

USANDO O LINUX

3.1 Introdução

Antes que você possa se tornar um administrador eficaz de sistemas Linux, você deve ser capaz de usar o Linux como desktop e ter proficiência em habilidades básicas de Tecnologia da Informação e Comunicação (TIC). Não só ajudará quando você estiver lidando com usuários, mas também imersão no Linux ajudará a melhorar suas habilidades mais rapidamente. Além disso, a vida de um administrador de sistemas é mais do que apenas trabalho de servidor - há e-mail e documentação para fazer!

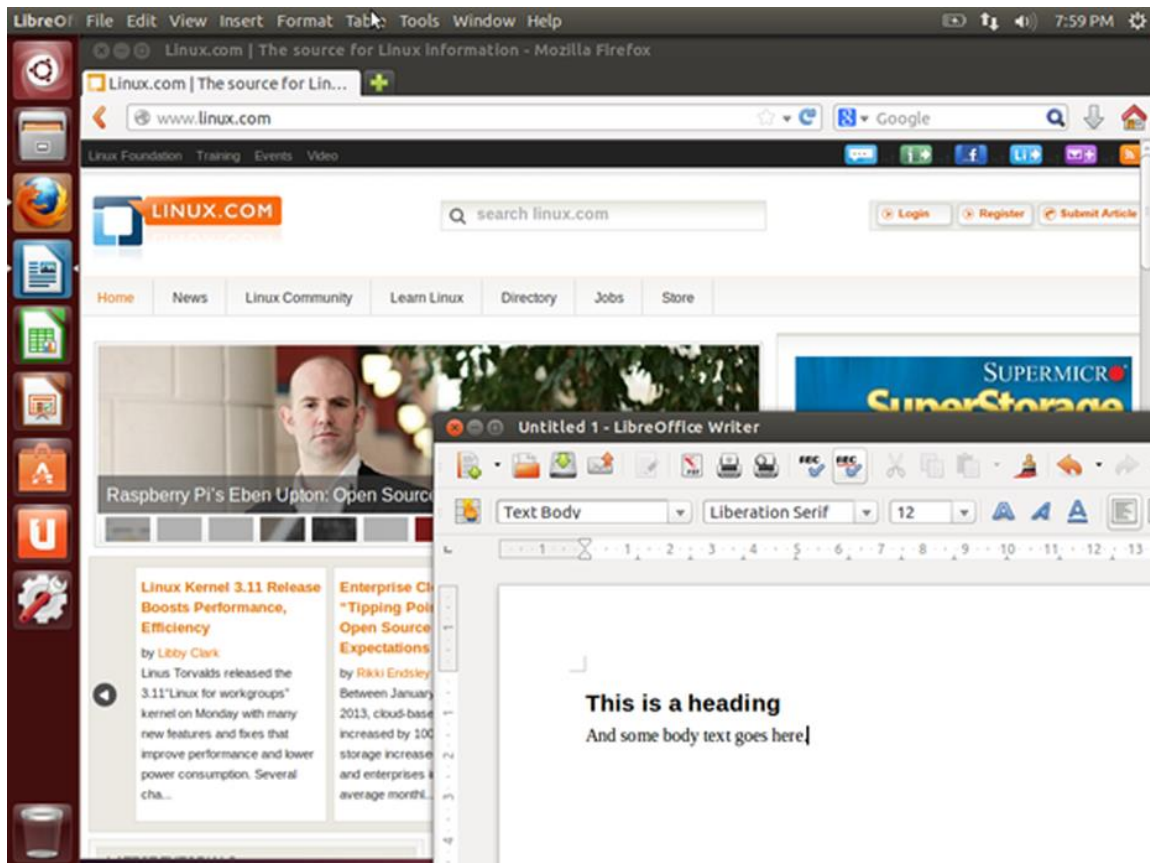
**The top Linux position IT Hiring Managers
are looking for?**

Systems Administrators

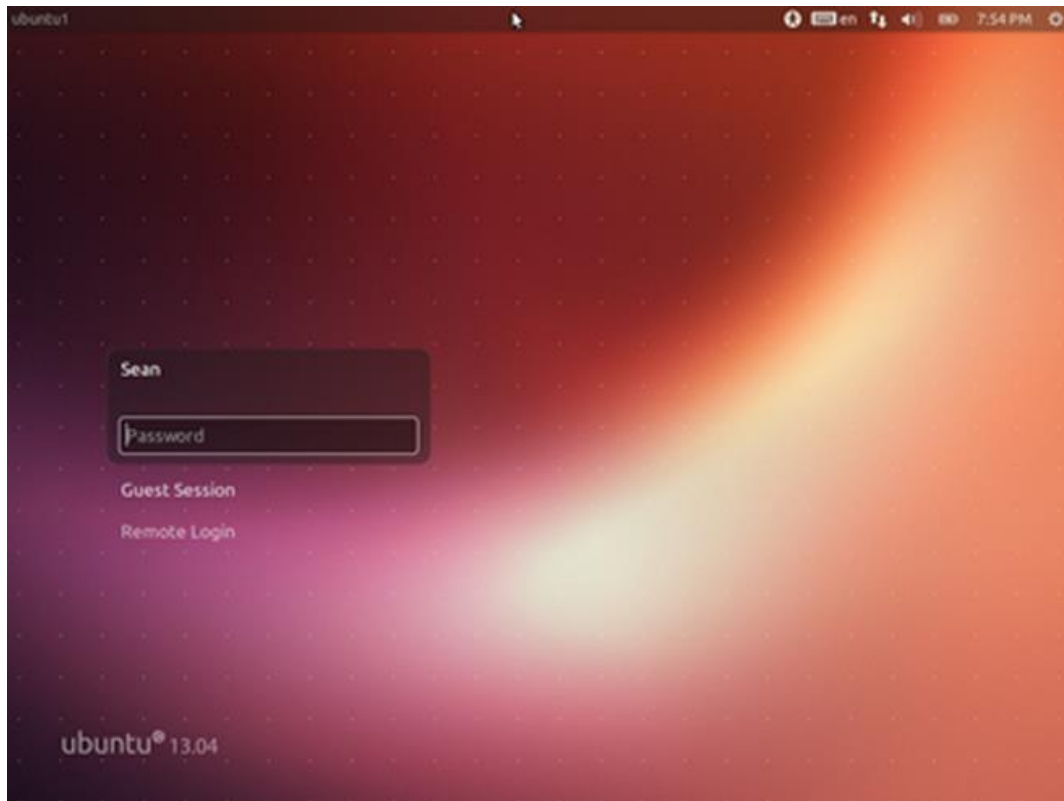
*- 2013 Linux Job Report,
Linux Foundation & Dice*

3.2 Modo Gráfico vs. Não-Gráfico

O Linux pode ser usado de duas maneiras: graficamente e não graficamente. No modo gráfico, seus aplicativos residem em janelas que você pode redimensionar e movimentar. Você tem menus e ferramentas para ajudar a encontrar o que procura. É aqui que você usará um navegador da Web, suas ferramentas de edição de imagens e seu e-mail. Aqui vemos um exemplo da área de trabalho gráfica, com uma barra de menu de aplicativos populares à esquerda e um documento do LibreOffice sendo editado com um navegador da Web em segundo plano.



No modo gráfico, você pode ter vários shells abertos, o que é muito útil quando você está executando tarefas em vários computadores remotos. Você até faz login com seu nome de usuário e senha por meio de uma interface gráfica. Um exemplo de login gráfico é mostrado na figura abaixo.



Após o login, você é levado para a área de trabalho, onde você pode carregar aplicativos.

O modo não gráfico começa com um login baseado em texto, mostrado abaixo. Você é simplesmente solicitado para o seu nome de usuário e depois disso, sua senha. Se o login for bem sucedido, você será levado diretamente para um shell.

```
ubuntu 13.04 ubuntu tty2
```

```
ubuntu login:
```

No modo não gráfico, não há janelas para se movimentar. Mesmo que você tenha editores de texto, navegadores da web e clientes de e-mail, eles são apenas de texto. É assim que o UNIX começou antes que os ambientes gráficos fossem a norma. A maioria dos servidores também executa nesse modo, pois as pessoas não fazem login diretamente, o que torna a interface gráfica um desperdício de recursos. Aqui está um exemplo da tela que você pode ver depois de efetuar login.

```
ubuntu 13.04 ubuntu tty2

ubuntu login: grace
Password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-19-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

212 packages can be updated.
91 updates are security updates.

grace@ubuntu:~$ w

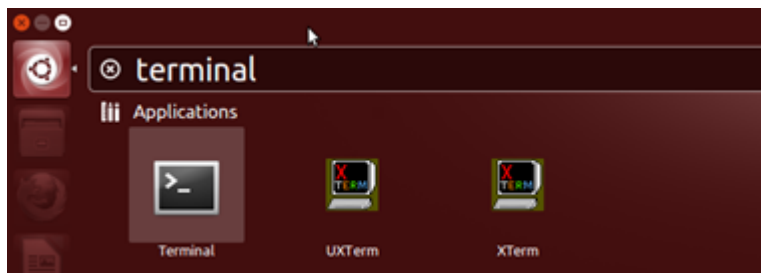
 17:27:22 up 14 min,  2 users,  load average: 1.73, 1.83, 1.69
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
grace     tty2                    20:08    14.35  0.05s  0.00s w
```

Você pode ver o prompt original para fazer login na parte superior com o texto mais recente adicionado abaixo. Durante o login, você pode ver algumas mensagens, chamadas de mensagem do dia (MOTD), que é uma oportunidade para o administrador de sistemas passar informações aos usuários. Após o MOTD é o prompt de comando. No exemplo acima, o usuário digitou o comando `w`, que mostra quem está conectado. À medida que novos comandos são inseridos e processados, a janela rola para cima e o texto mais antigo é perdido na parte superior. O próprio terminal é responsável por manter qualquer histórico, como permitir que o usuário role para cima e veja os comandos inseridos anteriormente. No que diz respeito ao Linux, o que está na tela é tudo o que existe. Não há nada para se mover.

3.3 Linha de Comando

A *linha de comando* é uma entrada de texto simples que permite inserir qualquer coisa, desde comandos de uma palavra até scripts complicados. Se você fizer login no modo de texto, estará imediatamente no console. Se você fizer login graficamente, será necessário iniciar um shell gráfico, que é apenas um console de texto com uma janela ao redor, para que você possa redimensioná-lo e movê-lo.

Cada desktop Linux é diferente, então você terá que procurar nos seus menus uma opção chamada **terminal** ou **x-term**. Ambas são shells gráficas, diferindo principalmente em aparências e não em funcionalidade. Se você tem uma ferramenta de busca como o Ubuntu One, você pode procurar pelo **terminal**, como mostrado aqui.



Essas ferramentas permitem que você pesquise rapidamente no seu sistema exatamente o que deseja executar, em vez de procurar pelos menus.

3.4 Virtualização e Computação em Nuvem

O Linux é um **sistema operacional multiusuário**, o que significa que muitos usuários diferentes podem trabalhar no mesmo sistema simultaneamente e, na maioria das vezes, não podem prejudicar outros usuários. No entanto, isso tem limitações - os usuários podem ocupar espaço em disco ou ocupar muita memória ou recursos da CPU e tornar o sistema lento para todos. Compartilhar o sistema no modo multiusuário também exige que todos sejam executados como usuários sem privilégios, portanto, permitir que cada usuário execute seu próprio servidor da Web é muito difícil.

A virtualização é o processo em que um computador físico, chamado de **host**, executa várias cópias de um sistema operacional, cada qual chamado de **guest** (convidado). O host executa o software chamado **hypervisor**, que alterna o controle entre os vários convidados, assim como o kernel do Linux faz para processos individuais.

A virtualização funciona porque os servidores passam a maior parte do tempo ociosos e não precisam de recursos físicos, como um monitor e um teclado. Agora você pode pegar uma CPU poderosa e distribuí-la por várias máquinas virtuais e manter um compartilhamento mais equitativo entre os guests do que é possível em um sistema Linux básico. A principal limitação é geralmente a memória e com os avanços na tecnologia de hypervisor e CPUs é possível colocar mais máquinas virtuais em um host do que nunca.

Em um ambiente virtualizado, um host pode executar dezenas de sistemas operacionais guests e, com o suporte da própria CPU, os guests nem sabem que estão sendo executados em uma máquina virtual. Cada convidado recebe sua própria CPU virtual, RAM e disco, e se comunica com a rede por conta própria. Nem é necessário executar o mesmo sistema operacional em todos os guests, o que reduz ainda mais o número de servidores físicos necessários.

A virtualização oferece um caminho para uma empresa reduzir o uso de energia e reduzir o espaço do datacenter em uma frota equivalente de servidores físicos. Os convidados agora são apenas configurações de software, por isso é fácil criar uma nova máquina para testá-la e destruí-la quando sua utilidade tiver passado.

Se for possível executar várias instâncias de um sistema operacional em uma máquina física e se conectar a ela pela rede, a localização da máquina não será realmente importante. A **computação em nuvem** adota essa abordagem e permite que você tenha uma máquina virtual em um datacenter remoto que você não possui e pague apenas pelos recursos que você usa. Os fornecedores de computação em nuvem podem aproveitar as escalas da economia para oferecer recursos de computação a preços melhores do que custaria para adquirir seu próprio hardware, espaço e resfriamento.

Servidores virtuais são apenas uma faceta da computação em nuvem. Você também pode obter armazenamento de arquivos, bancos de dados ou até mesmo software. A chave na maioria desses produtos é que você paga pelo que usa, como uma certa quantia por gigabyte de dados por mês, em vez de comprar o hardware e o software e hospedá-lo por conta própria.

Algumas situações são mais adequadas para a nuvem do que outras. Segurança e desempenho são geralmente os primeiros itens a aparecer, seguidos pelo custo e funcionalidade.

O Linux desempenha um papel fundamental na computação em nuvem. A maioria dos servidores virtuais é baseada em algum tipo de kernel Linux e o Linux é frequentemente usado para hospedar os aplicativos por trás dos serviços de computação em nuvem.

3.5 Utilizando o Linux para Trabalho

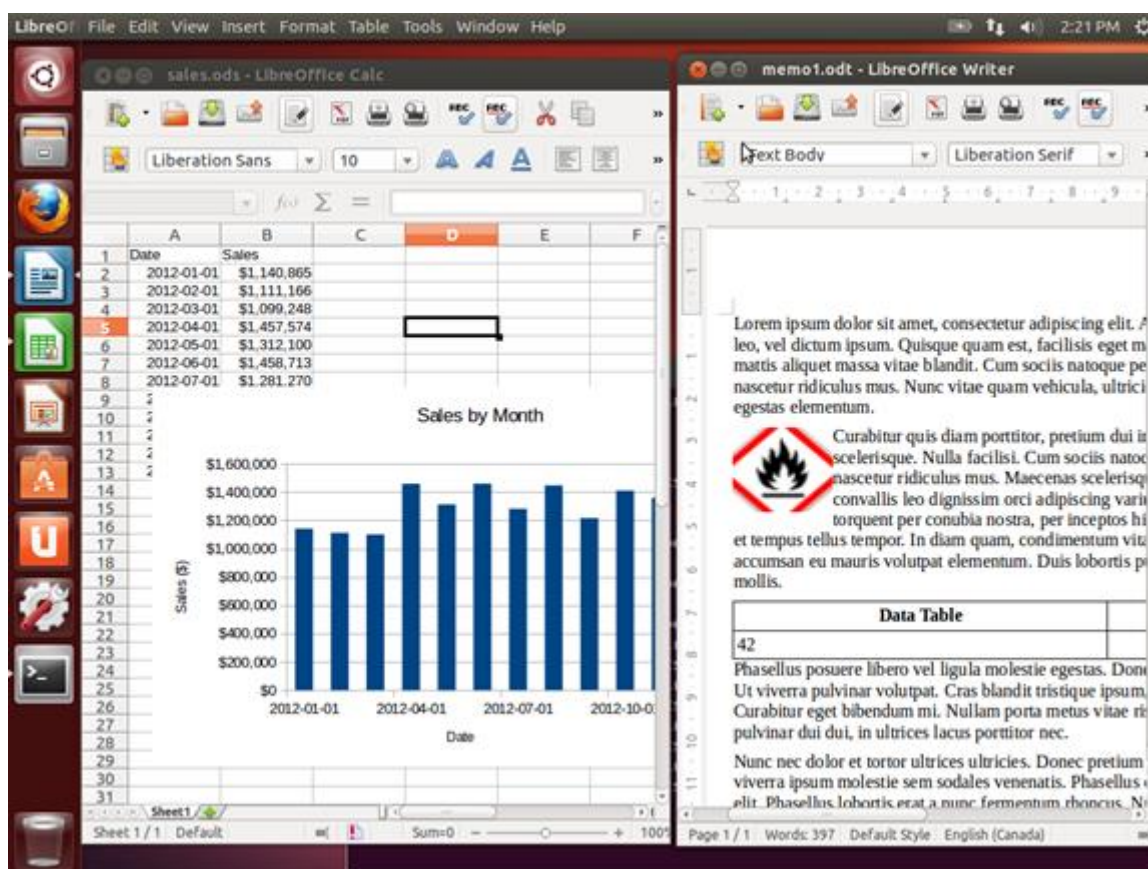
As ferramentas básicas usadas na maioria dos escritórios são:

- Processador de texto
- Planilha
- Pacote de apresentação
- navegador da Web

O **OpenOffice**, ou o **LibreOffice** mais ativo, cuida dos três primeiros papéis. Um processador de texto é usado para editar documentos, como relatórios e notas. As planilhas são úteis para trabalhar com números, como resumir dados de vendas e fazer previsões futuras. Um pacote de apresentação é usado para criar slides com recursos como texto, gráficos e vídeo incorporado. Os slides podem ser impressos ou exibidos em uma tela ou projetor para compartilhar com um público.

Abaixo, é mostrada a planilha e o editor de documentos do LibreOffice. Observe como a planilha, o LibreOffice Calc, não está limitada a linhas e colunas de números. Os números podem ser a fonte de um gráfico e fórmulas podem ser escritas para calcular valores com base em informações, como reunir taxas de juros e valores de empréstimos para ajudar a comparar diferentes opções de empréstimos.

Usando o LibreOffice Writer, um documento pode conter texto, gráficos, tabelas de dados e muito mais. Você pode vincular documentos e planilhas juntos, por exemplo, para resumir os dados por escrito e saber que as alterações na planilha serão refletidas no documento.



O LibreOffice também pode trabalhar com outros formatos de arquivo, como arquivos do Microsoft Office ou do Adobe Portable Document Format (PDF). Além disso, através do uso

de extensões, o LibreOffice pode ser integrado ao software Wiki para fornecer uma poderosa solução de intranet.

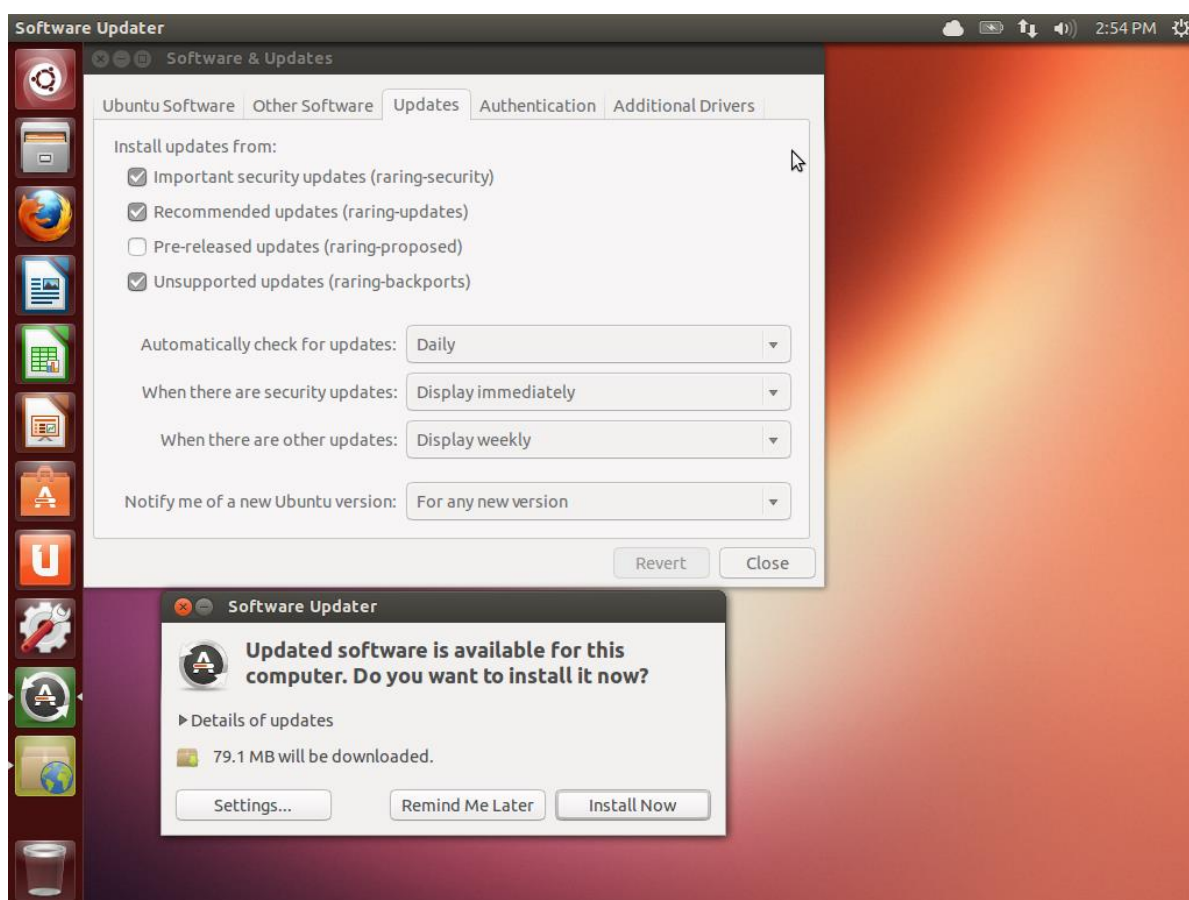
O Linux é um cidadão de primeira classe para os navegadores Firefox e Google Chrome. Como tal, você pode esperar ter o software mais recente disponível para sua plataforma e acesso oportuno a correções de bugs e novos recursos. Alguns plug-ins, como o Adobe Flash, nem sempre funcionam corretamente, pois dependem de outra empresa com prioridades diferentes.

3.6 Mantendo seu computador Linux seguro

O Linux não se importa se você está no teclado de um computador ou se conectando pela Internet. Portanto, tome algumas precauções básicas para garantir que seus dados estejam seguros e protegidos.

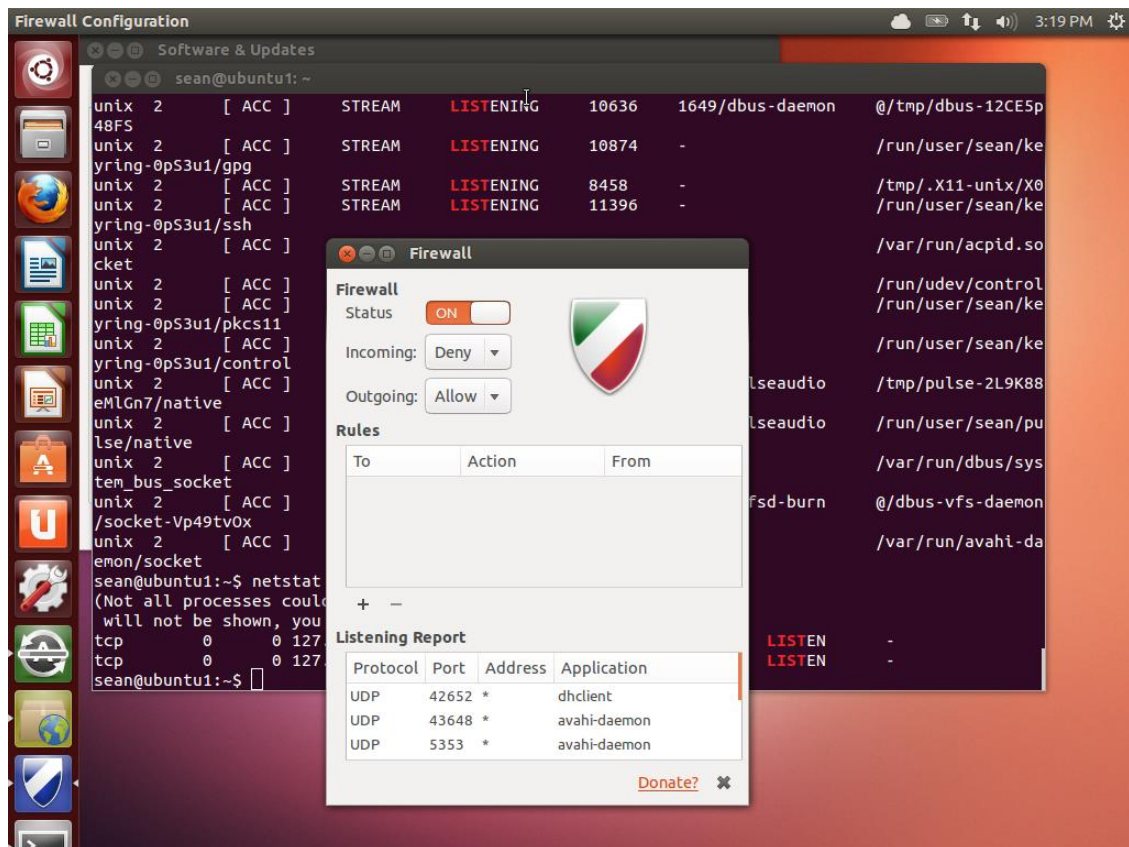
A coisa mais fácil que você pode fazer é usar uma senha boa e exclusiva em todos os lugares, especialmente em sua máquina local. Uma boa senha tem pelo menos 10 caracteres e contém uma mistura de números, letras (maiúsculas e minúsculas) e símbolos especiais. Use um pacote como o [KeePassX](#) para gerar senhas, e você só precisa ter uma senha de login em sua máquina e uma senha para abrir seu arquivo KeePassX.

Depois disso, verifique se há atualizações periodicamente. Aqui, mostramos a configuração de atualização de software do Ubuntu, que está disponível no menu Configurações.



Na parte superior, você pode ver que o sistema está configurado para verificar atualizações diariamente. Se houver atualizações relacionadas à segurança, você será solicitado imediatamente a instalá-las. Caso contrário, você receberá as atualizações em lote para execução toda semana. Na parte inferior da tela, está a caixa de diálogo que aparece quando há atualizações. Tudo que você precisa fazer é clicar em **Install Now** e você será atualizado!

Finalmente, você desejará proteger seu computador de aceitar conexões externas. Um **firewall** é um dispositivo que filtra o tráfego de rede e o Linux tem um incorporado. Se você estiver usando o Ubuntu, então o **gufw** é uma interface gráfica para o “firewall descomplicado” do Ubuntu.



Simplesmente mudando o status para "on", você bloqueará todo o tráfego que chega ao seu computador, a menos que você o tenha iniciado. Você pode permitir seletivamente as coisas, clicando no sinal de mais.

Sob o capô, você está usando o iptables, que é o sistema de firewall embutido. Em vez de digitar comandos complicados do iptables, você usa uma GUI. Embora essa GUI permita criar uma política eficaz para uma área de trabalho, ela apenas uma pequena amostra do que o iptables pode fazer.

3.7 Protegendo-se

Enquanto navega na web, você deixa uma pegada digital. Muitas dessas informações são ignoradas, algumas delas são coletadas para coletar estatísticas para publicidade e outras podem ser usadas para fins maliciosos.

Como regra geral, você não deve confiar em sites com os quais interage. Use senhas separadas em cada website para que, se esse site for invadido, a senha não possa ser usada para obter acesso a outros sites. Usar o KeePassX, mencionado anteriormente, é a maneira mais fácil de fazer isso. Além disso, limite as informações fornecidas aos sites apenas para o que é necessário. Embora o nome de solteira e a data de nascimento de sua mãe possa ajudar a desbloquear o login da sua rede social, se você perder sua senha, as mesmas informações poderão ser usadas para representar você no seu banco.

Os cookies são o principal mecanismo usado pelos sites para rastreá-lo. Às vezes, esse rastreamento é bom, como acompanhar o que está no seu carrinho de compras ou mantê-lo logado quando você retorna ao site.

Conforme você navega na Web, um servidor da Web pode enviar de volta o cookie, que é um pequeno texto, junto com a página da Web. Seu navegador armazena isso e envia de volta a cada solicitação para o mesmo site. Suponha que você não envie cookies para os sites `example.com` e `example.org`.

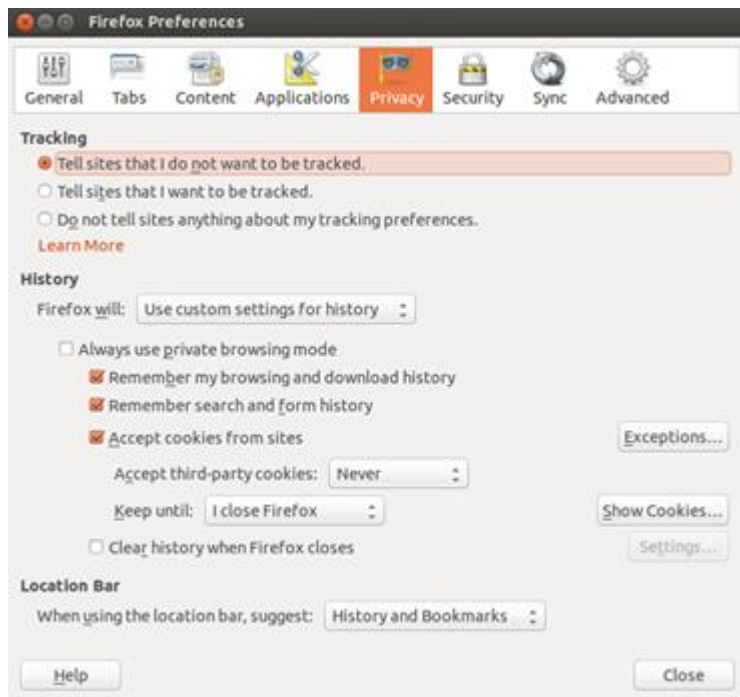
No entanto, muitos sites têm scripts incorporados que vêm de terceiros, como um anúncio de banner ou um pixel de análise. Se tanto `example.com` quanto `example.org` tiverem um pixel de rastreamento, como um de um anunciante, esse mesmo cookie será enviado ao navegar pelos dois sites. O anunciante sabe então que você visitou o `example.com` e o `example.org`.

Com um alcance amplo o suficiente, como os botões “Curtir” da rede social e outros, um site pode compreender quais sites você frequenta e quais são seus interesses e dados demográficos.

Existem várias estratégias para lidar com isso. Uma é ignorar isso. A outra é limitar os pixels de rastreamento que você aceita, bloqueando-os totalmente ou limpando-os periodicamente.

As configurações relacionadas ao cookie para o Firefox são mostradas na figura abaixo. No topo, você verá que o usuário optou por ter o Firefox dizendo ao site para não rastrear. Essa é uma tag voluntária enviada na solicitação que alguns sites honrarão. Abaixo disso, o navegador é avisado para nunca se lembrar de cookies de terceiros e para remover cookies comuns (como o site que você está navegando) depois que o Firefox for fechado.

Ajustar as configurações de privacidade pode torná-lo mais anônimo na Internet, mas também pode causar problemas em alguns sites que dependem de cookies de terceiros. Se isso acontecer, talvez seja necessário permitir que alguns cookies sejam salvos explicitamente.



Aqui você também tem a opção de esquecer o histórico de pesquisa ou de não rastreá-lo. Com o histórico de pesquisa removido, não haverá registro em seu computador local de quais sites você visitou.

Se você está muito preocupado em ser anônimo na Internet, você pode baixar e usar o **Tor Browser**. Tor é a abreviação de "The Onion Router", que é uma rede de servidores executados publicamente que roteiam seu tráfego para ocultar a origem. O navegador que acompanha o pacote é uma versão simplificada que nem sequer executa scripts, portanto, alguns sites podem não funcionar corretamente. No entanto, é a melhor maneira de esconder sua identidade, se você quiser fazê-lo.