BROADBAND TESTING

Remote Working: Avoiding Downtime And User Productivity Losses

A Broadband-Testing White Paper

First published April 2020 (V1.0)

Published by Broadband-Testing

E-mail : info@broadband-testing.co.uk
Internet : HTTP://www.broadband-testing.co.uk

Please note that access to or use of this Report is conditioned on the following:

1. The information in this Report is subject to change by Broadband-Testing without notice.

2. The information in this Report, at publication date, is believed by Broadband-Testing to be accurate and reliable, but is not guaranteed. All use of and reliance on this Report are at your sole risk. Broadband-Testing is not liable or responsible for any damages, losses or expenses arising from any error or omission in this Report.

3. *NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY Broadband-Testing. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY Broadband-Testing. IN NO EVENT SHALL Broadband-Testing BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.*

4. This Report does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products, or that the products will meet your expectations, requirements, needs or specifications, or that they will operate without interruption.

5. This Report does not imply any endorsement, sponsorship, affiliation or verification by or with any companies mentioned in this report.

6. All trademarks, service marks, and trade names used in this Report are the trademarks, service marks, and trade names of their respective owners, and no endorsement of, sponsorship of, affiliation with, or involvement in, any of the testing, this Report or Broadband-Testing is implied, nor should it be inferred.

TABLE OF CONTENTS

BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do… The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process.

Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

EXECTIVE SUMMARY

- Remote working and the need to support 24x7 access to critical applications and data has been on a gradual increase over the years, especially within the IT industry itself, but recent global events have shown that what might have been seen as an occasional alternative, might now become the norm across most industries.

- While there is undoubtedly a mindset change required by some employers and employees in order to fully embrace remote working, more important still is the ability of the IT infrastructure to support that remote workplace shift. Historically, solutions to enabling data and application access at the Data Centres (DCs) or server farms have been centred around hardware-based Load-Balancers/Application Delivery Controllers (LB/ADCs), but increasingly the software-managed virtual appliance is taking over.

- Key to the virtual LB/ADC approach is near infinite scalability and flexibility. For decades, IT has talked about "on demand" resource, both for performance and economy reasons. Now, the ability – using cloud-based architectures – to deliver this resource, and thereby support high-level, redundant 24x7 access to those critical applications and data sources is available, and at an affordable cost.

- A primary example of this approach is Kemp's Virtual LoadMaster (VLM) especially in uncapped, "MAX" format, where performance is designed to be infinitely scalable, on demand. In a world where there are no certainties, other than a combination of change and ever-increasing need for flexible and scalable IT architectures, VLM MAX makes a huge amount of sense as a critical foundation of a contemporary IT architecture.

DOWNTIME – THE SEQUEL…

Downtime – the data delivery devil of IT; the most reported end-user problem and the death knell of many an IT support individual.

And now, thanks to recent and – as we record here – ongoing global events, forcing a mass change in working habits, the dreaded "D" word has raised its presence more than ever. OK – so the aforementioned global events, leading to a forced human lockdown and the need to work from home for many, may seem relatively trivial, given the number of homes/home offices with Internet connectivity nowadays. However, as many who are new to the experience are finding, the home connection is only a minor part of the solution and the potential issues it raises.

Even where an IT solution – maybe an application, or a security authentication mechanism - has been designed for mass, global usage, a sudden ramp-up in users can cause outages, either local or total. One high-profile casualty early during this lockdown period was Microsoft's Teams unified communication and collaboration platform, while problems were reported across several platforms by end users, such as Zscaler's global cloud-based Internet security authentication solution.

But, such examples – regardless of the extremity of the situation – are not inevitable as many assume; they are absolutely avoidable. On a more regular basis, users of remote/virtual desktop applications report common outages, being logged out mid-session or unable to connect. Again, these are completely avoidable and are rarely resolved by the application provider themselves (see second boxout).

Even networking giants within the IT-world itself have reported massive increases in the number of help desk tickets being generated as a result of the work force shifting to homeworking almost overnight. Reports from the national media are suggesting that the situation in terms of office versus homeworkers won't go back to how it was, with many employees - for companies who have sent all staff home - already starting to question why they had to go in to the office in the first place.

Homeworking Could Become The New Norm – And With New Problems

Even the mainstream newspapers are identifying that the current homeworking shift could easily become a permanent trend. The Guardian recently noted that "many employees for companies who have sent all staff home are already starting to question why they had to go in to the office in the first place."

While, understandably, large technology firms were some of the first to make the switch to remote working for all their staff, the required technology is available for any company in any line of business. Looking beyond business and industry, education is another obvious candidate for more home-based connectivity being a long-term option.

Matt Mullenweg, chief executive and founder of WordPress, which is used globally to create a web presence, noted: "Millions of people will get the chance to experience days without long commutes, or the harsh inflexibility of not being able to stay close to home when a family member is sick… This might be a chance for a great reset in terms of how we work."

However, changes in usage patterns create more and different problems for service providers and DC management. In Italy for example, during the nationwide quarantine, peak internet traffic went up by over 30% and usage overall increased by around 70%. Moreover, from a traffic management perspective, usage patterns shifted, so peak traffic was occurring earlier in the day in impacted regions. The change in bandwidth peaks and troughs was further impacted by national school suspensions, meaning housebound schoolchildren were competing with workers for data and application access and Internet bandwidth in general.

And it's not simply remote/homeworkers who are increasing pressure on the existing IT and Internet infrastructure; with schools suspended in many countries, network traffic normally seen only in the evenings is flooding daytime connections.

Key to application and data availability however is primarily at the data centre (DC) or wherever those applications and data reside. Server overload – whether CPU, memory, disk access or network access – is not a new issue, but it is still the primary cause of unavailability and user frustration and, more importantly, loss of productivity. And, as noted previously, it is – in 99.999% of circumstances - completely avoidable.

Connection Loss: A Real-World “Frustrated Customer” Example

Here’s a genuine online conversation between Microsoft and a Windows 10 user experiencing ongoing problems using that platform’s integrated Remote Desktop Connection (RDC) application, commencing with the user request: “I have installed Windows 10 on five computers or my home network and I am finding that connections established using Remote Desktop Connection keep dropping out after about 10 seconds. This happens with connections between any two computers. I never had this problem before I upgraded to Windows 10.”

And here was the response from Microsoft (as printed), via the online help forum:

Method 1: Run network trouble-shooter.

Press Windows + X key.

Select Control panel.

In the search box, type Trouble-shooter and then click Troubleshooting.

Under Network and Internet.

Click on Network adaptor and Click on Next button.

If the issue still persist, I suggest you to perform method 2.

Method 2: Update Network adaptor.

Press Windows key + R key.

Type devmgmt.msc and press Enter.

In device manager go to Network adaptor.

Right click and click on Update drive software.

And here’s the feedback from the user: “This issue is still here. Remote desktop on Windows 10 keeps dropping out, even on gigabit Ethernet links.” Then followed more radio silence from Microsoft, prompting the customer to add: “Come on please Microsoft. This needs sorting out. I remote work all the time. Remote Desktop dropping the connection every two minutes for almost as long is not helping my work. All I can find is proposed solutions to this problem for Windows 8, none of which has worked for me”, followed by more radio silence and finally, the inevitable: “Anyone out there know of a good alternative to RDP? “

Moral: Don’t rely on the application vendor for assistance!

Then there is still the security issue to consider – another major cause of downtime. Preventing attacks is a 7x24, millisecond by millisecond process, as literally every few seconds a new threat is launched, in addition to the millions already out there and being constantly relaunched. Endpoint security – i.e. some form of antivirus (AV) software or other endpoint detect and response solution – on your laptop/PC/phone/tablet is still a primary barrier, but attacks at the server/DC are far more common – and damaging - as they impact on potentially thousands of users with one hit, not a single endpoint.

So, what is the solution to enabling remote working *en masse*, without users suffering application and data access outages and slow, to the point of near-unusable, performance? We will now look at the critical data and application access point – at the DC or server farm – a focal point of Broadband-Testing reviews and reports for over two decades and how LB/ADC technology in a contemporary, cloud-based architecture can provide that 24x7 access to a user base, wherever they are. Listed below are what we consider as key requirements in creating such a solution.

THE LOAD BALANCER (LB)/ADC SOLUTION BUILDING BLOCKS

Key to enabling 24x7 access to data and applications are flexibility and scalability.

Recent events have shown that, for all the predictive algorithms in the world, there are times when – out of the blue – more, far more, resource is required than ever anticipated and not at expected or typical times of day (or night). Historically, at Broadband-Testing, we’ve seen fixed hardware solutions that were designed to deliver to a given level of performance, in terms of data throughput and server accessibility, but then hit the buffers, due to the – literally – physical limitations of the design and architecture. This included key acceleration technologies such as SSL offload (primarily for speeding up https traffic) as well as WAFs (Web Application Firewalls), where a hardware-based architecture would eventually become overloaded. Moreover, these limitations meant that, in estimating peak throughputs, solutions for ADC (Application Delivery Control) were often over-specified and incredibly expensive. And still limited.

Moving from a physical to a virtual LB/ADC environment, as typified by Kemp’s Virtual LoadMaster (VLM) sees those estimations replaced by capacity on demand and total management of a completely flexible, scalable estate, regardless of where the data and applications live. Add in automation – the ability to be proactive – and those fixed limitations are able to be resolved in advance of their requirement.

Key to a virtualised LB/ADC solution is that is has to maintain the complete feature set of the hardware equivalent. This is very much true in the case of Kemp’s VLM product, which is still fully featured, including SSL offload functionality, a WAF and HA (High Availability) configurations, but can be deployed on all the major hypervisor platforms and leading public cloud services, such as AWS and Azure. Another important aspect is that the feature set is consistent, regardless of where it is deployed, to avoid deployment issues where some sites would have access to functionality that other sites had no visibility of.

Let us look in more detail, then, about some of the key features you would want to find on a virtual LB/ADC product, in order to maximise application and data availability to your user base.

Layer 4-7 ADC Functionality: Typically, this would include core functions like server and application health monitoring, SSL Encryption acceleration, caching, compression, TCP multiplexing, reverse proxy support, feature automation, integration options through a full set of APIs (typically RESTful – efficiently uses HTTP requests to GET, PUT, POST and DELETE data) and other data acceleration features.

Fully-featured Web Application Firewall (WAF): A WAF enables the secure deployment of web applications, preventing Layer 7 attacks while maintaining core LB services. Typically, it will work in tandem with other secure elements of the virtual device, to create a layered security model for delivering both safe and compliant services.

Global DNS & Traffic Management Services: Looking beyond a single DC, Global DNS supports resilient, multi-DC deployments with high availability so that, even when a primary site is down, traffic will be automatically diverted to a DR (disaster recovery) site, transparent to the user base. Here is one aspect of the LB/ADC world that has improved dramatically with cloud-based deployment, both in terms of performance and reliability, compared with the first phase, hardware-based solutions of the early 2000s.

IAM & Secure Application Access: Identity and access management (IAM) is fundamental in the secure distribution of applications with pre-authentication of clients and single sign-on (SSO), making secure application delivery both totally manageable centrally and as simple as possible from a user perspective. Other key features typically include persistent logging and reporting, Active Directory (AD) integration, RADIUS Authentication support, and support for dual factor authorization, such as working with an RSA SecurID platform or similar.

Single Management View: With potentially worldwide deployments, these environments must be manageable from a single platform and from essentially anywhere. The ability to see the "bigger picture" from top-down, then drill-down into specifics, is crucial to ensuring a truly optimised working architecture. Similarly, optimisation, analysis and security should be fully integrated, not individual components fighting for a limited pot of IT resource, and automation should further optimise the application delivery model.

Uncapped Performance And Scalability: The ultimate virtualized solution should be fully capable of supporting uncapped throughput, including uncapped SSL performance, the whole purely dependent on the allocated system resources in use. That way, further expansion is always available without changing any products or methodology.

Flexible Costing Options: As the IT world increasingly moves away from a fixed CapEx (Capital Expenditure) model to an OpEx (Operating Expenditure) based budget, having a range of licensing options, such as perpetual, subscription-based or metered (based on usage/data throughput or VM/container instances, for example) is another important consideration. The latter option especially, provides the flexibility to deploy and retire load balancing resources on-demand, thereby simplifying key operational areas such as DevOps environments and application scaling.

IN CONCLUSION

The recent COVID-19 pandemic has resulted in mass deployment of remote and homeworking and significant pressure on supporting 24x7 access to critical applications and data.

Importantly, what has come out of necessity might now become the norm across most industries. Key here is the ability of IT infrastructure to support that remote workplace shift and a fundamental layer of that infrastructure is at the DC and the role, therein, of LB/ADC technology. These solutions now need to offer near infinite scalability and flexibility in order to support the new demands on application and data availability - "on demand" resource, both in terms of performance and optimisation, including operating costs.

Using cloud-based architectures to deliver this resource, and support high-level, redundant 24x7 access to those critical applications and data sources, at an affordable cost, is the way forward. Kemp Technology's Virtual LoadMaster (VLM), notably in uncapped, "MAX" format, where performance is designed to be infinitely scalable, on demand, is a great example of what is now needed as a critical foundation of a contemporary IT architecture going forward.

Times change – technology has to change with them…