Greenbone Support Package for GOS 4.2

Technical Documentation

Tech Paper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2019-08-09

Table of Contents

1. About this Document

This technical documentation describes the contents of the Greenbone Support Package as created by Greenbone OS version 4.2.

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-4/en/systemadministration.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.

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 that are 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-logging/auth.log (Login attempts)
gsm-network/interfaces.d/*
gsm-network/resolv.conf
gsm-master/ssh_config (Sensor IP addresses)
gsm-masster/sensor_ports.tsv (sensor ports with IP addresses)
gsm-sshd/ssh-journal (Login attempts)
gsm-timesyncd (IP addresses about timeserver)

Commands executed as admin user:

gsm-cli-admin/.bash_history

Commands executed as root user:

gsm-cli-admin/sudo-journal

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.

3.1. gos-ansible

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

3.2. gos-state-manager

- Journal
  - /state_migration (command: **`journalctl --output=json SYSLOG_IDENTIFIER=state_migration`**)
- Command output
  - **`gos-state-manager dump beautify`**
- Included informationen
  - Logs about migration (Result message)
  - Selected GOS state values, i.e. contents of /opt/greenbone/valuable/system/gos-state/state on the GSM 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 (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=gsm-backup`**)
  - gsm-restore (Command: **`journalctl –output=json SYSLOG_IDENTIFIER=gsm-restore`**)
  - usb-backup (Command: **`journalctl –output=json SYSLOG_IDENTIFIER=usb-backup`**)
  - usb-restore (Command: **`journalctl –output=json SYSLOG_IDENTIFIER=usb-restore`**)
  - obnam (Command: **`journalctl –output=json SYSLOG_IDENTIFIER=obnam`**)
- Included information
  - Timestamps of started and finished backup services
  - List of files to backup

3.7. gsm-cli-admin

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

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

3.9. gsm-flash

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

3.10. gsm-greenbone-security-assistant

- Files
  - /etc/command-wrapper/greenbone-security-assistant.conf
  - /etc/openvas/gsad_log.conf
- Journal
  - greenbone-security-assistant (Command: **`journalctl --output=json -u greenbone-security-assistant`**)
- Service status
  - gsa (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

3.11. gsm-grub

- Files
  - /etc/default/grub
  - /proc/cmdline
- Included information
  - Boot entries
  - Kernel boot parameter

3.12. gsm-lcd (LC Display Daemon)

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

3.13. gsm-logging

- Files
  - /var/log/install.log.gz (only the first ten lines)
- Journal
  - syslog-ng (Command: **`journalctl --output=json -u syslog-ng`**)
  - systemd-journald (Command: **`journalctl --output=json -u systemd-journald`**)
  - auth.log (Command: **`journalctl --output=json SYSLOG_FACILITY=10`**)
- Service status
  - syslog-ng (Command: **`systemctl -l status syslog-ng`**)
  - systemd-journald (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.

3.14. gsm-master

- Files
  - /var/lib/gsm-master/known_hosts
  - /var/lib/gsm-master/ssh_config
  - /var/lib/openvas/sensor_ports.tsv
- Journal
  - gmp-slave[s|@*] (Command: **`journalctl --output=json -u gmp-slaves`**)
  - ssh-feed-push-journal (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=ssh-feed-push`**)
- Service status
  - gmp-slave[s|@*]
- Included information
  - Connection details to the slaves
  - Sync info messages to the slaves
  - `ssh_config` with sensor IP addresses
  - `sensor_ports.tsv` file with sensor ports and IP addresses

3.15. 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 (Command: **`journalctl --output=json -u systemd-networkd`**)
  - networking (Command: **`journalctl --output=json -u networking`**)
  - expertnet (Command: **`journalctl --output=json -u expertnet`**)
- Service status
  - systemd-networkd (Command: **`systemctl -l status systemd-networkd`**)
  - networking (Command: **`systemctl -l status networking`**)
  - expertnet (Command: **`systemctl -l status expertnet`**)
- Included information
  - Interfaces (dhcp|static network settings per interface)
  - Name server configuration
  - DNS

3.16. gsm-openvas-manager

- Files
  - /etc/openvas/openvasmd_log.conf
  - /etc/command-wrapper/openvas-manager.conf
- Journal
  - openvasmd (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=openvasmd`**)
  - greenbone-scapdata-sync (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=greenbone-scapdata-sync`**)
  - greenbone-certdata-sync (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=greenbone-certdata-sync`**)
  - postgres (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=postgres`**)
- Service status
  - openvas manager daemon (Command: **`systemctl -l status openvasmd`**)
  - postgresql (Command: **`systemctl -l status postgresql`**)
- Included information
  - Manager configuration
  - Database logging (failed queries)
  - Manager logging (migration)

3.17. gsm-openvas-scanner

- Files
  - openvassd.messages, openvassd.messages.1
  - openvassd.dump, openvassd.dump.1
  - /etc/command-wrapper/openvas-scanner.conf
  - /etc/openvas/openvassd.conf
- Journal
  - openvas-scanner (Command: **`journalctl --output=json -u openvas-scanner`**)
  - greenbone-nvt-sync (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=greenbone-nvt-sync`**)
  - redis-server (Command: **`journalctl --output=json -u redis-server`**)
- Service status
  - openvas-scanner (Command: **`systemctl -l status openvas-scanner`**)
  - redis-server (Command: **`systemctl -l status redis-server`**)
- Included information
  - NVT sync log
  - openvassd configuration files
  - openvassd status

3.18. gsm-sensor

- Files
  - fd/etc/ssh/sshd.d/00-sensor-port.conf
  - /etc/ssh/sshd.d/sensor.conf
  - /var/lib/gsm-sensor/authorized_keys

3.19. gsm-setup

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

3.20. gsm-sshd

- Files
  - /etc/ssh/sshd_config
- Journal
  - ssh (Command: **`journalctl --output=json -u ssh`**)
- Service status
  - sshd (Command: **`systemctl -l status sshd`**)
- Included information
  - SSH server daemon configuration file
  - Login attempts
  - Status about feed sync

3.21. gsm-support

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

3.22. gsm-system

- Journal
  - system (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 -n 1 # just for header summary`**
  - **`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/openvas/`**

  For PostgreSQL GSMs as root:
  - **`du -h --max-depth=1 /var/lib/postgresql/9.4/main/base/`**

  For SQLite GSMs:
  - **`ls -lah /var/lib/openvas/mgr`**
- Included information
  - General system information about boots, logins, processes and disk usage

3.23. gsm-timesync

- Files
  - /etc/systemd/timesyncd.conf
- Journal
  - systemd-timesyncd
- Service status
  - systemd-timesyncd

3.24. gsm-upgrade

- Files
  - /etc/apt/sources.list
  - /var/log/apt/*
  - /etc/apt/sources.list.d/*
- Journal
  - greenbone-apt-sync (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=greenbone-apt-sync`**)
  - gsm-upgrade (Command**`: journalctl --output=json SYSLOG_IDENTIFIER=gsm-upgrade`**)
- Command output
  - **`gsmctl info gsm-info.version`**
  - **`gsmctl info gsm-info.patch`**
  - **`gsmctl info gsm-upgrade.next`**
  - **`gsmctl info gsm-upgrade.synced_version`**
  - **`gsmctl info gsm-upgrade.reboot_pending`**
  - **`gsmctl info gsm-upgrade.failed`**
  - **`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

3.25. gsm-userdata-import

- Journal
  - userdata-import (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=userdata-import`**)
- Included information
  - Migration import results
  - Backup import results

3.26. gvmcg

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