Gigamon GigaVUE
Version 6.1
Supplemental Administrative Guidance for Common Criteria

Version: 2.0
May 5, 2023

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054

Prepared By:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Table of Contents

List of Tables

1 Introduction

The Target of Evaluation (TOE) is the Gigamon GigaVUE version 6.1 Visibility Appliance (GigaVUE). The TOE includes the model types: HC3, HC2, HC1, TA25, TA200, GTAP-ASF21, and GTAP-ATX21 with Gigamon GigaVUE software version 6.1. These models allow an Administrator to access the TOE through a serial port and remote Command Line Interface (CLI) via SSH. The TOE was evaluated against the requirements defined in the Gigamon GigaVUE Security Target.

The GigaVUE's primary functionality is to use the Gigamon Forwarding Policy to receive out-of-band copied network data from external sources (TAP or SPAN port) and forward that copied network data to one or many tool ports for packet capture or analyzing tools based on user selected criteria. GigaVUE can also copy the network traffic itself when sitting in-line with the network flow using passive, inline and bypass taps or any combination. GigaVUE features extensive filtering abilities enabling authorized users to forward precise customized data flows of copied data from many sources to a single tool, from a single source to many tools, or from many sources to many tools. The TOE was evaluated as a network device only and the GigaVUE's network traffic capture, filter, and forwarding capabilities described above were not assessed during this evaluation. The TOE is the general network device functionality (I&A, auditing, security management, trusted communications, etc.) of the GigaVUE, consistent with the claimed Protection Profile.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating Gigamon GigaVUE version 6.1. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is expected to be familiar with the Security Target for Gigamon GigaVUE version 6.1 and the general CC terminology that is referenced in it.

This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions on how to perform only the security functions that are defined by these SFRs. Additionally, this document includes references to Gigamon GigaVUE's standard documentation set for the product which contains functionality that is outside the scope of the evaluation. The GigaVUE product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described in this supplemental document or in the Gigamon GigaVUE version 6.1 Security Target was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the Gigamon GigaVUE Security Target.

Administrator: A user who is assigned the 'Admin' role on the TOE and has the ability to manage the TSF. Synonymous with Security Administrator.

CC: Stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Security Administrator: An authorized administrator role that is authorized to manage the TOE and its data. This TOE defines two separate user roles, but only the most privileged role (Admin) is authorized to manage the TOE's security functionality and is therefore considered to be the Security Administrator for the TOE.

SFR: Stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: Stands for Target of Evaluation. This refers to the aspects of Gigamon GigaVUE that contain the security functions that were tested as part of the CC evaluation process.

4 References

The following documents are part of the Gigamon GigaVUE version 6.1. This is the standard documentation set that is provided with the product.

[1] Gigamon GigaVUE version 6.1 Security Target, v2.0 [ST]
[2] GigaVUE-OS CLI Reference Guide, GigaVUE-OS, v1.0, Product Version 6.1, Document Version 1.0
[3] GigaVUE-HC1 Hardware Installation Guide, GigaVUE H Series, v1.0 Product Version 6.1, Document Version 1.0
[4] GigaVUE-HC2 Hardware Installation Guide, GigaVUE H Series, v1.0 Product Version 6.1, Document Version 1.0
[5] GigaVUE-HC3 Hardware Installation Guide, GigaVUE H Series, v1.0 Product Version 6.1, Document Version 1.0
[6] GigaVUE TA25 Hardware Installation Guide, GigaVUE TA Series, v1.0 Product Version 6.1, Document Version 1.0
[7] GigaVUE TA200 Hardware Installation Guide, GigaVUE TA Series, v1.0 Product Version 6.1, Document Version 1.0
[8] GigaVUE G-TAP A Series 2 Hardware Installation Guide, G-TAP A-TX21, G-TAP A-TX21-C, G-TAP A-SF21, v1.0 Product Version 6.1, Document Version 1.0

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims:

5.1 TOE Components

GigaVUE is a rack-mounted hardware device. The GigaVUE is a modular device to accommodate many variations of physical connectivity including copper, fiber, 1G, 10G, 40G and 100G ports.

The model specific hardware and their configurations are as follows:

Property	HC3	HC2	HC1
Model Number	GVS-HC301 (AC power) GVS-HC302 (DC power)	GVS-HC2A1 (AC power) GVS-HC2A2 (DC power)	GVS-HC101 (AC power) GVS-HC102 (DC power)
Size	3RU	2RU	1RU
Processor	Intel Atom C2758	NXP QorIQ P2041E	Intel Atom C2538
TAP Modules	None	TAP-HC0-D25AC0 TAP module, SX/SR Internal TAP module 50/125, 12 TAPs TAP-HC0-D25BC0 TAP module, SX/SR Internal TAP module 62.5125, 12 TAPs TAP-HC0-D35CC0 TAP module, LX/LR Internal TAP module, 12 TAPs TAP-HC0-G100C0 TAP and Bypass Module, Copper, 12 TAP or BPS pairs	TAP-HC1-G10040 TAP and Bypass module, 10/100/1000M Copper, 4 TAPs or BPC pairs
Bypass Combo Modules	BPS-HC3-C25F26 Bypass Combo Module, GigaVUE-HC3, 2 100Gb SR4 BPS pairs, 16 10G cages	BPS-HC0-D25A4G Bypass Combo Module 4 SX/SR 50/125 BPS pairs, 16 10G cages BPS-HC0-D25B4G Bypass Combo Module 4 SX/SR 62.5/125 BPS pairs, 16 10G cages BPS-HC0-D35C4G Bypass Combo Module 4 LX/LR BPS pairs, 16 10G cages BPS-HC0-Q25A28 Bypass Combo Module 2 40G SR4 BPS pairs, 8 10G cages	BPS-HC1-D25A24 Bypass Combo Module, 2 SX/SR 50/125 BPS pairs, 4 10G cages
GigaSMART Modules	SMT-HC3-C05 GigaSMART, GigaVUE-HC3, 5x100G QSFP28 cages (includes Slicing, Masking, Source Port Tagging, and Tunneling De-	SMT-HC0-R GigaSMART, GigaVUE-HC2 rear module; SMT-HC0-X16 GigaSMART, GigaVUE-HC2 front module, 16 10G cages	SMT-HC1-S GigaSMART GigaVUE-HC1, Gen3: Processing up to 30G (includes Slicing, Masking, Source Port Tagging, and Tunneling De-encapsulation)

Property	HC3	HC2	HC1
	encapsulation)	(includes Slicing, Masking, Source Port Tagging, and Tunneling De-encapsulation)	
Port Modules	PRT-HC3-C08Q08 Port Module, 8x100G QSFP28 cages, 8x40 QSFP+ cages PRT-HC3-X24 Port Module, GigaVUE-HC3, 24x10G	PRT-HC0-X24 Port Module, 24x10G (QSFP) PRT-HC0-Q06 Port Module, 6x40G (QSFP+) PRT-HC0-C02 Port Module, 2x100G (QSFP28)	None
Fixed Ports	10/100/1000M Mgmt. port Serial Console	10/100/1000M Mgmt. port Serial Console	10/100/1000M Mgmt. port Serial Console 12 1G/10G Ports (QSFP) 4 10/100/1000M Ports
Configurable Ports (provided functionality out of scope as stated in Section 2.3.3)	Provided by Port Modules	Provided by TAP modules, Bypass Combo modules, Port Modules	Provided by TAP modules, Bypass Combo modules

Table 1: Hardware Models – HC Series Properties

Property	TA25	TA200
Model Number	GVS-TAX21-HW (AC power) • all ports on GVS-TAX22-HW (DC power) • all ports on GVS-TAX21A-HW (AC power) • 24 10G/25G ports enabled GVS-TAX22A-HW (DC power) • 24 10G/25G ports enabled	GVS-TAC21 (AC power) GVS-TAC22 (DC power)
Size	1RU	2RU
Processor	Intel Atom Processor C3538	Intel Xeon D1527
Fixed Ports	10/100/1000M Mgmt. port Serial Console 8 40G/100G QSFP28 cages + 48 1G/10G/25G SFP28 cages	10/100/1000M Mgmt. port Serial Console 64 100G/40G ports
Configurable Ports	None	None

Table 2: Hardware Models – TA Series Properties

Property	GTAP-ATX21	GTAP-ASF21
Model Number	GTAP-ATX21 (AC power)	GTAP-ASF21 (AC power)
Size	1RU	1RU
Processor	Intel Atom Processor C3338	Intel Atom Processor C3338
Fixed Ports	10/100/1000M Mgmt. port 4x 10/100/1000BASE-T links	10/100/1000M Mgmt. port 4x 1Gb/10Gb Copper or Fiber links
Configurable Ports	None	None

Table 3: GTAP Series Properties

5.2 Supporting Environment Components

The following table lists components and applications in the TOE's operational environment that must be present for the TOE to operate in its evaluated configuration:

Component	Definition
Certification Authority (CA)	A server that acts as a trusted issuer of digital certificates and distributes a CRL that identifies revoked certificates.
LDAP Server	A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory.
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.
Audit Server	The audit server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.

Table 3: Evaluated Components of the Operational Environment

5.3 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Physical security:** The GigaVUE product does not claim any sort of physical tamper-evident or tamper-resistant security mechanisms. Therefore, it is necessary to deploy the product in a locked or otherwise physically secured environment so that it is not subject to untrusted physical modification.
- **Limited functionality:** The GigaVUE product must only be used for its intended networking purpose. General purpose computing applications, especially those with network-visible interfaces, may compromise the security of the product if introduced.

- **No through traffic protection:** The security boundary of the Common Criteria evaluation is limited to traffic flowing to or from the TOE. The intent is for GigaVUE to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
- **Trusted administration:** The GigaVUE product does not provide a mechanism to protect against the threat of a rogue or otherwise malicious administrator. Therefore, it is the responsibility of the organization to perform appropriate vetting and training for security administrators prior to granting them the ability to manage the product.
- **Regular updates:** Gigamon provides regular product updates for the GigaVUE product that include bug fixes as well as functionality and security enhancements. It is expected that administrators are reasonably diligent in ensuring that software patches are applied regularly as they are made available.
- **Secure admin credentials:** GigaVUE protects the administrator's credentials stored on GigaVUE that are used to access it. Additionally, it is assumed that any administrative credentials maintained by an environmental LDAP Server are secured in order to mitigate the risk of impersonation.
- **Residual information:** It is the responsibility of the administrator to ensure 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.

6 Secure Installation and Configuration

Documentation for how to order and acquire the TOE is described in the 'Contact Sales' section of documents [3] through [8]. When receiving delivery of a TOE model, this documentation should be checked as part of the acceptance procedures so that the correctness of the hardware can be verified. Additionally, documents [3] through [8] can be referenced for physical requirements such as unpacking the TOE, installing modules, racking the TOE, cabling (i.e., network and power), as well as verifying power and environmental operating conditions. The TOE comes with the software image installed on it by default. Depending on when the device was manufactured, the appliance may have a different GigaVUE software version initially installed on it than desired (.i.e., not certified version). If the version is not the desired version, follow the instructions in Section 7.8 to obtain and install the correct software image from Gigamon.

Regardless of the specific model being installed, the software is functionally identical with respect to the Common Criteria security requirements, so secure management for each device is described in the remainder of this document. Note that these steps can be performed using the initial default user account.

NOTE: Use the write memory command in the CLI to save configuration changes to flash. Otherwise, changes will be added to the active configuration immediately but will not be saved across a reboot unless the write memory command is used.

6.1 Initial Out-of-the-Box Setup

An administrator can use any general-purpose computer to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI. The TOE can also be managed locally, in which case the management workstation (local console) must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.

1. Connect to the TOE via the local console using the following settings on a terminal application:

   115,200 Baud
   8 data bits
   No parity
   1 stop bit
   No flow control

2. Authenticate using the default credentials:

   Username: admin
   Password: admin123A!

   NOTE: During the installation, the TOE forces the user to change the default password to a non-default password. The default password (admin123A!) will never be accepted as a valid password in any future attempts to change the password.

3. Start the jump-start script to configure basic setting by entering the following commands on the TOE:

   enable
   config terminal
   config jump-start

   Refer to the 'Run the Jump-Start Script' Section in documents [3] through [8] for more information on completing the jump-start setup.

6.2 Verify Software Version

Once the TOE is physically installed, it is recommended that an administrator verify the version of software operating on the TOE by issuing a "show version" command and compare the displayed version to the expected version.

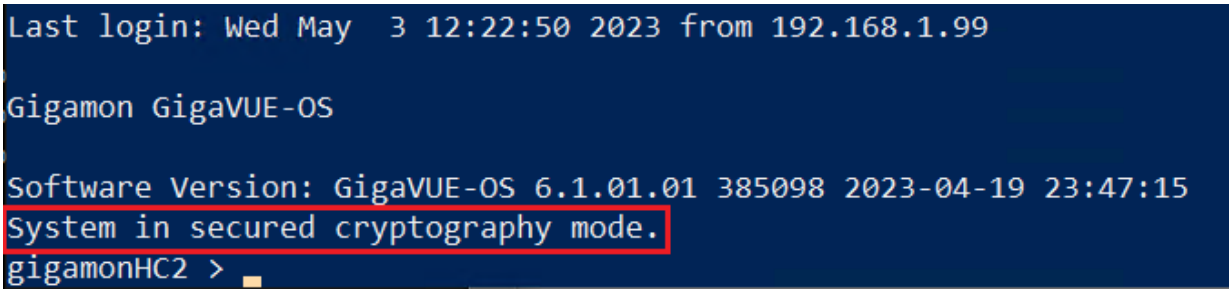
6.3 Configure the TOE to use Secure Cryptography Mode

Secure cryptography mode must be configured to limit the cryptographic options to be consistent with the claims made for the Common Criteria evaluation.

1. Authenticate to the TOE.
2. Enter the following commands to enable secure cryptography mode:

   enable
   config terminal
   system security crypto enhanced

3. Respond “yes” to “Confirm secure cryptography mode change?” and then wait for the device to reload.
4. Authenticate to the TOE.
5. Verify that after authenticating to the CLI, the TOE reports “System in secure cryptography mode.”



If the secure cryptography mode has been configured on the TOE and has been rebooted, the status is displayed after logging in.

NOTE: When enabling secure cryptography mode, the required TLS version 1.2 is enabled by default.

The administrator installing the TOE is expected to perform all of the operations in Sections 6.1 through 6.5 of this document. This will result in the TOE’s cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE’s cryptographic engine as the TOE already comes pre-configured to meet many of the Common Criteria requirements such as limiting all ciphersuites and algorithms to those defined in the Security Target [1] and automatic zeroization key destruction functionality. The TOE is not subject to any situations that would prevent or delay key destruction and strictly conforms to the key destruction requirements.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

6.4 Configure the TOE to Record Log and Audit Data (Locally)

In the evaluated configuration, all auditable events relevant to the Common Criteria evaluation are logged locally by following this process:

1. Authenticate to the TOE via SSH, then run the following commands:

```
enable
config terminal
logging level audit mgmt info
logging level cli commands info
logging local info
```

6.5 Disable/Enable Services

In the evaluated configuration, certain services will need to be configured on the TOE. The Security Administrator will need to disable these insecure services and enable SSH by performing the steps outlined in 6.5.1.

After verifying that the SNMP Server is disabled and SSH2 is enabled, attempt to authenticate to the TOE with a SSH2 client by pointing the client at the TOE's IP address and using the 'admin' accounts credentials (that were configured during the initial out-of-the-box setup in Section 6.1). To be able to connect to the TOE, the SSH2 client must support ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521 as the key exchange method, and one or more of the following encryption and data integrity algorithms.

- Encryption Algorithms: aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, or aes256-gcm@openssh.com
- Data Integrity Algorithms: hmac-sha2-256 or hmac-sha2-512

NOTE: The MAC algorithms defined in the ST are the only ones included in the evaluated configuration. If deviating from this configuration, the "none" MAC algorithm is never allowed for SSH.

NOTE: The SSH session key thresholds for time and amount of transmitted data are not configurable in the evaluated configuration. The TOE has been hard coded to initiate a rekey when the session keys have been used for one hour (3600 seconds) or when 256 MB of data has been transmitted when the TOE acts as a client and one hour or 1 GB when the TOE acts as a server. Rekeying is performed upon reaching the threshold that is hit first.

6.5.1 Configure Services

SSH2 can be configured for remote connections to the GigaVUE's Ethernet Management Port. By default, SSH2 is enabled.

1. Enter the following commands to disable the TOE's SNMP server:

```
enable
config terminal
no snmp-server enable
```

2. If SSH2 is disabled, enter the following commands:

```
enable
config terminal
ssh server enable
ssh server host-key generate
```

NOTE: SSHv2 is used for remote connections to the GigaVUE's Ethernet Management Port.

6.6 Certificate Validity Checking

The TOE performs certificate validity checking for outbound TLS connections to the LDAP Server. In addition to the validity checking that is performed by the TOE, the TOE will validate certificate revocation status using a certificate revocation list (CRL) that the TOE is configured to download automatically from a Certification Authority in the Operational Environment. The TOE determines the validity of certificates by ensuring that the certificate and the certificate path are valid. The TOE also ensures that the extendedKeyUsage field includes the correct purpose for its intended use, which includes Server Authentication for TLS server certificates; the TOE does not handle TLS client certificates,

certificates associated with OCSP responses, or code signing certificates. In the event that the revocation status cannot be verified, the certificate will not be accepted. The TOE does not claim handling certificate validation any differently whether a full certificate chain or only a leaf certificate is being presented.

6.7 Boot Time Integrity Self-Tests

All binaries (e.g., executables, libraries), are located on a read-only partition and cannot be modified. In addition, the TOE has a configuration database that is integrity checked at boot time using SHA-256.

The udiag is run under u-boot (microcode boot loader) which runs power-on self-tests of all the major components (e.g., memory, CPU, UART, Ethernet controllers) on the motherboard, including the components that connect to the i2c buses. This includes all transceivers used by the data plane. The pci_diag component is a Linux component that runs when the kernel is loading that is responsible for testing and checking the components connected to the PCIe interfaces. It is also responsible for Line card type detection. Example output from self-tests are below:

When the device boots up, memory scan/tests are performed.

```
DRAM:  Initializing....using SPD
Detected UDIMM WD3SN804G13LSQ
2 GiB left unmapped
4 GiB (DDR3, 64-bit, CL=8, ECC off)
Testing 0x00000000 - 0x7fffffff
Testing 0x80000000 - 0xffffffff
Remap DDR 1.8 GiB left unmapped

POST memory PASSED
```

PCI scans are done.

```
PCIe1: Root Complex, x1, regs @ 0xfe200000
  01:00.0     - 10b5:8608 - Bridge device
PCIe1: Bus 00 - 01
PCIe3: Root Complex, no link, regs @ 0xfe202000
PCIe3: Bus 02 - 02
```

If PCI tests fails, the system reboots and retries and these are being taken care at u-boot level.

Persistent memory (disc) integrity checks are also performed.

```
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda5
ROOT_1: clean, 7149/359040 files, 330602/716900 blocks
[/sbin/fsck.vfat (1) -- /boot] fsck.vfat -a /dev/sda2
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
/dev/sda2: 9 files, 3638/12016 clusters
[/sbin/fsck.ext3 (1) -- /bootmgr] fsck.ext3 -a /dev/sda1
BOOTMGR: clean, 18/6024 files, 1814/24096 blocks
[/sbin/fsck.ext3 (1) -- /config] fsck.ext3 -a /dev/sda7
CONFIG: clean, 29/102800 files, 22905/409601 blocks
[/sbin/fsck.ext3 (1) -- /var] fsck.ext3 -a /dev/sda8
VAR: clean, 467/3133440 files, 1263324/6261333 blocks
```

```
[  OK  ]
```

If file systems are corrupted, fsck attempts to repair them and system boots up normally. If fsck fails to repair, errors are displayed but system boots up normally.

Once booted, the TOE will execute a continuous RNG test in order to ensure that the entropy source has not degraded and also perform integrity checks on the TOE software. If an integrity test fails (cryptography or TOE software) the TOE is put into safe mode (Gigamon specific state). In safe mode, the device will operate in a limited manner which requires user intervention to bring the appliance back into a normal state after fixing the issues. The console display clearly indicates that the appliance is in safe mode along with the diagnostic information. For example:

```
CMAC AES-256-CBC test started
CMAC AES-256-CBC test OK
CMAC DES-EDE3-CBC test started
CMAC DES-EDE3-CBC test OK
Cipher AES-128-ECB test failure induced
Cipher AES-128-ECB test failed
ERROR:2D080086:lib=45,func=128,reason=134:file=fips_aes_selftest.c:line
=97
CCM test started
CCM test OK
GCM test started
GCM test OK
XTS AES-128-XTS test started
XTS AES-128-XTS test OK
XTS AES-256-XTS test started
XTS AES-256-XTS test O
…
POST Failed
Power-up self test failed
cryptographic algorithm test failed.
```

The appliance will then enter safe mode. When a node enters safe mode, it displays the following message when a user attempts to make a change to the configuration that is not available in safe mode:

```
The system has restricted provisioning in safe mode. Contact Gigamon
Support on how to troubleshoot and recover from safe mode.
```

These tests are sufficient to validate the correct operation of the TOE because they verify that the cryptographic module is operating correctly, the configuration database does an integrity check, and that the underlying hardware does not have any anomalies that would cause the software to be executed in an unpredictable or inconsistent manner.

6.8 Modes of Operations

The TOE has three modes of operation: operational, safe, and limited. Safe and limited modes were introduced to safeguard critical provisioning errors when the TOE is used in a cluster configuration. Cluster configuration was outside the scope of the evaluation. However, Safe mode is also applicable to

standalone devices that have failed integrity checks on startup (see section 6.7 of this document) or when the product experiences an unrecoverable error during operations.

While booting, the GigaVUE does not allow access to the administrator interfaces or process network traffic until the software image and configuration have loaded. During boot the TOE's Power-on self-tests (POST) are performed and as long as there are no errors during the POST, this TOE will transition into the operational mode (normal state).

If any of the POST self-tests fail or other unrecoverable error happens, the TOE will enter into Safe mode and the following actions should be taken:

- Restart the TOE to perform POST again and determine if normal operation can be resumed.
- If the problem persists, refer to Section 10 to contact Gigamon.

Operational mode – The GigaVUE software image and configuration are loaded and the GigaVUE is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all GigaVUE based security functions are operating.

6.9 TLS Functionality

The hostname reference identifier is the only supported value for the LDAP. Wildcards cannot be defined as part of the reference identifier on the TOE, but the TOE will accept certificates with wildcards in the left-most label (e.g. *.example.com). The TOE supports the SAN extensions for certificate validation. The only Supported Elliptic Curves Extension included in the Client Hello are the NIST curves secp256r1, secp384r1, and secp521r1. This is not configurable. Certificate pinning is not supported. When certificate validation fails, the connection is not established.

7 Secure Management of Gigamon GigaVUE

The following sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. Note that this information is largely derived from [2] but summarized here to discuss only actions that are required as part of the 'evaluated configuration'. The Security Administrator is encouraged to reference this document in full in order to have in-depth awareness of the security functionality of the GigaVUE, including functions that may be beyond the scope of this evaluation.

7.1 Authenticating to Gigamon GigaVUE

Users must authenticate to Gigamon GigaVUE in order to perform any management functions. Section 8.3 of the ST discusses the process in which Gigamon GigaVUE authenticates users access the TOE via the local console or remote CLI. Section 8.7 of the ST also discusses the trusted channels that are invoked in order to send the data securely.

Local users login to the CLI using username and password, while remote users can login to GigaVUE via the CLI using username and password or public key based authentication. User authentication information that is sent remotely via the CLI is protected using SSHv2. When authenticating using username and password, these credentials are verified using either the TOE's local mechanism and credential repository or by an LDAP server that provides external authentication decisions. LDAP authentication can be used for both the local console and remote CLI. When public key authentication is used, the TOE authenticates

users by verifying the message the TOE receives from the SSH client using the message's associated public key stored on the TOE.

While authenticating locally to the TOE, the user's password does not appear in the password field. Instead, asterisks will appear thus masking the password to prevent the password from being shared. In the case that a user enters invalid credentials (valid/invalid username or valid/invalid password), the TOE does not reveal any information about the invalid component of the credential.

NOTE: Connections to the LDAP server are protected with TLS v1.2. The TLS session for an LDAP request establishes and terminates almost immediately, making it nearly impossible to interrupt the TLS session. If the LDAP server is unreachable, the TOE will only perform a single attempt to connect to the LDAP server and will then default to verifying the authentication credentials to the TOE's local store.

7.1.1 Public-Key Based Authentication Configuration

SSH ecdsa-sha2-nistp384 public/private key pairs must be generated or loaded on the TOE so that SSH authentication using a public-key is possible. Perform the following steps to add an authorized public-key to a user on the TOE:

1. Authenticate to the TOE via the CLI as an Admin user.
2. Enter the following commands on the TOE:

   enable
   config terminal
   ssh client user <USERNAME> authorized-key sshv2 <PUBLIC KEY>

3. Provide the user the corresponding private key for their use to authenticate via SSH.
4. The user would then load the private key on their SSH client when attempting to authenticate.

LDAP Authentication Configuration

Perform the following steps to configure the LDAP client on the TOE via the CLI. Refer to 'Add an LDAP Server' section in document [2] beginning on page 826 for more information.

1. Authenticate to the TOE via the CLI as an Admin user.
2. Enter the following commands on the TOE to install the CA certificate(s) that issued the LDAP server certificate:

   enable
   config terminal
   crypto certificate name <NAME> public-cert pem "-----BEGIN CERTIFICATE--
   <CERT_DATA_HERE>-----END CERTIFICATE-----"
   NOTE: Install all the certificates in the certificate chain.
   crypto certificate ca-list default-ca-list name <INSTALLED CERTIFICATE>
   NOTE: Execute this for all the installed certificates.

   NOTE: CA certificates issued for the LDAP server connection must be ECDSA certificates to be able to be used with the ciphersuite claimed as part of the Common Criteria evaluation.

   The above is the only command needed for placing the TOE into evaluated configuration For further information on the `crypto` command and its capability see "crypto" in document [2] starting on page 160.

3. Refer to the ‘ldap’ section in document [2] end of page 272 to configure the LDAP parameters. The commands below are provided as an example of the LDAP parameters that need to be defined for a working configuration. The commands in bold must be configured as such in the evaluated configuration.

   ldap base-dn <STRING>
   ldap bind-dn <STRING>
   ldap bind-password <PASSWORD HERE>
   ldap group-attribute <STRING>
   ldap host <LDAP_SERVER_HOSTNAME_HERE>
   ldap login-attribute <STRING>
   ldap ssl mode ssl
   ldap ssl ssl-port 636
   ldap ssl ca-list default-ca-list
   ldap ssl cert-verify
   ldap version 3

4. Refer to the ‘aaa authentication’ section in document [2] beginning on page 39 to configure the AAA Authentication parameters. The command below is provided as an example of the AAA Authentication parameters that need to be defined for a working configuration. The command is in bold because it must be configured as such in the evaluated configuration.

   aaa authentication login default local ldap

5. Refer to the ‘aaa authorization’ section in document [2] beginning on page 44 to configure the AAA Authorization parameters. The commands below are provided as an example of the AAA Authorization parameters that need to be defined for a working configuration.

   aaa authorization map order <POLICY>
   aaa authorization map default-user <USER>

7.2 Failed Authentication Lockout

The TOE provides a configurable counter for consecutive failed authentication attempts that will lock a user account when the failure counter threshold is reached. When an account is locked a user cannot login to the remote CLI. A valid login that happens prior to the failure counter reaching its threshold will reset the counter to zero.

The remote CLI counter can be set to any 32-bit integer value (a value of 0 will disable lockout). While the Admin or user account is locked, no authentication is possible. The authentication failure settings can be configured such that the default ‘admin’ user account overrides this functionality (exempt) so that it is not possible to cause a denial of service. The lockout duration is a configurable number of seconds, with a default setting of 360.

7.2.1 Configure Failed Authentication Lockout

Follow these steps to configure unsuccessful authentication attempts for the remote CLI:

1. Authenticate to the TOE via either CLI.
2. Enter the following commands:

   enable
   config terminal

3. Enter the following commands to configure the number of successive unsuccessful authentication attempts before the account is locked and the time period that it remains locked.

```
aaa authentication attempts lockout max-fail <FAILURE COUNT>
aaa authentication attempts lockout unlock-time <SECONDS>
```

7.3 Managing Users

The security management functions available to authorized users of the TOE are mediated by a role-based access control system. The role-based access control system is enforced on the local console and the remote CLI. The TOE has two roles: Admin and Monitor. Each role has different authorizations in terms of the functions that they can perform. All SFR relevant management activity is performed by the Admin, role which corresponds to the NDcPP's definition of Security Administrator. Only users with the Admin role are permitted to create and assign roles to users. The Monitor role provides view-only access to ports and configurations.

Each user has the following security attributes associated with them:

- Username
- Password
- SSH public key (optional - used for remote CLI login only)
- One or more roles

The username and password are for authenticating to the TOE. These credentials are verified using the authentication mechanism that has been configured for the TOE. Once the username has been validated, the username is used to query the one or more roles which have been associated with that username within the TOE's local store. The TOE then uses the roles assigned to the authenticated user to determine if an action is authorized per GigaVUE's role-based access control system. When LDAP authentication is used, that user information is mapped to the internally-stored attributes so that the authentication event is associated with the correct user.

7.3.1 Create a New Admin User Account

1. Authenticate to the TOE via the CLI as an Admin user.
2. Select a password that meets the password strength requirements in Section 7.4.
3. Enter the following commands to create a new user account:

```
enable
config terminal
username <USERNAME> password <PASSWORD>
username < USERNAME> roles add admin
```

NOTE: An Admin user can delete user accounts with the 'no username' command.

7.3.2 Modify User Password

1. Authenticate to the TOE via SSH.
2. Enter the following commands to change the password of a user:

```
enable
config terminal
```

username <USERNAME> password <PASSWORD>

NOTE: Adding the password inline is optional as it does not obfuscate the password. The command will prompt the user for a password if it is not supplied and will obfuscate the password as its being typed.

7.4 Password Management

Passwords can be composed using any combination of upper case and lower-case letters, numbers and special characters. The special characters that are supported include the following: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, and “(“,”)”.

The password policy includes a configurable minimum length, which can be configured by an Admin user to any value between 8 and 30 in the evaluated configuration.

In order to minimize the risk of account compromise, it is recommended to use a password that includes a mixture of uppercase, lowercase, numeric, and special characters and is not a common word or phrase, but is not so complex that it must be written down in order to be remembered. Password information is never revealed during the authentication process including during login failures.

7.4.1 Configure the Password Length

Perform the following steps to configure minimum length for passwords:

1. Authenticate to the TOE via the CLI as an Admin user.
2. Enter the following commands to enable secure passwords mode:

   enable
   config terminal
   system security passwords enhanced
   system security passwords min-length 15
   show system

3. Verify the TOE reports “Configured secure passwords mode: enabled” and “Minimum password length: 15”.

7.5 Session Termination

7.5.1 Admin Logout

The Admin is able to terminate their own session by entering the "exit" command when logged into the local console or remote CLI via SSH.

7.5.2 Termination from Inactivity

The TOE is designed to terminate a local session after a specified period of time with a default setting of 15 minutes.

The TOE has a single configuration for the CLI accessed via the serial port and the CLI accessed via SSH. In the event that the inactivity setting is met while users are logged into the CLI via the serial port, the session will end. In the event that the inactivity setting is met while users are logged into the CLI via

SSH, the TOE tears down the SSH connection. This setting can be configured to 0 or between .25-35791 minutes. NOTE: The value of 0 means that this setting is disabled and there is no timeout configured.

The CLI timeout is configured via the CLI by an Admin user with the following commands:

```
enable
config terminal
cli default auto-logout <MINUTES>
```

7.6 Login Banner

There are two possible ways to authenticate to the TOE: local console and remote CLI. Each of these interfaces has a configurable login banner that is displayed prior to the user authenticating to the TOE. The login banner is created by an Admin user authenticated to the CLI with the following commands:

```
enable
config terminal
banner login <STRING>
```

7.7 System Time Configuration

In the evaluated configuration of the TOE, the system time is set manually. The use of NTP was not evaluated. Only an Admin user is able to perform this operation by performing the steps below.

1. Authenticate to the TOE via the CLI as an Admin user.
2. Enter the following command to view the current time:

   ```
   show clock
   ```

3. Enter the following commands to set the date and time:

   ```
   enable
   config terminal
   clock set <hh:mm:ss> [<yyyy/mm/dd>]
   ```

7.8 Secure Updates

To maintain security throughout the lifecycle of the GigaVUE product, the TOE provides a mechanism to apply software upgrades. In order to update the TOE, the Admin will access a Gigamon-hosted site and enter a username and password to download the image to their local machine. After downloading the image, the Admin will fetch the image through the remote CLI.

The image that is downloaded is compressed and stored in a .tar file and signed with a digital signature (SHA-256). All GigaVUEs are pre-loaded with a key for the signature verification performed as part of the update mechanism. Before the actual installation occurs, the signature is verified against the stored key. The image will not be installed if the update fails to be verified. If the signature is successfully verified, the update will be installed on the inactive partition. If the inactive partition already has a software version installed, the update will over-write the previously installed software. Once the new software is installed, the Admin will enter a command in the local console or remote CLI in order to boot off from the inactive partition on which the update was installed, thus making it the active partition.

The following sections describe the steps which must be taken in order to install a new software image.

7.8.1 Display the Current Version

Before downloading a new image, the current version of the software image should be identified. The current version of the software image is displayed via the CLI by using the command “show version”.

7.8.2 Downloading and Installing the New Image

The “image” command is used via the CLI to download and install the new image. For more information on the “image” command, refer to the ‘image’ section in document [2] beginning on page 230.

1. Authenticate to the TOE via the CLI as an Admin user.
2. Enter the following commands to fetch an update to the TOE:

   ```
   enable
   config terminal
   image fetch <PROTOCOL>://<HOSTNAME><PATH><FILENAME>
   ```

3. After the update has been fetched, enter the following command on the TOE to initiate the update:

   ```
   image install <FILENAME>
   ```

   NOTE: The update is currently on a separate partition other than the currently booted partition. As such, it is considered a delayed activation. The software version can be checked by performing the steps of Section 7.8.1 above prior to initiating the next command.

4. Enter the following command to complete installation:

   ```
   image boot next
   ```

5. If prompted to save modified configuration, answer “yes”.
6. Once the TOE reboots, enter the “write memory” command.

7.8.3 Rebooting TOE

Once the image has been installed, the TOE must be rebooted for the new image to take effect and become the executing image. On the CLI this is achieved by using the following command:

```
reload
```

Once the TOE fully reboots, the new version of the software can be checked by performing the steps of Section 7.8.1 above.

7.8.4 Actions to be Taken Upon Failure

The software image for the TOE contains a digital signature. If an attempt is made to download and install an illegitimate update, the update is not installed and cannot be overridden by the Admin user.

8 Auditing

In order to be compliant with Common Criteria, GigaVUE must audit the events in the table below. The audit records that GigaVUE creates include the date and time, outcome of the event, event type, subject identity and the source of the event.

Auditing is turned on and off by using the 'logging' command (refer to Section 6.4 for more information). The 'show log' command displays audit information. It is possible to use regular expressions in the 'show log' command to restrict the search.

The right most column in Table 4 provides examples for each audit event for which the TOE needs to produce a record. The following is one example of an audit record to describe the contents of the record:

> **2022-08-08T12:42:12.492482-04:00 gigamonTA200 sshd[22323]: User admin (System Administrator) logged in via from 192.168.1.99 port 49254**

The following are the fields for this audit record:

- **2022-08-08T12:42:12.492482-04:00** = This is the date and time the event occurred.
- **gigamonTA200** = This is the GigaVUE model that recorded the event.
- **sshd[22323]:** = This is the management channel for the event.
- **User admin (System Administrator)** = This is the subject identity; which for this case is the username of the user that caused the event.
- **logged in via from 192.168.1.99 port 49254** = This is a message that indicates the outcome (success), type of event (login) as well as identifies the IP address of the remote system connecting to the TOE.

Auditable Event	Sample Data
Start-up and shut-down of the audit functions	**Startup of audit functions** 2022-10-28T13:41:53.566898-04:00 gigamonASF21 systemd.INFO - Started System Logging Service. **Shutdown of audit functions** 2022-10-28T13:38:22.789687-04:00 gigamonASF21 systemd.INFO - Stopped System Logging Service.
Administrative login and logout	**Local Console Successful Login using Password** 2022-10-19T08:32:20.520691-04:00 gigamonTA200 login: pam_unix(login:session): session opened for user admin by LOGIN(uid=0) 2022-10-19T08:32:20.522618-04:00 gigamonTA200 login: DIALUP AT ttyS0 BY admin 2022-10-19T08:32:20.523582-04:00 gigamonTA200 login: ROOT LOGIN ON ttyS0 **Local Console Failed Login using Password** 2022-10-19T08:34:52.151729-04:00 gigamonTA200 login: FAILED LOGIN 1 FROM ttyS0 FOR admin, Authentication failure **Local Console Successful Login using LDAP Password** 2022-10-19T08:40:12.220901-04:00 gigamonTA200 login: pam_ldap: connection established to LDAP testUser1@server gigamon2022-ldap.catl.local:636: 2022-10-19T08:40:12.222075-04:00 gigamonTA200 login: pam_ldap: connection closed to LDAP admin@server gigamon2022-ldap.catl.local:636: 2022-10-19T08:40:12.223950-04:00 gigamonTA200 login: pam_unix(login:session): session opened for user testUser1 (admin) by

	LOGIN(uid=0) 2022-10-19T08:40:12.225371-04:00 gigamonTA200 login: DIALUP AT ttyS0 BY admin 2022-10-19T08:40:12.226556-04:00 gigamonTA200 login: ROOT LOGIN ON ttyS0 **Local Console Failed Login using LDAP Password** 2022-10-19T08:42:11.692971-04:00 gigamonTA200 login: pam_ldap(login:auth): authentication failure; user=testUser1 userdn="uid=testuser1,ou=Users,dc=catl,dc=local" 2022-10-19T08:42:11.693773-04:00 gigamonTA200 login: pam_ldap: connection failed to LDAP testUser1@server gigamon2022-ldap.catl.local:636: 2022-10-19T08:42:15.497600-04:00 gigamonTA200 login: FAILED LOGIN 2 FROM ttyS0 FOR testUser1, Authentication failure **Local Console Logout** 2022-03-16T14:32:44.366177+00:00 gigamonTA200 cli[3878]: - - user admin: Executing command: exit 2022-03-16T14:32:44.366765+00:00 gigamonTA200 cli[3878]: - - user admin: libevent: escaping from dispatch (sticky) 2022-03-16T14:32:44.367354+00:00 gigamonTA200 mgmtd[3552]: - - EVENT: /mgmtd/session/events/logout 2022-03-16T14:32:44.367911+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /mgmtd/session/events/logout 2022-03-16T14:32:44.368444+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /mgmtd/session/events/logout 2022-03-16T14:32:44.368984+00:00 gigamonTA200 mgmtd[3552]: - - User admin: logout from local through trusted cli channel. 2022-03-16T14:32:44.432212+00:00 gigamonTA200 cli[3878]: - - user admin: CLI exiting 2022-03-16T14:32:44.440935+00:00 gigamonTA200 login: pam_unix(login:session): session closed for user admin 2022-03-16T14:32:44.679208+00:00 gigamonTA200 systemd: serial-getty@ttyS0.service holdoff time over, scheduling restart. 2022-03-16T14:32:44.680271+00:00 gigamonTA200 systemd: Stopped Serial Getty on ttyS0. **Remote SSH Successful Login using Password** 2022-10-25T15:46:41.031171-04:00 gigamonTA200 sshd[19896]: Postponed keyboard-interactive/pam for admin from 192.168.1.101 port 56945 ssh2 [preauth] 2022-10-25T15:46:41.033501-04:00 gigamonTA200 sshd[19896]: Accepted keyboard-interactive/pam for admin from 192.168.1.101 port 56945 ssh2 2022-10-25T15:46:41.034905-04:00 gigamonTA200 sshd[19896]: User admin (System Administrator) logged in via from 192.168.1.101 port 56945 2022-10-25T15:46:41.036244-04:00 gigamonTA200 sshd[19896]: pam_unix(sshd:session): session opened for user admin by (uid=0)

	Remote SSH Failed Login using Password 2022-10-25T15:49:27.952313-04:00 gigamonTA200 sshd[20043]: error: PAM: Authentication failure for admin from 192.168.1.101 2022-10-25T15:49:27.955542-04:00 gigamonTA200 sshd[20043]: Failed keyboard-interactive/pam for admin from 192.168.1.101 port 56951 ssh2 2022-10-25T15:49:27.956995-04:00 gigamonTA200 sshd[20043]: error: User admin (System Administrator) failed to login via from 192.168.1.101 port 56951 2022-10-25T15:49:27.962401-04:00 gigamonTA200 sshd[20043]: Postponed keyboard-interactive for admin from 192.168.1.101 port 56951 ssh2 [preauth] **Remote SSH Successful Login using LDAP Password** 2022-10-25T15:52:00.106153-04:00 gigamonTA200 sshd[20184]: Postponed keyboard-interactive/pam for unknown user testUser1 from 192.168.1.101 port 56962 ssh2 [preauth] 2022-10-25T15:52:00.107433-04:00 gigamonTA200 sshd[20184]: Accepted keyboard-interactive/pam for admin from 192.168.1.101 port 56962 ssh2 2022-10-25T15:52:00.108426-04:00 gigamonTA200 sshd[20184]: User admin (System Administrator) logged in via from 192.168.1.101 port 56962 2022-10-25T15:52:00.109264-04:00 gigamonTA200 sshd[20184]: pam_unix(sshd:session): session opened for user testUser1 (admin) by (uid=0) 2022-10-25T15:52:00.167203-04:00 gigamonTA200 sshd[20184]: Starting session: shell on pts/0 for admin from 192.168.1.101 port 56962 id 0 2022-10-25T15:52:00.205183-04:00 gigamonTA200 mgmtd[2907]: - - TRUSTED_AUTH_INFO (user testUser1/admin): validated OK 2022-10-25T15:52:00.205658-04:00 gigamonTA200 mgmtd[2907]: - - User testUser1 (local user admin) authentication method: ldap **Remote SSH Failed Login using LDAP Password** 2022-10-25T15:57:01.867437-04:00 gigamonTA200 sshd[20455]: error: PAM: Authentication failure for unknown user testUser1 from 192.168.1.101 2022-10-25T15:57:01.867993-04:00 gigamonTA200 sshd[20455]: Failed keyboard-interactive/pam for unknown user testUser1 from 192.168.1.101 port 56973 ssh2 2022-10-25T15:57:01.868507-04:00 gigamonTA200 sshd[20455]: error: Unknown user testUser1 failed to login via from 192.168.1.101 port 56973 2022-10-25T15:57:01.879073-04:00 gigamonTA200 sshd[20455]: Postponed keyboard-interactive for unknown user testUser1 from 192.168.1.101 port 56973 ssh2 [preauth] **Remote SSH Successful Login using Public Key** 2022-10-27T14:11:12.344698-04:00 gigamonTA200 sshd[7198]: Connection from 192.168.1.101 port 61817 on 192.168.1.210 port 22 2022-10-27T14:11:12.622418-04:00 gigamonTA200 sshd[7198]: Accepted key ECDSA SHA256:havmFR4LbN5nMYuquRZPn5CqGZrM6gv2teekhMlAGIo found at /var/home/root/.ssh/authorized_keys2:1 2022-10-27T14:11:12.647012-04:00 gigamonTA200 sshd[7198]: Postponed publickey for admin from 192.168.1.101 port 61817 ssh2 [preauth] 2022-10-27T14:11:12.747772-04:00 gigamonTA200 sshd[7198]: Accepted key ECDSA SHA256:havmFR4LbN5nMYuquRZPn5CqGZrM6gv2teekhMlAGIo

	found at /var/home/root/.ssh/authorized_keys2:1 2022-10-27T14:11:12.773439-04:00 gigamonTA200 sshd[7198]: Accepted publickey for admin from 192.168.1.101 port 61817 ssh2: ECDSA SHA256:havmFR4LbN5nMYuquRZPn5CqGZrM6gv2teekhMlAGIo 2022-10-27T14:11:12.774897-04:00 gigamonTA200 sshd[7198]: User admin (System Administrator) logged in viaECDSA SHA256:havmFR4LbN5nMYuquRZPn5CqGZrM6gv2teekhMlAGIo from 192.168.1.101 port 61817 2022-10-27T14:11:12.777001-04:00 gigamonTA200 sshd[7198]: pam_unix(sshd:session): session opened for user admin by (uid=0) 2022-10-27T14:11:12.858630-04:00 gigamonTA200 sshd[7198]: Starting session: shell on pts/0 for admin from 192.168.1.101 port 61817 id 0 **Remote SSH Failed Login using Public Key** 2022-10-27T14:14:20.070223-04:00 gigamonTA200 sshd[7357]: Connection from 192.168.1.101 port 61825 on 192.168.1.210 port 22 2022-10-27T14:14:20.415203-04:00 gigamonTA200 sshd[7357]: Failed publickey for admin from 192.168.1.101 port 61825 ssh2: ECDSA SHA256:3nN5KfL4gdf6SRPwilm9Glvawmw2EbnWPcNCnqBcBhM 2022-10-27T14:14:20.415522-04:00 gigamonTA200 sshd[7357]: error: User admin (System Administrator) failed to login via ECDSA SHA256:3nN5KfL4gdf6SRPwilm9Glvawmw2EbnWPcNCnqBcBhM from 192.168.1.101 port 61825 2022-10-27T14:14:20.442928-04:00 gigamonTA200 sshd[7357]: Postponed keyboard-interactive for admin from 192.168.1.101 port 61825 ssh2 [preauth] **Remote SSH Logout** 2022-03-15T16:27:53.914538+00:00 gigamonTA200 cli[14805]: - - user admin: Executing command: exit 2022-03-15T16:27:53.915010+00:00 gigamonTA200 cli[14805]: - - user admin: libevent: escaping from dispatch (sticky) 2022-03-15T16:27:53.915476+00:00 gigamonTA200 mgmtd[3552]: - - EVENT: /mgmtd/session/events/logout 2022-03-15T16:27:53.915900+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /mgmtd/session/events/logout 2022-03-15T16:27:53.916307+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /mgmtd/session/events/logout 2022-03-15T16:27:53.916739+00:00 gigamonTA200 mgmtd[3552]: - - User admin: logout from 192.168.1.98 through trusted cli channel. 2022-03-15T16:27:53.985930+00:00 gigamonTA200 cli[14805]: - - user admin: CLI exiting
Security related configuration changes	**Administrator configured login banner** 2022-03-16T14:22:53.006128+00:00 gigamonTA200 mgmtd[3552]: - - Config change ID 87: requested by: user admin (System Administrator) via CLI, 2 item(s) changed 2022-03-16T14:22:53.006353+00:00 gigamonTA200 mgmtd[3552]: - - Config change ID 87: item 1: login message: local ("issue") changed from "#012Gigamon GigaVUE-OS#012" to "!!THIS IS A WARNING BANNER!!"

	2022-03-16T14:22:53.006536+00:00 gigamonTA200 mgmtd[3552]: - - Config change ID 87: item 2: login message: network ("issue_net") changed from "#012Gigamon GigaVUE-OS#012" to "!!THIS IS A WARNING BANNER!!"
Generating/import of, changing, or deleting of cryptographic keys	**Generation of SSH host keys** 2022-10-21T12:14:40.099638-04:00 gigamonASF21 cli[8775]: - - user admin: Executing command: ssh server host-key generate 2022-10-21T12:14:40.100485-04:00 gigamonASF21 mgmtd[2897]: - - Action ID 381: requested by: user admin (System Administrator) via CLI 2022-10-21T12:14:40.102186-04:00 gigamonASF21 mgmtd[2897]: - - Action ID 381: descr: regenerate SSH host keys 2022-10-21T12:14:40.103348-04:00 gigamonASF21 mgmtd[2897]: - - Action ID 381: param: key type: "all" 2022-10-21T12:14:40.104500-04:00 gigamonASF21 mgmtd[2897]: - - Generating new hostkey of type ecdsa 2022-10-21T12:14:40.131398-04:00 gigamonASF21 mgmtd[2897]: - - Generating new hostkey of type rsa2 2022-10-21T12:14:41.056204-04:00 gigamonASF21 mgmtd[2897]: - - Starting database commit 2022-10-21T12:14:41.056679-04:00 gigamonASF21 mgmtd[2897]: - - SET: /ssh/server/hostkey/public/ecdsa 2022-10-21T12:14:41.057147-04:00 gigamonASF21 mgmtd[2897]: - - SET: /ssh/server/hostkey/private/ecdsa 2022-10-21T12:14:41.057629-04:00 gigamonASF21 mgmtd[2897]: - - SET: /ssh/server/hostkey/public/rsa2 2022-10-21T12:14:41.058114-04:00 gigamonASF21 mgmtd[2897]: - - SET: /ssh/server/hostkey/private/rsa2 2022-10-21T12:14:41.058567-04:00 gigamonASF21 mgmtd[2897]: - - Commit verify pass count: 1 2022-10-21T12:14:41.058963-04:00 gigamonASF21 mgmtd[2897]: - - Change list has 4 records 2022-10-21T12:14:41.059397-04:00 gigamonASF21 mgmtd[2897]: - - Calling side_effects function for 3 interested mods 0 0 4 bool_is_del 0 cl_del 0 cl_add_mod 0 type 0 2022-10-21T12:14:41.059797-04:00 gigamonASF21 mgmtd[2897]: - - Calling side effects function for module ssh 2022-10-21T12:14:41.060289-04:00 gigamonASF21 mgmtd[2897]: - - Finished calling side effects functions 2022-10-21T12:14:41.060721-04:00 gigamonASF21 mgmtd[2897]: - - Calling check function for 3 interested mods 2022-10-21T12:14:41.061121-04:00 gigamonASF21 mgmtd[2897]: - - Calling check function for module ssh 2022-10-21T12:14:41.061550-04:00 gigamonASF21 mgmtd[2897]: - - Finished calling check functions 2022-10-21T12:14:41.061942-04:00 gigamonASF21 mgmtd[2897]: - - Commit verify pass count: 2 2022-10-21T12:14:41.062486-04:00 gigamonASF21 mgmtd[2897]: - - Finished db checks 2022-10-21T12:14:41.062889-04:00 gigamonASF21 mgmtd[2897]: - - Calling

	apply function for 3 interested mods bool_is_del 0 cl_del 0 cl_add_mod 0 2022-10-21T12:14:41.063285-04:00 gigamonASF21 mgmtd[2897]: - - Calling apply function for module ssh:-20000 2022-10-21T12:14:41.065207-04:00 gigamonASF21 mgmtd[2897]: - - Calling apply function for module changes:-10000 2022-10-21T12:14:41.065573-04:00 gigamonASF21 mgmtd[2897]: - - Config change ID 38: requested by: user admin (System Administrator) via CLI, 4 item(s) changed 2022-10-21T12:14:41.066050-04:00 gigamonASF21 mgmtd[2897]: - - Config change ID 38: item 1: SSH private ECDSA host key changed 2022-10-21T12:14:41.066416-04:00 gigamonASF21 mgmtd[2897]: - - Config change ID 38: item 2: SSH private RSA v2 host key changed 2022-10-21T12:14:41.066767-04:00 gigamonASF21 mgmtd[2897]: - - Config change ID 38: item 3: SSH public ECDSA host key changed from "ecdsa-sha2-nistp384 AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBFl817Fxt6wVz697wqp2ZHFYJa4xIg70A/z+wQgIvlensjM/suxEPl6FKFiQOJQQLw2532mXdpIl0vreTKb/Cx98UvjLXRe5i3y2IPqBxRK1ZD44l+naLycckMehA2gGnw== " to "ecdsa-sha2-nistp384 AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBMvK4JXnJpSJrPLykr1IZT498IsLBQUCcHQS3S7669ZDYob8qtV4pfyZ2FEdCp8An6bImGs9gjscDKmUMywSgtJrxiGH3GCPZq1BnDhmIVcQGsy/w/DJsAvWiMnf74Kgog== " 2022-10-21T12:14:41.068210-04:00 gigamonASF21 mgmtd[2897]: - - Config change ID 38: item 4: SSH public RSA v2 host key changed from "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCu54nOQ38YHQjEveoFnEXK+IJoFtS/bDLK6vFGPZirdYfcsqruP5O7n0yZwcxA+mEvIVvonoSfhZXx4WOOi4mC35HDvehQxszVbQeKcCN+a14l4yFBsOSzGEbFvV+JFK8fey5KM5d4oynr0Vi5HmJFsxT5Ej5Tdoldv4/5KDWEUkgAYWLJYq0UFK3AzXEnVs4zVduvhetjOmFyXtEvTo+T9DAgs0nJhFXUFkkQylzCSPstPkRw04ifkO/+CG9RuOC+1I7OfpzVQqT43jfJwSCTu6tnm4ifExKuHYBnHB/LEo7TAs4YfNE6/A6kMEkVM9SfkYOn72ma3+gLzBk8SBGo5kd..." (truncated) to "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCkYmb/wZ2owONzleEvhM8tLq43wvrCRG0it7GC/g+NLTjr08nWsYn8H3b0ZfyVtajbhPB16av+vZRieDq0/7q2p/OZatRYGsJVYn0GWbjYsmHZ3ud9b+g0Ig98vuzNuPLv79+GW0GcSUk5ePNh3C83uPVIzVE24De3aRtDpjNQDqHBNNX1lQPAb8fLbOU9jN8JocpjtVL5ry4P2CmbdnQ4Poc3RmDrCWmKmC0Ihy7EMF/vs4GvXflZY2YTlCAorXoqByJSGE6zVFzxi8woDJfjqFZ6cq4/6RLQZ6Eh6l4oWYCWrsJ4ZhGxqGZt+tlkYW++AvwIPjIxZErgN1r2Ef4O/T4xk0yr8hSb7xs5ynmadIG2dNkiM1Lk0y/2oLDqiUFRID4y0N2WGsA58nL2X2RgOJ3uxFGQLBzEGR/7FY75SrqSFSaqxiK712btRHuexNPfk+uVJ/lWVgIwDSXzMjn8Vo2zNu+mDAMht6bSEAa1VplSDBTGQgwxe6VWWdxRfdk= " **Import X.509 Certificate** 2023-02-03T11:46:14.470877-05:00 gigamonTA200 cli[22968]: - - user admin: Executing command matching: crypto certificate name root public-cert pem * 2023-02-03T11:46:14.471422-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: requested by: user admin (System Administrator) via CLI

	2023-02-03T11:46:14.473900-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: descr: import certificate string 2023-02-03T11:46:14.474487-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: param: certificate name: "root" 2023-02-03T11:46:14.475023-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: param: certificate data string: ******** 2023-02-03T11:46:14.475504-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: param: certificate key type: "rsaEncryption" 2023-02-03T11:46:14.475993-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: param: certificate format: "PEM" 2023-02-03T11:46:14.476456-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: param: private key format: "PEM" 2023-02-03T11:46:14.684930-05:00 gigamonTA200 mgmtd[3585]: - - Starting database commit 2023-02-03T11:46:14.685515-05:00 gigamonTA200 mgmtd[3585]: - - SET: /certs/config/certs/b787ef7651696897049ef3e80b00ccafef920f3b 2023-02-03T11:46:14.686046-05:00 gigamonTA200 mgmtd[3585]: - - SET: /certs/config/certs/b787ef7651696897049ef3e80b00ccafef920f3b/certificate 2023-02-03T11:46:14.686520-05:00 gigamonTA200 mgmtd[3585]: - - SET: /certs/config/certs/b787ef7651696897049ef3e80b00ccafef920f3b/cert_name 2023-02-03T11:46:14.687008-05:00 gigamonTA200 mgmtd[3585]: - - Commit verify pass count: 1 2023-02-03T11:46:14.687508-05:00 gigamonTA200 mgmtd[3585]: - - Change list has 6 records 2023-02-03T11:46:14.687994-05:00 gigamonTA200 mgmtd[3585]: - - Calling side_effects function for 6 interested mods 6 0 0 bool_is_del 0 cl_del 0 cl_add_mod 0 type 0 2023-02-03T11:46:14.688460-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module cert 2023-02-03T11:46:14.688936-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T11:46:14.691374-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T11:46:14.691943-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T11:46:14.692435-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T11:46:14.692964-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module web 2023-02-03T11:46:14.693441-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module gv_box 2023-02-03T11:46:14.693940-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module gv_gigastream 2023-02-03T11:46:14.694410-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling side effects functions 2023-02-03T11:46:14.694906-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for 6 interested mods 2023-02-03T11:46:14.695363-05:00 gigamonTA200 mgmtd[3585]: - - Calling

	check function for module cert 2023-02-03T11:46:14.695786-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T11:46:14.902193-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module web 2023-02-03T11:46:14.902768-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module gv_box 2023-02-03T11:46:14.903267-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking cluster config changes=6 2023-02-03T11:46:14.903757-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking cc changes=6 2023-02-03T11:46:14.904219-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking config_cc changes=6 2023-02-03T11:46:14.904691-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking line card changes=6 2023-02-03T11:46:14.905161-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking config linecard changes=6 2023-02-03T11:46:14.905612-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module gv_gigastream 2023-02-03T11:46:14.906084-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling check functions 2023-02-03T11:46:14.906532-05:00 gigamonTA200 mgmtd[3585]: - - Commit verify pass count: 2 2023-02-03T11:46:14.907015-05:00 gigamonTA200 mgmtd[3585]: - - Finished db checks 2023-02-03T11:46:14.907457-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for 6 interested mods bool_is_del 0 cl_del 0 cl_add_mod 0 2023-02-03T11:46:14.907910-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module cert:-21450 2023-02-03T11:46:14.910603-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T11:46:14.911086-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T11:46:14.911510-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 1 2023-02-03T11:46:14.911949-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module web:-20000 2023-02-03T11:46:14.914088-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 1 2023-02-03T11:46:14.914589-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module changes:-10000 2023-02-03T11:46:15.124526-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 8: requested by: user admin (System Administrator) via CLI, 6 item(s) changed 2023-02-03T11:46:15.125097-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 8: item 1: Certificate name root, ID b787ef7651696897049ef3e80b00ccafef920f3b add 2023-02-03T11:46:15.125614-05:00 gigamonTA200 mgmtd[3585]: - - Config

	change ID 8: item 2: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate name initially set to "root" 2023-02-03T11:46:15.126108-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 8: item 3: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate content initially set to "subject 'rootCA' issued by 'rootCA', expires 2038/01/18 22:14:07" 2023-02-03T11:46:15.126569-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 8: item 4: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate comment initially set to "" 2023-02-03T11:46:15.127072-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 8: item 5: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate private key initially set to "(not defined)" 2023-02-03T11:46:15.127537-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 8: item 6: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate private key present initially set to "false" 2023-02-03T11:46:15.128017-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /mgmtd/notify/dbchange/as_saved 2023-02-03T11:46:15.128503-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /mgmtd/notify/dbchange/cleartext 2023-02-03T11:46:15.128989-05:00 gigamonTA200 netdevd[4032]: - - Received event: /mgmtd/notify/dbchange/as_saved 2023-02-03T11:46:15.129451-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /mgmtd/notify/dbchange 2023-02-03T11:46:15.129934-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module db:0 2023-02-03T11:46:15.130388-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module gv_box:201 2023-02-03T11:46:15.130874-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /gv/internal/events/config_state_change 2023-02-03T11:46:15.131334-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 11 2023-02-03T11:46:15.131802-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module gv_gigastream:305 2023-02-03T11:46:15.132270-05:00 gigamonTA200 ugwd[4008]: - - Received event: /gv/internal/events/config_state_change 2023-02-03T11:46:15.132749-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 20 2023-02-03T11:46:15.133202-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling apply functions 2023-02-03T11:46:15.133671-05:00 gigamonTA200 mgmtd[3585]: - - Finished database commit 2023-02-03T11:46:15.134129-05:00 gigamonTA200 mgmtd[3585]: - - Action ID 30: status: completed with success 2023-02-03T11:46:15.134586-05:00 gigamonTA200 ugwd[4008]: - - Display

again, Received event: /gv/internal/events/config_state_change
2023-02-03T11:46:15.135061-05:00 gigamonTA200 ugwd[4008]: - - Display again again, Received event: /gv/internal/events/config_state_change
2023-02-03T11:46:15.135469-05:00 gigamonTA200 ugwd[4008]: - - gv_hndl_change_table_evt_update, Received event: 4
2023-02-03T11:46:20.749068-05:00 gigamonTA200 cli[22968]: - - user admin: Getting command line help: "crypto certificate ?"
2023-02-03T11:46:21.382228-05:00 gigamonTA200 syshth[4031]: syshth.INFO

Delete X509 Certificate
23-02-03T15:16:16.106283-05:00 gigamonTA200 cli[26413]: - - user admin: Executing command: no crypto certificate ca-list default-ca-list name root
2023-02-03T15:16:16.109296-05:00 gigamonTA200 mgmtd[3585]: - - Handling SET request (session 49356)
2023-02-03T15:16:16.109949-05:00 gigamonTA200 mgmtd[3585]: - - Starting database commit
2023-02-03T15:16:16.110409-05:00 gigamonTA200 mgmtd[3585]: - - SET DELETE: /certs/config/global/default/ca_certs/1
2023-02-03T15:16:16.110855-05:00 gigamonTA200 mgmtd[3585]: - - Commit verify pass count: 1
2023-02-03T15:16:16.111280-05:00 gigamonTA200 mgmtd[3585]: - - Change list has 4 records
2023-02-03T15:16:16.111726-05:00 gigamonTA200 mgmtd[3585]: - - Calling side_effects function for 7 interested mods 0 4 0 bool_is_del 1 cl_del 0 cl_add_mod 0 type 0
2023-02-03T15:16:16.112150-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module gv_gigastream
2023-02-03T15:16:16.112570-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module gv_box
2023-02-03T15:16:16.113007-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module cert
2023-02-03T15:16:16.113420-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed'
2023-02-03T15:16:16.113886-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed'
2023-02-03T15:16:16.114301-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed'
2023-02-03T15:16:16.114733-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed'
2023-02-03T15:16:16.115147-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling side effects functions
2023-02-03T15:16:16.115558-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for 7 interested mods
2023-02-03T15:16:16.116003-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module gv_gigastream
2023-02-03T15:16:16.116422-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module gv_box
2023-02-03T15:16:16.116863-05:00 gigamonTA200 mgmtd[3585]: - -

	md_gv_box_commit_check: Checking cluster config changes=4 2023-02-03T15:16:16.117253-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking cc changes=4 2023-02-03T15:16:16.117628-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking config_cc changes=4 2023-02-03T15:16:16.118025-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking line card changes=4 2023-02-03T15:16:16.118416-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking config linecard changes=4 2023-02-03T15:16:16.118819-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module cert 2023-02-03T15:16:16.119197-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.119568-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module ldap 2023-02-03T15:16:16.119960-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling check functions 2023-02-03T15:16:16.120413-05:00 gigamonTA200 mgmtd[3585]: - - Commit verify pass count: 2 2023-02-03T15:16:16.120775-05:00 gigamonTA200 mgmtd[3585]: - - Change list has 10 records 2023-02-03T15:16:16.121112-05:00 gigamonTA200 mgmtd[3585]: - - Calling side_effects function for 8 interested mods 0 10 0 bool_is_del 1 cl_del 0 cl_add_mod 0 type 0 2023-02-03T15:16:16.121452-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module gv_gigastream 2023-02-03T15:16:16.121803-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module gv_box 2023-02-03T15:16:16.122137-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module cert 2023-02-03T15:16:16.122469-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.122811-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.123143-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.123472-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.123822-05:00 gigamonTA200 mgmtd[3585]: - - Calling side effects function for module web 2023-02-03T15:16:16.124154-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling side effects functions 2023-02-03T15:16:16.124483-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for 8 interested mods 2023-02-03T15:16:16.124826-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module gv_gigastream 2023-02-03T15:16:16.125158-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module gv_box

	2023-02-03T15:16:16.125485-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking cluster config changes=10 2023-02-03T15:16:16.125824-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking cc changes=10 2023-02-03T15:16:16.126160-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking config_cc changes=10 2023-02-03T15:16:16.126488-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking line card changes=10 2023-02-03T15:16:16.126892-05:00 gigamonTA200 mgmtd[3585]: - - md_gv_box_commit_check: Checking config linecard changes=10 2023-02-03T15:16:16.127225-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module cert 2023-02-03T15:16:16.127523-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.127831-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module web 2023-02-03T15:16:16.128132-05:00 gigamonTA200 mgmtd[3585]: - - Calling check function for module ldap 2023-02-03T15:16:16.128436-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling check functions 2023-02-03T15:16:16.128747-05:00 gigamonTA200 mgmtd[3585]: - - Commit verify pass count: 3 2023-02-03T15:16:16.129047-05:00 gigamonTA200 mgmtd[3585]: - - Finished db checks 2023-02-03T15:16:16.129345-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for 8 interested mods bool_is_del 1 cl_del 0 cl_add_mod 0 2023-02-03T15:16:16.129715-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module gv_gigastream:305 2023-02-03T15:16:16.130026-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 20 2023-02-03T15:16:16.130326-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module gv_box:201 2023-02-03T15:16:16.130629-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /gv/internal/events/config_state_change 2023-02-03T15:16:16.130940-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 11 2023-02-03T15:16:16.131246-05:00 gigamonTA200 ugwd[4008]: - - Received event: /gv/internal/events/config_state_change 2023-02-03T15:16:16.131548-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module email:0 2023-02-03T15:16:16.131859-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 1 2023-02-03T15:16:16.132166-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module ldap:0 2023-02-03T15:16:16.132471-05:00 gigamonTA200 mgmtd[3585]: - - LDAP is congigured to use default-ca-list CA certificates, but none are configured. 2023-02-03T15:16:16.134401-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 84

	2023-02-03T15:16:16.134741-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module db:0 2023-02-03T15:16:16.135048-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module changes:-10000 2023-02-03T15:16:16.344743-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: requested by: user admin (System Administrator) via CLI, 10 item(s) changed 2023-02-03T15:16:16.345194-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 1: Certificate name root, ID b787ef7651696897049ef3e80b00ccafef920f3b deleted 2023-02-03T15:16:16.345589-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 2: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate name was "root" before deletion 2023-02-03T15:16:16.345980-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 3: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate content was "subject 'rootCA' issued by 'rootCA', expires 2038/01/18 22:14:07" before deletion 2023-02-03T15:16:16.346347-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 4: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate comment was "" before deletion 2023-02-03T15:16:16.346745-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 5: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate private key value before deletion was not defined 2023-02-03T15:16:16.347127-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 6: Certificate ID b787ef7651696897049ef3e80b00ccafef920f3b: Certificate private key present was "false" before deletion 2023-02-03T15:16:16.347455-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 7: System global default CA certificate 1 deleted 2023-02-03T15:16:16.347810-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 8: System global default CA certificate 1: CA Certificate id was "b787ef7651696897049ef3e80b00ccafef920f3b" before deletion 2023-02-03T15:16:16.348140-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 9: System global default CA certificate 1: CA Certificate name was "root" before deletion 2023-02-03T15:16:16.348474-05:00 gigamonTA200 mgmtd[3585]: - - Config change ID 10: item 10: System global default CA certificate 1: Certificate PEM string was "-----BEGIN CERTIFICATE----- MIICMTCCAdegAwIBAgIUK5tBFDecmergcLi2eVSEpcUJg2cwCgYIKoZIzj0EAwQw ZjELMAkGA1UEBhMCVVMxETAPBgNVBAgMCE1hcnlsYW5kMQ8wDQYDVQQHDAZMYXVy ZWwxEzARBgNVBAoMCkJvb3ogQWxsZW4xDTALBgNVBAsMBENBVEwxDzANBgNVBAMM BnJvb3RDQTAeFw0yMjA4MzExNTIyMTVaFw00MjA4MjYxNTIyMTVaMG

	YxCzAJBgNV BAYTAlVTMREwDwYDVQQIDAhNYXJ5bGFuZDEPMA0GA1UEBwwGTG F1cmVsMRMwEQYD VQQKDApCb296IEFsbGVuMQ0wCwYDVQQLDARDQVRMMQ8wDQYDV QQDDAZyb290Q0Ew WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQfOyr9ym66FRUaw265X8ke/ vdepxI6 exu32U+Ld1iftSCgRvapE2yE86wS/FcDcFwNQvpC5U2YyYI33FKsxFFVo2Mw YTAd BgNVHQ4EFgQUXJNN89arDZFKmCPPf4ALmfvXe94wHwYDVR0jBBgwFo AUXJNN89ar DZFKmCPPf4ALmfvXe94wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B Af8EBAMCAYYw CgYIKoZIzj0EAwQDSAAwRQIhAOzVq5BUB5YoMVLpSNGUG8sWFo/xBc+ +MCmaWPkU /S2QAiB1vz4xfYV5NLxTs+U5gVFcO3IJKcrtfOHDM72SNg47iQ== -----END CERTIFICATE-----" before deletion 2023-02-03T15:16:16.351591-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /mgmtd/notify/dbchange/as_saved 2023-02-03T15:16:16.351955-05:00 gigamonTA200 clusterd[4009]: - - Received event: /mgmtd/notify/dbchange/as_saved 2023-02-03T15:16:16.352303-05:00 gigamonTA200 clusterd[4009]: - - Got changes to some non-clustering config nodes 2023-02-03T15:16:16.352690-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /mgmtd/notify/dbchange/cleartext 2023-02-03T15:16:16.353046-05:00 gigamonTA200 netdevd[4032]: - - Received event: /mgmtd/notify/dbchange/as_saved 2023-02-03T15:16:16.353384-05:00 gigamonTA200 mgmtd[3585]: - - EVENT: /mgmtd/notify/dbchange 2023-02-03T15:16:16.355484-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module web:-20000 2023-02-03T15:16:16.355957-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 1 2023-02-03T15:16:16.356282-05:00 gigamonTA200 mgmtd[3585]: - - Calling apply function for module cert:-21450 2023-02-03T15:16:16.356617-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'root' 2023-02-03T15:16:16.459822-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.460288-05:00 gigamonTA200 mgmtd[3585]: - - 1 certificates named 'system-self-signed' 2023-02-03T15:16:16.460759-05:00 gigamonTA200 mgmtd[3585]: - - get_start_event_id: Select the event number: 1 2023-02-03T15:16:16.461182-05:00 gigamonTA200 mgmtd[3585]: - - Finished calling apply functions 2023-02-03T15:16:16.461637-05:00 gigamonTA200 mgmtd[3585]: - - Finished database commit 2023-02-03T15:16:16.462305-05:00 gigamonTA200 mgmtd[3585]: - - Enqueued

	request message while waiting: type query_request session 11 id 1927383 2023-02-03T15:16:16.462957-05:00 gigamonTA200 mgmtd[3585]: - - Enqueued request message while waiting: type query_request session 17 id 443 2023-02-03T15:16:16.463574-05:00 gigamonTA200 mgmtd[3585]: - - Starting to handle backlogged messages: 2 in queue 2023-02-03T15:16:16.464158-05:00 gigamonTA200 mgmtd[3585]: - - Looking at request: type query_request session 11 id 1927383 2023-02-03T15:16:16.464745-05:00 gigamonTA200 mgmtd[3585]: - - Looking at request: type query_request session 17 id 443 2023-02-03T15:16:16.465301-05:00 gigamonTA200 mgmtd[3585]: - - Finished handling backlogged messages: had 2, now 0 2023-02-03T15:16:16.465880-05:00 gigamonTA200 ugwd[4008]: - - Display again, Received event: /gv/internal/events/config_state_change 2023-02-03T15:16:16.466433-05:00 gigamonTA200 ugwd[4008]: - - Display again again, Received event: /gv/internal/events/config_state_change 2023-02-03T15:16:16.466993-05:00 gigamonTA200 ugwd[4008]: - - gv_hndl_change_table_evt_update, Received event: 4
Resetting passwords	**Successful password change for user cctl** 2022-10-20T13:45:26.263027-04:00 gigamonASF21 mgmtd[2897]: - - Config change ID 34: requested by: user admin (System Administrator) via CLI, 1 item(s) changed 2022-10-20T13:45:26.263394-04:00 gigamonASF21 mgmtd[2897]: - - Config change ID 34: item 1: local user account 'cctl': password changed from (undisclosed password set) to (undisclosed password set)
Failure to establish an SSH session	**Failure to establish SSH session (SSHC)** 2022-08-11T12:24:01.158298-04:00 gigamonTA200 ssh.INFO 23258 Unable to negotiate with 192.168.1.202 port 22: no matching host key type found. Their offer: ssh-dss **Failure to establish SSH session (SSHS)** 2022-04-05T11:00:49.643950-04:00 gigamonTA200 sshd[10000]: Connection from 192.168.1.98 port 51431 on 192.168.1.210 port 22 2022-04-05T11:00:49.647213-04:00 gigamonTA200 sshd[10000]: Unable to negotiate with 192.168.1.98 port 51431: no matching MAC found. Their offer: hmac-md5 [preauth]
Failure to establish a TLS session	2022-09-05T17:20:59.445290+00:00 gigamonTA200 sshd.ERR 22051 pam_ldap: ldap_simple_bind: server gigamon2022-ldap.catl.local:636: Can't contact LDAP server: certificate verify failed (unsupported certificate purpose)
Unsuccessful login attempts limit is met or exceeded.	2022-08-10T10:18:11.269161-04:00 gigamonTA200 sshd[20468]: error: User admin (System Administrator) failed to login via from 192.168.1.233 port 52736 2022-08-10T10:18:17.758532-04:00 gigamonTA200 sshd[20468]: error: User admin (System Administrator) failed to login via from 192.168.1.233 port 52736 2022-08-10T10:18:23.491691-04:00 gigamonTA200 sshd[20468]: error: User admin (System Administrator) failed to login via from 192.168.1.233 port 52736 2022-08-10T10:18:34.305719-04:00 gigamonTA200 sshd[20606]: error: User admin (System Administrator) failed to login via from 192.168.1.233 port 58382 2022-08-10T10:18:40.318694-04:00 gigamonTA200 sshd[20606]: error: User admin (System Administrator) failed to login via from 192.168.1.233 port 58382 2022-08-10T10:18:40.322540-04:00 gigamonTA200 sshd[20635]:

	pam_tallybyname(sshd:auth): Denying access to user 'admin': Maximum number of failed logins reached, account locked. You may try again in 56 second(s).
All use of the identification and authentication mechanism	See 'Administrative login and logout'
Unsuccessful attempt to validate a certificate	**Issuer Certificate Failed** 2022-09-09T20:46:47.623613+00:00 gigamonTA200 sshd[12592]: pam_ldap: ldap_simple_bind: server gigamon2022-ldap.catl.local:636: Can't contact LDAP server: certificate verify failed (unable to get local issuer certificate) 2022-09-09T20:46:47.624177+00:00 gigamonTA200 sshd[12592]: pam_ldap: connection failed to LDAP testUser1@server gigamon2022-ldap.catl.local:636: **Certificate Expired** 2035-10-03T16:44:08.965665+00:00 gigamonTA200 sshd[26613]: pam_ldap: ldap_simple_bind: server gigamon2022-ldap.catl.local:636: Can't contact LDAP server: certificate verify failed (certificate has expired) 2035-10-03T16:44:08.966143+00:00 gigamonTA200 sshd[26613]: pam_ldap: connection failed to LDAP testUser1@server gigamon2022-ldap.catl.local:636: **Certificate Revoked** 2022-10-12T15:21:25.893577+00:00 gigamonTA200 sshd[14004]: pam_ldap: ldap_simple_bind: server gigamon2022-ldap.catl.local:636: Can't contact LDAP server: certificate verify failed (certificate revoked) 2022-10-12T15:21:25.894040+00:00 gigamonTA200 sshd[14004]: pam_ldap: connection failed to LDAP testUser1@server gigamon2022-ldap.catl.local:636: **Missing CRL signing** 2022-10-12T15:55:57.862536+00:00 gigamonTA200 sshd[20371]: pam_ldap: ldap_simple_bind: server gigamon2022-ldap.catl.local:636: Can't contact LDAP server: certificate verify failed (key usage does not include CRL signing) 2022-10-12T15:55:57.863041+00:00 gigamonTA200 sshd[20371]: pam_ldap: connection failed to LDAP testUser1@server gigamon2022-ldap.catl.local:636: **Invalid CA** 2022-10-03T17:15:57.109156+00:00 gigamonTA200 sshd[31865]: pam_ldap: ldap_simple_bind: server gigamon2022-ldap.catl.local:636: Can't contact LDAP server: certificate verify failed (invalid CA certificate) 2022-10-03T17:15:57.109787+00:00 gigamonTA200 sshd[31865]: pam_ldap: connection failed to LDAP testUser1@server gigamon2022-ldap.catl.local:636:
Any attempt to initiate a manual update	See 'Initiation of update; result of the update attempt'
All management activities of TOE's Security Functionality data	See 'Security related configuration changes'
Discontinuous changes to time – either Administrator actuated or changed via an automated process	2022-03-15T13:17:51.894184+00:00 gigamonTA200 cli[13170]: - - user admin: Executing command: clock set 11:17:30 2022/03/15 2022-03-15T15:17:30.000118+00:00 gigamonTA200 mgmtd[3552]: - - Action ID 137: requested by: user admin (System Administrator) via CLI

	2022-03-15T15:17:30.000549+00:00 gigamonTA200 mgmtd[3552]: - - Action ID 137: descr: system clock: set date and time 2022-03-15T15:17:30.001086+00:00 gigamonTA200 systemd: Time has been changed 2022-03-15T15:17:30.001785+00:00 gigamonTA200 mgmtd[3552]: - - Action ID 137: param: date and time: 2022/03/15 11:17:30 2022-03-15T15:17:30.002470+00:00 gigamonTA200 mgmtd[3552]: - - Action ID 137: status: completed with success 2022-03-15T15:17:30.003025+00:00 gigamonTA200 pm[3551]: - - Restarting process crond (Cron Daemon) from RUNNING state 2022-03-15T15:17:30.003456+00:00 gigamonTA200 pm[3551]: - - Terminating process crond (Cron Daemon) 2022-03-15T15:17:30.003862+00:00 gigamonTA200 pm[3551]: - - Sending SIGTERM to process crond (Cron Daemon) (pid 17610) 2022-03-15T15:17:30.004464+00:00 gigamonTA200 pm[3551]: - - Ignoring request to restart nonexistent process statsd 2022-03-15T15:17:30.004877+00:00 gigamonTA200 mgmtd[3552]: - - EVENT: /pm/events/proc/restart 2022-03-15T15:17:30.005308+00:00 gigamonTA200 pm[3551]: - - Closed output logging pipe(s) for process crond (Cron Daemon) 2022-03-15T15:17:30.005714+00:00 gigamonTA200 pm[3551]: - - PM caught a SIGCHLD during normal operation; looking for dead children 2022-03-15T15:17:30.006135+00:00 gigamonTA200 pm[3551]: - - Process crond (Cron Daemon) (pid 17610) exited with code 0 2022-03-15T15:17:30.006543+00:00 gigamonTA200 pm[3551]: - - pm_signal_sigchld_normal: Process crond (Cron Daemon) terminated 2022-03-15T15:17:30.006956+00:00 gigamonTA200 mgmtd[3552]: - - EVENT: /pm/events/process_terminated 2022-03-15T15:17:30.007392+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /pm/events/process_terminated 2022-03-15T15:17:30.007801+00:00 gigamonTA200 pdiscd[3956]: - - Received event /pm/events/process_terminated 2022-03-15T15:17:30.008242+00:00 gigamonTA200 pm[3551]: - - Launched crond (Cron Daemon) with pid 13267 2022-03-15T15:17:30.008651+00:00 gigamonTA200 mgmtd[3552]: - - EVENT: /pm/events/process_launched 2022-03-15T15:17:30.009068+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /pm/events/process_launched 2022-03-15T15:17:30.009479+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /pm/events/process_launched 2022-03-15T15:17:30.009882+00:00 gigamonTA200 pdiscd[3956]: - - Received event /pm/events/process_launched 2022-03-15T15:17:30.060297+00:00 gigamonTA200 mgmtd[3552]: - - Recording in permanent log file: Time change detected, clock was moved 1h 59m 38.106s forward 2022-03-15T15:17:30.060812+00:00 gigamonTA200 mgmtd[3552]: - - EVENT: /time/notify/time_change 2022-03-15T15:17:30.061316+00:00 gigamonTA200 mgmtd[3552]: - - Calling

	internal interest callback for event /time/notify/time_change 2022-03-15T15:17:30.061785+00:00 gigamonTA200 licd[3963]: - - Received event: /time/notify/time_change inside licd_mgmt_handle_event_request 2022-03-15T15:17:30.062290+00:00 gigamonTA200 sched[3933]: - - Processing event: /time/notify/time_change 2022-03-15T15:17:30.062749+00:00 gigamonTA200 sched[3933]: - - System clock changed, rechecking job schedules 2022-03-15T15:17:30.063232+00:00 gigamonTA200 netdevd[3960]: - - Time changed event 2022-03-15T15:17:30.063692+00:00 gigamonTA200 netdevd[3960]: - - Unexpected NULL 2022-03-15T15:17:31.427392+00:00 gigamonTA200 cli[13170]: - - user admin: Executing command: show clock
Initiation of update; result of the update attempt (success or failure)	**Initiation of update** 2022-09-04T14:44:11.675433-04:00 gigamonTA200 cli.INFO 14977 - - user admin: Executing command: image install gvta200.img **Result of the update attempt (Success)** 2022-09-04T14:44:57.948417-04:00 gigamonTA200 mgmtd.NOTICE 3591 - - Image installation finished successfully **Result of the update attempt (Failed)** 2022-09-04T13:59:36.092809-04:00 gigamonTA200 mgmtd.INFO 3591 - - Action ID 564: status: completed with failure: *** Could not verify image gvta200_mod_bin.img
The termination of a remote session by the session locking mechanism	2022-08-25T15:08:10.405174-04:00 gigamonTA200 cli[18264]: - - user admin: Inactive for 4 minutes -- automatically logging out 2022-08-25T15:08:10.405667-04:00 gigamonTA200 cli[18264]: - - user admin: libevent: escaping from dispatch (sticky) 2022-08-25T15:08:10.406138-04:00 gigamonTA200 mgmtd[3591]: - - EVENT: /mgmtd/session/events/logout 2022-08-25T15:08:10.406589-04:00 gigamonTA200 mgmtd[3591]: - - Calling internal interest callback for event /mgmtd/session/events/logout 2022-08-25T15:08:10.407028-04:00 gigamonTA200 mgmtd[3591]: - - Calling internal interest callback for event /mgmtd/session/events/logout 2022-08-25T15:08:10.407447-04:00 gigamonTA200 mgmtd[3591]: - - User admin: logout from 192.168.1.99 through trusted cli channel. 2022-08-25T15:08:10.479230-04:00 gigamonTA200 cli[18264]: - - user admin: CLI exiting
The termination of an interactive session	2022-03-15T16:27:53.914538+00:00 gigamonTA200 cli[14805]: - - user admin: Executing command: exit 2022-03-15T16:27:53.915010+00:00 gigamonTA200 cli[14805]: - - user admin: libevent: escaping from dispatch (sticky) 2022-03-15T16:27:53.915476+00:00 gigamonTA200 mgmtd[3552]: - - EVENT: /mgmtd/session/events/logout 2022-03-15T16:27:53.915900+00:00 gigamonTA200 mgmtd[3552]: - - Calling internal interest callback for event /mgmtd/session/events/logout 2022-03-15T16:27:53.916307+00:00 gigamonTA200 mgmtd[3552]: - - Calling

	internal interest callback for event /mgmtd/session/events/logout 2022-03-15T16:27:53.916739+00:00 gigamonTA200 mgmtd[3552]: - - User admin: logout from 192.168.1.98 through trusted cli channel. 2022-03-15T16:27:53.985930+00:00 gigamonTA200 cli[14805]: - - user admin: CLI exiting
The termination of a local session by the session locking mechanism	2022-03-16T14:41:38.786930+00:00 gigamonTA200 cli[4919]: - - user admin: Inactive for 3 minutes -- automatically logging out 2022-03-16T14:41:38.848485+00:00 gigamonTA200 login: pam_unix(login:session): session closed for user admin
Initiation of the trusted channel	**Initiation of the trusted channel (Remote audit server via SSH)** 2022-09-13T15:19:29.534529+00:00 gigamonTA200 mgmtd.NOTICE 13105 [mgmtd.NOTICE]: SSH connection to cctl@192.168.1.202:514 established **Initiation of the trusted channel (LDAP authentication server)** 2022-09-13T15:09:27.893174+00:00 gigamonTA200 sshd[11202]: pam_ldap: connection established to LDAP testUser1@server gigamon2022-ldap.catl.local:636:
Termination of the trusted channel	**Termination of the trusted channel (Remote audit server via SSH)** 2022-09-13T15:19:24.479651+00:00 gigamonTA200 mgmtd.NOTICE 3598 - - Any SSH connections to all remote syslog servers are being closed and restarted. **Termination of the trusted channel (LDAP authentication server)** 2022-09-13T15:09:27.893670+00:00 gigamonTA200 sshd[11202]: pam_ldap: connection closed to LDAP admin@server gigamon2022-ldap.catl.local:636:
Failure of the trusted channel functions	**Failure of the trusted channel (Remote audit server via SSH)** 2022-08-11T12:24:01.158298-04:00 gigamonTA200 ssh.INFO 23258 Unable to negotiate with 192.168.1.202 port 22: no matching host key type found. Their offer: ssh-dss **Failure of the trusted channel (LDAP authentication server)** 2022-09-05T17:20:59.445290+00:00 gigamonTA200 sshd.ERR 22051 pam_ldap: ldap_simple_bind: server gigamon2022-ldap.catl.local:636: Can't contact LDAP server: certificate verify failed (unsupported certificate purpose)
Initiation of the trusted path	**Initiation of the trusted path (SSH)** 2022-08-08T12:42:12.491354-04:00 gigamonTA200 sshd[22323]: Postponed keyboard-interactive/pam for admin from 192.168.1.99 port 49254 ssh2 [preauth] 2022-08-08T12:42:12.491881-04:00 gigamonTA200 sshd[22323]: Accepted keyboard-interactive/pam for admin from 192.168.1.99 port 49254 ssh2 2022-08-08T12:42:12.492482-04:00 gigamonTA200 sshd[22323]: User admin (System Administrator) logged in via from 192.168.1.99 port 49254 2022-08-08T12:42:12.493657-04:00 gigamonTA200 sshd[22323]: pam_unix(sshd:session): session opened for user admin by (uid=0)
Termination of the trusted path	**Termination of the trusted path (SSH)** 2022-08-08T12:42:37.598048-04:00 gigamonTA200 mgmtd[3591]: - - User admin: logout from 192.168.1.99 through trusted cli channel. 2022-08-08T12:42:37.669314-04:00 gigamonTA200 cli[22333]: - - user admin: CLI exiting 2022-08-08T12:42:37.709608-04:00 gigamonTA200 sshd[22323]: Close session:

	user admin from 192.168.1.99 port 49254 id 0 2022-08-08T12:42:37.710098-04:00 gigamonTA200 sshd[22323]: Received disconnect from 192.168.1.99 port 49254:11: disconnected by user 2022-08-08T12:42:37.710642-04:00 gigamonTA200 sshd[22323]: Disconnected from user admin 192.168.1.99 port 49254 2022-08-08T12:42:37.711098-04:00 gigamonTA200 sshd[22323]: pam_unix(sshd:session): session closed for user admin
Failure of the trusted path functions	**Failure of the trusted path functions (SSH)** 2022-04-05T10:49:20.775557-04:00 gigamonTA200 sshd[8128]: Connection from 192.168.1.98 port 51426 on 192.168.1.210 port 22 2022-04-05T10:49:20.777225-04:00 gigamonTA200 sshd[8128]: Unable to negotiate with 192.168.1.98 port 51426: no matching host key type found. Their offer: ssh-rsa [preauth]

Table 4: Sample Audit Records

8.1 Audit Storage

New audit records are stored locally on the TOE under the /var/log directory in the file named “messages". The "message" file is archived when it reaches a specific size (8 MB) by compressing it and saving the file as "messages.1.gz”. Meanwhile, a new "messages" file is created for new audit records and the other compressed messages files are rotated so that the 8 most recent compressed messages files are saved. The 8 compressed files are named "messages.1.gz”, “messages2.gz”, and so on. Therefore, as part of the file rotation “messages8.gz” will be deleted, "messages.7.gz" will be saved as "messages.8.gz", "messages.6.gz" will be saved as "messages.7.gz", and so on until the "messages" file is compressed into "messages.1.gz”. This mechanism guarantees a maximum limit of disk usage used by the log files.

The TOE allows viewing of the audit records through the CLI with the following command:

```
enable
config terminal
show log
```

Users of any role can view audit log files, however, only Admin users can delete audit log files. No modification of log files is permitted, regardless of role. If an Admin deletes a log file, an audit record of that action is also recorded. Users with the Admin role are considered trusted users and are not expected to delete the audit records.

The TOE generates audit records which are stored locally or on a configured audit server. Once the audit server is configured audit records are stored both locally and also sent immediately to the audit server over an SSH encrypted channel. Section 8.1.1 explains how to create an SSH ECDSA key and configure communications with the audit server.

If the audit server connectivity is unavailable, audit records will only be stored locally. Upon re-establishment of communications with the audit server, new audit records will resume being transmitted to it but the audit records that were generated during the time the audit server connection was down remain stored locally and are not sent to the audit server.

The TOE allows deleting audit logs through the CLI with the following command:

```
enable
config terminal
```

```
log files delete <CURRENT | OLDEST [NUMBER]>
```

8.1.1 Configuring the Audit Server

In order for the communications between the TOE and the audit server to be encrypted by SSH, an ECDSA key with 256-bit key size must be generated on the TOE, which acts as the SSH client, and copied over to the audit server which acts as the SSH server. This is achieved by the following steps.

1. Create the ECDSA key on the TOE using the command:

```
enable
config terminal
ssh client user <USERNAME> identity ecdsa generate
show ssh client
```

2. Copy the ECDSA public key to audit server and insert it into the "~/.ssh/authorized_keys" file.

The "logging" command is used to configure the audit server. For more information on the "logging" command, refer to the 'logging' section in document [2] beginning on page 278. The configuration must be performed by an Admin user via the CLI and the following commands must be used in the evaluated configuration of the TOE for connecting to an audit server.

```
enable
config terminal
logging <AUDIT_SERVER_IP_ADDRESS> tcp <0-65535> ssh username <USERNAME>
logging trap info
```

9 Communications Protocols and Services

In the evaluated configuration, the SSH2 protocol was tested for remote administration and secure transfer of audit data to the audit server. TLS was also tested in the evaluated configuration to secure the LDAP server trusted channel. The product supports numerous communications protocols in support of the data plane operations that were not evaluated as part of the Common Criteria evaluation because they provide functionality that is not assessed by the Protection Profile. These protocols include the following:

- ARP
- CDP
- DHCP
- DHCPv6
- FTP
- GRE
- GTP
- HTTP
- IGMP
- ICMP
- ISL
- IPv4

- IPv6
- LLDP
- MPLS
- NTP
- RADIUS
- RSVP
- SCP
- SFTP
- SNMP
- SSL
- TACACS+
- TCP
- TFTP
- UDP

Information about the configuration and usage of these protocols can be found in the standard Gigamon documentation for the product as specified in Section 4 of this document.

10 Obtaining Technical Assistance

Gigamon offers technical assistance through their website: www.gigamon.com under the heading "Support and Services". There is a specific customer support portal with website: https://gigamoncp.force.com/gigamoncp/ where customers can login with a username and password.

Support in North American can be contacted using the telephone number: +1 855-430-0813 (Toll Free). In addition, the support team can be contacted by email at: support@gigamon.com

Other support contact information can be found at: https://www.gigamon.com/support-and-services/contact-support