bash

/var/log/websrv-02/rsyslog\_sshd.log {

daily

rotate 30

compress

lastaction

DATE=$(date +"%Y-%m-%d")

echo "$(date)" >> "/var/log/websrv-02/hashes\_"$DATE"\_rsyslog\_sshd.txt"

for i in $(seq 1 30); do

FILE="/var/log/websrv-02/rsyslog\_sshd.log.$i.gz"

if [ -f "$FILE" ]; then

HASH=$(/usr/bin/sha256sum "$FILE" | awk '{ print $1 }')

echo "rsyslog\_sshd.log.$i.gz "$HASH"" >> "/var/log/websrv-02/hashes\_"$DATE"\_rsyslog\_sshd.txt"

fi

done

systemctl restart rsyslog

endscript

}

**Explanation**

1. **Path Specification:**

bash

/var/log/websrv-02/rsyslog\_sshd.log {

This indicates that the configuration block applies to the log file /var/log/websrv-02/rsyslog\_sshd.log.

1. **Logrotate Options:**

daily

rotate 30

compress

* + daily: Rotate the log file every day.
  + rotate 30: Keep the last 30 rotated log files. Older files will be deleted.
  + compress: Compress the rotated log files to save space.

1. **lastaction Section:** This section specifies actions to be taken after the log file has been rotated and compressed. The lastaction block is executed after log rotation is complete.

lastaction

* + DATE=$(date +"%Y-%m-%d"): This assigns the current date in YYYY-MM-DD format to the DATE variable.
  + echo "$(date)" >> "/var/log/websrv-02/hashes\_"$DATE"\_rsyslog\_sshd.txt": This appends the current date and time to a file named hashes\_YYYY-MM-DD\_rsyslog\_sshd.txt in the /var/log/websrv-02/ directory.

bash

for i in $(seq 1 30); do

FILE="/var/log/websrv-02/rsyslog\_sshd.log.$i.gz"

if [ -f "$FILE" ]; then

HASH=$(/usr/bin/sha256sum "$FILE" | awk '{ print $1 }')

echo "rsyslog\_sshd.log.$i.gz "$HASH"" >> "/var/log/websrv-02/hashes\_"$DATE"\_rsyslog\_sshd.txt"

fi

done

* + This loop iterates from 1 to 30, checking for the existence of each log file in the sequence rsyslog\_sshd.log.1.gz to rsyslog\_sshd.log.30.gz.
  + For each existing file, it computes the SHA-256 hash using sha256sum and appends the file name and its hash to the hashes\_YYYY-MM-DD\_rsyslog\_sshd.txt file.

systemctl restart rsyslog

* + This command restarts the rsyslog service after log rotation and hash computation. This may be necessary to ensure the rsyslog service starts logging to the new log file properly.

1. **End of Block:**

endscript

}

* + endscript: Marks the end of the lastaction block.
  + The closing brace } marks the end of the logrotate configuration block.