```
.* CONNECT TCP Peer: "10.0.2.8:[0-9]+" Local: "_IP_:[0-9]+"
.* CONNECT TCP Peer: "206.71.189.157:[0-9]+" Local: "_IP_:[0-9]+"
_DATEHOST_ anacron_PID_: Anacron started on_YYYY-MM-DD_
_DATEHOST_ anacron_PID_: Normal exit _DIGITS_ jobs run\)
_DATEHOST_ anacron_PID_: Updated timestamp for job ‘cron\.daily’ to_YYYY-MM-DD_
_DATEHOST_ anacron_PID_: Updated timestamp for job ‘cron\.monthly’ to_YYYY-MM-DD
_
_DATEHOST_ anacron_PID_: Updated timestamp for job ‘cron\.weekly’ to_YYYY-MM-DD_
_DATEHOST_ auditd_PID_: Audit daemon rotating log files
_DATEHOST_ crond_PID_: \(CRON\) chdir\(HOME\) failed: \(No such file or director
y\)
_DATEHOST_ crond_PID_: pam_unix\(crond:session\): session closed for user
_DATEHOST_ crond_PID_: pam_unix\(crond:session\): session opened for user .* by
\(uid_DIGITS_\)
_DATEHOST_ crond_PID_: \(root\) CMD \(   /etc/init\.d/iptables restart >> /dev/n
ull\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/etc/init\.d/iptables restart > /dev/null\
)
_DATEHOST_ crond_PID_: \(root\) CMD \(/etc/init\.d/puppet restart > /dev/null_DI
GITS_>&1\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(/etc/init\.d/puppet restart > /dev/null_DI
GITS_>&1\)
_DATEHOST_ crond_PID_: \(root\) CMD \(find /var/spool/mail/ -type f -size \+1c\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(find /var/spool/mail/ -type f -size \+1c\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/home/nagios/bin/passive-checks\.sh\)
_DATEHOST_ crond_PID_: \(root\) CMD \(run-parts /etc/cron\.daily\)
_DATEHOST_ crond_PID_: \(root\) CMD \(run-parts /etc/cron\.hourly\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(run-parts /etc/cron.hourly\)
_DATEHOST_ crond_PID_: \(root\) CMD \(run-parts /etc/cron\.monthly\)
_DATEHOST_ crond_PID_: \(root\) CMD \(run-parts /etc/cron\.weekly\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/usr/lib64/sa/sa1_DIGITS__DIGITS_\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(/usr/lib64/sa/sa1 -S DISK 1 1\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/usr/lib64/sa/sa2 -A\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(/usr/lib64/sa/sa2 -A\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/usr/local/bin/find-hg\.sh\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(/usr/local/bin/find-hg\.sh\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/usr/local/bin/scrub-raid\.sh\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(/usr/local/bin/scrub-raid\.sh\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/usr/local/lollerskates/lollerskates\.py\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(/usr/local/lollerskates/lollerskates\.py\)
_DATEHOST_ crond_PID_: \(root\) CMD \(/usr/local/nagios/bin/passive-checks\.sh\)
_DATEHOST_ CROND_PID_: \(root\) CMD \(/usr/local/nagios/bin/passive-checks.sh\)
_DATEHOST_ crontab_PID_: \(root\) LIST \(munin\)
_DATEHOST_ crontab_PID_: \(root\) LIST \(root\)
_DATEHOST_ crontab_PID_: \(root\) LIST \(treed\)
_DATEHOST_ kernel: IN=eth0 OUT= MAC=.* SRC=_IP_ DST=_IP_ LEN_DIGITS_ TOS_DIGITS_
x00 PREC_DIGITS_x00 TTL_DIGITS_ ID_DIGITS_ DF PROTO=TCP SPT_DIGITS_ DPT=22 WINDO
W_DIGITS_ RES_DIGITS_x00 SYN URGP_DIGITS_
_DATEHOST_ kernel: IN=.* OUT= MAC=.* SRC=_IP_ DST=_IP_ LEN_DIGITS_ TOS_DIGITS_x0
0 PREC_DIGITS_x00 TTL_DIGITS_ ID_DIGITS_ PROTO=TCP SPT_DIGITS_ DPT_DIGITS_ WINDO
W_DIGITS_ RES_DIGITS_x00 SYN URGP_DIGITS_
_DATEHOST_ kernel: ip_conntrack version_DIGITS_\.4 _DIGITS_ buckets,_DIGITS_ max
\) -_DIGITS_ bytes per conntrack
_DATEHOST_ kernel: ip_tables: \(C\)_DIGITS_-2006 Netfilter Core Team
_DATEHOST_ kernel: Netfilter messages via NETLINK v0\.30\.
_DATEHOST_ kernel: Removing netfilter NETLINK layer\.
_DATEHOST_ last message repeated_DIGITS_ times
_DATEHOST_ ntpd_PID_: synchronized to _IP_, stratum_DIGITS_
_DATEHOST_ ntpd_PID_: synchronized to LOCAL_DIGITS_\), stratum_DIGITS_
_DATEHOST_ ntpd_PID_: time reset .* s
_DATEHOST_ postfix/anvil_PID_: statistics: max cache size
_DATEHOST_ postfix/anvil_PID_: statistics: max connection count
_DATEHOST_ postfix/anvil_PID_: statistics: max connection rate
_DATEHOST_ postfix/cleanup_PID_: _PFQID_ _EMAIL_
_DATEHOST_ postfix/cleanup_PID_: _PFQID_ message-id=<_EMAIL_>
_DATEHOST_ postfix/local_PID_: _PFQID_ to=
_DATEHOST_ postfix/pickup_PID_: _PFQID_ uid_DIGITS_ from=<.*>
_DATEHOST_ postfix/qmgr_PID_: _PFQID_ from=<_EMAIL_>, size_DIGITS_, nrcpt_DIGITS
_ \(queue active\)
```



```
_DATEHOST_ postfix/qmgr_PID_: _PFQID_ removed
_DATEHOST_ postfix/scache_PID_:
_DATEHOST_ postfix/smtpd_PID_: _PFQID_ client_HOST__IP_\]
_DATEHOST_ postfix/smtpd_PID_: _PFQID_ reject: RCPT from_HOST__IP_\]:_DIGITS__DI
GITS_\.1\.1 <_EMAIL_>: Recipient address rejected: User unknown in virtual mailb
ox table; from=<_EMAIL_> to=<_EMAIL_> proto=ESMTP helo=_HOST_
_DATEHOST_ postfix/smtp_PID_: _PFQID_ to=
_DATEHOST_ postfix/virtual_PID_: _PFQID_ to=
_DATEHOST_ puppet-agent_PID_: \(//Base/Exec\[Setting Xen independent wallclock\]
/returns\) executed successfully
_DATEHOST_ puppet-agent_PID_: Caught TERM; calling stop
_DATEHOST_ puppet-agent_PID_: Finished catalog run in \d+\.\d+ seconds
_DATEHOST_ puppet-agent_PID_: Reopening log files
_DATEHOST_ puppet-agent_PID_: \(/Stage\[main\]/Base/Exec\[Setting Xen independen
t wallclock\]/returns\) executed successfully
_DATEHOST_ puppet-agent_PID_: Starting Puppet client version 2\.6\.6
_DATEHOST_ puppetd_PID_: Caching catalog at /var/lib/puppet/localconfig\.yaml
_DATEHOST_ puppetd_PID_: Caught TERM; calling stop
_DATEHOST_ puppetd_PID_: Caught TERM; shutting down
_DATEHOST_ puppetd_PID_: Could not retrieve catalog from remote server: Connecti
on refused
_DATEHOST_ puppetd_PID_: Could not retrieve catalog from remote server: end of f
ile reached
_DATEHOST_ puppetd_PID_: Could not retrieve catalog from remote server: executio
n expired
_DATEHOST_ puppetd_PID_: Could not retrieve catalog; skipping run
_DATEHOST_ puppetd_PID_: .* Failed to retrieve current state of resource:  Could
 not retrieve file metadata for
_DATEHOST_ puppetd_PID_: Finished catalog run in .* seconds
_DATEHOST_ puppetd_PID_: \(//Node\[basenode\]/base/Exec\[Setting Xen independent
 wallclock\]/returns\) executed successfully
_DATEHOST_ puppetd_PID_: Reopening log files
_DATEHOST_ puppetd_PID_: Shutting down
_DATEHOST_ puppetd_PID_: \(/Stage\[main\]/Base/Exec\[Setting Xen independent wal
lclock\]/returns\) executed successfully
_DATEHOST_ puppetd_PID_: Starting catalog run
_DATEHOST_ puppetd_PID_: Starting Puppet client version_DIGITS_\.24\.8
_DATEHOST_ puppetd_PID_: Starting Puppet client version_DIGITS_\.25\.4
_DATEHOST_ puppetd_PID_: Starting Puppet client version_DIGITS_\.25\.5
_DATEHOST_ puppetd_PID_: Using cached catalog
_DATEHOST_ puppetd_PID_: Value of ‘preferred_serialization_format’ \(pson\) is i
nvalid for report, using default \(marshal\)
_DATEHOST_ restorecond: Will not restore a file with more than one hard link \(/
etc/resolv\.conf\) Invalid argument
_DATEHOST_ run-parts\(/etc/cron\.hourly\)_PID_: finished 0anacron
_DATEHOST_ run-parts\(/etc/cron\.hourly\)_PID_: starting 0anacron
_DATEHOST_ snmpd_PID_: Connection from UDP: \[_IP_\]:
_DATEHOST_ snmpd_PID_: Received SNMP packet\(s\) from UDP: \[_IP_\]:
_DATEHOST_ sshd_PID_: Accepted publickey for brian from _IP_ port_DIGITS_ ssh2
_DATEHOST_ sshd_PID_: Accepted publickey for dgibby from _IP_ port_DIGITS_ ssh2
_DATEHOST_ sshd_PID_: Accepted publickey for root from 10.0.2.31 port_DIGITS_ ss
h2
_DATEHOST_ sshd_PID_: Accepted publickey for root from 206.71.189.157 port_DIGIT
S_ ssh2
_DATEHOST_ sshd_PID_: Accepted publickey for treed from _IP_ port_DIGITS_ ssh2
_DATEHOST_ sshd_PID_: Address _IP_ maps to_HOST_, but this does not map back to
the address - POSSIBLE BREAK-IN ATTEMPT!
_DATEHOST_ sshd_PID_: Address _IP_ maps to localhost, but this does not map back
 to the address - POSSIBLE BREAK-IN ATTEMPT\!
_DATEHOST_ sshd_PID_: Connection closed by _IP_
_DATEHOST_ sshd_PID_: Connection closed by UNKNOWN
_DATEHOST_ sshd_PID_: Did not receive identification string from _IP_
_DATEHOST_ sshd_PID_: Failed password for .* from _IP_ port_DIGITS_ ssh2
_DATEHOST_ sshd_PID_: Failed password for invalid user .* from _IP_ port_DIGITS_
 ssh2
_DATEHOST_ sshd_PID_: Failed password for root from _IP_ port_DIGITS_ ssh2
_DATEHOST_ sshd_PID_: fatal: Read from socket failed: Connection reset by peer
_DATEHOST_ sshd_PID_: input_userauth_request: invalid user .*
_DATEHOST_ sshd_PID_: Invalid user .* from _IP_
```

```
_DATEHOST_ sshd_PID_: pam_succeed_if\(sshd:auth\): error retrieving information
about user
_DATEHOST_ sshd_PID_: pam_unix\(sshd:auth\): authentication failure; logname= ui
d_DIGITS_ euid_DIGITS_ tty=ssh ruser=
_DATEHOST_ sshd_PID_: pam_unix\(sshd:auth\): check pass; user unknown
_DATEHOST_ sshd_PID_: pam_unix\(sshd:session\): session closed for user
_DATEHOST_ sshd_PID_: pam_unix\(sshd:session\): session closed for user root
_DATEHOST_ sshd_PID_: pam_unix\(sshd:session\): session opened for user .* by \(
uid_DIGITS_\)
_DATEHOST_ sshd_PID_: Received disconnect from _IP_:_DIGITS_: Bye Bye
_DATEHOST_ sshd_PID_: Received disconnect from _IP_:_DIGITS_: Goodbye
_DATEHOST_ sshd_PID_: reverse mapping checking getaddrinfo for .* failed - POSSI
BLE BREAK-IN ATTEMPT\!
_DATEHOST_ sshd_PID_: reverse mapping checking getaddrinfo for_HOST_failed - POS
SIBLE BREAK-IN ATTEMPT\!
_DATEHOST_ sshd_PID_: reverse mapping checking getaddrinfo for_HOST_\[_IP_\] fai
led - POSSIBLE BREAK-IN ATTEMPT\!
_DATEHOST_ su: pam_unix\(su-l:session\): session closed for user root
_DATEHOST_ su: pam_unix\(su-l:session\): session opened for user root by .*\(uid
_DIGITS_\)
_DATEHOST_ syslogd _CLASSC_ restart\.
.* _PID_ Connection timed out
.* _PID_ Service '.*' timed out\.
type=.* msg=audit\(.*\): login
type=.* msg=audit\(.*\): pid
type=.* msg=audit\(.*\): user
_DATEHOST_ puppetd_PID_: Could not retrieve catalog from remote server:
_DATEHOST_ puppetd_PID_: \(.*\) Skipping because of failed dependencies
\d+ \d\d:\d\d:\d\d \[ERROR\] Invalid \(old\?\) table or database name '.*'
_DATEHOST_ puppetd_PID_: Run of Puppet configuration client already in progress;
 skipping
_DATEHOST_ puppet-agent_PID_: Starting Puppet client version_DIGITS_\.6\.12
```