FreeNAS - Bug #18615

Skip old login failures in daily security run output

10/29/2016 01:56 PM - Daniel Shaffer

Status:	Resolved		
Priority:	Nice to have		
Assignee:	Vladimir Vinogradenko		
Category:	Middleware		
Target version:	11.1-BETA1		
Seen in:	9.10.1-U2	**Needs Merging:**	Yes
Severity:	New	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	Platform: Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz Memory: 130964MB M1015 Flashed to IT mode w/ no BIOS boot option 4x4tb RaidZ2 + 4x4tb RaidZ2 3x4tb are on motherboard SATA ports 5x4tb are on M1015 SAS/SATA ports
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	Yes		

Description

I received a daily security run output email last week which reported that I had login failures. Since I hadn't logged in at all that day, I immediately went to check them out thinking a hacker had been targeting my system. It turns out the script which checks for login failures doesn't check the auth.log for a year since the auth.log doesn't log the year, so I was getting reports about errors from 2015 instead of this year (2016).

Summary: The /var/log/auth.log file doesn't include a year when it reports login failures. It also doesn't seem to automatically rollover each year or something equivalent. The /etc/periodic/security/800.loginfail script seems to look for all errors from 'yesterday', where 'yesterday' is defined by

```
date -v-1d "+%b %e "
```

and can't check for a year. Possible solutions:

- Cause auth.log to rollover either each day/week/month/year?
- Only count a report as coming from yesterday if there are no more days following it in the log?
- Start logging the year of the login error as well?
- etc.

Related issues:

Related to FreeNAS - Bug #18319: [Regression] Outdated Security Run Outputs	**Closed: Duplicate**	**10/18/2016**
Has duplicate FreeNAS - Bug #24090: Log from last year sent again in the same...	**Closed: Duplicate**	**05/22/2017**

Associated revisions

Revision 15b43bc2 - 08/31/2017 04:56 AM - Vladimir Vinogradenko

fix(etc): /etc/periodic/security/800.loginfail-freenas that skips messages from previous years

Ticket: #18615

Revision 7f201c55 - 08/31/2017 05:13 AM - Vladimir Vinogradenko

fix(etc): /etc/periodic/security/800.loginfail-freenas that skips messages from previous years

Ticket: #18615

Revision 701af451 - 08/31/2017 05:25 AM - Vladimir Vinogradenko

fix(etc): /etc/periodic/security/800.loginfail-freenas that skips messages from previous years

Ticket: #18615

Revision 5f12b64b - 08/31/2017 05:34 AM - Vladimir Vinogradenko

fix(etc): /etc/periodic/security/800.loginfail-freenas that skips messages from previous years

Ticket: #18615

Revision 2f393449 - 09/27/2017 01:25 PM - Vladimir Vinogradenko

fix(etc): /etc/periodic/security/800.loginfail-freenas that skips messages from previous years

Ticket: #18615

History

#1 - 10/29/2016 01:59 PM - Daniel Shaffer

The following link helped me in my debugging in case it helps anyone else.

https://forums.freebsd.org/threads/32926/

#2 - 10/31/2016 06:07 AM - Bonnie Follweiler

- Assignee set to Alexander Motin

#3 - 10/31/2016 12:09 PM - Kris Moore

- Assignee changed from Alexander Motin to Suraj Ravichandran

I dunno about changing the log format, but perhaps we could do better rotation?

#4 - 10/31/2016 12:12 PM - Alexander Motin

I had no time to look how it works on FreeBSD, but I would guess it should be handled there somehow. I would start investigation from what FreeNAS could break.

#5 - 10/31/2016 12:13 PM - Suraj Ravichandran

- Status changed from Unscreened to Screened

- Priority changed from No priority to Nice to have

- Target version set to 9.10.2

#6 - 11/17/2016 11:24 AM - Kris Moore

- Target version changed from 9.10.2 to 9.10.2-U1

#7 - 11/28/2016 11:13 AM - Suraj Ravichandran

- Related to Bug #18319: [Regression] Outdated Security Run Outputs added

#8 - 12/23/2016 06:00 AM - Kris Moore

- Target version changed from 9.10.2-U1 to 9.10.2-U2

#9 - 02/08/2017 10:21 AM - Kris Moore

- Target version changed from 9.10.2-U2 to 9.10.4

#10 - 04/19/2017 07:57 AM - Kris Moore

- Target version changed from 9.10.4 to 11.1

#11 - 04/19/2017 10:05 AM - Daniel Shaffer

Sorry, but is this really so unimportant that it won't be fixed until the next version? I realize it may not be a top priority, but I thought it was definitely a bug. If I were to try to look into fixing this myself (it would be my first time in this codebase), would one of those suggestions I made earlier be preferable, or is there something else I should look at?

#12 - 04/19/2017 01:04 PM - Suraj Ravichandran

@Daniel 9.10.3 got renamed to being called 11.0 and 9.10.4 went to 11.1 (so not so much a postponing issue as much as a versioning change).

Any changes you make and submit will be gladly looked at and reviwed.

#13 - 04/19/2017 03:46 PM - Daniel Shaffer

Oh okay, thanks for the information.

#14 - 08/22/2017 08:54 AM - Dru Lavigne

- Status changed from Screened to 46

- Assignee changed from Suraj Ravichandran to Kris Moore

Kris: is this still an issue given the related bug?

#15 - 08/22/2017 12:24 PM - Kris Moore

- Status changed from 46 to Unscreened

- Assignee changed from Kris Moore to William Grzybowski

Over to William, who can Load Balance it now.

#16 - 08/23/2017 04:12 AM - William Grzybowski

- Assignee changed from William Grzybowski to Vladimir Vinogradenko

Vladimir, can you please take a look at this? Thanks!

#17 - 08/27/2017 02:13 AM - Vladimir Vinogradenko

- Status changed from Unscreened to Screened

#18 - 08/31/2017 05:07 AM - Vladimir Vinogradenko

- Status changed from Screened to Needs Developer Review

- Assignee changed from Vladimir Vinogradenko to William Grzybowski

Cause auth.log to rollover either each day/week/month/year?

It is already being rotated every year as configured in /etc/newsyslog.conf

```
# logfilename          [owner:group]    mode count size when  flags [/pid_file] [sig_num]
/var/log/auth.log             600  7     100  @0101T JC
```

@0101T means «on January 1st». Rotation occurs between 00:00 and 01:00. If device was not powered on in that time interval (which I think is OK for SOHO NAS), next rotation will occur only next year (or when auth.log reaches size of 100 kilobytes).

> Start logging the year of the login error as well?

This may break a lot of other scripts depending on current syslog record format. Definitely not an option.

> Only count a report as coming from yesterday if there are no more days following it in the log?

This is much less intrusive approach. As bash performance won't be satisfying for required logic (will spawn a lot of egrep processes), I've implemented new periodic script with python.

#19 - 08/31/2017 05:38 AM - William Grzybowski

- Status changed from Needs Developer Review to Reviewed by Developer

- Assignee changed from William Grzybowski to Vladimir Vinogradenko

#20 - 08/31/2017 05:38 AM - Vladimir Vinogradenko

- Status changed from Reviewed by Developer to Ready For Release

#21 - 09/09/2017 10:54 AM - Dru Lavigne

- Subject changed from Daily Security Run Output includes old login failures to Skip old login failures in daily security run output

#22 - 09/26/2017 04:22 PM - Dru Lavigne

- Target version changed from 11.1 to 11.1-BETA1

#23 - 10/24/2017 04:48 AM - Dru Lavigne

- Status changed from Ready For Release to Resolved

#24 - 11/07/2017 11:17 AM - Rishabh Chauhan

- File authlogin1.png added

I accessed auth.log file and there were no entries prior to today.. It seems it refreshes everyday. Refer screenshot.

#25 - 11/08/2017 06:16 AM - Bonnie Follweiler

- Needs QA changed from Yes to No

- QA Status Test Passes FreeNAS added

- QA Status deleted (Not Tested)

#26 - 12/05/2017 05:47 AM - Dru Lavigne

- Has duplicate Bug #24090: Log from last year sent again in the same day current year added

Files

authlogin1.png	13.8 KB	11/07/2017	Rishabh Chauhan