

# SUMMARY WAS: OT? Philosophical Question on SA responsibilities

*Source:* <http://unix.derkeiler.com/Mailing-Lists/SunManagers/2004-01/0645.html>

---

*From:* Bruntel, Mitchell L, ALABS ([mbruntel\\_at\\_att.com](mailto:mbruntel_at_att.com))

*Date:* 01/30/04

Date: Fri, 30 Jan 2004 15:18:14 -0600

To: <[sunmanagers@sunmanagers.org](mailto:sunmanagers@sunmanagers.org)>

SUMMARY : I've left the original attached too.

I am not sure if I will send the script to the list, or simply to the folks who requested, but it will follow!

SUMMARY: OT: What would YOU DO? (A LENGTHY Analysis)

26 Responses today:

Quick Summary:

=====

LOOK before you leap. If you're an administrator, find out if your new boss is interested in someone who can take charge, and has a brain, or just wants a body to do exactly what they say, and no more! Also helpful for managers interested in hiring new administrators. Perhaps ask THEM the questions, and ask them to discuss. The general consensus is that politics unfortunately gets into everything these days! And remember, that you are part of a team, not a solo Unix jock!

As a brand new employee anywhere, even if I was in charge, I would not presume to change things without first finding out why things are they way they are.

As an admin, I always assume that my job includes "doing the right thing". I would work with whomever to get security as tight as it needs to be, but no tighter.

Detailed Responses:

=====

Note: I am not thanking by names those who helped out with answers. Amazing how many people (more than 2!) were scared that people they worked with might disapprove (of) (or recognize) the comments.

I personally think that this discussion will actually go down as being an ON topic, or an ON TOPIC discussion for EVERYONE reading this list BEFORE going on an interview, OR offering a job to someone!

SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

RESULTS of the sunmanager's PROFESSIONAL'S POLL:

=====

NOTE: Please see original message (at end) for questions.

Overall Comments:

=====

\* A great deal of the respondents essentially said:

POLITICS rears its ugly head again. Furthermore, there are essentially two different schools of thought. Bosses either want an automaton (robot), or want someone who will be "proactive".

\* Most important point to note is this:

The SA MUST either ASK, or find out what kind of a manager they are going to work for.

\* IF the boss wants a robot, be a robot. If the boss wants someone with a mind, also fine. But never shall the twain meet.

\* To me this is very very very sad. The fact that there ARE people who WANT someone who DOESN'T work at their fullest potential is a very sad commentary on today.

\* The quickest way to start a fight or create hard feelings is to dive in as though you are the owner of the systems and make them over in your own style.

\* Until your PS, I assumed the questions were sort of rhetorical. Then I wondered if perhaps you were the new but experienced SA being called on the carpet for doing these things.

\*\*\*\* Guilty as charged\*\*\*\* and unfortunately, one of the 3 other administrators is my boss, who did actually ask me to log in and install the xyz software (and tell me rebooting/working as root was ok).

\* My answer to all would be to not make presumptions or overstep your authority or assignment, especially as a new SA working with others who were already there. You can certainly bring things to their attention, ask them about things you see, and/or ask permission to do things. But, the quickest way to start a fight or create hard feelings is to dive in as though you are the owner of the systems and make them over in your own style.

\*Show respect for others' work and take the time to develop a good working relationship. If the new SA in the shop is really good, best results for all come about if that new SA also works confidently but cautiously without trying to take over, "prove" himself, or show off.

\*In some shops "doesn't play well with others" qualifies an individual for being thrown out, regardless of how much they know.

SUMMARY WAS: OT? Philosophical Question on SA responsibilities

SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

\*Just as an example, I have some systems with telnet open. They need to be. You don't need to know why, but if you worked with me, you should ask why. They happen to also be secured with TCP/Wrappers and other things as well, but general policy would presume that SSH should be everywhere and telnet closed. In this instance there is an exception to the general policy for a particular reason.

\*My own take on this is that there is a massive hole in the company's management practices. Gray areas of responsibility and the degree to which individual SAs should be permitted to use their own discretion, should be spelled out as much as possible in advance, preferably in the form of a policy/procedure document.

\*That really sucks. Its sad because I continually have to put up with dorks that need to be told what to do constantly. I work with more people that don't move a finger to keep a system up to date, check logs, or anything. They wait for a ticket to come in or a phone call and then get bent out of shape when its a call and not a ticket.

\*I'd look through some of them to see if it's some kind of system error generating them then I'd delete them. I'd be sure to check back the next day to see if any more was there. Something must be generating all those emails and I would want to know what it is.

Question 1: Would you go thru the 14,600 messages in root and admin mailboxes, and delete them?

Further clarification:

=====

(very important, sorry I didn't specify this in advance: ALL messages were caused by cron entries (running about 4 per hour, or 200/day.) ALL messages were checked (by size, # day before (spot checking, then deleting all. ALSO: This was a production system, with NO users, ONLY running scripts. NO regular output is expected from systems via mail.

YES: 6

NO 2

Maybe 3

Comments: YES

=====

I'd say yes to this, with the caveat that you don't delete important ones and that you also set these mail boxes to forward to someone live who can monitor them in a timely fashion. Also take steps to determine why there's 14K of them.

I would truncate the entire message file, install XYZ software and then monitor the messages for applications using the syslog facility.

I guess I would check the most recent mail, max. X week old. If the mail files are not filling disk, then I would be inclined to leave them

SUMMARY WAS: OT? Philosophical Question on SA responsibilities

SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

until I can talk to the other admins as there might be some absurd company policy. Bearing in mind that mail jobs rarely report anything serious though they often report on failed backups or other processes. All of which, if important, should be in the last 5 days worth of mail (making sure you check mail for a Sunday as this is the most likely time for a FULL backup). I would be more interested in the messages file and any explorer output, etc.

Comments NO:

=====

Absolutely not -- we're a development house, and those messages are often pertaining to nightly build failures, and are very often used for POP and IMAP testing -- so if a new admin came in and took the initiative to do that, I'd have to point out to them they made an error in judgement.

My further experience says:

- A) If it's a development machine it BETTER NOT have 14,000 UNREAD MESSAGES.
- B) They DAMN better be cleaning and or moving them somewhere else.
- C) Note: was production machine with NO users!

A new admin should be "look but don't touch", ask first.

Maybe so

=====

The first thing I do when I get on a system I haven't seen before is to look around, check disk space, see what's new in crons, look for scripts I can borrow or copy, look in the /etc for anything amiss. Just snoop around.

If I was a new SA I would if encountering a security hole, I would contact my immediate boss and inform them what I found and ask what are the policies for the site.

My \$.02 is that it would depend on the environment, applications, personalities, etc. So I'd ask first, get a feel for things before making changes.

Question B:

Would you presume your charge also includes "doing the right thing" to tighten the security on the box?

YES 1

No 7

Maybe 6

Mitch's Comments:

=====

See question on politics at start of message.

## SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

Main point to take away (for others, please forgive the, "DUH, NO KIDDING" point coming up!)

Main Point? There is a significant difference in administrating machines by yourself or sharing administrative responsibilities with a group.

Life as a solo system administration is DIFFERENT. Not better, not worst.. BUT DIFFERENT.

YES COMMENTS:

=====

Yep.

NO COMMENTS:

=====

- \* new admin should be look but don't touch; ask first.
- \* In that environment of shared responsibility, if that is all a new admin is told, then no, they should not do anything else without checking.
- \* Who is to say that "doing the right thing" won't actually be "doing the wrong thing" when you tighten security a bit too much and break something.
- \* All too often, I find that vendor apps require taking a few risks with permissions, locations, etc. Hardening a box too far can cause trouble , but there isn't much you can do because you are committed to those apps. until you can find better alternatives.
  
- \* As for doing it all as part of a team without checking with the rest of the team. No way! If you are new, you don't have all the reasons the boxes might be set up the way they are. I have several here at work, behind firewall, that are wide open, not a lot I can do about it except to monitor them.
  
- \* If I was a new SA I would if encountering a security hole, I would contact my immediate boss and inform them what I found and ask what are the policies for the site.
  
- \* I would not change anything without a change request agreement. It is okay to identify but not to change functionality or configurations
  
- \* d) I don't presume b but I would implement d if given the option.
  
- \* I would not change anything without a change request agreement. It is okay to identify but not to change functionality or configurations
  
- \* I don't presume b but I would implement d if given the option.
  
- \* My own take: There is a massive hole in the company's management practices. Gray areas of responsibility and the degree to which individual SAs should be permitted to use their own discretion, should

SUMMARY WAS: OT? Philosophical Question on SA responsibilities

## SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

be spelled out as much as possible in advance, preferably in the form of a policy/procedure document.

o Furthermore, I believe there should be controls on how each server is administered, so as to provide you with a head start on solving any problems that arise on a server that someone else may have been responsible for recently but is absent.

o Imagine 15 different machines being administered willy-nilly. I think all these things can be accomplished without unduly curtailing creativity and a modicum of independence on the part of each SA.

o

o In the past young SA's with enthusiasm think that "trying to impress" is a good thing, but then I've noticed the sys user has gone due to the sys user never being logged in and they thought it best to just run a

# "userdel -r sys", this in turn deleted a hell of a lot of the system and the SA in turn got a severe "data-entry" task to do for a week or so.

Maybe SO

=====

o B, c, d ... Hmm, strong arguments on both side of this one. As the "new guy" you should avoid ruffling feathers. You definitely should look if you have the expertise to do so. You should report your findings and determine what the policy (or lack thereof) is. Reaction could vary from "we're ignorant on the topic and could use your help" to "mind your own business" to "there's a reason for that."

o You may not consider any reason given to be a good one, but the reason might exist, and making the changes break something.

o most certainly ask -- there are lots of reasons that people have chosen to accept security risks for different reasons -- again, as a development house we've made multiple decisions to allow security risks in our environment -- this is totally something that needs to be discussed with the existing systems administrators, as the new administrator might be unaware of requirements on the systems for what they would consider to be security vulnerabilities.

o I wouldn't install patches or replace system software (eg., solaris bind with latest ISC), but I might add non-intrusive monitoring (ie., not snort, or a dictionary checker to PAM).

o For patching or replacing, I would check with my new supervisor: "Hey, I'm doing the work instructed on these systems and I noticed <foo>. May I do <bar>?"

o b) Depends on the environment. If this box is in a DMZ then yes. If it is a no nothing dev box, maybe/maybe not. Theoretically, every box should be locked down, and if you have jumpstart then that is easily done. In practice, different boxes need different applications and

## SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

should be done on a categorical bases. IE web servers should look the same, DB servers should look the same, etc..

o If you do b, and find security vulnerabilities, would you shut them down, (fix them directly), or ask for permission to fix them.

o most certainly ask --- there are lots of reasons that people have chosen to accept security risks for different reasons --- again, as a they would consider to be security vulnerabilities decisions to allow security risks

o in our environment --- this is totally something that needs to be discussed with the existing systems administrators, as the new administrator might be unaware of requirements on the systems.

o I've worked at places where the parameters included only my specific task and no more; check your brain at the door.

o I've also worked for people who said "keep the users happy, the systems up, and corporate off of my back"

I'll Summarize Question C:

=====

If you do b, and find security vulnerabilities, would you shut them down, (fix them directly), or ask for permission to fix them.

Pretty much, everyone said, ask first. (and I did! And the vulnerabilities are STILL OPEN)

Question D:

=====

if you presume b( do right thing) includes Ensuring security on the boxes, would you do the following:

Add a NON-INVASIVE (log only) Cron that does the following:

for all id's on system:

do

1) passwd -s userid

# comment #< gets user password status # #(locked/nopassword,etc)

2) crontab -l userid

#(check if user is in cron.allow, deny, etc.)

3) Log results to a file in /var/adm, automatically by day date/month/year (creating directories as necessary.

Comment on D:

I can see some use for the passwd -s part of the crontab script, but not for the crontab -l part.

SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

ANSWER: You'd be surprised how many times I found that my users LIED, and or installed their own "subversive" cron scripts in previous places, that I discovered by monitoring the differences in the crontab -l command.

ALSO stuff run by people no longer there, etc.

OR even simply UUCP(or its remains). (we've depreciated it at our company, but some systems still had logins ,and other unneeded stuff!)

Question D:

YES: 6

NO ?

MAYBE SO: 4

Yes Comments:

=====

Once you have permission for B&C, then add the scripted cron jobs

As regards, putting any non-invasive security checks, etc. I would feel free to do whatever I thought would benefit the company and systems and over all argue the case for whatever changes I feel are required based on my experience, best practise, etc. even if it is against company policy but I would be more inclined to use freeware security utilities that are around rather than re-inventing the wheel.

Yep!

Sure, if you already have a script and there is no other monitoring. Its pretty non-evasive so it should be ok. Just make sure that you don't fill /var...rotate logs. Checking passwords and crons aren't that informative vs. a true tripwire type of config or cfengine.

MAYBE SO:

=====

I don't presume b but I would implement d if given the option

Probably, but I'd also make sure the other folks in the group knew it was there, probably via an email.

When the new admin started, was he or she given a briefing about the security stance and policies of the group? How about CM policies for the servers? It's on the boss' shoulders to orient the new guy appropriately and it's on new guy to make sure he understands what the group expects and wants.

Really depends on the company. What you're describing sounds like good admin practice, but I would take the company culture in to account. Working for the government this action probably equals social suicide. Tightening up security means you think (and express openly ) the other 3 admins did a bad job at this. They will might never forgive you for such an open criticism. So sometimes I think it is smarter to form some friendships first. In a small company with an open culture I can see me doing something like this on the first day though.

SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

You may only not quote me except without my name. It's surprised me more than once how a remark like this can backfire on you at a point where you forgot you ever made it.

Once you have permission for B&C, then add the scripted cron jobs.

SUMMARIZING AGAIN:

=====

Interesting. Majority would Delete the old, stale email messages.  
Majority would NOT presume that taking working on a system as root means you should try and make it as "bullet-proof" as possible.  
MAJORITY feel that as the jr. team member, need to work with colleagues.  
HOWEVER

Majority seems to feel installing a NON Invasive, NON system affecting cron would NOT be offensive, and would help tighten security.

As I always say, "go figure".

-----Original Message-----

From: Bruntel, Mitchell L, ALABS  
Sent: Friday, January 30, 2004 9:47 AM  
To: sunmanagers@sunmanagers.org  
Subject: OT? Philosophical Question on SA responsibilities

Here's a question for other administrators:

Question:  
Presume the following:  
15 remotely located machines (all solaris)  
3 people allowed to use root password.

New admin joins group.  
Told to install XYZ software on machines.  
Told Reboot, if necessary is ok.  
Told install ok to install additional pre-requisites if needed...

OH, and there are NO users on the box, just those administrators.

Here are the questions:  
As a experienced SA logging into the machine for the first time:

- a) would you go thru the 14,600 messages in root and admin mailboxes, and delete them?
- b) Would you presume your charge also includes "doing the right thing" to tighten the security on the box?
- c) If you do b, and find security vulnerabilities, would you shut them down, (fix them directly), or ask for permission to fix them.
- d) if you presume b, is correct, would you install a cron job that does the following?

SUMMARY WAS: OT? Philosophical Question on SA responsibilities

## SunManagers: SUMMARY WAS: OT? Philosophical Question on SA responsibilities

for all id's on system: do

- 1) passwd -s userid (gets user password status (locked/nopassword,etc))
- 2) crontab -l userid (sees if user is in cron.allow, deny, etc.)
- 3) Log results to a file in /var/adm, automatically by day date/month/year (creating directories as necessary).

Thanks: I'll summarize.

PS: want the script? Email me. It's saved me a few times, and found a few unauthorized things in the past!

---

sunmanagers mailing list  
sunmanagers@sunmanagers.org  
<http://www.sunmanagers.org/mailman/listinfo/sunmanagers>

---

sunmanagers mailing list  
sunmanagers@sunmanagers.org  
<http://www.sunmanagers.org/mailman/listinfo/sunmanagers>