

Zoho and Remke Markets

Joe Walter

Chief Information Officer

Agenda

- Introduction
- Infrastructure Monitoring
 - OpManager
- PCI Compliance
 - EventLog Analyzer, Security Manager Plus, Desktop Central
- More Detailed Monitoring
 - NetFlow Analyzer, Application Manager
- Why Zoho Products?
- Questions?

Introduction

Remke Markets

- Employee-owned, independent grocer in operation since 1897.
- 14 stores across the greater Cincinnati area.
- Doubled store count in 2010 with acquisition of a local competitor.

Infrastructure

- 16 locations with high-speed connectivity between all locations.
- Approximately 1,200 employees
- Primarily Microsoft environment with growing mix of Linux and MySQL.

Infrastructure Monitoring

- Zoho (then AdventNet) first introduced at Remke many years ago for infrastructure monitoring.
- Primary tool for monitoring system available, utilization, SNMP trap management.
- Used to monitor everything – from Windows to Linux to IVRs to VMware to switches/routers/APs to desktops to 'generic' SNMP-capable devices.
- Alerts on specific Windows service outages and, if possible, restarts the service.



Infrastructure Monitoring

Proactive Monitoring

- Send alerts when critical devices experience outages – in many instances, correcting issues before users notice the outage.
- Monitor for pending hardware failures

Capacity Planning

- Long-term monitoring of CPU, disk, and memory usage.
- Used to plan for upgrades and capacity expansion.

PCI Compliance

Zoho provided some of the key components to help achieve PCI compliance.

- EventLog Analyzer
- Desktop Central
- Security Manager Plus

PCI Compliance

Desktop Central

- Originally used for automated desktop patch management in compliance with PCI DSS requirement 5.
- Since expanded for other purposes:
 - General desktop updates (i.e., new software deployment, configuration changes, local admin password)
 - Hardware inventory – upgrade planning
 - Software inventory
 - License management and compliance



PCI Compliance

Security Manager Plus

- Server patch management and weekly vulnerability scanning
- Covering both Windows and Linux servers
- Part of PCI DSS requirement 11

Severity	Reference ID	Package Name	Download Status	Status	History
Critical	MS10-081	WindowsServer2003-40873710-485-080.exe	Failed	Rejected	
Critical	MS10-079	WindowsServer2003-40871910-485-080.exe	Failed	Rejected	
Critical	MS10-077	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-076	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-075	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-074	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-073	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-072	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-071	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-070	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-069	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-068	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-067	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-066	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-065	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-064	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-063	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-062	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-061	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-060	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-059	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-058	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-057	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-056	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-055	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-054	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-053	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-052	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-051	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-050	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-049	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-048	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-047	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-046	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-045	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-044	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-043	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-042	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-041	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-040	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-039	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-038	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-037	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-036	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-035	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-034	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-033	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-032	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-031	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-030	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-029	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-028	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-027	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-026	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-025	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-024	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-023	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-022	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-021	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-020	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-019	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-018	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-017	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-016	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-015	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-014	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-013	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-012	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-011	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-010	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-009	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-008	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-007	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-006	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-005	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-004	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-003	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-002	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	
Critical	MS10-001	WindowsServer2003-40871800-485-080.exe	Failed	Rejected	

Host Information

IP Address	: 192.168.20.231
Last Scanned Time	: 2011-03-03 06:17:51
Operating System	: Windows Server 2003, Standard x64 Edition SP2
Vulnerabilities	: 10 (21%), 9 (19%), 24 (50%)
Open Ports	: 7
Missing Patches	: 0 (0%), 1 (2%), 0 (0%), 0 (0%), 6 (12%)
Missing SPs	: 0
Installed Patches	: 36 (76%), 45 (95%), 9 (19%), 1 (2%), 27 (56%)
Antivirus	: -
Scan Initiated By	: root
Vulnerability Group	: Complete Scan
Reboot Initiation Time (Status)	: Not yet initiated by Security Manager Plus

Vulnerability Risk Percentage

High	: 9 (14%)
Medium	: 21 (33%)
Low	: 1 (2%)
Information	: 24 (44%)

Open Ports Found: 7

Port	Protocol	Service Running	Service Info
25	TCP	smtp	Microsoft ESMTIP

Further Monitoring

NetFlow Analyzer

- To monitor usage of Internet bandwidth.
- Helped pinpoint some users that were “taking advantage” of the bandwidth.

The screenshot displays the NetFlow Analyzer interface for an Autonomous System. It shows a list of routers and their interfaces, with columns for IN Traffic and OUT Traffic. The data is as follows:

Router Name	Interface Name	IN Traffic	OUT Traffic
corp-rtr1.remkes.com IP: 192.168.4.2 Flows Received: 270960430	<< Corp >>	1% 6.56 Mbps	1% 6.14 Mbps
	<< Lab 10 >>	0% 2.12 Mbps	0% 196.23 Kbps
	<< WAN >>	1% 726.54 Kbps	3% 3.05 Mbps
corp-rtr180.remkes.com IP: 192.168.4.3 Flows Received: 32682269	<< Corp >>	3% 4.63 Mbps	3% 3.32 Mbps
	<< WAN >>	12% 3.32 Mbps	47% 4.65 Mbps
	<< ORlan >>	2% 2.12 Mbps	2% 2.11 Mbps
dr-rtr.remkes.com IP: 192.168.1.2 Flows Received: 35424994	<< WAN >>	0% 17.16 Kbps	0% 27.94 Kbps
	<< ORlan >>	3% 3.31 Mbps	5% 4.65 Mbps
	<< WAN >>	17% 4.61 Mbps	13% 3.31 Mbps
vpn-dr.remkes.com IP: 192.168.1.254 NetFlow Packets Recv: 235898	Inside	0% 0.00	0% 0.00
	dmz	0% 13.89 Kbps	2% 612.97 Kbps
	inside	0% 612.98 Kbps	0% 7.65 Kbps
	outside	0% 16.43 Kbps	0% 14.01 Kbps
vpn.remkes.com IP: 192.168.4.254 NetFlow Packets Recv: 2033884	SVORZ	0% 1.28 Kbps	0% 6.17 Kbps
	dmz	0% 29.52 Kbps	2% 863.56 Kbps
	inside	3% 2.34 Mbps	0% 140.19 Kbps
	outside	0% 146.57 Kbps	2% 1.5 Mbps

The screenshot displays the 'Top Source' traffic report, showing the top 10 source IP addresses and their respective traffic volume and percentage.

Source	Traffic	Traffic Percentage
192.168.4.16	9.21 GB	34%
192.168.4.30	1.45 GB	5%
10.224.29.29	989.09 MB	4%
192.168.4.127	708.6 MB	3%
192.168.4.143	551.91 MB	2%
192.168.103.218	388.23 MB	1%
192.168.109.122	378.77 MB	1%
192.168.4.196	343.41 MB	1%
192.168.4.179	314.03 MB	1%
192.168.4.125	299.35 MB	1%
Others	12.66 GB	46%

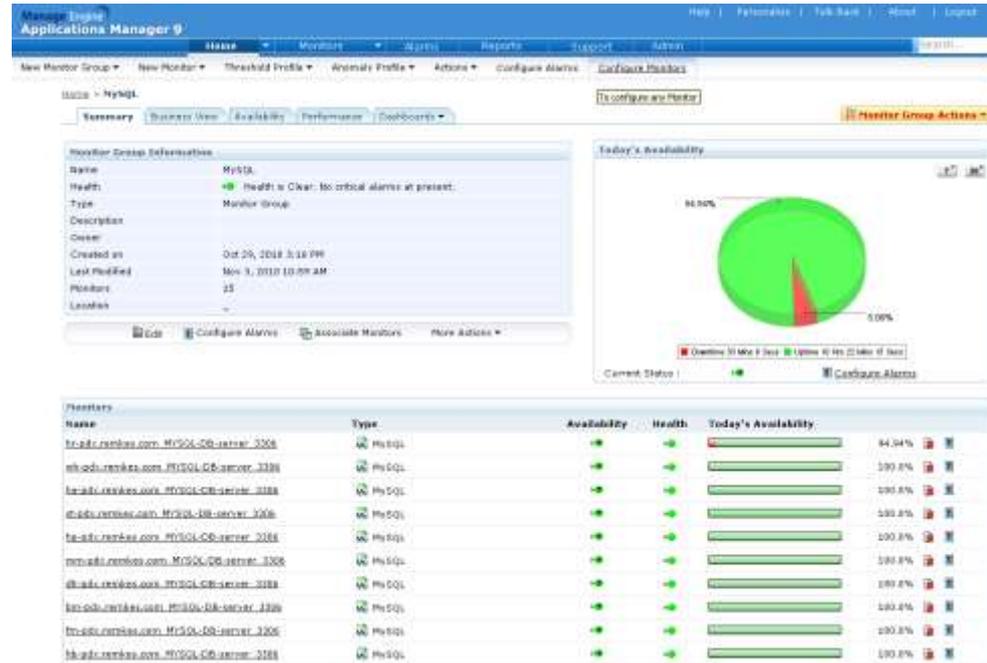
The screenshot displays the 'Top Destination' traffic report, showing the top 10 destination IP addresses and their respective traffic volume and percentage.

Destination	Traffic	Traffic Percentage
192.168.20.231	7.33 GB	27%
192.168.20.20	1.78 GB	7%
69.16.175.42	642.07 MB	2%
38.116.147.117	531.94 MB	2%
216.68.10.169	525.97 MB	2%
184.85.41.188	514.84 MB	2%
216.68.10.147	432.31 MB	2%
216.68.10.155	416.54 MB	2%
216.68.10.146	357.27 MB	1%
216.68.10.178	314.07 MB	1%
Others	14.44 GB	53%

Further Monitoring

Application Manager

- Brought in to monitor MySQL environment – specifically replication and query performance.
- Sends out alerts when replication ‘breaks’ with any of the slave servers.



Replication Details					
Attribute	Value	Threshold	Attribute	Value	Threshold
Replication Status	Up	🟢	Master Host	lba.remkes.com	-
Slave IO Running	Yes	-	Master User	hh_replication	-
Slave SQL Running	Yes	-	Master Port	3306	-
Last Error	No Errors	-	Time Behind Master	0	🟢

[Configure Alarms](#)
[Configure Alarms](#)

Why Zoho Products?

- Free trials
 - Allowed us to confirm the product would do what we needed it to do.
 - Able to explore the overall functionality of the product.
- Comprehensive suite of products
 - Single vendor to deal with
- Aggressive pricing

Questions

