SAND2011-3586C

6/15/2011

SCOM System Center Operation Manger capturing application crash events

Kevin Hall

Cyber Security Technology Department

Sandia National Laboratories

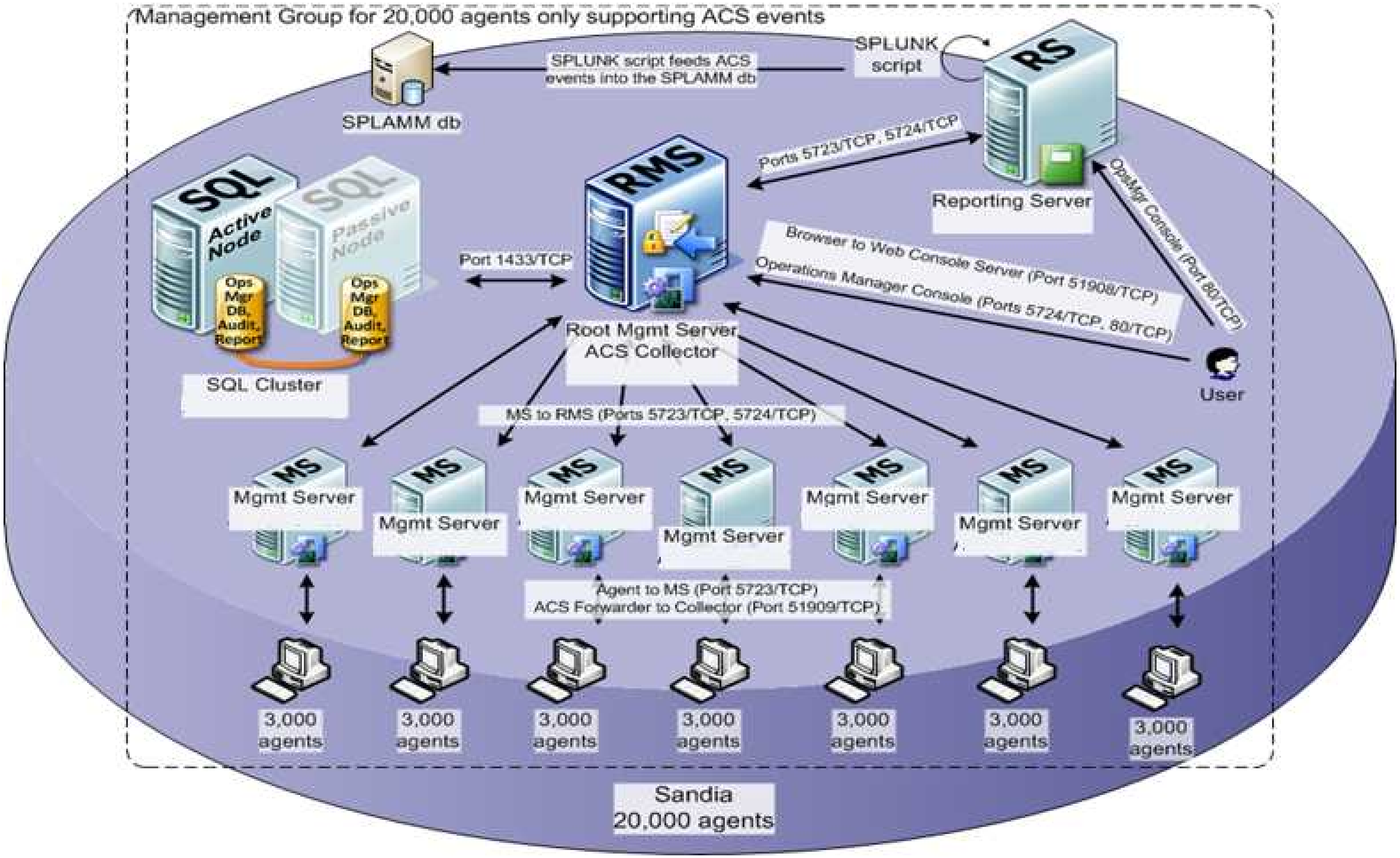
Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2011-0439P
.

Topics we will be covering

- Architecture Overview
- Operating System Security Log Events (ACS)
- Agent less Monitoring (AEM)
- Spunk Integration
- Data Trends

Architecture

Since a correctly-sized ACS Collector/Database pair can support up to 20,000 workstations, the goal will be to implement a single Management Group supporting up to 20,000 workstations.


Management Group for 20,000 agents only supporting ACS events
SPLAMM db
SPLUNK script feeds ACS events into the SPLAMM db
SPLUNK script
RS
Reporting Server
Ports 5723/TCP, 5724/TCP
RMS
SQL Active Node
SQL Passive Node
Ops Mgr DB, Audit, Report
Ops Mgr DB, Audit, Report
SQL Cluster
Port 1433/TCP
Root Mgmt Server ACS Collector
Browser to Web Console Server (Port 51908/TCP)
Operations Manager Console (Ports 5724/TCP, 80/TCP)
OpsMgr Console (Port 80/TCP)
User
MS to RMS (Ports 5723/TCP, 5724/TCP)
MS
Mgmt Server
MS
Mgmt Server
MS
Mgmt Server
MS
Mgmt Server
MS
Mgmt Server
MS
Mgmt Server
MS
Mgmt Server
Agent to MS (Port 5723/TCP)
ACS Forwarder to Collector (Port 51909/TCP)
3,000 agents
3,000 agents
3,000 agents
3,000 agents
3,000 agents
3,000 agents
3,000 agents
Sandia 20,000 agents

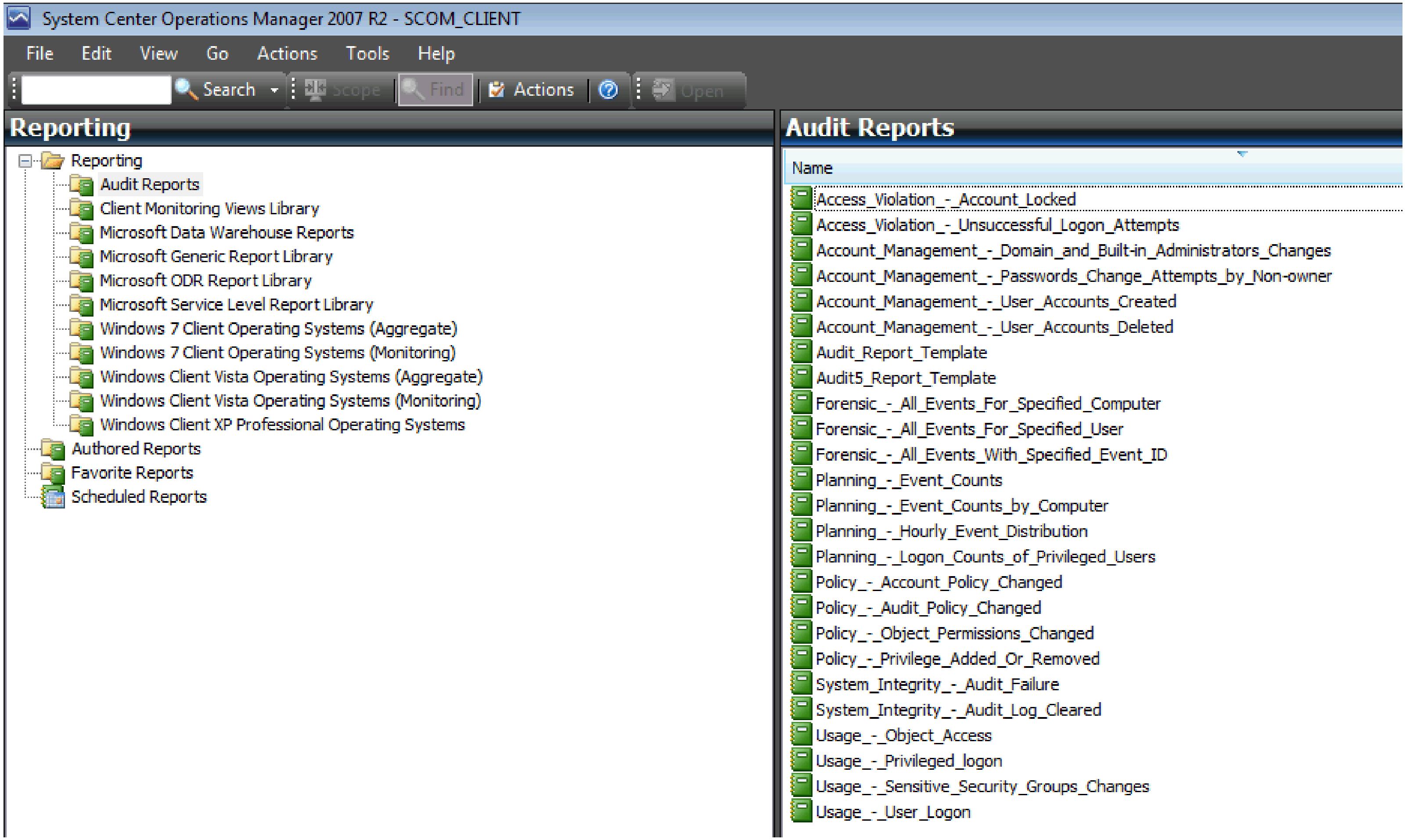
Architecture

- Microsoft OpsMgr 2007 Server is highly scalable. It will expand easily to meet the needs of the organization, as the environment grows. There are two dimensions to scalability: horizontal scalability, in which more servers are added doing the same tasks, and vertical scalability, in which a single server can be configured for better performance.
- The agent manager is responsible for discovering computers, deploying agents, updating agents with new or changed processing rules, managing the configuration of individual agents and uninstalling agents.
- There are a number of methods available for installing the agent.
- We leveraged SCCM to deploy silently to each group of machines.
- Permissions for the agent are running as SYSTEM
- 23MB installed average memory footprint 3k to 11k

Architecture

- Management Packs consist of pre-configured Operations Manager rule-sets and Knowledge Base articles, each pack providing rules for a specific range of applications or services. These Management Packs have been developed and refined by experts both to provide a complete off-the-shelf solution, as well as a strong foundation for more advanced administrators to customize and extend. Included as a standard part of OpsMgr is a Management Pack that enables management of all critical Windows services.
- Windows Client OS, Library, and Monitoring
- We have an audit or monitor only permissions model

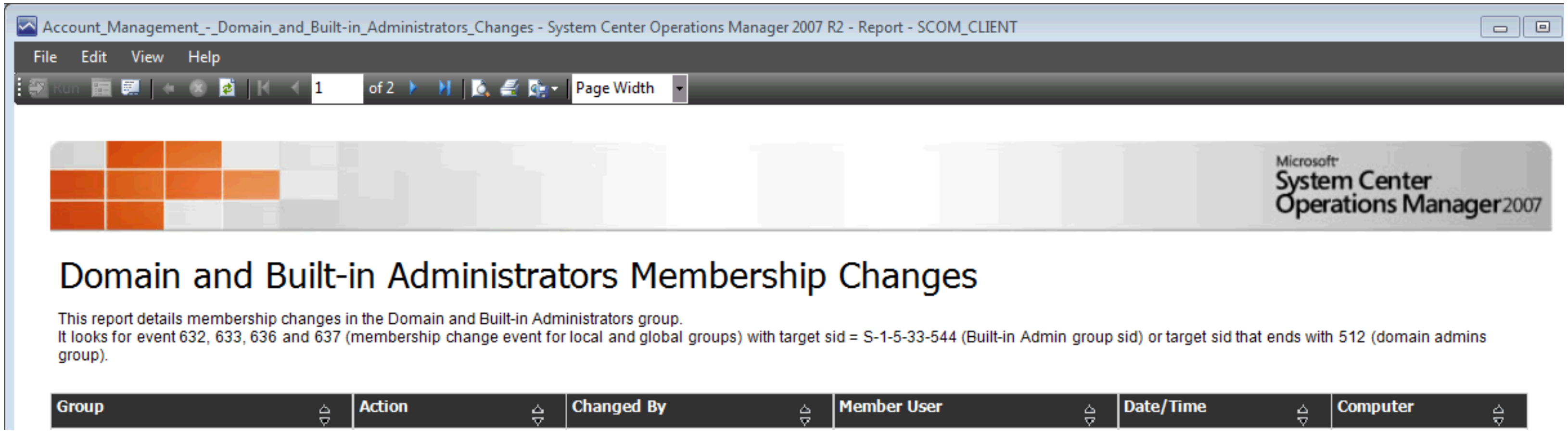
ACS



- Reporting
  - Audit Reports
  - Client Monitoring Views Library
  - Microsoft Data Warehouse Reports
  - Microsoft Generic Report Library
  - Microsoft ODR Report Library
  - Microsoft Service Level Report Library
  - Windows 7 Client Operating Systems (Aggregate)
  - Windows 7 Client Operating Systems (Monitoring)
  - Windows Client Vista Operating Systems (Aggregate)
  - Windows Client Vista Operating Systems (Monitoring)
  - Windows Client XP Professional Operating Systems
- Authored Reports
- Favorite Reports
- Scheduled Reports

Access_Violation_-_Account_Locked
Access_Violation_-_Unsuccessful_Logon_Attempts
Account_Management_-_Domain_and_Built-in_Administrators_Changes
Account_Management_-_Passwords_Change_Attempts_by_Non-owner
Account_Management_-_User_Accounts_Created
Account_Management_-_User_Accounts_Deleted
Audit_Report_Template
Audit5_Report_Template
Forensic_-_All_Events_For_Specified_Computer
Forensic_-_All_Events_For_Specified_User
Forensic_-_All_Events_With_Specified_Event_ID
Planning_-_Event_Counts
Planning_-_Event_Counts_by_Computer
Planning_-_Hourly_Event_Distribution
Planning_-_Logon_Counts_of_Privileged_Users
Policy_-_Account_Policy_Changed
Policy_-_Audit_Policy_Changed
Policy_-_Object_Permissions_Changed
Policy_-_Privilege_Added_Or_Removed
System_Integrity_-_Audit_Failure
System_Integrity_-_Audit_Log_Cleared
Usage_-_Object_Access
Usage_-_Privileged_logon
Usage_-_Sensitive_Security_Groups_Changes
Usage_-_User_Logon

ACS



Account_Management_-_Domain_and_Built-in_Administrators_Changes - System Center Operations Manager 2007 R2 - Report - SCOM_CLIENT
File
Edit
View
Help
Run
1
of 2
Page Width
Microsoft
System Center
Operations Manager 2007

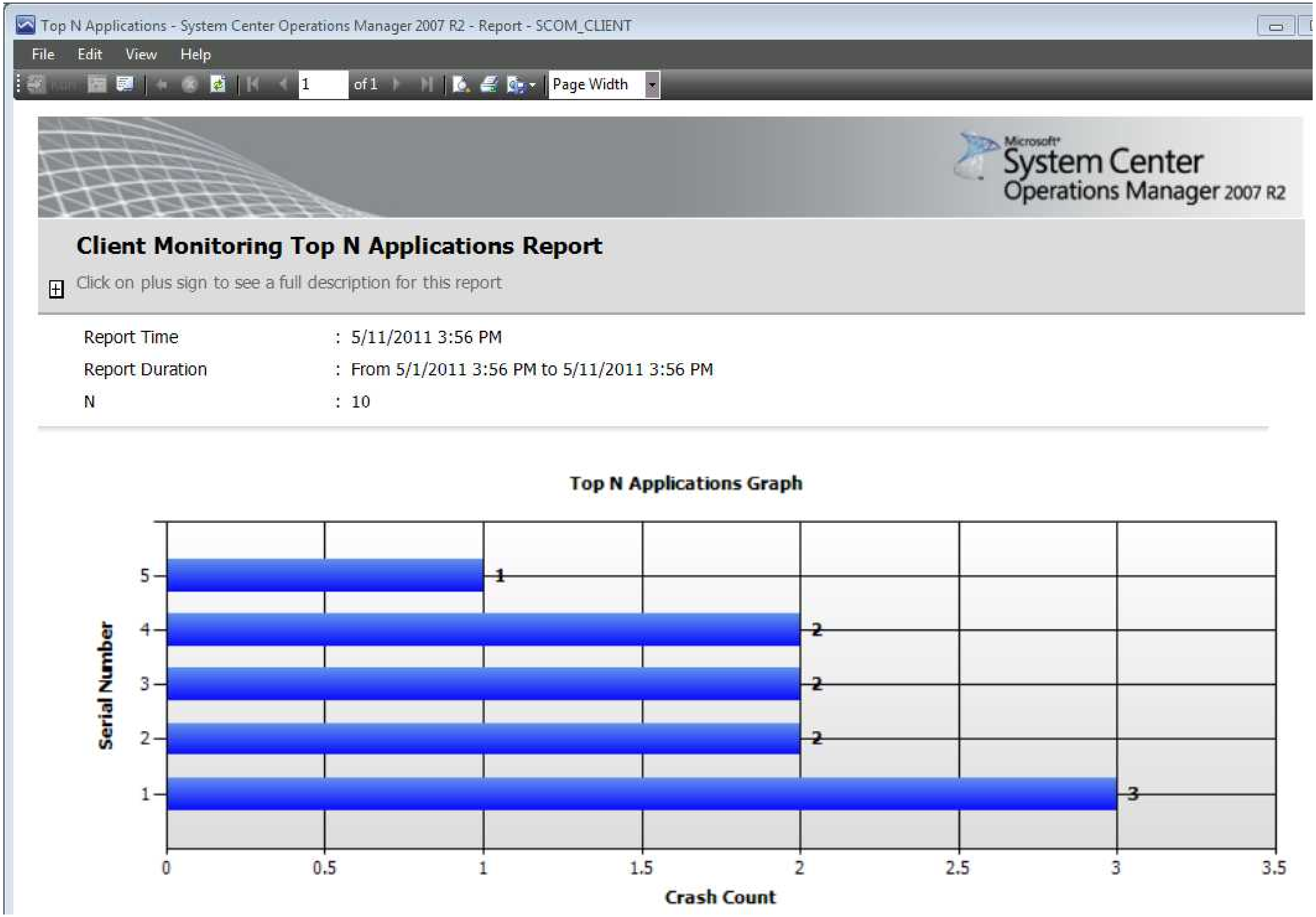
Domain and Built-in Administrators Membership Changes

This report details membership changes in the Domain and Built-in Administrators group.
It looks for event 632, 633, 636 and 637 (membership change event for local and global groups) with target sid = S-1-5-33-544 (Built-in Admin group sid) or target sid that ends with 512 (domain admins group).

Group	Action	Changed By	Member User	Date/Time	Computer

- **There are multiple reports that can be generated for administrators for log review**
- **This is a sample of administrative changes on clients.**

AEM


Top N Applications - System Center Operations Manager 2007 R2 - Report - SCOM_CLIENT
File
Edit
View
Help
1
of 1
Page Width
Microsoft
System Center
Operations Manager 2007 R2

Client Monitoring Top N Applications Report

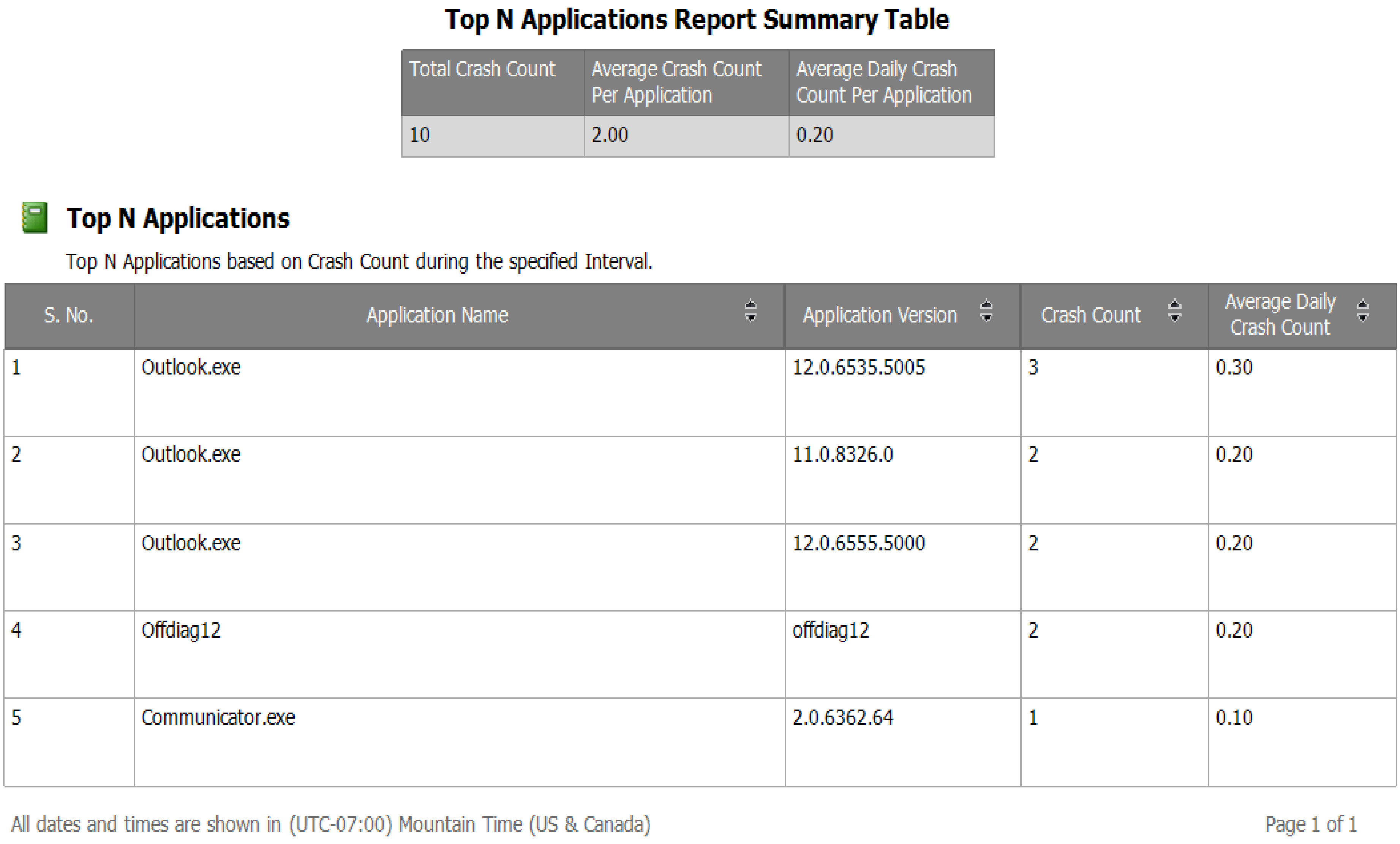
⊞ Click on plus sign to see a full description for this report

Report Time	:	5/11/2011 3:56 PM
Report Duration	:	From 5/1/2011 3:56 PM to 5/11/2011 3:56 PM
N	:	10

Top N Applications Graph

Serial Number
5
4
3
2
1
1
2
2
2
3
0
0.5
1
1.5
2
2.5
3
3.5
Crash Count

AEM



Top N Applications Report Summary Table

Total Crash Count	Average Crash Count Per Application	Average Daily Crash Count Per Application
10	2.00	0.20

Top N Applications

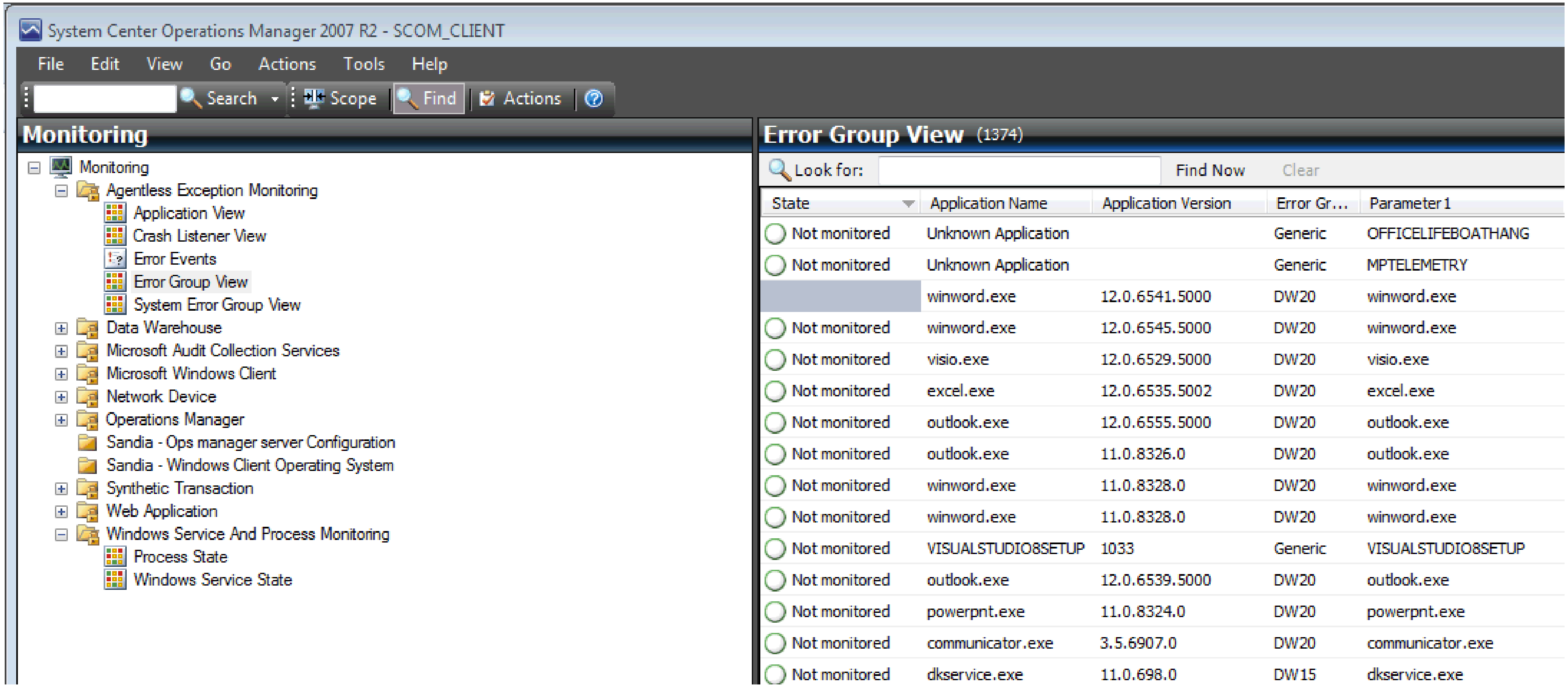
Top N Applications based on Crash Count during the specified Interval.

S. No.	Application Name	Application Version	Crash Count	Average Daily Crash Count
1	Outlook.exe	12.0.6535.5005	3	0.30
2	Outlook.exe	11.0.8326.0	2	0.20
3	Outlook.exe	12.0.6555.5000	2	0.20
4	Offdiag12	offdiag12	2	0.20
5	Communicator.exe	2.0.6362.64	1	0.10

All dates and times are shown in (UTC-07:00) Mountain Time (US & Canada)

Page 1 of 1

AEM



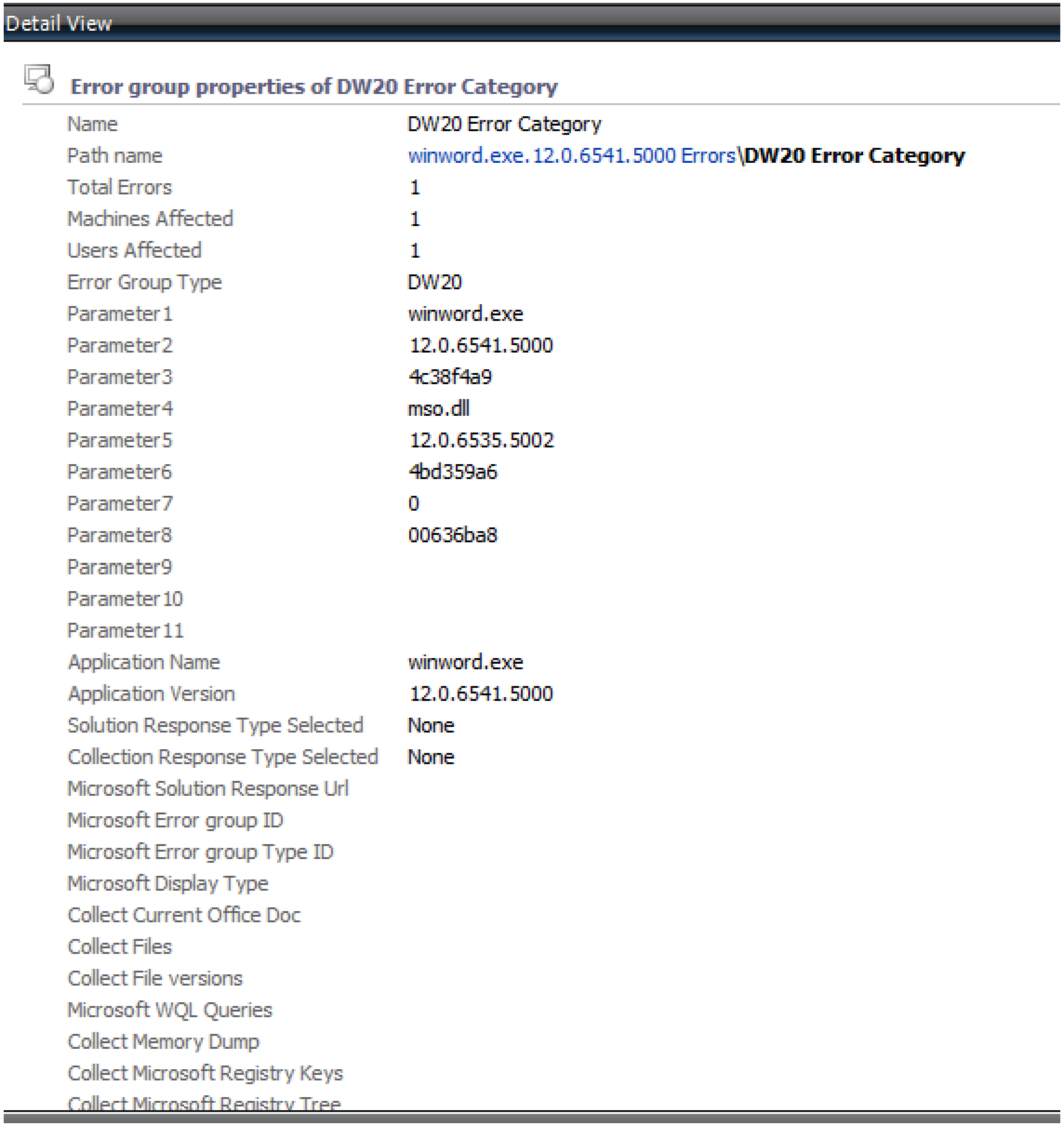
Monitoring

- Monitoring
  - Agentless Exception Monitoring
    - Application View
    - Crash Listener View
    - Error Events
    - Error Group View
    - System Error Group View
  - Data Warehouse
  - Microsoft Audit Collection Services
  - Microsoft Windows Client
  - Network Device
  - Operations Manager
  - Sandia - Ops manager server Configuration
  - Sandia - Windows Client Operating System
  - Synthetic Transaction
  - Web Application
  - Windows Service And Process Monitoring
    - Process State
    - Windows Service State

Error Group View (1374)

State	Application Name	Application Version	Error Gr...	Parameter 1
○ Not monitored	Unknown Application		Generic	OFFICELIFEBOATHANG
○ Not monitored	Unknown Application		Generic	MPTELEMETRY
	winword.exe	12.0.6541.5000	DW20	winword.exe
○ Not monitored	winword.exe	12.0.6545.5000	DW20	winword.exe
○ Not monitored	visio.exe	12.0.6529.5000	DW20	visio.exe
○ Not monitored	excel.exe	12.0.6535.5002	DW20	excel.exe
○ Not monitored	outlook.exe	12.0.6555.5000	DW20	outlook.exe
○ Not monitored	outlook.exe	11.0.8326.0	DW20	outlook.exe
○ Not monitored	winword.exe	11.0.8328.0	DW20	winword.exe
○ Not monitored	winword.exe	11.0.8328.0	DW20	winword.exe
○ Not monitored	VISUALSTUDIO8SETUP	1033	Generic	VISUALSTUDIO8SETUP
○ Not monitored	outlook.exe	12.0.6539.5000	DW20	outlook.exe
○ Not monitored	powerpnt.exe	11.0.8324.0	DW20	powerpnt.exe
○ Not monitored	communicator.exe	3.5.6907.0	DW20	communicator.exe
○ Not monitored	dkservice.exe	11.0.698.0	DW15	dkservice.exe

AEM



Detail View

Error group properties of DW20 Error Category

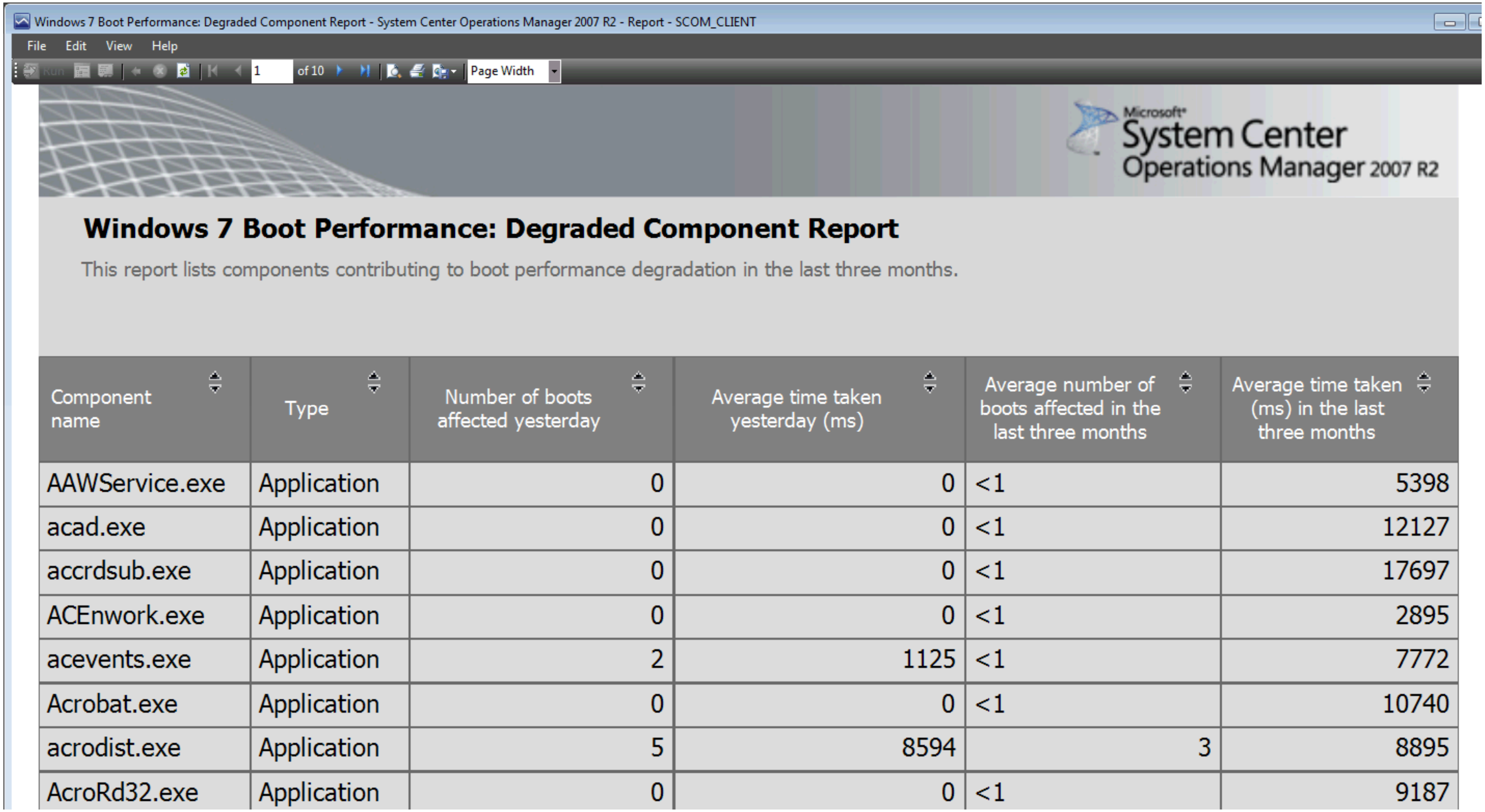
Name	DW20 Error Category
Path name	winword.exe.12.0.6541.5000 Errors**DW20 Error Category**
Total Errors	1
Machines Affected	1
Users Affected	1
Error Group Type	DW20
Parameter1	winword.exe
Parameter2	12.0.6541.5000
Parameter3	4c38f4a9
Parameter4	mso.dll
Parameter5	12.0.6535.5002
Parameter6	4bd359a6
Parameter7	0
Parameter8	00636ba8
Parameter9	
Parameter10	
Parameter11	
Application Name	winword.exe
Application Version	12.0.6541.5000
Solution Response Type Selected	None
Collection Response Type Selected	None
Microsoft Solution Response Url	
Microsoft Error group ID	
Microsoft Error group Type ID	
Microsoft Display Type	
Collect Current Office Doc	
Collect Files	
Collect File versions	
Microsoft WQL Queries	
Collect Memory Dump	
Collect Microsoft Registry Keys	
Collect Microsoft Registry Tree	

I chose a Word crash to show the details from agent less monitoring

Spunk Integration

- What is Splunk?
- Splunk is the engine for machine data. Use Splunk to collect, index and harness the fast moving machine data generated by all your applications, servers and devices — physical, virtual and in the cloud. Search and analyze all your real-time and historical data from one place.
- http://www.splunk.com/
- Currently we have a powershell script running on the RMS for Splunk log collection.
- We have a new API that will create a custom template for Cyber ops.
- The binary will stream all the data from the custom template on the RMS to Splunk.

Data Trends

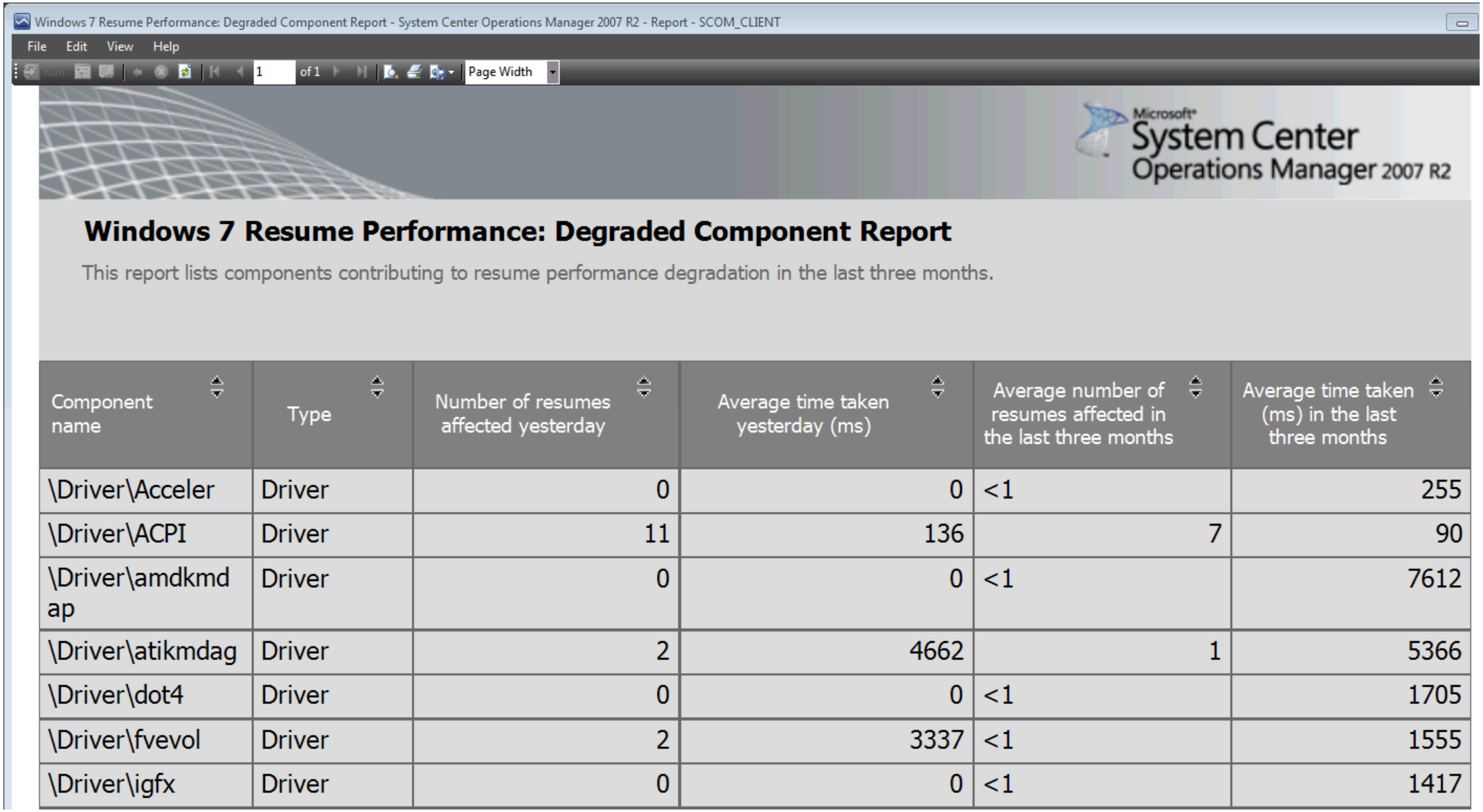

Windows 7 Boot Performance: Degraded Component Report - System Center Operations Manager 2007 R2 - Report - SCOM_CLIENT
File
Edit
View
Help
Run
1
of 10
Page Width
Microsoft
System Center
Operations Manager 2007 R2

Windows 7 Boot Performance: Degraded Component Report

This report lists components contributing to boot performance degradation in the last three months.

Component name	Type	Number of boots affected yesterday	Average time taken yesterday (ms)	Average number of boots affected in the last three months	Average time taken (ms) in the last three months
AAWService.exe	Application	0	0	<1	5398
acad.exe	Application	0	0	<1	12127
accrdsub.exe	Application	0	0	<1	17697
ACEnwork.exe	Application	0	0	<1	2895
acevents.exe	Application	2	1125	<1	7772
Acrobat.exe	Application	0	0	<1	10740
acrodist.exe	Application	5	8594	3	8895
AcroRd32.exe	Application	0	0	<1	9187

Data Trends

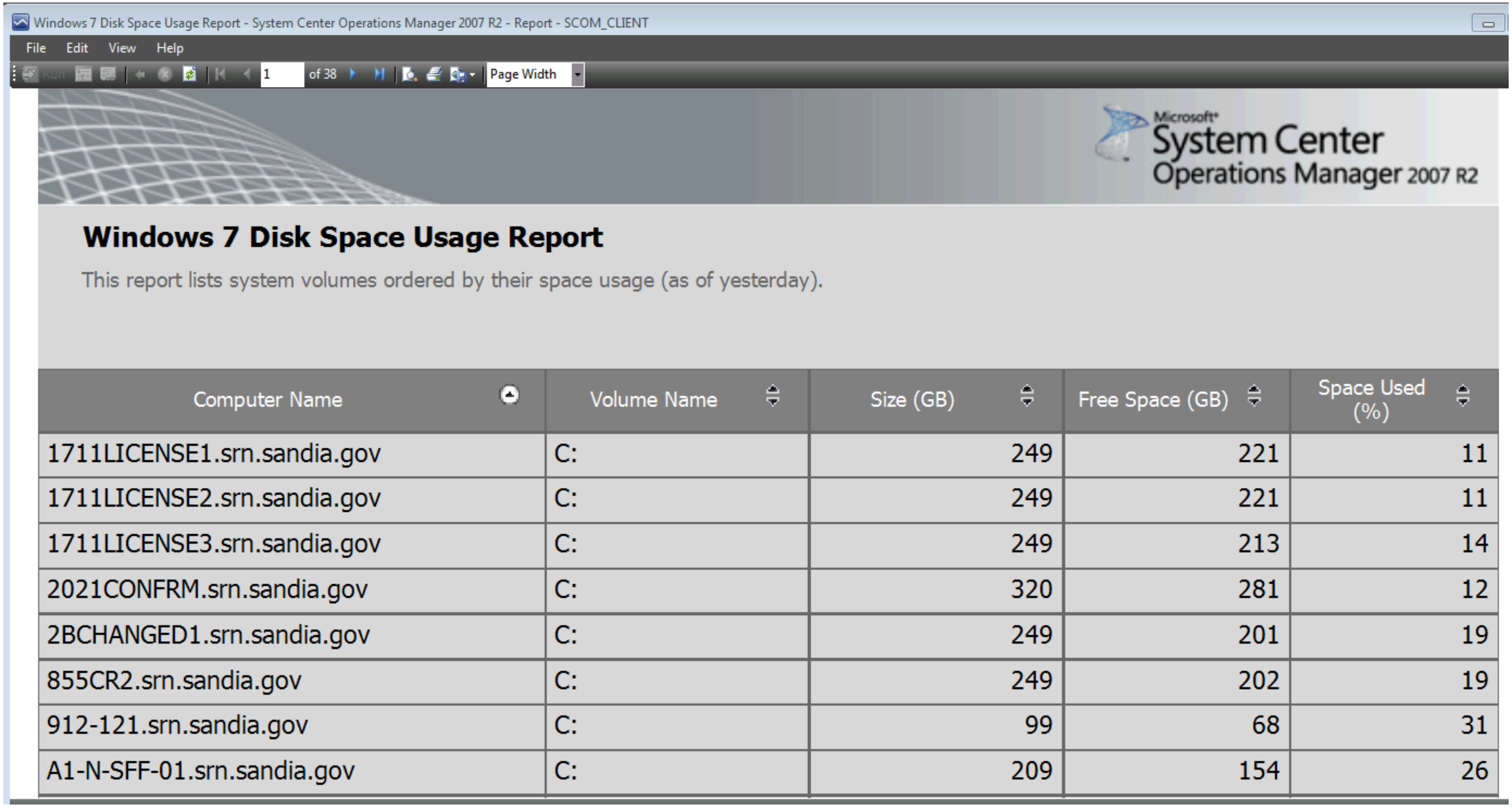

Windows 7 Resume Performance: Degraded Component Report - System Center Operations Manager 2007 R2 - Report - SCOM_CLIENT
File
Edit
View
Help
Run
1
of 1
Page Width
Microsoft
System Center
Operations Manager 2007 R2

Windows 7 Resume Performance: Degraded Component Report

This report lists components contributing to resume performance degradation in the last three months.

Component name	Type	Number of resumes affected yesterday	Average time taken yesterday (ms)	Average number of resumes affected in the last three months	Average time taken (ms) in the last three months
\Driver\Acceler	Driver	0	0	<1	255
\Driver\ACPI	Driver	11	136	7	90
\Driver\amdkmdap	Driver	0	0	<1	7612
\Driver\atikmdag	Driver	2	4662	1	5366
\Driver\dot4	Driver	0	0	<1	1705
\Driver\fvevol	Driver	2	3337	<1	1555
\Driver\igfx	Driver	0	0	<1	1417

Data Trends

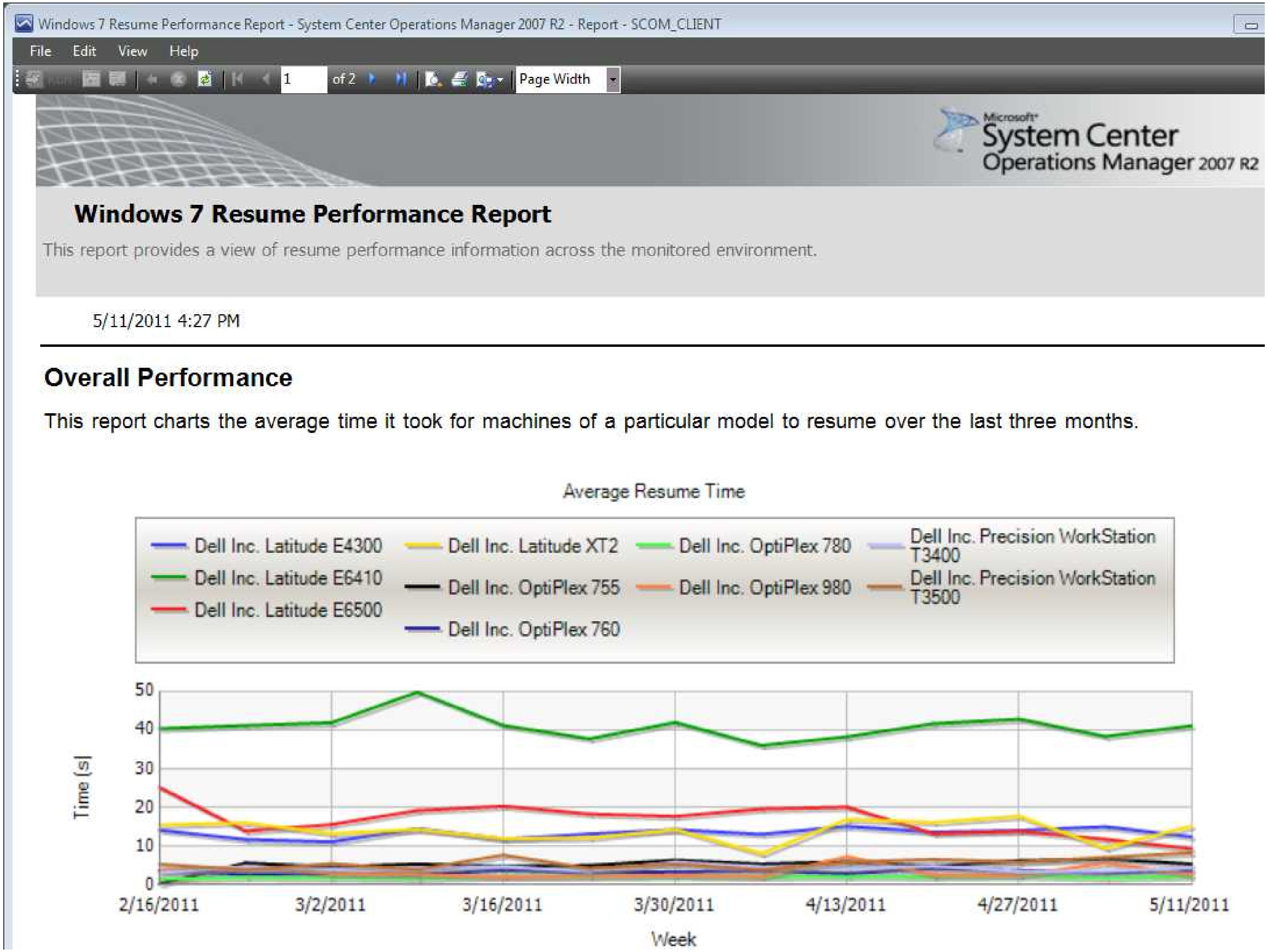

Windows 7 Disk Space Usage Report - System Center Operations Manager 2007 R2 - Report - SCOM_CLIENT
File Edit View Help
1 of 38
Page Width
Microsoft System Center Operations Manager 2007 R2

Windows 7 Disk Space Usage Report

This report lists system volumes ordered by their space usage (as of yesterday).

Computer Name	Volume Name	Size (GB)	Free Space (GB)	Space Used (%)
1711LICENSE1.srn.sandia.gov	C:	249	221	11
1711LICENSE2.srn.sandia.gov	C:	249	221	11
1711LICENSE3.srn.sandia.gov	C:	249	213	14
2021CONFRM.srn.sandia.gov	C:	320	281	12
2BCHANGED1.srn.sandia.gov	C:	249	201	19
855CR2.srn.sandia.gov	C:	249	202	19
912-121.srn.sandia.gov	C:	99	68	31
A1-N-SFF-01.srn.sandia.gov	C:	209	154	26

Data Trends



Windows 7 Resume Performance Report

This report provides a view of resume performance information across the monitored environment.

5/11/2011 4:27 PM

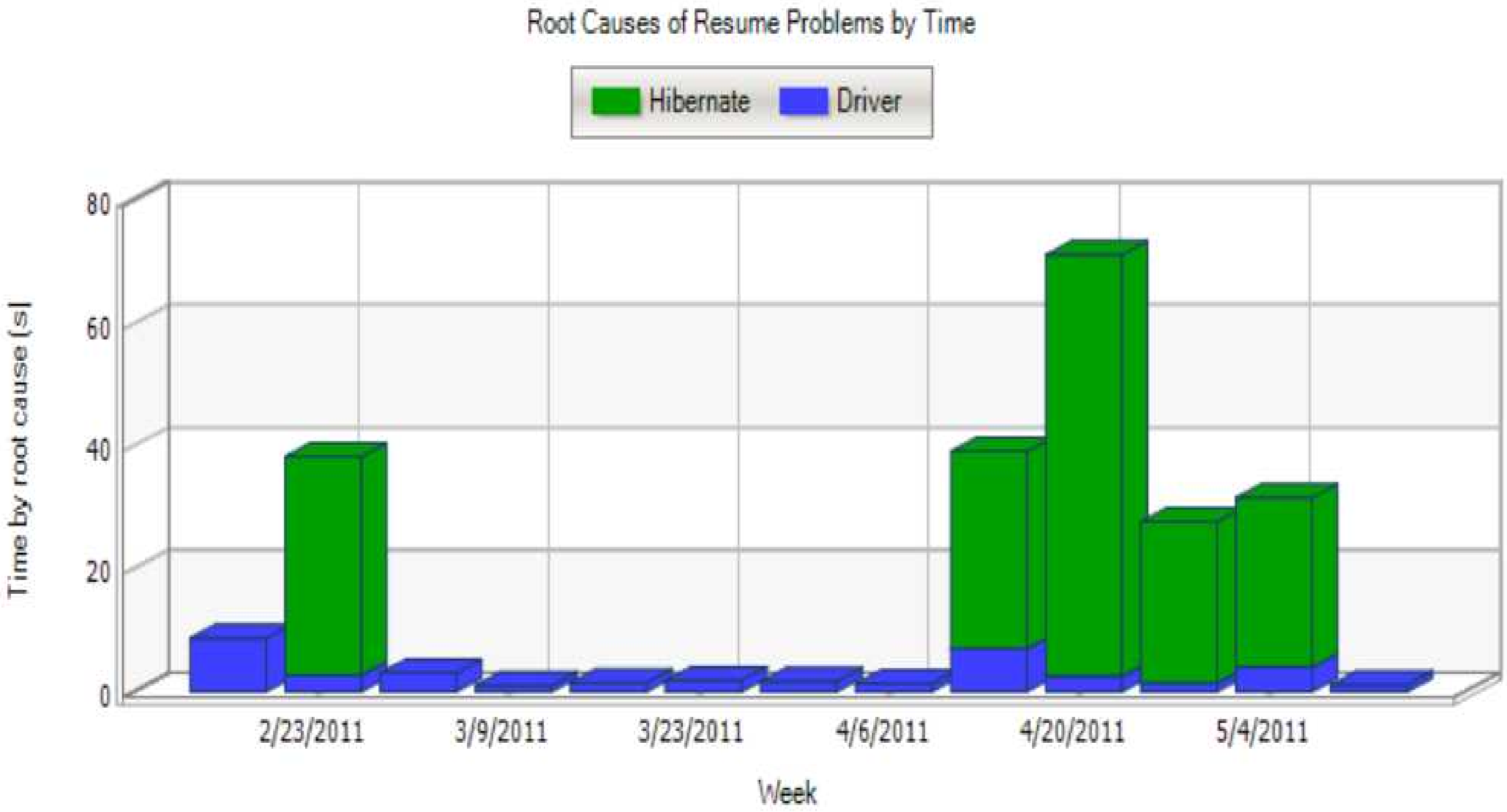
Overall Performance

This report charts the average time it took for machines of a particular model to resume over the last three months.

Data Trends

Root Causes (cont.)

This report shows the amount of time spent in the major areas of the resume sequence that caused significant resume performance degradation in the last three months.



Questions