Diagnostika systému

Zobrazte datum instalace systému:

```
# rpm -qi basesystem | grep "^Install Date"
```

Zobrazte čas posledního spuštění systému:

```
# who -b
```

nebo

```
# uptime
```

Zobrazte informace o použitém hardwaru a BIOSu:

```
# dmidecode
```

Zobrazte stav všech systemd objektů (jednotek):

```
# systemctl
```

(platí od RHEL 7)

Zobrazte informace o stavu daného zařízení (podporujícího SMART technologii):

```
# smartctl -a /dev/sda
```

Zobrazte dynamické informace o procesech, které nejvíce zatěžují disky:

```
# iotop -o
```

Zobrazte 5 výpisů se statistikami o zatížení disků včetně jejich oddílů a/nebo logických svazků ve 2sekundových intervalech:

```
# iostat -dpxh 2 5
```

nebo

```
# sar -dh 2 5
```

Zobrazte statistiky o zatížení disků včetně jejich logických svazků během daného dne:

```
# sar -dh -f /var/log/sa/sa<n>
```

Zobrazte statické informace o 10 procesech, které nejvíce využívají procesor:

```
# ps -eo %cpu,pid,user,args --sort=-%cpu | head -11
```

Zobrazte dynamické informace o procesech, které nejvíce využívají procesor (případně paměť či swap):

```
# top
```

Zobrazte 5 výpisů se statistikami o využití procesoru ve 2sekundových intervalech:

```
# mpstat -P ALL 2 5
```

nebo

```
# sar -P ALL 2 5
```

Zobrazte statistiky o využití procesoru během daného dne:

```
# sar -P ALL -f /var/log/sa/sa<n>
```

Zobrazte statické informace o celkovém množství volné a použité fyzické paměti a swapu v MB:

```
# free -m
```

Zobrazte statické informace o 10 procesech, které nejvíce využívají paměť:

```
# ps -eo %mem,pid,user,args --sort=-%mem | head -11
```

Zobrazte 5 výpisů se statistikami o využití paměti ve 2sekundových intervalech:

```
# sar -hr ALL 2 5
```

Zobrazte statistiky o využití paměti během daného dne:

```
# sar -hr ALL -f /var/log/sa/sa<n>
```

Zobrazte statické informace o 10 procesech, které nejvíce využívají swap včetně procentuálních hodnot:

```
# find /proc -maxdepth 2 -path "/proc/[0-9]*/status" -readable -exec awk -v
FS=":" -v TOTSWP="$(sed 1d /proc/swaps | awk 'BEGIN{sum=0} {sum=sum+$(NF-2)}
END{print sum}')" '{process[$1]=$2;sub(/^[ \t]+/,"",process[$1]);} END
{if(process["VmSwap"] && process["VmSwap"] != "0 kB")
{used_swap=process["VmSwap"]; sub(/[ a-zA-Z]+/,"",used_swap);
percent=(used_swap/TOTSWP*100); printf "%10s %-30s %20s
%6.2f%\n",process["Pid"],process["Name"],process["VmSwap"],percent}}' '{}'
\; | awk '{print $(NF-2),$0}' | sort -hr | head | cut -d " " -f2-
```

Zobrazte 5 výpisů se statistikami o využití swapu ve 2sekundových intervalech:

```
# sar -Sh 2 5
```

Zobrazte statistiky o využití swapu během daného dne:

```
# sar -Sh -f /var/log/sa/sa<n>
```

Zobrazte statické informace o provozu na síťových rozhraních:

```
# ifstat
```

Zobrazte 5 výpisů se statistikami o provozu na síťových rozhraních ve 2sekundových intervalech:

```
# sar -n DEV -h 2 5
```

Zobrazte statistiky o provozu na síťových rozhraních během daného dne:

```
# sar -n DEV -h -f /var/log/sa/sa<n>
```

Zobrazte 5 výpisů se statistikami o využití paměti, swapu, disků a procesoru ve 2sekundových intervalech:

```
# vmstat -w 2 5
```

Zobrazte dynamické informace o procesoru, paměti, swapu, síti, discích, jádru, souborových systémech, NFS a hlavních procesech:

```
# nmon
```

Zobrazte souborové systémy s využitou kapacitou 90 % a více:

```
# fs=$(df -P | awk '+$5 >= 90 {print}'); [[ -z "$fs" ]] && echo "NONE" ||
echo "$fs"
```

Zobrazte sestupně 50 souborů větších než 100 MB v adresáři /var:

```
# find /var -type f -size +100M -exec du -h '{}' \+ | sort -rh | head -50
```

Zobrazte všechny soubory, které byly změněny za poslední den v adresáři /tmp:

```
# find /tmp -mtime -1
```

Zobrazte soubory s právy zápisu pro ostatní:

```
# files="/etc /opt /tmp /usr /var"; for file in $files; do find $file \( -
type f -o -type d \) -perm -o=w -exec ls -adl {} \; 2> /dev/null; done |
egrep -v '^[l]|^[d].{8}t' || echo "NONE"
```

Ověřte informace o souborech všech nainstalovaných balíčků s informacemi v rpm databázi:

```
# rpm -Va
```

Zobrazte časové údaje o přihlášení všech uživatelů do systému za poslední období:

```
# last
```

Zobrazte povolené potenciálně zranitelné služby:

```
# if [[ -n $(which systemctl 2> /dev/null) ]]; then { vs1=$(systemctl list-
unit-files -t service | egrep -w "avahi-daemon|bind|cups|dhcpd|dhcp-
server|dnsmasq|dovecot|finger|http|ldap|named|^nfs[ ]|nfs-
server|nmb|postfix|rexec|rlogin|rpcbind|rsh|rstatd|rsync|rusersd|sendmail|sl
apd|smb|snmp|squid|telnet|tftp|vsftpd|who|xinetd" | grep "enabled" | awk
'{print $1}'); [[ -n "$vs1" ]] && echo "$vs1";}; else if [[ -n $(which
chkconfig 2> /dev/null) ]]; then { vs2=$(chkconfig --list | egrep -i "avahi-
daemon|bind|cups|dhcpd|dhcp-
server|dnsmasq|dovecot|finger|http|ldap|named|^nfs[ ]|nfs-
server|nmb|postfix|rexec|rlogin|rpcbind|rsh|rstatd|rsync|rusersd|sendmail|sl
apd|smb|snmp|squid|telnet|tftp|ttdbserver|vsftpd|who|xinetd" | grep "on" |
awk '{print $1}'); [[ -n "$vs2" ]] && echo "$vs2";}; fi; fi
if [[ -f /etc/xinetd.conf ]]; then { vs3=$(grep -R "disable" /etc/xinetd.d |
grep "no"); [[ -n "$vs3" ]] && echo "$vs3";}; else if [[ -f /etc/inetd.conf
]]; then { vs4=$(sed '/^[^#]/!d' /etc/inetd.conf | egrep
'bootps|chargen|cmsd|daytime|discard|dtspcd|echo|finger|ftp|imap|netstat|nnt
p|pcnfsd|pop-3|rexd|rexec|rlogin|rsh|rstatd|rsync|rusersd|rwalld|rwho|sprayd
|systat|talk|telnet|tftp|time|ttdbserver|who'); [[ -n "$vs4" ]] && echo
"$vs4";}; fi; fi
```

Zobrazte potenciálně zranitelné otevřené standardní porty:

```
# ports="avahi chargen daytime discard dns echo finger ldap ldaps netstat
nntp nntps snmp systat time"; avahi="5353"; chargen="19"; daytime="13";
discard="9"; dns="53"; echo="7"; finger="79"; ldap="389"; ldaps="636";
netstat="15"; nntp="119"; nntps="563"; snmp="161"; systat="11"; time="37";
for port in $ports; do open_ports=$(netstat -antu | awk 'NR>2{print $4}' |
awk -F ":" '{print $NF}' | egrep -w "${!port}$" | uniq); if [[ -n
"$open_ports" ]]; then echo "${port} --> YES"; else echo "${port} --> NO";
fi; done
ports="cups dtspcd ftp http https imap imaps pop3 pop3s rexec rlogin rsh
rsync smb smtp smtps squid telnet"; cups="631"; dtspcd="6112"; ftp="21";
http="80"; https="443"; imap="143"; imaps="993"; pop3="110"; pop3s="995";
rexec="512"; rlogin="513"; rsh="514"; rsync="873"; smb="445"; smtp="25";
smtps="465"; squid="3128"; telnet="23"; for port in $ports; do
open_ports=$(netstat -ant | awk 'NR>2{print $4}' | awk -F ":" '{print $NF}'
| egrep -w "${!port}$" | uniq); if [[ -n "$open_ports" ]]; then echo
"${port} --> YES"; else echo "${port} --> NO"; fi; done
ports="bootps nmb rwho talk tftp who"; bootps="67"; nmb="137"; rwho="513";
talk="517"; tftp="69"; who="513"; for port in $ports; do
open_ports=$(netstat -anu | awk 'NR>2{print $4}' | awk -F ":" '{print $NF}'
| egrep -w "${!port}$" | uniq); if [[ -n "$open_ports" ]]; then echo
"${port} --> YES"; else echo "${port} --> NO"; fi; done
ports="cmsd nfs pcnfsd rstatd rusersd rwalld sprayd ttdbserver"; for port in
$ports; do open_ports=$(rpcinfo -p 2> /dev/null | grep -i $port); if [[ -n
"$open_ports" ]]; then echo "${port} --> YES"; else echo "${port} --> NO";
fi; done
```

Zobrazte stav SELinuxu:

```
# getenforce
```