

Sistemas Operativos

1. Administração em Windows Server 2003* e XP

Objectivos de aprendizagem

- Identificar potencialidades dos sistemas Microsoft Windows
- Operar tarefas de administração do sistema operativo
- Utilizar mecanismos de diagnóstico do sistema
- Identificar aspectos críticos de segurança e agir em conformidade

Identificação da versão do sistema operativo

- Natureza das versões “servidor” e “workstation”
- Formas de identificação da versão do Windows em execução
- Informações de sistema (software e hardware)
 - System Properties
 - Device Manager
 - System Information (msinfo32.exe)

Redes Microsoft

- **Workgroup versus Domínio**
 - **Características de um Workgroup:**

Pequeno grupo de computadores numa rede que permite aos utilizadores trabalhar em grupo e que não necessita de administração centralizada.

 - ♦ Os recursos são localizados em cada computador no workgroup;
 - ♦ A administração e autenticação dos utilizadores é feita em cada computador do workgroup;
 - ♦ Cada computador tem o seu Security Accounts Manager (SAM) localmente. O utilizador deve ter a sua conta criada em cada computador para ganhar acesso aos recursos;
 - **Características de um Domínio:**

Termo utilizado pela MS para designar rede ou conjunto de redes, com segurança e administração centralizada, ou seja, que existe um servidor que é responsável pela segurança de rede no que diz respeito à validação de utilizadores. Cada domínio tem um nome único e cada computador desse domínio tem um único nome.

 - ♦ Suporta facilmente um pequeno ou grande número de computadores.
- **Workgroup vs Domínio**

Devemos optar por um domínio sempre que tenhamos situações em que seja importante garantir a segurança da rede. Com um modelo de domínio, podemos fazer auditoria as tentativas falhadas e sucedidas de validação na rede, a quem acedeu, a que ficheiros e em que dia e hora, etc. Vantagem: uma administração da rede centralizada, já que é o servidor quem faz a validação das contas de todos os utilizadores quando estes se ligam a rede. Notar-se-á um melhor desempenho em ambiente de domínio à medida que a rede vai crescendo em relação ao workgroup.

O workgroup terá vantagens sempre que queiramos ter uma rede pequena, sem necessidade de servidor, ou quando as necessidades de segurança forem muito reduzidas.
- **Active Directory**

Serviço para ambiente Microsoft Windows capaz de gerir todos os activos da organização de modo seguro.

É um serviço e pode ser definido como uma fonte de informação hierárquica e que contém informação sobre utilizadores, ficheiros e outros objectos de rede, como impressoras e servidores fax. A informação está disponível tanto para administradores como para utilizadores, facilitando a tarefa a ambos.

Os benefícios:

Segurança de informação: O controlo de acesso pode ser definido quer ao nível de cada objecto quer ao nível das suas propriedades.

Administração baseada em políticas: a implementação de políticas de grupo permite determinar regras que restringem o acesso aos objectos de directório e aos recursos de domínio.

Extensibilidade: representa a capacidade de introduzir novas classes de objectos e de criar os seus próprios atributos, ou ainda, de alterar os atributos dos objectos já existentes.

Escalabilidade: Consiste na capacidade de adicionar novos domain controllers, permitindo assim o aumento das capacidades de rede e uma mais eficaz distribuição de recursos.

Replicação: replicação de informação entre os domain controllers permite uma mais eficaz tolerância a falhas, disponibilidade de informação e aumento de eficácia.

Integração com DNS: permite a "tradução" de endereços IP em nomes perceptíveis.

Compatibilidade: Utiliza protocolos de acesso standard, como o LDAP.

Permissões

- **NTFS**
 - É o sistema de ficheiros (NT File System) nativo dos sistemas Windows NT, Windows 2000 e Windows Server 2003.
 - Tal como os sistemas de ficheiros ext2 (do Linux), mas contrariamente ao FAT (aplicado nas versões mais "leves" do Windows), fornece segurança, fiabilidade e performance. Fornece entre outras capacidades:
 - ♦ Recuperação da consistência do sistema através do log de actividade;
 - ♦ Definição de permissões sobre ficheiros e directórios;
 - ♦ Quotas;
 - ♦ Cifragem;
 - ♦ Compressão.
- **Permissões NTFS para pastas:**
 - Read (Ler): lista as pastas e arquivos localizados dentro de uma pasta, visualiza as permissões, donos e atributos.
 - Write (Gravar): cria arquivos, subpastas, altera o atributo da pasta e visualiza o dono e as permissões.
 - List Folder Contents (Listar conteúdo de pastas): lista o conteúdo das pastas, visualiza o nome do arquivo e subpastas.
 - Read & Execute (Ler e Executar): equivale às permissões ler e listar conteúdo de pastas. Permite a um usuário navegar por pastas que não tenha permissão para alcançar um arquivo ou pasta que tenha permissão.
 - Modify (Modificar): equivale às permissões gravar e ler e executar. Conseguir excluir uma pasta.
 - Full Control (Controle Total): equivale à soma de todas as outras permissões NTFS. Pode alterar as permissões da pasta, tornar-se dono da pasta e excluir pastas e arquivos.
- **ACL(Access Control List)**
 - Cada ficheiro ou directório em NTFS tem uma DACL (Descriptive Access Control List) associada, vulgarmente denominada ACL.

- Existe uma outra lista, denominada SACL (System Access Control List), que define quais os eventos que o utilizador ou grupo está autorizado a auditar.
- Nesta lista são definidos as permissões que utilizadores ou grupos têm acesso ao ficheiro bem como os tipos de acesso que cada um tem. Cada utilizador ou grupo é identificado na lista através do SID (Security Identifier).
- **Utilizadores e Grupos**
 - Existem **três tipos de contas** (accounts):
 - ♦ de **Utilizadores**: que contém toda a informação referente a um utilizador do domínio, nomeadamente:
 - nome;
 - password;
 - grupos a que pertence no domínio;
 - localização de perfil de utilizador;
 - localização de My Documents;
 - ...
 - ♦ de **Computadores**: que guarda a informação necessária para identificar univocamente um computador no domínio;
 - ♦ de **Grupos** de utilizadores: são grupos de utilizadores. Permissões e directos de utilizador deve ser prioritariamente associados a grupos de utilizadores, com todas as vantagens que daí advêm.
 - Existem **dois tipos de grupos** de utilizadores:
 - ♦ **Grupos de distribuição**
 - não podem ser usados na atribuição de permissões de acessos e controlo sobre recursos;
 - são usados como listas de distribuição de e-mail;
 - ♦ **Grupos de segurança**
 - São usados na atribuição de permissões e direitos de utilizadores; também podem ser usados como listas de distribuição de e-mail.
- **Como configurar a herança de permissão**
 - Clique no botão Avançado na guia Segurança para acessar o Advanced Security caixa de diálogo Configurações. Isto é onde você configurar a herança de permissão. Você pode definir a herança de permissão das seguintes opções:
 - ♦ Permitir que as permissões herdáveis do pai se propaguem para este objecto e todos os objectos filho. Incluir estas com entradas definidas explicitamente aqui.
 - ♦ Substituir entradas de permissões em todos os objetos filho com entradas exibidas aqui que se aplicam a objetos filho.
 - Quando você desmarcar a Permitir que permissões herdáveis do pai se propaguem para este objeto e todos os objetos filho. Incluir estas com entradas definidas explicitamente aqui checkbox, uma caixa de diálogo de segurança é exibida. A caixa de diálogo de segurança permite que você quer remover completamente as permissões existentes herdadas ou alterar as permissões existentes herdadas permissões explícitas.

Ferramentas de administração

- System tools
- Computer management
- Device management
- Registry
 - Base de dados central hierarquica usada pela Microsoft para guardar as informações que são necessárias para configurar o sistema para os users, applications and hardware devices.

- **Information (msinfo32.exe)** - essa ferramenta exibe informações sobre o hardware de um computador, drivers, Internet Explorer, aplicativos do Office, etc
- **SYSTEMINFO.EXE** - Exibe informações detalhadas de configuração sobre um computador e seu sistema operacional, incluindo a configuração do sistema operacional, segurança da informação, identificação do produto e as propriedades de hardware, como RAM, espaço em disco e placas de rede.

Políticas de Segurança

- **Utilizador(Domain)** : as GPO's aplicadas aos usuários serão carregadas em todos os computadores em que o usuário fizer logon. As políticas são aplicadas ao computador no momento em que o usuário efetuar logon.
- **Computador(Local)** : as GPO's aplicadas aos computadores serão aplicadas no computador, independente do usuário que efetuar logon. Essas políticas são aplicadas no momento em que o Sistema Operacional for inicializado no computador.
- Por padrão, existem 2 GPO's que são automaticamente configuradas durante a instalação do Active Directory (A.D). São elas:
 - **Default Domain Policy (Diretiva de Domínio Padrão)** : as alterações efectuadas nesta GPO serão aplicadas a todos os usuários e computadores do domínio. Sendo assim, devemos definir nela todas as configurações que devem ser aplicadas aos usuários e computadores dentro de determinado domínio. Está GPO está ligada ao domínio.
 - **Default Domain Controllers Policy (Diretiva de Controladores de Domínio Padrão)** : as configurações nesta GPO serão aplicadas aos Domain Controllers (Controladores de Domínio). Essa GPO está associada à OU (Unidade Organizacional) Domain Controllers.
- **GPO** - conjunto de políticas de segurança utilizadas dentro do Active Directory.
 - **GPO definido para um site:** Todas as configurações feitas no site serão aplicadas a todos os domínios que fazem parte dele.
 - **GPO d domínio:** As configurações aqui feitas afetarão todos os utilizadores e grupos dentro do domínio.
 - **GPO d OU (Organization Units):** O que se aplica nas OU afetarão todos os utilizadores dentro dela.
- Flexibilização na aplicação das GPO's trás ao administrador da rede o total controle sobre a abrangência de suas políticas. Assim como as contas de usuários e grupos de usuários, as diretivas de segurança também podem ser criadas e aplicadas localmente ou no domínio.
 - **Gpedit.msc:** Editor de Políticas de Grupo Local
- **Registry**
 - **Função:** Sua função é concentrar todas as configurações necessárias ao sistema e aos aplicativos executados nele de modo a tornar sua administração mais fácil. Todas as configurações alteráveis no Painel de Controle, associações das extensões de arquivos e configuração de hardware são armazenadas no registro do sistema
 - **Estrutura:** Há estruturas semelhantes em outros sistemas operacionais. No Linux e outros sistemas da família Unix existe no sistema de arquivos o diretório /etc/ que concentra boa parte dos arquivos de configuração utilizados pelo sistema operacional e suas ferramentas.
- **System Configuration Utility (msconfig.exe)**
 - O processo msconfig.exe (msconfig) é um processo standard do Windows XP (e versões ulteriores) que permite editar a configuração do arranque de Windows.

Assim, o MsConfig permite nomeadamente suprimir processos carregados aquando do arranque do Windows.

- **Comando net (a partir da linha de comando)**
 - Conecta um computador ou desconecta um computador de um recurso compartilhado ou exibe informações sobre conexões de computadores. O comando também controla conexões de rede persistentes. Utilizado sem parâmetros, net use recupera uma lista de conexões de rede. Exemplo:
 - ♦ net use LETRA \SERVIDOR\COMPARTILHAMENTO /user:USUÁRIO SENHA

Partilhas

- Além das permissões NTFS, temos as permissões de compartilhamento, que tornam ainda mais seguro o armazenamento de nossas informações.
- As permissões de compartilhamento, diferentemente das permissões NTFS, não impedem que um utilizador acesse um recurso localmente, ou seja, se um utilizador fizer logon em um computador onde esteja localizada uma pasta compartilhada, as permissões de compartilhamento não terão efeito, pois as permissões de compartilhamento só têm efeito quando o recurso é acessado através da rede. Para garantir a segurança de informações através do acesso local, utilizamos as permissões NTFS.
- Ao compartilharmos uma pasta, o Windows Server 2003 por padrão atribui a permissão Leitura para o grupo Todos. No grupo Todos, como o nome já sugere, estão presentes todos os possíveis usuários com acesso ao computador, seja esse acesso local ou através da rede. Não se esqueça desse detalhe, pois caso esteja compartilhando uma pasta com informações confidenciais, por padrão todos usuários terão acesso a essa pasta. Portanto, ao compartilhar uma pasta, configure as permissões necessárias imediatamente.

AutoShare

É uma partilha oculta e é identificada pelo símbolo dólar (\$) no final do nome de partilha. As partilhas ocultas não são apresentadas quando percorre as partilhas de um computador. Há versões de win que criam partilhas administrativas ocultas que os administradores, programas e serviços podem utilizar para gerir o ambiente informático da rede.

Corrigir: Edição do registry,
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters, adicionar 2 DWORD Value, AutoShareWks, AutoShareServer com valor 0.

Gestão de utilizadores

- **Home directory:** Todas as configurações do utilizador são gravadas e mantidas em uma estrutura de subpastas, dentro de C:\Documents and settings\user.
- **Perfil**
 - **Local:** existe para todos os users que fazem ou fizeram logon ao dominio a partir dessa máquina.
 - **Ambulante:** o profile não é guardado localmente, mas num ponto da rede, por forma a que o utilizador possa usar o mesmo profile em qualquer máquina.
 - **Obrigatório:** são colocados no servidor, mas ao contrário destes ultimos, não são actualizaveis. Estes perfis dão ao adminstrador da rede o maior conforto possivel. O grande ganho está na diminuição dos tempos necessários para a administração da rede. Um profile Mandatory pode ser criado por cópia de um profile normal, alterando a extensão do ficheiro NTUSER:DAT para NTUSER.MAN
- **Perfil Mandatário vs Perfil Super Mandatário:** Perfil mandatário ou perfil d utilizador obrigatório é um tipo especial de perfil de utilizador pré-configurado de roaming que os administradores podem usar para especificar as configurações para os utilizadores. Com o

perfil mandat3rio, um utilizador pode modificar o seu ambiente d trabalho, mas as altera33es n3o s3o guardadas quando o utilizador fizer logoff. A pr3xima vez que o utilizador fizer logon, o perfil d utilizador mandat3rio 3 carregado tal como o administrador tinha criado. O perfil d utilizador torna-se perfil mandat3rio quando o administrador renomeia o ficheiro NTuser.dat (no registry) no servidor para NTuser.man. A extens3o .man faz com que o utilizador s3o tenha permiss3es d leitura no perfil. Os perfis tornam-se super-mandat3rios quando o nome d pasta d caminho termina em .man, por exemplo: \\servidor\share\mprofile.man\. Os perfis super-mandat3rios s3o id3nticos aos mandat3rios, com a diferen3a que os utilizadores super-mandat3rios n3o podem fazer logon enquanto o servidor que armazena o perfil mandat3rio n3o esteja dispon3vel. Os utilizadores com perfis mandatorios podem fazer logon com a c3pia de cache local de perfil mandat3rio. Os administradores s3o os 3nicos k podem fazer altera33es nestes perfis.

- **Perfis de utilizador:** Constitui uma muito poderosa ferramenta de administra33o de rede e de produtividade de utilizadores finais. Chama-se User Profile ao conjunto dos par3metros do ambiente de trabalho de cada utilizador da rede. Usando User Profiles, alcan3am-se objectivos t3o diferentes e t3o importantes como o de dar ambientes de trabalho diferentes a v3rios utilizadores que usam a mesma m3quina ou o de dar o mesmo ambiente de trabalho a um utilizador que usa m3quinas diferentes de dia para dia.

Configura33o de servi3os

- **Event Viewer** (permite ver erros ou alertas da m3quina).
- **Start up services** (MSconfig)

DiskManager

- **Convers3o de disco b3sico em din3mico:**
 - O Windows XP Professional 3 compat3vel com dois tipos de armazenamento em disco: b3sico e din3mico.
O armazenamento em **disco b3sico** usa discos orientados por parti33o. Um disco b3sico cont3m volumes b3sicos (parti33es prim3rias, parti33es estendidas e unidades l3gicas).
 - O armazenamento de **disco din3mico** usa discos orientados por volume e inclui recursos que os discos b3sicos n3o t3m, como a capacidade de criar volumes que abrangem diversos discos (volumes estendidos e distribu3dos).
- **Montagem de parti33o em directoria (mounting point):**
 - Se voc3 tem no seu disco rigido duas parti33es, uma com linux e outra com windows 3 poss3vel fazer o que chamamos de montar a parti33o, ou seja, carregar os arquivos que est3o na parti33o do windows para o sua parti33o linux, ent3o execute as seguintes tarefas:
 - **Criando ponto de Montagem**
 - ◆ #cd /mnt
 - ◆ # mkdir windows
 - **Montando a parti33o**
 - ◆ Agora que j3 temos as informa33es necess3rias podemos montar a parti33o do Windows no linux utilizando o comando mount, veja o comando abaixo:
 - # mount -t ntfs /dev/hda1 /mnt/windows
 - ◆ No comando acima eu pedi para o mount montar uma parti33o com o sistema de arquivos ntfs que est3 em /dev/hda1 no ponto de montagem /mnt/windows
 - ◆ **Optimize for quick removal vs. Optimize for performance**
 - **Optimize for quick removal:** Esta configura33o desactiva a grava33o em cache no disco e no Windows, ent3o voc3 pode desligar este dispositivo sem usar o 3cone Remo33o Segura.

- **Optimize for performance:** A configuração permite a gravação em cache no Windows para melhorar o desempenho do disco. Para desligar o dispositivo do computador, clique no ícone Remover hardware com segurança na área de notificação da barra de tarefas.

Gestão de memória

• Definições da memória virtual e hibernação

▪ Memória Virtual:

- ♦ A Memória Virtual é uma extensão da memória RAM. Quando a Memória RAM está ocupada, não sendo mais possível carregar dados nela, ou existem dados que não estão sendo utilizados por muito tempo, ocupando desnecessariamente a RAM, é utilizada a Memória Virtual, que pode ser um arquivo ou vários arquivos que armazenam dados dos processos carregados, ou seja, utilizando a Memória Secundária (de armazenamento), com uma partição dedicada ou utilizando a mesma partição do sistema, liberando a Memória RAM para que dados possam ser carregados nela. Esses dados carregados na Memória Virtual podem ser carregados na Memória RAM novamente conforme a necessidade de processamento dos mesmos. Então ocorre o processo de "troca" em que os dados ficam alternando entre a Memória RAM e a Virtual a fim de serem processados, executados, ou seja, para que o "programa" funcione, falando grosseiramente. Esse processo de troca é o chamado processo de SWAP e ocorre de modo imperceptível para o usuário, porém não substitui o uso da Memória RAM, pois a leitura do Disco-Rígido é mais lenta (centenas de vezes mais lenta) que a da Memória RAM.

▪ Swapping ou Paging (Paginação)?

- ♦ Swapping é uma técnica utilizada pelo sistema de memória virtual do Linux, para simular uma quantidade de memória maior do que realmente existe. Para este efeito, é reservada uma determinada porção do disco rígido, que entra em funcionamento assim que a memória física se esgota.
- ♦ Paging (Paginação) foi introduzido como uma otimização para o swapping onde apenas partes ("pages", páginas) menos utilizadas ou ociosas do processo são movidas para a Memória Virtual, assim quando um processo é executado, apenas partes do processo são movidas da Memória Virtual para a Memória RAM, diminuindo o volume da troca de dados entre elas. As primeiras versões do Unix System V (conhecidos também como SysV) funcionavam apenas com o swapping. Posteriormente (a partir do release 2.0, aparentemente) foi implementado o paging ao Unix System V. Os sistemas operacionais atuais não utilizam o processo de Swapping, apenas o Paging, mas é comum que se utilize apenas o termo Swapping (ou Swap) para a definição deste processo, sem a diferenciação entre os termos Paging e Swapping, tratando-os pelo mesmo nome, excepto quando se estuda esses processos de maneira específica.

▪ Tamanho do ficheiro de hibernação

- ♦ Ora bem, a função de hibernação, que é uma das minhas características preferidas no Windows XP, permite "congelar" o estado actual do PC, desactivando-o totalmente, tal como se tivesse sido desligado, mas gravando o estado dele antes de ser colocado em hibernação: programas

- ♦ e janelas abertos, etc., para voltar a esse estado quando for "acordado" da hibernação.
 - ♦ Antes que pergunte, a hibernação não é o mesmo que a "suspensão". Na suspensão, apenas alguns componentes são desligados, para poupar energia, mas o computador continua ligado.
 - ♦ Mas voltando ao tal ficheiro hiberfil.sys, se você tiver, por exemplo, 512 MB de RAM, então o ficheiro deverá estar a ocupar 512 MB.
 - ♦ Se tiver 1 GB de RAM, ele deverá ocupar 1 GB, e assim sucessivamente.
 - ♦ Basicamente, o que o Windows faz, é copiar tudo aquilo que está na memória do computador no momento que você activa a hibernação, para o tal ficheiro hiberfil.sys.
- **Encerrar: Limpar o ficheiro de paginação de memória virtual**
 - ♦ Esta definição de segurança determina se o ficheiro de paginação de memória virtual é limpo quando o sistema é encerrado.
 - ♦ O suporte de memória virtual utiliza um ficheiro de paginação do sistema para trocar páginas da memória para o disco, quando não são utilizadas. Num sistema em execução, este ficheiro de paginação é aberto em modo exclusivo pelo sistema operativo e está bem protegido. No entanto, os sistemas configurados para permitir o arranque a outros sistemas operativos podem ter de se certificar de que o ficheiro de paginação do sistema é totalmente limpo quando este sistema encerrar. Isto garante que as informações sensíveis da memória do processo, que podem ser incorporadas no ficheiro de paginação, não estão disponíveis para um utilizador não autorizado, que tem acesso directo ao ficheiro de paginação.
 - ♦ Quando esta política for activada, o ficheiro de paginação do sistema será limpo num encerramento com êxito. Se activar esta opção de segurança, o ficheiro de hibernação (hiberfil.sys) também será limpo quando a hibernação for desactivada num computador portátil.

DHCP

O DHCP é um serviço utilizado no protocolo TCP/IP nos dispositivos d rede. Permite ao administrador configurar todas as máquinas automaticamente. Para além d IP, poderá dar-nos outras informações. Podemos ter n máquinas, que os IP's vão sendo reciclados. Exclusão de Endereços: Endereços que ã queremos que sejam atribuídos pelo DHCP a clientes da rede. Ao definirmos a exclusão d certos endereços estamos a especificar endereços que ã serão oferecidos a clientes DHCP quando estes solicitarem a configuração ao servidor DHCP. Reserva de Endereços: Uma reserva é quando um endereço IP é atribuído permanentemente a um cliente específico. Uma reserva é feita com base no endereço MAC do dispositivo.

Funcionalidades decorrentes da utilização de NTFS

- O sistema de arquivos NTFS, introduzido na primeira versão do Windows NT, é um sistema de arquivos completamente diferente do FAT. Ele oferece segurança muito melhor, compactação arquivo por arquivo, cotas e até criptografia. É o sistema de arquivos padrão para novas instalações do Windows XP.
- O sistema de arquivos NTFS geralmente não é compatível com outros sistemas operacionais instalados no mesmo computador e não está disponível se você iniciou o computador a partir de uma unidade de disquete. Por isso, muitos administradores de sistemas, costumam recomendar que os utilizadores formatem pelo menos uma pequena partição no começo do disco rígido principal como FAT. Essa partição ofereceu um local para armazenar arquivos de recuperação emergenciais.

2. Agendamento De Tarefas Linux

Objectivos de aprendizagem

- Distinguir alternativas de calendarização
- Configurar tarefas, recorrendo aos respectivos comandos e ficheiros de configuração.

Agendamento de tarefas

- “Serviços” **crond** e **anacron**:

O **crond** é um daemon do sistema cuja a função é executar comandos e programas em datas e horários determinados. Possui um arquivo de configuração, **/etc/crontab**, onde são especificados os comandos ou programas a serem executados. Possui também um diretório, **/var/spool/cron**, onde se encontram os arquivos **crontab** dos usuários.

A sintaxe do arquivo **/etc/crontab** é:

```
<minuto><hora><dia_do_mes><mes><dia_da_semana><usuário><comando>
```

Um asterisco "*" pode ser utilizado para indicar qualquer valor permitido a qualquer campo.

Exemplo de entrada do arquivo **/etc/crontab**:

```
30 23 * 1-12 1-6 root /usr/local/scripts/bkpggeral.sh
```

Essa entrada solicita ao daemon **crond** que execute o script de backup, como superusuário (root), de segunda à sábado, de janeiro a dezembro, às 23:30h.

Eventuais mensagens de erro são enviadas para o e-mail do usuário root.

Exemplo real do arquivo **/etc/crontab**:

```
# /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/
#run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * * root run-parts /etc/cron.weekly
42 4 * * * root run-parts /etc/cron.monthly
```

Essas entradas solicitam ao daemon **crond** que execute o programa **run-parts** em datas e horários determinados. Esse programa executa os Scripts de shell, comandos e programas existentes nos diretórios a seguir.

Diretorio - Descrição

/etc/cron.hourly - A aplicação será executada toda hora.

/etc/cron.daily - A aplicação será executada todo dia.

/etc/cron.weekly - A aplicação será executada uma vez por semana.

/etc/cron.monthly - A aplicação será executada uma vez por mês.

- **cron**
Quando existem tarefas, realiza-as e procede à sua verificação cada minuto, se o pc estiver desligado, esta morre (tarefa).
- O comando **CRONTAB**
É possível criar arquivos **crontab** individuais para que cada usuário possa definir suas próprias tarefas rotineiras, que são executadas automaticamente. Esses arquivos **crontab** estão localizados no directório **/var/spool/cron** e não podem ser editados directamente, sendo esta função realizada pelo comando **crontab**.

Instala, lista ou remove o arquivo **crontab** de usuário. A permissão para usar o comando **crontab** é determinada pelos arquivos **/etc/cron.allow** e **/etc/cron.deny**. Se o arquivo **/etc/cron.allow** existir, somente os usuários mencionados neste será permitido usar o comando **crontab**. Se o arquivo **/etc/cron.allow** não existir, é verificada a existência do arquivo **/etc/cron.deny** e todos os usuários não mencionados no mesmo receberão permissão para usar o comando **crontab**. Se nenhum destes existir, somente o superusuário terá permissão o comando **crontab**. Um arquivo **/etc/cron.deny** vazio significa que todos os usuários têm permissão para usar o comando **crontab**, sendo esta a configuração-padrão.

- **Anacron**

Garante que todas as tarefas sejam realizadas, nem que seja depois de um ano, basta a máquina estar ligada que ele põe em dia o que ta atrasado.

3. Gestao de Aplicacoes

Objectivos de aprendizagem

- Descrever processos de instalação de aplicações consoante o sistema operativo
- Comparar abordagens de gestão de aplicações consoante o sistema operativo
- Descrever a invocação de aplicações, via interface gráfica, consoante o sistema operativo
- Descrever a invocação, via linha de comando, consoante o sistema operativo

4. Gestao Utilizadores Linux

Objectivos de aprendizagem

- Identificar ficheiros de configuração relacionados com manutenção de utilizadores
- Criar e parametrizar contas de utilizadores manipulando directamente os ficheiros e directorias envolvidos
- Utilizar ferramentas para criação e parametrização das contas dos utilizadores
- Identificar aspectos relacionados com a mudança de identidade

Gestão de Utilizadores (Linux)

Como você já deve saber, o Linux é um sistema multi-usuário, então, é claro que não só pode existir um usuário usando o sistema. Uma primeira coisa que podemos dizer é que o Linux não pode de alguma maneira ser usada sem estar sendo um usuário. O usuário **'root'** é o administrador do sistema, e é ele quem você vai usar primeiro para criar outros usuários depois (a não ser que você tenha criado um usuário comum durante a instalação do seu Linux).

Antes de mais nada, fique sabendo que o **root** é um usuário especial, ele pode fazer TUDO em seu sistema, não importa o que acontecer, ele faz. Ao contrário dos usuários comuns, que têm restrições. Se você já instalou algum Linux, você verá que a primeira coisa que você irá fazer antes de usar o sistema é se logar como **root**, ou seja, preencher aquele campo login: com o usuário **root**. Mas aí por alguma razão você quer mudar de usuário, ou criar outro, ou qualquer coisa do tipo, então você se pergunta: "Como?"

Há um comando específico para isto. Este comando é o **"adduser"** ou **"useradd"**. Dependendo da distribuição, o comando **"adduser"** vai ser apenas um comando igual ao **"useradd"**, ou então um script interativo que irá lhe fazendo perguntas, você irá preenchendo, e então o script criará um usuário no sistema para você.

No caso do **"adduser"** ser um comando mesmo, você poderá utilizar assim:

adduser hugo

passwd hugo

Isso respectivamente irá criar um usuário padrão chamado hugo, e depois com o comando "**passwd**", você definirá uma senha para este usuário. Você pode especificar outros parâmetros para o usuário, como no comando a seguir:

adduser hugo -d /var/usuarios/hugo -s /dev/null

Com estes parâmetros, especifiquei que o usuário hugo terá como directório **home** o "**/var/usuarios/hugo**" e como shell o "**/dev/null**" (ou seja, não terá shell). Sem estes parâmetros, o directório home seria "**/home/hugo**" e o shell seria "**/bin/bash**".

Vamos entender agora como este comando funciona, que é uma coisa essencial que todos deveriam saber em relação ao sistema Linux. Cada um desses programas escrevem o usuário no arquivo de configuração do Linux referente aos usuários do sistema. Este arquivo é o "**/etc/passwd**". Cada linha deste arquivo é um usuário cadastrado no sistema. Com as informações que vou lhe dar aqui, você pode muito bem criar uma conta sem usar estes programas/scripts citados acima.

O passwd é formado por linhas onde cada linha é um usuário, como falei acima, então vamos aprender a montar cada linha desta. Vou pegar um exemplo para vocês:

hugo:x:1001:100:Hugo Cisneiros:/home/hugo:/bin/bash

Vamos dividir esta linha em "campos", onde cada um é separado por : (dois pontos), olhe só:

Campo	Significado
hugo	Login do Usuário, aqui você pode colocar o nome que quiser com até 8 caracteres.
x	Aqui diz que o password está no arquivo /etc/shadow. Se estivesse *, a conta estaria desabilitada, e se estivesse sem nada (:), a conta não teria password.
1001	UID (User IDentification), o número de identificação do usuário.
100	GID (Group IDentification), o número de identificação do grupo do usuário.
Hugo Cisneiros	Comentários do usuário, como nome, telefone, etc
/home/hugo	O directório HOME do usuário, ou seja, o directório pertencente a ele. Geralmente estes directórios sempre estão no /home
/bin/bash	Shell do usuário, ou seja, o programa que irá interpretar os comandos que o usuário executar.

Obs: O **/etc/shadow** é um arquivo que contém a senha do usuário criptografada, se alguém tiver posse dela, esta pessoa pode muito bem comparar as senhas com uma lista de palavras, e pode descobrir as senhas dos usuários. Felizmente este arquivo está muito bem protegido pelo sistema :)

Bem, legal, aprendi sobre adicionar um usuário, mas como faço para removê-lo? Simples, você pode apagar a linha referente a ele no **/etc/passwd** e os seus arquivos, ou simplesmente digitar **userdel usuario**. Combine com a opção **-r** para deletar junto o directório HOME do usuário.

Quer deixar um utilizador como se fosse

root? O **root** possui o UID e o GID igual à 0 (zero), e um usuário comum não. Se nós forçássemos a mudança do UID e GID de um usuário para 0, ele ficaria como se fosse o root! Por exemplo, eu tenho a linha do usuário no **/etc/passwd** e mudo:

hugo:x:1001:100:Hugo Cisneiros:/home/hugo:/bin/bash

hugo:x:0:0:Hugo Cisneiros:/home/hugo:/bin/bash

Pronto, o usuário hugo vai ser também o **root** do sistema, o administrador do sistema, o deus do sistema, etc. Outra dica: Não é muito bom ficar usando o usuário **root**, este usuário é somente para a

administração do sistema, então eu recomendo à você a usar sempre um usuário normal, ser da plebe :) E se for precisar usar o **root**, logar como ele ou utilizar o comando "su -" para se tornar o próprio **root**.

Outro arquivo que tem muito haver com os usuários no Linux é o **/etc/group**. Que contém as definições de cada grupo, como por exemplo seus nomes, GIDs, e usuários adicionais que pertencem à ele. Você adicionando uma linha neste arquivo estará criando um novo grupo. Vamos criar aqui um novo grupo no **/etc/group**:

```
metal:x:666:hugo,jim,eitch
```

Adicionando esta linha acima no arquivo **/etc/group**, um novo grupo é criado: com o nome '**metal**', o GID '**666**' e como usuários adicionais pertencentes a ele, '**hugo, jim, eitch**'.

/etc/passwd

Contem informações relativas as contas de utilizadores, qualquer utilizador/aplicação tem permissões de leitura, muitos executáveis recorrem a estes ficheiros para recolher informação sobre os utilizadores. Antigamente continha password codificada, actualmente não (embora possível), recorre a shadowing 'x' no campo da password.

/etc/shadow

Contém o shadowing das passwords dos utilizadores, utilizadores "normais" não têm acesso, utiliza algoritmo de codificação MD5 de 128 bits.

5. Instalacao SO – Aspectos Diversos

Objectivos de aprendizagem

- Reconhecer eventual impossibilidade de configurar firmware para possibilitar arranque por USB
- Identificar alternativas para arranque por USB quando não suportado por firmware
- Reconhecer tipos de firmware, tradicional e moderno, em computadores pessoais
- Reconhecer esquemas preferenciais de particionamento de discos em função do tipo de firmware
- Recorrer a imagens de discos como forma de virtualização de suportes físicos
- Recorrer a dispositivos virtuais que suportem o acesso transparente a imagens de discos
- Identificar os aspectos técnicos relacionados com emulação de arquitecturas
- Identificar os aspectos técnicos relacionados com a virtualização da instalação de sistemas
- Distinguir convenientemente os cenários de emulação e virtualização

Configuração da BIOS para arranque por USB

- **Arranque por CD que transfira execução para o dispositivo USB**

Este USB Boot CD pode ser usado para arrancar um Ubuntu 8.10 drive flash USB em computadores com um BIOS que não suporta arrancar a partir de USB. O CD de inicialização contém um bootloader grub que carrega o initrd eo kernel vmlinuz a partir do CD e então começa a localizar o sistema de arquivos na unidade flash USB. Porque os drivers USB são carregados a partir do initrd no CD, a unidade flash USB podem ser facilmente detectados.

MBR versus GPT, BIOS versus EFI, Partição ESP

- **MBR(Master Boot Record)**

Ao instalar o sistema operacional, é gravado mais um componente: o gerenciador de boot, responsável por carregar o sistema durante o boot.

- Tanto o gerenciador de boot quanto a tabela de particionamento do HD são salvos no primeiro setor do HD (a famosa trilha MBR).
- **O que é um disco GPT?**
 - O GPT (Tabela de partições GUID) foi apresentado como parte da iniciativa EFI (Extensible Firmware Interface). O GPT fornece um mecanismo mais flexível para particionar discos do que o esquema antigo de particionamento MBR (Registro mestre de inicialização) comum aos PCs.
 - Partição GPT foi desenvolvida para solucionar problemas de tamanho conhecidos da partição MBR; o tamanho máximo de uma partição MBR é de 2 Terabytes (TB). As partições GPT permitem que esse limite seja excedido.
 - O esquema GPT foi implementado no Microsoft Windows XP edição x64, Windows Server 2003 (64 bits), Windows Server 2003 SP1 (todas as versões), Windows Vista e nos próximos sistemas operacionais do Windows Server com codinome Longhorn.
- **EFI (Extended Firmware Interface)**
 - É uma interface criada pela Intel para substituir BIOS. A EFI é uma especificação que define uma interface de software entre o sistema operacional e a plataforma de firmware. A EFI destina-se a ser um substituto significativamente melhorado para o velho BIOS firmware interface, historicamente usado por todos os computadores pessoais IBM PC compatíveis. A especificação EFI foi originalmente desenvolvida pela Intel, e é actualmente gerida pelo Unified EFI Forum que é oficialmente conhecido como Unified EFI (UEFI).
 - ♦ EFI requer que uma partição conhecida como uma **EFI System Partition (ESP)** esteja presente. O GNU Parted identifica a ESP como se tivesse um sinalizador de boot configurado. A ESP é por volta de 200MB de tamanho normalmente e é formatada para FAT-32. Ela retém drivers que a EFI pode usar durante o processo de boot. Esta partição não é necessária se seu computador usa o BIOS para fazer boot.

Virtualizadores (Máquinas Virtuais) versus Emuladores

- Virtualização (maquina virtual) de um sistema operativo num dado hardware, ex: virtualbox, vmware.
- Emulador: é criada uma virtualização de um dado hardware por um SO. Ex. Qemu.

6. Instalações Linux

Objectivos de aprendizagem

- Identificar formas alternativas de instalação e execução do sistema operativo Linux
- Instalar e executar o sistema operativo Linux em diversos cenários
- **GRUB, Lilo, Ntloader**, gestores de ficheiros de arranque instalados no MBR.
- Persistent: instala-se de raiz
- Live: não se instala

7. RAID

Objectivos de aprendizagem

- Explicar a validade da utilização de RAID enquanto ferramenta de segurança activa.
- Distinguir diferentes abordagens técnicas para implementação de RAID.
- Caracterizar diferentes modelos (“níveis”) de implementação de RAID.
- Descrever os aspectos relacionados com a implementação de RAID em Linux e MS Windows.

RAID

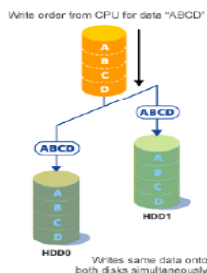
- Sistema por hardware ou software que gere vários discos como se fosse um único. Vários RAIDs (configurações) são possíveis, oferecendo mais performance e /ou mais segurança.

RAID 0

- É na verdade um RAID (perde o R de **Redundant** Array of Independent Disks): visto que não oferece segurança, só performance: Vários discos divididos em faixas são vistos como um só. Operações de escrita e de leitura são repartidas (striping) por eles em paralelo duplicando a rapidez por cada disco. 4 discos de 80 GB, por exemplo, correspondem a um único grande disco de 320 GB com velocidade quadruplicada. (convém serem idênticos, senão os maiores ficam nivelados ao disco mais lento e pequeno, por exemplo bastaria que um deles fosse de 40GB para totalizar só160MB (40MB x 4)). A segurança não é beneficiada porque não há dados duplicados (até é prejudicada visto vários discos aumentam a probabilidade de um deles falhar).
- disco virtual RAID é distribuido por faixas de K sectores, num modo round-robin.
- **Pouca segurança:** a avaria de um disco pode levar à perda de eventualmente todos os dados
- **Probabilidade de falha** do conjunto aumenta

RAID 1

- Difere num aspecto: replica (mirroring) os dados em cada disco. Como o faz em simultâneo, essa escrita replicada não é mais morosa. Porém a velocidade de leitura duplica por disco. Para além disso essas réplicas oferecem mais segurança de dados caso um disco falhe (*hot-swap* (troca à quente) permite substituição sem interrupção e com auto-sincronismo). Contudo, quanto a capacidade total, é a do disco mais pequeno visto os outros serem réplicas.



- **A informação é duplicada** noutro conjunto de discos
- **É mais seguro:** se algum disco avariar o outro tem uma cópia exacta da mesma informação.
- Mesmo com avaria de um disco o sistema pode continuar a funcionar sem interrupção
- **Performance na leitura** pode duplicar

RAID 2

- **Baixa performance**
- Os discos já tem ECC (Error Connecting Code) eles próprios
- Não há implementações comerciais por não ser economicamente viável

RAID 3

- RAID 0 (striping)+1 disco para paridade (a nível dos bytes)
- **3 ou mais discos**

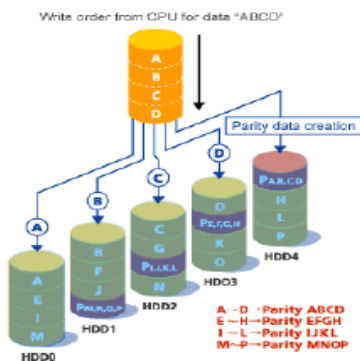
- Para ser interessante tem de ser **implementado ao nível do hardware**

RAID 4

- Dedicar um disco a paridades que permitem a reconstrução dos dados caso um dos discos falhe.
- **Alguma segurança:** em caso de avaria de um disco a informação pode ser recuperada com base no conteúdo dos outros discos
- **Performance na leitura bastante boa**
- **Performance na escrita tem alguma degradação:** a paridade tem de ser lida, recalculada e escrita de novo (ciclo read-modify-write)
- **Maior Desgaste do disco de paridade**

RAID 5

- Difere no facto de repartir essas paridades por todos os discos distribuindo a carga (esforço e usura) e ganha simultaneidade parcial de leitura e escrita.



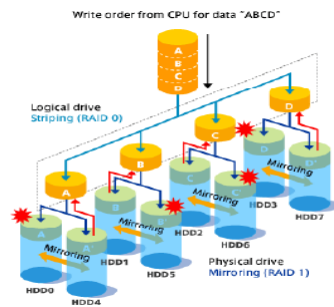
- Este nível diminui o peso no acesso ao disco de paridade, de acordo com o nível 4, distribuindo as faixas de paridade uniformemente por todos os discos segundo um esquema round-robin.

- Similar ao RAID 4 mas a paridade é distribuída pelos vários discos em vez de estar guardada num único (evita o bottleneck dos níveis 2 a 4). Relativamente ao RAID 4: Performance bastante superior (pode eventualmente haver escritas simultâneas porque as paridades estão distribuídas (mas em cada escrita continua a ter de se fazer o ciclo read-modify-write)). Relativamente ao RAID 4: mais complexo e (tipicamente) caro do que RAID 4.
- W2K3: O RAID 5 por software não pode ter o boot dentro da zona striped; Por hardware já pode (porque o sistema não "sabe" disso).

RAIDs compostos

- **Pertinência:** combinar vantagens e/ou reduzir desvantagens dos níveis simples. Nível "XY" (ou "X+Y") normalmente é entendido como 1º X, depois sobre ele Y (cada disco do Y é um RAID X). Mais relevantes: 01, 10, 05, 50, 15, 51.

- **RAID 0+1:** raid 0 dentro de raid 1
- **RAID 1+0:** raid 1 dentro de raid 0



- **RAID 5+1:** (entenda-se raid 5 dentro de raid1) Consiste em 3 discos (Raid 5) duplicados (mirroring) totalizando 3x2=6 discos.

Tabela comparativa:

RAIDs	Segurança	Vel. escrita	Vel. leitura	Capacidade	Recup.
0	- (a)	++	++	++	--
1	++	=	++	Menor disco	++(b)

4	+	-(c)	+	-1/3(d)	++
5	+	+	++	-1/3(d)	++

a) Número de discos multiplica probabilidade de falha
b) Auto-recuperação com disco suplente
c) Implica leitura-alteração-escrita das paridades
d) Espaço das paridades

Nota: Paridades: Conhecendo a soma do par e uma das partes, infere-se a parte ausente (se total = 3 e uma das partes é 1, a outra só pode ser 2, pois 1+2=3). A Tabela de Verdade usa esta lógica (*xor= ou exclusivo*): 0+0=0...0+1=1...1+0=1...1+1=0.

8. Registry

Objectivos de aprendizagem

- Identificar o tipo de informação abrangida pelo registry
- Identificar a estrutura do registry
- Relacionar a informação agregada no registry com os respectivos pontos de armazenamento
- Operar o registry a partir do editor nativo
- Manipular e exportar configurações através de ficheiros de texto
- Identificar exemplos de pertinência de manipulação do registry

Principais aspectos

Uma base de dados hierárquica central utilizada no Microsoft Windows 98, Windows CE, Windows NT e Windows 2000 para guardar informações necessárias para configurar o sistema para um ou mais utilizadores, aplicações e dispositivos de hardware.

O Registo contém informações que o Windows referencia continuamente durante o funcionamento, tais como os perfis de cada utilizador, as aplicações instaladas no computador e os tipos de documentos que cada uma pode criar, definições de folhas de propriedades para pastas e ícones de aplicações, o hardware existente no sistema e as portas que estão a ser utilizadas.

O Registo substitui a maioria dos ficheiros .ini baseados em texto utilizados nos ficheiros de configuração do Windows 3.x e do MS-DOS, como o Autoexec.bat e o Config.sys. Embora o Registo seja comum a vários sistemas operativos Windows, existem algumas diferenças entre as diferentes versões

- **Hives (Ramos)**
 - Um ramo de registo é um grupo de chaves, subchaves e valores do registo que tem um conjunto de ficheiros de suporte com cópias de segurança dos respectivos dados. Os ficheiros de suporte de todos os ramos de registo, com excepção do HKEY_CURRENT_USER, estão na pasta %SystemRoot%\System32\Config no Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 e Windows Vista. Os ficheiros de suporte de HKEY_CURRENT_USER estão na pasta %SystemRoot%\Profiles\NomeDoUtilizador. As extensões dos nomes dos ficheiros nessas pastas indicam o tipo de dados que contêm. A ausência de uma extensão também poderá indicar o tipo de dados destas pastas.

Ramo do registo	Ficheiros de suporte
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

- **Regedit.exe**

O Regedit.exe é o editor de configuração do Windows XP e do Windows Server 2003. O Regedit.exe é utilizado para modificar a base de dados de configuração do Windows NT ou o registo do Windows NT. Este editor permite visualizar ou modificar o registo do Windows NT. E permite aplicar definições de segurança nas chaves de registo, visualizar e editar REG_EXPAND_SZ e REG_MULTI_SZ e guardar e restaurar ficheiros de ramo. Do lado esquerdo, existem pastas que representam chaves de registo. Do lado direito, estão os valores associados à chave de registo seleccionada. O Regedit é uma ferramenta com muitas capacidades. Deverá ter muito cuidado quando a utilizar para alterar valores de registo. Valores em falta ou incorrectos no registo podem danificar a instalação do Windows.

- **Regedt32.exe**

No Windows XP e no Windows Server 2003, o Regedt32.exe é um pequeno programa que apenas executa o Regedit.exe.

- **Ficheiros .reg**

O Regedit.exe utiliza ficheiros .reg para importar e exportar subchaves e valores do registo. Pode utilizar estes ficheiros .reg para distribuir remotamente alterações de registo para vários computadores baseados no Windows. Quando executa um ficheiro .reg, o conteúdo do ficheiro é incluído no registo local. Consequentemente, terá de ter cuidado ao distribuir os ficheiros .reg.

9. Runlevels e Servicos em Linux

Objectivos de aprendizagem

- Explicar o processo de carregamento do sistema operativo
- Descrever o funcionamento dos diferentes níveis de execução (runlevels)
- Configurar características dos runlevels
- Relacionar runlevels com serviços em execução
- Operar alterações ao estado de execução de serviços
- Descrever processo de instalação de serviços
- Configurar serviços de forma persistente

Os níveis de execução definem como o Sistema Operacional (SO) inicializará; o Linux possui 7 níveis, e diferem de distro para distro:

0. **Halt:** desliga o sistema
1. **Modo single-user:** apenas suporta um utilizador, mas este pode lançar qualquer nº de tarefas. Os serviços de rede estão desligados.
2. **Modo multi-user sem rede (sem NFS):** suporta vários utilizadores a trabalhar na consola ou em terminais ligados directamente nas portas serie (terminais locais).
3. **Modo multi-user com rede:** suporta vários utilizadores em terminais locais ou remotos.
4. **Não utilizado.**

5. **Modo multi-user com o sistema de janelas X:** idêntico ao modo 3, mas o sistema de janelas X é lançado automaticamente.
6. **Modo de reinicialização:** reinicializa o sistema.

Falando sobre os níveis, eles permitem que eu escolha quais serviços vão iniciar ou não em cada nível; em geral, os daemons de inicialização dos serviços ficam localizados dentro de **/etc/init.d**.

Cada script do diretório **/etc/init.d** é escrito para aceitar argumentos como **start**, **stop**, **restart**, **status** e pode ser executado manualmente caso seja necessário.

Por exemplo, para parar, iniciar e restartar o daemon ssh:

```
# /etc/init.d/ssh stop
# /etc/init.d/ssh start
# /etc/init.d/ssh restart
```

Os 7 **runlevels**, que são definidos no **/etc/inittab**; uma coisa que é importante falar, é que cada **runlevel** possui seu próprio diretório, localizado dentro de **/etc**.

```
# ls -d /etc/rc?.d
```

/etc/rc?.d => irá listar os diretórios que comecem com rc com qualquer caracter onde esta o '?'.
O comando que mostra qual nível o sistema iniciou é o runlevel:

```
# runlevel
```

```
N 2
```

Acima, podemos ver que o sistema inicia no nível 2; lembrando que por padrão, sistemas Debian tem como padrão o nível 2.

Sabendo qual nível o sistema inicia, basta consultar o diretório correspondente ao nível, que no caso é o **/etc/rc2.d**.

Exemplo:

```
# ls /etc/rc2.d/
```

```
K89cron S10syslogd S11klogd S20acpid S20gpm S20makedev S20openbsd-inetd S20ssh S99rc.local
S99rmnologin S99stop-bootlogd
```

Quando você instala algum serviço na máquina, o daemon é colocado dentro de **/etc/init.d** e é criado um link para que o inicie nos runlevels de 2 a 5.

Tabela inittab

Contém a lista d tarefas k o processo init têm k realizar.

Cada linha é composta por 4 campos separadas por “:”, sendo id:runlevel:opções:nome_programa. A linha inicial serve para identificar o runlevel c/k o sistema arranca. A 1ª linha k contém realmente dados vai ser executada logo k o sistema arranque e por isso ã contem nenhum runlevel associado, para k este corra o script k executa a inicialização d todo o hardware. Depois têm se uma sequencia d 7 linhas praticamente iguais, k executam o script /etc/rc.d/rc d acordo c/o nível d execução. Nas linhas seguintes, define-se as acções para eventos ou aquando d uso d uma UPS. As 6 linhas seguintes são mt importantes pois executam o mingetty (sistema utilizado para fazer login).

Ferramenta `chkconfig`

O `chkconfig` é uma ferramenta que permite adicionar, editar ou remover serviços. Por exemplo editar os runlevels, ou seja, escolher quais os serviços que são iniciados automaticamente no arranque do computador.

O `Chkconfig` manipula as várias ligações simbólicas em `/etc/init.d/`, para aliviar um pouco os administradores de sistema da tarefa tediosa de editar manualmente as ligações simbólicas.

```
# chkconfig --level 12345 avahi-daemon off
# chkconfig --level 12345 avahi-dnscnfd off
# chkconfig --level 12345 bluetooth off
```

O comando `chkconfig` também pode ser usado para ativar e desativar serviços. O comando `chkconfig --list` exibe uma lista de serviços do sistema e se eles estão iniciados (**on**) ou parados (**off**) nos níveis de execução 0-6. No fim da lista 'a uma seção para serviços gerenciados pelo `xinetd`.

Se o comando `chkconfig --list` for usado para questionar um serviço gerenciado pelo `xinetd`, exibirá se o serviço do `xinetd` está ativado (**on**) ou desativado (**off**). Por exemplo: o comando `chkconfig --list finger` retorna o seguinte output:

```
finger    on
```

Conforme exibido, o `finger` está ativado como um serviço do `xinetd`. Se o `xinetd` estiver rodando, o `finger` estará ativado.

Se você usar `chkconfig --list` para questionar um serviço em `/etc/rc.d`, a configuração do serviço para cada nível de execução é exibida. Por exemplo: o comando `chkconfig --list httpd` retorna o seguinte output:

```
httpd    0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Scripts de configuração “rc”

Quando o sistema arranca, o processo `init` executa vários scripts de inicialização `rc` (runtime configuration) que estão na directoria `/etc/rc.d` de acordo com a tabela `/etc/inittab`, o conhecimento destes scripts é essencial para um administrador de sistemas Linux, quando bem geridos são uma ferramenta bastante poderosa e versátil que permite personalizar todo o sistema e adapta-lo as necessidades.

Daemons

Sempre que um dos serviços ou um dos componentes do sistema, pode ser implementado em user mode, é criado um programa para realizar essa tarefa. Quando o sistema arranca, os scripts `RC` lançam todos esses programas, que ficam a correr silenciosamente em background, esses programas são quase imortais, porque estão sempre presentes desde o arranque até o sistema ir abaixo, mesmo quando não estão a fazer nada. Por essa razão, é normal serem designados por daemons.

Xinetd

O `xinetd` é o principal serviço de Linux que é lançado durante o arranque do sistema pelos scripts de inicialização `/etc/rc.d`.

O serviço `inetd` (Internet Deamon) funcionou como rampa d lançamento para os serviços d rede. Ou seja, o `inetd` é o programa encarregue d lançar os restantes serviços, à medida k estes vão sendo

necessários. Recentemente o inetd foi substituído pelo xinetd, k possui funcionalidades extendidas e bastantes melhorias, tanto em termos de funcionalidades como em termos de segurança. O xinetd é o principal serviço d sistema operativo Linux e por isso costuma estar sempre instalado, mesmo em PCs que ã estão ligados em rede. Por essa razão, o xinetd deve ser lançado durante o arranque pelo script /etc/rc.d.

10. Conversoes de medidas decimais para binarias

$$1000/1024 = 0,9765625 = 97,66\%$$

$$(1000*1000)/(1024*1024) = (1000/1024)*(1000/1024) = 0,9765625*0,9765625 = 0,9765625^2 = 95,37\%$$

$$(1000*1000*1000)/(1024*1024*1024) = (1000/1024)*(1000/1024)*(1000/1024) = 0,9765625*0,9765625*0,9765625 = 0,9765625^3 = 93,13\%$$

$$(1000*1000*1000*1000)/(1024*1024*1024*1024) = (1000/1024)*(1000/1024)*(1000/1024)*(1000/1024) = 0,9765625*0,9765625*0,9765625*0,9765625 = 0,9765625^4 = 90,95\%$$

$$K = (1000/1024)^1 \text{ Ki}$$

$$M = (1000/1024)^2 \text{ Mi}$$

$$G = (1000/1024)^3 \text{ Gi}$$

$$T = (1000/1024)^4 \text{ Ti}$$

--

exemplos, para K, M, G, T decimais,

$$16K = 16 * 0,9765625^1 = 15,655 \text{ Ki}$$

$$16M = 16 * 0,9765625^2 = 15,2587890625 \text{ Mi}$$

$$16G = 16 * 0,9765625^3 = 14,901161193847656 \text{ Gi}$$

$$16T = 16 * 0,9765625^4 = 14,551915228366852 \text{ Ti}$$