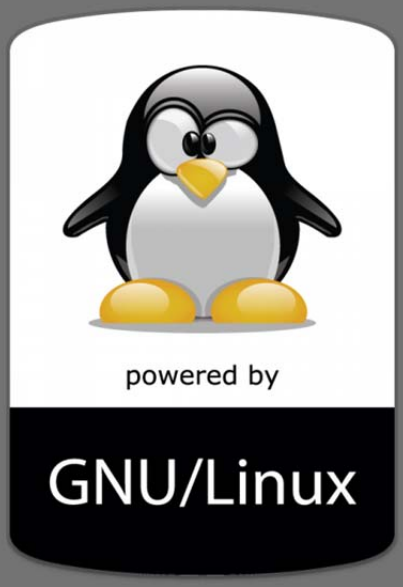
2015

# مدیریت Log ها با Syslog و Log rotate

نویسنده حسام الدین توحید




skywan13@chmail.ir


skywan13@chmail.ir
**نویسنده : حسام الدین توحید**

## مقدمه مولف :

آنچه پیش رو دارید ویرایش سوم مقاله مدیریت Log ها با Syslog و Log rotate است که به صورت رایگان و تحت لیسانس GNU GPLv3 به علاقه مندان لینوکس هدیه می گردد . در تهیه این مقاله از سر فصل های درسی گفته شده در دوره هایLPIc2 و RHCE و RHCSA استفاده شده ولازم می دانم از **مهندس مهدوی فر** به خاطر راهنمایی های مفیدشان و **مرکز آموزشهای پیشرفته دانشگاه شریف (لایتک)** تشکر کافی را داشته باشم. این مطالب با نگاهی کاربردی و بدون پرداختن به بحث های تئوریک و بر اساس توزیع CentOS گردآوری و عرضه شده است. امیدوارم مطالب ارائه شده بتواند باعث ارتقاء دانش فنی کاربران لینوکس و متخصصین IT شود. زکات علم نشر آن است.

موفق باشید

**حسام الدین توحید**

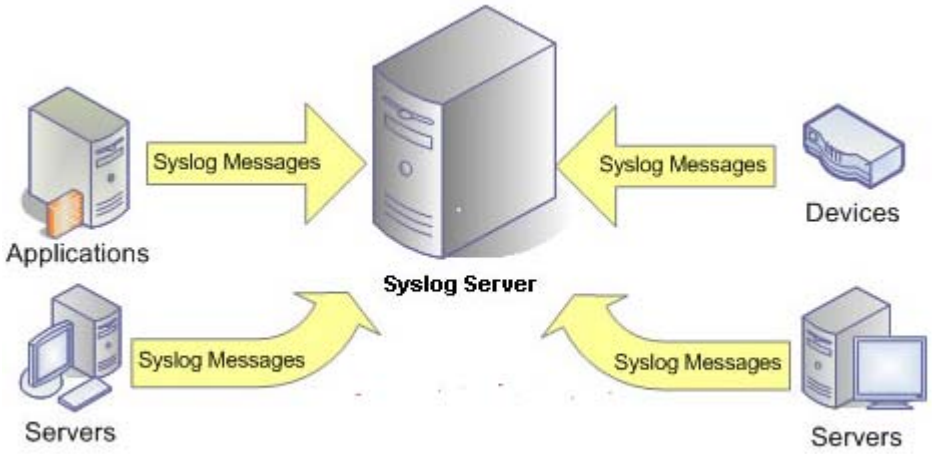
بهمن 1395

# فهرست


- پیکربندی و مدیریت لاگها با syslog 6
- نصب و راه اندازی سرویس syslog 6
- مبناهای کاری syslog 6
- تنظیم لاگ بر اساس Unix domain socket 9
- تنظیم لاگ بر اساس Internet socket 10
- فایل های مهم log 11
- ابزارهای گزارش گیری در CLI 12
- چرخش لاگها با Log rotate 13
- نصب و راه اندازی سرویس Log rotate 13
- مهمترین فایل های Log rotate 14
- بررسی /etc/logrotate.d/ 16


# پیکربندی و مدیریت لاگها با Syslog

در سیستم عامل لینوکس سرویس ها ، نرم افزار ها و خود هسته در هر لحظه رویداد هایی مانند خطاها و تغییر در روند سرویس و یا هر چیز دیگری را ، در غالب فایل هایی متنی ثبت می کنند که به این کار Logingیا ثبت رویداد گفته می‌شود. مدیران این فایل ها را دسته‌بندی کرده و در هنگام بروز مشکل و حوادث امنیتی آنها را بررسی می‌کنند. مستند کردن این فایل ها یکی از وظایفی است که مدیران شبکه در شرکت ها انجام می‌دهند. هنگامی که یک سرویس Start یا Stop می شود و یا هر تغییر و خطایی رخ می‌دهد حتی هنگامی که یک عمل با موفقیت انجام می‌شود یک پیام در فایل Log مرتبط با آن سرویس ثبت خواهد شد. syslog سرور بر روی هر دو پلتفرم ویندوز و لینوکس قابل راه اندازی است.




فایل های Log در مسیر دایرکتوری /var/log/ ذخیره می‌شوند و مرتبط با هر سرویس مانند sshd یا dhcpd یک فایل Logوجود دارد. لینوکس ردهت تا ورژن5 از ابزاری به نام syslogd که مخفف System Log Daemon است برای ثبت رویداد ها استفاده می‌کرد ولی از ورژن 6 به بعد از rsyslog برای این کار استفاده می‌کند. این برنامه با سرویس ها و نرم افزارهای در ارتباط بوده و آنها رویدادهای خود را به این ابزار می‌دهند. syslogd رویدادها را جمع‌آوری کرده و در فایل‌های Log خود آنها ثبت می‌کند.

فایل های Log فایل های متنی هستند و می توان با دستور های cat , less , vim, vi و دستور های tail, head آنها را مشاهده کرد اما پیشنهاد می‌شود از دستور های head , tail وless استفاده کنید. از ابزار های دیگر مرتبط با Log ها در لینوکس نرم افزار logwatch است که در بیشتر توزیع های لینوکسی وجود دارد و در دایرکتوری /etc/log.d/ و تحت فایل logwatch.conf قابل پیکربندی می باشد.

از اعمال مرتبط با Log ها، Log Rotate یا گردش Log است. وقتی که اندازه فایل های Log زیاد می شود بایستی از آنها یک پشتیبان تهیه کرد و یا اینکه دنباله Log کردن را دریک فایل جدید ادامه داد و فایل قدیمی را آرشیو کرد. این

اعمال بصورت خودکار و در غالبRotate کردن انجام می‌شود. پیکربندی عملیات Rotate به کنترل حجم و بازخوانی ساده تر فایل ها کمک می‌کند.

بهتر است که در هنگام پارتیشن‌بندی، یک پارتیشن مجزا برای دایرکتوری /var/log/ در نظر گرفته شود چونکه رشد اندازه فایل های Log بسیار بالاست و در نظر گرفتن پارتیشن مجزا خارج از دایرکتوری / از بروز مشکل جلوگیری می‌کند.

یکی دیگر از موضوعاتی که قابل بحث است ذخیره رویداد ها بصورت محلی و راه دور می‌باشد. محلی بودن ثبت رویداد کاملا واضح است و رویداد در خود آن ماشین ذخیره می‌شوند اما راه دور به این معنی است که یک سیستم را بعنوان Log Server انتخاب کرده و تمام ماشین ها رویدادهایشان را به این سرور ارسال کنند. توصیه می‌شود برای حفظ محرمانگی ، داده ها تحت ssh مبادله شوند و بهتر است که ثبت رویداد را هم بصورت محلی(یعنی در خود همان ماشین) و هم بصورت راه دور(یعنی در یک سرور مجزا) انجام شود.

Logging راه دور یک قابلیت امنیتی فوق‌العاده است. با قراردادن log هایتان در سیستم راه دور، می‌توانید از رخنه‌ها و نفوذهای امنیتی که به راحتی می‌توانند فایل های log را تغییر دهند، جلوگیری کنید.

دو سرویس یا دایمون به نامهای klogd و syslogd وجود دارد که کار گزارش گیری را کنترل می‌کنند. klogd فقط با پیغامهای کرنل و syslogd با دیگر پیغامهای سیستم مانند برنامه های کاربردی سر و کار دارد. شما می‌توانید رفتار این دو ابزار را با ویرایش فایل /etc/syslog.conf و فایل تغییر فیچرهای سرویس یعنی /etc/sysconfig/syslog پیکربندی کنید. همچنین می‌توانید اطلاعات بیشتر را از صفحه راهنمای /etc/syslog.conf کسب نمایید.

هر پیامی که توسط یک نرم‌افزار تولید می‌شود، اطلاعاتی در مورد محتوای پیغام ، مبدا و تولید کننده آن می‌دهد. فایل /etc/syslog.conf به شما امکان می‌دهد که هر گونه پردازشی را بر روی پیام ها تعیین کنید.

به طور موقت می‌توانید این اطلاعات را در فایل message انبار کنید. همچنین می‌توانید آنها را در یک فایل سفارشی ذخیره سازید یا آنها را به یک میزبان (host) راه دور، جایی که میزبان ، آنها را مطابق با پیکربندی syslogd خودش پردازش خواهد کرد، ارسال نمایید .

# نصب و راه اندازی سرویس Syslog

در بیشتر مواقع سرویس syslog در موقع نصب سیستم عامل نصب می شود و نیازی به نصب مجدد آن نیست. ولی جهت اطمینان از نصب بودن پکیج syslog با دستور زیر از سیستم query می گیریم :

**#rpm -qa | grep syslog**

در صورت نصب نبودن ، در سیستم های ردهت جهت نصب syslog از yum استفاده می کنیم :

**#yum –y install syslog**

بعد از نصب ، باید اطمینان حاصل کنیم که آیا پکیج syslog بر روی سیستم نصب شده است یا خیر لذا با دستور زیر از سیستم دوباره query می گیریم :

**#rpm -qa | grep syslog**

سپس با دستور زیر شاخه ها و مسیرهایی که فایل های این سرویس در آن ایجاد شده است را چک می کنیم :

**#rpm -ql syslog**

و با این دستور هم اطلاعات لازم را در مورد پکیج این سرویس به دست می‌آوریم :

**#rpm -qi syslog**

سپس با دستور chkconfig مشخص می کنیم در چه runlevel هایی فعال باشد :

**#chkconfig --level 35 syslog on**

و در انتها سرویس را reset می کنیم :

**#service syslog restart**

**نکته مهم :** در لینوکس های redhat base سری 6 به بعد به جای syslog از rsyslog استفاده می شود.

# مبناهای کاری Syslog

syslog بر دو مبنا کار می کند:

1. Unix domain socket
2. Internet socket

اگر syslog ، لاگهای را در سیستم local ذخیره کند بر مبنای Unix domain socket کار می کند و اگر لاگها از طریق پورت 514 udp به درون سیستم مشخص شده‌ای در شبکه منتقل شود در مد Internet socket فعالیت می کند.

فایل کانفیگ این سرویس در مسیر /etc/syslog.conf قرار دارد. در این فایل یکسری rule یا همان قوانین وجود دارد که از سه قسمت عمده زیر تشکیل شده است :

- **Facility**
- **Severity**
- **Where**

که در زیر هر کدام از آنها مختصرا توضیح داده می‌شود.

1)**Facility**: مشخص میکند از چه چیزهایی log برداری شود مثل:

**auth** - authentication (login) messages
**cron** - messages from the memory-resident scheduler
**daemon** - messages from resident daemons
**kern** - kernel messages
**lpr** - printer messages (used by JetDirect cards)
**mail** - messages from Sendmail
**user** - messages from user-initiated processes/apps
**local0-local7 -** user-defined (for cisco,servers,...)
**syslog** - messages from the syslog process itself

اگر بخواهیم log پروسه ای ، به صورت جداگانه در جایی به غیر از facility ثبت شود از **local** استفاده می‌کنیم.علاوه بر آنکه می توان مشخص کنیم لاگ ها به کجا بروند ، می‌توانید نوع پیغام هایی که برای سرور لاگ فرستاده می شود را توسط سطوح مختلف severity مشخص کنیم. این سطوح که به آنها level هم گفته می‌شود استاندارد بوده و براساس شماره و یا حروف اختصاری بکار برده می‌شوند.

2) **Severity**: درجه اهمیت ، یا level لاگ را مشخص می کند.

7 - Emergency (emerg)
6 - Alerts (alert) اخطار
5 - Critical (crit) شرایط بحرانی
4 - Errors (err) خطا
3 - Warnings (warn) هشدار
2 - Notification (notice) اطلاعیه
1 - Information (info) اطلاعات بیستر
0 - Debug (debug)

در سیستمهای Unix Base درجه اهمیت از صفر الی 7 متغییر است. بالاترین درجه اهمیت کمترین اطلاعات را به ما می‌دهد و بیشترین اطلاعات را debug اعلام می کند.

اگر تعریف کنیم لاگ برداری از debug شروع شود، سرور از debug به بالا، همه لاگ ها را ثبت می‌کند. یعنی از هر کجا تعریف کنیم از آن سطح و تمام سطوح بالاتر از آن لاگ برداری انجام می‌شود.

3) **where** : این قسمت مکان ذخیره سازی فایل های لاگ را مشخص می کند. در اینجا سه متغیر می تواند قرار گیرد :

- Tty
- File address
- /dev/console

اگر مشخص کنیم که لاگ بر روی /dev/console قرار بگیرد بر روی مانیتور تمام یوزرها قابل رویت می شود.



## سطوح Log ها

| رتبه بندی | واژه | شرح |
|---|---|---|
| 0 | emergencies | سیستم عملا غیرقابل استفاده است |
| 1 | alerts | باید سریعا عکس العمل نشان دهیم |
| 2 | critical | شرایط بحرانی می باشد |
| 3 | errors | خطائی در سیستم وجوددارد |
| 4 | warnings | اخطار... |
| 5 | notifications | شرایط عادی ولی مشکلاتی وجوددارد |
| 6 | informational | جهت اطلاع.... |
| 7 | debugging | پیام های مربوط به Debugging سیستم |

توضیح : جدول سطوح Log

# تنظیم لاگ بر اساس Unix domain socket

اگر بخواهیم لاگها در سیستم local ذخیره شوند از شیوه زیر برای نوشتن تنظیمات در فایل کانفیگ log بهره می‌بریم .

**facility.severity** **where+ log-file-name**

در ادامه برای درک بهتر مفهوم Unix domain socket چند مثال آورده شده است. در اینجا ستاره به معنی همه می‌باشد.

**مثال یک:**

*.info;mail.none;authpriv.none;cron.none /var/log/message

*: در اینجا به معنی همه facility ها می باشد.

info: آوردن این کلمه یعنی از info به بالا لاگ بگیرد.

none: اگر بخواهیم از سرویس و یا پروسه ای لاگ بردار نشود از کلمه none استفاده می‌کنیم.none به معنای منفی شدن است.

**مثال دو:**

Authpriv.* /var/log/secure
Mail.* /var/log/maillog
Cron.* /var/log/cron

ستاره در سه مثال قبل یعنی اینکه لاگ مربوطه تمام severity ها را شامل شود.

**مثال سه:**

*.emerg *

*. اول این خط یعنی تمام facility ها را شامل می‌شود و ستاره آخر مشخص می کند خروجی لاگ در tty , file , /dev/console نشان داده شود.

**مثال چهار:**

به طور پیش فرض لاگ های dhcp در مسیر /var/log/message/ ذخیره می‌شود. حال می‌خواهیم کاری کنیم لاگ های dhcp در مسیر /var/log/dhcp/ ذخیره گردد.

ابتدا وارد فایل کانفیگ dhcp شده و عبارت زیر را به آن اضافه می کنیم :

log-facility local2;

سپس فایل /etc/syslog.conf را باز کرده و مشخص می کنیم لاگهای مربوط به local2 درون چه فایل ذخیره شوند.

**#vi /etc/syslog.conf**

*.info;mail.none;authpriv.none;cron.none;local2.none **/var/log/message**
local2.* **/var/log/dhcp**

همانطور که از مثال ها مشخص است , می توان به چندین شکل syslog را جهت نگه داری پیام ها تنظیم کنیم .

می توانید با * تمامی severityها را مشخص کنید تا در یک فایل ذخیره شوند یا اینکه با مشخص کردن نام آن فقط، آن severity را ذخیره کنید. همچنین می توانیدseverity های مختلف را در فایل های مختلف ذخیره کنید. توصیه می شود که لاگ ها را بر اساس نیازتان در فایل های مجزا تقسیم بندی کرده تا در آینده آنالیز آنها راحت تر باشد.

# تنظیم لاگ بر اساس Internet Socket

برای استفاده از syslog به جهت دریافت لاگ از دستگاه ها وسرورهای دیگر، می‌بایست ویژگیUdp logging را در سیستمهای مورد نظر فعال کنیم تا ارسال لاگ در شبکه از طریق پورت 514 پروتکل udp و آدرس تنظیم شده انجام پذیرد.

ابتدا در سرور syslog ، وارد مسیر /etc/sysconfig شده و فایل syslog را edit می کنیم.

```
# vi /etc/sysconfig/syslog
SYSLOG_OPTIONS= “m 0  -r “
```

در اینجا ستاره به معنی همه می باشد.

r: برای فعال کردنremote UDP logging

m 0: برای حذف پیام هاMARK

X: برای غیر فعال کردنDNS lookup

برای آنکه مطمئن شویم که UDP logging فعال شده و سرور بر روی پورت 514 به حالت Listen رفته از دستور زیر استفاده می کنیم.

```
# service  syslog  restart
# netstat  -nulp | grep  514
udp    0    0.0.0.0:514    0.0.0.0:*
          8621/syslogd
```

حال برای اینکه سیستم های دیگر لاگ خود را به سرور ارسال کنند در سیستمهای ارسال کننده لاگ ، وارد فایل /etc/syslog.conf شده و طبق مثال زیر آدرس سروری که می خواهیم لاگها به آن ارسال شوند را وارد می کنیم.

```
# vi   /etc/syslog.conf
*.info;mail.none;authpriv.none;cron.none                @10.10.10.1
```

و در انتها سرویس را ریست می کنیم:

```
# service  syslog  restart
```

توضیح : در قسمت آدرس به جای وارد کردن یک مسیر local آدرس سرور syslog را وارد کنید.

# Log فایل های مهم

در توزیع CentOS و دیگر توزیع ها در زیر دایرکتوری /var/log/ فایلهای لاگ متعددی وجود دارد. بسیاری از این فایل ها مربوط به پروسه های سیستمی است و مواردی هم مربوط به نرم افزارهای است که بر روی سیستم نصب میشوند. در ادامه به مهمترین آنها اشاره می‌شود:

**message** : لاگ پیامهای (message logs) هسته سیستم می باشند. این فایل، شامل پیغامهای بوت و پیغامهای وضعیت و اجراهای سیستم می‌باشد. خطاهای IO ، خطاهای شبکه و دیگر خطاهای عمومی سیستم در این فایل گزارش می‌شوند. سایر اطلاعات از قبیل مواقعی که یک فرد، root می‌شود نیز در اینجا فهرست می گردد. اگر سرویسهایی مانند سرور DHCP اجرا شوند، فعالیتها را در فایلهای پیغام می توانید مشاهده کنید. فایل /var/log/messages/ معمولا اولین مکانی است که در مواقع به وجود آمدن مشکل می‌توانید به آن مراجعه نمائید.

**XFree86.0.log** : این log نتایج آخرین اجرای سرور Xfree86 Xwindow را نشان می‌دهد. اگر در بالا آمدن محیط گرافیکی دچار مشکل شدید، این فایل معمولا جوابهایی برای عوامل سوال برانگیز مشکل فراهم می‌آورد.

**auth.log**: لاگهای مربوط به احراض هویت در این فایل ذخیره می‌شود.

**kern.log** : این فایل حاوی اطلاعات و رویداد های کرنل سیستم عامل می‌باشد.

**cron.log** : این فایل حاوی اطلاعات مربوط به این سرویس cron است.

**mail.log** : اطلاعات و رویدادهای Mail Server ها و MTA هایی مانندsendmail در این فایل ثبت می‌شود.

**qmail** : در صورتی که qmail را نصب کرده باشید. رویدادهای این سرویس دهنده میل در این فایل قرار می گیرند.

**httpd** : این فایل مرتبط با وب سرور آپاچی است و در صورتی که httpd را نصب کرده باشید ، وجود دارد.

**boot.log** : این فایل مرتبط با اطلاعات و رویداد های فرایند بوت شدن سیستمی می‌باشد.

**mysqld.log** : این فایل مرتبط با پایگاه داده MySQL می‌باشد البته در صورتی که MySQL استفاده کنید.

**secure** : حوادث امنیتی سیستم در این فایل ثبت می‌شود.

**yum.log** : مختص سیستم های مبنتی بر RedHat و در ارتباط با دستور yum است.

خواندن و مشاهده این فایل ها و حتی استفاده از دستورهای خاصی مانند last نیاز به دسترسی کاربر ریشه دارد. یعنی یک کاربر عادی نمی‌تواند این فایل ها را تغییر دهد یا حتی خود مدیر هم شاید نتواند این فایل ها مانند wtmp را تغییر دهد چون اطلاعات ضروری در آنها ثبت شده است.

❋❋❋

# ابزارهای گزارش گیری در CLI

هر گونه ابزار متنی را می‌توان برای کار با فایلهای log به کار برد. با ابزار زیر می توان در محیط cli فایل های لاگ را خوانده یا تغییر و یا از روند اضافه شدن دیتا به آنها مطلع شد. در ادامه برخی از این ابزارهای مفید پرداخته خواهد شد:

## dmesg

برای مرور اجمالی log بوت در آخرین بار بوت شدن سیستم، می‌توانید از دستور dmesg استفاده کنید. خروجی این دستور، عموما متن طولانی است.

## tail

برخی اوقات می‌خواهید فقط با یک مرور اجمالی و کوتاه در فایل log فعالیتهای در حال وقوع را ببینید. tail برای نمایش آخرین خطوط یک فایل متنی طراحی شده است. با افزودن سوییچ -f ، دستور tail به نمایش خروجیهای جدیدی که ناشی از رخ دادن آخرین وقایع است، ادامه می‌دهد.

**#tail -f /var/log/messages**

دستور فوق، آخرین ۱۰ خط فایل /var/log/messages/ را نشان داده و سپس به نظارت در فایل و خروجی هر فعالیت جدید ادامه می دهد. جهت متوقف ساختن دستور فوق، می‌توان از Ctrl + C برای کنسل کردن این فرایند استفاده کرد.

## more

دستور more همان کاری را انجام می‌دهد که در نگارش DOS انجام می‌داد. می‌توان آن را به همراه اسم فایل و نیز برای پایپ کردن اطلاعات در صفحه نمایش استفاده کرد.

## less

دستور less نیز یک مشاهده گر متنی دیگر است که به ما امکان scroll در یک فایل و نیز جستجوی اطلاعات در آن را می‌دهد.

## logger

ممکن است بخواهید پیغامهای خودتان را در یک فایل log قرار دهید. کافی است پیغام log را به انتهای فایل متنی، ضمیمه (append)کنید. اما مجبور خواهید شد که اطلاعات گزارش را تکرار کنید.

همچنین باید کد خود را در صورت سفارشی بودن سیستم logging تغییر دهید . دستور logger امکان ارسال پیغامهای شما را به ابزار موجود برای logging می‌دهد. از این دستور در اسکریپتهایی برای تهیه پیغامهایی در مورد نحوه اجرا و خطاها استفاده می‌شود.

# چرخش لاگها با Log rotate

زمانی که سرور تراکنش دیتا بالا و یوزر استفاده کننده زیادی داشته باشد حجم فایلهای log به مرور می تواند خیلی بزرگ شود که این حجیم شدن فایلهای لاگ هم فضای سیستم را اشغال می‌کند و هم واکشی و خواندن آنها را با تاخیر همراه می‌سازد. لینوکس ابزاری برای چرخش این log ها در اختیار دارد که به صورت دوره ای لاگهای قدیمی را جابه جا کرده و می‌چرخاند. بنابراین اطلاعات log جاری شما با اطلاعات نامربوط قدیمی، ترکیب نمی‌شوند. با این کار حجم لاگها کمتر و مدیریت آنها بهتر می‌شود.

معمولا logrotate به طور خودکار بر اساس یک برنامه زمان بندی اجرا می‌شود اما به طور دستی نیز قابل تنظیم و اجراست. فایلهایی که در شاخه /var/log/ مشاهده می‌کنید با یک عدد تمام می‌شوند اینها آرشیوهای دوار (چرخشی) هستند. هنگامی که این سرویس اجرا می‌شود، logrotate نگارش جاری فایلهای log را گرفته و عدد یک را به انتهای نام فایل می‌افزاید. از آن به بعد، ترتیب دیگر فایلهای چرخش یافته به صورت "۲،" ، "۳،" و غیره خواهد بود. عدد بزرگتر بعد از نام فایل، نشان دهنده گزارشهای جدیدتر می‌باشد. رفتار خودکار logrotate را می‌توانید با ویرایش فایل /etc/logrotate.conf/ پیکربندی کنید.

# نصب و راه اندازی سرویس Log rotate

در بیشتر زمان ها logrotate در موقع نصب سیستم نصب می شود و شما نیازی به نصب مجدد ندارید. ولی جهت اطمینان از نصب بودن پکیج logrotate با دستور زیر ابتدا از سیستم یک query می گیریم :

**#rpm -qa | grep logrotate**

در صورت نصب نبودن ، در سیستم های ردهت جهت نصب logrotate از yum استفاده می کنیم :

**#yum –y install logrotate**

بعد از نصب ، جهت اطمینان دوباره از سیستم query می گیریم :

**#rpm -qa | grep logrotate**

سپس با دستور زیر شاخه ها و مسیرهایی که فایل های این سرویس در آن ایجاد شده است را چک می کنیم :

**#rpm -ql logrotate**

و با این دستور هم اطلاعات لازم را در مورد پکیج این سرویس به دست می آوریم :

**#rpm -qi logrotate**

سپس با دستور chkconfig مشخص می کنیم در چه runlevel هایی فعال باشد :

**# chkconfig --level 35 logrotate on**

**نکته مهم :** logrotate یک سرویس است ولی اسکریپت اجرایی ندارد و خودش فایل ها را چک نمی کند بلکه این کار را با cron کامل می کند.

# مهمترین فایل های Log rotate

بعد از نصب این سرویس، تعدادی مسیر و فایل به سیستم اضافه می‌شود .در ادامه سه عدد از مهتمرین آنها که کار تنظیم و پیکربندی این سرویس را انجام می‌دهند توضیح داده می‌شود:

**/etc/cron.daily/logrotate**
**/etc/logrotate.conf**
**/etc/logrotate.d**

## /etc/cron.daily/logrotate

این فایل ارتباط بین logrotate و سرویس cron را برقرار ساخته و به logrotate می گوید از چه مسیری فایل کانفیگش را بخواند.

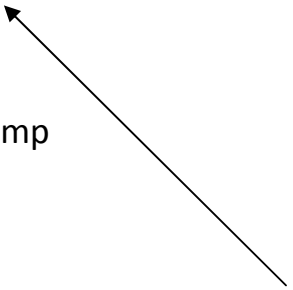
## /etc/logrotate.conf

فایل logrotate.conf فایل پیکربندی گلوبال این سرویس است. تنظیمات این فایل به همه اعمال می‌شود ولی کانفیگ لاگ هر سرویس به تنهایی بر کانفیگ گلوبال ارجحیت دارد. اگر در خود فایل گلوبال و در انتهای آن تنظیماتی برای یک سرویس نوشته شود (داخل کروشه) این بر تنظیمات اصلی ارجحیت اجرایی دارد. در ادامه نمونه‌ای از یک فایل پیکربندی آورده شده که بعضی از جزئیات آن شرح داده می‌شود:

**# vi /etc/logrotate.conf**

```
# see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# use date as a suffix of the rotated file
dateext
# uncomment this if you want your log files compressed
compress
```

```
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
   monthly
   create 0664 root utmp
      minsize 1M
   rotate 1
}
/var/log/btmp {
   missingok
:
monthly
   create 0600 root utmp
rotate 1
```



توضیح بعضی از قسمتهای فایل **logrotate.conf**

**# rotate log files weekly**
**weekly**

این گزینه زمان rotate شدن log فایل ها را مشخص می کند که سه مقدار daily,weekly,monthly می تواند داشته باشد.

**# keep 4 weeks worth of backlogs**
**rotate 4**

مقدار این خط مشخص می کند تعداد دفعات rotate چند مرتبه باشد.

**# RPM packages drop log rotation information into this directory**
**include /etc/logrotate.d**

این خط مشخص می کند اطلاعات log های rotate شده به چه مسیری اضافه شود.

**# uncomment this if you want your log files compressed**
**# compress**

این خط مشخص می کند که آیا لاگهای rotate شده در هنگام ذخیره شدن فشرده شوند. این آپشن به بقیه فایل‌های کانفیگ لاگ اعمال نمی‌شود مگر اینکه کانفیگ لاگ یک سرویسی را درون خود فایل اصلی پیکربندی logrotate بیاوریم.

**size 100k**

اگر بخواهیم به جای هفتگی یا تایمی به صورت حجمی عمل rotate انجام شود از این گزینه استفاده می کنیم.

# بررسی /etc/logrotate.d/

در زیر این دایرکتوری، فایل کانفیگ logrotate سرویس های مختلفی قرار دارد. تمام سرویس‌هایی که باید از عملکرد آنها لاگ جداگانه تهیه شود در این مسیر یک فایل پیکربندی دارند تا توسط logrotate عمل چرخش لاگ آنها انجام شود. اگر بخواهیم logهای سرویس های مورد نظر در این دایرکتوری فشرده شوند باید فیلد **compress** را درون هر کدام که می‌خواهیم اضافه کنیم.

یکی از مهمترین فایلهای کانفیگی که در این مسیر وجود دارد فایل لاگ سرویس httpd می‌باشد. جهت آشنایی با گزینه های دیگر کانفیگ logrotate ، این فایل را مورد بررسی قرار می‌دهیم .

**# vi /etc/logrotate.d/httpd.log**

```
/var/log/httpd/*log {
size 100k
compress
rotate 5
missingok
notifempty
sharedscripts
postrotate
Sbin/service httpd reload > /dev/null 2> /dev/null || true
endscript
}
```

**نکته مهم :** چون rotate این فایل درون خودش نیامده ، rotate آن را از فایل global سرویس logrotate خوانده و اجرا می‌کند. اگر زمان بندی rotate را در این فایل بیاوریم ارجحیت پیدا می‌کند به زمان بندیی که در فایل کانفیگ سرویس درج شده است.

در ادامه به تشریح بعضی از قسمتهای این فایل می‌پردازیم:

**/var/log/httpd/*log :** این خط مشخص کننده مسیر لاگ فایل ها می‌باشد.

**size :** عدد درج شده در مقابل این کلمه سایز لاگ فایل را مشخص می کند.

**rotate :** تعداد دفعاتی که لاگ فایل قبل از پاک شدن rotate می‌شود را نشان می‌دهد.

**missingok :** این کلمه بیان می‌کند اگر فایل لاگی موجود نبود ایراد نگیرد .

**notifempty :** معین می‌کند اگر فایل لاگ خالی بود آن را rotate نکند.

**postrotate :** این گزینه یک فایل لاگ جدید ساخته و سرویس را reload میکند.

**postscripts :** مشخص میکند بعد از اینکه rotate را انجام داد اسکریپت و یا دستور مورد نظر را انجام دهد.

**prescripts** : این کلمه مشخص می کند قبل از اینکه rotate را انجام بدهد اسکریپت و یا دستور مورد نظر را اجرا کند .

**dateext** : این گزینه خیلی مهم و کاربردی است چون باعث می‌شود در انتهای فایل لاگ تاریخ rotate شدن درج شود.

**Mail** : با درج این کلمه نتیجه به آدرس مشخص شده میل می‌شود.

**مثال :** فایل کانفیگ لاگی بنویسید که اگر حجم فایل مشخصی به 300 بایت رسید آن را rotate کرده و نتیجه را میل و در انتها به جای عدد در نام فایل ها تاریخ را درج کند.

ابتدا با دستور dd چند فایل با حجم های متفاوت ایجاد می کنیم.

```
# mkdir  /root/logs
# dd   if=/dev/zero   of=/root/logs/test.log  bs=300  count=1
```

سپس یک فایل کانفیگ می نویسیم تا لاگ این فایل را rotate کند.

```
# vi  /etc/logrotate.d/test
/root/logs/*.log  {
size 100k
compress
rotate 5
mail  root@localhost
dateext
}
```

سپس با دستور زیر آن را rotate می کنیم :

```
# logrotate   /etc/logrotate.conf
```

**نکته مهم :**

در مسیر های /var/log/ و /var/run/ دو فایل به نام های wtmp و utmp وجود دارد .

```
/var/log/wtmp
/var/run/utmp
```

این فایل ها باینری هستند و به سادگی خوانده نمی شوند.

wtmp فایل لاگ History Call سیستم است و درون آن اتفاقاتی مثل crash کردن سیستم ، یا اینکه چه یوزری از چه pts ای لاگین کرده است ، ثبت می شود.

utmp هم برای لاگ کردن لاگین های موفق و نا موفق به کار می رود ولی History Call نیست.

دستور last آخرین اطلاعات سیستم را به صورت History Call نمایش می دهد و با دستور lastb می توان Bad login های سیستم را مشاهده کرد.