Case, Dowty-Case, Cray, Case Technology Legacy Products

NEWSLETTER

Specialists in high-speed and rugged access solutions

March 2011

In this edition:

Welcome

Welcome to the Case Communications March 2011 Newsletter.

Cloud Apps – functionality and specification

Are you getting what you need from your 'cloud' software services (SaaS)?

Read more...

Vodaphone users lose connection in UK

Stolen network equipment causes Vodafone UK network outage

Read more...

A quantum communications switch

The device that could one day let super fast quantum computers talk to each other

Read more...

Critical NASA network open to Internet attack

Six NASA servers exposed to the Internet had critical vulnerabilities that could have endangered Space Shuttle, International Space Station and Hubble Telescope missions

Read more...

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the newsletter, please feel free to email them to us: Email feedback/Enquiry

Monitoring Linux network interfaces with vnStat

With tools like vnStat, command-line aficionados can get the low-down on their network with just a few useful commands

Read more...

Is £650m enough for UK cyber defences?

£650m will be provided for UK cyber defences over a four-year period but the IT security industry has expressed concerns about how this will be allocated

Read more...

---

case communications
Specialists in high-speed and rugged access solutions
Case, Dowty-Case, Cray, Case Technology Legacy Products
LINUX
NEWSLETTER
March 2011

In this edition:

Other newsletters:

Cloud apps – functionality and specification

By **Chris Challis**

As you know, there is now a whole host of software applications available in the "cloud" – accounting, order processing, manufacturing, projects, HR etc – supplied as "Software as a Service" (SaaS).

The key difference between SaaS and software you'd run "on-premise" is that SaaS is hosted remotely by a third party, usually accessed via the internet. This opens up a number of benefits, such as worldwide access, not having to buy the system, and not having to run it day-to-day. Instead you pay a form of subscription.

Like packaged on-premise software, the functionality available in a SaaS app is limited to what the system provides, including any configurable options. It may be possible to link to other systems and maybe to bolt-on additional functionality, depending on the APIs (application programming interfaces) available.

But unlike some packaged on-premise software, it is not usually possible to make any custom changes to SaaS software. SaaS systems typically operate on the basis that the software is shared amongst all the users. Any customer-specific functionality would either need to be made available to all users, or be switched on as an option. Unless you can come to a binding arrangement with the SaaS provider, it's best to assume what you see now is what you'll get.

This can be a benefit, as the lack of temptation to make changes is a key reason cloud systems are quicker to implement in sectors where heavy customisation is common.

If a SaaS system proves to be inadequate, it's tempting to think it would be easier than on-premise to change to another system. Sadly you would still need to repeat data conversion, change user procedures, re-training and all the other aspects of a traditional implementation.

It is therefore as important as traditional packages to ensure that the SaaS system selected will adequately do the job required. This is especially so as new SaaS systems may not be as well developed as equivalent on-premise systems. Depending on the range of SaaS options available, it is often worth comparing SaaS alongside on-premise options.

As with on-premise packages, it is still a good first step with SaaS to establish who is already using the system in organisations of a similar type and size to yours and in the same territories.

Having found potential SaaS offerings, a key advantage is that you can quickly trial the functionality, either free or at a low cost. The question then is to how to do so effectively. This is where a concise but comprehensive specification helps.

Specification

As a general rule, if you would have produced a specification for an on-premise system, it is worth doing so for SaaS. This is because:

1. **Vision and Objectives**: It is still worth setting out what you are trying to achieve, not only for selection but also for those people involved in the subsequent implementation
2. **Scope and Interfaces**: What do you want the system to cover? What other systems do you want to link to? Are the necessary APIs available?

3. **Key Reporting**: The right system should produce what you need quickly and easily. Best not taken for granted.
4. **Functionality**: This provides a concise checklist of what else you need the system to do, especially anything that may be unusual.
5. **Test Transactions**: A minimum range of transactions that adequately represent what you'll need the system to handle. Together with the functionality checklist, this provides the means to trial a system.
6. **Cloud Hygiene Factors**: Alongside the benefits come a new set of management issues such as security, data ownership and continuity of access. Whilst these can often be adequately overcome, it's worth checking each SaaS option for any weaknesses, especially for any show-stoppers.
7. **Assessing On-Premise Options**: The spec can also be used to assess on-premise options, either initially or if no satisfactory SaaS option is found.

In Conclusion

Usually the only functionality available in a SaaS system is what you see. Except for the simplest application, it's worth producing a specification. Properly constructed this specification can be used to trial SaaS systems, and if required assess on-premise packages.

▲ Top

case communications
Specialists in high-speed and rugged access solutions
Case, Dowty-Case, Cray, Case Technology Legacy Products
LINUX
NEWSLETTER
March 2011

In this edition:

Other newsletters:

Vodafone users lose connection in UK

The theft of specialist equipment prevented thousands of UK users from accessing the Vodafone network at the end of February this year.

Overnight, thieves stole specialist network equipment and IT hardware after breaking down a door at the Vodafone exchange facility in Basingstoke, Hampshire.

The damage left thousands of Vodafone users unable to make calls or send text messages since the early hours of the morning.

According to a Vodafone spokesman, "several hundred thousand" users were affected in the "M4 corridor area".

Internet forums and social networking sites were flooded with complaints as users were unable to use Vodafone's network for hours.

The spokesman claimed that 2G and 3G voice services were restored quite quickly but Vodafone voice-mail and SMS services took longer to restore.

▲ Top

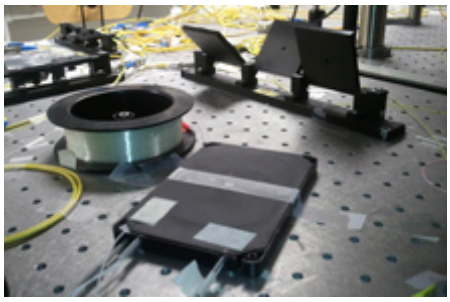
Case, Dowty-Case, Cray, Case Technology Legacy Products
LINUX
NEWSLETTER
case communications
Specialists in high-speed and rugged access solutions

March 2011

In this edition:

Other newsletters:

A quantum communications switch



The device that could one day let super fast quantum computers talk to each other

The Internet is made of photons that zip through fibre-optic cables and flow through devices like switches, modulators, and amplifiers. But those standard devices would be inadequate for super fast quantum computing or communications—experimental approaches that exploit the peculiar properties of particles at the quantum scale to carry out complex calculations incredibly quickly or to prevent anyone from eavesdropping on messages.

Commercial switches have various problems that make them unsuitable for re-routing entangled photons. Those that are made of micro-electromechanical components keep entangled states in tact, but operate too slowly. Other opto-electronic switches either add too much noise so that single photons are difficult to detect, or they completely destroy the quantum information.

Prem Kumar, professor of electrical engineering and computer science at Northwestern University, has developed a quantum routing switch that can shuttle entangled photons along various paths while keeping the quantum information intact.

The device could be particularly useful for quantum computing, says James Franson, professor of physics at the University of Maryland, Baltimore County. "To build a quantum computer using photons, we need the ability to switch [entangled] photons," says Franson. A quantum switch could also someday allow entangled photons from different quantum computers to be shared over long distances—like cloud computing, but with quantum information.

Kumar says the switch will also make ultra-secure quantum networks a reality. Today's information is typically secured using what's called public key encryption, which relies on the practical impossibility of performing certain mathematical tasks, like factoring extremely large numbers. Quantum networks would offer an even more secure alternative to public key encryption. Using entangled photons to communicate ensures security because any attempt to intercept a message would disturb the particles' quantum state.

To build the new quantum switch, the researchers used commercial optic-optic cable and other standard optical components, says Kumar. "My goal is to do things in the quantum information space that are very compatible with existing fibre infrastructures," he says

The first step is to prepare the photons. Entangled photons have properties, such as polarization, that are fundamentally linked. If two photons are entangled, then the measured polarization of one reveals the corresponding state of the other. The researchers used a technique in which they mixed together multiple wavelengths of light within a standard fibre to create entangled photon pairs.

The next step is to send one photon down the optical fibre to the switch, which changes the photon's course. The researchers' switch is made of only optical components, including a

spool of 100 meters of optical fibre arranged in a loop. One photon of an entangled pair is sent through one end of the loop, and through a multiplexer, while a powerful laser sends pulses of light into the spool. The photon is shifted in such a way that at the other end of the loop it separates out along a separate path, while remaining entangled with its partner.

The end result is a switch that's very fast, has low background noise, and most importantly, preserves the quantum information. Single photon detectors at the end of the fibres confirm that both photons maintained their entangled state, showing that the quantum information was preserved. The work is described in a recent issue of the journal Physical Review Letters.

"It's an important development, because switching photons is really the main difference in going ahead in further progress in quantum computing using photons," says Franson

▲ Top

Case, Dowty-Case, Cray, Case Technology Legacy Products
LINUX
NEWSLETTER
case communications
Specialists in high-speed and rugged access solutions

March 2011

In this edition:

Other newsletters:

Critical NASA network open to Internet attack

Network is used to run Space Shuttle, International Space Station and Hubble Telescope missions

Six NASA servers exposed to the Internet had critical vulnerabilities that could have endangered Space Shuttle, International Space Station and Hubble Telescope missions – flaws that would have been found by a security oversight program the agency agreed to last year but hasn't yet implemented, according to a report by the agency's inspector general.

NASA's CIO Linda Cureton says she has patched the vulnerabilities, but IG Paul Martin found that NASA still has no ongoing program for spotting and correcting similar problems as they arise and is giving itself until the end of September just to come up with a plan, according to the report titled "Inadequate Security Practices Expose Key NASA Network to Cyber Attack." The deadline for the plan is Sept. 30.

The six vulnerable servers were associated with IT projects that control spacecraft or contain critical NASA information, the report says. The audit also found other servers that exposed encryption keys, encrypted passwords and user-account information, all of which could enable attackers to gain unauthorized network access. The report didn't assess the agency wide network that isn't directly used for missions.

"These deficiencies occurred because NASA had not fully assessed and mitigated risks to the network and had not assigned responsibility for IT security oversight to ensure the network was adequately protected," the report says. "A security breach of a moderate- or high-impact system or project on this key network could severely disrupt NASA operations or result in the loss of sensitive data."

One server was found vulnerable to FTP bounce attacks, which if exploited, "could have significantly disrupted NASA's space flight operations and stolen sensitive data," the report says. Other servers weren't securely configured, exposing the encryption keys, encrypted passwords and user account lists to attackers.

The IG says NASA didn't know about these problems but could have if it performed broad risk assessment, part of the agreed-to security program. "As a result, NASA's Agency-wide mission network was vulnerable to a variety of cyber attacks with the potential for devastating adverse effects on the mission operations the network supports," the report says.

In addition to the oversight program on Internet-connected servers, NASA's CIO promises she will start a pilot program by Aug. 21 for spotting risks on the rest of NASA's networks that don't have Internet connectivity.

The IG performed port scans using Nmap and manually verified open ports. It also performed NESSUS vulnerability scans.

Top

Case, Dowty-Case, Cray, Case Technology Legacy Products
case communications
Specialists in high-speed and rugged access solutions
NEWSLETTER
March 2011

In this edition:

Other newsletters:

Newsletter Archive

Monitoring Linux network interfaces with vnStat

Getting network stats on a Linux machine is not particularly difficult. With tools like **sar**, **Iperf**, and **vnStat** available for nearly every distribution, command-line aficionados can get the low-down on their network with just a few useful commands.

Take, for instance, vnStat, a popular network traffic logger. vnStat is different from a network sniffer like **Wireshark** since it polls the network interface stats going to and from the kernel. Wireshark, on the other hand, actually monitors packets coming in and out of your machine.

As useful as vnStat is, it is still predominantly a command-line application, which can make it tricky to visualize what's going on with your machine's network interface. But there does exist a useful PHP-based front-end for vnStat that can generate useful reports from vnStat logs.

Because vnStat is very light on resources, running it full-time in the background will not affect your system's performance at all. Of course, running a Web server will, so you will need to weigh the benefits of having a nifty GUI for the traffic data.

▲ Top

case communications
Specialists in high-speed and rugged access solutions
Case, Dowty-Case, Cray, Case Technology Legacy Products
LINUX
NEWSLETTER
March 2011

In this edition:

Other newsletters:

Is £650m enough for UK cyber defences?

Prime minister David Cameron confirmed that £650m will be provided for UK cyber defences over a four-year period in the Strategic Defence and Security Review, and while this is about a third more than expected, the IT security industry has expressed concerns about how this will be allocated.

The announcement has been widely welcomed by the industry because it demonstrates the government understands the importance of cyber security defences, as well as joined-up thinking on how this integrates with national security.

"We need to fix the shortfalls in the critical cyber infrastructure on which the whole country relies," says Cameron.

The biggest concern of the IT security industry is around the allocation of funding for cyber security training, especially within law enforcement agencies.

Fighting the cyber war requires an army of prize troops, and the UK does not have enough of them, says William Beer, director, OneSecurity, PricewaterhouseCoopers.

"The people element is often overlooked in building strong cyber defences, but this funding will be vital in attracting top talent into the industry as well as providing security professionals with the best training and support," he says.

Although it is impossible to predict the future, says Beer, gaining insight into new developments will help to build better defences against potentially crippling cyber attacks

Judy Baker, director of the UK Cyber Security Challenge set up to identify and attract talent to the industry, says priorities for the funding should include supporting professional organisations that are working to constantly adapt to counter threats to our cyber security.

"We look forward to seeing the impact of such a significant investment in the sector and watch with interest to see how this investment can support the development of a pool of talented cyber security specialists upon which the UK will undoubtedly rely," she says.

Adequate investment in national and international cyber threat information sharing systems is another area of industry concern.

Cybercriminals have established cross-border alliances and trading markets to carry out and monetise their attacks, says Paul Judge, chief research officer at Barracuda Networks.

"Governments must do the same in order to effectively pursue these criminals," he says.

It remains to be seen if these objectives will be met by the establishment of a UK Defence

Cyber Operations Group, as outlined in the Strategic Defence Review.

Judge also highlights a common call for greater collaboration between the IT security industry to develop the best tools and the best policy.

The government must work with security experts from across the country, and if necessary the world, to produce a watertight, considered strategy to battle international cybercrime, says Rob Cotton, chief executive of NCC Group.

"While much of this protection can be achieved by patching simple vulnerabilities in existing networks, other threats will require specialist defence strategies and responsive action," he says.

The UK and US are drafting a Cyber Operations memorandum of understanding covering cyber security responses, the government says.

Having recognised the importance of cyber security and allocated funds for its provision, the government's real challenge is in allocating those funds in an effective way.

The funding, while a positive move, also has to be seen in perspective because, as IT security professionals point out, cyber criminals are extremely well funded.

The £650m is a large some of money, but this must be set against the enormous resources of the underground economy and the potential financial losses to the UK.

Top