

# SAGE *Advice*

The Journal of The System Administrators Guild of

ISSN: 1447-5049

Volume 14 Number 4

**June 2008 Edition**

## ***This Issue***

***SAGE-AU Mail System Changes***

***Password Recovery***

***Meet our members***

***New Members***

***Coming Events***

**SAGE-AU**

The System Administrators Guild of Australia

<http://www.sage-au.org.au>

# Contents

# Information

## Regional Groups

Regional Group contact information ..... 12

## General Information / Articles

SAGE-AU Mail System Changes ..... 3

Meet our Members ..... 6

SAGE-AU welcomes our new members ..... 7

Password Recovery ..... 8

SAGE-AU Events ..... 11

Coming Events ..... 11

SAGE Advice is the official newsletter of the System Administrator's Guild of Australia. It is available in PDF format free of charge to members of SAGE-AU via download from the SAGE-AU website. Past copies are available online at [www.sage-au.org.au/newsletters\\_index.html](http://www.sage-au.org.au/newsletters_index.html)

### Editors

Jess Wightman  
[editor@sage-au.org.au](mailto:editor@sage-au.org.au)

### Membership & General Information

Phil Gerner  
[office@sage-au.org.au](mailto:office@sage-au.org.au)

### Contact Details

Contact details for SAGE-AU are:

SAGE-AU  
 PO Box 193  
 Surrey Hills VIC 3127  
 Phone: (03) 9895 4484  
 Fax: (03) 9898 0249

### Website

<http://www.sage-au.org.au/>

### SAGE-AU Executive Committee

#### President

Donna Ashelford  
[president@sage-au.org.au](mailto:president@sage-au.org.au)

#### Vice President

Leslie Elliott  
[vice-president@sage-au.org.au](mailto:vice-president@sage-au.org.au)

#### Secretary

Robert Hudson  
[secretary@sage-au.org.au](mailto:secretary@sage-au.org.au)

#### Treasurer

Jacinta Richardson  
[treasurer@sage-au.org.au](mailto:treasurer@sage-au.org.au)

#### General Committee

Jess Wightman  
[jess.wightman@member.sage-au.org.au](mailto:jess.wightman@member.sage-au.org.au)

#### Immediate Past President

Phil Kernick  
[phil.kernick@member.sage-au.org.au](mailto:phil.kernick@member.sage-au.org.au)

#### Associate Representative

Position Vacant

## Broken or lost keyring?

Contact Phil Gerner in the SAGE-AU office ([office@sage-au.org.au](mailto:office@sage-au.org.au)) and he will arrange a replacement to be mailed to you and for your password to be re-set to the new keyring number.

## Advertising Rates (all prices are GST inclusive) Inclusions with SAGE Advice

### Normal Rates

Full page, 170 x 250 mm .....	\$275
1/2 page, 170 x 120 mm .....	\$165
1/4 page, 170 x 55 mm .....	\$88
1/8 page, 80 x 55 mm .....	\$44

### Bulk Rates

Ad space in four or more issues paid in advance attract a 20% discount.

See [www.sage-au.org.au/newsletters\\_advert.html](http://www.sage-au.org.au/newsletters_advert.html) for our publication schedule for 2008.

# SAGE-AU Mail System Changes

We've recently had some changes made to the way our mail system works. To give you an idea of what's going on with our mail system, Simon Coggins has written an incredibly informative article on what's changed, and how things are working at the moment.

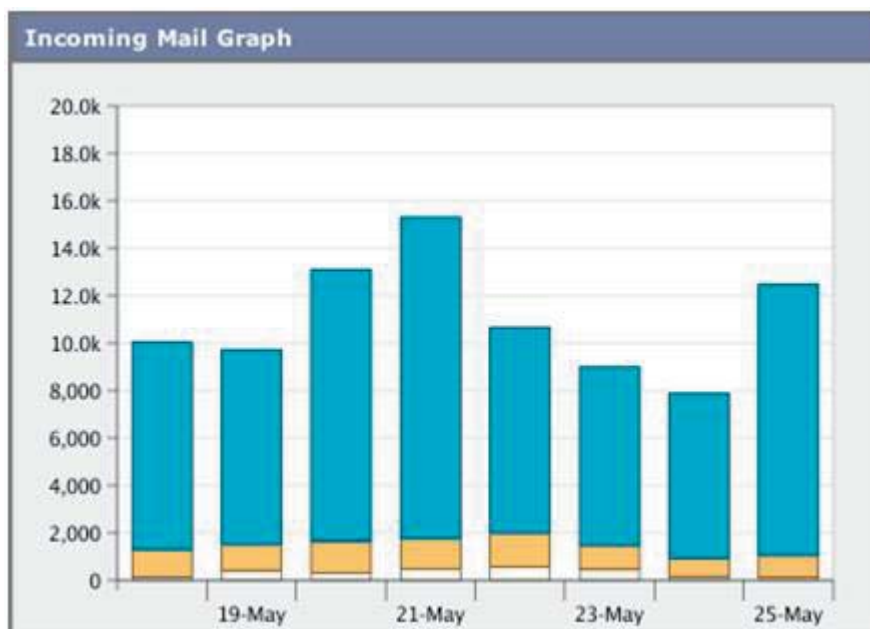
Ever wonder how the SAGE\_AU mail system works? No, excellent. I can stop here. Alas if only my article could be that short. I'm not really going to talk about how the whole mail system works. I'm just going to give an update on what has changed recently, and show some impressive numbers about our mail flow.

We were using spamassasin, a huge regex and clamav to filter the SAGE-AU mail. This worked for many years, but in recent times, more and more spam has been slipping past. A few months ago, things changed, Ironport was kind enough give SAGE-AU an Ironport C100 Mail Appliance to use as our mail gateway. This server does virus and spam filtering before passing the emails on to our Sun X4100 server to be processed. All outgoing email is then sent back to the C100 to ensure we aren't sending viruses or spam out to the world. It also ensures that we have one exit point for mail, and allows us to collect some stats.

So anyway, about those impressive numbers I was talking about. In the week 18 May 2008 00:00 to 25 May 2008 23:11 our stats look like this:

Incoming Mail Summary		
Message Category	%	Messages
Stopped by Reputation Filtering	86.7%	76.4k
Stopped as Invalid Recipients	0.1%	82
Spam Detected	10.2%	8,950
Virus Detected	0.0%	0
Stopped by Content Filter	0.0%	0
<b>Total Threat Messages:</b>	<b>97.0%</b>	<b>85.5k</b>
Clean Messages	3.0%	2,670
<b>Total Attempted Messages:</b>		<b>88.1k</b>

The daily break down of mail flow looks like this:



# INTERNODE Business Connect

**Internode Business Connect (IBC)** is a flexible, reliable and secure wide area networking solution. IBC connects sites across Australia using a variety of access technologies and is the 21st Century alternative to traditional Frame Relay and ISDN wide area networks.

IBC is a 'private' IP network. Within such a network, traffic engineering is used to ensure optimal network performance – in terms of a very high data delivery ratio, a very low latency (or 'round trip transit delay'), and minimal latency variation (or 'jitter').

These parameters combine to provide the necessary 'Quality of Service' to meet the demanding requirements of internal business networks.

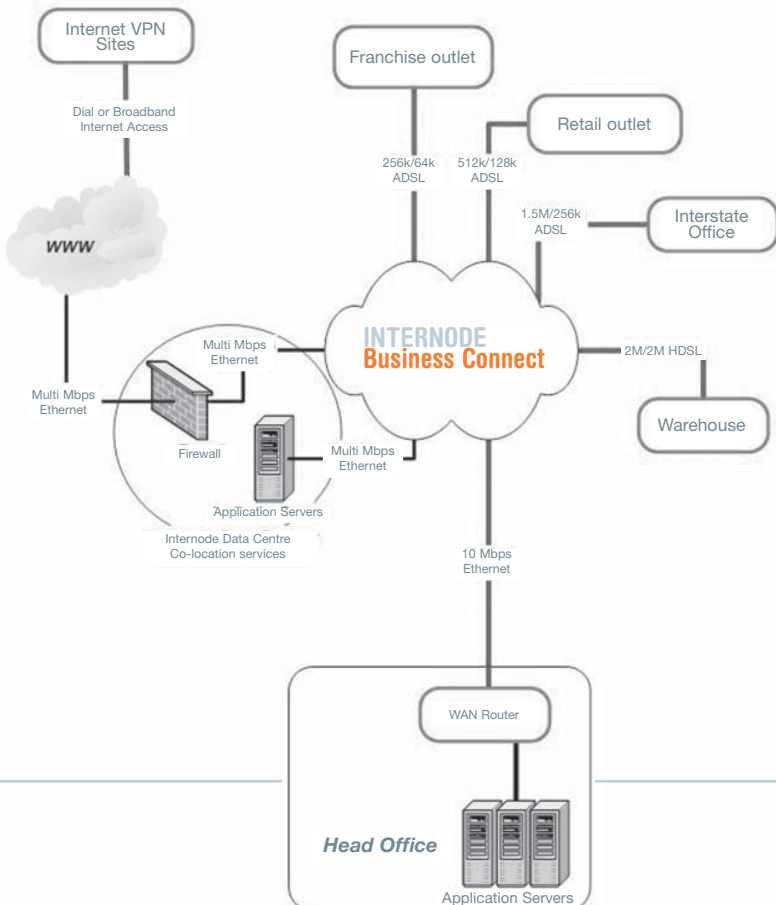
The Internode Business Connect private IP network has multiple levels of security, including physical POP security, strict authentication requirements and L2TP traffic separation. This security is fully managed by Internode staff.

**Internode Business Connect solutions are tailored to meet the exact requirements of individual corporate customers. This includes:**

- Flexible network topologies; ranging from a traditional virtual circuit 'Layer 2' approach through to a fully routed 'Layer 3' internetwork.
- A variety of high-speed access technologies; ranging from cost-effective DSL (Digital Subscribe Line) services, through to high performance Agile Ethernet services utilising optical fibre, radio and HDSL technologies. Critical business sites may use ISDN backup services for redundancy.
- Access to our world-class Internode Internet Data Centre; for connection to co-located equipment, managed servers, data storage systems or fire walled Internet.
- Equipment services including design, supply, configuration and maintenance of class-leading Cisco networking equipment.
- Optional ad-hoc 'secure roaming' access - for mobile staff, management and teleworkers – through our well-proven Virtual Private Dial Network service.
- Dynamic Class of Service for applications with differing network requirements (for example, voice and video over IP).

For more information call 1300 788 233 or visit our website:

[www.internode.on.net/ibc](http://www.internode.on.net/ibc)



# SAGE-AU Mail System Changes

## Continued

In the same time period, the mail servers sent 89.9k emails out, 100% of which were clean.

So there you have it, 97% of our email comes from a can (of spam). SAGE-AU now has an effective virus/spam filtering system in place that is defiantly an improvement over the old spamassasin system. Not sure about everyone else but I've certainly noticed a difference to the amount of spam going to my @member alias. So if you haven't started using your alias yet, this might give you some reason to start.



Randall Munroe xkcd.com

## Meet our members

---

Most of the time, members join our ranks silently, and unless they are very active on the mailing lists, regularly attend regional group meeting or speak at our national conference the existing membership doesn't really get the opportunity to find out who they are and what they do. In this section we hope to introduce you to a snapshot of users who've joined over the past few months.

### Today we introduce Eric Rose.

---

**Name:** Eric Rose  
**State:** New South Wales  
**Member since:** May 2008

#### What's your job title/description?

Officially, the business card says Software Engineer but I was also hired as a backup Sysadmin. He left for greener pastures last year and I am now the Sysadmin, as well as Build Manager and Programmer.

#### What's your business name?

Integeio

#### What does your business do?

Mapping for Business Intelligence.

#### What do you do in your work?

General systems administration duties in a mixed Windows/Linux environment, as well as manage the software build environment and the software release process.

#### How long have you been working in the System Administration field?

On and off since the early 1990s when I was working on support for Intelligence Network products in Telstra.

#### Please tell us a story about one of your professional experiences.

A Junior Sysadmin was hired as someone who might be compatible with the staff, and who would be trainable to take over more and more of what I was doing, so that I would go back to being a full-time programmer (where management wants me). He was selected primarily on the basis of some basic linux sysadmin experience, and that ehe had looked after the mail server at his previous company.

On the Sunday of the first weekend he was with us, the mail server crashed due to issues with the RAID drivers. We were both paged and arrived at the office, where he was going to fix it with me looking over his shoulder. As he was looking blankly at the console, I suggested that we need to fsck the filesystems. He looked blankly at me and asked what fsck was.

He didn't make it out of the probationary period.

#### How did you first hear about SAGE-AU?

I first heard about it a few years ago on-line somewhere, but didn't join as I wasn't primarily a Sysadmin at that point. A few weeks ago, a friend, who is a memeber, reminded me about SAGE-AU when I lamented that I might have to re-join the Scary Devil Monastery due to the amount of sysadmin work I'd been doing. Becoming a member of SAGE-AU is my self-admission that I'm again lost to civilized society.

#### What have you gained from SAGE-AU in that time?

So far, a key ring. It's only been a couple of weeks.

#### Does your business support your SAGE-AU membership?

I'm not sure what you mean by this question, but I guess that the answer is no; I paid for my membership.

#### Do you work in a team or on your own? How big is your team?

On my own, but the head of the Development Team has some sysadmin experiece and can help out when I need a hand.

#### What do you do for fun?

Cycle

# SAGE-AU welcomes our new members

SAGE-Au extends a warm welcome to our newest members. These include:

## Queensland

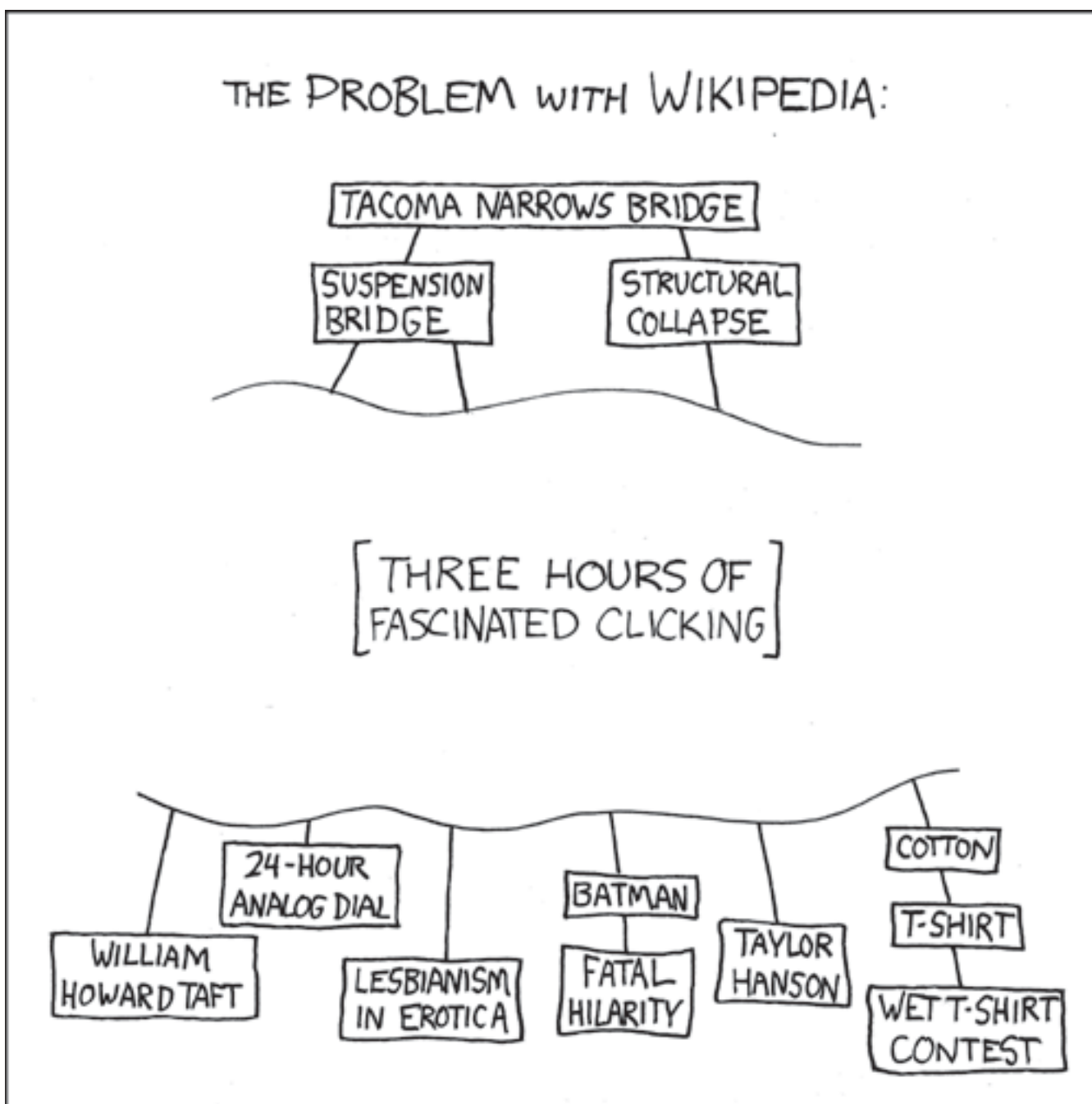
- James Hodgkinson from JH Online
- Marc Collins from DETA

## New South Wales

- Brad King from Australian Business Lawyers
- Scott Kristiansen
- Mark Lang from Macquarie Regional Library

## Victoria

- Oliver Lemmel from Bureau of Meteorology
- Bienifer Vinluan from Bureau of Meteorology
- Viviene Cucevic form Bureau of Meteorology
- Paul Dyson from Bureau of Meteorology
- George Kabiotis from Bureau of Meteorology
- Mick Read from Armstrong World Industries
- Paul Roccasalva from Armstrong World Industries
- Wayne Scott from ARRB



# Wiki Article for the month

## ***Password Recovery***

---

This month's article was based on a **SAGE-AU Tech discussion** which started with a problem proposed by **Stacy Porter**. Thanks to **Stacy** for summarizing this discussion & to **John McKirdy** for adding some information for \*nix systems.

Breaking into a system or document when the password isn't known is euphemistically called password recovery. Here we consider gaining access to be sufficient, without necessarily obtaining the password itself.

### Microsoft Windows

Passwords for user accounts under Microsoft Windows are stored in the SAM userdatabase file.

The Offline NT Password and Registry Editor <http://home.eunet.no/pnordahl/ntpasswd/> by Peter Nordahl-Hagen will unlock or clear the password of any account on the Windows NT family of operating systems. It doesn't run under Windows, rather the PC boots this program which lists the user accounts.

The same thing might be accomplished with any offline registry editor.

Other possibilities are:

- Bart's Preinstalled Environment (BartPE) <http://www.nu2.nu/pebuilder/> bootable live Windows CD/DVD lets you run Windows from a CDROM and from his change the password. Third party plugins exist specifically for changing the administrator password.
- Forgot the Administrator's Password? [http://www.petri.co.il/forgot\\_administrator\\_password.htm](http://www.petri.co.il/forgot_administrator_password.htm) at Petri IT Knowledgebase.
- Cain & Abel <http://www.oxid.it/cain.html> uses various methods to obtain passwords.
- Ophcrack <http://sourceforge.net/projects/ophcrack/> a Windows password cracker.
- LCP <http://www.darknet.org.uk/2006/09/lcp-a-good-free-alternative-to-10phtcrack-lc5/> a Windows password cracker.

Reference: **[SAGE-AU] Windows 2003 password cracker[SUMMARY]** <https://lists.sage-au.org.au/pipermail/sage-au/2007-October/024490.html> by Stacy Porter, 2007-10-02 and associated thread.

### Unix Passwd Files

If login authentication is done using `/etc/passwd` and `/etc/shadow` (rather than some other database), then to replace the user password, simply edit the shadow password file as root.

For password crackers, see Password Checkers/Crackers [http://www.softpanorama.org/Authentication/password\\_crackers.shtml](http://www.softpanorama.org/Authentication/password_crackers.shtml) at Softpanorama.

Under Solaris, to break into the root account it's simplest to boot from the installation CDROM which gives you a full shell by just opening a new terminal window. Mount the root partition (which is usually `/dev/dsk/c0t0d0s0`) onto a directory under the RAM filesystem established by the installer and then edit `/etc/shadow`. Gory details are in Solaris root password recovery [http://www.softpanorama.org/Solaris/Security/solaris\\_root\\_password\\_recovery.shtml](http://www.softpanorama.org/Solaris/Security/solaris_root_password_recovery.shtml) at Softpanorama. It's possible but unlikely that the root password would not be in `/etc/shadow` but is obtained via another database, so you may have to edit `/etc/nsswitch.conf` to ensure that the root password is fetched from files before some other source.

The same technique should work with any Linux distro which has a live CD <http://en.wikipedia.org/wiki/LiveDistro>.

### Sun SPARC Hardware Password

Sun SPARC systems (including sun4c, sun4u, and sun4m) have a hardware password to control access to the boot monitor (which is OpenBoot, the firmware in the OpenBoot PROM or OBP). The password is stored in an NVRAM chip (also called EEPROM) which is a battery powered clock and nonvolatile RAM; it is socketed for easy removal. Unlike x86 hardware, there is no jumper to reset the NVRAM settings.

EEPROM variables may be set from within the OpenBoot monitor or using the Solaris `eeprom` command. There are the variables which control access to the system:

# Wiki Article for the month

## Continued

security-password contains the password and is readonly

security-mode controls whether access to the monitor is restricted and whether the password is required to boot the system

boot-device is a list of devices to boot from (default "disk net")

diag-device is an alternate list of devices to boot from (default "net")

If you don't have hardware password, here's various things you can try to clear it, in order of preference. Pick the first that fits your situation and apply recursively if necessary.

(I've not confirmed that all these will work, so if someone tries them please amend this article.)

1. Login to Solaris as root and use the eeprom command to either clear the password or set security-mode=none.
2. If the boot-device list includes a CDROM drive then you can boot from the Solaris installation CDROM which gives you a full Solaris OS (see above), including the eeprom command. (Not confirmed.)
3. If the diag-device path includes a CDROM drive, then set the diagnostic switch and boot from CDROM. How to go into diagnostic mode is platform specific.
4. If you have another Solaris SPARC system of sufficiently similar (!) type with known hardware or root passwords, swap the NVRAM chip or the system hard drive and boot Solaris.
5. If you don't have the root password either, remove the system hard drive and reset the root password by editing /etc/shadow (as above).
6. Replace the NVRAM chip. As well as Sun vendors, electronic retailers such as "Farnell" and "RadioSpares" may carry compatible types. See the NVRAM FAQ for details.
7. Call your friendly Sun vendor.
8. The absolute last resort is to hot swap the NVRAM chip. This is risky and not recommended. See the NVRAM FAQ for details.

Note that if security-mode=full you won't be able to boot the machine without the password. Similarly, even if the machine tries to boot via the network, a network install via Jumpstart won't work without the password (not confirmed).

See also:

- Sun NVRAM/hostid FAQ <http://www.squirrel.com/sun-nvram-hostid.faq.html>
- OpenBoot <http://docs.sun.com/app/docs/coll/216.2>

### See Also

- LostPassword.com <http://www.lostpassword.com/> – password recovery tools and services for many file formats (MS-Windows, MS-Office, Acrobat, hard disks, and others)
- DMOZ category "Password Recovery" [http://www.google.com/Top/Computers/Security/Products\\_and\\_Tools/Password\\_Recovery/](http://www.google.com/Top/Computers/Security/Products_and_Tools/Password_Recovery/)
- Wikipedia > Password cracking [http://en.wikipedia.org/wiki/Password\\_cracking](http://en.wikipedia.org/wiki/Password_cracking)
- Top 10 Password Crackers <http://sectools.org/crackers.html> from Insecure.org.



Randall Munroe xkcd.com



# Diamond Support for VMware



## Your Trusted IT Partner!

- Do you want a trusted partner that not only knows the technology that runs your business but also how your business relies on that technology?
- Need a partner to support and mentor your team?
- Need access to a pool of resources with knowledge of your environment for overflow, project and backfill?
- Concerned about how your environment stays at its originally configured best practice, high performance level to ensure your business continues to operate optimally?

**TAS Diamond support** provides you with the launching platform to establish a trusted partner relationship with TAS. Diamond support extends the current vendor relationships you have in place and goes a step further by providing:

1. A formal complete health check of your VMware infrastructure with a full report – once per year.
2. An interim health check, six months later which identifies issues, risks etc
3. Access to fully trained VMware consultants, who know and understand your VMware environment and provide local support to help you keep your business running:
  - a) Ability to call TAS for support during business hours.
  - b) Ability to call TAS for support after hours
4. Notification, via email of all patches which have become available
5. Notification, via email of all new releases, minor/major which have become available
6. TAS monthly newsletter detailing, tips, techniques and general industry info
7. 10% discount on all additional services you purchase from TAS excluding already discounted prepaid bundles
8. TAS VMware certified engineer on site 1 day a month

## Diamond Support Options

- On-site, or remote access, systems administration out-tasking
- VMware residency program
- Update training on new releases and features
- ITIL consulting for virtualisation infrastructure
- VMware Mentoring
- Extra monthly onsite days
- Architectural, strategy and design services
- Backfill services for when your staff are on annual leave or away for training
- SAN, DataCore, PlateSpin, SQL Server, Sybase and Oracle Diamond support uplifts

To find out more about Diamond support contact TAS on the numbers below or visit our website at [www.techarchsolutions.com](http://www.techarchsolutions.com)

NSW 02 99848133  
VIC 03 96539625  
WA 08 92782521  
SA 08 81135398  
QLD 07 33030220  
[www.techarchsolutions.com](http://www.techarchsolutions.com)  
[sales@techarchsolutions.com](mailto:sales@techarchsolutions.com)

# SAGE-AU Events

SAGE-AU is pleased to announce the sixteenth annual Australian System Administrators' conference (SAGE-AU'2008) will be held at the Holiday Inn Adelaide (65 Hindley Street), Adelaide from 11th - 15th August 2008.

Registrations for SAGE-AU'2008 will be available soon!

The training (tutorial) program will be held on Monday 11th August through Wednesday 13th August.

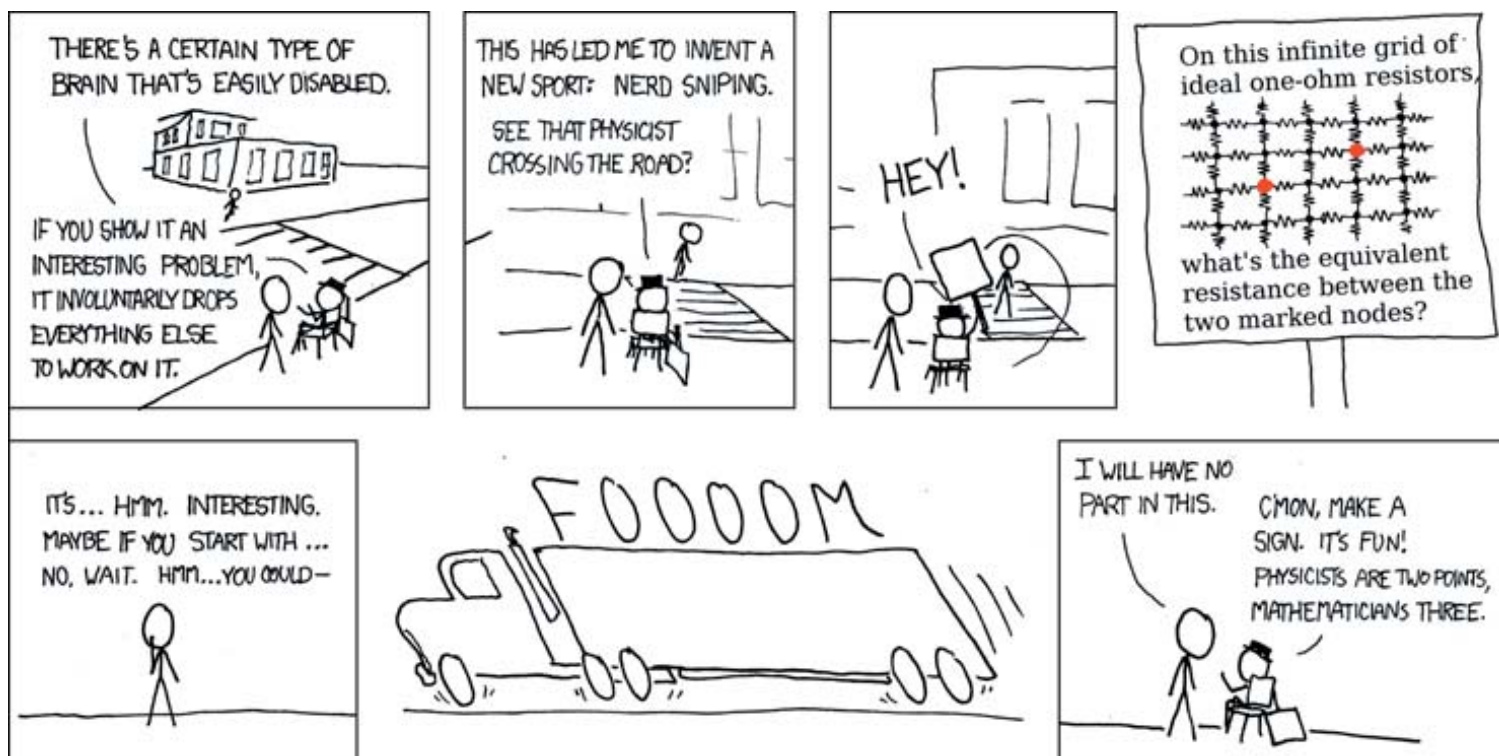
The technical program will be held on Thursday 14th and Friday 15th August.

During the tutorial and technical programs, from Wednesday 13th to Friday 15th August, we run a trade exhibition. If your company would like to participate, please contact the SAGE-AU office ([office@sage-au.org.au](mailto:office@sage-au.org.au)).

## Coming Events

### 16th Australian System Administrators Conference 11th - 15th August 2008 Holiday Inn - Adelaide

Program Details now available online



Randall Munroe xkcd.com

## Regional Groups

Full lists of Chapter executive committee members, meeting schedules and up to date Chapter information can be found at <http://www.sage-au.org.au/regional.html>

### Victorian Chapter

The Victorian group currently meets on the second Tuesday of the month at 7:00pm at:  
Ground Floor Tutorial Room, Baillieu Library  
University of Melbourne, Parkville

#### President

Chris Burgess  
[chris.burgess@member.sage-au.org.au](mailto:chris.burgess@member.sage-au.org.au)

#### Vice President

Jason Wood  
[jason.wood@member.sage-au.org.au](mailto:jason.wood@member.sage-au.org.au)

The group mailing list is: [sage-vic@sage-au.org.au](mailto:sage-vic@sage-au.org.au)

### Queensland Chapter

The Queensland group currently meets on the second Thursday of the month at 7:00pm at:  
Room 621  
General Purpose South Building (No. 78)  
Staffhouse Road  
University of Queensland, St Lucia

#### President

Jason Andrade  
[jason.andrade@member.sage-au.org.au](mailto:jason.andrade@member.sage-au.org.au)

#### Vice President

Iain Robertson  
[iain.robertson@member.sage-au.org.au](mailto:iain.robertson@member.sage-au.org.au)

The group mailing list is: [sage-qld@sage-au.org.au](mailto:sage-qld@sage-au.org.au)

There is also a **Rockhampton** group - see  
[www.sage-au.org.au/rgqld.html](http://www.sage-au.org.au/rgqld.html)

### South Australian Chapter

The South Australian group currently meets on the last Tuesday of the month at 6:30pm at:  
Internode  
Level 3, 150 Grenfell Street, Adelaide SA 5000

#### President

Steve Challans  
[steve.challans@member.sage-au.org.au](mailto:steve.challans@member.sage-au.org.au)

#### Secretary

Matthew Benwell  
[matthew.benwell@member.sage-au.org.au](mailto:matthew.benwell@member.sage-au.org.au)

#### Treasurer

Greg Warner  
[greg.warner@member.sage-au.org.au](mailto:greg.warner@member.sage-au.org.au)

The group mailing list is: [sage-sa@sage-au.org.au](mailto:sage-sa@sage-au.org.au)

### NT Chapter

If you are interested in being involved in getting the NT Chapter up and running again, please contact the Executive Committee ([exec@sage-au.org.au](mailto:exec@sage-au.org.au))

### New South Wales Chapter

The New South Wales group currently meets in Sydney on the third Tuesday of each month at 7:00pm at:  
Ernst & Young Building  
680 George Street, Sydney  
Meet in the Equilibrium Hotel

#### President

Stephen 'Max' Gillies  
[stephen.gillies@member.sage-au.org.au](mailto:stephen.gillies@member.sage-au.org.au)

#### Secretary

Sam Lor  
[sam.lor@member.sage-au.org.au](mailto:sam.lor@member.sage-au.org.au)

The group mailing list is: [sage-nsw@sage-au.org.au](mailto:sage-nsw@sage-au.org.au)

### Tasmanian Chapter

The Tasmanian group currently meets on the second Thursday of every month at:  
Bridie O'Reilys  
124 Davey Street, Hobart

#### President

Geoffrey Day  
[geoffrey.day@member.sage-au.org.au](mailto:geoffrey.day@member.sage-au.org.au)

#### Secretary

Sim Alam  
[sim.alam@member.sage-au.org.au](mailto:sim.alam@member.sage-au.org.au)

The group mailing list is: [sage-tas@sage-au.org.au](mailto:sage-tas@sage-au.org.au)

### West Australian Chapter

The West Australian group currently meets on the first Tuesday of every month at:

The Moon and Sixpence Pub  
300 Murray Street, Perth

#### Regional Co-ordinator

Andrew Shugg  
[andrew.shugg@member.sage-au.org.au](mailto:andrew.shugg@member.sage-au.org.au)

The group mailing list is: [sage-wa@sage-au.org.au](mailto:sage-wa@sage-au.org.au)

### ACT Chapter

The ACT chapter meets on the third Wednesday of each month at:  
Staff Training Lab, ICTS - Building 14  
Ground Floor, Australian Defence Force Academy  
Northcott Drive

#### Chapter Contact

Tim Carson  
[tim.carson@member.sage-au.org.au](mailto:tim.carson@member.sage-au.org.au)

The group mailing list is: [sage-act@sage-au.org.au](mailto:sage-act@sage-au.org.au)