

**108 Serviços essenciais do sistema**  
**108.1 Manutenção da data e hora do sistema**  
**Lição 1**

**Mantendo a hora do sistema**

**Real Time Clock, RTC, CMOS clock, hardware clock ou relógio da máquina** - mantido pela bateria da placa mãe, e conta o tempo mesmo enquanto o sistema está desligado

**System clock, kernel clock, software clock ou relógio do sistema** - Esse relógio é por software que conta o tempo baseado nas interrupções do processador. Ele precisa ser inicializado pelo RTC durante a carga do sistema. É atualizado pelo sistema operacional

Pode ocorrer uma flutuação entre a hora da máquina e a hora do sistema, pode-se fazer esse ajuste com o protocolo ntp.

**Relógio do sistema - date - mostrar ou definir a hora e data do sistema**

date - mostra data e hora. qui 27 mai 2021 10:53:38 -03

date -R - mostra as informações no formato de email. Thu, 27 May 2021 10:53:03 -0300

date -u - exibe hora UTC atual

date -I - mostra somente data

date --rfc-3339

date --debug

**Configurar data e hora com date - muda relógio do sistema**

date --set="11 Nov 2011 11:11:11" ou date -s "mm/dd/yyyy"

date +%Y%m%d -s "20111125"

date +%T -s "13:11:00"

date --date=' ' = definir tempo baseado no tempo do Unix

**Relógio do hardware - RTC - hwclock**

**hwclock -r / --show** - exibe a hora mantida no relógio de tempo. Parâmetro: --verbose

**hwclock --systohc ou hwclock -w** - Configura o relógio do hardware a partir do relógio do sistema (significa "relógio do sistema para relógio do hardware")

**hwclock --hctosys ou hwclock -s** - Configura o relógio do sistema a partir do relógio do hardware (relógio do hardware para relógio do sistema)

**hwclock --set --date "mm/dd/yyyy 11:15:19"** - Configurar data e hora - muda relógio do hardware

**Comando timedatectl** - retorna as informações de date, RTC e status do serviço NTP

- **Mudar time zone**

timedatectl list-timezones

timedatectl set-timezone "*Time zone escolhido*" - mudar time zone

- **Configurar data e hora - muda relógio do sistema**

timedatectl set-time HH:MM:SS - mudar a hora

timedatectl set-time "YY-MM-DD HH:mm:ss" - mudar a dia e hora

- **Habilitar/desabilitar NTP**

timedatectl set-ntp true/false - habilita/desativa sincronização automática da hora

## Lição 2

### Network Time Protocol (NTP)

**Deslocamento (offset)** - Refere-se à diferença absoluta entre a hora do sistema e a hora NTP

**Salto (step)** - Se o deslocamento de tempo entre o provedor NTP e um consumidor for maior que 128ms, o NTP executará uma única alteração significativa na hora do sistema

**Ajuste Gradativo (slew)** - Refere-se às alterações feitas na hora do sistema quando o deslocamento entre a hora do sistema e o NTP é menor que 128ms

**Relógio insano** - Se o deslocamento entre a hora do sistema e a hora NTP for maior que 17 minutos, o tempo do sistema é considerado insano e o daemon NTP não introduzirá nenhuma alteração no relógio do sistema. Será preciso tomar medidas especiais para trazer a hora do sistema até menos de 17 minutos da hora correta.

**Escorregamento ou deslizamento (drift)** - Refere-se ao fenômeno em que dois relógios ficam fora de sincronia com o tempo

**Variação (jitter)** - A variação refere-se à quantidade de escorregamento desde a última vez em que um relógio foi consultado.

**Estrato** - A distância de um relógio de referência, em passos ou saltos. Pode ser de 1 até 16

NTP - a hora do sistema é regularmente comparada à hora da rede. É necessário ter um daemon rodando, o **ntpd**.

#### Configurações do NTP.

Arquivo **/etc/ntp.conf** - contém informações de configuração sobre como o sistema se sincroniza ao tempo da rede

Os servidores NTP usados serão especificados em uma seção como esta:

```
pool 0.ubuntu.pool.ntp.org iburst
pool 1.ubuntu.pool.ntp.org iburst
pool 2.ubuntu.pool.ntp.org iburst
pool 3.ubuntu.pool.ntp.org iburst
```

Sintaxe para adicionar servidores NTP é assim:

server (IP Address)

server server.url.localhost

### Comandos:

**ntpd** - atualizar hora e data do sistema de acordo com os servidores

-g - iniciar o ntpd em um sistema com relógio errado além do limite de pânico

-n - ntpd rodará em foreground

-q - ntpd finaliza após ajustar a hora uma vez

**ntpdate <address>** - realizar uma sincronização inicial única (em caso que o deslocamento for maior que 17 min). Similar a **ntpd**. É necessário parar o serviço ntp antes de realizar esse ajuste. Ex: ntpdate pool.ntp.org

**ntpq** - utilitário para monitorar o status do ntp. Programa de consulta NTP padrão. Sintaxe: ntpq [opções] host

ntpq -p - consultar o servidor em busca de uma lista de peers (máquinas possíveis para fazer o sincronismo)

ntpq -n - substitui as URLs (hosts) por endereços IP

-i - entrar no modo interativo

## Chrony

É outra forma de implementar o NTP. **chronyd** é o daemon chrony e **chronyc** é a interface de linha de comando

**Iniciar serviço chrony** - systemctl start chronyd

**Arquivo de configuração** - /etc/chrony.conf ou /etc/chrony/chrony.conf

### Comandos

chronyc - abre menu interativo do chrony, sendo possível executar alguns comandos:

- makestep
- sources
- tracking

chronyc tracking - fornece informações sobre o NTP e a hora do sistema (UTC)

chronyc ntpdata - ver informações sobre as últimas atualizações válidas do NTP

chronyc sources - retorna informações sobre os servidores/provedores NTP usados para sincronizar a hora

chronyc makestep - realiza uma atualização manual única do NTP

## 108.2 Logs do sistema

Arquivos em que todos os eventos do sistema e da rede são registrados em ordem cronológica a partir do momento em que o sistema é inicializado (tentativas de autenticação malsucedidas, erros de programas e serviços, hosts bloqueados pelo firewall, etc\_

Os logs tradicionalmente são tratados por três serviços dedicados principais: syslog, syslog-ng (syslog nova geração) e **rsyslog** (“o sistema mais veloz para processamento de log”)

**Arquivo de configuração rsyslog** - **/etc/rsyslog.conf** e/ou o diretório **/etc/rsyslog.d/**

Os logs costumam ser encontrados em **/var/log**

Alguns serviços cuidam de seus próprios logs.

Podem ser classificados em logs do sistema e logs de serviços ou programas.

**Ler logs:** less, more, zless, zmore, tail, head, grep

/var/log/wtmp - who

/var/log/btmp - utmpdump ou lasat -f

/var/log/faillog - faillog -a

var/log/lastlog - lastlog

O rsyslogd recebe as informações relevantes de arquivos especiais (sockets e buffers de memória) antes de processá-las.

### **Recursos, prioridades e ações**

Arquivo /etc/rsyslog.conf - MODULES, GLOBAL DIRECTIVES e RULES

MODULES inclui suporte modular para registro de eventos, capacidade de mensagem e recepção de log UDP/TCP

GLOBAL DIRECTIVES permite configurar uma série de coisas, como logs e permissões de diretório de log

RULES é onde entram os recursos, prioridades e ações.

Cada mensagem de log recebe um número de recurso (facility - 0 a 23) e uma palavra-chave, ambos associados ao subsistema interno do Linux que produz a mensagem. Além disso, cada mensagem recebe um nível de prioridade (0 a 7)

### **Algumas Facilidades do rsyslog - de onde as mensagens vem**

**auth** - mensagens de segurança/autorização

**authpriv** - mensagens de segurança/autorização

**cron**

**daemon** - outros daemons do sistema que não possuem facilidades específicas

**kern** - mensagens do kernel

**lpr** - subsistema de impressão

**mail**

### Níveis de prioridade

debug (7)

info (6)

notice (5)

warning (4)

err (3)

crit (2)

alert (1)

emerg (0)

### Ações do rsyslog

**Arquivo** - grava em arquivo especificando o caminho completo

**PIPE** - mensagens para outro programa

**Terminal e console** - especifica uma tela local do computador para envio de mensagens

**Computador Remoto** - envia as mensagens para uma máquina remota, com @ seguido do nome do host

**Usuário** - nome do usuário que receberá a mensagem

O formato das regras (RULES) é o seguinte: **<facility>.<priority> <action>**

Ex:

- mail.alert /var/log/mail.urgent
- \*.\*;cron.none;ntp.none /var/log/allmessages
- mail.\* @@192.168.1.88:514
- \*.warning -/var/log/warnings

Comando **logger**: prático para scripts do shell ou para testes. Anexa todas as as mensagens recebidas a /var/log/syslog. Qualquer usuário pode inserir suas próprias mensagens no log do sistema manualmente com o utilitário logger.

Ex: logger this comment goes into "/var/log/syslog". -t - adiciona uma etiqueta a mensagem

### O mecanismo de rotação do log - logrotate

Os logs são rotacionados regularmente, o que serve a dois propósitos principais:

- Evitar que arquivos de log antigos usem mais espaço em disco do que o necessário.
- Manter os registros em um tamanho gerenciável para facilitar a consulta.

O utilitário responsável pela rotação de log é o logrotate.

O logrotate é executado diariamente como um processo automatizado ou cron job por meio do script **/etc/cron.daily/logrotate**.

Ele consulta o arquivo de configuração **/etc/logrotate.conf**, que define os passos a serem feitos, este arquivo inclui algumas opções globais e é bem comentado; cada opção é apresentada por uma breve explicação de sua finalidade.

Também o diretório **/etc/logrotate.d**, que contém opções de conf específicas de alguns programas.

### **Buffer de anel do kernel**

Comando **dmesg**: ver as mensagens. É uma estrutura de dados de tamanho fixo e, portanto, à medida que novas mensagens são gravadas, as mais antigas vão desaparecendo.

**Após análise da documentação verificamos que vc mandou o DAE e o pagamento que foi utilizado, tem que enviar o DAE nº 18-213207633/86, com o respectivo pagamento, a restituição tem que ser feita com esse DAE que não foi utilizado. Prazo para regularização de 10 dias.**

## **Lição 2**

### **Journaling**

Com a adoção geral do systemd por todas as principais distribuições, o daemon de diário (systemd-journald) tornou-se o serviço de log padrão.

Armazena as próprias mensagens que o sistema produz, o systemd mantém um sistema de log próprio chamado de journal. É mantido pelo daemon journald e centraliza mensagens do kernel, initrd, serviços, etc

**systemd-journald** é o serviço do sistema que se encarrega de receber as informações de log de uma variedade de fontes: mensagens do kernel, mensagens do sistema simples e estruturadas, saída padrão e erro padrão dos serviços, bem como registros de auditoria do subsistema de auditoria do kernel

### **Configuração do journaling - /etc/systemd/journald.conf**

**/run/log/journal**

Pode-se ter arquivos de configuração .conf em **/etc/systemd/journald.conf.d/**

**systemctl start,stop,status, restart systemd-journald**

O diário não é um arquivo de texto simples, mas sim binário. Usa-se o comando **journalctl** para ler as mensagens.

Comando **journalctl** - ver as mensagens de journal

Parâmetros:

- r - mostra do fim para o começo, ordem inversa
- f - imprime as mensagens mais recentes do diário e continua a imprimir as novas mensagens conforme são anexadas ao diário — semelhante a tail -f (mostra últimas informações de forma dinâmica)
- e - mostra últimas informações do journal
- n <value>, --lines=<value> - mostra as linhas mais recentes, de acordo com value (padrão 10)
- k (--dmesg) - mostra mensagens do kernel desde o boot
- x - mostra somente o texto das mensagens
- o - exportar mensagens

### **Navegando e pesquisando no diário**

< > - início e fim do diário

/ pesquisa algo depois

? - pesquisa algo antes

N - Ir para próxima correspondência

Shift N - Ir para correspondência anterior

Mandar mensagem para o log do sistema. Ex: echo "Olá mundo" | systemd-cat

### **Filtrando os dados do diário**

#### **Número de inicialização**

- list-boots - lista boots disponíveis (0 refere-se ao boot atual, -1 ao anterior, -2 ao anterior ao anterior)
- b --boot - especificar número do id do boot específico para ver as mensagens

#### **Intervalo de tempo**

--since --until AAAA-MM-DD HH:MM:SS - ver mensagens registrar no período de tempo. Ex

- journalctl --since "19:00:00" --until "19:01:00"
- journalctl --since "2 minutes ago/-2 minutes"
- minutes, yesterday, today, tomorrow, now

#### **Unidade**

-u - mostra mensagens sobre uma unidade específica.

#### **Programa**

/path/to/executable - mostra mensagem do executável

## Prioridade

-p - filtrar por prioridade. Ex: journalctl -b -0 -p err - mostra mensagens com prioridade error ou acima

## Campos

<field-name>=<value>

\_**<field-name>**<value>

Ex: **journalctl**

- PRIORITY=3
- SYSLOG\_FACILITY=1
- \_PID=1
- \_ID=1001
- \_UID=0
- \_BOOT\_ID
- \_TRANSPORT

É possível somar campos

## Entradas manuais no diário: systemd-cat

Semelhante ao logger. Possível mandar stdin, stdout, stderr para o diário

Ex:

- Somente digitar systemd-cat. Pressionar ctrl + c no final
- echo "And so does this line." | systemd-cat
- systemd-cat echo "And so does this line too."
- systemd-cat -p emerg echo "This is not a real emergency."

## Armazenamento persistente do diário

- Desativar totalmente registro em diário
- Mantê-lo na memória, torna volátil (remove a cada reinicialização) usa diretório **/run/log/journal**
- Torná-lo persistente no disco - **/var/log/journal**

O comportamento padrão é o seguinte: se **/var/log/journal/** não existir, os logs serão salvos de forma volátil em um diretório em **/run/log/journal/** e — portanto — perdidos na reinicialização.

Configurações em **/etc/systemd/journald.conf**

**Storage:** volatile, persistent, auto, none

Tamanho do diário: journalctl --disk-usage

Os logs do systemd têm como padrão um máximo de 10% do tamanho do sistema de arquivos onde estão armazenados.

Por exemplo, em um sistema de arquivos de 1 GB, eles não ocuparão mais do que 100 MB. Assim que esse limite for atingido, os logs antigos começarão a desaparecer para se aproximar desse valor.



Pode-se ajustar esse limite em `/etc/systemd/journald.conf` (`SystemMaxUse`, `RuntimeMaxUse`), desde que não ultrapasse 4GiB

### **Limpando o diário**

Limpar manualmente os arquivos de diário arquivados;

`journalctl --vacuum-time=`

- sufixos: s, m, h, d, months, weeks (w), years (y)

`journalctl --vacuum-size=`

- K, M, G ou T

`journalctl --vacuum-files=` - cuida para que não restem mais arquivos de diário arquivados do que o número especificado

- Opção **--rotate** remove até diários ativos

### 108.3 Noções básicas do Mail Transfer Agent (MTA)

**Mail User Agent:** é um aplicativo que o usuário utiliza para enviar, receber, escrever e ler emails como o outlook, thunderbird, etc

**SMTP:** É um protocolo para envio de mensagens entre os leitores de email e o servidor de email MTA e entre os servidores de email

**Mail transfer agent (MTA):** software que recebe emails dos leitores e também envia email para outros MTA's quando a mensagem não é local

**MX** - Tipo de registro no DNS que indica qual é o servidor MTA responsável por receber os email de um determinado domínio

#### MTA

**sendmail** - era um agente de transferência de e-mail muito popular na internet. Devido a sua complexidade de configuração deixou de ser utilizado.

**Exim** - MTA de configuração simples. Geralmente é encontrado como MTA padrão de versões antigas do Debian.

#### Qmail

**Postfix** - Utilizado na maioria das distribuições devido a sua facilidade de configuração. Suporta diversos domínios, criptografia, proteção contra spam, etc.

#### Diretórios e arquivos importantes

**/var/spool/mail** - onde fica as caixas postais de cada usuário

**/var/spool/mqueue** - fila de mensagens que estão para serem enviadas (em processamento)

**/etc/aliases** - encaminhamento de mensagens (para quem as mensagens de certo usuário serão mandadas). Executar comandos **newaliases**, **sendmail -bi** ou **sendmail -I** para atualizar banco de dados.

Formato do arquivo: name: value1, value2

Entrega personalizada: mecanismo de roteamento de email fornecido pelo arquivo

#### **/etc/aliases**

**~/forward** - Arquivo que pode ser criado para redirecionar as mensagens

#### Comandos

- **sendmail** - enviar mensagens
- **mailq** ou **sendmail -bp** - ver mensagens não enviadas (queue)
- **mail** - Se um endereço de email for fornecido como argumento para o comando mail, ele entrará no modo de envio; caso contrário, entrará no modo normal (leitura).
  - **Modo leitura:**
  - **print 1** - exibir o conteúdo da mensagem número 1
  - **print** ou **p**, **delete** ou **d**, **reply** ou **r**
  - **quit** ou **q** sai do programa
  - **Modo de envio:**

- Ex: `mail -s "Maintenance fail" henry@lab3.campus <<<"The maintenance script failed at `date`"`
  - `-s` - assunto do email
  - `-a` - enviar um anexo

## 108.4 Gerenciamento de impressoras e impressão

Pacote CUPS (Common Unix Printing System) foi projetado para ser um sistema de impressão robusto e modular, com suporte a impressão local e remota.

Arquivos de configuração:

/etc/cups/cupsd.conf - contém as configurações do próprio serviço CUPS

/etc/printcap

/etc/cups/printers.conf - contém as impressoras configuradas para serem usadas, bem como a fila de impressão

/etc/cups/ppd/

Arquivos de log em /var/log/cups/

Comando **lpstat**

**Parâmetros:**

- a - mostra todas as impressoras
- d - mostra impressora padrão
- p - ver impressoras disponíveis
- t - ver condições das impressoras
- o - ver fila de impressão

**Comandos**

- **lpadmin** - adicionar/remover impressoras
  - -p NAME - especificar impressora
  - -u allow:user,user,user - aceitar trabalhos somente destes usuários
  - -u deny:user,@group - negar trabalhos para este usuário e grupo
  - -x NAME - remover uma impressora
- **lpoptions -d [nameimpr]** - definir impressora padrão
- **lpr** - imprimir na impressora padrão
  - -P - especificar impressora
  - -o - adicionar opções: landscape, two-sided-long-edge, two-sided-short-edge, media, collate, page-ranges, fit-to-page, outputorder
  - **lpr-#N** - imprimir certo número de cópias
- **lpinfo** - utilizado para exibir os dispositivos e drivers suportados pela base interna do cups
  - -m - mostra todos os drivers suportados.
  - -v - mostra todos os dispositivos e protocolos suportados no momento
- **lp** - imprimir
  - -d - especificar impressora
- **lpq** - ver lista de impressão
  - -a - mostra fila de todas as impressoras
- **lprm N** - cancelar impressão do trabalho de número N
  - - - excluir todos os trabalhos da fila de impressão

- `cancel [nameimpr][N°]` - alternativa ao comando `lprm`
- `lpmove [nameimpr]-[N°trab] [novaimpr]` - mover trabalho de uma para outra
- `cupsctl` - ver configurações habilitadas
- `cupsreject` - rejeitar trabalhos em certa impressora
- `cupsaccept` - habilitar impressões em certa impressora
- `cupsdisable` - desabilita impressora temporariamente, mas aceita novos jobs
- `cupsenable` - habilitar impressora