How to enable command line audit logging in linux | Confluence | Atlassian Support

By Atlassian

Published: 2025-04-08 · Archived: 2026-04-06 01:04:16 UTC

Platform Notice: Data Center Only - This article only applies to Atlassian apps on the Data Center platform.

Note that this KB was created for the Data Center version of the product. Data Center KBs for non-Data-Center-specific features may also work for Server versions of the product, however they have not been tested. Support for Server* products ended on February 15th 2024. If you are running a Server product, you can visit the Atlassian Server end of support announcement to review your migration options.

*Except Fisheye and Crucible

Summary

The content on this page relates to platforms which are not supported. Consequently, Atlassian Support **cannot guarantee providing any support for it**. Please be aware that this material is provided for your information only and using it is done so at your own risk.

This KB article contains information that is outside of the Atlassian Support Offerings and is provided as a suggestion to achieve the mentioned goal.

This is not intended as a complete solution nor as a recommendation to use on production instances.

As this involves security concerns, the administrator should work in conjunction with their security team to understand the best solution available to their company.

To record all commands entered into the shell in a linux environment to a log file. This can be useful for auditing user actions or for security audits.

This is not specific to Confluence or any product, but it will audit command line actions including those things related to Confluence. Service restarts, all inputs from bash, and user actions should all be logged using this method.

As an alternative you may consider Snoopy:

Snoopy is a small library that logs all program executions on your Linux/BSD system.

Solution

1. Login to the linux box and assume root

```
sudo su -
```

2. Edit **/etc/profile** and add the following lines to the bottom of the file:

```
# command line audit logging function log2syslog { declare COMMAND COMMAND=$(fc -ln -0) logger -p local1.notice -t bash -i -- "${USER}:${COMMAND}" } trap log2syslog DEBUG
```

3. Save and exit **/etc/profile**

4. Edit **/etc/rsyslog.conf** and add the following lines to the bottom of the file:

```
# command line audit logging local1.* -/var/log/cmdline
```

5. Save and exit **/etc/rsyslog.conf**

6. Either restart the rsyslog service, or restart the whole machine to release all user sessions - forcing a reload of the bash profile and enacting the changes

```
/etc/init.d/rsyslog restart
```

7. The audit logging will be visible under **/var/log/syslog** and **/var/log/cmdline** and will look like this:

```
Aug 22 15:04:39 ip-10-10-34-56 bash[15856]: jsmith: Aug 22 15:04:40 ip-10-10-34-56 bash[15859]: jsmith:#011 sudo su - Aug 22 15:04:43 ip-10-10-34-56 bash[15893]: root: Aug 22 15:04:49 ip-10-10-34-56 bash[15903]: root:#011 ls -lart /var/log Aug 22 15:05:01 ip-10-10-34-56 CRON[15927]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1) Aug 22 15:05:06 ip-10-10-34-56 bash[15937]: root:#011 ls -lart /var/log | grep cmd Aug 22 15:15:01 ip-10-10-34-56 CRON[17254]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1) Aug 22 15:17:01 ip-10-10-34-56 CRON[17513]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly) Aug 22 15:20:02 ip-10-10-34-56 bash[17921]: root:#011 cd /var/log Aug 22 15:20:03 ip-10-10-34-56 bash[17924]: root:#011 ls Aug 22 15:20:16 ip-10-10-34-56 bash[17969]: root:#011 service confluence restart Aug 22 15:20:16 ip-10-10-34-56 systemd[1]: Stopping SYSV: Confluence... Aug 22 15:20:16 ip-10-10-34-56 confluence[17975]: Stopping confluence Aug 22 15:20:16 ip-10-10-34-56 systemd[1]: Started Session c8 of user confluence. Aug 22 15:20:27 ip-10-10-34-56 confluence[17975]: confluence stopped successfully Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Stopped SYSV: Confluence. Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Starting SYSV: Confluence... Aug 22 15:20:27 ip-10-10-34-56 confluence[18103]: Starting confluence Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Stopping User Manager for UID 1300... Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Stopped target Default. Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Stopped target Basic System. Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Stopped target Paths. Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Stopped target Timers. Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Reached target Shutdown. Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Starting Exit the Session... Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Stopped target Sockets. Aug 22 15:20:27 ip-10-10-34-56 systemd[20231]: Received SIGRTMIN+24 from PID 18107 (kill). Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Stopped User Manager for UID 1300. Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Removed slice User Slice of
```

```
confluence. Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Created slice User Slice of confluence. Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Starting User Manager for UID 1300... Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Started Session c9 of user confluence. Aug 22 15:20:27 ip-10-10-34-56 systemd[18113]: Reached target Paths. Aug 22 15:20:27 ip-10-10-34-56 systemd[18113]: Reached target Timers. Aug 22 15:20:27 ip-10-10-34-56 systemd[18113]: Reached target Sockets. Aug 22 15:20:27 ip-10-10-34-56 systemd[18113]: Reached target Basic System. Aug 22 15:20:27 ip-10-10-34-56 systemd[18113]: Reached target Default. Aug 22 15:20:27 ip-10-10-34-56 systemd[18113]: Startup finished in 9ms. Aug 22 15:20:27 ip-10-10-34-56 systemd[1]: Started User Manager for UID 1300. Aug 22 15:20:28 ip-10-10-34-56 systemd[1]: Started SYSV: Confluence. Aug 22 15:20:41 ip-10-10-34-56 bash[18207]: root:#011 ls Aug 22 15:20:54 ip-10-10-34-56 bash[18271]: root:#011 less syslog
```

8. You may consider saving the log on an NFS mount and/or pushing the syslog logs to another machine.

Updated on September 25, 2025

Was this helpful?

It wasn't accurateIt wasn't clearIt wasn't relevant

Still need help?

The Atlassian Community is here for you.
