Greenbone Support Package

Technical Documentation

Status:
January 31, 2019
GOS 4.3

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück
https://www.greenbone.net

About this document

This technical documentation describes the contents of the Greenbone Support Package as created by Greenbone OS version 4.3.

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: http://docs.greenbone.net/GSM-Manual/gos-4/en/systemadministration.html#advanced

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.

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 may occur in the following files:

gsm-backup/ssh_known_host
gsm-feed (Ips 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 IPs)
gsm-masster/sensor_ports.tsv (sensor ports with IPs)
gsm-sshd/ssh-journal (Login attempts)
gsm-timesyncd (IPs about timeserver)

Commands executed as admin user:

gsm-cli-admin/.bash_history

Commands executed as root user:

gsm-cli-admin/sudo-journal

Content of 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 directly copied files into the support package are also listed here.

gos-ansible

- Files
  - /var/log/gos-ansible.log

- Included information
  - Status of configuration files and processes

gos-state-manager

- Journal
  - state_migration (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=state_migration`**)

- Included information
  - Logs about migration (Result message)

greenbone-sourcefire-connector

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

greenbone-verinice-connector

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

greenbone-vfire-connector

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

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 service
  - list of files to backup

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

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 (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)
  - plugin info (set, feed)
  - list of known feed servers and their fingerprints

gsm-flash

- Journal
  - 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

gsm-greenbone-security-assistant

- Files
  - /etc/command-wrapper/greenbone-security-assistant.conf
  - /etc/openvas/gsad_log.conf

- Service status
  - gsa (Command: **`systemctl -l status greenbone-security-assistant`**)

- Journal
  - greenbone-security-assistant (Command: **`journalctl --output=json -u greenbone-security-assistant`**)

- Included information
  - timestamps about start stop of service
  - error messages
  - authentication logs with username and ip
  - status of tasks

gsm-grub

- Files
  - /etc/default/grub
  - /proc/cmdline

- Included information
  - boot entries
  - kernel boot parameter

gsm-info

- Files
  - /etc/gsm_type
  - /etc/gsm_name

- Included information
  - generic GSM product type
  - individual brand of this machine (if applicable)

gsm-lcd (LCD display daemon)

- Files
  - /etc/LCDd.conf
  - /etc/lcdproc.conf

- 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`**)

- 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`**)

- Included information
  - start stop of service

gsm-logging

- Files
  - /var/log/install.log.gz

- 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 is saved as “tmp*.txt”. These are the first ten commands executed during the installation of the GSM. It only set variables for hdd environment, efi and LVM.

gsm-master

- Files
  - /var/lib/gsm-master/known_hosts
  - /var/lib/gsm-master/ssh_config
  - /var/lib/openvas/sensor_ports.tsv

- Service status
  - gmp-slave[s|@*]

- Journal
  - gmp-slave[s|@*] (Command: **`journalctl --output=json -u gmp-slaves`**)
  - ssh-feed-push-journal (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=ssh-feed-push`**)

- Included information
  - connection details to the slaves
  - sync info messages to the slaves
  - ssh_config with sensor ips
  - sensor_ports.tsv file with sensor ports and ips

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)

- Service status
  - systemd-networkd (Command: **`systemctl -l status systemd-networkd`**)
  - networking (Command: **`systemctl -l status networking`**)
  - expertnet (Command: **`systemctl -l status expertnet`**)

- Journal
  - systemd-networkd (Command: **`journalctl --output=json -u systemd-networkd`**)
  - networking (Command: **`journalctl --output=json -u networking`**)
  - expertnet (Command: **`journalctl --output=json -u expertnet`**)

- Included information
  - interfaces (dhcp|static network settings per interface)
  - name server configuration
  - dns

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 informationen
  - manager configuration
  - database logging (failed queries)
  - manager logging (migration)

gsm-openvas-scanner

- Files
  - openvassd.messages
  - openvassd.dump
  - /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

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)

gsm-sensor

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

gsm-setup

- Files
  - /opt/greenbone/valuable/system/gsm-setup/stop

- Included information
  - GOS setup wizard status

gsm-sshd

- Files
  - /etc/ssh/sshd_config

- Journal
  - ssh (Command: **`journalctl --output=json -u ssh`**)

- Service status
  - sshd (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

gsm-support

- Journal
  - kernel (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=kernel`**)

- Included information
  - all related information from the kernel
  - hardware information

gsm-system

- Journal
  - system (Command**: `journalctl --output=json SYSLOG_IDENTIFIER=system`**)
- Command output
  - **`date`**
  - **`uptime`**
  - **`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`**

gsm-timesync

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

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`**)

- Included information
  - history about the installed packages
  - package installation results
  - package source configuration file

gsm-userdata-import

- Journal
  - userdata-import (Command: **`journalctl --output=json SYSLOG_IDENTIFIER=userdata-import`**)

- Included information
  - migration import results
  - backup import results

gvmcg

- Included information
  - system performance graphs as shown in Web-UI under *Extras→Performance* for intervals 2h, 1d and 7d