session): session opened for user backups by (uid=0) 2022-06-07 09:48:30 infinistream sshd[25295]: Failed password for backups from 172.16.200.22 port 56573 ssh2 2022-06-07 09:48:23 infinistream sshd[24000]: Disconnected from user backups X.X.X.X port 56557

Requirement	Audit Events	Examples
		2022-06-07 09:48:23 infinistream sshd[23966]: pam_unix(sshd:session): session closed for user backups