Sistemas Operacionais
Linux para Concursos II

Gustavo Pinto Vilar

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Gustavo Vilar – Mini CV

- PCF / DPF – Perito Criminal Federal
- Pós-Graduado em Docência do Ensino Superior – UFRJ
- Graduado em Ciência da Computação e Processamento de Dados – ASPER/PB
- Aprovações: PRF 2002, PPF-PF 2004, PCF-PF 2004, MPU 2010, ABIN 2010, PCF-PF 2013

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Gustavo Vilar

- Contatos:

http://www.itnerante.com.br/profile/GustavoPintoVilar
http://www.provasdeti.com.br/index.php/por-professor/gustavo-vilar.html

gustavopintovilar@gmail.com
p3r1t0f3d3r4l@yahoo.com.br

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

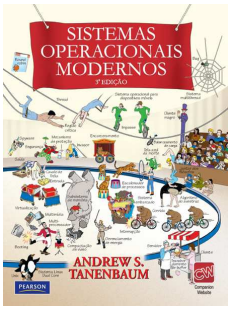
Escopo

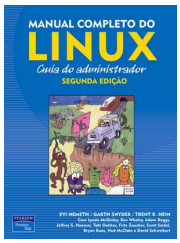
- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais frequentes.
- Abordar as metodologias de resolução de questões das principais bancas

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Bibliografia





Google

cespeUnB

Fundação Carlos Chagas

FUNDAÇÃO CESGRANRIO

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Linux para Concursos – Carga Horária

- **13 vídeo aulas (04h15m13s / 00h19m38s)**
  - Introdução
  - Hierarquia de Sistemas de Arquivos
  - Principais Diretórios
  - Comandos de Terminal
  - Comandos de atividades e logins
  - Arquivos de Configuração
  - Fundamentos do registro de atividades
  - Syslog, Logrotate, Logger (teoria e prática)
  - Duas baterias de questões de aprendizagem

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Sistemas Operacionais

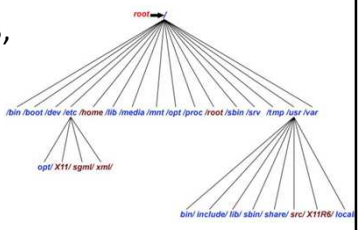
FHS - Filesystem Hierarchy Standard

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

FHS - Filesystem Hierarchy Standard

- Virtual Filesystem switch
  - Camada de abstração do kernel
  - Fica entre o S.O e Sistema de arquivo
  - Os sistemas de arquivos registrados no VFS podem ser classificados em 3 grupos
    - dispositivos de blocos (Ext2, Ext3, Ext4, Reiserfs, XFS, VFAT)
    - associados a rede (NFS, SMB)
    - dispositivos especiais (procfs, tempfs)
      - Não estão no disco nem na rede

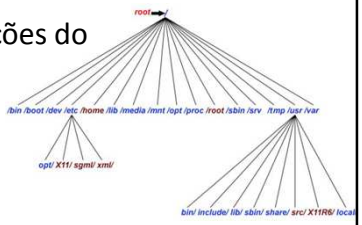


ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

FHS - Filesystem Hierarchy Standard

- Interface comum para operações com sistemas de arquivos
  - tem um open que usa o open dos sistemas de arquivos
  - Cada sistema suportado deve fornecer as funções para seu funcionamento
  - VFS se encarrega de apontar as funções do kernel para o sistema suportado
- Usuário não mexe com VFS, núcleo mexe.



ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Nomenclatura, extensões e limitações

- Todos caracteres são válidos, exceto NULL
- "." vale por um caractere
- Tamanho e quantidade de extensões é livre
- Diretórios são armazenados como arquivos
  - Hierárquico

Esquema de partição

- Bloco 0 - Não usado pelo Unix, contém o boot
- Bloco 1 - Superbloco, informações sobre o sistema de arquivos, i-nodes, etc...
  - Sua perda implica na ineligibilidade do sistema de arquivos
- i-nodes
  - 128 bytes
  - unix trad 64 bytes
  - Descrevem exatamente um arquivo

Esquema de partição

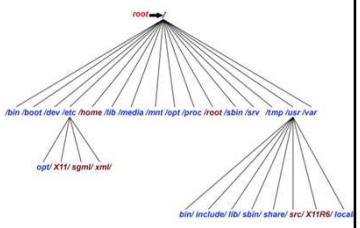
- Blocos de dados
  - Arquivos e diretórios são aqui armazenados
- fdisk / cfdisk
  - utilitários para criação de partições
- mkfs
  - formata a partição criada com o sistema de arquivos desejado

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

FHS - Árvore de diretório

- Windows atribui letras
- Unix não usa essa notação de letras, usa barras: /
- Mesma notação usada na internet, ou seja, barras inclinadas para direita: http://www.provasdeti.com.br/por-professor/col2/gustavo-vilar.html? SID=U
- Nem todos diretórios são obrigatórios



ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

/proc

- Montado na memória durante a inicialização
- Acesso a dados do kernel
  - Processos
  - discos
  - utilização de memória
- Usada pela forense para coleta de vestígios
- Não se consegue editar nada
  - Apesar de não ser somente de leitura
- Cada processo possui um subdiretório dentro do /proc
  - Ex: /proc/PID

/proc/sys

- Não existe fisicamente
- Caindo em desuso
- Fica dentro de /proc
- Estruturas para mudança do comportamento do kernel

/etc

- Configurações do sistema
- Ainda é "uma grande bagunça"
- Arquivos diversos
- Concentra os arquivos de configuração do sistema, substituindo de certa forma o registro do Windows

/var

- Dados variáveis
- Gravados durante execução do software
- Ex: Arquivos de log

/dev

- Acesso a dispositivos
- Serve para indicar o dispositivo físico
  - Ponteiro
- Não disponibiliza o conteúdo do drive
  - Contém os drivers de dispositivos (device drivers)

/dev

- udev
  - usado atualmente para montar o /dev
  - lê os dados do /sys
  - reage a mudanças de forma automática

/tmpfs

- É um sistema de arquivos
- Não existe fisicamente
- Situa-se na RAM
- Região de pastas e arquivos temporários (daquela sessão) na RAM

/tmpfs

- Conteúdo volátil
- Forma rápida de acelerar processos com arquivos
  - Acesso a disco é lento
  - Acesso à RAM é mais rápido
- Velocidade importante, persistência não

/home

- home dos usuários
- Aqui fica a lixeira /thrash (por usuário)
- Acomoda as estruturas individuais de cada usuário por ocasião da criação dos mesmos.
- /root: home do root

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

/usr

- Unix System Resources
- Armazena os executáveis e bibliotecas da maioria dos programas instalados no sistema, e que são usados pelos usuários
- Pasta padrão para código fonte de programas
- /usr/bin" (bin de binário), por exemplo, armazena cerca de 2.000 programas e atalhos para programas numa instalação típica
- /usr/lib", onde ficam armazenadas bibliotecas usadas pelos programas
- Não confundir com /home

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

/bin e /sbin

- Binários
- Armazena os executáveis de alguns comandos básicos do sistema
- /sbin = /bin do root

Outros diretórios

- /lib
  - Bibliotecas: "System32“
  - Mesmo em ambiente 64 bits, onde existe a pasta /lib64, os módulos do kernel de 64 bits ficam em lib, e não em lib64
- /opt
  - forma de melhor organizar a instalação de programas extras
- /boot
  - Armazena o Kernel e alguns arquivos usados pelo Lilo / grub
- /mnt
  - Servir de ponto de montagem
  - Montagem temporária
- /skel
  - Armazena arquivos que serão criados em cada /home por ocasião de criação de contas
- /media
  - montagem de mídia removível

Sistemas Operacionais

Principais Comandos de Terminal

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

aluno@provasdeti:~$ CONSIDERAÇÕES INICIAIS

- Case sentivive
  - Ls <> LS <> lS <> ls
- Tab Completion
- Aceita os curinhas * e ?

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

aluno@provasdeti:~$ ls (list)

- ls -l
  - Mostra os arquivos e diretórios em nome longo + data de modificação
- ls – lu
  - Data de acesso
- ls –a
  - Mostra os arquivos que começam com um ".", ou seja, ocultos

aluno@provasdeti:~$ cd (change dir)

- Muda o diretório corrente
- Se usar “/” no início da hierarquia, o diretório base é a raiz
- Se não usar “/”, toma-se como base o diretório corrente
- cd sem parâmetros = home do usuário
- cd ~ = cd = home do usuário
- OBS: Não existe “cd..” como no windows

aluno@provasdeti:~$ mkdir (make dir), rmdir (remove dir)

- Criar e e excluir diretórios respectivamente
- A remoção do diretório pelo comando rmdir só ocorre se o diretório estiver vazio.

aluno@provasdeti:~$ rm(remove dir ou arquivos)

- Remover diretórios ou arquivos
- Em caso de diretórios, é possível realizar a exclusão de diretórios não vazios: -r -R

aluno@provasdeti:~$ tail (cauda) / head (cabeça)

- Retorna, por padrão, as 10 últimas/primeiras linhas de determinado arquivos
- "-n" exibe-se a quantidade de linhas desejadas

aluno@provasdeti:~$ ps(process status / instantâneo) / top (lista as tarefas / interativo)

- Exibem os processos em execução
- O primeiro faz de forma estática, o segundo de forma dinâmica

aluno@provasdeti:~$ du (disk usage), df (disk space file system), man (manual)

- du: tamanho de cada arquivo dentro da pasta
- df: tamanho de cada partição
- man: manual de um comando

aluno@provasdeti:~$ clear, pwd, touch, cat

- clear: Limpar a tela
- pwd: imprime o nome do diretório de trabalho (print work directory)
- touch: Cria um arquivo vazio
  - modifica a data e hora de acesso e modificação de arquivos
- cat: Exibe o conteúdo ou concatena arquivos
  - Arquivos muito extensos podem necessitar de apoio do more ou less

aluno@provasdeti:~$ uptime, cal

- uptime: Tempo que o sistema está on-line
- cal: Mostra um calendário

aluno@provasdeti:~$ gzip, tar

- gzip: Compactador de arquivos. Reduz o tamanho final do conjunto.
  - Sem parâmetros ele sobrepõe o antigo
- tar: Empacotador, junta vários arquivos num só, mas o tamanho final equivale ao somatório de todos.
- O comando tar é por padrão recursivo

aluno@provasdeti:~$ find , whereis, lsusb, lshw

- **find**: Busca arquivos no disco segundo algum critério
- **whereis**: busca por arquivos executáveis, man pages, arquivos de configuração e fontes
- **lsusb**: Lista os dispositivos usb
  - apenas conexões ativas
- **lshw**: Lista informações sobre o HW da máquina

ITnerante PROVAS DE TI TUDO PARA VOCÊ PASSAR

aluno@provasdeti:~$ netstat

- Mostra as conexões da máquina
- -t: Todas tcp
- -u: Todas udp
- -a: Abertas
- -p: Processos
- -r: Tabela de roteamento

ITnerante PROVAS DE TI TUDO PARA VOCÊ PASSAR

```
aluno@provasdeti:~$ file, lsof, pstree
```

- file: Identifica o tipo de arquivo
- lsof: Lista arquivos abertos e quais processos os abriu
- pstree: Exibe a árvore dos processos, mostrando as relações de pais e filhos


```
aluno@provasdeti:~$ shutdown
```

- desligar

  -P [now + 1] unidade em minuto
- Reiniciar

  -r
- aceita AGORA ou tempo futuro

aluno@provasdeti:~$ grep, pgrep

- grep: imprime linhas contendo determinada ocorrência
- pgrep: Exibe o PID do processo que possuem a ocorrência passada como parâmetro

aluno@provasdeti:~$ kill, pkill

- kill: Enviar sinais para o processo
- pkill: Envia sinal para todos processos que possuem uma ocorrência
  - pgrep + kill

aluno@provasdeti:~$ Comandos sobre atividades e logins de usuários

- **history**: Exibe os últimos 500 comandos digitados pelo usuário
  - Root: /root/.bash_history
  - Outros usuários: /home/usuario/.bash_history
- **Binários**: Alguns comandos gravam seus registros em arquivos binários em vez de arquivos texto. Não podem ser lidos por um simples editor de textos
- **lastlog**: Exibe uma lista de todos os usuários do sistema e a data do último login com sucesso
  - join entre passwd e os logs
- **last**: Mostra uma lista com os últimos logins efetuados com sucesso no sistema
  - /var/log/wtmp
- **lastb**: Mostra uma lista com todas as tentativas de login sem sucesso, seja com usuários válidos ou desconhecidos
  - /var/log/btmp

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

aluno@provasdeti:~$ redirecionamentos

- Entrada: <
- Saída: > Sobrepõe o antigo conteúdo
- Append: >> adiciona ao antigo conteúdo
- | (pipe): Concatenar saída com entrada
  - Elimina-se a criação de arquivos temporários
- Saída de erro: 2>

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

aluno@provasdeti:~$ Arquivos de configuração

- /etc/fstab
  - devices e pontos de montagem
  - lido na hora que a máquina liga
  - análogo ao autoexec.bat
- /etc/modules
  - usado para carregamento dinâmico de módulos
- /etc/lilo.conf e /boot/grub/menu.lst
  - Grub é o mais popular
  - gerenciamento de boot

aluno@provasdeti:~$ Arquivos de configuração

- /etc/x11/xorg.conf
  - Ambiente gráfico
- /etc/passwd, /etc/shadow, /etc/group
  - usuários e grupos
- /etc/login.defs
  - arquivo de configuração do programa de login
  - especifica os valores default da política de segurança
    - nº de dias para expiração da senha
    - tamanho da senha

Linux Para Concursos II

Bateria de Questões de Aprendizagem

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

1. Marcos, usuário de um computador com sistema operacional Linux Red Hat listou o conteúdo do seu diretório home e observou a presença do arquivo manual.txt com 31.251 bytes de tamanho, o que representa cerca de 20 páginas de texto se visualizado em um terminal Linux padrão. Para que Marcos possa visualizar diretamente o final do arquivo manual.txt, sem a necessidade de iniciar a visualização a partir do começo do arquivo, ele deve executar o comando:

A. cat manual.txt | more
B. more manual.txt
C. list manual.txt | end
D. tail manual.txt
E. cat manual.txt | end

ITnerante

FCC 2014 – TRF 4 – Técnico Judiciário TI

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

1. Marcos, usuário de um computador com sistema operacional Linux Red Hat listou o conteúdo do seu diretório home e observou a presença do arquivo manual.txt com 31.251 bytes de tamanho, o que representa cerca de 20 páginas de texto se visualizado em um terminal Linux padrão. Para que Marcos possa visualizar diretamente o final do arquivo manual.txt, sem a necessidade de iniciar a visualização a partir do começo do arquivo, ele deve executar o comando:

A. cat manual.txt | more
B. more manual.txt
C. list manual.txt | end
D. tail manual.txt
E. cat manual.txt | end

ITnerante *FCC 2014 – TRF 4 – Técnico Judiciário TI* Provas de TI

2. Julgue os próximos itens, com relação ao sistema Linux.

[55] Na estrutura de arquivos do sistema operacional, o diretório /var/ contém o spool de impressora.

[56] No Linux, a notação ~ é utilizada para acessar o diretório /root/ do sistema.

[57] No diretório /dev/, são encontrados diversos dispositivos de hardware instalado no Linux.

ITnerante *CESGRANRIO 2014 – FINEP – Informática Suporte* Provas de TI

2. Julgue os próximos itens, com relação ao sistema Linux.

[55] Na estrutura de arquivos do sistema operacional, o diretório /var/ contém o spool de impressora.

~~[56] No Linux, a notação ~ é utilizada para acessar o diretório /root/ do sistema.~~

[57] No diretório /dev/, são encontrados diversos dispositivos de hardware instalado no Linux.

ITnerante — *CESGRANRIO 2014 – FINEP – Informática Suporte* — Provas de TI

3. Dentre os comandos básicos do sistema operacional Linux existe o cd (Change Directory) que pode ser utilizado para navegar entre os diretórios do sistema. Caso o comando cd seja executado sem qualquer parâmetro, ou opção,

A. será apresentada a estrutura de diretório da raiz (/) até o diretório corrente.
B. o prompt permanecerá no mesmo diretório.
C. será acessado o diretório raiz (/) do sistema.
D. o prompt retornará ao diretório anteriormente acessado.
E. será acessado o diretório home do usuário corrente

ITnerante — *FCC 2014 – TRT 16 – Técnico Judiciário TI* — Provas de TI

3. Dentre os comandos básicos do sistema operacional Linux existe o cd (Change Directory) que pode ser utilizado para navegar entre os diretórios do sistema. Caso o comando cd seja executado sem qualquer parâmetro, ou opção,

A. será apresentada a estrutura de diretório da raiz (/) até o diretório corrente.
B. o prompt permanecerá no mesmo diretório.
C. será acessado o diretório raiz (/) do sistema.
D. o prompt retornará ao diretório anteriormente acessado.
E. será acessado o diretório home do usuário corrente

4. A estrutura de diretórios do sistema operacional Linux possui uma organização padronizada e adotada por todas as distribuições. Considerando que um novo usuário de nome superior seja criado no Linux, o diretório do usuário será criado em:

A. /root.
B. /home.
C. /usr/local.
D. /tmp.
E. /usr.

4. A estrutura de diretórios do sistema operacional Linux possui uma organização padronizada e adotada por todas as distribuições. Considerando que um novo usuário de nome superior seja criado no Linux, o diretório do usuário será criado em:

A. /root.
B. /home.
C. /usr/local.
D. /tmp.
E. /usr.

ITnerante FCC 2014 – TRT 16 – Técnico Judiciário TI PROVAS DE TI TUDO PARA VOCÊ PASSAR

5. No Unix não há o conceito de nomes de drives, como C:, mas todos os paths partem de uma raiz comum, o root directory "/''. Quando a máquina possui vários discos diferentes (ou ao menos várias partições diferentes de um mesmo disco), cada uma delas em geral corresponderá a uma ramificação do sistema de arquivos, como /usr, /var ou ainda nomes como /disco2, que são chamados pontos de montagem. Dentre os principais diretórios do sistema está o diretório padrão para armazenamento das configurações do sistema e eventuais scripts de inicialização. Este diretório é o

A. /conf
B. /usr
C. /etc
D. /proc
E. /settings

ITnerante FCC 2014 – TRT 3 – Informática Infraestrutura PROVAS DE TI TUDO PARA VOCÊ PASSAR

5. No Unix não há o conceito de nomes de drives, como C:, mas todos os paths partem de uma raiz comum, o root directory "/''. Quando a máquina possui vários discos diferentes (ou ao menos várias partições diferentes de um mesmo disco), cada uma delas em geral corresponderá a uma ramificação do sistema de arquivos, como /usr, /var ou ainda nomes como /disco2, que são chamados pontos de montagem. Dentre os principais diretórios do sistema está o diretório padrão para armazenamento das configurações do sistema e eventuais scripts de inicialização. Este diretório é o

A. /conf
B. /usr
C. /etc
D. /proc
E. /settings

ITnerante — *FCC 2014 – TRT 3 – Informática Infraestrutura* — Provas de TI Tudo para você passar

6. Um comando muito utilizado em distribuições Linux é o PS. Com este comando é possível

A. exibir uma lista de processos em execução.
B. alterar a senha (password) de um usuário.
C. exibir o status corrente da impressora.
D. enviar uma mensagem para o grupo de trabalho.
E. alterar os privilégios de acesso de um arquivo ou diretório.

ITnerante — *FCC 2013 – TRT 15 – Técnico Judiciário TI* — Provas de TI Tudo para você passar

6. Um comando muito utilizado em distribuições Linux é o PS. Com este comando é possível

A. exibir uma lista de processos em execução.
B. alterar a senha (password) de um usuário.
C. exibir o status corrente da impressora.
D. enviar uma mensagem para o grupo de trabalho.
E. alterar os privilégios de acesso de um arquivo ou diretório.

ITnerante — *FCC 2013 – TRT 15 – Técnico Judiciário TI* — Provas de TI Tudo para você passar

7. Para alterar o arquivo de configuração do serviço de DHCP no Linux, deve-se acessar o diretório

A. /dev.
B. /mnt.
C. /etc.
D. /usr/bin.
E. /boot

ITnerante — *CESPE 2013 – TRT 8 – Analista Judiciário TI* — Provas de TI Tudo para você passar

7. Para alterar o arquivo de configuração do serviço de DHCP no Linux, deve-se acessar o diretório

A. /dev.
B. /mnt.
C. /etc.
D. /usr/bin.
E. /boot

ITnerante *CESPE 2013 – TRT 8 – Analista Judiciário TI* PROVAS DE TI TUDO PARA VOCÊ PASSAR

8. No sistema operacional Linux, por padrão, os programas aplicativos para os usuários, como por exemplo o pico e o write, são instalados no diretório:

A. /bin
B. /usr
C. /lib
D. /sbin
E. /home

ITnerante *VUNESP 2013 – ITESP– Analista de Sistemas e Ciência da Computação* PROVAS DE TI TUDO PARA VOCÊ PASSAR

8. No sistema operacional Linux, por padrão, os programas aplicativos para os usuários, como por exemplo o pico e o write, são instalados no diretório:

A. /bin
B. /usr
C. /lib
D. /sbin
E. /home

ITnerante *VUNESP 2013 – ITESP– Analista de Sistemas e Ciência da Computação* PROVAS DE TI TUDO PARA VOCÊ PASSAR

9. Uma ferramenta muito utilizada em sistemas operacionais Linux permite a exibição da utilização do espaço por arquivos. Analise o seguinte comando efetuado com este utilitário:

du -ahc

A execução deste comando com os parâmetros informados irá apresentar

A. todos os arquivos da pasta atual, exceto arquivos ocultos e armazenados em cache.
B. todas as pastas do sistema, incluindo arquivos ocultos e armazenados em cache.
C. a taxa de compactação dos arquivos juntamente com informações sobre a memória heap.
D. apenas os arquivos que contenham os atributos hidden e compacted.
E. apresentar todos os arquivos, com valores descritos de forma mais legível e com um total ao final.

ITnerante *FCC2013 – ALE RN– Técnico em Hardware* PROVAS DE TI TUDO PARA VOCÊ PASSAR

9. Uma ferramenta muito utilizada em sistemas operacionais Linux permite a exibição da utilização do espaço por arquivos. Analise o seguinte comando efetuado com este utilitário:

du -ahc

A execução deste comando com os parâmetros informados irá apresentar

A. todos os arquivos da pasta atual, exceto arquivos ocultos e armazenados em cache.
B. todas as pastas do sistema, incluindo arquivos ocultos e armazenados em cache.
C. a taxa de compactação dos arquivos juntamente com informações sobre a memória heap.
D. apenas os arquivos que contenham os atributos hidden e compacted.
E. apresentar todos os arquivos, com valores descritos de forma mais legível e com um total ao final.

ITnerante FCC2013 – ALE RN– Técnico em Hardware PROVAS DE TI TUDO PARA VOCÊ PASSAR

10. Em ambientes operacionais Linux, um símbolo, quando utilizado em conjunto com o comando cd em uma janela de terminal (shell), permite que a mudança de diretório seja efetuada para o diretório home do usuário. Este símbolo é

A. ~ (til).
B. ^ (circunflexo).
C. \ (barra invertida).
D. | (barra vertical).
E. * (asterisco).

ITnerante FCC2013 – MPE SE – Analista MP PROVAS DE TI TUDO PARA VOCÊ PASSAR

10. Em ambientes operacionais Linux, um símbolo, quando utilizado em conjunto com o comando cd em uma janela de terminal (shell), permite que a mudança de diretório seja efetuada para o diretório home do usuário. Este símbolo é

A. ~ (til).
B. ^ (circunflexo).
C. \ (barra invertida).
D. | (barra vertical).
E. * (asterisco).

11. Com relação ao sistema operacional Linux, julgue os itens a seguir.

[116] A nomenclatura dos discos no Linux é semelhante ao ambiente Windows, visto que a estrutura de diretórios inicia com unidades de disco definidas por letras.

[117] Os comandos do Linux são arquivos com permissão para serem executados e estão armazenados, em sua maioria, no diretório /bin.

[118] Ao se executar o comando de administração ps -aux, serão apresentados todos os processos correntes no sistema Linux.

[119] Durante a instalação do Linux, é criada uma conta root — uma conta de administrador ou superusuário —, que garante ao usuário root o direito de realizar qualquer atividade no sistema.

[120] Por meio do comando rm –r, é possível acessar diretamente o diretório raiz do ambiente Linux.

11. Com relação ao sistema operacional Linux, julgue os itens a seguir.

~~[116] A nomenclatura dos discos no Linux é semelhante ao ambiente Windows, visto que a estrutura de diretórios inicia com unidades de disco definidas por letras.~~

[117] Os comandos do Linux são arquivos com permissão para serem executados e estão armazenados, em sua maioria, no diretório /bin.

[118] Ao se executar o comando de administração ps -aux, serão apresentados todos os processos correntes no sistema Linux.

[119] Durante a instalação do Linux, é criada uma conta root — uma conta de administrador ou superusuário —, que garante ao usuário root o direito de realizar qualquer atividade no sistema.

~~[120] Por meio do comando rm –r, é possível acessar diretamente o diretório raiz do ambiente Linux.~~

ITnerante *CESPE 2013 – Ministério das Comunicações – Especialidade 12* PROVAS DE TI TUDO PARA VOCÊ PASSAR

GABARITO

1. D
2. C, E, C
3. E
4. B
5. C
6. A
7. C
8. B
9. E
10. A
11. E, C, C, C, E

ITnerante PROVAS DE TI TUDO PARA VOCÊ PASSAR

Linux Para Concursos II

Registros de Atividades

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Fund. dos registros de atividades

- Em uma grande rede, o registro em log centralizado é fundamental
- Maior facilidade no controle dos dados
- Dados de auditoria indisponíveis para uma pessoa que viola a segurança de uma máquina
- Hackers normalmente editam logs de sistema para encobrir seus vestígios

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Fund. dos registros de atividades

- Perigos
  - Qualquer um pode chamar syslog e falsificar entradas de log por meio de qualquer daemon ou utilitário
  - Syslog utiliza UDP: Mensagens podem ser perdidas
  - Mensagens de Syslog podem ser usadas para DoS

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Fund.dos registros de atividades

- Firewalls
  - O servidor Syslog deve ser protegido por firewall do restante da rede
  - O firewall deve permitir conexões somente na porta do syslog
  - O firewall somente libera conexões dos hosts com permissão para fazer registro log no Servidor
  - Conexões ssh podem ser permitidas a partir das estações de trabalho dos administradores de rede, para tornar mais fácil lerem os logs a partir de seus computadores

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Kernel e Registro em Log na inicialização

- Kernel armazena entradas de logs em um BUFFER INTERNO de tamanho limitado.
- Buffer é grande o suficiente para acomodar mensagens sobre todas as atividades do kernel na inicialização
- Após a inicialização, um processo de usuário acessa o buffer de log do kernel
- O SO faz isso executando o comando DMESG e direcionando a saída para /var/log/dmesg
- Melhor lugar para procurar detalhes sobre o ciclo de inicialização

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Kernel e Registro em Log na inicialização

- Klogd
  - Após a inicialização, o log do kernel é tratado por este daemon
  - O klogd é o daemon responsável por capturar as mensagens lançadas pelo kernel.
  - O klogd guarda suas mensagens em dois locais, no /proc ou usando a "sys_syslog interface".
  - Pode fazer o DUMP completo do buffer do Kernel
  - Pode ler mensagens do Buffer do Kernel à medida que são geradas
  - Poderá gravar as informações diretamente em um arquivo
  - Poderá passar as informações para o syslog (padrão)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Kernel e Registro em Log na inicialização

- LOG do KERNEL no console de sistema
  - Na inicialização, é importante que a saída vá para o console
  - O Sistema de pé e funcionando, as MSG de console podem ser uma amolação

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

O que registrar?

- Erros
- Ameaças de segurança
- Informações de debug ou tunning
- registro de eventos do SO e de aplicativos executados sobre ele
- Eventualmente concentrador de eventos de outras plataformas
- "trilha de auditoria"

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Quem produz logs?

- Daemons de Sistema
- Kernel
- Programas

Qual destino dos logs?

- Resumos
- Compactados
- Arquivados
- Descartados

SYSLOG

- Syslog é um protocolo para coleta de eventos em redes TCP/IP
  - –Padronizado pela RFC 3164 e 5424
  - –Padrão IETF
  - –UDP 514
  - –TLS 6514

ITnerante PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG

- A maioria dos programas delega a função de gerenciar logs ao SYSLOG, cujo arquivo de configurações é /etc/syslog.conf
- Arquivos de log geralmente possuem o modo 644 (RW-,R--,R--)
- Além de terem nomes aleatórios, os arquivos de log ficam dispersos em diretórios e sistemas de arquivos
  - Geralmente ficam em /var/log
- Aceita eventos do windows
  - Centralizando logs
  - Kiwi Syslog Daemon Service (Windows)
  - NTsyslog

ITnerante PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG

- Habilidade de centralizar o registro em log para uma rede inteira
  - Suportado por uma grande variedade de dispositivos
  - Importante se houver comprometimento da máquina
- Funcionamento
  - Programas cientes de syslog gravam as entradas de log no arquivo especial /dev/log em um socket
  - syslogd lê as mensagens a partir deste arquivo, consulta seu arquivo de configuração (syslog.conf) e envia cada mensagem ao destino apropriado

ITnerante PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG

- Separação de papéis
  - gerador de eventos
  - coletor de eventos
  - visualizador
- Vantagens importantes
  - Liberar os programadores da mecânica de gravação de logs. Antes de Syslog, cada programador criava seu sistema de logs
  - Colocar os administradores de rede no controle do processo dos registros em log

ITnerante PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG

- Arquivos e diretórios relacionados
  - /etc/syslog.conf
  - /etc/init.d/sysklogd
  - /etc/logrotate.conf
  - /var/log/
  - Curiosidades: O boot.log armazena o log do processo responsável pela inicialização do sistema; e o dmesg é um log do boot do SISTEMA

SYSLOG

- Destino dos Logs
  - Arquivos
  - Terminais de usuários
  - Outras máquinas

SYSLOG - Arquitetura

- syslogd
  - Daemon de registro em log
  - Permite qualquer programa ou comando registre mensagens de Log no Console ou em um arquivo
  - Recebe as mensagens dos comandos e as envia para o destino especificado em syslog.conf
  - Lê o syslog.conf em sua inicialização e quando recebe um sinal HUP

SYSLOG - Arquitetura

- openlog
  - Rotinas de Biblioteca que submetem mensagens ao syslogd
- logger
  - Comando em nível de usuário que submete entradas de log do shell
  - Provê interface para o Daemon Syslogd
  - Uso muito comum em Shell Scripts
  - Sempre que precisar registrar algo nos arquivos de Log usar o Logger.

SYSLOG - Arquitetura

- /etc/syslog.conf controla o comportamento do syslogd
  - Arquivo de texto com um formato relativamente simples

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

- **SELETOR**:RECURSO.PRIORIDADE<TAB>AÇÃO

- **Recursos / facilities**
- Definição para que um programa relate em que grupo de registros um log se enquadra
  - *: Todos os recursos, exceto "mark"
  - auth: Comandos relacionados com segurança e autorização
  - Authpriv: Mensagens de autorização sigilosas / privadas
- cron: Daemon de cron
- daemon: Outros daemons do sistema ex:(sshd, inetd, pppd, ...)
- ftp: Daemon de FTP, o ftpd
- kern: Mensagens relativas ao kernel.
- lpr: Sistema de spooling de impressora de linha
- mail: Sendmail e outros programas relacionados com E-mail
- syslog: Mensagens internas do syslog.
- user: Todo o tipo de mensagens a nível de usuário.
- news
- uucp
- local0-local7: 8 níveis

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

- **SELETOR**:RECURSO.PRIORIDADE<TAB>AÇÃO
- **Nível/Prioridade**
- Ordem DECRESCENTE por níveis de gravidade
- O log da severidade apontada ou superior, receberá a mesma ação
- **emerg**: Situações de Pânico
  - Um exemplo de mensagens de nível de emergência é aquela gerada por shutdown quando o sistema está prestes a ser desligado.
- **alert**: Deverá ser providenciada algum tipo de ação logo de imediato.
- **crit**: Condições críticas.
- **err**: Outras condições de erro.
- **warning**: Mensagens de alerta.
- **notice**: Coisas que podem merecer investigação, Condições normais
- **info**: Mensagens de informação.
- **debug**: Mensagens de depuração.

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Níveis/Prioridades

Nível	Significado
Emerg	Pânico
Alert	Urgent
Crit	Condições críticas
Err	Outras cond de erro
Warning	Advertência
Notice	Coisas que talvez mereçam investigação
Info	Msg informativas
Debug	Somente para depuração

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

- **SELETOR**:RECURSO.PRIORIDADE<TAB>AÇÃO
- **AÇÃO**
- **nomeDoArquivo**
  - **Anexa a mensagem a um arquivo na máquina local**
  - **Deve ser informado o path absoluto para o arquivo**
  - **Especificando um nome de arquivo inexistente, syslogd o criará quando a mensagem for encaminhada pela primeira vez**
- **@nome do host / Ip do Host**
  - **Encaminha a mensagem para o syslogd na máquina informada**
  - **Deve ser usado com um esquema DNS ou NIS (dns da SUN) para tradução**
- **usuário1, usuario2,...**
  - **Grava a mensagem na tela dos usuários, se eles estiverem conectados**

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

Exemplos

Seletor	Significado
Mail.info	Seleciona msg relacionadas ao correio com prioridade info ou + altos
Mail.=info	Apenas igual a info
Mail.info; mail.!err	Info, notice, warning
Mail.debug; mail.!=warning	Todas exceto warning

- Em syslog.conf os caracteres = e ! indicam prioridades. “Apenas esta” e “exceto esta e outras superiores" respectivamente

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

Exemplos

Seletor	Significado
Mail.info	Seleciona msg relacionadas ao correio com prioridade info ou + altos
Mail.=info	Apenas igual a info
Mail.info; mail.!err	Info, notice, warning
Mail.debug; mail.!=warning	Todas exceto warning

- recurso.nível <tab> ação
- mail.debug /var/log/maillog
  - Faz com que as mensagens do sistema de e-mail fossem salvas no arquivo /var/log/maillog

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

Exemplos

Seletor	Significado
Mail.info	Seleciona msg relacionadas ao correio com prioridade info ou + altos
Mail.=info	Apenas igual a info
Mail.info; mail.!err	Info, notice, warning
Mail.debug; mail.!=warning	Todas exceto warning

- O Seletor está enviando uma mensagem de log e o nível de gravidade da mensagem: mail.debug (no mínimo)
- Nomes de recursos e de níveis de gravidade devem ser escolhidos de uma breve lista de valores definidos

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

Exemplos

Seletor	Significado
Mail.info	Seleciona msg relacionadas ao correio com prioridade info ou + altos
Mail.=info	Apenas igual a info
Mail.info; mail.!err	Info, notice, warning
Mail.debug; mail.!=warning	Todas exceto warning

- Recursos podem conter palavras-chaves especiais com "*" e "none" (tudo ou nada, respectivamente)

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Formato Básico

Exemplos

Seletor	Significado
Mail.info	Seleciona msg relacionadas ao correio com prioridade info ou + altos
Mail.=info	Apenas igual a info
Mail.info; mail.!err	Info, notice, warning
Mail.debug; mail.!=warning	Todas exceto warning

- Podemos usar vários Recursos e Níveis em um Seletor (separados por ;)
  - Mesma ação para todos
- Não podemos usar várias AÇÕES
  - Para isso, temos que incluir, por exemplo, duas linhas com os mesmos seletores e ações diferentes

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

SYSLOG – Ferramentas Alternativas ao Syslog

- syslog-ng (syslog next-generation)
  - Utilizados em Sistemas Suse por padrão
  - Recursos adicionais de configuração
  - filtragem baseada no conteúdo das mensagens
  - Integridade de mensagem
  - Melhor suporte às restrições de firewall, quando as mensagens são encaminhadas pela rede
- SDSC Secure Syslog
  - San Diego Supercomputing Center
  - Também conhecido como Syslog de Alto Desempenho

Políticas de registro em LOG

1. Descartar imediatamente todos os dados do LOG
2. Redefinir os arquivos de LOG em intervalos Periódicos
3. Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado (se houver espaço suficiente, não compactar os arquivos de LOG)
4. Compactar/empacotar e arquivar LOGS em fita ou outra mídia permanente.

Políticas de registro em LOG

- A escolha dependerá
  - Quanto espaço em disco disponível
  - Grau de Preocupação com a Segurança
  - As diretivas giram em torno do crescimento e da quantidade de Logs
    Ex: Logs de Análise de Tráfego

Política 01: Descartar imediatamente todos os dados do LOG

- Não é recomendado jogar fora todas as informações de um Registro de Log
- Importância dos Logs
  - Logs fornecem evidências importantes de Intrusão
  - Importante para alertas sobre HW e SW
  - Certos arquivos de Log podem servir como Provas em Tribunais

Política 02: Redefinir os arquivos de LOG em intervalos Periódicos

- "Apagar/Reinicicializar de tempos em tempos o arquivo de log“
- Qual periodicidade?
- Problemas na fronteira temporal final têm impacto maior

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- Esquema de armazenamento de arquivos de log
- Consiste em classificar arquivos separados por semanas ou meses
- Uso de scripts
  - Renomear cada arquivo a fim de posicionar os dados mais antigos no final da cadeia
  - Exemplo: arquivo 1 torna-se arquivo2, arquivo torna-se arquivo1...

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- Logs por data
  - Algumas empresas criam arquivos de Log por data
  - Mais difícil de ser implementado
  - Vale o esforço, caso com frequência, sejam consultados Logs antigos
  - Comando: mv logfile logfile.`date + %Y.%m.%d`
  - ls poderá classificar arquivos cronologicamente
  - Exemplo: log.terca; 10102010.log

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- Logrotate
  - Utilitário de rodízio de logs
  - Mais fácil e mais confiável do que criar seus próprios script
  - Ferramenta para administração dos Logs do Sistema

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- Oferece configurações para...
  - –Manutenção
  - –Rotação
  - –Envio por e-mail
  - –Exclusão de Arquivos

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- Alguns scripts são incluídos no diretório /etc/logrotate.d
- Desenhado para facilitar a Administração de Sistemas que geram muitos logs
- Arquivos de Logs devem ser vigiados pois ocupam muito espaço em disco

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- Arquivos de logs que não sofrerem rotação (ou seja, não forem apagados e recriados) irão crescer indefinidamente
- Normalmente o Logrotate é rodado pelo CRON com tarefas diárias, semanais ou mensais
- Também é possível acessar o Logrotate diretamente.

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- /etc/logrotate.conf
  - Arquivo de configuração padrão
  - Vários arquivos de configuração (ou diretórios contendo arquivos de configuração) podem aparecer na linha de comando (diretório /etc/logrotate.d)
  - SWs cientes do LogRotate podem inserir instruções de gerenciamento de logs (como parte da sua instalação)

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 03: Fazer a rotação dos arquivos de LOG, mantendo os dados por um período pré-determinado

- Savelog
  - Mais simples que o Log Rotate
  - Usados pelo Debian e o Ubuntu
  - Gerencia o rodízio para arquivos individuais
  - Não utiliza um arquivo de configuração
  - Alguns SWs também utilizam o savelog

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 04: Compactar/empacotar e arquivar LOGS em fita ou outra mídia permanente.

- Estender o tempo de retenção
- gzip
  - Cópia compactada de um arquivo
  - Não é capaz de compactar vários arquivos em um só
  - Trabalha de maneira eficiente, por isso é amplamente usado

ITnerante

PROVAS DE TI TUDO PARA VOCÊ PASSAR

Política 04: Compactar/empacotar e arquivar LOGS em fita ou outra mídia permanente.

- tar
  - Capaz de armazenar vários arquivos em um só
  - Trata-se de um empacotador e não de um compressor
- zgrep
  - Pesquisa os arquivos compactados sem desempacotá-los

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Linux Para Concursos II

Bateria de Questões de Aprendizagem

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

1. O administrador de um computador com sistema operacional Linux Red Hat executou o comando dmesg no prompt de comandos. Como resultado ele obteve

A. as informações do processo de boot do sistema operacional.
B. a listagem das mensagens de e-mail recebidas.
C. a listagem das mensagens enviadas pelos usuários para o administrador.
D. a eliminação (deleção) das mensagens de e-mail da caixa temporária.
E. as informações das ocorrências diárias de uso do sistema operacional.

1. O administrador de um computador com sistema operacional Linux Red Hat executou o comando dmesg no prompt de comandos. Como resultado ele obteve

A. as informações do processo de boot do sistema operacional.
B. a listagem das mensagens de e-mail recebidas.
C. a listagem das mensagens enviadas pelos usuários para o administrador.
D. a eliminação (deleção) das mensagens de e-mail da caixa temporária.
E. as informações das ocorrências diárias de uso do sistema operacional.

ITnerante FCC 2014 – TRF 4 – Técnico Judiciário TI PROVAS DE TI TUDO PARA VOCÊ PASSAR

2. O comando usado para visualizar as mensagens de inicialização do Linux quando este já está em execução, é

A. cat /proc/bootmsg
B. cat /boot/messages
C. cat /var/bootlog
D. bootmsg | more
E. dmesg | more

2. O comando usado para visualizar as mensagens de inicialização do Linux quando este já está em execução, é

A. cat /proc/bootmsg
B. cat /boot/messages
C. cat /var/bootlog
D. bootmsg | more
E. dmesg | more

ITnerante FGV 2012 – Analista Legislativo – Análise de Sistemas Provas de TI

3. Os sistemas operacionais Linux possuem mecanismos para registrar determinados eventos que ocorrem durante sua operação. Isso é comumente chamado de registro de log, e um desses sistemas de maior abrangência é o Syslog. O Syslog é bastante flexível e permite que as mensagens sejam ordenadas pela fonte e pela importância (nível de gravidade). Além disso, as mensagens podem ser direcionadas para múltiplos destinos: arquivos de log, terminais de usuários ou outros computadores. Os níveis do Syslog, em ordem decrescente de importância (nível de gravidade), são

A. crit, emerg, alert, err, warning, notice, info, debug.
B. emerg, crit, alert, err, warning, notice, info, debug.
C. crit, err, emerg, alert, warning, notice, info, debug.
D. crit, emerg, err, alert, warning, notice, info, debug.
E. emerg, alert, crit, err, warning, notice, info, debug.

ITnerante *CESGRARIO 2010 – Petrobrás – Técnico de TI e Telecom* PROVAS DE TI TUDO PARA VOCÊ PASSAR

3. Os sistemas operacionais Linux possuem mecanismos para registrar determinados eventos que ocorrem durante sua operação. Isso é comumente chamado de registro de log, e um desses sistemas de maior abrangência é o Syslog. O Syslog é bastante flexível e permite que as mensagens sejam ordenadas pela fonte e pela importância (nível de gravidade). Além disso, as mensagens podem ser direcionadas para múltiplos destinos: arquivos de log, terminais de usuários ou outros computadores. Os níveis do Syslog, em ordem decrescente de importância (nível de gravidade), são

A. crit, emerg, alert, err, warning, notice, info, debug.
B. emerg, crit, alert, err, warning, notice, info, debug.
C. crit, err, emerg, alert, warning, notice, info, debug.
D. crit, emerg, err, alert, warning, notice, info, debug.
E. emerg, alert, crit, err, warning, notice, info, debug.

ITnerante *CESGRARIO 2010 – Petrobrás – Técnico de TI e Telecom* PROVAS DE TI TUDO PARA VOCÊ PASSAR

```
kern.*                  /var/adm/kernel
kern.crit               @prova
kern.crit               /dev/console
kern.info;kern.!err     /var/adm/kernel-info
```

4. Considerando o trecho de arquivo mostrado acima, julgue os itens seguintes.

[84] O trecho mostra a configuração do arquivo syslog.conf em um sistema operacional Linux. Nesse sistema, existem dois serviços que controlam o processo de logging, klogd e syslogd. O primeiro trata mensagens do sistema e o segundo trata mensagens do kernel, por exemplo, mensagens dos protocolos.

[85] A primeira linha mostrada permite que qualquer mensagem que tem kernel facilities seja enviada para o arquivo /var/adm/kernel. A quarta linha informa ao syslogd para salvar todas as mensagens do kernel que têm prioridades de info até warning no arquivo /var/adm/kernel.

[86] A segunda linha direciona todos as mensagens do kernel do tipo crit para um host remoto chamado prova. A terceira linha redireciona as mensagens crit para a console, caso o servidor prova não esteja disponível.


```
kern.*                  /var/adm/kernel
kern.crit               @prova
kern.crit               /dev/console
kern.info;kern.!err     /var/adm/kernel-info
```

4. Considerando o trecho de arquivo mostrado acima, julgue os itens seguintes.

~~[84] O trecho mostra a configuração do arquivo syslog.conf em um sistema operacional Linux. Nesse sistema, existem dois serviços que controlam o processo de logging, klogd e syslogd. O primeiro trata mensagens do sistema e o segundo trata mensagens do kernel, por exemplo, mensagens dos protocolos.~~

[85] A primeira linha mostrada permite que qualquer mensagem que tem kernel facilities seja enviada para o arquivo /var/adm/kernel. A quarta linha informa ao syslogd para salvar todas as mensagens do kernel que têm prioridades de info até warning no arquivo /var/adm/kernel.

~~[86] A segunda linha direciona todos as mensagens do kernel do tipo crit para um host remoto chamado prova. A terceira linha redireciona as mensagens crit para a console, caso o servidor prova não esteja disponível.~~

ITnerante CESPE 2008 – CTII – Técnico Pl. Seg Sis Info PROVAS DE TI TUDO PARA VOCÊ PASSAR

5. No Unix, qual comando pode ser utilizado para verificar que conexões estão no estado TIME_WAIT?

A. ifconfig
B. dmesg
C. strace
D. ipcs
E. netstat

5. No Unix, qual comando pode ser utilizado para verificar que conexões estão no estado TIME_WAIT?

A. ifconfig
B. dmesg
C. strace
D. ipcs
E. netstat

ITnerante CESGRANRIO 2008 – Petrobrás – Analista de Sistemas Infra Provas de TI Tudo para você passar

6. Acerca do sistema operacional Linux, julgue os itens a seguir.

[66] O Linux com kernel 2.6, que tem como sistema de arquivo o EXT3, suporta também outros tipos de sistemas de arquivos.

[67] O gerenciador de boot do Linux não suporta as informações da MBR (master boot record).

[68] Durante a carga do sistema operacional, após a descompactação do kernel e a leitura e o processamento dos arquivos necessários, o último run level tratado é o 2.

[69] As mensagens de erro ou de eventos do sistema operacional, na maioria das vezes, são gerados com o auxílio do syslog.

[70] A criação de contas de usuários no Linux é realizada por qualquer usuário, porque o sistema operacional é multiusuário.

6. Acerca do sistema operacional Linux, julgue os itens a seguir.

[66] O Linux com kernel 2.6, que tem como sistema de arquivo o EXT3, suporta também outros tipos de sistemas de arquivos.

~~[67] O gerenciador de boot do Linux não suporta as informações da MBR (master boot record).~~

~~[68] Durante a carga do sistema operacional, após a descompactação do kernel e a leitura e o processamento dos arquivos necessários, o último run level tratado é o 2.~~

[69] As mensagens de erro ou de eventos do sistema operacional, na maioria das vezes, são gerados com o auxílio do syslog.

~~[70] A criação de contas de usuários no Linux é realizada por qualquer usuário, porque o sistema operacional é multiusuário.~~

ITnerante CESPE 2008 – MPE RR – Técnico em Informática PROVAS DE TI TUDO PARA VOCÊ PASSAR

7. Ainda no que se refere a conceitos de sistemas operacionais e browsers, assinale a opção correta.

A. Os arquivos de shortcut em sistemas Windows contêm indicações do nome do arquivo ao qual se referem, o caminho completo do arquivo e as datas de modificação, alteração e consulta desse arquivo.

B. O sistema de arquivos EXT2, originalmente concebido para o sistema Linux, contém um arquivo de nome $LOGFILE, o qual mantém informações de natureza transacional usadas para recuperação do sistema de arquivos após uma pane.

C. Em sistemas Windows XP, os logs de eventos do sistema são armazenados geralmente na pasta C:\Windows\system32, em arquivos com terminação sys. Tais arquivos contêm todas as informações necessárias para a identificação da natureza de cada evento, como data, hora, categoria e código do evento e descrição do evento.

D. Os logs ou registros de atividade no sistema Linux, em geral, estão armazenados no arquivo /etc/syslog.conf.

7. Ainda no que se refere a conceitos de sistemas operacionais e browsers, assinale a opção correta.

A. Os arquivos de shortcut em sistemas Windows contêm indicações do nome do arquivo ao qual se referem, o caminho completo do arquivo e as datas de modificação, alteração e consulta desse arquivo.

B. O sistema de arquivos EXT2, originalmente concebido para o sistema Linux, contém um arquivo de nome $LOGFILE, o qual mantém informações de natureza transacional usadas para recuperação do sistema de arquivos após uma pane.

C. Em sistemas Windows XP, os logs de eventos do sistema são armazenados geralmente na pasta C:\Windows\system32, em arquivos com terminação sys. Tais arquivos contêm todas as informações necessárias para a identificação da natureza de cada evento, como data, hora, categoria e código do evento e descrição do evento.

D. Os logs ou registros de atividade no sistema Linux, em geral, estão armazenados no arquivo /etc/syslog.conf.

ITnerante *CESPE 2007 – CPC Renato Chaves – Perito Criminal* PROVAS DE TI TUDO PARA VOCÊ PASSAR

8. Considere as afirmativas:

I. */bin contém arquivos executáveis e comandos, tais como, df, date, kill, dmesg, pwd, ls e outros, utilizados frequentemente pelo sistema.*

II. /etc contém os arquivos de configuração do Linux, tais como arquivos de usuários e senhas, arquivos de inicialização, configurações de rede etc.

III. /proc hospeda algumas bibliotecas essenciais para o funcionamento do sistema e também os módulos do kernel.

IV. /usr hospeda as bibliotecas e arquivos dos vários programas instalados no sistema.

Em relação aos diretórios do LINUX, é correto o que consta em

A. I e III, apenas.
B. II e III, apenas.
C. I, II e IV, apenas.
D. II, III e IV, apenas.
E. I, II, III e IV.

ITnerante *FCC 2006 – TRE SP – Técnico Judiciário* PROVAS DE TI TUDO PARA VOCÊ PASSAR

8. Considere as afirmativas:

I. */bin contém arquivos executáveis e comandos, tais como, df, date, kill, dmesg, pwd, ls e outros, utilizados frequentemente pelo sistema.*

II. /etc contém os arquivos de configuração do Linux, tais como arquivos de usuários e senhas, arquivos de inicialização, configurações de rede etc.

III. /proc hospeda algumas bibliotecas essenciais para o funcionamento do sistema e também os módulos do kernel.

IV. /usr hospeda as bibliotecas e arquivos dos vários programas instalados no sistema.

Em relação aos diretórios do LINUX, é correto o que consta em

A. I e III, apenas.
B. II e III, apenas.
C. I, II e IV, apenas.
D. II, III e IV, apenas.
E. I, II, III e IV.

ITnerante *FCC 2006 – TRE SP – Técnico Judiciário* PROVAS DE TI TUDO PARA VOCÊ PASSAR

GABARITO

1. A
2. E
3. E
4. E, C, E
5. E
6. C, E, E, C, E
7. A
8. C

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR