Improve business productivity with application & IT service monitoring solutions

White Paper



Contents

+ Introduction

What does your network look like?

+ Separate Monitoring for Applications and Services Consider what your network monitoring solution does for you

+ Visualising Data How is your information delivered to you?

+ Conclusion

wanstor

2

Introduction

Company productivity in today's digital age is heavily dependent on the applications and services used within the organisation.

For example, many companies use central (web) applications to organise internal workflows, or Microsoft SharePoint to support project management. If a workflow service crashes, entire work processes grind to a halt. In order to use such collaboration platforms and important company applications without interruption, permanent monitoring of the applications is strongly advised. This is the same for the company website. Any problems with the company website will leave customers frustrated or even prevent them from making a purchase.

Additionally email systems, data backup solutions and Windows security updates are some of the most important applications run by your company. If all of these applications are running smoothly, they create a well-organised, solid foundation on which a company can function and staff can be productive.

To avoid cracks in your company's application foundation, professional monitoring software can be used to monitor applications so factors like availability, bandwidth and general usage of the IT infrastructure can be displayed transparently at all times, and give your IT teams the information they need to take preventative action.



Separate Monitoring for Applications and Services

Many monitoring solution providers offer bulk monitoring of application servers and services. Large-scale network monitoring is good, e.g. basic ping and traffic monitoring on routers or switches with customised parameters, but often companies overlook individual aspects, such as the performance of important applications.

Detailed monitoring of individual applications and services is more precise and reliable. Network monitoring solutions like Wanstor and PRTG's Network Monitor use preconfigured sensors to maintain a detailed overview of the status of each application separately.

Reliable Operation of Sharepoint and IIS

These special sensor types provide detailed monitoring of various application and server processes. For example: the web application SharePoint serves companies as a collaboration platform for teams. The tool is used to manage projects, define responsibilities and coordinate work processes. Even SharePoint's content management functions help to accelerate daily work. Additionally, many companies use the IIS Windows server solution to load their websites, services and applications onto the net.



figure 1 : Detailed SharePoint process values

In order to make sure IIS and SharePoint are always running reliably, the sensors which are deployed monitor seamless execution of various processes. The monitoring software provides administrators with information regarding number of page requests and active threads, CPU usage or the number and response time of currently executed SQL queries in SharePoint. With IIS servers, the solution logs sent and received Bytes, speed of GET and POST requests, number of users per second, etc. Any delays or crashes will be reported to administrators immediately so they can respond appropriately in addressing issues.

Monitoring your website

Administrators want the same kind of reaction speed for incidents concerning the company website. The website is the company's shop window on the web, a way of presenting itself to customers at all times. Because of this, the availability of the website is crucial. Businesses can lose customers quickly if pages load too slowly or purchases in the web shop fail due to technical errors.

In order to avoid possible losses due to annoyed customers, a network monitoring solution can report any unusual website behaviour immediately. In addition to the various HTTP sensors that check the website's availability and loading speed, the right network monitoring tool should offer a HTTP Full Web Page Sensor, for example the sensor will check the time of complete page downloads, including images, etc, and will be able to create a visual history of the page.

The HTTP Transaction Sensor simulates transactions in the web shop and monitors their successful completion. An HTTP Apache ModStatus Totals Sensor is available as well as part of many network monitoring tools.

This checks how often a corresponding web server is accessed and the transferred data volumes, helping to identify peak demand times, meaning the administrator can decide whether additional bandwidth is necessary for peak website performance.

Status: D K	Sensors: 1 🔽 1 🔽 (of 11)	DNS/IP: Testdevice	Dependency: Parent	Default Interval: every 5 minutes	La (n	ist Au iever)
⊦ ← 1 to	9 11 of 11 → →					P
os 🔻	Sensor	Status	Message	Graph	Priority	
1.	HTTP Advanced 2	Up	ОК	Loading time 211 mse	< *** **	
2.	HTTP Content 2	Down	Unexpected Format: 'GoogleAnalyticsObject'	Value 1 No dat	*****	
3.	HTTP Full Web Page 2	Up	ok https gerald1/index.htm	Loading Time 827 mse	< *** **	
4.	HTTP 6	Up	ОК	Loading time 101 mse	• *** **	
5.	HTTP Transaction Standard- Post & Get & Keyword	Up	ок	Sum June Material 440 mse	*****	
6.	HTTP Transaction .NET- Post & Get & Keyword check	Up	Ok	Sum 0 mse	« *** **	
7.				Sumhar Vitalian and Apple 239 mar	****	
8.	HIIP Iransaction			Syntrody Hill Jan Jurph & 6 also	****	
9.	CLocal Probe (Local Probe » 🔤 1st group » 📟 HTTP S	erver	^	(Sum) ((, () () () () () () (463 mse	*****	
10.	Last Message:			Sum 0 mse	* ****	
11.	ок			Sum 0 mse	*****	
← 1 to					894L	ø
A	Last Scan: Last Up: Last Down: Uptime: Do	owntime: Covera	ge:			
U 40	4 m 1 s 4 m 1 s 86 d 98,9898% 1,0	0102% 99%				
RECO	Sensor Type: Dependency: Interval:	ID:				
	HTTP Transaction Parent every 5 min	utes #15920				

figure 2 : There are several sensors for monitoring websites and services

Monitoring Email Systems

In (nearly) all companies, a functioning email system is nearly as important as website performance in regards to public image. If email communication with clients and business partners crashes, or even internally between staff and departments, productivity suffers.

This is why it is important for companies to keep an eye on their mail server.

A professional monitoring system can monitor POP3, SMTP and IMAP mail servers with specialised sensors. Companies can then guarantee they are able to send and receive emails and this occurs without delays.



figure 3 : Monitoring an exchange server, including different mail queues

In addition to standard email sensors which monitor mail queues, sending times and latency, it is recommended that companies who are interacting with customers through email deploy two additional sensors so they can monitor the whole 'Email Round Trip'.

These extra sensors record the time it takes for an email to be sent, received and resent to the initial server. To measure, the monitoring solution sends an email via SMTP to an external mail account.

This account must be configured to forward the email directly to another email address on the company's mail server. After sending the test email, the sensors check the corresponding inbox continuously via IMAP or POP3.

As soon as the email is received, the monitoring software writes the 'round trip time' in its database. Companies are then able to define limits for the email round trip time and can put in place SLA's around their email. Exceeding the SLA's put in place will enable companies to identify slower or defective email processes or even failures.

However with these extra sensors, the administrator can start to see where problems may be occurring and start to put a fix in place straight away rather than waiting for all email to come to a standstill.



Overview	Live Data 2 da	rs 30 days	365 day	Historic	Data Log		Settings	(2) Notif	ications	ø				
Last Message:	8													
ок														
Last Scan: 11 m 22 s	Last Up: 11 m 22 s	Last Do 3 d 6 h	wn: 11 m	Uptime: 99,2027	D % 0	owntime: ,7973%	C 9	overage: \$%	Sens SMT	or Type: P&POP3 Rd	ound Trip		Dependency: Parent	Interval: every 30 minutes
														C 8 8
7.000 6.000 5.000 4.000 2.000 1.000	1a:: 7.653 mesc					~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~		~~~		Mini	5.878 msec_		
04.05	04:00 am 04.05 08:00 am	04.05 12:00 pm	04:00 pm	04.05 08:00 pm	12:00 am	04:00 am	08:00 am	12:00 pm	04:00 pm	mq 00:80	12:00 am	04:00 am	08:00 am 06.05 12:00 pm	
Downtim	ie (%) 🔽	Total	(msec)	Respons	s e Tim (mse	<) 🗸 Re	sponse Tim	(msec)					06.05.2015 02:39:441	91 66 C + X = > 3 3
														Show all Hide all

figure 4 : Email round trip monitors the time necessary for email delivery

Backup Monitoring

All types of data that is generated during daily business operations should be secured regularly, not just email accounts. Data backups contribute to reliable business operations. It is recommended you use IMAP sensors to monitor data backups. The sensors can also monitor data storage on virtual machines, in the operating system, on an SQL server, etc.

There are various backup solutions available for securing data. Many of these solutions can send emails that report the status of the nightly data backups. With this method, however, the administrator has to analyse multiple emails daily, in order to make sure that all backups were completed successfully and that no problems have happened. Alternatively, the IT department could set up their network monitoring software to analyse all emails in a certain account automatically using IMAP sensors.

Set to Error	 Never (default) 	
Set to Error	 Always 	
	O If subject contains	
	If subject does not contain	
	If mail body contains	
	 If mail body does not contain 	
Check Method	String search	
	• Regular expression	
Search Text	Successful	
Error Message	Failure email received	
Set to Warning	Never (default)	
Set to Warning	 Always 	
	 If subject contains 	
	 If subject doesn't contain 	
	If mail body contains	
	 If mail body doesn't contain 	
No Matching Mail Behavior	Set sensor to "Down" status	
	 Set sensor to "Warning" status 	
	O None	
Massaga	No. and the second	

In simple terms, if all status emails are sent to one email address, the administrator can use the monitoring solution to keep an overview of all data backups. The administrator then receives a notification immediately if backups are not completed properly.

figure 5 : Filter settings of IMAP sensor monitoring backup

Overview of Server & Services

In addition to options for monitoring applications, various sensor types are available that have been specially designed to take care of Windows services. If errors occur here, usually the only way to solve the problem is to restart the service or the entire server. If, for example, the administrator uses the network monitor to monitor the Windows services, they will receive a text message or email notification if a service crashes, meaning that they can restart the service straight away.

Additionally, if a service or server fails for a certain period of time, the monitoring sensor can execute the script by means of a special type of notification and the restart is executed automatically. This saves administrator time and the IT department operational costs as the process is no longer manual but automated.

Database Performance Checks

Database crashes in the company network are frustrating, annoying and in the worst cases disruptive to users and customers. In order to avoid database outages, and make sure that all data is available for staff at all times, the right monitoring software will continuously monitor the status of your companies databases. If the performance fluctuates, the reasons for fluctuation must be determined. WMI SQL Server sensors show, for example, the number of user connections. If the performance suffers at certain times, it may be that too many users are active at once. In this case, the administrator would be able to increase the available memory on the SQL server and solve the problem.



figure 6 : Performance statistics of Microsoft SQL database

Visualising Data

There are many different methods for visualising the data gathered during monitoring. The data can be viewed directly in the device selection area, for example.

Here, all components monitored and sensors used are clearly displayed, with options available to customise the display.

Libraries in the software offer alternative customised views of the devices used. Filter options can be used to display lists of sensors that monitor dedicated applications or services collectively, independent of the device arrangement.

A Home Devices Libra	ries Sensors	Alarms	Maps Rep	orts Logs	Tickets S	etup						4	? ٺ	Search. P
Libraries Library with sen	ors grouped by st	ate *												
								Net	v Alarms 9 N	ew Log Entries	262 !! 179	: 4 w 11	✓ 339	60 ? 153
Library Library with sensors grouped by state														
Overview Ø Management	≁ Settings	② Notification	s @!											@ 8 ¥ •
Sensors:	<mark>7</mark> 339 🗹 💷 42	✓ 🖸 149 (of 7	24)		5	Search: P Search		• ⊖ ⊝	0				ID: #710	
E Library with sensors grouped b	y state													^
🖽 🔯 Alarms	179 Sensors	4 Sensors	11 Sensors											
🗄 🔯 Paused or unknown	PC Custom	42 Sensors	7 149 Sensors											
🖃 👸 Up and running	Core Health	DiskFree_Local	HTTP4 261 msec (NV)	HTTP Transa 237 msec (W	HTTP Transa 13 msec (N)	450 msec (N	Pingdom 29 msec (N	Probe Health 1.247 MByte IN	SNMP Trap R	Sysiog Receiv	System Health 6 % PM	Windows Las 235 Days (W	HTTP 1 191 msec	-
	CPU Load 4	SQL Server 2	EXE/Script Se	EXE/Script Se	MSEichange	WM Exchang	WMI Exchano	MSExchangel 6 msec (N)	(007) Larry NL. 75.413 kb/c/ PM	Sensor Factory	PING 2 msec IN	PING3 1 msec (N	CPU Load	1
	Free Memory 1 14.807 kb (N	(001) 1 0 kbit/s (W)	(002) 2 0 kbit/s (W)	(005) 5 0 ktb/s (W)	(006) 6 0 kbit/s (W)	SNMP Traffic	(006) 8 0 kb//s (W	(009) 9 815 kbit/s (##	(010) 10 0 ktb/t/s (N)	(015) 15 0 kb/s 🔎	(016) 16 0 kbit/s (198	(017) 17 79 kbit/s (W	(019) 19 0 kb/s	~
	(021) 21 0 kbit/s (W	HTTP 2 15 msec (NV	ICMP Messa 1 ICMP/s (N	ICMP Messa 1 ICMP/s (M	CMP DestUn	OICMP/s (W	O ICMP/s IN	O ICMP Errors	TCP Segmen 1 TCP/s IN	CP Segmen	SNMP Messa 9 SNMP/s (N	SNMP Messa 9 SNMP/s (W	UDP Data 9 UDP/s	29 N
	UDP Datagra	SNMP RMO 0 kb/t/s (N	Ping 1 1 msec (NV	PING Jitter	Traceroute H	Port 1 msec (N)	HTTP 15 msec (N)	HTTP Advanc 9 msec (N)	HTTP Full We 156 msec (N)	HTTP SSL Cer 1.103 Days IN	POP3 Email 945 Emails (N	HTTP Full We_ 219 msec (N	HTTP Trail	58 RJ
	Active Mailbo	Exchange Da 1.3 (N	Eschange Ba 62.44 h (N	Exchange Ma	✓ IMAP 945 # IN	POP3 Roundt 6.034 msec (N	POP3 7 msec (N	6.641 msec (NV	9 msec (N	MAP 1 453 msec IN	POP3 1 19 msec (N	APC UPS: ups 450.000 # 198	ups adv b 450.000 #	itte
	ups high prec 28 V DC IN	ups high prec	SNMP APC B	ups high prec 50 Hz /W	ups high prec 235 V AC IN	ups high prec 50 Hz (N)	ups high prec	ups high prec 235 V AC W	Active Direct 0 Emors (N	DNS 2 0 msec (N)	Active Direct	PING 7 0 msec (N)	SNMP CP	J L
	Disk Free: /v 27 % (N	DiskFree: /v 81 % (N	Disk Free: /v 32 % (N	DiskFree: / K 28 % (M	CPU Load 3 12 % /W	SNMP Disk Fr 27 % IN	Disk Free: /v 81 % /W	Disk Free: /v 32 % (N	Disk Free: /v 28 % /W	Uptime 1 107 d IN	(002) 01:00.1 274 kbit/s IN	(003) 02:00.0 19:804 kb/c/ /W	(004) 02:0 197 kbit/s	0.1
	(006) 06:00.1 5.361 kbit/s (W	(006) 07:00.1 303 kbit/s (W	(009) 10:00.0 190 kb//s IN	(010) 10:00.1 190 kbit/s /W	(013) vSwitch0 17.306 kbit/; (W)	(014) v\$witch0 17.305 kbit/ (N	 (015) vSwitch1 5.307 kbit/s (N) 	HTTPS 31 msec (NV	Sensor ESX(0 81 % (N)	Seroor ESX() 76 % (N)	Prodificata 81% (N)	QA_Linux02 76.% (N	GSA Syste	m N
	HP ProLiant P	SNMP HP Pro	Memory Con	Memory Con	Logical Disic	HTTP Transa	HTTP Transa	HTTP Transa	HTTP Transa	HTTP Transa	Cione of HTT	Cione of HTT	LDAP	

figure 7 : Library showing sensors by current status

Administrators can even select desired objects in the device selection, which are then automatically merged into a library by Wanstor & PRTG.

9

Conclusion

A network monitoring solution provided by Wanstor and PRTG is a central information point for companies who want to have full control over applications and services in the entire network.

The monitoring software continuously monitors the performance of internal applications, inconsistencies in the email system, on the company's website, in data backups, in the database and all applications and services in the IT infrastructure are recognised and reported by the monitoring solution.

In the event that a service is unavailable or a threshold is crossed, the software notifies the responsible party immediately. This enables IT departments to resolve inconsistencies before outages occur, and all applications and services run continuously and reliably.

Wanstor are a trusted independent provider of IT infrastructure services to businesses across the UK. We provide our customers with highly available technology platforms and 24 x 7 IT support. This enables our customers to deliver a great IT experience. Our partnership with Paessler extends over a decade, with high levels of technical competencies and a wealth of real-world expertise, our customers receive real technical and commercial value from our network monitoring solutions and services.

For more information about network monitoring solutions please contact us on **0333 123 0360** or email us at **info@wanstor.com** and one of our network monitoring experts will give you a call back.



info@wanstor.com

