MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 29 No. 6, February 2017 Editor: Kevin McGregor

Next Meeting: February 21st, 2017

RTFM: Fixing drive sector SMART errors

Ruh roh!
Device: /dev/sdb [SAT], 5 Offline uncorrectable sectors.
7 Currently unreadable (pending) sectors.
Those just flashed across your console. Is your hard drive dying? Panic time? Not so fast: Trevor Cordes will show you how to gracefully repair such errors, allowing you to delay or obviate RMAs or replacement drive purchases.

Daemon Dash: VSFTPD

Wyatt Zacharias will present VSFTPD - the very secure FTP daemon. VSFTPD supports FTP and FTPS protocols, and boasts being one of the fastest and most secure FTP daemons available. Wyatt will demo running the daemon with both anonymous and authenticated modes, chroots, whitelists, and more.

Wine 2.0 Released

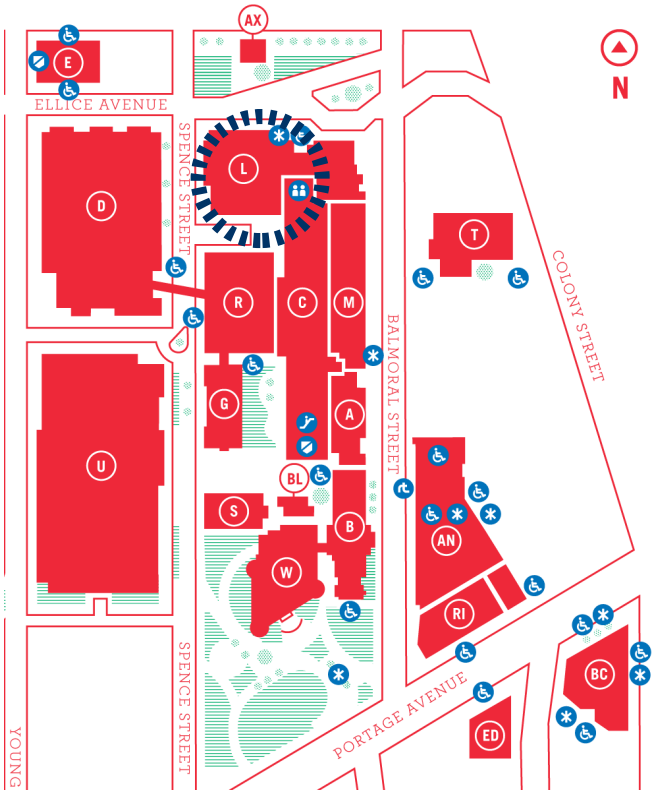
There are huge numbers of updates, but the main highlights are support for Microsoft Office 2013, and the 64-bit support on macOS.

Why 2.0? This is the first release made on the new time-based, annual release schedule, so a major version change was felt to be in order.

More DirectWrite features were implemented. The user interface improvements include a reimplementation of clipboard support, improving copy & paste of HTML text, plus drag & drop works more smoothly.

The macOS graphics drive supports Retina mode. More Direct3D 10 and 11 features are implemented. See all the details at
https://www.winehq.org/announce/2.0

Where to Find the Meeting



Meetings are held in the University of Winnipeg's Lockhart Hall (marked "L" on the map), at the south-east corner of Spence Street and Ellice Avenue. We can normally be found in room 1L11, but occasionally get relocated to nearby rooms. If there is a change, it should be conveyed via a sign on the door to 1L11. Parking is available on the surrounding streets. Please see http://www.uwinnipeg.ca/maps for further information about parking and access to the campus.

I give permission for IBM, its customers, partners, and minions, to use JSLint for evil.

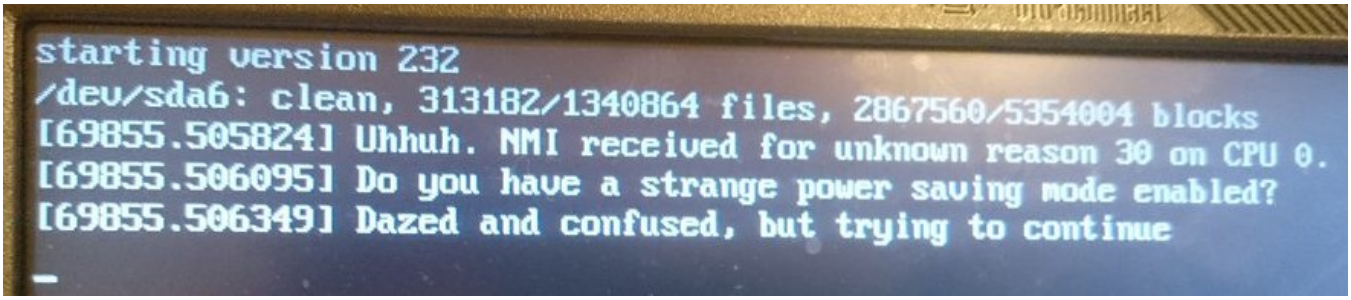
-- Douglas Crockford

You Are Not Expected To Understand This

You may have heard someone say this, perhaps even to you. Was it meant as an insult? An in-joke? Who said it first? Where did it come from?

While the person you heard it from may have meant it as an insult (we can't vouch for him), we can confirm that it was not meant as an insult in its original context.

It appeared as a comment in the source code of the Sixth Edition Unix operating system, specifically in the section describing context switching. "Context switching" is what modern operating systems do which allow them to give the appearance – at a large scale – that they are running multiple programs simultaneously, even if they only have one CPU core available.



A NMI is usually a bad sign.

The code that supports context switching is usually quite complicated, and the authors of the code did make an effort to explain it. But as Dennis Ritchie (one of the authors) put it:

> *'You are not expected to understand this' was intended as a remark in the spirit of 'This won't be on the exam,' rather than as an impudent challenge.*

So the next time you hear that, you can take your context into account to decide whether the speaker meant it as an insult or not!

For more details, see http://thenewstack.io/not-expected-understand-explainer

LibreOffice 5.3.0

February 1st marked the release of LibreOffice 5.3.0. This is interesting to the MUUG Board to the extent that LibreOffice has for some time been the tool used to produce this newsletter.

Not the least of these new features is a new cross-platform text layout engine that uses HarfBuzz for consistent text layout on all platforms, with significant advantages across languages and alphabets; and better import/export filters to new and legacy MS Office documents.

There are also many other under-the-hood changes; so many that it would fill this newsletter (why am I still typing?). For example, 50,000 lines of German comments have been translated to English, but there are still 3700 to go, stubbornly sticking around.

A lot of effort continues to be put into code quality, to great effect. For all the fun details, see https://people.gnome.org/~michael/blog/2017-02-01-under-the-hood-5-3.html.

Linux Tutorial

No, we're not going to start that here. However, if you have some time on your hands and like watching tutorial videos, check out this "complete" Linux course:
https://youtu.be/wBp0Rb-ZJak

It's almost 7.5 hours long, and covers much of the Linux basics, but also delves into installing Apache, Eclipse, MongoDB and more. We are not vouching for the quality, but you might find something useful in there. We suspect it might need some re-organizing of topics.

Doing It Manually

In the only politics-related item this month, we note that the Dutch elections coming up in March will be tallied by hand.

Some realistic concerns were raised about the electronic portions of the election process, and so the decision was made that all voting, counting and tallying will be done manually, avoiding those security concerns in the most direct possible way.

The New York Times reports: https://tinyurl.-com/gnbvv8v

Oracle 12 Is No More

Oracle has finally cleared this up. Oracle Solaris is moving to a "Continuous Delivery Model" (resembling Microsoft's approach with Windows 10, we suppose). Oracle Solaris 11 will now be supported until January 2031!

From the blog post of the Solaris team:

Oracle Solaris is moving to a continuous delivery model using more frequent updates to deliver the latest features faster, while fully preserving customer and ISV qualification investment in the vast array of ISV applications available on Oracle Solaris 11 today. New features and functionality will be delivered in Oracle Solaris through dot releases instead of more disruptive major releases, consistent with trends seen throughout the industry. This addresses customer requirements for an agile and smooth transition path between versions, while providing ongoing innovation with assured investment protection. By moving to a continuous delivery model based on Oracle Solaris 11, customers will have a seamless update experience to better fit their move to agile deployment models.

Customers can be confident that we plan to release new innovations into Oracle Solaris 11 in an ongoing manner. The Oracle SPARC and Oracle Solaris roadmap has been updated to reflect this new strategy.

As we will deliver new features and capabilities as part of Oracle Solaris 11, we have extended the Oracle Solaris 11 and Oracle Solaris Cluster 4 Premier and Extended Support lifespans to January 2031 and January 2034, respectively. Support dates are evaluated for update annually, and will be provided through at least the dates above. For more information, see page 34 of the Oracle Lifetime Support Policy: Oracle and Sun Systems Software.

The Oracle Solaris continuous delivery model has been silently in place for some time and is now the official delivery mechanism going forward. Oracle Solaris customers under Premier Support receive regular innovation, bug fix, and security vulnerability updates through both dot releases and Oracle Solaris 11 Support Repository Updates, as well as 24/7 access to Oracle systems specialists and online access to knowledge, proactive tools and communities. There are no changes to Oracle Solaris licensing or Premier Support pricing associated with this model.

OpenVMS Lives!

Well, it will, if VSI keeps at it. VSI (the men and women porting OpenVMS to x86 hardware) has released an update outlining some of the issues so far in porting this old battleship of an operating system to x86 and liberating it from IA64.

This update provides a high level view of our current efforts to port OpenVMS to the Intel x86 hardware platform. The report highlights topics including: Compilers, Objects & Images, Early Boot Path, Virtual Machines, Dump Kernel, Paravirtualization, and Condition Handling.

To give you an idea of the scope of the project, here are some samples of the work being done:

Compilers

One measure of the GEM-to-LLVM converter (G2L) work is the conversion of GEM tuples to LLVM's internal language constructs. 109 have been completed and 37 remain – 12 for C and 25 for BLISS

Early Boot Path

The early boot path continues to be streamlined and modernized to be more suitable for the UEFI/ACPI environment. The functions of the former primary bootstrap (VMB/APB/IPB) have been merged into the Boot Manager and SYSBOOT

Virtual Machines

This has been, and will almost certainly continue to be, an adventure. Initial work is done on HP Pro3500 Intel i3 systems. When stable up to a

known point, VMS_BOOTMGR.EFI, SYSBOOT.EXE, and SYS$MD.DSK are moved to kvm, VirtualBox, and Fusion (VMware on the MAC). In most cases all three behave differently form one another and from the HP system. The most noticeable differences are the VMs' emulation of UEFI differ in 1) device identification, 2) the creating, saving, and restoring of environment variables (EVs), and 3) console I/O.

The full report can be found at https://www.vmssoftware.com/pdfs/State_of_Port_20170105.pdf

For the Security Conscious

Tails 2.10 has been released! The Amnesic Incognito Live System (Tails) distribution is a Debian-based project which focuses on security and anonymity.

Tails includes tools for removing meta data from files and routes Internet traffic through the Tor anonymizing network. The project's latest release, Tails 2.10, now includes the OnionShare utility for sharing files from the user's computer over the Tor network. The Tor web browser now features a circuit viewer which will show the nodes a person's web traffic is routed through as it makes its way through the Tor network.

Stop Disabling SELinux

As blogger "SamDroid" says, "It's 2017, and your New Year's resolution should be to stop disabling SELinux." This article covers Fedora 25 running nginx, but may be helpful for other environments. Check it out at https://tinyurl.com/z7jm2mt

Or Just Print A Lot Of Stuff

How to make 60,000 printers print whatever you want

This may still work, but it's probably not a good idea to try it. From kur0sec.org:

Most, if not all, modern printers have a variety of online capabilities. You can print wirelessly, you can print from your phone, you can send an email to a "secure" address and have your document already printed and waiting for you when you arrive.

But what if we want to print to someone else's printer and not just our own? Don't worry, you can! One feature they don't advertise is the PCL/PJL port.

Most networked printers will utilize the following ports: HTTP, HTTPS, Telnet, SNMP, but also a PCL/PJL port – port 9100 to be exact. This is essentially a remote maintenance port. Its purpose is letting admins write PCL/PJL scripts that are then sent over the network and executed. But what's interesting is that while a lot of printers have these ports open, I've found that many in my explorations (rightly) have their actual code-execution turned off or severely limited.

A lot of the example PCL/PJL code injections I found from 2010/2011 didn't work on newer printers – code as simple as changing the READYMSG (the status text on the printers display) would be ignored/unexecuted (Although a lot of the time you can do this from the printer's web face anyway). Indeed, after some high profile hacks in 2010, many printers have 'locked down' their security a bit and use their own vendor languages for configuration and only implement a small subset of PCL/PJL. But most still have the port open and 99.9% of the time not password protected. So what happens to data that you send to these inert ports?

It gets printed.

More detail at https://kur0sec.org/print

TLS 1.3 Showing Up

Nick Sullivan and Filippo Valsorda gave a talk about TLS 1.3 at 33c3, the latest Chaos Communication Congress. The congress, attended by more that 13,000 hackers in Hamburg, has been one of the hallmark events of the security community for more than 30 years. The talk introduces TLS 1.3 and explains how it works in technical detail, why it is faster and more secure, and touches on its history and current status.

Watch the talk at https://tinyurl.com/zrh9ol3