Greenbone Support Package for GOS 20.08

Technical Documentation

TechPaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

Contents

CHAPTER 1

About this Document

This technical documentation describes the contents of the Greenbone Support Package as created by Greenbone OS version 20.08.

Such packages collect various information about the system state and system logs and are meant to help the Greenbone Support Team or even the Greenbone Development Team to troubleshoot a problem.

The Greenbone Support Package can be created via the GOS administration as described in the User Manual: https://docs.greenbone.net/GSM-Manual/gos-20.08/en/managing-gos.html#generating-and-downloading-a-support-package

The created package is a zip archive file that at user's option is either encrypted with the public GPG key owned by the Greenbone Support Team or it is unencrypted for the user to review and strip-down prior to a submission to Greenbone Support Team.

This documentation describes the content of the zip archive files and provides hints on where to find which type of information. It is the user's choice or customer's policy which pieces of information are regarded sensible and thus removed or anonymized.

CHAPTER 2

Environment-Specific Information

Most parts from the journal log and the status of any services are in the Greenbone Support Package. Some logs may contain information specific to the customer environment like IP addresses:

Passwords:

No passwords are included in the support package.

IP and/or MAC addresses may occur in the following files:

gsm-backup/ssh_known_host

gsm-feed (IP addresses about ftp server)

gsm-greenbone-security-assistant/greenbone-security-assistant.journal (login attempts)

gsm-greenbone-security-assistant/greenbone-security-assistant-systemctl (login attempts)

gsm-greenbone-vulnerability-manager/gvmd-journal (scan targets)

gsm-greenbone-vulnerability-manager/gvmd-systemctl (scan targets)

gsm-logging/auth.log (login attempts)

gsm-logging/gsmlog

gsm-master/ssh_config (sensor IP addresses)

gsm-master/sensor_ports.tsv (sensor ports with IP addresses)

gsm-master/check_protocols-journal (failed sensor IP addresses)

gsm-network/interfaces

gsm-network/interfaces.d/*

gsm-network/networking-journal (e.g., DHCP messages)

gsm-network/networking-systemctl (e.g., DHCP messages)

gsm-network/resolv.conf

gsm-network-namespaces/interfaces

gsm-network-namespaces/resolv.conf

gsm-openvas/openvas-journal (scan targets)

gsm-sshd/ssh-journal (login attempts)

gsm-timesyncd (IP addresses about timeserver)

ospd-openvas/ospd-openvas-journal (scan targets)

ospd-openvas/ospd-openvas-systemctl (scan targets)

Commands executed as admin user:

gsm-cli-admin/.bash_history

Commands executed as root user:

gsm-cli-admin/root-command-journal

gsm-cli-admin/sudo-journal

Commands executed as postgres user:

gsm-greenbone-vulnerability-manager/gvmd_psql_history

gsm-greenbone-vulnerability-manager/postgres_bash_history

gsm-greenbone-vulnerability-manager/postgres_psql_history

CHAPTER 3

Content of the Greenbone Support Package

The following list shows the contents of each folder in the package. The folders correspond to the respective modules and the modules are in alphabetical order. There are up to five sections for a module:

- Files: the files that are copied 1:1 into the package.
- Journal: excerpt from the journal log for the module. The applied filter command is provided.
- Service status: the status of a service at the time the package was created.
- Command output: the executed shell commands whose output is redirected into the file `commands.txt`.
- Included information: description text about the nature and topic of the contents.

For a better understanding, all commands used for gathering information are provided as well.

All files directly copied into the support package are also listed here:

- Service status
  - systemctl_overview.txt (command: `systemctl`)
- Included information
  - Global overview of all system services.

3.1 gos-ansible

- Files
  - /var/log/gos-ansible.log
  - /var/log/gos-ansible.oldlogs/*
- Included information
  - Status of configuration files and processes

3.2 gos-state-manager

- Journal
  - state_migration-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=state_migration`)
- Command output
  - `gos-state-manager dump beautify`
- Included information
  - Logs about migration (result message)
  - Selected GOS state values are written to `commands.txt`. **By default, any sensitive data is filtered out.** To include more (potentially helpful) data the GOS state `support_package_policy` may be set via admin shell with:

    ```
    set support_package_policy [strict|moderate|complete] && save
    ```

    The default is `strict`.

    strict: like moderate but also exclude network information like IP addresses, host names

    moderate: exclude sensitive data like user names, passwords, keys

    complete: will contain all variables

3.3 greenbone-sourcefire-connector

- Journal
  - greenbone-sourcefire-connector-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=greenbone-sourcefire-connector`)

3.4 greenbone-verinice-connector

- Journal
  - verinice-connector-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=verinice-connector`)

3.5 greenbone-vfire-connector

- Journal
  - vfire-connector-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=vfire-connector`)

3.6 gsm-backup

- Files
  - /etc/obnam.conf
  - /etc/cron.daily/10-gsm-backup
  - /var/lib/gsm-backup/ssh_known_host
- Journal
  - gsm-backup-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=gsm-backup`)
  - gsm-restore-journal (command: `journalctl -output=json SYSLOG_IDENTIFIER=gsm-restore`)
  - usb-backup-journal (command: `journalctl -output=json SYSLOG_IDENTIFIER=usb-backup`)
  - usb-restore-journal (command: `journalctl -output=json SYSLOG_IDENTIFIER=usb-restore`)
  - obnam-journal (command: `journalctl -output=json SYSLOG_IDENTIFIER=obnam`)
  - gos-restic-journal (command: `journalctl -output=json SYSLOG_IDENTIFIER=gos-restic`)
- Command output
  - `gos-restic -q -q check --check-unused`
  - `gos-restic -q -q check`
  - `gos-restic -q -q snapshots | tail -1`
  - `gos-restic -q -q stats --mode raw-data -v`
  - `gos-restic -q -q stats latest --mode raw-data -v`
- Included information
  - Timestamps of started and finished backup services
  - List of files to backup
  - Backup repository configuration and statistics

3.7 gsm-cli-admin

- Files
  - /home/admin/.bash_history
- Journal
  - pyspatch-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=pyspatch`)
  - root-command-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=root-command`)
  - sudo-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=sudo`)

- Included information
  - All commands executed as admin user
  - All commands executed as root user
  - Actions done in GOS menu
  - Selfcheck results

3.8 gsm-debug (optional)

- Journal
  - rasdaemon-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=rasdaemon`)
  - smartd-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=smartd`)
- Command output
  - ras-mc-ctl –summary
  - ras-mc-ctl –errors
- Included information
  - RAS/MCE events to identify hardware problems
  - SMART info about HDD health status

3.9 gsm-feed

- Files
  - /opt/greenbone/feed/plugins/plugin_feed_info.inc
  - /opt/greenbone/valuable/system/gsm-feed/gsf-access-key (first line only)
  - /opt/greenbone/valuable/system/gsm-feed/known_hosts
- Journal
  - feed_check-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=feed_check`)
  - greenbone-feed-sync-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=greenbone-feed-sync`)
  - FTP-Airgap-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=FTP-Airgap`)
  - airgap_usb-journal (command: `journalctl --output=json -u airgap_usb`)
- Command output
  - `find /opt/greenbone/feed/plugins/ -iname "*nasl" | wc -l`
- Included information
  - Timestamps of `feed_check`
  - Feed info (name, home, vendor)
  - Plug-in info (set, feed)

  - List of known feed servers and their fingerprints
  - NVT count

3.10 gsm-flash

- Journal
  - greenbone-flash-sync-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=greenbone-flash-sync`)
  - gsm-flash-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=gsm-flash`)
- Included information
  - Flash feed download information
  - Flash image existence
  - Flashing status
  - Error messages if something failed

3.11 gsm-greenbone-security-assistant

- Files
  - /etc/command-wrapper/greenbone-security-assistant.conf
  - /etc/gvm/gsad_log.conf
- Journal
  - greenbone-security-assistant-journal (command: `journalctl --output=json -u greenbone-security-assistant`)
- Service status
  - greenbone-security-assistant-systemctl (command: `systemctl -l status greenbone-security-assistant`)
- Included information
  - Timestamps about start/stop of service
  - Error messages
  - Authentication logs with user name and IP address
  - Status of tasks

3.12 gsm-greenbone-vulnerability-manager

- Files
  - /etc/gvm/gvmd_log.conf
  - /etc/command-wrapper/greenbone-vulnerability-manager.conf
  - /run/gvmd/.psql_history (saved as 'gvmd_psql_history')
  - /var/lib/postgresql/.bash_history (saved as 'postgres_bash_history')
  - /var/lib/postgresql/.psql_history (saved as 'postgres_psql_history')
- Journal
  - gvmd-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=gvmd`)
  - greenbone-scapdata-sync-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=greenbone-scapdata-sync`)
  - greenbone-certdata-sync-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=greenbone-certdata-sync`)
  - postgres-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=postgres`)
- Service status
  - gvmd-systemctl (command: `systemctl -l status gvmd`)
  - postgresql-systemctl (command: `systemctl -l status postgresql`)
- Command output
  - `sudo -Hiu postgres -H -- psql -d tasks -c "`

```
SELECT \*, pg_size_pretty(total_bytes) AS total
   , pg_size_pretty(index_bytes) AS INDEX
   , pg_size_pretty(toast_bytes) AS toast
   , pg_size_pretty(table_bytes) AS TABLE
FROM (
   SELECT \*, total_bytes-index_bytes-COALESCE(toast_bytes,0)
   AS table_bytes
   FROM (
     SELECT c.oid,nspname AS table_schema, relname AS
     TABLE_NAME
     , c.reltuples AS row_estimate
     , pg_total_relation_size(c.oid) AS total_bytes
     , pg_indexes_size(c.oid) AS index_bytes
     , pg_total_relation_size(reltoastrelid) AS toast_bytes
     FROM pg_class c
     LEFT JOIN pg_namespace n ON n.oid = c.relnamespace
     WHERE relkind = 'r'
   ) a
```

```
        ) a
        ORDER BY table_bytes DESC;"
```

  - `sudo -Hiu postgres -H -- psql -d gvmd -c 'select * from pg_stat_all_tables;'`
  - `sudo -Hiu postgres -H -- psql -d gvmd -c "SELECT COUNT(*) FROM nvts;"`
- Included information
  - Manager configuration
  - Database logging (failed queries)
  - Manager logging (migration)
  - Postgres
    - Size of tables
    - Dead tuples
    - Last vacuum
    - NVT count
    - PSQL Command line history

3.13 gsm-grub

- Files
  - /etc/default/grub
  - /proc/cmdline
- Command output
  - `efibootmgr -v`
- Included information
  - Boot entries
  - Kernel boot parameters

3.14 gsm-hardware

- Command output
  - `dmidecode`
- Included information
  - Description of the system's hardware components

3.15 gsm-info

- Files
  - /etc/gsm_type
  - /etc/gsm_name
- Included information
  - Generic GSM product type
  - Individual brand of this machine (if applicable)

3.16 gsm-integrity-check

- Journal
  - integrity-check-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=integrity-check`)
- Commands
  - `integrity-check --debug`
  - `gsmctl info gsm-integrity-check.status`
  - `for check in $(find /usr/share/gsm-integrity-check/checks/ -type f -executable -print); do printf "%s:\n" "$check"; output="$ ("$check")";if [ "$?" != "0" ];then printf "%s\n" "$output";fi;done;`
- Included information
  - Current status report of the GSM's integrity
  - Errors of any failed integrity checks

3.17 gsm-lcd

- Files
  - /etc/LCDd.conf
  - /etc/lcdproc.conf
- Journal
  - LCDd-journal (command: `journalctl --output=json -u LCDd`)
  - lcdproc-journal (command: `journalctl --output=json -u lcdproc`)
  - gsm-lcd-client-journal (command: `journalctl --output=json -u gsm-lcd-client`)
- Service status
  - LCDd-systemctl (command: `systemctl -l status LCDd`)
  - lcdproc-systemctl (command: `systemctl -l status lcdproc`)
  - gsm-lcd-client-systemctl (command: `systemctl -l status gsm-lcd-client`)
- Included information
  - Start/stop of service

3.18 gsm-logging

- Files
  - /var/log/install.log.gz (only the first ten lines)
  - /var/log/gsmlog
- Journal
  - syslog-ng-journal (command: `journalctl --output=json -u syslog-ng`)
  - systemd-journald-journal (command: `journalctl --output=json -u systemd-journald`)
  - auth.log (command: `journalctl --output=json SYSLOG_FACILITY=10`)
- Service status
  - syslog-ng-systemctl (command: `systemctl -l status syslog-ng`)
  - systemd-journald-systemctl (command: `systemctl -l status systemd-journald`)
- Included information
  - Login and logout messages
  - Executed commands
  - Timestamps about start/stop of service
  - `install.log.gz.txt` contains the initial commands executed at the start of the GSM installation to set the variables for HDD environment, EFI and LVM.
  - gsmlog is a fall-back error log and used if /dev/log is inaccessible. It should usually be empty.

3.19 gsm-master

- Files
  - /var/lib/gsm-master/known_hosts
  - /var/lib/gsm-master/ssh_config
  - /var/lib/gvm/sensor_ports.tsv
- Journal
  - gsm-sensors-journal (command: `journalctl --output=json -u gsm-sensors`)
  - gmp-sensor@*-journal (command: `journalctl --output=json -u gmp-sensor@*`)
  - osp-sensor@*-journal (command: `journalctl --output=json -u osp-sensor@*`)
  - ssh-feed-push-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=ssh-feed-push`)
  - check_protocols-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=check_protocols`)
- Service status
  - gsm-sensors-systemctl (command: `systemctl -l status gsm-sensors`)
  - gmp-sensor@*-systemctl (command: `systemctl -l status gmp-sensor@*`)
  - osp-sensor@*-systemctl (command: `systemctl -l status osp-sensor@*`)

- Included information
  - Connection details for the sensors
  - Sync info messages for the sensors
  - `ssh_config` with sensor IP addresses
  - `sensor_ports.tsv` file with sensor ports and IP addresses
  - IP addresses of the failed sensors and the reason determined by the check

3.20 gsm-network

- Files
  - /etc/systemd/network/*
  - /etc/network/interfaces.d/*
  - /etc/network/interfaces
  - /etc/resolv.conf
  - /run/systemd/resolve/resolv.conf
  - /etc/systemd/resolved.conf
  - /etc/sysctl.d/ipv6.conf (configuration about ipv6)
- Journal
  - systemd-networkd-journal (command: `journalctl --output=json -u systemd-networkd`)
  - networking-journal (command: `journalctl --output=json -u networking`)
- Service status
  - systemd-networkd-systemctl (command: `systemctl -l status systemd-networkd`)
  - networking-systemctl (command: `systemctl -l status networking`)
- Included information
  - Interfaces (dhcp|static network settings per interface)
  - Name server configuration
  - DNS

3.21 gsm-network-namespaces

- Files
  - /etc/netns/scan1/network/interfaces
  - /etc/netns/scan1/resolv.conf
  - /etc/netns/scan1/sysctl.d/ipv6.conf

3.22 gsm-openvas

- Files
  - /etc/openvas/openvas.conf
- Journal
  - openvas-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=openvas`)
  - redis-server-journal (command: `journalctl --output=json -u redis-server`)
- Service status
  - redis-server-systemctl (command: `systemctl -l status redis-server`)
- Command output
  - `redis-cli -s /var/run/redis/redis.sock "info"`
  - `echo -e "SELECT 1\nkeys nvt:*" | redis-cli -s /run/redis/redis.sock | grep -o "nvt" | uniq -c`
- Included information
  - NVT count
  - openvas configuration files
  - redis info

3.23 gsm-overcommitment (optional)

- Command output
  - `gsmctl info gsm-info.settings 'defaults'`
  - `gsmctl info gsm-info.settings 'overrides'`
- Included information
  - The machine's default settings and active overrides (if any)

3.24 gsm-sensor

- Files
  - /etc/ssh/sshd.d/00-sensor-port.conf
  - /etc/ssh/sshd.d/sensor.conf
  - /var/lib/gsm-sensor/authorized_keys
- Included information
  - Sensor configuration

3.25 gsm-setup

- Files
  - /opt/greenbone/valuable/system/gsm-setup/stop
- Included information
  - GOS setup wizard status

3.26 gsm-sshd

- Files
  - /etc/ssh/sshd_config
- Journal
  - ssh-journal (command: `journalctl --output=json -u ssh`)
- Service status
  - sshd-systemctl (command: `systemctl -l status sshd`)
- Command output
  - `pam_tally2 --file=/var/log/ssh_tallylog`
  - `gos-state-manager get ssh_login_max_tries`
- Included information
  - SSH server daemon configuration file
  - Login attempts
  - Status about feed sync
  - Count of failed login attempts via SSH

3.27 gsm-support

- Journal
  - kernel-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=kernel`)
- Included information
  - All related information from the kernel
  - Hardware information

3.28 gsm-system

- Journal
  - system-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=system`)
- Command output
  - `date`
  - `uptime`
  - `journalctl --list-boots`
  - `ps --forest -ewwo \`
    `user,pid,pcpu,pmem,vsz,rss,tty,stat,lstart,cputime,args`
  - `top -bn1`
  - `vmstat -s`
  - `vmstat -D`
  - `vmstat -d`
  - `df -h`
  - `du -h --max-depth=1 / 2>/dev/null`
  - `du -h --max-depth=2 /root 2>/dev/null`
  - `du -h --max-depth=2 /opt/greenbone 2>/dev/null`
  - `du -h --max-depth=2 /var/log`
  - `du -h --max-depth=3 /tmp`
  - `ls -lah /tmp/`
  - `ls -lah /var/log/gvm/`
  - `du -h --max-depth=1 /var/lib/postgresql/11/main/base/`
- Included information
  - General system information about boots, logins, processes and disk usage

3.29 gsm-timesync

- Files
  - /etc/systemd/timesyncd.conf
- Journal
  - systemd-timesyncd-journal (command: `journalctl --output=json -u systemd-timesyncd`)
- Service status
  - systemd-timesyncd-systemctl (command: `systemctl -l status systemd-timesyncd`)

3.30 gsm-upgrade

- Files
  - /etc/apt/sources.list
  - /etc/apt/sources.list.d/*
  - /var/log/apt/*
  - /var/log/installed_gos_versions.log
- Journal
  - greenbone-apt-sync-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=greenbone-apt-sync`)
  - gsm-upgrade-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=gsm-upgrade`)
- Command output
  - `gsmctl info gsm-info.full_version`
  - `gsmctl info gsm-upgrade.patch`
  - `gsmctl info gsm-upgrade.next`
  - `gsmctl info gsm-upgrade.synced_version`
  - `gsmctl info gsm-upgrade.switchrelease_last_status`
  - `gsmctl info gsm-upgrade.last_status`
  - `gsmctl info gsm-upgrade.last_status_msg`
  - `gsmctl info gsm-upgrade.reboot_pending`
  - `gsmctl info gsm-system.status`
  - `gsmctl info gsm-feed.age`
  - `dpkg -l`
- Included information
  - The current GOS version and system status
  - List of all installed packages and their versions
  - History about the installed packages
  - Package installation results
  - Package source configuration file
  - History of installed GOS versions

3.31 gvmcg

- Included information
  - System performance graphs as shown in the web interface under *Extras > Performance* for intervals 2 h, 1 d and 7 d

3.32 ospd-openvas

- Journal
  - ospd-openvas-journal (command: `journalctl --output=json -u ospd-openvas`)
- Service status
  - ospd-openvas-systemctl (command: `systemctl -l status ospd-openvas`)
- Included information
  - Journal and status of the OpenVAS scanner wrapper

3.33 selfcheck

- Journal
  - selfcheck-journal (command: `journalctl --output=json SYSLOG_IDENTIFIER=selfcheck`)
- Command output
  - `selfcheck`
- Included information
  - GSM selfcheck results and journal