rsyslog にてロギングされる時刻フォーマットを変更したい

著者が使用しているメインのLinuxディストリビューションはRockyLinux
シングルボードコンピューター(RaspberryPiやOrangePIなど)は、「Raspberry Pi OS」「Armbian」を使用している。
Armbianの最新OSを使用しだしたら、rsyslogの時刻フォーマットが変更されていた。
まあ、検証や調査等で他のディストリビューションを使用したりしていた時に、チラホラ見かけていたのだが。

(A) Armbian 24.2.1 bookworm で使用されているrsyslogの時刻フォーマット

2024-02-13T03:22:26.022354+00:00 orangepi5 kernel: [4.767558] Linux version 5.10.160-legacy-rk35xx (armbian@next) (aarch64-linux-gnu-gcc (Ubuntu 11.4.0-1ubuntu122.04) 11.4.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #1 SMP Fri Feb 2 07:51:33 UTC 2024
2024-02-13T03:22:26.022358+00:00 orangepi5 kernel: [4.778703] Machine model: Orange Pi 5
2024-02-13T03:22:26.022360+00:00 orangepi5 kernel: [4.778870] efi: UEFI not found.

(B) よく見る時刻フォーマット

May 12 06:00:48 rocky8 kernel: Linux version 4.18.0-513.18.1.el89.x8664 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc version 8.5.0 20210514 (Red Hat 8.5.0-20) (GCC)) #1 SMP Wed Feb 21 21:34:36 UTC 2024
May 12 06:00:48 rocky8 kernel: Command line: BOOTIMAGE=(hd0,gpt2)/vmlinuz-4.18.0-513.18.1.el89.x8664 root=UUID=bad16281-a882-42c0-aec0-d7e2d5e712d6 ro crashkernel=auto resume=UUID=4912a5e2-2ddd-4121-8164-a44ebf092b2b
May 12 06:00:48 rocky8 kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'

今回は(諸事情により)、時刻フォーマットを(A) から (B)に変更します

○ rsyslogでロギングされる全てのファイルの時刻フォーマットを変更する場合

rsyslog.conf に、

$ActionFileDefaultTemplate RSYSLOGSysklogdFileFormat

を追加してrsyslogを再起動する

○ 任意のログファイルのみ変更する

(例) /var/log/syslog に定義部分を変更
rsyslog.confにて、

.;auth,authpriv.none -/var/log/syslog
を
.;auth,authpriv.none -/var/log/syslog;RSYSLOGSysklogdFileFormat

に変更(赤文字を追記)して、rsyslogを再起動する

【補足】

rsyslogでは、出力フォーマットをカスタマイズできる機能がある。
自分で定義しても良いが、rsyslog本体に予め定義されている形式を使用した。
「RSYSLOG」で始まるテンプレート名である。
定義済みテンプレートの種類については、本家ドキュメントを参照して欲しい。
https://www.rsyslog.com/doc/configuration/templates.html

著者が参考にしたサイト
・ rsyslog のログフォーマットを変更する
https://tech-lab.sios.jp/archives/37409

【本番運用では】

後々の事を考えて、rsyslogで定義されているルールは変更せずに、ルールを追加する事になるだろう。
.;auth,authpriv.none -/var/log/syslog
.;auth,authpriv.none /var/log/syslogkanshi;RSYSLOGSysklogdFileFormat # この行を追加

logrotateの設定も忘れずに！
/etc/logrotate.d/kanshi

```
/var/log/syslogkanshi
{
  missingok
  sharedscripts
  postrotate
  /usr/bin/systemctl -s HUP kill rsyslog.service >/dev/null 2>&1 || true
  endscript
}
```

添付ファイル::

一意的なソリューション ID: #1051
製作者: n/a
最終更新: 2024-05-14 03:45