Monitoring of Private Clouds

White Paper

Authors: Dirk Paessler, CEO at Paessler AG
Dorte Winkler, Technical Editor at Paessler AG

Published: May 2011 – Last Update: August 2011

Contents

Introduction

'Cloud computing' as a concept isn't nearly as new as you might think. Previous approaches have been called 'outsourcing' and 'server hosting,' but insufficient processor performance, enormous hardware costs and slow Internet connections made everyday use difficult. However, today's technology, broadband Internet connections and fast, inexpensive servers, provide the opportunity to access only the services and storage space that are actually necessary, and the ability to adjust these to meet current needs. Using a virtual server, which is provided by a service provider, introduces a wide range of possibilities for cost savings, improved performance and higher data security. The goal of such cloud solutions is a consolidated IT environment that effectively absorbs fluctuation in demand and capitalizes on available resources.

The Private Cloud

The public cloud concept presents a number of challenges for a company's IT department. Data security and the fear of 'handing over' control of the systems are significant issues. If an IT department is used to sequestering its systems with firewalls and to monitoring the availability, performance and capacity usage of its network infrastructure with an extensive monitoring solution, it is much more difficult to implement both measures in the cloud. Of course, all large public cloud providers offer well-thought-out security mechanisms and control systems, but the user must rely on the provider to guarantee constant access and to maintain data security.

Private clouds offer many of the advantages of cloud computing while also minimizing the risks.

The creation of a 'private cloud' as an alternative to the use of public cloud is therefore an interesting possibility. Private clouds enable staff and applications to access IT resources as they are required, while the private computing centre or a private server in a large data centre is running in the background. All services and resources used in a private cloud are found in defined systems that are only accessible to the user and are protected from external access. Private clouds offer many of the advantages of cloud computing and at the same time minimise the risks. As opposed to many public clouds, the quality criteria for performance and availability in a private cloud can be customised, and compliance to these criteria can be monitored to ensure that they are achieved.

Network Monitoring as the Foundation for Private Cloud Planning

In order to guarantee consistent performance across virtual systems, information regarding trends and peak loads can be attained via network monitoring evaluations.

Before moving to a private cloud, an IT department must consider the performance demands of individual applications and cyclic fluctuations. Long-term analysis, trends and peak loads can be attained via extensive network monitoring evaluations, and resource availability can be planned according to demand. This is necessary to guarantee consistent IT performance across virtualized systems.

However, a private cloud will only function smoothly if a fast, highly reliable network connects the physical servers. For this reason, the entire network infrastructure must be analysed in detail before setting up a private cloud. This network must satisfy the requirements relating to transmission speed and stability, otherwise hardware or network connections must be upgraded. Ultimately, even minor losses in transmission speed can lead to extreme drops in performance. The IT administrator can use a comprehensive network monitoring solution like PRTG Network Monitor, in the planning of the private cloud. If an application (which usually equates to multiple virtualized servers) is going to be operated over multiple host servers ("cluster") in the private cloud, the application will need to use Storage Area Networks (SANs), which convey data over the network as a central storage solution. This makes network performance monitoring even more important.

Consistent Network Monitoring Gains Importance in the Cloud

The new cloud complies with the old mainframe concept of centralized IT.

In terminal set ups in the 1980s, if a central computer broke down it was capable of paralyzing an entire company. The same scenario could happen if systems in the cloud fail. Current developments show that we – coming from the concept of the mainframe-computer – have gone through a phase of widely distributed computing and storage power (each workstation had a 'full-blown' PC) and returned to centralized IT concepts. The data is located in the cloud, and end devices are becoming more streamlined (RDP/Citrix terminals, tablets, smart phones, etc.). The new cloud, therefore, complies with the old mainframe concept of centralized IT.

A private cloud – like any other cloud – depends on the efficiency and dependability of the IT infrastructure and presents new challenges to network monitoring.

The failure of a single VM in a highly-virtualized cloud environment can quickly interrupt access to 50 or 100 central applications. Modern clustering concepts are used to try to avoid these failures, but if a system fails despite these efforts, it must be dealt with immediately. If a host server crashes and pulls a large number of virtual machines down with it, or its network connection slows down or is interrupted, all virtualized services on this host are instantly affected, which, even with the best clustering concepts, often cannot be avoided.

A private cloud – like any other cloud – depends on the efficiency and dependability of the IT infrastructure. Physical or virtual server failures, connection interruptions and defective switches or routers can become expensive if they cause staff, automated production processes or online retailers to lose access to important operational IT functions. This means a private cloud also presents new challenges to network monitoring.

A network monitoring solution provides instant notifications when a disruption occurs within the IT landscape, both at the company location and in the private cloud.

To ensure that users have constant access to remote business applications, the performance of the connection to the cloud must be monitored on every level and from every perspective. At the same time, smooth operation of all systems and connections within the private cloud must be guaranteed. And, of course, the administrator must keep an eye on the interaction between the private cloud and their own local IT landscape at the company location. An appropriate network monitoring solution accomplishes all of this with a central system; it notifies the IT administrator immediately in the event of possible disruptions within the private IT landscape both on location and in the private cloud – even if the private cloud is run in an external computing centre.

A private cloud allows the IT administrator to closely monitor the condition of all relevant systems directly with the network monitoring solution of his or her choice.

A feature of private cloud monitoring is that external monitoring services cannot ‘look into’ the cloud, as it – as the name suggests – is private. An operator or client must therefore provide a monitoring solution within the private cloud and, as a result, the IT staff can monitor the private cloud more accurately and directly than a purchased service in the public cloud. A private cloud also enables unrestricted access when necessary. This allows the IT administrator to track the condition of all relevant systems directly with a private network monitoring solution. This encompasses monitoring of every individual virtual machine as well as the VMware host and all physical servers, firewalls, network connections, etc.

Private Cloud Monitoring from Two Perspectives

For comprehensive private cloud monitoring, the network monitoring should have the systems on the radar from user and server perspectives. If a company operates an extensive website with a web shop in a private cloud, for example, network monitoring could be set up as follows:

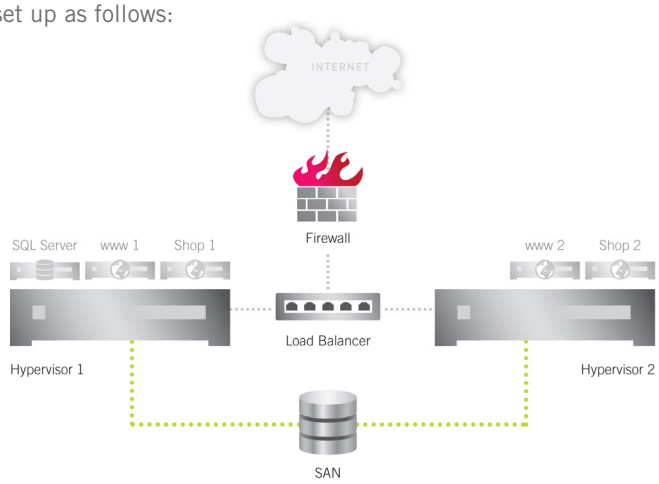


Figure 1:
Schematic diagram of Paessler AG's web hosting in a private cloud

From the User's Perspective

A website operator aims to ensure that all functions are permanently available to all visitors, regardless of how this is realised technically. The following questions are especially relevant in this regard:

- Is the website online?
- Does the web server deliver the correct contents?
- How fast does the site load?
- Does the shopping cart process work?

These questions can only be answered if network monitoring takes place from outside the server in question. Ideally, network monitoring should be run outside the related computing centre, as well. It would therefore be suitable to set up a network monitoring solution on another cloud server or another computing centre. It is crucial that all locations are reliable and a failover cluster supports monitoring so that interruption-free monitoring is guaranteed.

This remote monitoring should include, in the above example of website monitoring:

- Firewall, HTTP load balancer and Web server pinging
- HTTP/HTTPS sensors for
  - Monitoring loading time of the most important pages
  - Monitoring loading time of all assets of a page, including CSS, images, Flash, etc.
  - Checking whether pages contain specific words, e.g.: "Error"
  - Measuring loading time of downloads
- HTTP transaction monitoring, for shopping process simulation
- Sensors that monitor the remaining period of SSL certificate validity

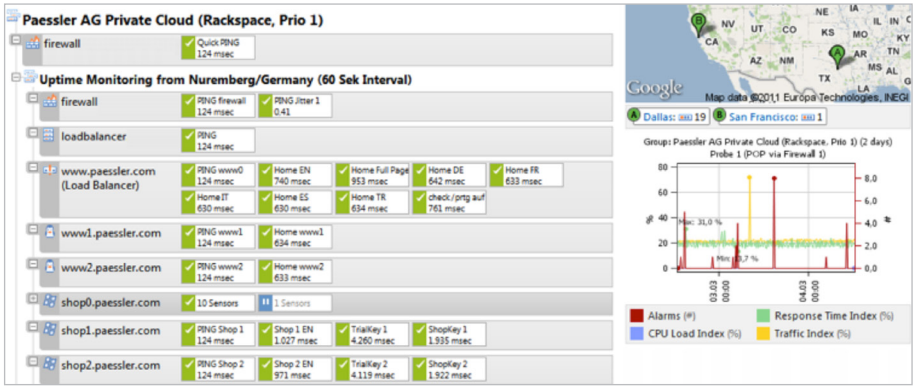


Figure 2:
This screenshot displays several PRTG sensors that are used for monitoring from the user perspective.

If one of these sensors finds a problem, the network monitoring solution will send a notification to the administrator. Rule-based monitoring is helpful here. If a Ping sensor for the firewall, for example, times out, the PRTG Network Monitor offers the possibility to pause all other sensors to avoid a flood of notifications, as, in this case, the connection to the private cloud is clearly completely disconnected.

From the Server's Perspective

Other questions are crucial for monitoring the (virtual) servers that are operating in the private cloud:

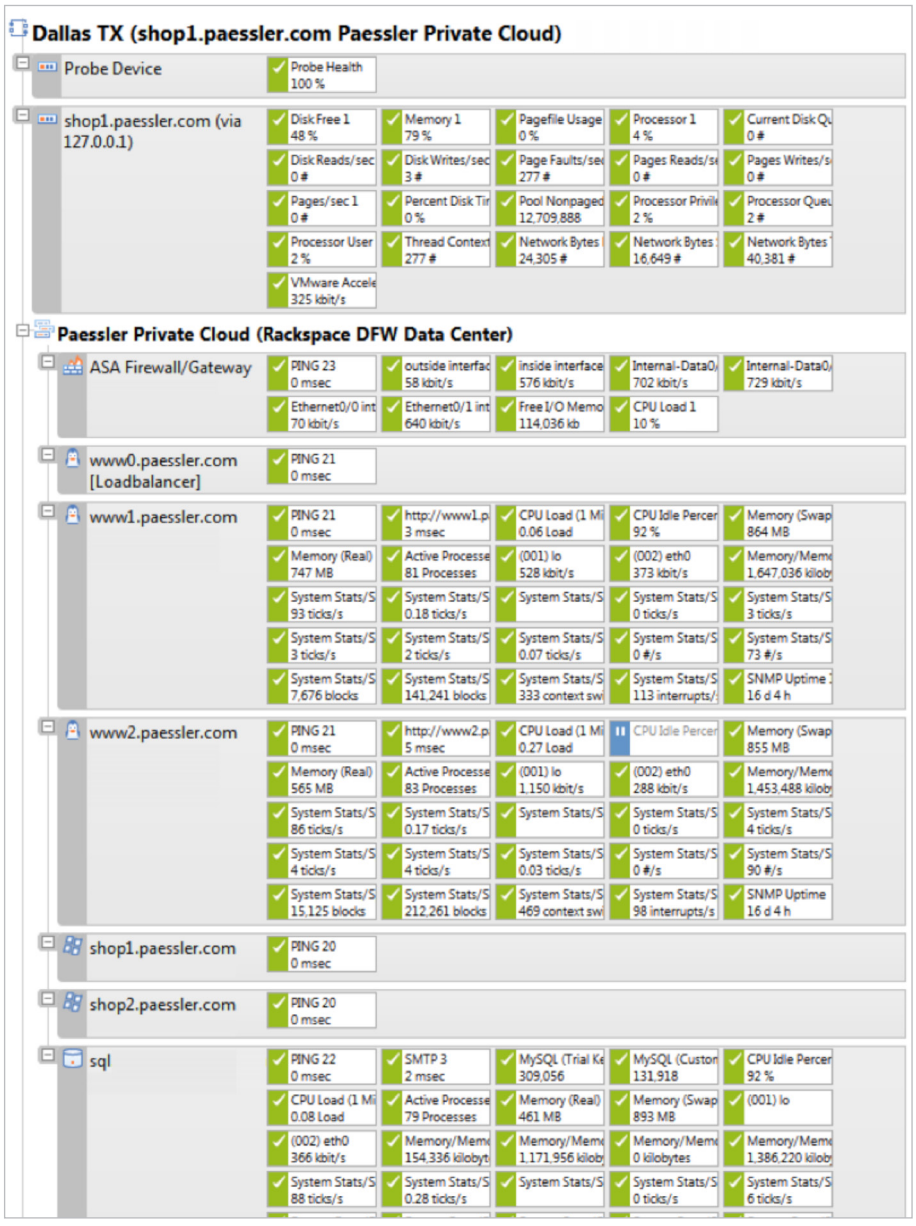
- Does the virtual server run flawlessly?
- Do the internal data replication and load balancer work?
- How high are the CPU usage and memory consumption?
- Is sufficient storage space available?
- Do email and DNS servers function flawlessly?

These questions cannot be answered with external network monitoring. Monitoring software must be running on the server or the monitoring tool must offer the possibility to monitor the server using remote probes. Such probes monitor the following parameters, for example, on each (virtual) server that runs in the private cloud, as well as on the host servers:

- CPU usage
- Memory usage (page files, swap file, page faults, etc.)
- Network traffic
- Hard drive access, free disc space and read/write times during disc access
- Low-level system parameters (e.g.: length of processor queue, context switches)
- Web server's http response time

Critical processes, like SQL servers or Web servers, are often monitored individually, in particular for CPU and memory usage. In addition, the firewall condition (bandwidth use, CPU) can be monitored. If one of these measured variables lies outside of a defined range (e.g. CPU usage over 95% for more than two or five minutes), the monitoring solution will send notifications to the administrator.

Figure 3:
This screenshot displays the majority of the PRTG sensors that monitor the productive system from the server perspective.



Conclusion

With the increasing use of cloud computing, system administrators are facing new challenges. A private cloud – like any other cloud – depends on the efficiency and dependability of the IT infrastructure. This means that the IT department must look into the capacity requirements of each application in the planning stages of the cloud in order to calculate resources to meet the demand. The connection to the cloud must be extensively monitored, as it is imperative that the user has constant access to all applications during operation. At the same time, smooth operation of all systems and connections within the private cloud must be guaranteed. A network monitoring solution should therefore monitor all services and resources from every perspective. This ensures continuous system availability. Capacity overloads can be systematically avoided through long-term planning based on extensive monitoring data.

About Paessler AG

Founded in 1997 and headquartered in Nuremberg, Germany, Paessler AG builds cost effective software that is both powerful and easy to use. The product range is specialized on network monitoring and testing as well as website analysis. Its products are used by network administrators, website operators, Internet service providers, and other IT professionals worldwide. Freeware and Free Trial versions of all products can be downloaded from www.paessler.com.

Paessler AG
Bucher Str. 79a, 90419 Nuremberg, Germany
www.paessler.com, info@paessler.com

VAT-ID: DE 217564187
TAX-ID: FA Nuremberg 241/120/60894
Registration: Amtsgericht Nuremberg HRB 23757

CEO/COO: Dirk Paessler, Christian Twardawa
Chairman: Dr. Marc Roessel