

Capítulo 1

Qual Unix usar ?

Na implementação de um servidor de Rede sempre surge a dúvida : Qual Unix eu devo usar ? Linux, FreeBSD, Solaris, HP-UX, etc. Qual deles ?

Muitos pontos devem ser ponderados. A finalidade, a facilidade de uso, disponibilidade de recursos, conhecimentos em Unix, etc.

Uma listagem de distribuições Linux e *BSD, com detalhes, pode ser obtida nos seguintes URLs : (www.distrowatch.com) (www.ugu.com)

É difícil escolher o que melhor atende suas necessidades. Deve-se conhecer bem as distribuições e escolher a ideal para cada caso.

Como diz um velho ditado: O ideal ainda é desconhecido. O real está mais próximo e dá para entender.

O servidor Unix ideal é aquele que lhe oferece, dentre muitos itens, os mais básicos:

1.1 Atender as necessidades:

Todo S.O. Unix (www.unix.org) deve atender as necessidades básicas de um Servidor de Redes, por exemplo: E-Mail, FTP, WEB, DNS, dentre outros serviços. Se for Linux, *BSD, ou Unix comercial, tais necessidades já são prontamente atendidas.

Tem que atender também as necessidades futuras. Novos serviços sempre são solicitados.

Constantes adaptações e modificações são necessárias e também devem ser atendidas. Aumento das capacidades, melhoria da performance, refinamento do servidor, etc, são exigências constantes. Integração com outros Sistemas Operacionais, tais como o Windows, Mac OS, etc.

Os serviços de Rede devem ser considerados como ferramentas prontas e disponíveis em praticamente todas as distribuições Unix/Linux. O Unix é o principal Sistema Operacional que provê serviços de rede atualmente. Sem ele a Internet praticamente não existiria.

É o mínimo que eles podem oferecer. E fazem isso muito bem. Melhor que muitos outros Sistemas Operacionais não Unix, comerciais ou não.

Praticamente todos os Unix oferecem estes recursos, atende as mais diversas necessidades e não tem custos exorbitantes. Será que os Sistemas Operacionais de código fechado são tão bons assim ? Pelo menos os Unix atendem muito bem as necessidades, sejam elas banco de dados, servidores de Rede TCP/IP, Backup, alta disponibilidade, dentre outras.

A portabilidade (de aplicativos e do Sistema Operacional) também deve ser mantida.

1.2 Facilidade de uso:

Conhecimentos básicos de Unix é o mínimo necessário. Os Unix se diferenciam em poucos aspectos e funcionalidades. Todo Unix apresenta compatibilidade com o Padrão POSIX (Portable Operation System Interface) - (www.posix.org).

Linus Torvalds, quando criou o Linux (www.linux.org), criou ele nos padrões "POSIX", que é o mesmo padrão que os Unix usam.

É por esse mesmo uso do padrão POSIX que o Linux é parecido com o Unix. Além do mais, existem vários tipos de Unix, que têm seu código-fonte fechado, e pago.

O Linux não é Unix. O Linux é um Unix.

O Unix foi um sistema criado e registrado pela Unix Lab. Todos os sistemas baseados naqueles códigos são chamados de uma forma geral de Unix.

Linux foi escrito desde o início pelo Linus Torvalds e não contém nenhuma linha de código do Unix. Mas o Linux foi escrito para ser conforme o padrão POSIX, que deve ser o padrão da API (Application Programming Interface) Unix, que em última análise pode ser resumido como sendo as chamadas do sistema. Por isso se diz que o Linux é um Unix (não Unix).

Por causa da API POSIX, do conjunto de utilitários (FSF/GNU em sua maioria) e do uso do X-Window (XFree - www.xfree.org) o Linux é tão parecido com o Unix que existe empresas que usam o Linux para desenvolver para Unix que não seja o dela mesma (por exemplo a IBM).

Treinamento em Unix é fundamental nos dias de hoje. Quem não tem conhecimentos em Unix (e seus derivados) está fora de sintonia com o mercado. Há muita discussão acerca dos custos de treinamento em Linux.

Na Internet e' facil encontrar muitos sites dedicados a fazer comparações e análise de performance dos Sistemas Operacionais existentes, servidores, Servidores WEB, Redes, Hardware, etc. (www.osopiniom.com) (www.netcraft.com)

Para quem pretende ficar preso a teconologias fechadas, código-fonte fechado, dependência eterna do fabricante, sistema fechado é uma boa opção. O Marketing é cruel e não respeita fronteiras.

1.3 Atualização dos softwares:

Os servidores devem ser sempre atualizados. O Sistema Operacional Unix escolhido deve permitir atualizações.

Podem sofrer Upgrades de versão ou ser substituídos por outra versão mais recente, mantendo compatibilidade com a versão anterior.

Uma distribuição Linux que faz isso muito bem é a Debian Linux (www.debian.org). As ferramentas de atualização do Debian proliferaram muito no mundo Linux. Muitas outras surgiram e funcionam de forma parecida com as ferramentas do Linux Debian.

São ferramentas baseadas em Software Livre, de livre distribuição.

A última versão, ou a mais estável, de cada serviço instalado, por exemplo, o Servidor de E-Mail, disponibilizada pelo fabricante traz as últimas correções e os recursos mais novos implementados.

É fundamental ter todos os Softwares servidores atualizados.

As falhas encontradas nas versões anteriores são corrigidas e disponibilizadas novas versões. Para Software código-fonte aberto ou fechado deve ser assim. É a garantia do produto.

Há muitas maneiras de atualizar os Softwares servidores. Vão desde a recompilação de todo o software servidor (o principal e os auxiliares) até a troca do Sistema Operacional, parcial ou integral.

Um vício de muitos Administradores FreeBSD é recompilar todo o Sistema Operacional e o Kernel e, depois disso tudo feito, adicionar os novos **ports** (pacotes) e configurá-los. O Sistema Operacional está praticamente novo, de acordo com os programas e códigos-fonte mais novos e mais confiáveis, patches aplicados, livres de problemas, bugs, etc.

No Linux, a compilação do Kernel (www.kernel.org) já é tarefa comum e serve para alcançar uma melhor performance e ajustes de acordo com o Hardware do Servidor de Rede. É raro recompilar todo o Sistema Operacional, mas tem como ser feito.

Nos Unixes comerciais essa tarefa é mais complicada, uma vez que o código fonte não é disponibilizado. É guardado nos cofres do fabricante. Segredo de fábrica.

É possível trabalhar com módulos do Kernel. A atualização nos Unix comerciais envolve custos e softwares fornecidos apenas pelos fabricantes.

Com a experiência a atualização torna-se tarefa rotineira e simples de se fazer.

Cuidados com Backup do S.O., dados dos usuários, dos Softwares instalados e outros itens, fazem parte da rotina de uma boa administração.

1.4 Segurança

É o item mais preocupante nos Sistemas Operacionais existentes.

Partindo do princípio de que quanto mais conectado, mais vulnerável se está, a disponibilidade e a segurança se tornam preocupantes e dignos de serem bem cuidados. Vide pacotes de correção para Microsoft (Services Pack, ou BUG PACK :), patches para Unix, Linux, *BSD, dentre outros.

A contribuição da Internet para a ampla divulgação do Software Livre é muito grande. O preço é a questão da Segurança.

Graças à Internet, muitos problemas foram encontrados (e resolvidos) nos serviços de rede, nos aplicativos, nos S.O., e a segurança dos mesmos aumentou. Muitos serviços de rede, tais como o Servidor de E-Mail Sendmail (www.sendmail.org) e o Bind (www.isc.org/sw/bind/) sofreram inúmeros ataques durante muito tempo.

O Software Livre mostrou os problemas e a comunidade de Software Livre, juntamente com os projetistas do Sendmail e Bind resolveram inúmeros problemas. Os serviços agora estão livres de muitos problemas e apresentam melhor desempenho.

É lógico que as correções e adaptações, melhorias, modificações, etc, não param. Estão sempre procurando fazer melhorias nos produtos.

Novos servidores de E-Mail apareceram e se apresentam melhores, mais bem elaborados e mais eficientes que seus antecessores. É o caso do QMAIL (www.qmail.org) e do Postfix (www.postfix.org), dentre outros.

O mesmo aconteceu com muitos produtos, nas diversas plataformas de Hardware existentes.

O Windows que o diga ...

O Sistema Operacional OpenBSD (www.openbsd.org) é tido como o mais seguro da atualidade.

Totalmente de livre distribuição, exige bons conhecimentos de Unix e pode ser usado em pequenos computadores.

É o S.O. mais indicado para Segurança, Firewalls, Proxy e serviços de rede. Há também muitas distribuições Linux destinadas a trabalhar com um alto grau de Segurança.

Bons conhecimentos de Unix e um profundo conhecimento de Redes TCP/IP são exigidos. Conhecer muita coisa assim não é para qualquer um. Dedique-se e mantenha-se constantemente atualizado.

Ainda não há ferramentas "clicáveis" (O Windows gosta disso...) que resolva problemas de segurança em Sistemas Operacionais e Redes TCP/IP.

Vírus e SPAM sempre estarão presentes. Quem eliminar estes dois problemas merece um prêmio Nobel, e até mais que isso. (www.cirp.usp.br/secoes/screde/virus/tudovi.html) (cirp.usp.br/Virus/spam.html)

O Unix não sofre tanto com vírus, pelo menos por enquanto. Com a proliferação do Linux os vírus vão infernizar a vida dos usuários Linux.

O mundo do Software Livre tem que se preparar para isso. Já tem Antivírus para Software Livre. Um exemplo é o CLAMAV (www.clamav.net), dentre outros. Os fabricantes mais tradicionais de AntiVírus já disponibilizam a muito tempo AntiVirus para Servidores Unix.

Treínamento é fundamental !

A atualização e troca de conhecimentos também exige que os Administradores de Sistemas fiquem em constante estado de alerta e sempre atualizados fazendo cursos, assistindo palestras, seminários, congressos e participar ativamente de listas de discussão.

(www.ssi.org.br) (www.security.unicamp.br) (www.linuxsecurity.com) (www.unixsecurity.com)
(www.nbso.nic.br)

Muitos cursos relacionados a segurança são amplamente divulgados e os pré-requisitos mais exigidos são Redes TCP/IP e Linguagens de programação, além de conhecimento técnico de elementos de Hardware e Informática.

Nos cursos de graduação, a disciplina Redes de Computadores (TCP/IP) já faz parte do elenco de disciplinas dos primeiros Semestres. Há dez anos atrás era assunto de Pós-Graduação.

Alguma coisa mudou : a necessidade de conhecimento mais amplo e atualização constante.

No site (www.levenez.com/unix/) é possível conhecer a história de todos os Unix existentes, sua evolução e variações desde sua criação.

1.5 Hardware

Escolher Hardware não é uma tarefa fácil. Um bom equipamento ajuda, boas placas de rede e CPU com bom desempenho.

Há Hardwares especialmente dedicados a servidores. Depende de quanto dinheiro tem para gastar.

Não é necessário um poderoso servidor, de última geração, com tecnologias mais recentes para montar um simples servidor de E-Mails.

Nada exagerado para simples aplicações. Não precisa se ter o melhor e modelo mais novo do mercado.

A preocupação maior deve ser em reposição de peças e compatibilidade entre elas.

Escolher um Servidor com estas características não é fácil. Consulte sempre as listas de discussão de Hardware e escolha os mais apropriados (de acordo com as condições financeiras) para servidor.

Há pessoas e empresas especializadas nos diversos itens de Hardware. Uma rede bastante uniforme, com placas e equipamentos de um único modelo, marca e fabricante é uma boa solução. Adote um padrão. Os Desktops e servidores devem possuir, quando possível, placas de rede de uma mesma linha, único modelo e fabricante. Os demais equipamentos de rede também.

Dimensionar os Discos do servidor, nunca fazer apenas uma partição. Elaborar um esquema de partições adaptados às suas necessidades. Dimensionar os tamanhos das partições e prever expansões.

Elabore sempre um Sistema de Backup, em qualquer mídia, mas sempre tenha um. Backups parciais e Backups completos, periodicidade e facilidade de manipulação. Enfim, tenha uma política de Backup. Há inúmeros Softwares para Backup, comerciais e baseados em Software Livre. Para equipamentos com Hardware dedicado sempre há uma linha de Unix apropriada e dedicada.

Geralmente quem faz o Hardware faz o Sistema Operacional. É o caso da SUN com o Solaris, IBM com o AIX, HP com o HP-UX, dentre outras. São alguns dos Unix comerciais.

O Unix NetBSD pode ser instalado numa extensa lista de Hardware (www.netbsd.org).

Outros Unixes são mais limitados e podem ser instalados em poucos tipos de Hardware.

(www.guiadohardware.net) .

Procure sempre analisar o Unix que deseja instalar e o Hardware que pretende utilizar. A aplicação é quem vai definir praticamente tudo.

Se optar por Linux, consulte a lista de Hardware compatível, distribuição que melhor se adapta a certos elementos de Hardware, compatibilidade, performance, drivers, etc. A documentação do Unix escolhido traz estas informações.

Não há um tipo de Hardware que suporte todos os tipos de Unix e

Não há um tipo de Unix para todos os tipos de Hardware.

1.6 Enfim, qual Unix usar ?

A escolha do Unix mais apropriado ao seu Servidor de Rede vai depender da análise que foi feita e das conclusões a que se chegou.

Para Software Livre tem mais de cem distribuições Linux. Para Unix BSD tem menos de dez atualmente. Para Unix comercial tem bastante também.

Começar por um Unix é o melhor conselho. Treinar bem neste Unix escolhido e aprofundar nos conhecimentos de Rede e Sistemas Operacionais também é fundamental. Depois dessa fase deve-se analisar os outros Unix, com bons olhos e com bastante senso crítico. Assim, chega-se bem próximo do Unix perfeito, ou seja, aquele que mais lhe agrada, você domina totalmente, atende a todas as suas necessidades e está pronto para novos desafios.

Tudo depende das necessidades e performance desejada.

Alguns cuidados que devem ser tomados na escolha do Unix:

- Continuidade da distribuição escolhida
- Suporte técnico
- Atualização
- Compatibilidade com Hardware
- Softwares estáveis e confiáveis
- Portabilidade
- Escalabilidade
- Estabilidade
- Gerenciamento de memória
- Administração simplificada
- Documentação
- outros

Alguns erros cometidos na escolha do Unix:

- Escolha pelo mais famoso
- Falta de conhecimento
- Vivência
- Falta de orientação técnica
- Instalações inadequadas
- Hardware obsoleto e/ou inadequado
- Unix grátis —> suporte técnico gratuito ?
- Excesso de Hardware
- Excesso de Software para instalar
- Incompatibilidade de softwares aplicativos
- outros

Depois de ter escolhido o Unix o próximo passo é efetuar a instalação. A lista de detalhes é extensa e apropriada para um outro artigo.