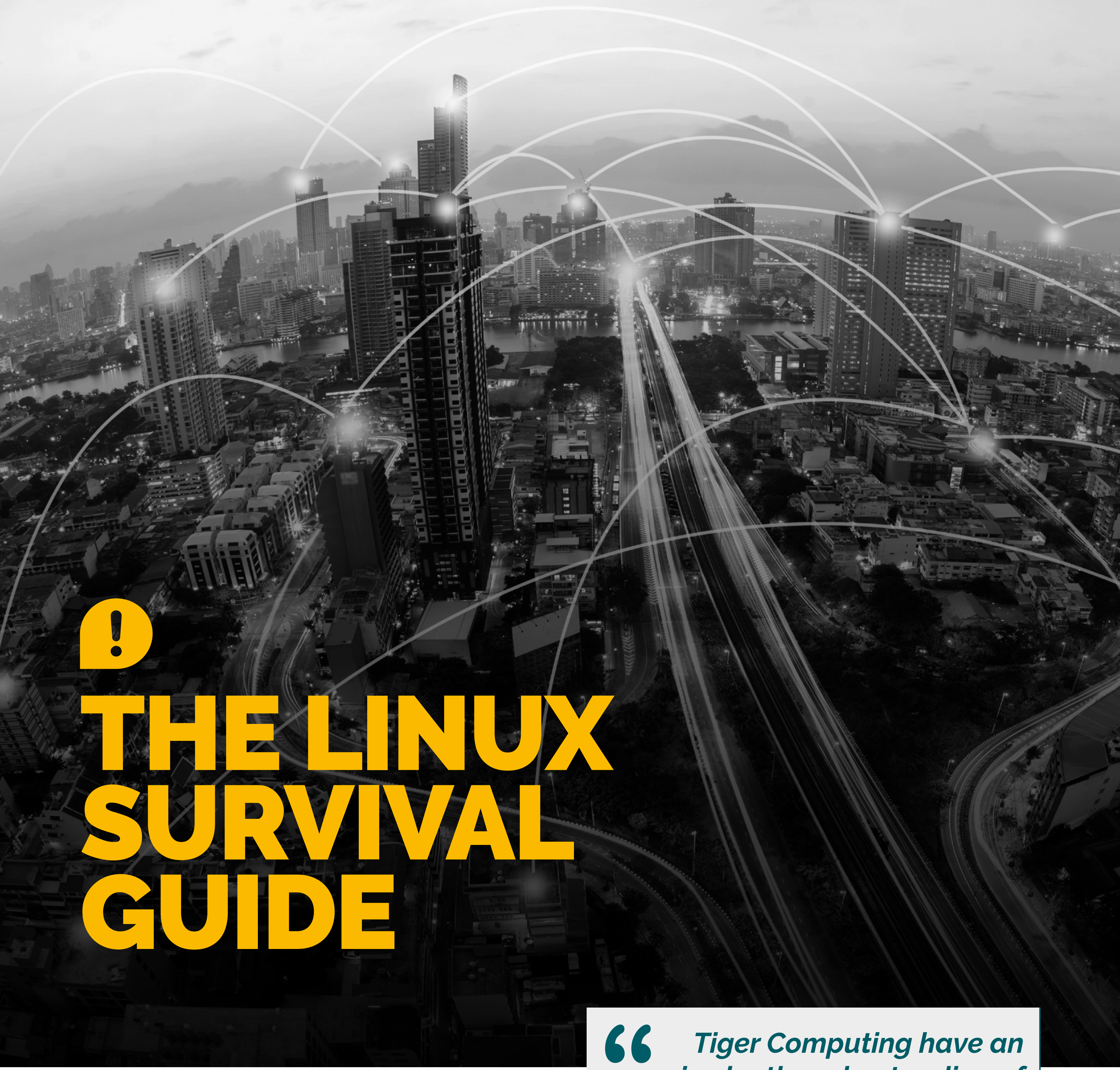


THE LINUX SURVIVAL GUIDE

> Tiger Computing have an in-depth understanding of Linux and how to use it in a business context
>
> **Timothy O'Hara**
> Managing Director
> *Rent4sure Ltd*

TIGER COMPUTING
Linux for Business

LEADING LINUX SUPPORT IN THE UK SINCE 2002

INTRODUCTION

For your business to survive (let alone thrive), you need to be aware of the risks, threats and challenges, and then you need to deal with them. "Survival" in this sense means:

- making sure you're not put out of business because of data loss
- not upsetting or, worse, losing staff because of unreliable IT systems
- not waking up at 03:07 worrying about backups

The threats you know about may cause you sleepless nights, but the biggest problems are often the ones that business managers are not even aware of.

In this guide, we'll explain what the common risks are, how to recognise them and what to do about them. The goal? To have reliable systems, secure data and not have your day interrupted by IT issues.

> *We believe that if you have to tell your IT company about a server problem, they have already failed.*
>
> **Keith Edmunds**
> Managing Director
> *Tiger Computing*

LET'S GET STARTED

BACKUPS

Oh, we know. There must be something more boring in life than backups, but nothing immediately springs to mind. Like dental check-ups, updating your gym programme and returning Aunt Alice's call, maybe tomorrow. That'll be fine.

Until it isn't.

Once you really need the backups, there's nothing you can do to create them.

For backups to be effective:

- They need to be automated
- They need to actually run. This is best checked by effective, automated monitoring
- They need to complete without error. Again, this is best handled by monitoring.
- They need to complete within (or by) a reasonable time. What is "reasonable" will vary from businesses to business, but for many they should complete before the start of the working day. Yet again monitoring is the answer.
- You need to backup the right data. Some of your data will be business critical data. That's data that, if lost, would threaten the survival of your business. Maybe it's personal, GDPR-type data. Or maybe it's your Intellectual Property, the very purpose of your business. Identify that critical data, and ensure that it is backed up off site.
- They need to be stored off site. By all means, keep a local backup for convenience, but make sure you have your key backups stored off site.
- You need a clear, documented process to restore data from the backups. In this documentation, it's safe to make assumptions about the reader's skill levels but not their knowledge. Instructions such as "log into the backup system" will need more detail ("by going to the following URL and logging in with the credentials stored at X"). Store those instructions off site, too, for hopefully obvious reasons.
- The restore process must be regularly tested. This is the only way to be sure you have usable backups of the right data. They should be tested by someone who has had no involvement in setting them up or managing them on a day-to-day basis. Don't wait until you need the backups before you test them. In the heat of the moment, with the pressure on to restore your data, you'll be grateful for a clear, tested, step by step process.

Backups. Boring but essential.
Make sure they're working as you expect before you need them.

SYSTEM UPDATES

If your data matters to you, keeping your systems up to date is not optional.

Barely a week goes by without a security update to some part of Linux. Many of those security updates address a proven vulnerability, and those vulnerabilities are public knowledge.

You need a maintenance process to keep your systems in top form. Installing security updates as they're released is good IT hygiene.

Your Linux distribution will provide updates for much of the software installed on your systems. How long each Linux release receives security updates for depends upon the distribution and, in some cases, the specific version of Linux installed. Most Linux distributions will provide security updates for between three and ten years after initial release.

Any third party software will need special handling for updates. Here are some options:

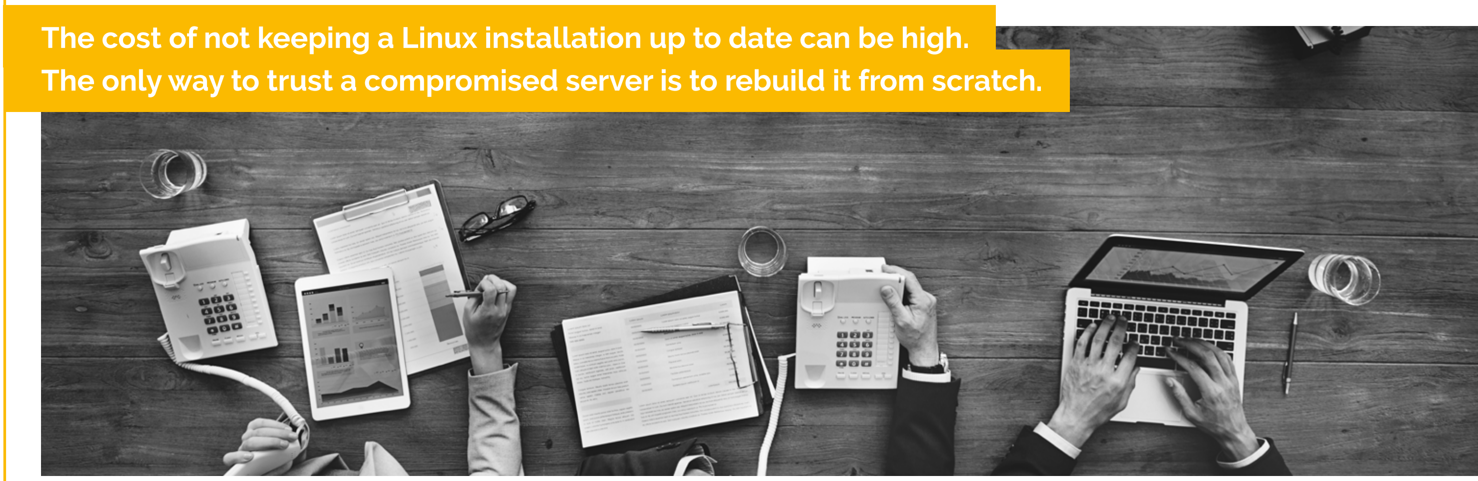
- If the software vendor makes a package repository available, use that. This means that updates to their software will be included in the routine system security update. This makes installing updates much simpler.
- Subscribe to the vendor's "security updates" mailing list. You can then manually update the software when new releases become available.
- Check for updates with the vendor from time to time.

If you develop software in-house, package it using your distribution format before installation. This simplifies both system management and software updates.

At some point you'll need to upgrade the operating system itself. This is more complex than installing routine security updates, and has the potential to be more disruptive. Plan for it and test the new release in advance.

Do not run unsupported versions of Linux in production. Even when the server is not exposed to the outside world, running unsupported systems is not recommended.

The cost of not keeping a Linux installation up to date can be high. The only way to trust a compromised server is to rebuild it from scratch.



MONITORING

You can either fix system problems before they impact your business or after. We've found "before" works better for most people.

Status monitoring will warn you of impending problems. It gives you the chance to fix them at a time convenient to you, and it will help keep your systems secure and available.

There are plenty of Open Source system monitoring programs. If you're not sure what to monitor, start by installing one and accepting the defaults.

If you experience an issue that the monitoring didn't pick up, add it to your monitoring. If you follow that rigorously, you'll soon have a comprehensive monitoring setup that's specific to your environment.

Many of the status monitoring parameters can also be tracked over time to show trends. For example, it can be useful to monitor how a disk fills up over time which in turn lets you then make a reasonable prediction of when to expand disk capacity.

There are also some things you shouldn't do with monitoring:

- Don't monitor what you won't react to. If you get an alert when your system load is high, what will do you do? After all, you want the system to earn its keep so it being busy is not, in itself, a problem. Instead, monitor how long it takes to do some meaningful work such as render a specific webpage.
- Don't have your systems send you automated emails. A mail saying, "Backups completed OK" is of little value (and will you notice when it doesn't arrive?). Report all status information via the monitoring system.
- Don't ignore errors. "Known issues" can mask deeper problems. If your monitoring system has reported a problem, fix it.

In the same vein, there is no need to reboot Linux servers on a regular basis. If you find you need to, fix the underlying problem that the reboot addresses.

Effective system monitoring will result in both better system availability and less stress.

TICKETING SYSTEM

Good record keeping is part of effective system management.
In this context, record keeping takes two forms: tickets and documentation.

A ticketing system is almost a necessity if you are managing IT systems, and there are some very good Open Source solutions available. If you don't have a ticketing system in place today, pick one, install it and start using it.

Tickets are a way of tracking work items. Those work items might be requests for changes or details of incidents that impact your systems. Tickets can track:

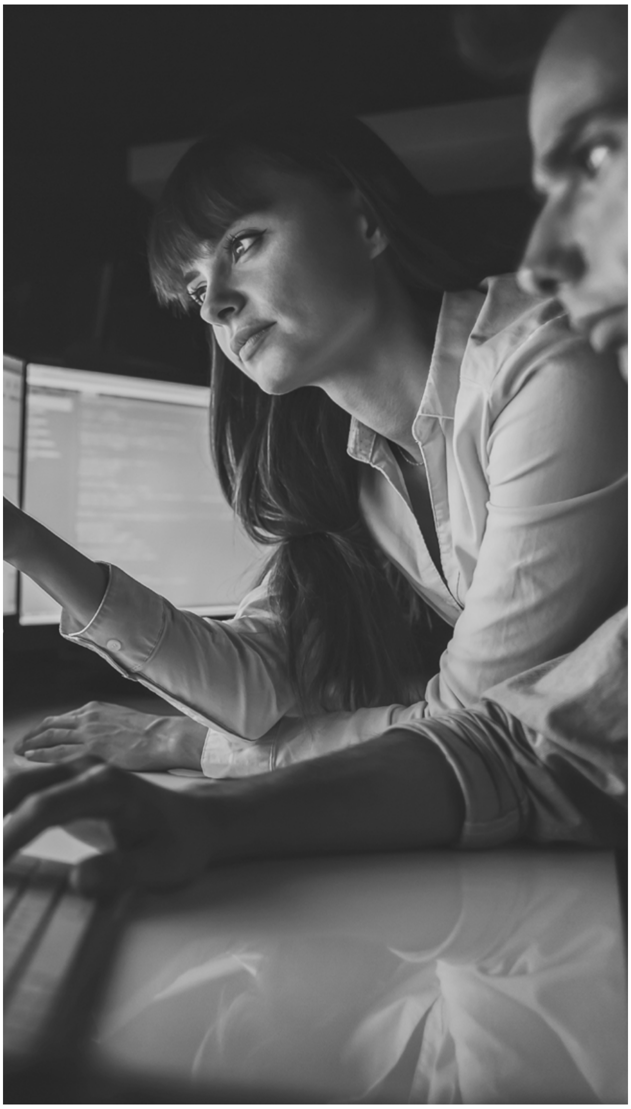
- the status of work (pending, in progress, or completed)
- who's doing what
- which systems are affected
- the priority of the work
- ...and much more

They can maintain a record of communication and comments about the work. Now you'll know who did what when, and you have a record of that for future reference, too.

The second part of record keeping is documentation, the bane of IT people everywhere. We all want perfect documentation so long as someone else writes it.

When the documentation is lacking or, worse, incorrect, the impact ripples outwards. A lack of clear, accurate documentation means more reliance on key personnel for their knowledge rather than their skill. It also means that the same task will be performed differently depending upon who performs it.

> ***I've been faced with knowing more than the tech guys many times in the past, but never with Tiger Computing. They make stuff work without fuss, fanfare and hyperbole.***
>
> **Dr Jonny Wray**
> Head of Discovery Informatics
> *e-therapeutics plc*



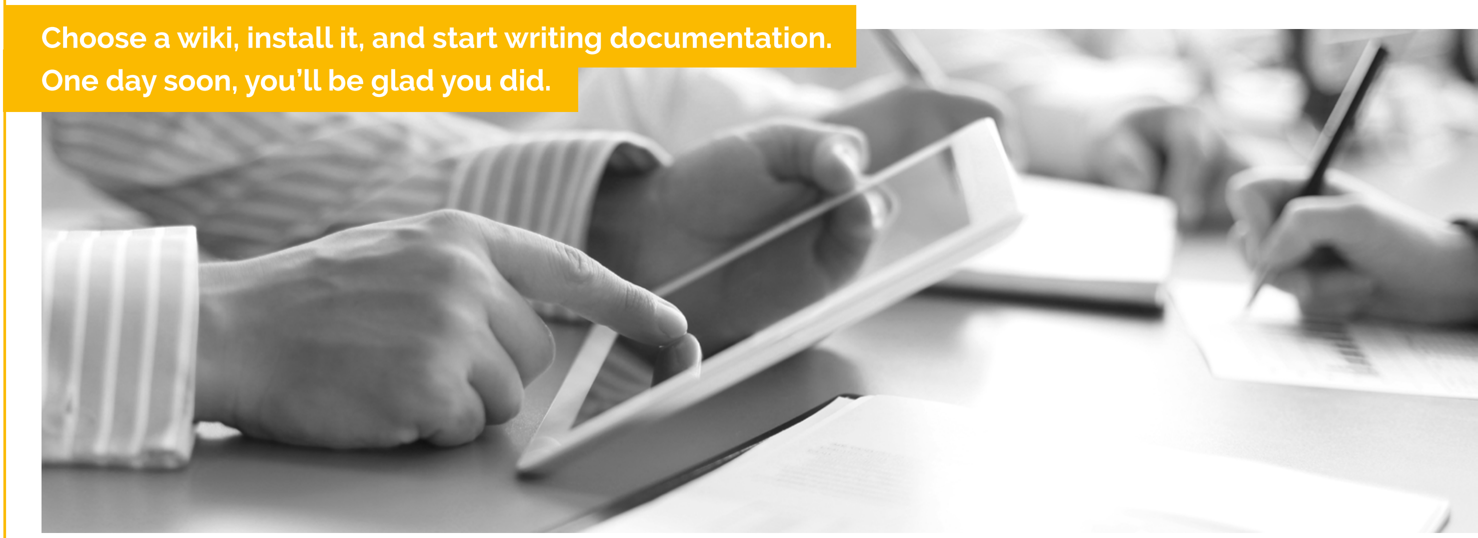
DOCUMENTATION

Your documentation system needs to be:

- **Scalable:**
  Your infrastructure is likely to grow over time, and the documentation system must be capable of scaling with it. The handy notebook might work when there are three people and one server, but it won't scale much beyond that.
- **Resilient:**
  Documentation needs to be backed up, which implies it should be online. Handwritten notes on a printout will not be there when the documentation is reprinted.
- **Secure:**
  As ever, security is a balancing act. We want to keep our documentation up to date and accessible, but we also need to control who may read and update it.
- **Accurate:**
  Inaccurate documentation is not only confusing: it also casts doubt on the validity of the rest of the documentation. It must be everybody's responsibility to report or correct errors in documentation.
- **Accessible:**
  Documentation needs to be easy to find and easy to read. It should be clear, and it should be recognised that keeping it clear is an ongoing task.
- **Complete:**
  Do not rely on people's knowledge and experience. Capture that knowledge in documentation, which will still be around long after the knowledgeable person has left your business.

The days of printed process manuals on the bookshelf are (or should be) long gone. Today, a wiki is a simple, pragmatic and low-cost solution and there are some very good Open Source wiki systems available. Whilst it is worth putting some thought into what features you need, don't make that process too long.

Choose a wiki, install it, and start writing documentation. One day soon, you'll be glad you did.



INFRASTRUCTURE PLAN

At the start, setting up an AWS instance or a local hardware server is easy. As soon as you need a second instance, or a second server, you also need a plan. It's easy to set up more resources to fix today's issue, but in reality that often merely postpones the problem.

If it seems that you always have "just one more issue to fix", the real problem may be the lack of a thought-through plan. A plan – even an imperfect one peppered with caveats – will make your thinking clearer and your infrastructure more efficient.

There are two parts to an IT plan: an analysis of the requirements and an implementation plan. The requirements should focus on what you are trying to achieve, not how it could be achieved. The requirements also double as a check list later: is everything you need now in place?

The requirements can include known issues: "There are no off-site backups". Recognising the issue is the first step in resolving it.

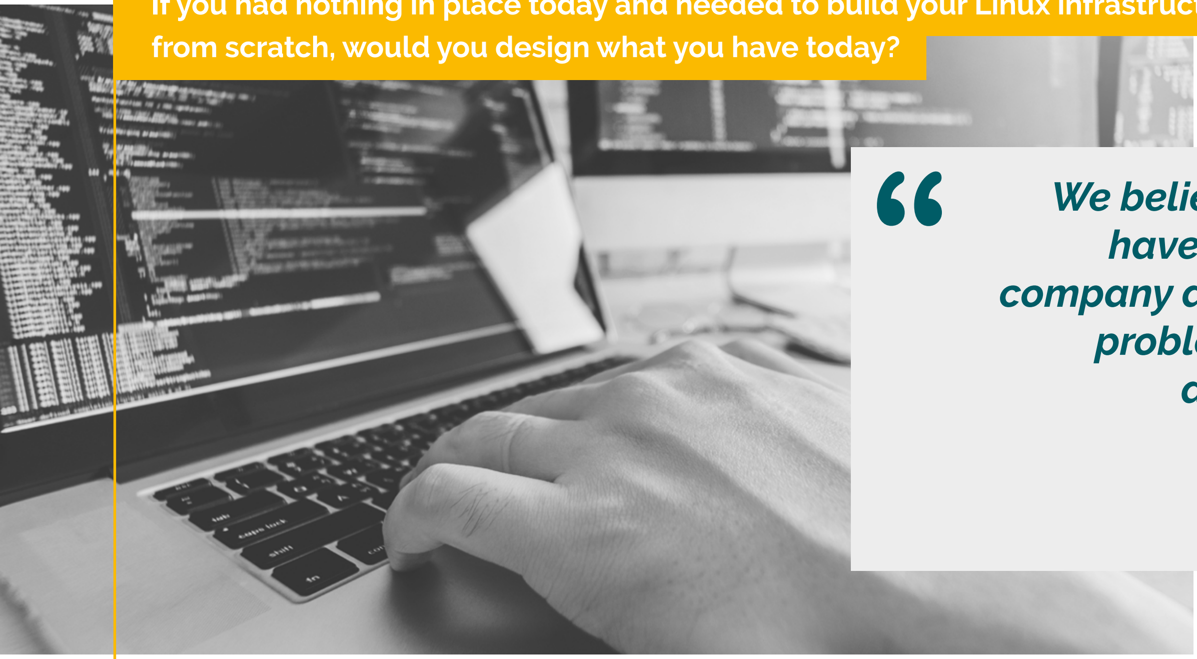
Questions such as whether you should be in the cloud or in a local data centre are a matter of implementation. The implementation plan should define the most cost-effective way of meeting your requirements.

Symptoms of poor planning include:

- Not having enough disk space available where you need it
- Wasting money on the cost of too many cloud instances
- Frequent firefighting
- Emergency hardware purchases

The plan should be reviewed regularly – at least annually - because both the requirements and reality change.

If you're unconvinced, look at it another way.
If you had nothing in place today and needed to build your Linux infrastructure from scratch, would you design what you have today?



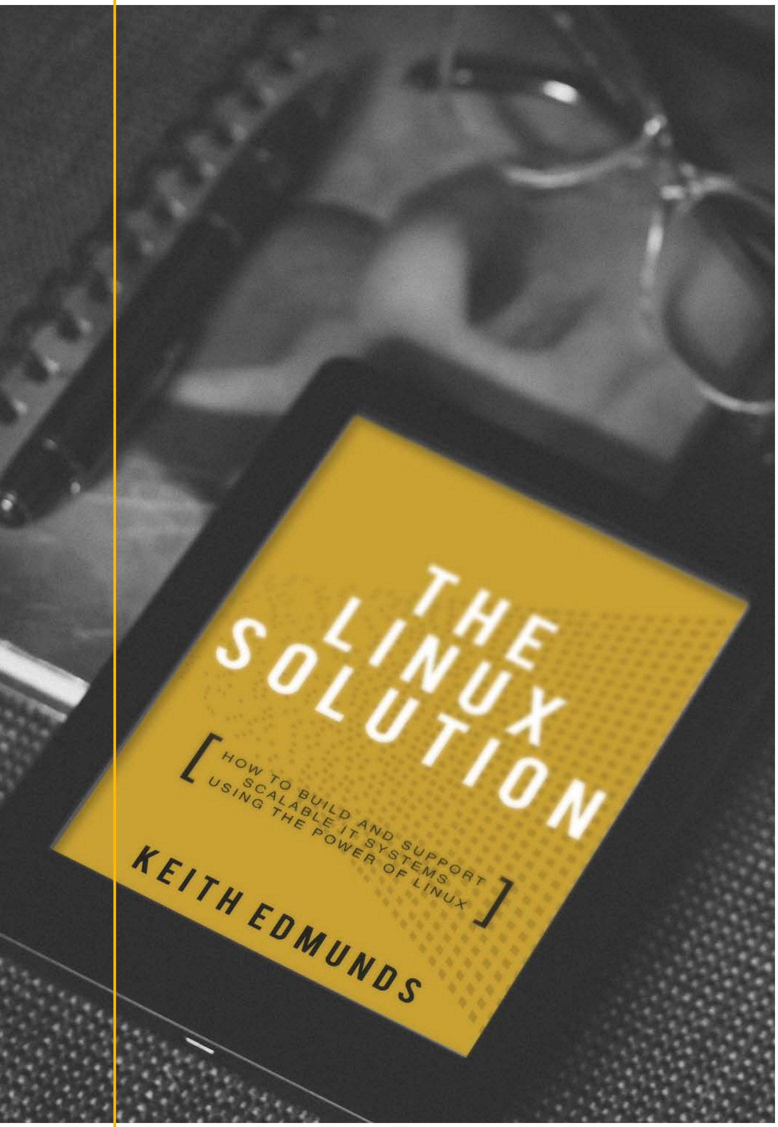
> ***"We believe that if you have to tell your IT company about a server problem, they have already failed.***
>
> **Keith Edmunds**
> Managing Director
> *Tiger Computing*

THE LINUX SOLUTION

We've covered all the above, and much much more, in our Amazon #1 best selling book, "The Linux Solution".

If you're using Linux for business - whether in the cloud or on local hardware - then you need to read this book.

It's written for CTOs, department heads, and anyone responsible for Linux in a business context. It describes a proven methodology to design, build and maintain a world-class Linux infrastructure.


THE LINUX SOLUTION
[HOW TO BUILD AND SUPPORT SCALABLE IT SYSTEMS USING THE POWER OF LINUX]
KEITH EDMUNDS

You can download a PDF of the book for free by going to:

www.tiger-computing.co.uk/download-book

READER REVIEWS

> *This is a rare definitive guide around deploying and managing Linux-based servers and systems. The author clearly has great real-life operational experience.*

> *This book is clear, concise, well thought out and methodical, leaving the reader educated and enlightened. A great read - for the novice and the experienced. Highly recommended.*

> *The book is very well written. It does not preach but just makes it clear on what to focus on and gets you asking the right questions.*

> *Full of practical tips and ideas, this book captures in an easily digestible format the kind of knowledge that can only be achieved through years of hands-on, real-life experience. A must read for IT managers everywhere.*

> *Decades of invaluable experience and learning distilled into a simple, easy to understand guide.*

ABOUT TIGER COMPUTING

We've been building and supporting Linux solutions for businesses since 2002, and we've worked with companies like Ericsson, the NHS and leading BioScience companies.

We have Red Hat Certified Engineers and accredited Debian Developers on staff, and we're certified under ISO27001, the Information Security standard. We write a regular business column for an industry magazine, and in March 2019, our book "The Linux Solution" was published and went on to be an Amazon #1 best seller.

We work only with Linux. We work with it all day, every day, and we understand how to get the best from it.

WEB:
www.tiger-computing.co.uk

EMAIL:
info@tiger-computing.co.uk

PHONE:
01600 483 484

> *Tiger have had a major impact on our business. Their careful and professional management has entirely relieved the team of any Linux system admin responsibilities.*
>
> *Their Linux expertise is obvious from every interaction we have.*
>
> **Ross Fraser**
> Head of Bioinformatics
> *Synpromics Ltd*

WE BELIEVE THAT IF YOU HAVE TO TELL YOUR IT COMPANY ABOUT A SERVER PROBLEM, THEY HAVE ALREADY FAILED.

HERE'S A CHECKLIST TO GET YOU STARTED:

BACKUPS

❒ They're automated

❒ They are monitored to ensure they run...

❒ ...and complete without error...

❒ ...within a reasonable time

❒ I've identified the business critical data

❒ The business critical data is backed up off-site

❒ I have a documented process to restore my business critical data

❒ I've tested that restore process

❒ Someone else has tested the restore process

❒ There's a copy of the restore process held off site

❒ At least three people know where that process is held

UPDATES

❒ My systems are fully up to date

❒ I have a process that ensures they are kept fully up to date

❒ That process includes all third-party software installed

❒ All my in-house software is packaged for my production systems

❒ I know when the next major release of my chosen version of Linux will be

❒ I have a strategy for testing my systems using the next release

> ***“Working with Tiger Computing saved us a huge amount of time and money***
>
> **Mike Smith**
> Managing Director
> *Cadmia Ltd*

MONITORING

❒ I have status monitoring in place

❒ Someone is notified when the monitoring system detects a problem

❒ We have a process to follow for every possible notification

❒ We don't have ad hoc emails to report on systems: everything is managed via the monitoring system

❒ We have no “known errors” that are not actively being worked on

❒ We do not regularly reboot any of our Linux servers

❒ I have trend monitoring in place

RECORD KEEPING

❒ We are using a ticketing systems

❒ All incidents and requests are recorded on the ticketing system

❒ We have a documentation system in place

❒ The documentation is up to date

❒ We don't rely on the knowledge stored in anyone's head

PLAN

❒ We have a written IT plan

❒ The plan separate requirements from implementation

❒ The requirements section lists known infrastructure issues

❒ We review the plan at least annually

❒ The date for the next plan review is in the calendar

THE LINUX SOLUTION

❒ I've downloaded the PDF

❒ I've read the book

❒ I've decided to get a physical copy of the book

❒ It would be nice if the author would sign it. I'll mail him and ask: you never know.