Five things you need to know about disaster recovery planning

It's time to make disaster recovery a high priority

IT is integral to business. The infrastructure you support is critical to keeping your company up and running. But faced with the constant challenge to do more with less, you may have been forced to put some projects on the back burner. If disaster recovery is among them, you're probably keen to return it to the front of the priority queue, and with good reason.

Reports of potential risk in the world—such as turbulent weather, natural disasters and man-made accidents—seem to clog the media. What would happen if the ceiling collapsed in your data centre? What would you do if an employee forgot to unplug a humidifier and the power grid feeding your servers and storage imploded?

This guide discusses five elements that should be considered as part of your disaster recovery planning:

1. Mixed-platform data centres—the challenges they pose
2. Virtualisation—how it can change everything
3. Cloud computing—on-demand resource delivery
4. Measuring the return on investment (ROI) of disaster recovery
5. Planning and testing for greater confidence

The challenges of the multi-platform data centre

Most data centres used to be based on single-vendor mainframe computers and so were fairly easy to manage. Then inexpensive servers built with cheap x86 processors came along and quickly found their way into the data centre. The move from mainframes to smaller servers made the data centre strategy simple. When you needed torun more applications, you just bought more servers—leading to server sprawl.

Virtualisation solved the problem of sprawl by enabling data centres to be consolidated to a more manageable size and footprint. But all these changes overlapped, and because a typical data centre has evolved over a number of years, it now contains a variety of platforms from various vendors—a mix of mainframe, x86 servers and virtualised resources.

The impact of that on disaster recovery planning means multiple plans, one for each platform. Or does it?

Virtualisation: Simplified disaster recovery planning

You can use the virtual resources in your data centre for more than just virtual machine recovery. Virtual machines are flexible. They can run many different types of workloads, so you can create a virtual recovery platform that offers protection for all your workloads—physical, virtual, Windows and Linux.

Virtual recovery plans can simplify, and in some cases eliminate, many of the platform-specific headaches of recovering from a disaster.

The process for recovering a physical server typically involves a number of steps, from acquiring an equivalent or compatible physical server; through installing the operating system, applications, patches and updates; to uploading the backup data.

When you use virtual recovery, all those steps become a thing of the past. To recover a physical server you simply need to power on its virtual equivalent—an elegant approach that can save a great deal of time for users and the IT department.

Cloud computing: Disaster recovery resources on demand

However efficient your disaster recovery planning is, there are still a number of unknowns. You don't know when you'll need those extra resources, how many you'll need, or for how long.

Cloud computing has a number of characteristics that make it easier and cheaper to plan for the unknown aspects of disaster recovery: rapid elasticity; on-demand, self-service resource acquisition; and per-use billing. Taken together they offer a resource-consumption model that makes cloud computing a perfect solution for disaster recovery.

But how do you get there? Virtualisation is the main technology underlying the cloud delivery model. So the first step is to virtualise as many of the elements that make up your disaster recovery plan and infrastructure as possible.

For more information:
Worldwide: +1 713.548.1700 • **N. America Toll Free:** 888.323.6768
E-mail: info@netiq.com • NetIQ.com

NetIQ®

Measuring the ROI of disaster recovery

Virtual machines are a cheaper way to run workloads, this is an accepted reality. Not only do you dramatically lower your server hardware costs, you also reduce the cost of power, cooling and maintenance.

As part of a disaster recovery plan, one virtual machine host can take the place of up to 20 or more traditional standby physical servers. You can eliminate the expensive duplicate infrastructure that data centres used to need, and the burden of keeping backup versions of each make, model and vendor version of all the servers you run.

Replacing all of that with a simple pool of virtual resources immediately reduces the cost of your disaster recovery plan. But infrastructure isn't the only thing that costs money, time costs too. Virtualisation saves you time by reducing the overhead and labour associated with older backup and recovery-based protection approaches. With virtual machines, everything from day-to-day maintenance to recovery and testing, can be as simple as a few clicks of a mouse.

Planning and testing for greater confidence

When was the last time you tested your ability to restore a workload? How many did you test? And what fraction of your total workloads was that? If organising the testing is simply too challenging, the risk is that it never gets done.

But lack of adequate testing leads to lack of confidence. How can you be sure your plans will work? How can you publish and guarantee service levels without an accurate prediction of what a worst-case scenario will look like? Ambiguous service levels, such as 'one or two days', are no longer acceptable.

Virtualisation makes testing much more straightforward by eliminating the issues associated with a bare-metal restore. You don't need to match hardware or go through multiple steps to get a test server up and running. You simply select the virtual machines you want to test, create copies of them, and power them on—with no disruption to your production processes.

The ability to run frequent disaster recovery tests lets you accurately measure the time you expect to take to recover workloads when needed. Instead of hoping that you can recover from an outage in a day or two, now you can guarantee an accurate recovery time objective (RTO).

This can even be a competitive advantage for your company. People want to know that you can help them get back to routine as quickly as possible after a disaster. Your customers' confidence in your organisation will get a huge boost when you publish service levels that you're confident about.

Next steps

Take some time to review your current disaster recovery plans. Virtualisation and cloud computing make disaster recovery much easier, but moving to either of those technologies require's a certain amount of effort, time and planning.

Initiate some conversations within your organisation about the business-critical nature of their activities and the applications they use. This will help you understand the RTO needs of each workload running in the data centre.

Required uptime and allowable downtime for workloads

Required availability	Required uptime hours / year	Allowable downtime / year
90% (0.9)	7,889	36.5 days
99% (0.99)	8,678	3.6 days
99.9% (0.999)	8,757	9 hours
99.99% (0.9999)	8,765	50 minutes
99.999% (0.99999)	8,766	5 minutes

Use the uptime-downtime chart above to talk to users about the cost impact these service levels might translate to. For example, if your order processing application is classified as having three nines (0.999) of importance, how many transactions would be lost or delayed—and what would that cost—if you allow for nine hours of downtime? Does that align with the cost of providing a three-nines guarantee?

There's a lot to consider when you review, update or redefine your organisation's disaster recovery plans. Arm yourself with as much knowledge as you can and start talking to people. With the complexity of modern data centres, the budgetary constraints many of us are working under, and the new techniques available to aid disaster recovery planning, these are important discussions to have as soon as you can.

Find out more

Product information:

http://www.novell.com/products/protect/

Customer success stories:

http://www.novell.com/success/hps_pharmacies.html

http://www.novell.com/success/reed_smith.html

White paper:

www.novell.com/consolidated-dr-wp.pdf

Webinar:

http://www.novell.com/media/dr

Austria: +43 1 595 43 35 0
Benelux: +31 (0) 172 505 575
Europe: +44 (0) 1784 454 500
France: +33 1 46 04 10 10
Germany: +49 (0) 89 99351 0
Italy: +39 02 9906 0201

Middle East: +971 50 650 8224
Nordics: +46 8 630 1700
South Africa: +27 11 700 4250
Spain: +34 (0) 91 151 71 11
Switzerland: +41 43 399 2090
UK: +44 (0)1784 454 500

NetIQ Europe Limited
Building 2,
2nd Floor
Parkmore East Business Park
Galway,
Ireland

Worldwide Headquarters

1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: +1 713.548.1700
N. America Toll Free: 888.323.6768
info@netiq.com
NetIQ.com
http://community.netiq.com

For a complete list of our offices in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit **www.netiq.com/contacts.**

Follow us:

561-A41001-001 DS 02/12