

## BSM Audit Troubleshooting help

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2002-02/0005.html>

---

**From:** Anupam ([frj780jdy85533001@sneakemail.com](mailto:frj780jdy85533001@sneakemail.com))

**Date:** 02/11/02

From: "Anupam" <[frj780jdy85533001@sneakemail.com](mailto:frj780jdy85533001@sneakemail.com)>

To: <[focus-sun@securityfocus.com](mailto:focus-sun@securityfocus.com)>

Date: Mon, 11 Feb 2002 05:48:21 -0500

Hi,

We enabled BSM auditing on a remotely administered Solaris 8 server. We took the machine down to single-user mode and enabled auditing, then rebooted the machine. For a certain period of time the system was logging data.

The audit file `/var/audit/*not*` just stopped growing. I tried running the following commands:

- `auditconfig -chkconf` (No output when the command is run)
  - `audit -s` (Created a new audit file with just the time stamp)
  - `modinfo | fgrep -i audit`
- 54 78180000 11f8c 186 1 c2audit (C2 system call)

Unfortunately we can't reboot the machine at will, because it is a production machine.

Any suggestion on how to troubleshoot this would be greatly appreciated. BTW is there any real reason to bring down the machine to single-user mode before enabling BSM? Is it necessary to ensure that the system is quiet, or is it something more important?

I have included below data from the `audit_control`, `audit_user` and `audit_startup` files if it helps.

Thanks,

- Anupam

FWIW Software on the box:

- Veritas DB Edition for Oracle
- Oracle 8i
- BMC patrol for monitoring

`/etc/security/audit_control:`

`dir:/var/audit`

`flags:ad,lo,ex,fw,fc,fd`

`minfree:20`

## SecurityFocus SUN: BSM Audit Troubleshooting help

naflags:lo,ad

/etc/security/audit\_user

root::no,-io

user1::no,-io

user2::no,-io

user3::no,-io

user4::no,-io

oracle::no,-io

patrol::no,-io

/etc/security/audit\_startup

auditconfig -conf

auditconfig -setpolicy none

auditconfig -setpolicy +cnt

- 
- **Previous message:** [Darren Moffat: "Re: Trouble changing BSM/audit options without reboot"](#)
  - **Next in thread:** [Anupam: "Re: BSM Audit Troubleshooting help"](#)
  - **Reply:** [Anupam: "Re: BSM Audit Troubleshooting help"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)