Cellcrypt Federal Stack - Auditing and Monitoring

02/22/2022

Legal

Information in this document is subject to change without notice. Cellcrypt Inc. makes no warranty of any kind with regard to this information, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Cellcrypt Inc. and the authors shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

Warning: This document is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Patents pending Cellcrypt Inc.

Every effort has been made to ensure that the contents of this document are correct. However, neither the authors nor Cellcrypt Inc. accept any liability for loss or damage caused or alleged to be caused directly or indirectly by this document.

Table of Contents

1 Introduction

This manual will provide instructions on how to audit each component of the Cellcrypt Stack.

As this is a technical manual, it is worth mentioning that more information about how auditing works is available on the **Auxiliary services - Audit** section of the **Technical Specifications and Requirements** manual.

If you have any questions or concerns, please contact us at support@csghq.com.

2 Paths to Logs

Detailed location of the log files for every instance of the Cellcrypt Stack.

2.1 DB

2.1.1 MariaDB

- Database Errors and Warnings:

  ```
  /var/log/mariadb/mariadb.log
  ```

2.2 API

2.2.1 Nginx

- TLS Access - Registers every TLS connection to the HTTPS Proxy

  ```
  /var/log/nginx/api.domain.com-access.log
  ```

- TLS Error - Registers every TLS error when connecting to the HTTPS Proxy

  ```
  /var/log/nginx/api.domain.com-error.log
  ```

2.2.2 Stunnel

- Stunnel service logs

```
/var/log/stunnel/stunnel.log
```

2.3 ECS

2.3.1 ECS Supervisor

- ECS actions and errors

```
/var/log/supervisor/ecs-stderr-*
```

- ECS Connectivity errors

```
/var/log/supervisor/ecs-stdout-*
```

- Sync actions and errors

```
/var/log/supervisor/sync-emp-stderr-*
```

- Sync Connectivity errors

```
/var/log/supervisor/sync-emp-stdout-*
```

- Supervisor Log - Registers whenever server is spawned, stopped or rebooted.

```
/var/log/supervisor/supervidord.log
```

2.3.2 Asterisk

- Asterisk logs, actions and error messages

```
/var/log/asterisk/messages
```

2.3.3 Nginx

- TLS Access - Registers every TLS connection to the HTTPS Proxy

```
/var/log/nginx/ecs.domain.com-access.log
```

- TLS Error - Registers every TLS error when connecting to the HTTPS Proxy

```
/var/log/nginx/ecs.domain.com-error.log
```

2.4 SAS

2.4.1 SAS Supervisor

- SAS NodeJS Workers logs, actions and error messages

```
/var/log/supervisor/*
```

- Backend-v4 transactions, messages and logs

```
/var/log/supervisor/backend-v4-*
```

- Supervisor Log - Registers whenever server is spawned, stopped or rebooted.

```
/var/log/supervisor/supervidord.log
```

2.4.2 Secure Application Server

- SAS Gearman Workers logs, actions and error messages

```
/var/log/secure-application-server/*
```

2.4.3 Gearman

- Gearman server runtime errors

```
/var/log/gearman-job-server/gearman.log
```

2.4.4 Redis

- Redis operations logs

```
/var/log/redis/redis-server.log
```

2.4.5 Revinetd

- Revinetd transactions and connections logs

```
/var/log/supervisor/sip-reverse-stderr-*
```

2.4.6 Stunnel

- Stunnel service logs

```
/var/log/stunnel/stunnel.log
```

2.5 SIP

2.5.1 SIP Supervisor

- Revinetd - SIP Reverse service logs

```
/var/log/supervisor/sip-reverse-stderr-*
```

- Supervisor Log - Registers whenever server is spawned, stopped or rebooted.

```
/var/log/supervisor/supervidord.log
```

2.5.2 Opensips

- Registers every SIP connection attempt

```
/var/log/opensips.log
```

2.5.3 Stunnel

- Stunnel service logs

```
/var/log/stunnel/stunnel.log
```

2.6 Vault

2.6.1 Vault Supervisor

- Vault service file download/upload notices and error logs

```
/var/log/supervisor/vault-v3-stderr-*
```

2.6.2 **Nginx**

- TLS Access - Registers every TLS connection to the HTTPS Proxy

```
/var/log/nginx/vault.domain.com-access.log
```

- TLS Error - Registers every TLS error when connecting to the HTTPS Proxy

```
/var/log/nginx/vault.domain.com-error.log
```

2.7 Portal (EMP/My)

2.7.1 Laravel

- Registers Portal events, actions and errors

```
/opt/secure/portal/app/storage/logs/laravel.log
```

2.7.2 **Nginx**

- TLS Access - Registers every TLS connection to the HTTPS Proxy (EMP)

```
/var/log/nginx/emp.domain.com-access.log
```

- TLS Error - Registers every TLS error when connecting to the HTTPS Proxy (EMP)

```
/var/log/nginx/emp.domain.com-error.log
```

- TLS Access - Registers every TLS connection to the HTTPS Proxy (MY)

```
/var/log/nginx/my.domain.com-access.log
```

- TLS Error - Registers every TLS error when connecting to the HTTPS Proxy (MY)

```
/var/log/nginx/my.domain.com-error.log
```

2.7.3 Stunnel

- Stunnel service logs

```
/var/log/stunnel/stunnel.log
```

2.8 AUX

2.8.1 Nginx

- TLS Access - Registers every TLS connection to the HTTPS Proxy

```
/var/log/nginx/aux.domain.com-access.log
```

- TLS Error - Registers every TLS error when connecting to the HTTPS Proxy

```
/var/log/nginx/aux.domain.com-error.log
```

2.9 Shared logs

2.9.1 Syslog

- All log messages sent to syslog.

```
/var/log/messages
```

2.9.2 NTP

- Every NTP related statistic and log.

```
/var/log/ntpstats/*
```

2.9.3 SSH

- SSH daemon logs.

```
/var/log/secure
```

3 Stack Auditing

Many of the auditing features of the application were designed in order to comply with NIAP Requirements and are enabled by default.

This informative section provides insights on what requirements are fulfilled and where you can find those pieces of information.

3.1 DB

Network Device NDcPP Ref	Event	Where to find it	Evidence
FMT_SMF.1	Database query	-	-

3.2 API

Network Device NDcPP Ref	Event	Where to find it	Evidence
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	/var/log/nginx/api-[DOMAIN]-error.log	
FCS_TLSC_EXT.1	Failure to establish a TLS Session	/var/log/nginx/api-[DOMAIN]-error.log	

FCS_TLSS_EXT.1	Failure to establish a TLS Session	/var/log/nginx/api-[DOMAIN]-error.log	

3.3 EMP

Network Device NDcPP Ref	Event	Where to find it	Evidence
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	-	-
FAU_GEN.1.1	Resetting passwords	/var/log/messages /opt/secure/portal/app/storage/logs/laravel.log	
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	/var/log/nginx/emp-[DOMAIN]-error.log	
FCS_TLSC_EXT.1	Failure to establish a TLS Session	/var/log/nginx/emp-[DOMAIN]-error.log	

FCS_TLSS_EXT.1	Failure to establish a TLS Session	/var/log/nginx/emp-[DOMAIN]-error.log	

3.4 MY

Network Device NDcPP Ref	Event	Where to find it	Evidence
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	/var/log/nginx/my-[DOMAIN]-error.log	
FCS_TLSC_EXT.1	Failure to establish a TLS Session	/var/log/nginx/my-[DOMAIN]-error.log	
FCS_TLSS_EXT.1	Failure to establish a TLS Session	/var/log/nginx/my-[DOMAIN]-error.log	

3.5 SAS

Network Device NDcPP Ref	Event	Where to find it	Evidence
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	/var/log/messages	

FIA_UAU_EXT.2	All use of identification and authentication mechanism.	/var/log/messages	
FMT_SMF.1	All management activities of TSF data.	/var/log/messages	
FCS_TLSC_EXT.1	Failure to establish a TLS Session	/var/log/stunnel/stunnel.log	
FCS_TLSS_EXT.1	Failure to establish a TLS Session	/var/log/stunnel/stunnel.log	
FCS_TLSS_EXT.2	Failure to authenticate the client	/var/log/stunnel/stunnel.log	
-	activate_remote_wipe -	/var/log/messages	
-	authenticate_admin_user	/var/log/messages	
-	admin_logout	/var/log/messages	
-	admin_session_expired	/var/log/messages	
-	send_password_reset_mail	/var/log/messages	
-	check_password_reset	/var/log/messages	

-	reset_password	/var/log/messages	
-	add_admin_user_partner_group	/var/log/messages	
-	create_admin_user	/var/log/messages	
-	delete_admin_user	/var/log/messages	
-	user_register	/var/log/messages	
-	modify_user_roles	/var/log/messages	
-	update_by_id	/var/log/messages	
-	device_update_status	/var/log/messages	
-	add_alias	/var/log/messages	
-	remove_alias	/var/log/messages	
-	remove_account	/var/log/messages	
-	auth_my_user	/var/log/messages	

-	user_logout	/var/log/messages	

3.6 Vault

Network Device NDcPP Ref	Event	Where to find it	Evidence
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	/var/log/nginx/vault-[DOMAIN]-error.log	
FCS_TLSC_EXT.1	Failure to establish a TLS Session	/var/log/nginx/vault-[DOMAIN]-error.log	
FCS_TLSS_EXT.1	Failure to establish a TLS Session	/var/log/nginx/vault-[DOMAIN]-error.log	

3.7 SIP

Network Device NDcPP Ref	Event	Where to find it	Evidence

FAU_GEN.1/CDR	Audit Data Generation (Call Detail Record)	/var/log/opensips.log	2022-12-07T19:17:55.672734+00:00 sip-* /usr/local/sbin/opensips[35710]: ACC: call ended: created=1645211866;call_start_time=1645211867;duration=8;ms_duration=8296;setuptime=1;method=INVITE;from_tag=fa6f84b3-38a2-4709-8ffd-3e10f52df51d;to_tag=809ab268-06ba-41e1-9f03-4270ebe692af;call_id=ba07fafd-963c-4639-a454-6bba4627c887;code=200;reason=OK;src_ip=;dst_ip=13.90.174.9;call_end_time=1645211875;call_type=Audio;caller=;callee=
FIA_UAU.2/VVoIP	Successful or failed registration of VVoIP endpoint/device	/var/log/opensips.log	
FIA_UAU.2/VVoIP	Authentication of external VvoIP endpoint/device	/var/log/opensips.log	
FMT_SMF.1	Enabling/disabling VVoIP endpoint/device features	/var/log/opensips.log	
FCS_TLSS_EXT.2	Failure to authenticate the client	/var/log/opensips.log	

3.8 Aux

Network Device NDcPP Ref	**Event**	**Where to find it**	**Evidence**

FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	/var/log/nginx/aux-[DOMAIN]-error.log	

4 NIAP Compliant Auditing Features

Some of the auditing features required by NIAP are available once the audit module is installed.

This section explains in further detail each of the available features provided.

4.1 Start-up/shutdown date/time of audit functions

FAU_GEN.1.1 mandates that the TOE shall generate an audit record of the start-up and shutdown of the audit functions

```
Jul 23 14:49:34 ip-172-31-33-210.us-west-2.compute.internal auditd[2207]: The audit daemon is exiting.

Jul 23 14:49:36 ip-172-31-33-210.us-west-2.compute.internal systemd[1]: Starting Security Auditing Service...

Jul 23 14:49:36 ip-172-31-33-210.us-west-2.compute.internal auditd[22693]: Started dispatcher: /sbin/audispd pid: 22695

Jul 23 14:49:36 ip-172-31-33-210.us-west-2.compute.internal auditd[22693]: Init complete, auditd 2.8.4 listening for events (startup state enable)
```

4.2 IP connections

FAU_GEN.1.1/Log states that the TSF shall be able to generate a system log record of IP connections.

Nftables outputs any IP connections directly into the syslog file.

Example output for IP Connections:

```
Aug 5 19:07:41 ip-172-31-33-210 kernel: LOG_IPTABLES_PING_REQUEST: IN=eth0 OUT=
MAC=06:d6:65:61:b7:fe:06:b1:01:79:45:47:08:00 SRC=179.184.19.129 DST=172.31.33.210 LEN=84 TOS=0x00
PREC=0x00 TTL=38 ID=6627 DF PROTO=ICMP TYPE=8 CODE=0 ID=32536 SEQ=200

Aug 5 19:07:42 ip-172-31-33-210 kernel: LOG_IPTABLES_PING_REQUEST: IN=eth0 OUT=
MAC=06:d6:65:61:b7:fe:06:b1:01:79:45:47:08:00 SRC=179.184.19.129 DST=172.31.33.210 LEN=84 TOS=0x00
PREC=0x00 TTL=38 ID=6791 DF PROTO=ICMP TYPE=8 CODE=0 ID=32536 SEQ=201

Aug 5 19:07:43 ip-172-31-33-210 kernel: LOG_IPTABLES_PING_REQUEST: IN=eth0 OUT=
MAC=06:d6:65:61:b7:fe:06:b1:01:79:45:47:08:00 SRC=179.184.19.129 DST=172.31.33.210 LEN=84 TOS=0x00
PREC=0x00 TTL=38 ID=6835 DF PROTO=ICMP TYPE=8 CODE=0 ID=32536 SEQ=202
```

Note**:** Per FAU_GEN.1/CDR's test no. 1, the IP connections are tested through the "ping" command (hence the log format shown above)

4.3 Miscellaneous status logs

FAU_GEN.1.1/Log also calls for disk and file storage capacity, NTP status, CPU usage, memory usage, audit storage capacity and fan status. The evaluation tests revolve around monitoring said parameters for a 10-minute period and performing calls/messaging. These are handled using a simple shell script to forward the outputs from existing OS monitoring services. The OS utility top is used for CPU/memory status, and df, for available disk space. These outputs are redirected to the syslog log file.

Disk/file storage capacity:

```
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: Filesystem Size Used Avail Use% Mounted on
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: /dev/xvda2 10G 3.4G 6.7G 34% /
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: devtmpfs 897M 0 897M 0% /dev
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 919M 0 919M 0% /dev/shm
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 919M 79M 840M 9% /run
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 919M 0 919M 0% /sys/fs/cgroup
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 184M 0 184M 0% /run/user/1000
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 184M 0 184M 0% /run/user/0
```

NTP Status:

```
Aug 5 18:55:01 ip-172-31-33-210 ntpstat: synchronised to NTP server (204.11.201.10) at stratum 3
Aug 5 18:55:01 ip-172-31-33-210 ntpstat: time correct to within 37 ms
Aug 5 18:55:01 ip-172-31-33-210 ntpstat: polling server every 1024 s
```

CPU/Memory usage:

```
Aug 6 14:41:54 ip-172-31-33-210 top: top - 14:41:54 up 19 days, 3:04, 2 users, load average: 0.00, 0.01, 0.05
Aug 6 14:41:54 ip-172-31-33-210 top: Tasks: 182 total, 2 running, 180 sleeping, 0 stopped, 0 zombie
Aug 6 14:41:54 ip-172-31-33-210 top: %Cpu(s): 0.0 us, 6.2 sy, 0.0 ni, 93.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Aug 6 14:41:54 ip-172-31-33-210 top: KiB Mem : 1880524 total, 64660 free, 1247988 used, 567876 buff/cache
Aug 6 14:41:54 ip-172-31-33-210 top: KiB Swap: 0 total, 0 free, 0 used. 352988 avail Mem
Aug 6 14:41:54 ip-172-31-33-210 top: mbie
Aug 6 14:41:54 ip-172-31-33-210 top: PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
Aug 6 14:41:54 ip-172-31-33-210 top: 21324 ec2-user 20 0 162028 2104 1540 R 6.2 0.1 0:00.01 top
Aug 6 14:41:54 ip-172-31-33-210 top: 1 root 20 0 128148 5032 2504 S 0.0 0.3 4:03.70 systemd
Aug 6 14:41:54 ip-172-31-33-210 top: 2 root 20 0 0 0 0 S 0.0 0.0 0:00.36 kthreadd
```

4.4 Local Administrative Logins

The first item of FAU_GEN.1.1 states that all administrative login and logout events must be accounted for, as well as the start/stop of trusted channels.

The stack handles this by setting watching rules on login/logout binaries, which, in addition to "aureport -l" functionality, produces reports on all login attempts on the server.

The aulast package is used for trusted channels initiation/termination info. Additionally, rsyslog is configured to audit all attempts to initiate a super-user session (including commands such as sudo).

Login info:

```
Login Report
============================================
# date time auid host term exe success event
============================================
1. 08/06/2019 15:50:09 ec2-user 200.175.61.81.static.gvt.net.br /dev/pts/0 /usr/sbin/sshd yes 919456
2. 08/06/2019 18:13:41 ec2-user 200.175.61.81.static.gvt.net.br /dev/pts/0 /usr/sbin/sshd yes 919808
3. 08/07/2019 09:17:17 ec2-user 200.175.61.81.static.gvt.net.br /dev/pts/0 /usr/sbin/sshd yes 921179
4. 08/07/2019 13:24:55 ec2-user 200.175.61.81.static.gvt.net.br /dev/pts/0 /usr/sbin/sshd yes 921613
5. 08/07/2019 13:27:52 ec2-user 200.175.61.81.static.gvt.net.br /dev/pts/0 /usr/sbin/sshd yes 921820
6. 08/07/2019 14:46:53 ec2-user 200.175.61.81.static.gvt.net.br /dev/pts/0 /usr/sbin/sshd yes 924724
7. 08/07/2019 16:05:17 ec2-user 200.175.61.81.static.gvt.net.br /dev/pts/0 /usr/sbin/sshd yes 926211
```

Trusted channel info:

```
ec2-user pts/0 179.184.19.129.s Mon Aug 5 18:16 - 19:58 (01:41)
ec2-user ssh 200.175.61.81.st Mon Aug 5 20:27 - 20:27 (00:00)
ec2-user pts/2 200.175.61.81.st Mon Aug 5 19:24 - 22:42 (03:17)
ec2-user pts/5 200.175.61.81.st Mon Aug 5 19:52 - 23:59 (04:06)
ec2-user pts/2 200.175.61.81.st Tue Aug 6 14:28 - 14:38 (00:09)
ec2-user pts/0 179.184.19.129.s Tue Aug 6 14:20 - 14:43 (00:23)
ec2-user pts/2 200.175.61.81.st Tue Aug 6 14:38 still logged in
```

Super-user sessions:

```
Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_tty_audit(sudo:session): unknown option `ec2-user'
Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_tty_audit(sudo:session): changed status from 1 to 1
Aug 8 20:41:39 ip-172-31-33-210 sudo: pam_unix(sudo:session): session closed for user root
Aug 8 20:41:54 ip-172-31-33-210 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/systemctl restart rsyslog
```

4.5 Bad SSH Authentication

FAU_GEN.1.1 also requires the TOE to log unsuccessful login attempts, including when they exceed some preset limit. The TOE uses auditd's own summary reporting plugin - aureport - and through specifying auditing rules for the pam_tty service.

Example output:

```
aureport -i -au --failed

Authentication Report
=============================================
# date time acct host term exe success event
=============================================
1. 07/31/2019 12:29:42 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 845672
2. 07/31/2019 13:12:40 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 845839
3. 07/31/2019 13:31:19 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 845872
4. 07/31/2019 19:01:13 ec2-user 200.175.61.81 ssh /usr/sbin/sshd no 848199
5. 07/31/2019 19:28:00 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 848260
```

4.6 Changes to Time and Date

The FPT_STM_EXT.1 requirement makes it necessary to audit any discontinuous changes in time. Monitoring time-related binaries and executables (see example below) audit any attempts to discontinuous time changes on the stack.

Example output:

Summary report of executables involved in changing TOE server's timezone

```
Executable Report
===================================
# date time exe term host auid event
===================================
332. 08/06/2019 13:23:34 /usr/lib/systemd/systemd ? ? unset 877714
333. 08/06/2019 13:23:34 /usr/lib/systemd/systemd-timedated (none) ? unset 877713
334. 08/06/2019 13:23:34 /usr/lib/systemd/systemd-timedated (none) ? unset 877715
335. 08/06/2019 13:24:04 /usr/lib/systemd/systemd ? ? unset 877716
336. 08/06/2019 13:25:45 /usr/lib/systemd/systemd ? ? unset 877729
337. 08/06/2019 13:25:45 /usr/bin/timedatectl pts0 ? administrator 877726
338. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset 877728
339. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset 877731
340. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset 877732
```

4.7 Manual Update Attempts

FMT_MOF.1/ManualUpdate mandates that all attempts to initiate a manual code update must be audited. Even though FPT_TUD_EXT.1 events are no longer needed to be audited (initiation/result of update attempts), logging the outputs of the manual updates fulfils both requirements.

Direct modifications to the setup script were made to log all update messages prompted. E.g.:

```
Aug 6 18:31:54 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Running precondition checks.
Aug 6 18:32:50 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Running precondition checks.
Aug 6 18:32:50 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Configuring system.
Aug 6 18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Starting services.
Aug 6 18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Running final checks.
Aug 6 18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Installed.
```

4.8 Call Detail Records

The protected local logs include the Call Detail Records (CDR's). These permissions are automatically set during the TOE software installation process. The CDR's are generated by the ESC OpenSIPS service and consist of the following information:

- TOE unique identifier
- Call originator identifier
- Call receiver identifier
- Unique transaction sequence number
- Call status (missed / connected / terminated / failures)
- Call type (voice / voice + video)
- Call start time
- Call end time
- Call duration
- Call direction (incoming / outgoing)
- Call routing into TOE
- Call routing out of TOE
- Time zone

Example call log showing CDR details:

```
2022-02-18T19:17:55.672734+00:00 sip-alpha /usr/local/sbin/opensips[35710]: ACC: call ended:
created=1645211866;call_start_time=1645211867;duration=8;ms_duration=8296;setuptime=1;method=INVIT
E;from_tag=fa6f84b3-38a2-4709-8ffd-3e10f52df51d;to_tag=809ab268-06ba-41e1-9f03-4270ebe692af;call_id=
ba07fafd-963c-4639-
a454-6bba4627c887;code=200;reason=OK;src_ip=;dst_ip=13.90.174.9;call_end_time=1645211875;call_type=A
udio;caller=;callee=
```

4.9 Shared auditing information

This information is produced on every machine running any of the Cellcrypt stack services.

4.10 SSH / Direct access

Network Device NDcPP Ref	Event	Where to find it	Evidence
FCS_SSHS_EXT.1	Failure to establish an SSH session	/var/log/messages	

4.11 NTP

Network Device NDcPP Ref	Event	Where to find it	Evidence
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	/var/log/ntpstats/*	

4.12 Hardware information

Network Device NDcPP Ref	Event	Where to find it	Evidence

FAU_GEN.1/Log	CPU and Memory usage	/var/log/messages	2021-12-06T11:09:30.302105-05:00 api-* top: top - 14:41:54 up 19 days, 3:04, 2 users, load average: 0.00, 0.01, 0.05 2021-12-06T11:09:30.302105-05:00 api-* top: Tasks: 182 total, 2 running, 180 sleeping, 0 stopped, 0 zombie 2021-12-06T11:09:30.302105-05:00 api-* top: %Cpu(s): 0.0 us, 6.2 sy, 0.0 ni, 93.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st 2021-12-06T11:09:30.302105-05:00 api-* top: KiB Mem : 1880524 total, 64660 free, 1247988 used, 567876 buff/cache 2021-12-06T11:09:30.302105-05:00 api-* top: KiB Swap: 0 total, 0 free, 0 used. 352988 avail Mem 2021-12-06T11:09:30.302105-05:00 api-* top: mbie 2021-12-06T11:09:30.302105-05:00 api-* top: PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND 2021-12-06T11:09:30.302105-05:00 api-* top: 21324 admin 20 0 162028 2104 1540 R 6.2 0.1 0:00.01 top 2021-12-06T11:09:30.302105-05:00 api-* top: 1 root 20 0 128148 5032 2504 S 0.0 0.3 4:03.70 systemd 2021-12-06T11:09:30.302105-05:00 api-* top: 2 root 20 0 0 0 0 S 0.0 0.0 0:00.36 kthreadd
FAU_GEN.1/Log	NTP Status	/var/log/messages	2021-12-06T11:09:30.302105-05:00 api-* ntpstat: synchronised to NTP server (204.11.201.10) at stratum 3 2021-12-06T11:09:30.302105-05:00 api-* ntpstat: time correct to within 37 ms 2021-12-06T11:09:30.302105-05:00 api-* ntpstat: polling server every 1024 s

FAU_GEN.1/Log	Disk and file storage capacity	/var/log/messages	2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: Filesystem Size Used Avail Use% Mounted on 2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: /dev/xvda2 10G 3.4G 6.7G 34% / 2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: devtmpfs 897M 0 897M 0% /dev 2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: tmpfs 919M 0 919M 0% /dev/shm 2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: tmpfs 919M 79M 840M 9% /run 2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: tmpfs 919M 0 919M 0% /sys/fs/cgroup 2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: tmpfs 184M 0 184M 0% /run/user/1000 2021-12-06T11:09:30.302105-05:00 api-* kernel: df -h: tmpfs 184M 0 184M 0% /run/user/0

4.13 General system activity

Network Device NDcPP Ref	Event	Where to find it	Evidence
FAU_GEN.1.1	Start-up and shutdown of the audit functions	/var/log/messages	2021-12-06T11:09:31.340131-05:00 api-* auditd[1548]: Init complete, auditd 2.8.5 listening for events (startup state enable)
FAU_GEN.1.1	Changes to TSF data related to configuration changes	/var/log/aide/aide.log	

FAU_GEN.1.1	Generating/import of, changing, or deleting of cryptographic keys	-	
FAU_GEN.1.1	Administrative login and logout	/var/log/audit/audit.log	Login Report === # date time auid host term exe success event === 1. 08/06/2019 15:50:09 admin 172.31.33.210 /dev/pts/0 /usr/sbin/sshd yes 919456 2. 08/06/2019 18:13:41 admin 172.31.33.210 /dev/pts/0 /usr/sbin/sshd yes 919808 3. 08/07/2019 09:17:17 admin 172.31.33.210 /dev/pts/0 /usr/sbin/sshd yes 921179 4. 08/07/2019 13:24:55 admin 172.31.33.210 /dev/pts/0 /usr/sbin/sshd yes 921613 admin pts/5 172.31.33.210.st Mon Aug 5 19:52 - 23:59 (04:06) admin pts/2 172.31.33.210.st Tue Aug 6 14:28 - 14:38 (00:09) admin pts/0 179.184.19.129.s Tue Aug 6 14:20 - 14:43 (00:23) admin pts/2 172.31.33.210.st Tue Aug 6 14:38 still logged in

			Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_unix(sudo:session): session opened for user root by admin(uid=0) Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_tty_audit(sudo:session): unknown option `administrator' Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_tty_audit(sudo:session): changed status from 1 to 1 Aug 8 20:41:39 ip-172-31-33-210 sudo: pam_unix(sudo:session): session closed for user root Aug 8 20:41:54 ip-172-31-33-210 sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/systemctl restart rsyslog
FAU_GEN.1.1/ Log	Current IP connections	/var/log/ messages	2021-12-06T11:09:33.134510-05:00 api-* kernel: LOG_IPTABLES_PING_REQUEST: IN=eth0 OUT= MAC=06:d6:65:61:b7:fe:06:b1:01:79:45:47:08:00 SRC=179.184.19.129 DST=172.31.33.210 LEN=84 TOS=0x00 PREC=0x00 TTL=38 ID=6627 DF PROTO=ICMP TYPE=8 CODE=0 ID=32536 SEQ=200

FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update.	/var/log/ messages	2021-12-06T18:31:54 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Running precondition checks. 2021-12-06T18:32:50 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Running precondition checks. 2021-12-06T18:32:50 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Configuring system. 2021-12-06T18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Starting services. 2021-12-06T18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Running final checks. 2021-12-06T18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m: Installed.
FIA_X509_EXT .1/ITT	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store		

FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1).	/var/log/audit/audit.log	==================================== # date time exe term host auid event ==================================== 332. 08/06/2019 13:23:34 /usr/lib/systemd/systemd ? ? unset 877714 333. 08/06/2019 13:23:34 /usr/lib/systemd/systemd-timedated (none) ? unset 877713 334. 08/06/2019 13:23:34 /usr/lib/systemd/systemd-timedated (none) ? unset 877715 335. 08/06/2019 13:24:04 /usr/lib/systemd/systemd ? ? unset 877716 336. 08/06/2019 13:25:45 /usr/lib/systemd/systemd ? ? unset 877729 337. 08/06/2019 13:25:45 /usr/bin/timedatectl pts0 ? admin 877726 338. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset 877728 339. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset 877731 340. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset 877732
FTA_SSL_EXT.1 (if “lock the session” is selected)	Any attempts at unlocking of an interactive session.		
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.		

FTA_SSL.3	The termination of a remote session by the session locking mechanism.		
FTA_SSL.4	The termination of an interactive session.		
FPT_TUD_EXT.2	Failure of update		
FIA_UAU.2/TC	Successful or failed authentication of trunk connected network component		
FAU_STG_EXT.3/LocSpace	Low storage space for audit events.		
FIA_X509_EXT.1/ITT	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store		

FPT_ITT.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.		
FTP_TRP.1/ Join	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.		