

Sections

- [Archive](#)
- [Newsletter](#)
- [Popular Posts](#)
- [Privacy](#)
- [Submit](#)
- [Contact us](#)

Admon Linux

Insight into Linux system Administration work

Categories

- [Databases](#)
- [FAQs](#)
- [Hardwares](#)
- [Networking](#)
- [Reviews](#)
- [Scripting](#)
- [Security](#)
- [System Tuning](#)

Bash: Enable rsyslog support to record command history in CentOS

Posted on [January 12, 2017](#) by [joseph](#) [Leave a comment](#)



In this post, we show how to patch the default release of bash in CentOS-7.3 to enable built-in support of Rsyslog, in order to send command history to a central log server. This is helpful for internal users' behaviour auditing.

Get the source code package

To patch bash, we need the source code package. By default, **bash version in CentOS-7.3 is 4.2.46-21.el7_3**, we need to find and download it. The recommended search engine is rpm.pbone.net, you can [download it here](#).

The source package can be installed as normal RPM package. After installed we'll have a new directory created as ~/rpmbuild. In this example the path is /root/rpmbuild/.

Create Patch file and update bash.spec

This step is the key part. Please follow my steps below. First, let's edit the source code.

```
cd /root/rpmbuild/SOURCES
tar zxf bash-4.2.tar.gz
cp -prf bash-4.2 bash-4.2-orig
cd bash-4.2
```

There are two files needs to be edited, config-top.h and bashhist.c. Open config-top.h, and uncomment the line 104, and specify log output level as local1.debug. After edited, the file would look like this,

```
#define SYSLOG_HISTORY
#if defined (SYSLOG_HISTORY)
# define SYSLOG_FACILITY LOG_LOCAL1
# define SYSLOG_LEVEL LOG_DEBUG
#endif
```

Edit bashhist.c, to make the log more meaningful to understand. Basically we redefined the log format for the function bash_syslog_history(). Here are my settings,

```
void
bash_syslog_history (line)
    const char *line;
{
    char trunc[SYSLOG_MAXLEN];

    if (strlen(line) < SYSLOG_MAXLEN)
        syslog (SYSLOG_FACILITY|SYSLOG_LEVEL, "HISTORY: PID=%d UID=%d USER=%s CMD=%s", g
    else
    {
        strncpy (trunc, line, SYSLOG_MAXLEN);
        trunc[SYSLOG_MAXLEN - 1] = '\0';
        syslog (SYSLOG_FACILITY|SYSLOG_LEVEL, "HISTORY: PID=%d UID=%d USER=%s CMD(TRUN
    }
}
```

Now create the patch file,

```
[root@localhost SOURCES]# diff -Npru bash-4.2-orig bash-4.2 > bash_history_rsyslog.p
```

[This patch can be downloaded here](#). And then update the spec file bash.spec, which is located at /root/rpmbuild/SPECS/bash.spec

The sequence of our new patch is 145, so let's add new after line 170, as below,

```
#Enable detailed syslog info
Patch145: bash_history_rsyslog.patch
```

And after line 295, add new line,

```
%patch145 -p1 -b .history_rsyslog
```

The new bash.spec file is also [available for download](#).

Build new bash package

After editing bash.spec, we are ready to go. switch to /root/rpmbuild/SPECS, and run,

```
rpmbuild -ba bash.spec
```

It may take 2-3 minutes to generate new RPM package. When thing is done in this step, you will see something like this, which means new package has been created smoothly.

```
Processing files: bash-debuginfo-4.2.46-22.el7.centos.x86_64
Provides: bash-debuginfo = 4.2.46-22.el7.centos bash-debuginfo(x86-64) = 4.2.46-22.e
Requires(rpmlib): rpmlib(FileDigests) <= 4.6.0-1 rpmlib(PayloadFilesHavePrefix) <= 4
Checking for unpackaged file(s): /usr/lib/rpm/check-files /root/rpmbuild/BUILDROOT/b
Wrote: /root/rpmbuild/SRPMS/bash-4.2.46-22.el7.centos.src.rpm
Wrote: /root/rpmbuild/RPMS/x86_64/bash-4.2.46-22.el7.centos.x86_64.rpm
Wrote: /root/rpmbuild/RPMS/x86_64/bash-doc-4.2.46-22.el7.centos.x86_64.rpm
Wrote: /root/rpmbuild/RPMS/x86_64/bash-debuginfo-4.2.46-22.el7.centos.x86_64.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.FD7F6J
+ umask 022
+ cd /root/rpmbuild/BUILD
+ cd bash-4.2
+ rm -rf /root/rpmbuild/BUILDROOT/bash-4.2.46-22.el7.centos.x86_64
+ exit 0
```

Copy the new bash RPM package, and installed it on related servers. Since we did exactly when we know for Bash, we can use `—force` to install it,

```
rpm -ivh -force /root/rpmbuild/RPMS/x86_64/bash-4.2.46-22.el7.centos.x86_64.rpm
```

Update rsyslog.conf and Setup log server

Now what we have to do next is to enable logging. The settings need to be done on both client side and server side.

Config rsyslog servers

Uncomment these lines of /etc/rsyslog.conf on log server,

```
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514
```

The add these new line below the line “##### GLOBAL DIRECTIVES #####”

```
$template IpTemplate, "/var/log/bash-log/%FROMHOST-IP%.log"
*. * ?IpTemplate
& ~
```

On client side, we also need to update `/etc/rsyslog.conf`, to ask it send out command history to central log server. Add new line,

```
local11.debug                @@10.12.10.33
```

10.12.10.33 is the IP address of our log server.

Restart rsyslogd on both side,

```
systemctl restart rsyslog
```



Then re-login, to make sure we are using the new bash. Run some commands on the servers with bash updated, then we would see new files generated on log server as below,

```
[root@ns SPECS]# cd /var/log/bash-log/
[root@ns bash-log]# ls
10.12.10.28.log  10.12.10.48.log  10.12.11.221.log  10.12.11.28.log  127.0.0.1.log
[root@ns bash-log]# tail 10.12.10.48.log
Jan 12 13:46:52 nl-node-3 -bash: HISTORY: PID=113638 UID=1000 USER=jchen CMD=pwd
Jan 12 13:46:53 nl-node-3 -bash: HISTORY: PID=113638 UID=1000 USER=jchen CMD=dmesg
Jan 12 15:48:36 nl-node-3 -bash: HISTORY: PID=124905 UID=1000 USER=jchen CMD=df -kh
Jan 12 15:48:37 nl-node-3 -bash: HISTORY: PID=124905 UID=1000 USER=jchen CMD=ls
Jan 12 15:49:03 nl-node-3 -bash: HISTORY: PID=124905 UID=1000 USER=jchen CMD=ls *
Jan 12 15:49:15 nl-node-3 -bash: HISTORY: PID=124905 UID=1000 USER=jchen CMD=ls *@#&
```

Files mentioned in this post:

- [Updated bash-4.2.46-22 spec file in CentOS-7.3 \(276 downloads\)](#)
- [Bash patch that enables rsyslog support in CentOS-7.3 \(313 downloads\)](#)

More related posts

-  [Set system variables in Debian and CentOS](#)
-  [SysAdmin Tips: Bash Shell Shortcuts](#)

-  [How to install Go lang on CentOS?](#)

-  [Convert RHEL 5 to CentOS 5](#)

-  [Update CentOS 4 to CentOS 5 remotely.](#)

Categories: [System Tuning](#)

Tags: [bash](#), [centos](#), [rsyslog](#)

Leave a comment

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

☐ Save my name, email, and website in this browser for the next time I comment.

☐ Notify me of follow-up comments by email.






☐ Notify me of new posts by email.

[« ZooInspector: zookeeper graphic interface](#)
[Enable HTTP/2 Support for Nginx on Debian Jessie »](#)

Email

Search for:

More related posts

-  [Set system variables in Debian and CentOS](#)[Set system variables in Debian and CentOS](#)
-  [SysAdmin Tips: Bash Shell Shortcuts](#)[SysAdmin Tips: Bash Shell Shortcuts](#)
-  [How to install Go lang on CentOS?](#)[How to install Go lang on CentOS?](#)
-  [Convert RHEL 5 to CentOS 5](#)[Convert RHEL 5 to CentOS 5](#)
-  [Update CentOS 4 to CentOS 5 remotely](#)[Update CentOS 4 to CentOS 5 remotely](#)
- [Archive](#)
- [Newsletter](#)
- [Popular Posts](#)
- [Privacy](#)
- [Submit](#)
- [Contact us](#)

Powered by [WordPress](#) and [HeatMap AdAptive Theme](#)

%d bloggers like this: