Server Monitoring Redhat / CentOS

Server Monitoring from inside - Commandline

Systemweites Logging aller User Commands

Gewünscht wird das loggen von sämtlichen Kommandos, aller Usern System-weit. Um dies zu realisieren müssen dazu zwei Files angepasst und der `rsyslog` Dienst neugestartet werden.

- **Schritt 1** - Editieren der global geltenden System Bahrc:

```
# vim /etc/bashrc
```

```
# /etc/bashrc

# System wide functions and aliases
# Environment stuff goes in /etc/profile

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.

# are we an interactive shell?
if [ "$PS1" ]; then
  if [ -z "$PROMPT_COMMAND" ]; then
    case $TERM in
    xterm*|vte*)
      if [ -e /etc/sysconfig/bash-prompt-xterm ]; then
          PROMPT_COMMAND=/etc/sysconfig/bash-prompt-xterm
      elif [ "${VTE_VERSION:-0}" -ge 3405 ]; then
          PROMPT_COMMAND="__vte_prompt_command"
      else
          PROMPT_COMMAND='printf "\033]0;%s@%s:%s\007" "${USER}"
"${HOSTNAME%%.*}" "${PWD/#$HOME/~}"'
      fi
      ;;
    screen*)
      if [ -e /etc/sysconfig/bash-prompt-screen ]; then
          PROMPT_COMMAND=/etc/sysconfig/bash-prompt-screen
      else
          PROMPT_COMMAND='printf "\033k%s@%s:%s\033\\" "${USER}"
"${HOSTNAME%%.*}" "${PWD/#$HOME/~}"'
      fi
      ;;
    *)
```

```
      [ -e /etc/sysconfig/bash-prompt-default ] &&
PROMPT_COMMAND=/etc/sysconfig/bash-prompt-default
      ;;
    esac
  fi
  # Turn on parallel history
  shopt -s histappend
  history -a
  # Turn on checkwinsize
  shopt -s checkwinsize
  [ "$PS1" = "\\s-\\v\\$ " ] && PS1="[\u@\h \W]\\$ "
  # You might want to have e.g. tty in prompt (e.g. more virtual machines)
  # and console windows
  # If you want to do so, just add e.g.
  # if [ "$PS1" ]; then
  #   PS1="[\u@\h:\l \W]\\$ "
  # fi
  # to your custom modification shell script in /etc/profile.d/ directory
fi

if ! shopt -q login_shell ; then # We're not a login shell
    # Need to redefine pathmunge, it get's undefined at the end of
/etc/profile
    pathmunge () {
        case ":${PATH}:" in
            *:"$1":*)
                ;;
            *)
                if [ "$2" = "after" ] ; then
                    PATH=$PATH:$1
                else
                    PATH=$1:$PATH
                fi
        esac
    }

    # By default, we want umask to get set. This sets it for non-login
shell.
    # Current threshold for system reserved uid/gids is 200
    # You could check uidgid reservation validity in
    # /usr/share/doc/setup-*/uidgid file
    if [ $UID -gt 199 ] && [ "`/usr/bin/id -gn`" = "`/usr/bin/id -un`" ];
then
       umask 002
    else
       umask 022
    fi

    SHELL=/bin/bash
    # Only display echos from profile.d scripts if we are no login shell
```

```
    # and interactive - otherwise just process them to set envvars
    for i in /etc/profile.d/*.sh; do
        if [ -r "$i" ]; then
            if [ "$PS1" ]; then
                . "$i"
            else
                . "$i" >/dev/null
            fi
        fi
    done

    unset i
    unset -f pathmunge
fi

# Need to be added for logging! By Michael.R
PROMPT_COMMAND='history -a >(tee -a ~/.bash_history | logger -p local6.info
-t "$USER[$$] $SSH_CONNECTION")'
# vim:ts=4:sw=4
```

- **Schritt 2** - Editieren der rsyslog Konfiguration und hinzufügen eines neuen Log-Pfades:

```
# vim /etc/rsyslog.conf
```

```
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see
http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source instead of
imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via
logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
```

```
#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is usually
not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state


#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog

# Added By Michael
local6.info                                             /var/log/history.log

# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
```

```
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log


# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule ###
```

- **Schritt 3** - Initiales erstellen des Log-Files und setzen der File Berechtigung:

```
# touch /var/log/history.log
# chmod 600 /var/log/history.log
```

- **Schritt 4** - Restarten des rsyslog services:

```
# systemctl restart rsyslog.service
# systemctl status rsyslog.service
```

Logging Stacks - Infrastructure Logging

- https://angristan.xyz/monitoring-telegraf-influxdb-grafana/
- https://www.blog.labouardy.com/monitor-your-infrastructure-with-tig-stack/
- https://gist.github.com/mlabouardy/c4d8effdb31ba75ac63326a8d911a379

Server Monitoring from outside - Webpages

- Matomo

Weiteres

Zabbix:
http://www.geekpills.com/operating-system/linux/zabbix-installation-of-zabbix-server-on-centos

TICK Stack:
https://www.digitalocean.com/community/tutorials/how-to-monitor-system-metrics-with-the-tick-stack-on-centos-7

Interessante Monitoring Projekte

- https://github.com/Jahaja/psdash
- https://www.librenms.org
- https://mmonit.com/monit/
- https://github.com/k3oni/pydash

- https://github.com/nicolargo/glances →> Infos:
  https://home-assistant.io/blog/2015/09/18/monitoring-with-glances-and-home-assistant/

```
 cd /tmp
wget
https://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-2.noarch.rpm
sudo yum install epel-release-7-2.noarch.rpm
sudo yum install python-pip python-devel
sudo pip-python install glances

vim /etc/systemd/system/glances.service
```

```
[Unit]
Description=Glances
After=network.target

[Service]
ExecStart=/usr/local/bin/glances -w
Restart=on-abort

[Install]
WantedBy=multi-user.target
```

- https://github.com/kizniche/Mycodo
- **Tool wie Patchnix:** https://github.com/furlongm/patchman
- https://github.com/mlazarov/supervisord-monitor

Last update: **2020/03/05 16:10**