MUUGLines

The Manitoba UNIX User Group Newsletter

March 2012 Volume 24 No. 7

Next Meeting: March 13th, 2012

RTFM: sort(1) & uniq(1)

March's RTFM will feature the sort(1) and uniq(1) commands, presented by Brad Vokey.

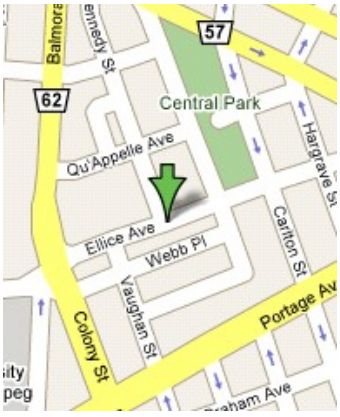
Topic: The Cloud: The catchphrase of the last year, and two years to come. The basics.

Everyone by now has heard of "The Cloud." Most people, even in the IT industry, are baffled as to what the cloud actually is. This no-frills, down-to-earth presentation by Rob Keizer will be on what it is, what its uses are, and the basics of setting up a private one.

Upcoming Meetings

April 10th, 2012: TBA

Where to Find the Meeting



Meetings are held at the IBM offices at 400 Ellice Ave. (between Edmonton and Kennedy Streets). When you arrive, you will have to sign in at the reception desk. Please try to arrive by about 7:15pm, so the meeting can start promptly at 7:30pm.

Limited parking is available for free on the street, either on Ellice Ave. or on some of the intersecting streets. Indoor parking is also available nearby, at Portage Place, for $5.00 for the evening. Bicycle parking is available in a bike rack under video surveillance located behind the building on Webb Place.

Can a Useful SSL Certificate Be Free?

The initial shock of the $199, 128-bit SSL certificate from Verisign has stuck with me for many years. Even to this day, basic certficates cost a bit too much, though prices have floored over the past few years. "Floored" isn't the right word, as there have been more resellers and intermediate Certificate Authorities and, assuming you only care about the "little lock" icon, then you can get a certificate for around $29.

That "little lock" doesn't imply any form of security, but for most, it makes them feel warm and fuzzy, so you're not "secure" without it. Browsers are trying to reflect this with "green bars" and other forms of extended validation. These extensions confuse the whole situation and are driving prices back up.

There are a number of "free" Certificate Authorities out there and all have varying degrees of quality expectations. CAcert.org for instance uses a Web of Trust model, but their root certificate isn't installed by default in most browsers and keystores. (SSL is used in all kinds of applications, not just web browsers. Java, for instance, ships with its own keystore for validating code signing.) This is very annoying to deal with, and you have to have "customers" manually add the CAcert root certificate in their browser in order to get that shiny lock icon. This is far from ideal.

Recently, my attention was drawn to a company called StartCom who runs StartSSL.com (**https://www.startssl.com**). They offer a full range of certificates at surprisingly reasonable prices. Their hook is that they provide simple Class 1 certificates for free. That's in *no money*. You do some basic identity declaration and they will give you a certificate that gives you that basic little lock for $0. Another huge offering is that, for only $59, they will give you a Class 2 or a UCC/wildcard certificate. That's HUGE; getting a wildcard certificate at other CA's is no less than $200. Wildcard certificates are not a good idea, generally (unless you are running some form of high-available nonsense, where all hosts need the same certificate). For situations where you want a certificate to match two names (that is, www.domain.com AND domain.com) you can/should use what is referred to as subjectAltName properties and the Class 2 certificates support that. (Class 1 will give you 1 alt name but, for more than one, you'll need a class 2.)

So, seeing is believing. I decided to request a certificate for a DAV host I don't really care about, but in reality should do more than basic HTTP auth on. Setting up a certificate was not too difficult, but did require I use a browser with no extensions on it. (My FireFox installation has a dozen extensions, so I wasn't sure which was messing the site up.)

The setup process involves you supplying StartCom with basic identity information (like giving them your mailing address) that they do some verification on and provide you with an S/MIME certificate you will use to log in. If you have extensions on, the certificate installation into your browser may fail and you have to restart the whole signup process again. I found this a bit annoying, but I appreciate their process. Using SSL client certificates is a fantastic idea, should your browser support it. Chome didn't for the longest time, but newer releases now do, partially. That being said, the site will suggest heavily that you don't use Chrome to set up your account. During the process, you'll get emails with confirmation codes, and after you've setup your identity certificate, you'll go through another email to validate your domain.

From here, you can now generate keys. If you use their "Express Tool," it will be straightforward. You can generate your own certificate signing request if you want, but they ignore all the x.509 properties in the certificate and just use the private key to generate the signed certificate. This makes the certificate look a little odd, but it still does the trick.

The whole process took me about an hour each attempt (two attempts due to browser issues) and a human did contact me to confirm my address (since I live on a street that doesn't exist on maps yet).

You can check out the certificate by viewing the certificate attached to **https://bitbucket.ca** and see what I mean when I say it looks a bit odd. I expect to drop a few dollars on the Class 2 certificate once my current mail server certificate expires, since the subjectAltName support would make my life easier, given my mail server is known by at least 4 host names.

You can't really get a FREE SSL certificate that both does work AND can already be verified in almost all browsers. (I validated "default inclusion" by using Chrome, FireFox, Safari and Internet Explorer 8.)

Linus Takes a Swipe at OpenSUSE

Mr. Tovalds stuck his head out recently to express his frustration with "default security" having an issue with his child's MacBook Air using OpenSUSE. His biggest contention is that there are certain things one expects to be able to set on their computer without being an admistrator (e.g. setting the clock/timezone or wireless network connections). In this, he's exactly right. Linux distributions have been designed around a server model crushed into also a Desktop class operating system. This design choice did not also take into account how the security model should change to meet the expected use. The majority of desktops are single user and while isolating a user from root (or in the case of Ubuntu, removing root from view) is a good idea, a user shouldn't have to *be* an adminsitrator to do daily tasks. Regardless if you agree with him or not, the discussion is pretty interesting, and you can find an article on it here: **http://itwnewsletters.itworld.com/t/8033012/15805 1762/615518/0/**

The Unintended Consequences of Virtual Servers

While it is a developing story, a small group of folks who use the Linode virtual server service were robbed of their BitCoins through the back-end system access to the Linode virtual machine infrastructure.

http://bitcoinmedia.com/compromised-linode-coins-stolen-from-slush-faucet-and-others/

BitCoin has some interesting security implications and there are a bunch of stories around that, but the point of this one is that otherwise "secured" hosts were compromised by maintenance infrastructure required by their Virtual Server ISP. It is a small and sobering reminder of the costs associated with leasing services from other providers. If you have access to a management interface for VM infrastructure, that is akin to having physical access, and once you have physical access, it's game over; your system is compromised.

Did You Know Mac OS X Lion Ships With PF?

You may be familar with OpenBSD's PF packet filter. It is also used in FreeBSD, NetBSD etc. You may also recall that Mac OS X is a userland derivative of FreeBSD, so it's not entirely unexpected to see this code make it down stream, but there are some really interesting implications of this, such as Apple is shipping a version of PF that is NEWER than FreeBSD and they have made a bit of changes to the underlying code that, by virtue of their licensing policy, makes it impossible to push back upstream to OpenBSD.

In an article entited "How Apple Treats The Gift Of Open Source: The OpenBSD PF Example" (**http://callfortesting.org/macpf/**), the author describes how Apple is using PF and its changes. The comments of the article are just about as valueable as the article parenting, it so it is definitely worth a read. Apple completely understands the license of the code they have acquired and is making full use of the privileges granted. You can tell that the OpenBSD folks are a bit insulted about Apple not contributing anything back (but the BSD license allows this). Regardlesss of your point of view, this is a perfect example of the consequence of licensing. When there is no moral imperative in the license, you can't expect a corporation to act morally without incentive.

BSDCan and PGCon Schedules Are Released!

Another spring is right around the corner and that signals another round of BSDCan and PGCon conferences.

BSDCan (**http://bsdcan.org**) this year is being held on May 11th and 12th at the University of Ottawa (as per usual), and will be preceeded by a couple days of tutorials. The tutorials don't differ too much from last year, except for the inclusion of an SSH tutorial by Michal Lucas (of Absolute OpenBSD, SSHMaster, Network Flow Analysis etc.).

The talks are literally all over the map. Adam Thompson commented that this year they had so many papers that the conference organizers only accepted 20% of them. The talks cover the entire spectrum, from theory to implementation and policy, though the distribution is largely FreeBSD-centric.

If you can spare the time and the air-fare, this is definitely one of the best and most cost-efficient conferences in the BSD community. If you have a few more days to spare, also check out the following PGCon.

PGCon (**http://pgcon.org**) follows BSDCan this year and runs on May 17th and 18th, with tutorials on the 15th and 16th. This conference focuses on the usage and implementation of PostgreSQL (which is becoming ever more important with the relative demise of MySQL).

The tutorials are focused on administration, which is one of the weaker sides (IMHO) of the PostgresSQL

system. Having some hands-on guidance to weather the client authentication jungle would be invaluable, as well as having a bit of time to look at replication, which is not the most advertised of the PostgreSQL feature set.

The talks range from operations topics to database adminstration and all the nigling details in between. This is definitely a more user-centric set of talks, but unlike previous years, it's more about making use of the tool and not so many "here is my big implementation" kind of talks. This looks to be a good year for both conferences. Check them out when/if you can!

Apache, BIND and Sendmail Are Not Long for OpenBSD

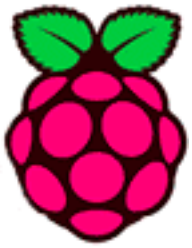
Both BIND and Apache have been shipping with OpenBSD forever. The project has little to no love for either product and has been looking for viable BSD-licensed alternatives to ship. This has been a bit of a roller coaster over the years and it looks like there is a bit of progress.

On the Apache side, it is looking like NGINX is the scrappy underdog. Having recently been "activated" (**http://www.daemonforums.org/showthread.php?t=6360**) in the OpenBSD tree, this is the closest any web server has come to unseating Apache 1.3 (heavily modified) as the default web server. As a web server, it is quite capable and VERY different from Apache, though in recent years it has shaped to be able to do as much of, if not more than, Apache ships stock, with a much smaller footprint and a BSD-friendly license.

On the BIND (DNS server) end, we have something called *unbound* (**http://unbound.net**). A recursive DNS resolver like BIND, but again smaller and BSD licensed. Originally written in Java, this resolver shed that language and was rewritten in C. While not as far along as NGINX is, there has been some serious talk about including it in the source tree **(http://old.nabble.com/Unbound-in-base-td33318306.html).**

I'm a bit split-brained on the results of this as, while I approve of radical change, neither project fits in with the direction that the OpenBSD daemon design is following. If either project was build around the privilege separation and control model as well as the PF-like configuration syntax, I'd have far less of an issue, as that model is not only superior but the consistency and high quality we come to expect from OpenBSD is pretty critical to end users. I suppose I have a lot more invested in Apache and BIND configuration than I care acknowledge, so a conversion tool may sway my apprehension a bit. Then again, I could just be spoiled by OpenSMTPD which is the product being groomed to replace sendmail (probably by the 5.2 release). OpenSMTPD mimics enough of sendmail to not break known system conventions and its configuration is PF-like and simple (well, third-order calculus is simple compared to sendmail's configuration).

Raspberry-Pi Finally Ripens



Just recently, the Raspberry-Pi $25 ARM computer has finally reached over the hurdle into a shipping product, but of course it sold out almost instantanously. (**http://www.cbc.ca/news/technology/story/2012/03/01/technology-raspberry-pi-launch.html**) The approved resellers/distributors have accounted for most of the purchases, though they sold out in rather quick order as well.

Originally designed as a platform to teach low level computing to schools, the concept of a complete $25 computer is just too enticing. Even more so with the $35 including ethernet (lack of which, in my opinion, is why Arduino isn't as popular as it should be).

There is no word quite yet when more will be available, but you can get on a waiting list. The $35 model ends up being $37 in Canada, and is being distributed by Newark (**http://t.co/2fWkqB5**), as well as Allied Electronics (**http://www.alliedelec.com/raspberrypi/**) at $35. Since one can't get one right now, we can't find shipping estimates; but hopefully it isn't much. I'm very anxious to get my hands on the ethernet-enabled model and I want to use it as a sensor aggregator for a home data collection project.