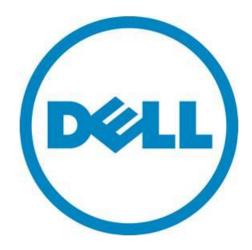
Proactively Managing Servers with Dell KACE and Open Manage Essentials

A Dell Technical White Paper

Dell | KACE

Dell Open Manage Essentials



THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2011 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, and the DELL badge, PowerConnect, and PowerVault are trademarks of Dell Inc. Symantec and the SYMANTEC logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the US and other countries. Microsoft, Windows, Windows Server, and Active Directory are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

December 2011

ii

Contents

Introduction	4
Inventorying and Managing Data Center Assets	6
Managing System Configurations	8
Managing System Updates	11
Assessing and Resolving Security Vulnerabilities	12
Monitoring and Fault Resolution	14
Reporting on Data Center Assets and Activities	15
Conclusion	17



Introduction

Constant change in computing environments represents a daunting challenge for every IT organization. Change is often driven from new requirements by the enterprise to meet the goals and demands of the business. But changes are also introduced by external influences, often in unplanned ways, in the form of component faults and remediation, required driver and firmware updates and software patches, and necessary configuration modifications to thwart security threats. IT staff can be diligent in planning for change and scheduling system updates accordingly. But effective planning gets sidetracked by surprises in system downtime or the discovery of critical issues that alter priorities. To ensure project planning remains on track and system health is maintained, it is essential to proactively control the discovery, testing, and implementation of system changes.

This is especially true for servers. They are typically housed in secured, air conditioned environments and therefore are not constantly monitored, yet they are responsible for tasks critical to the day-today operations of the enterprise and therefore warrant additional scrutiny. If our approach to identifying and addressing issues with these systems is to react when a problem arises, we risk significant disruption to IT services, to the organizations that rely on those services, and to the staff responsible for managing them. To begin proactively managing our servers, the following questions need to be answered:

- What models of devices do we have in our data center? What components are installed on them? Are the drivers and firmware for those components up-to-date?
- What software is installed on those systems? Have we applied all necessary patches from our software vendors?
- Are our system configurations consistent across servers? How do we manage server boot options and BIOS settings across those servers without having to visit each server and attach a console?
- Are our service contracts up-to-date on our servers? When will our warranties expire? How can we be notified of this event before it occurs?
- Are our systems vulnerable to security threats? How are we identifying our vulnerabilities? What are we doing to remediate these threats and how do we track that the remediation has been performed successfully?
- How do we know when a component has failed? How quickly are we able to react? How do we track the resolution of a component failure and record what we've learned?

To answer these questions effectively, we need a comprehensive view of the systems under management with the necessary tools to assess and update these systems before issues arise. Of course, this needs to be accomplished with minimal impact on the IT budget. So the tools need to be easy to acquire and learn with existing staff. Deployment of these management tools should minimize investment in time and resources and quantitatively return that investment quickly.

In this whitepaper, we will address these questions with Dell's innovative approach to systems management. The Dell | KACE K1000 Systems Management Appliance, combined with Dell OpenManage Essentials, provides a simple, cost-effective, and comprehensive approach that meets the needs of most enterprises. The following diagram illustrates how these products interact to provide a solution for proactive systems management.



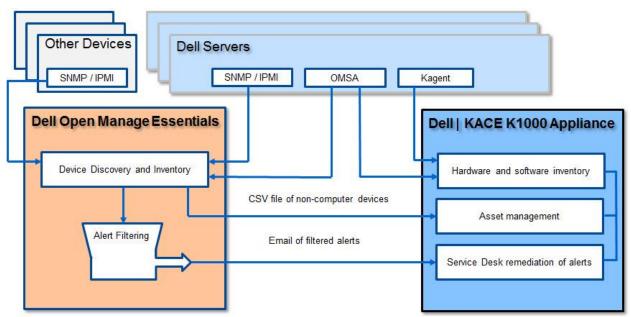


Figure 1: Solution Overview of Dell OpenManage and Dell | KACE

<u>Inventorying and Managing Data Center Assets</u> - Compute environment inventory requires that the data collected be comprehensive for virtualization platforms, network devices, printers, computer hardware and software. This data collection must be kept up-to-date in a way that does not distract from other day-to-day tasks. Both OME and the K1000 leverage industry-standard SNMP, IPMI, CIM, WMI, and other protocols to fully automate this task.

<u>Managing System Configurations</u> - Managing consistent system configurations across multiple systems is essential to maintaining overall compute environment health. The combination of OpenManage and KACE allow this capability to be centrally controlled across a heterogeneous environment.

<u>Managing Dell System Updates</u> - Keeping driver and firmware updates in control is key to protecting your Dell computing investment. Both OME and the K1000 offer fully integrated Dell system update capabilities to provide you choices that best meet your environments needs.

<u>Assessing and Resolving Security Vulnerabilities</u> - The Dell|KACE K1000 Systems Management Appliance provides vulnerability assessment tools based on industry standards and fully integrated patch management, configuration management, and distribution capabilities to resolve identified threats.

<u>System Monitoring and Fault Resolution -</u> The Dell OpenManage Essentials toolset provides active system monitoring via SNMP and IPMI, and delivers issues that have been identified for remediation to the Dell|KACE service desk for ownership assignment and resolution.

<u>Reporting on Data Center Assets and Activities -</u> Extensive reporting capabilities are provided to track progress and validate processes.



Inventorying and Managing Data Center Assets

The automation of inventory data collection is an essential first step in proactively managing data center assets. Since change is constant, this task must be performed consistently and on a regular basis to reflect an accurate baseline of the systems under management. While both OpenManage Essentials and the Dell|KACE K1000 appliance can discover devices on the network using ICMP and SNMP, far richer capabilities for servers are enabled by deploying agent software to the operating systems running on Dell PowerEdge Servers. For OpenManage Essentials this agent is the OpenManage Server Administrator software. OMSA may be deployed to Windows, Linux, and ESX/ESXi platforms and provides a consistent interface across all of these.

The data collected into OpenManage Essentials inventory by OMSA details the various hardware



components and associated firmware and driver packages in the PowerEdge chassis, including model and manufacturer information, relevant interface capabilities and form factor data. Any changes that occur due to field servicing would be reflected when new data is collected. Additionally, OME will collect ICMP and SNMP data on other devices, such as storage arrays, network devices, printers, and virtualization platforms for VMWare and Microsoft.

For the Dell | KACE K1000, the KAgent manages the required data collection for inventory and extends

this collection into the software applications that are running on the platform. It is also responsible for managing vulnerability assessment, patching, configuration, and deployment tasks for the managed systems and their software. The Dell | KACE K1000 appliance can also leverage the OMSA agent provided by OpenManage to collect additional data and manage configurations for Dell Servers running Windows Server 2000, 2003, and 2008, as well as Red Hat Linux 4 and 5. Information for other assets such as printers, network devices, and virtualization hosts can be loaded into the

K1000 Asset Management module.

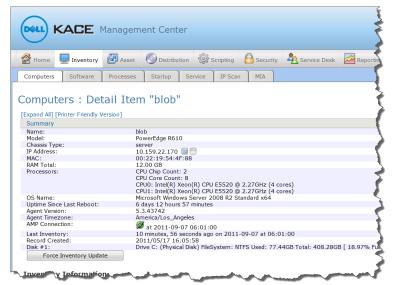


Figure 3: K1000 Inventory



~~~	Sortwal
	Installed Programs (32)
	7-Zip 4.65 (4.65.00.0)
	Dell KACE Agent (5.3.43742)
	Dell OpenManage Server Administrator (6.5.0)
	Dell Remote Access Port
	EZ GPO Power Management Config Tool (2.2.3)
	Intel(R) Network Connections Drivers (14.2)
	Matrox Graphics Software (remove only)
	Microsoft .NET Framework 1.1 (1.1.4322)
	Microsoft Application Error Reporting (12.0.6015.5000)
	Microsoft Security Compliance Manager (1.1.3.0)
	Microsoft SQL Server 2008 (64-bit)
	Microsoft SQL Server 2008 Browser (10.1.2531.0)
	Microsoft SQL Server 2008 Common Files (10.1.2531.0)
•	

Figure 4: K1000 Software Inventory

The K1000 agent leverages the relevant registry information on the operating system to identify the software packages that have been installed, including their version number, location within the file system, online links for additional information about each software title, and metadata for categorizing the inventory entry. Multiple software packages may be rolled up into a software title for management, including metering and license management.

Using the Managed Installation functionality of the K1000, the OMSA agent may be installed on multiple machines, greatly simplifying the deployment of the overall solution. The managed installation will transfer the installation package for OMSA to the target servers and execute the installation using the supplied installation parameters as shown below:

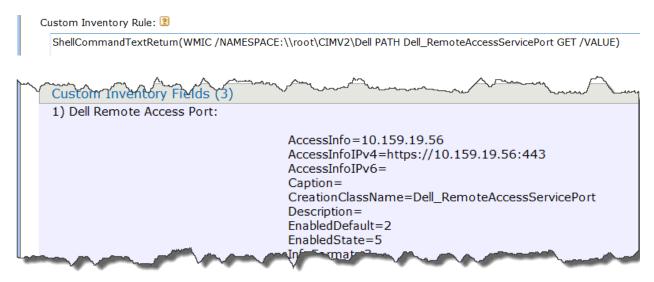
Install using "on-srvadmin-del-web-win-6.5.0-2247_a01.10.exe":
Favorites Fa
Imaged Installation     Imaged Software Installation : Edit Detail
Warsged Installation       Edit Detail         Install using "om-srvadmin-del-web-win-65.0-2247_a01.10.exe":       Managed Installations         There windows clerk will install to is vie:       The windows clerk will install to is vie:
KACE Management Center     Cobal Search     C
Managed Installations         File Synchronization         Wake-on-LAN         Replication         Phone         Dell Updates           Managed Installations:         Edit Detail         Back to MI Listing           Install using 'om-srvadmin-del-web-win-6.5.0-2247_a01.10.exe*:         Managed Installations           The windows clent will install this via:         Managed Installations           'Om-srvadmin-del-web-win-6.5.0-2247_a01.10.exe*         If your package file is a ap file
Managed Software Installation : Edit Detail       Back to MI Listing         Instal using 'om-srvadmin-del-web-win-6.5.0-2247_a01.10.exe':       Managed Installations         The windows cleft will install this via:       Managed Installations         'Om-srvadmin-del-web-wind-del-so.2247_a01.10.exe':       Managed Installations         The windows cleft will install this via:       If your package file is a ap file
Install using "om-srvadmin-dell-web-win-6.5.0-2247_a01.10.exe": The windows client will install this via: The windows client will install this via: If your package file is a zip file If your package file is a zip file
The windows client will install this via: "om-srvadmin -dell-web-win-6.3.0-2247_a01.10.exe" msiexec.exe /i SysMgmt.msi / qn If your package file is a zip file
The windows clent will install this via:
[Software Detail for Dell OpenManage Server Administrator (6.5.0) ] inside of that z ₀ please specify
This software will only be installed on the following Operating Systems: (edit) Windows Server 2008 R2 Std x64
Software: Dell OpenManage Server Administrator (6.5.0)  See the MGI commend Line documentation for MGI related documentation for MGI related
Filter: (3) Subtraction allows switches.Managed Action allows
Also show software without an Associated File 🔤
Upload & Associate New File: Browse.
before logon will install when the machine boots up, befault @ configure Manually the method is a set of the machine boots up, befault when the machine boots up, befault @ configure Manually the method is a set of the machine boots up, befault and the machine boots up, befaul
Run Parameters: msievec.eve /i Systemat.msi /an generation and an agoint and a systematic a
Delete Downloaded Files:
Use Alternate Download:
ApDeptor Live desktor is displayed.
Selecting Snoze will cause the
Threat: Not Reported user: Do not create a
Category: Unknown     Snoozeable package that is to     be deployed at a buse that the
More details at AppDeploy.com     user will not be logged in.     Encourse with existing will not be logged in.
E      Coal intranet   Protected Mode: Off     G      Coal intranet   Protected Mode: Off     G      Coal intranet   Protected Mode: Off     G     Coal intranet   Protected Mode: Off     G     Coal intranet   Protected Mode: Off     G     Coal intranet   Protected Mode: Off     G     Coal intranet   Protected Mode: Off     G     Coal intranet   Protected Mode: Off     G     Coal intranet   Protected Mode: Off     G     Coal intranet   Protected Mode: Off     G     G     Coal intranet   Protected Mode: Off     G     G     Coal intranet   Protected Mode: Off     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G     G

KACE

DELL

## Managing System Configurations

When OMSA is deployed to a server version of the Windows operating system of a Dell PowerEdge Server, it introduces Dell CIM instrumentation providers that deliver a WMI namespace (\\root\CIMv2\Dell) with several new classes and extensions to existing classes for managing devices within the Dell PowerEdge chassis and their associated applications and events. OpenManage Essentials leverages these CIM providers in its data collection for these devices as part of its core functionality. The Dell|KACE K1000 appliance can also collect this information as part of its inventory by defining custom inventory fields against the provided namespace.



#### Figure 5: Custom Inventory with Dell CIM

In the above example, the Dell WMI namespace is accessed to retrieve information about the out-ofband management facilities of the Dell Remote Access Controller, allowing the administrator to quickly identify and access a remote console for the server and control power management, BIOS settings, and other options even if the operating system on the server isn't available. However, this approach is limited to Windows platforms.

For cross-platform support, the OMREPORT and OMCONFIG command line interfaces of the OMSA agent may also be leveraged within the K1000 inventory for consistent data collection and operational control across both Windows and Linux operating systems.

Custom Inventory Rule: 😰

ShellCommandTextReturn(omreport storage pdisk controller=0)



<ol><li>System Physical Disks:</li></ol>	List of Physical Disks on Controller PERC 6/i Integrated (Embedded)
	Controller PERC 6/i Integrated (Embedded)
	ID: 0:0:0
	Status : Ok
	Name : Physical Disk 0:0:0
	State : Online
	Power Status : Not Applicable
	Bus Protocol : SAS
	Media : HDD
	Revision : S22C
	Failure Predicted : No
	Certified : Not Applicable
	Encryption Capable : No
	Encrypted : Not Applicable
	Progress : Not Applicable
	Mirror Set ID : Not Applicable
	Capacity: 136.13 GB (146163105792 bytes)
	Used RAID Disk Space : 136.13 GB (146163105792 bytes)
	Available RAID Disk Space : 0.00 GB (0 bytes)
	Hot Spare : No
	Vendor ID : DELL(tm)
_	Product ID : ST9146802SS
	Serial No. : 3NM8HLBK

#### Figure 6: Custom Inventory with OMSA OMREPORT

Actions may be enabled within the K1000 inventory that direct the administrator to the OMSA and DRAC web interfaces, conveniently placing remote control access to the server directly within the system management interface.

C	ompi	uter Inventory			View by: All Items -
Cł	noose A	rection  Found 4 computers.			Advanced Search
	ø	Name [labels hidden]	Last Sync 🖑	Description	IP
	ø	ns7	18m		96.245.105.253
	S	lightening.test.kace.com	19m	empty	10.159.17.43
-	100	and the second		• · · · · · · · · · · · · · · · · · · ·	

	NAGE™ SERVER ADMINISTRATOR	
blob PowerEdge R610 BLOB\administrator Admin	Properties Setup BIOS	
System     Main System Chassis     Batteries     BIOS     Fans     r	BIOS Setup Jump to: General   Serial Communications General	
Firmware Hardware Performai Intrusion	Instructions: Click each BIOS setup object to set its state.	
Memory Metwork Ports Power Management Power Supplies Processors Remote Access Slots Temperatures Voltages	Boot Sequence         Num Lock         User Accessible USB Ports         Processor Virtualization Technology         Processor Logical Processor (HyperThreading)         AC Power Recovery Mode         Embedded SATA Controller         SATA Port 0         Dual NIC (1/2)         Dual NIC (3/4)	On All Ports On Enabled Enabled Last ATA Auto Enabled with 1st NIC PXE and 2nd NIC None

DELL) KACE

#### Figure 7: Attaching a Machine Action to enable OMSA or DRAC

As changes occur to the system over time, these changes are recorded in the asset history of the system within the K1000 inventory, providing a single location to review what's been altered, when, and by whom.

[Show All History]						
History						
Time	Changes	Who				
2011/08/17 19:25:39 Machine disconnected.						
2011/08/14 13:23:57	Machine connected with address 12.201.5.178.					
2011/08/11 07:01:03	Found software item Security Update for Microsoft Windows (KB2539634) in inventory. Found software item Security Update for Microsoft Windows (KB2550532) in inventory. Found software item Security Update for Microsoft Windows (KB2550049) in inventory. Found software item Security Update for Microsoft Windows (KB2560656) in inventory. Found software item Security Update for Microsoft Windows (KB2560937) in inventory. Found software item Security Update for Microsoft Windows (KB256394) in inventory. Found software item Security Update for Microsoft Windows (KB2567680) in inventory. Found software item Security Update for Microsoft Windows (KB2567680) in inventory. Found software item Update for Microsoft Windows (KB2567680) in inventory. Found software item Update for Microsoft Windows (KB2567680) in inventory.					

#### Figure 8: Tracking Change History with the K1000 Asset History

The K1000 scripting module may be used to configure various system attributes on the managed services by leveraging the OMCONFIG command line interface of the OMSA agent. In this fashion, multiple Red Hat Linux and Windows servers in the managed environment may be consistently configured, even at the BIOS level. The OMCONFIG CLI provides extensive options for managing SNMP configurations and alert actions, log settings for system event logs (alert, command, and ESM), system shutdown and recovery options, chassis configurations, asset management, and power management and monitoring.

For example, SNMP events may be enabled or disabled for specific event types (e.g. power supplies, redundancy, temperature, fans, voltage, system power, memory, chassis intrusion, battery, and logs) and severity levels. The OMCONFIG command for enabling all event types would look like:

>omconfig system events enable type=<all>

Detailed documentation for the OMCONFIG command set for version 6.5 of OMSA may be found at

http://support.dell.com/support/edocs/software/svradmin/6.5/CLI/HTML/config.htm

## Managing System Updates

Both OME and the K1000 integrate with the Dell Update Center to provide the latest firmware and drivers updates for the components installed in your Dell equipment purchases. Updates are identified as critical, recommended or optional in accordance with the Dell Update Center and contain all pertinent details such as the version number and date of release,

Repository Information ftp.dell.com/catalog/Catalog.cab 🔹 🗗 🖸	pen Remove	: Details @ Compare					
Bundles Components	Repo	sitory: ftp.dell.com/cata	log/Cata	alog.c	ab (ftp	.dell.co	om/
Select Search Filter *	Bundle	(Selected/Total): (0/369)					
▼ Text Search		Name	Version 🔺	OS	Date	Size	Auth
		System Bundle (Linux) PE2970 v380	B107896.380	Linux	4/8/2011	264.05 MB	DEL
		System Bundle (Windows) PE2970 v380	B107896.380	Windows	4/8/2011	552.27 MB	DEL
▼ Update Type *		System Bundle (Linux) PE2970 v390	B107896.390	Linux	8/3/2011	264.12 MB	DEL
• opuale type		System Bundle (Windows) PE2970 v390	B107896.390	Windows	8/3/2011	552.5 MB	DEL
🗸 Drivers 🖌 Firmware 🗸 BIOS 🗹 Applications 🖌 Utilities		System Bundle (Linux) PE860 v380	B110855.380	Linux	4/8/2011	102.06 MB	DEL
		System Bundle (Windows) PE860 v380	B110855.380	Windows	4/8/2011	280.24 MB	DEL
▼ Criticality		System Bundle (Linux) PE860 v390	B110855.390	Linux	8/3/2011	102.1 MB	DEL
Optional Recommended Urgent		System Bundle (Windows) PE860 v390	B110855.390	Windows	8/3/2011	280.28 MB	DEL
		System Bundle (Linux) PE840 v380	B110857.380	Linux	4/8/2011	159.62 MB	Auth B DEL
<ul> <li>Form Factor</li> </ul>		System Bundle (Windows) PE840 v380	B110857.380	Windows	4/8/2011	393.2 MB	DEL
Component Version		System Bundle (Linux) PE840 v390	B110857.390	Linux	8/3/2011	159.7 MB	DEL
		System Bundle (Windows) PE840 v390	B110857.390	Windows	8/3/2011	393.29 MB	DEL
<ul> <li>Operating System</li> </ul>		System Bundle (Linux) PE6950 v380	B115842.380	Linux	4/8/2011	131.65 MB	DEL
Supported Platforms		System Bundle (Windows) PE6950 v380	B115842.380	Windows	4/8/2011	406.4 MB	DEL
<ul> <li>Supported Platforms</li> </ul>		System Bundle (Linux) PE6950 v390	B115842.390		8/3/2011		

OME introduces an optional component for loading driver and firmware updates into a local repository to manage reporting of available packages and scheduling deployment of the packages to systems. This functionality relies on the OMSA agent, and allows updates to be deployed to Windows, Linux, and ESX/ESXi host computers within the environment.

Figure 9: OME Dell Update Repository

The K1000 integrates Dell Updates as well, allowing the administrator to leverage a consistent set of functionality to schedule a set of driver and firmware updates to be applied to the machines that need them in the same fashion that they schedule OS and application patching. Unlike OME, these same processes for Dell updates and software patching may also be used for client systems, providing a consistent approach to all systems management. Extensive reporting is also provided including driver and firmware comparison reporting by each individual machine or across a range of machines in the environment

11

	mparison Report  2					
Se	rver Catalog	1				
ŧ	Package Name		Package Type	Device Version	Catalog Version	Criticality
L	DELL LIFECYCLE CONTROLLER, V.1.5.0.672, A01	Dell Lifecycle Controller	Application	1.3.0.350	1.5.0.672	Optional
2	DELL 32 BIT DIAGNOSTICS, V.5148A0, 5148.3	Dell 32 Bit Diagnostics	Application	5130A0	<b>1</b> 5148A0	Optional
3	DELL OS DRIVERS PACK, V.6.5.0.12, A00	Dell OS Drivers Pack, v.6.2.0.9, A00	Application	6.2.0.9	<b>1</b> 6.5.0.12	Optional
1	DELL SERVER BIOS 11G, 3.0.0	BIOS	BIOS	1.3.6	<b>1</b> 3.0.0	Recommende
5	MATROX G200EW VIDEO CONTROLLER, V.1.1.3.0, A00	Matrox G200eW (Nuvoton) - English	Driver	1.0.41.0	1.1.3.0	Optional
5	BROADCOM NETXTREME FAMILY OF ADAPTERS, NETXTREME II FAMILY OF ADAPTERS, V.16.2.0, A01	Broadcom NetXtreme I and NetXtreme II Driver Family	Driver	12.6.0	16.2.0	Recommende
7	INTEL INTEL PCI-E 10GIG AND 1GIG FAMILY OF SERVER ADAPTERS, V.12.5.5, A01	Intel PCI-E 10Gig and 1Gig Family of Server Adapters	Driver	0	<b>1</b> 2.5.5	Recommende
3	DELL IDRAC6, V.1.70, A02	iDRAC6	Firmware	1.70	1.70	
)	DELL PERC 6/I INTEGRATED, V.6.3.0-0001, A12	PERC 6/i Integrated Controller 0	Firmware	6.2.0- 0013	1 6.3.0- 0001	Recommende
10	SEAGATE HD,146G,SAS,3,10K,2.5,SGT2,DU, HD,73G,SAS,3,10K,2.5,SGT2,DU, V.S22C, A01	ST9146802SS	Firmware	S22C	\$22C	

Figure 10: K1000 Dell Update Comparison per Machine

While a choice will typically be made to use the Dell Update Center processes exclusively from either OME or the K1000, that choice can be driven by the needs of the environment rather than any incremental costs to the solution since both offerings provide Dell Update Center integration as part of their core functionality.



## Assessing and Resolving Security Vulnerabilities

Because the K1000 extends systems management to include the operating system and software applications, it is enabled to assess and address vulnerabilities across a full range of configurations. Assessments are performed using industry-standard approaches such as the Open Vulnerability Assessment Language and the Security Content Automation Protocol. Use of OVAL and SCAP ensures a reliable and reproducible set of metrics that are constantly updated as new threats are identified.

(Dell)	KACE Management Center	Organ	ization: ITA
0		Glo	bal Search
🚰 Home	: 🖳 Inventory 🖉 Asset 🕘 Distribution 🔹 Scripting 🔒 Security 🐴 Service Desk 🜌 Reporting 🛞 Settings		🕐 Helj
Patching	OVAL Assessment SCAP Scan Secure Browsers		
OVAL	Tests View by: Vulnerat	bilty •	Search
Choose A	Showing I-150 of 2982 tests. [Next]	Last Updated: 2011	/09/07 03:25:00
VALID 👌	Description	CVE Number	
	The Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to obtain sensitive information via crafted requests that leak information in SMB buffers, which are not properly initialized, aka "SMB Information Disclosure Vulnerability."	CVE-2006-1315	
	Integer overflow in Microsoft Word 2000, 2002, 2003, 2004 for Mac, and v.X for Mac alows remote user-assisted attackers to execute arbitrary code via a crafted string in a Word document, which overflows a 16-bit integer length value, aka "Memmove Code Execution," a different vulnerability than CVE-2006-3651 and CVE- 2006-4693.	CVE-2006-3647	
	string in a Word document, which overflows a 16-bit integer length value, aka "Mermove Code Execution," a different valuerability than CVE-2006-3651 and CVE- 2006-4903. Microsoft Internet Explore 5 SP4 and 6 do not properly garbage collect when "multiple imports are used on a styleSibeets collection" to construct a chain of		
	string in a Word document, which everflows a 16-bit integer length value, aka "Memmove Code Execution," a different valuerability than CVE-2006-3651 and CVE- 2006-4693. Nonsoft Internet Explorer 5544 and 6 do not propely aphrage codera when "Imagine importa are used on a styleSheets collection" to construct a chain of Coscarding Syle-Sheets (SS), which alsens rome a traduces to construct a trading and program definitions.	CVE-2006-3451	
	string in a Word document, which overflows a 16-bit integer length value, aka "Mermove Code Execution," a different valuerability than CVE-2006-3651 and CVE- 2006-4903. Microsoft Internet Explore 5 SP4 and 6 do not properly garbage collect when "multiple imports are used on a styleSibeets collection" to construct a chain of		
2	string in a Word ocument, which overflows a 16-bit integer length value, aka "Mermmove Code Execution," a different vulnenability than CVE-2006-3651 and CVE- 2006-4693. Wooshil talemet Explores 5 SH4 and 6 do not properly garlage collect when "multiple imports are used on a style/Sheets collection" to construct a chain of Cascading Syn& Steets (CSS), which allows remote structeers to execute athiltary code was unspecified vectors. Howported Valenability in the Server server is functored Windows (MA) Server 2003 SH and earlier, and XF SP2 and earlier allows remote attackers to execute abitrary code via a crited potect, aka SHR Reamant WineshBM; ¹ Internet Explores SS and 6 allows remote attackers to typess restrictions for executing scripts via an object that processes asynchronous events after the Initial	CVE-2006-3451	
2	string in a Word document, which overflows a 16-bit integer length value, alsa "Merrmove Code Execution," a different valenability than CVE-2006-3651 and CVE- 2006-4693. Monosoft hitement Explorer 55M and 66 in ont propely gatapage collect when "multiple imports are used on as style/Selets collection" to construct a chain of Coscarding SyNE-Selection (CSS), which alses reservice in Microsoft Windows 2000 SP4, Server 2000 SP4,	CVE-2006-3451 CVE-2006-4696	
	string in a Word ocument, which overflows a 16-bit integer length value, aka "Mermmove Code Execution," a different vulnenability than CVE-2006-3651 and CVE- 2006-4693. Wooshil talemet Explores 5 SH4 and 6 do not properly garlage collect when "multiple imports are used on a style/Sheets collection" to construct a chain of Cascading Syn& Steets (CSS), which allows remote structeers to execute athiltary code was unspecified vectors. Howported Valenability in the Server server is functored Windows (MA) Server 2003 SH and earlier, and XF SP2 and earlier allows remote attackers to execute abitrary code via a crited potect, aka SHR Reamant WineshBM; ¹ Internet Explores SS and 6 allows remote attackers to typess restrictions for executing scripts via an object that processes asynchronous events after the Initial	CVE-2006-3451 CVE-2006-4696	
	string in a Wed document, which overflows a 16-bit integer length value, als. "Memmore Cold Execution," a different valuesability than CHE-2006-3651 and CHE- 2006-4693. Morsolit hittenet Explorer SSM and 6-for to propely gataget collect when "multiple imports are used on as style/Sheets collection" to construct a data of Catacolog SyME-Based (CS), which alises meet activacies to executing collect when a collection and the construct a data of Catacolog SyME-Based (CS), which alises meet activacies to executing collect values. Dispected whenebly in the Somer service in Riccosoft Winking 2000 SM, Server 2000 SM and Catacolog SM, Server 2000 SM and Catacolog SM, Server 2000 SM,	CVE-2006-3451 CVE-2006-4696 CVE-2002-0026	
3	string in a Nord document, which overflows a 16-bit integer length value, alsa "Merrmove Code Execution," a different valenability than CVE-2006-3651 and CVE- 2006-4693. Monosch Thement Explorer 55M and 66 not spropely gatapage collect when "multiple imports are used on as stylic/betts collection" to construct a chain of Coscarding SyNE-Stear (CSS), which also are rearised in Microsoft Withows 2000 SP4, Serier 2000 SP4 and earlier, and XP SP2 and earlier allows remote attackes to exerce a cascalta abstry code values and constraints. "SPRB fearmer Valueshamble". Interest Explorer SS and 6.0 allows remote attackes to exerce a thirdness" to constraint attackes to execute abstry code values and code and code string and and and the string string and and and and and and executly codes takes been made. Harap-based buffer overflow in RNH, Mely CAVed control (Michickov) in Microsoft Themest Explorer 6.0 allows remote attackes to cause a denial d revine (regoration casca) and long strings.	CVE-2006-3451 CVE-2006-4696 CVE-2002-0026	
5	string in a Wed document, which overflows a 16-bit integer length value, als. "Memmore Cold Execution," a different valuesability than CHE-2006-3651 and CHE- 2006-4693. Morsolit hittenet Explorer SSM and 6-for to propely gataget collect when "multiple imports are used on as style/Sheets collection" to construct a data of Catacolog SyME-Based (CS), which alises meet activacies to executing collect when a collection and the construct a data of Catacolog SyME-Based (CS), which alises meet activacies to executing collect values. Dispected whenebly in the Somer service in Riccosoft Winking 2000 SM, Server 2000 SM and Catacolog SM, Server 2000 SM and Catacolog SM, Server 2000 SM,	CVE-2006-3451 CVE-2006-4696 CVE-2002-0026 CVE-2006-3357 CVE-2002-0079	
2 3 6	string in a Word document, which overflows a 16-bit integer length value, als "Merminove Code Execution," a different valuesability than CHE-2006-3651 and CME- 2006-4693. Moreosoft histement Explorer SSPA and 6 is not spropely pathage collect when "multiple imports are used on as style/bettes collection" to construct a data of Cascading SyNE-Description (CSS), which also remote attackets to research alteriary cole values/general description (CSS), which also remote attackets to execute actuation style-Description (CSS), which also remote attackets to research alteriary cole values/general description (CSS), which also remote attackets to execute actuation attacket and a collegation (CSA). SSRE Reame Valuesability," Interest Explorer SS and 6.0 allows remote attackets to research theorem Explorer 6.0 allows remote attackets to exacu- ated after overlaw in the Histophic Coll (MecAlcoc) in Microsoft Interest Explorer 6.0 allows remote attackets to exacu- ated addition (CSA) and allows remote attackets to the sense in the Interest Explorer 6.0 allows remote attackets to cause a denial of sense: actuation activation of the Allow (MecAlcoc) in Microsoft Interest Explorer 6.0 allows remote attackets to cause a denial of sense: denial definer verifies in TMI-Meg Actived control (MecAlcoc) in Microsoft Interest Explorer 6.0 allows remote attackets to cause a denial of sense: denial denial deni	CVE-2006-3451 CVE-2006-4696 CVE-2002-0026 CVE-2006-3357	
	string in a Nord document, which overflows a 16-bit integer length value, alsa "Merrmove Code Execution," a different valenability than CVE-2006-3651 and CVE- 2006-4693. Monosch Thement Explorer 55M and 66 in ont spropely gatapage collect when "multiple imports are used on as style/Settes collection" to construct a chain of Coscarding SyNE-Setters (CSS), which alses reservice in Microsoft Windows 2000 SP4, Server 2000 SP4, S	CVE-2006-3451 CVE-2006-4696 CVE-2002-0026 CVE-2006-3357 CVE-2002-0079	

KACE

Figure 11: OVAL Vulnerability Assessment Tests

Assessments may be applied across multiple machines using the same dynamic grouping mechanism available to all features of the K1000, allowing scanning schedules to account more frequently for those systems that are of highest concern. When vulnerabilities are identified, patching and system configuration changes for the affected system may be addressed directly within the appliance.

Patching Detect/Deploy St	atus and a second a s
Threat Level 5 List (0)	
Oval Vulnerabilities (2)	
OVAL Test Runner	🖋 View Logs
Å Vulnerable	3556: The Microsoft .NET forms authentication capability for ASP.NET allows remote att
Å Vulnerable	1039: Buffer overflow in a component of SQL-DMO for Microsoft Data Access Components (
ᢞ True	454: Microsoft XML Core Services 6 is installed
ᢞ True	4870: The operating system installed on the system is Microsoft Windows Server 2008 (3
🗹 True	5525: Test if this OS should support WMI service. Note: different Objects are
ᢞ True	1934: Microsoft .NET Framework 2.0 (Original RTM or later) is installed
🗹 True	310: Microsoft .NET Framework 2.0 is installed
ᢞ True	324: Microsoft Visual Studio .NET 2005 is installed
ᢞ True	415: Microsoft XML Core Services 3 is installed
ᢞ True	6210: A version of Microsoft Internet Explorer 8 is installed 1853 other yulnerabilities

Figure 12: OVAL Test as Applied to a Machine in Inventory

The K1000 provides an extensive patch management system as part of its feature set that includes a constantly updated patch repository, and scheduling system for deploying different sets of patches to different machines based on the attributes of the patches and machines in question. The flexibility of this approach allows differing policies to be applied to different servers in the environment, while providing a single, unifying view of vulnerability assessment and remediation across all systems in the environment. Extensive reporting delivers the assurance that systems are up-to-date, including detailed reporting of each individual system and any operating system or applications patches that have been identified as needed for that system.

∖64~-	?	Sun_o/JRE 1.6.0_25 for Windows (64Bit) (Full/Upgrade) (All Languages) (See Notes)	MOTPÂTCHÊL⁄	2011-00- 14T17:08:00- 07:00		0000-00- 0000:00	0~~~	0000-00-00-00-00-00-00-00-00-00-00-00-0	Sun
65	?	Sun Java JRE 1.6.0_25 for Windows (Full/Upgrade) (All Languages) (See Notes)	NOTPATCHED	2011-06- 14T17:08:00- 07:00		0000-00- 00 00:00	0	0000-00- 00 00:00	0
66	?	WinZip 14.5 (Full Install) (All Languages) (See Notes)	NOTPATCHED	2011-06- 14T17:08:00- 07:00		0000-00- 00 00:00	0	0000-00- 00 00:00	0
67	Ľ	2443685 Update for Windows Server 2008 R2 x64 (KB2443685)	PATCHED	2011-06- 14T17:08:00- 07:00		0000-00- 00 00:00	0	0000-00- 00 00:00	0
68	Ľ	974431 Update for Windows Server 2008 R2 x64 Edition (KB974431)	PATCHED	2011-06- 14T17:08:00- 07:00		0000-00- 00 00:00	0	0000-00- 00 00:00	0
69	2	977074 Update for Windows Server	PATCHED	2011-06-	~~~	0000-00-	0	0000-00-	0

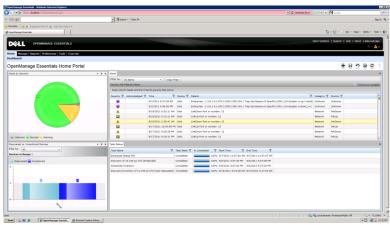
#### Figure 13: Patching Status for a Machine in Inventory

This ability to detect system vulnerabilities using industry-standard protocols, and resolve those vulnerabilities by applying needed system firmware and driver updates, as well as operating system and application software patches all within a single system management platform means greater productivity for your IT staff. System administrators will spend less time identifying and researching issues, and applying appropriate remedies to resolve vulnerabilities. And management will have the assurance and accountability that system weaknesses have been addressed via the compliance reports.



## System Monitoring and Fault Resolution

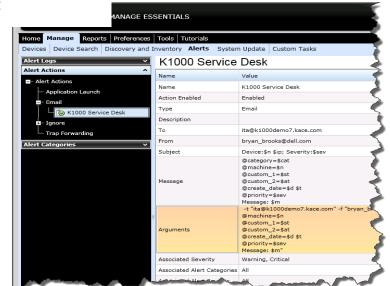
Possibly the most important task to be automated is proactive identification of faults within the systems being monitored, and tracking of the fault remediation to its conclusion. OME provides active monitoring of Dell and non-Dell computer systems and other devices via industry-standard SNMP and



IPMI protocols. Specific faults to be monitored may be configured within the OpenManage Server Administrator or OME may capture any SNMP trap information that has been issued on a monitored system. Because the K1000 can control configurations across a range of machines by accessing the OMSA OMCONFIG command line interface, SNMP and IPMI settings can be consistently applied for multiple systems.

Figure 14: Monitoring and Filtering Alerts in OME

Once a fault has been identified by OME, filters may be applied to determine if it is a fault that requires administrative intervention. If so, the alert information is transmitted as an email via SMTP to the K1000 service desk for ownership assignment and remediation within the IT team. Information contained within the alert is assigned into the appropriate fields within the email that will generate the ticket so that the necessary reference information is available to the assigned administrator. In this fashion, complete control can be maintained for those faults



that require intervention and remediation.



When configuring the Alert Action in OME,

14

the administrator has options for filtering the alerts to only those that require action, and defining which attributes of the alert need to be transferred to the service desk in the K1000 so the assigned administrator may resolve the issue. Alerts may be filtered based on the severity of the event, user defined alert category, device type, and time of the event.

When configuring the email that will be sent to the K1000 service desk for a filtered alert, the following attributes may be communicated as part of the event:

- Device (\$n) the fully qualified domain name of the device as returned from DNS
- Device IP (\$ip) The assigned IP address for the device
- Service Tag (\$st) The Dell Service Tag assigned to the device



- Asset Tag (\$at) The asset tag assigned by the customer to the device within BIOS
- Date and Time (\$d and \$t)- The date and time of the alert event
- Severity (\$sev) The severity of the event (Normal, Warning, Critical, Unknown)
- Alert Category Name (\$ct) The category of the alert. Several default values are preconfigured and more may be configured within OME
- Alert Source Name (\$st) The source of the alert.
- Package Name (\$pkn) The package associated with the alert event.
- Enterprise OID (\$e) The object identifier for the type of managed object that generated the trap
- Specific Trap OID (\$sp) The specific trap code identifier for the generated trap
- Generic Trap OID (\$g) One of a number of generic trap types as generated from SNMP
- Message (\$m) The message of the alert identifying details of the identified issue

These attributes are assigned to fields in the K1000 service desk ticket by mapping them to the appropriate receiving field in the K1000 service desk. The receiving field is identified by using an '@' sign and the name or label of the field in the service desk ticket configuration. For example, to map the Asset Tag to a custom field in the service desk ticket, the mapping may appear as:

- @custom_n=\$at (where 'n' is the custom field in the ticket being used for asset tag); or
- @asset_tag=\$at (where asset_tag is the label assigned to the custom_n field used for asset tag)

When the ticket is created within the K1000 Service Desk, the category of the alert is available to manage routing of the ticket to the right team for resolution, and all of the controls necessary for managing ownership assignment, approvals, and other tracking are available. When the Kagent is present on the machine, its entry in the K1000 inventory is directly accessible from the ticket by clicking on the "Machine" link in the ticket. If the device in the ticket does not have the Kagent installed on it, it may still be referenced using the "Asset" link

provided the asset information has been

loaded into the K1000.

DELL KACE Management Center 🖀 Home 📃 Inventory 🛛 Asset 💿 Distribution 🔅 Scripting 🔒 Security 🤱 Service Desk Tickets Software Library Knowledge Base Users Roles Configuration Ticket TICK:0218 [Printer Friendly] [Find Related Articles] [Email Ticket] [New Ticket For Submitter] [Ticket Actions] Title: Device:blob 10.159.22.170; Severity:Warning Impact: Many people can't work Category: Storage Peripheral Status: New Priority: Warning -Owner: brvan brooks@dell.com Filter: (2) Machine: 🗹 blob Unassigned Filter: Asset: (11) 92091J1 Service Tag: set Tarr - A A A MAN James Brance Bra

Figure 16: Ticket for an Alert in the K1000 Service Desk

Working together, OME and the K1000 provide an end-to-end solution for proactively identifying and resolving issues within the environment.



## **Reporting on Data Center Assets and Activities**

Delivering effective reporting to the IT team and to management communicate issues that may impact priorities and illustrates successful and timely execution of processes. Both OME and the K1000 provide out of the box reports that describe the inventory under management.

	KACE Management Center	
🔗 н	me 📃 Inventory 🖾 Asset 💿 Distribution 🕸 Scripting 🔒 Secu	2
Repo	ts Classic Reports Schedule Reports Alerts Email Alerts	Ì
К10	00 Reports	1
Choo	e Action	Ì
	Report	į.,
	Closed Satisfaction Survey last 31 days by Owner	$\langle$
	Closed Ticket Resolutions last 7 days by Owner	2
	Closed Ticket Resolutions last 31 days by Owner	Ş
	Closed Tickets last 7 days by Owner	Į
	Closed Tickets last 31 days by Category	Ļ
	Closed Tickets last 31 days by Owner	5
	Escalated/Open Tickets by Owner	5
	Open Tickets by Category	Ì
	Open Tickets by Owner	
	Open Tickets last 7 days by Owner	
	Stallad/Open Tickets by Category	2

Figure 17: K1000 Service Desk Reports

The K1000 extends this to provide reporting on activities being conducted within the environment, including service desk ticket resolution, patching status across multiple machines, top vulnerabilities that need to be addressed, software compliance issues, and so on. Custom reports may also be configured to address processes that are specific to the environment.

Additionally, the K1000 will collect the warranty information for machines in inventory and provide reporting and alerting for warranty expirations that are coming due. This provides the peace of mind that the servers under management have up-to-date service contracts.

	Date:	2009/06/22				
_		2003/00/22				
Cou	ntry:	United States				
#	Descriptio	'n	Provider	Start Date	End Date	Days Left
1	Next Business Day Support		UNY	2010/06/23	2012/09/20	380
2	Next Business Day Support		UNY	2009/06/22	2010/06/22	0





## Conclusion

The Dell | KACE K1000 System Management Appliance, combined with OpenManage Essentials and OpenManage Server Administrator, provide a simple, cost-effective solution for managing your data center assets. Deployment can be completed quickly and with existing staff so the return on investment is quickly realized. With the combined solution in place, your staff will know all aspects of the hardware and software you have deployed in your data center and their update status. They will be able to track what changes have taken place over time and by whom. When vulnerabilities are identified, service contracts are nearing expiration, or components fail, you staff will be in a position to address these concerns quickly and proactively. Most importantly, the organization as a whole will harvest the benefits of reliable IT services to achieve overall business objectives.



#### **Other Resources**

Dell OpenManage is a collection of software tools developed by Dell that helps you discover, monitor, manage, and update Dell servers.

Documentation and downloads for OpenManage Server Administrator may be found at http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.aspx

Documentation and downloads for OpenManage Essentials may be found at <a href="http://delltechcenter.com/ome">http://delltechcenter.com/ome</a>

#### Dell KACE Corporate Background

Dell (NASDAQ: DELL) creates, enhances and integrates technology and services customers count on to provide them reliable, long term value. Dell provides systems management solutions for customers of all sizes and system complexity. The award-winning Dell KACE family of appliances delivers easy-to-use, comprehensive, and affordable systems management capabilities.

Dell KACE is headquartered in Mountain View, California. To learn more about Dell KACE and its product offerings, please visit www.dell.com/kace or call 1-877-MGMT-DONE. Helpful Links:

• KACE Systems Management Appliances

• KACE Systems Deployment Appliances

#### **Dell KACE Headquarters**

2001 Landings Drive Mountain View, California 94043 (877) MGMT-DONE office for all inquiries (+1) (650) 316-1050 International (650) 649-1806 fax kaceinfo@dell.com European Sales: kaceemea@dell.com Asia Pacific Sales: kaceapac@dell.com Australia New Zealand Sales: kaceanz@dell.com While every effort is made to ensure the information given is accurate. Dell does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

