

# localhost 11/25/14:00.00 system check

**Date:** Tue, 25 Nov 2014 00:00:01 -0600  
**To:** cpollock@embarqmail.com  
**From:** root <cpollock@embarqmail.com>

## Security Violations

==--==--==--==--==--==  
Nov 24 23:00:05 localhost postfix/smtp[30181]: 37E5E100034D: to=  
<cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
delay=3.5, delays=0.17/0.08/2.6/0.65, dsn=2.0.0, status=sent (250 SPF  
validation soft failure)  
Nov 24 23:58:02 localhost postfix/smtp[31452]: 3D72A100034D: to=  
<cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
delay=0.48, delays=0.09/0/0.2/0.19, dsn=2.0.0, status=sent (250 SPF  
validation soft failure)  
Nov 24 23:59:01 localhost postfix/smtp[31452]: 68903100034D: to=  
<cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
delay=0.56, delays=0.32/0/0.14/0.1, dsn=2.0.0, status=sent (250 SPF  
validation soft failure)  
Nov 24 23:59:02 localhost postfix/smtp[31452]: 45F9F100034D: to=  
<cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
delay=0.63, delays=0.19/0/0.14/0.3, dsn=2.0.0, status=sent (250 SPF  
validation soft failure)

## Unusual System Events

==--==--==--==--==--==  
Nov 24 23:00:02 localhost postfix/pickup[29180]: 37E5E100034D: uid=0 from=  
<root>  
Nov 24 23:00:02 localhost postfix/cleanup[30179]: 37E5E100034D: message-id=  
<20141125050002.37E5E100034D@cpollock.localdomain>  
Nov 24 23:00:02 localhost postfix/qmgr[2667]: 37E5E100034D: from=  
<cpollock@embarqmail.com>, size=17895, nrcpt=1 (queue active)  
Nov 24 23:00:05 localhost postfix/smtp[30181]: 37E5E100034D: to=  
<cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
delay=3.5, delays=0.17/0.08/2.6/0.65, dsn=2.0.0, status=sent (250 SPF  
validation soft failure)  
Nov 24 23:00:05 localhost postfix/qmgr[2667]: 37E5E100034D: removed  
Nov 24 23:11:53 localhost spamd[1511]: spamd: connection from ip6-localhost  
[::1]:53632 to port 783, fd 5  
Nov 24 23:11:53 localhost spamd[1511]: spamd: setuid to chris succeeded  
Nov 24 23:11:53 localhost spamd[1511]: spamd: processing message  
<54740E32.2000104@ubuntu.com> for chris:1000  
Nov 24 23:11:16 localhost clamd[2290]: message repeated 4 times: [  
SelfCheck: Database status OK.]  
Nov 24 23:11:54 localhost clamd[2290]: Accepted connection from 127.0.0.1 on  
port 1946, fd 13  
Nov 24 23:11:54 localhost dnsmasq[1125]: Maximum number of concurrent DNS  
queries reached (max: 150)  
Nov 24 23:12:13 localhost spamd[1511]: spamd: clean message (3.7/5.0) for  
chris:1000 in 20.1 seconds, 42435 bytes.  
Nov 24 23:12:13 localhost spamd[1511]: spamd: result: . 3 -  
AWL,BAYES\_00,KAM\_STOCKTIP,RCVD\_IN\_BRBL\_RELAY,RCVD\_IN\_MSPIKE\_H4,RCVD\_IN\_MSPIKE\_WL,RDNS\_NONE,UNPARSEABLE\_RELAY  
scantime=20.1,size=42435,user=chris,uid=1000,required\_score=5.0,rhost=ip6-  
localhost,raddr>:::1,rport=53632,mid=  
<54740E32.2000104@ubuntu.com>,bayes=0.000000,autolearn=disabled  
Nov 24 23:12:35 localhost freshclam[2404]: Received signal: wake up  
Nov 24 23:12:35 localhost freshclam[2404]: Max retries == 3  
Nov 24 23:12:35 localhost freshclam[2404]: ClamAV update process started at  
Mon Nov 24 23:12:35 2014  
Nov 24 23:12:35 localhost freshclam[2404]: Using IPv6 aware code  
Nov 24 23:12:35 localhost freshclam[2404]: Querying current.cvd.clamav.net  
Nov 24 23:12:35 localhost freshclam[2404]: TTL: 621  
Nov 24 23:12:35 localhost freshclam[2404]: Software version from DNS: 0.98.5  
Nov 24 23:12:35 localhost freshclam[2404]: Your ClamAV installation is  
OUTDATED!  
Nov 24 23:12:35 localhost freshclam[2404]: Local version: 0.98.4 Recommended  
version: 0.98.5  
Nov 24 23:12:35 localhost freshclam[2404]: DON'T PANIC! Read  
<http://www.clamav.net/support/faq>  
Nov 24 23:12:35 localhost freshclam[2404]: main.cvd version from DNS: 55  
Nov 24 23:12:35 localhost freshclam[2404]: main.cvd is up to date (version:  
55, sigs: 2424225, f-level: 60, builder: neo)  
Nov 24 23:12:35 localhost freshclam[2404]: daily.cvd version from DNS: 19677  
Nov 24 23:12:35 localhost freshclam[2404]: daily.cld is up to date (version:  
19677, sigs: 1273509, f-level: 63, builder: neo)  
Nov 24 23:12:35 localhost freshclam[2404]: bytecode.cvd version from DNS:  
242  
Nov 24 23:12:35 localhost freshclam[2404]: bytecode.cvd is up to date  
(version: 242, sigs: 46, f-level: 63, builder: dgoddard)  
Nov 24 23:12:38 localhost freshclam[2404]: -----  
-----  
Nov 24 23:14:14 localhost postfix/pickup[29180]: 37E5E100034D: uid=0 from=  
<root>

Nov 24 23:14:14 localhost spamd[1511]: spamd: connection from ip6-localhost  
 [::1]:53637 to port 783, fd 5  
 Nov 24 23:14:14 localhost spamd[1511]: spamd: setuid to chris succeeded  
 Nov 24 23:14:14 localhost spamd[1511]: spamd: processing message  
 <52B4453E4614AA724993B4207A4372DF-  
 46942e4687d14270b2eeac79f1cb2fd0@response.foxnews.com> for chris:1000  
 Nov 24 23:14:15 localhost clamd[2290]: Accepted connection from 127.0.0.1 on  
 port 1542, fd 13  
 Nov 24 23:14:31 localhost spamd[1511]: spamd: clean message (-114.0/5.0) for  
 chris:1000 in 16.9 seconds, 5360 bytes.  
 Nov 24 23:14:31 localhost spamd[1511]: spamd: result: . -114 -  
 AWL,BAYES\_00,DCC\_CHECK,DCC\_CHECK\_NEGATIVE,DIGEST\_MULTIPLE,DKIM\_SIGNED,DKIM\_VALID,DKIM\_VALID\_AU,HTML\_IMAGE\_ONLY\_24,HTML\_MESSAGE  
 scantime=16.9,size=5360,user=chris,uid=1000,required\_score=5.0,rhost=ip6-  
 localhost,raddr=::1,rport=53637,mid=<52B4453E4614AA724993B4207A4372DF-  
 46942e4687d14270b2eeac79f1cb2fd0@response.foxnews.com>,bayes=0.000000,autolearn=disabled  
 Nov 24 23:24:15 localhost clamd[2290]: SelfCheck: Database status OK.  
 Nov 24 23:36:46 localhost spamd[1511]: spamd: connection from ip6-localhost  
 [::1]:53659 to port 783, fd 5  
 Nov 24 23:36:46 localhost spamd[1511]: spamd: setuid to chris succeeded  
 Nov 24 23:36:46 localhost spamd[1511]: spamd: processing message <2082D3B2-  
 A075-48B4-BC41-11B25CEAA4D8@kitterman.com> for chris:1000  
 Nov 24 23:34:15 localhost clamd[2290]: SelfCheck: Database status OK.  
 Nov 24 23:36:46 localhost clamd[2290]: Accepted connection from 127.0.0.1 on  
 port 1707, fd 13  
 Nov 24 23:37:04 localhost spamd[1511]: spamd: clean message (-1.2/5.0) for  
 chris:1000 in 18.0 seconds, 14172 bytes.  
 Nov 24 23:37:04 localhost spamd[1511]: spamd: result: . -1 -  
 AWL,BAYES\_00,DKIM\_SIGNED,DKIM\_VALID,DKIM\_VALID\_AU,RDNS\_NONE,SPF\_HELO\_PASS,SPF\_PASS,UNPARSEABLE\_RELAY  
 scantime=18.0,size=14172,user=chris,uid=1000,required\_score=5.0,rhost=ip6-  
 localhost,raddr=::1,rport=53659,mid=<2082D3B2-A075-48B4-BC41-  
 11B25CEAA4D8@kitterman.com>,bayes=0.000000,autolearn=disabled  
 Nov 24 23:46:46 localhost clamd[2290]: SelfCheck: Database status OK.  
 Nov 24 23:58:02 localhost postfix/pickup[29180]: 3D72A100034D: uid=0 from=  
 <root>  
 Nov 24 23:58:02 localhost postfix/cleanup[31450]: 3D72A100034D: message-id=  
 <20141125055802.3D72A100034D@cpollock.localdomain>  
 Nov 24 23:58:02 localhost postfix/qmgr[2667]: 3D72A100034D: from=  
 <cpollock@embarqmail.com>, size=11271, nrcpt=1 (queue active)  
 Nov 24 23:58:02 localhost postfix/smtp[31452]: 3D72A100034D: to=  
 <cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
 delay=0.48, delays=0.09/0/0.2/0.19, dsn=2.0.0, status=sent (250 SPF  
 validation soft failure)  
 Nov 24 23:58:02 localhost postfix/qmgr[2667]: 3D72A100034D: removed  
 Nov 24 23:59:01 localhost postfix/pickup[29180]: 68903100034D: uid=0 from=  
 <root>  
 Nov 24 23:59:01 localhost postfix/cleanup[31450]: 68903100034D: message-id=  
 <20141125055901.68903100034D@cpollock.localdomain>  
 Nov 24 23:59:01 localhost postfix/qmgr[2667]: 68903100034D: from=  
 <cpollock@embarqmail.com>, size=3647, nrcpt=1 (queue active)  
 Nov 24 23:59:01 localhost postfix/smtp[31452]: 68903100034D: to=  
 <cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
 delay=0.56, delays=0.32/0/0.14/0.1, dsn=2.0.0, status=sent (250 SPF  
 validation soft failure)  
 Nov 24 23:59:01 localhost postfix/qmgr[2667]: 68903100034D: removed  
 Nov 24 23:59:02 localhost postfix/pickup[29180]: 45F9F100034D: uid=0 from=  
 <root>  
 Nov 24 23:59:02 localhost postfix/cleanup[31450]: 45F9F100034D: message-id=  
 <20141125055902.45F9F100034D@cpollock.localdomain>  
 Nov 24 23:59:02 localhost postfix/qmgr[2667]: 45F9F100034D: from=  
 <cpollock@embarqmail.com>, size=25456, nrcpt=1 (queue active)  
 Nov 24 23:59:02 localhost postfix/smtp[31452]: 45F9F100034D: to=  
 <cpollock@embarqmail.com>, relay=smtp.embarqmail.com[205.219.233.11]:587,  
 delay=0.63, delays=0.19/0/0.14/0.3, dsn=2.0.0, status=sent (250 SPF  
 validation soft failure)  
 Nov 24 23:59:02 localhost postfix/qmgr[2667]: 45F9F100034D: removed