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

Copyright © 2011 Dell | KACE. All rights reserved.

Contents

Copyright © 2011 Dell | KACE. All rights reserved.

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-to-day 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.

Copyright © 2011 Dell | KACE. All rights reserved.

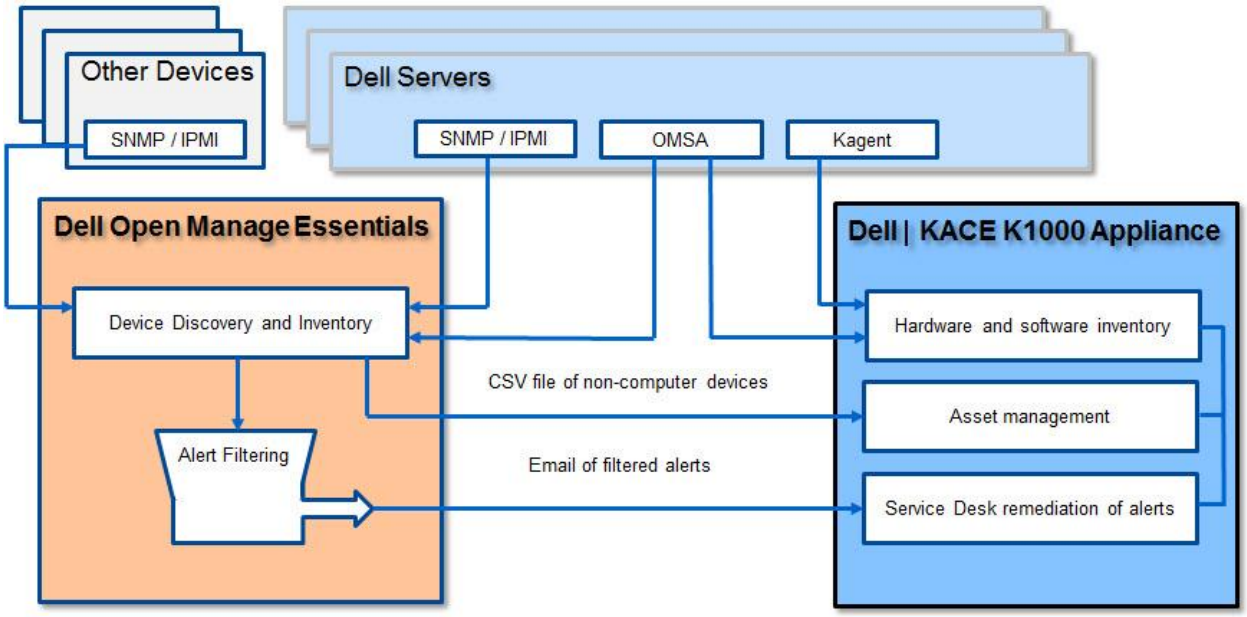


Figure 1: Solution Overview of Dell OpenManage and Dell|KACE

Inventorying and Managing Data Center Assets - 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.

Managing System Configurations - 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.

Managing Dell System Updates - 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.

Assessing and Resolving Security Vulnerabilities - 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.

System Monitoring and Fault Resolution - 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.

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

Copyright © 2011 Dell | KACE. All rights reserved.

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.

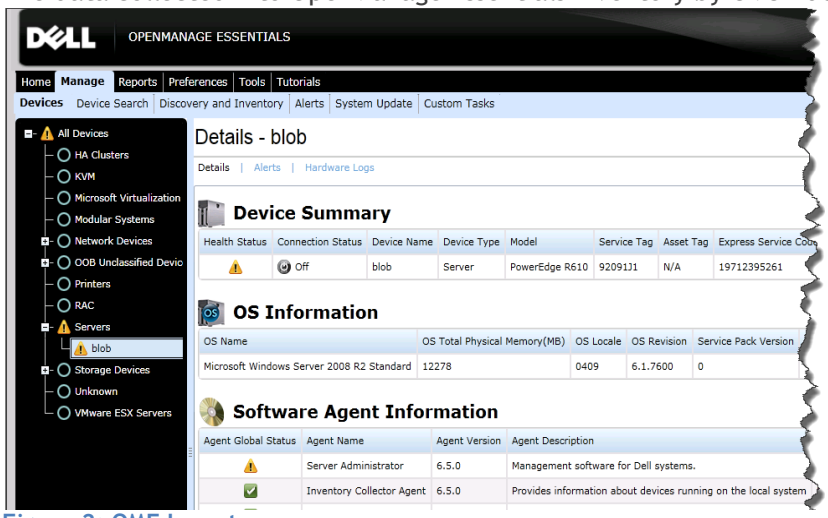


Figure 2: OME Inventory

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.

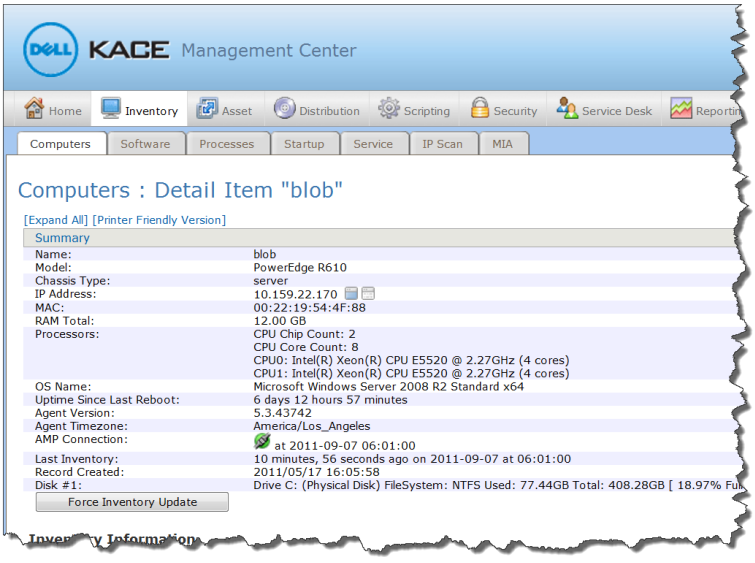


Figure 3: K1000 Inventory

Copyright © 2011 Dell | KACE. All rights reserved.

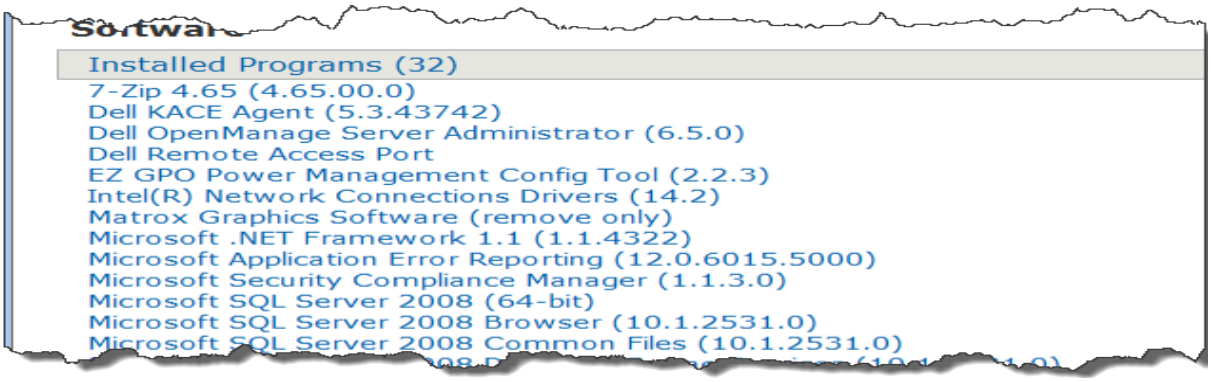
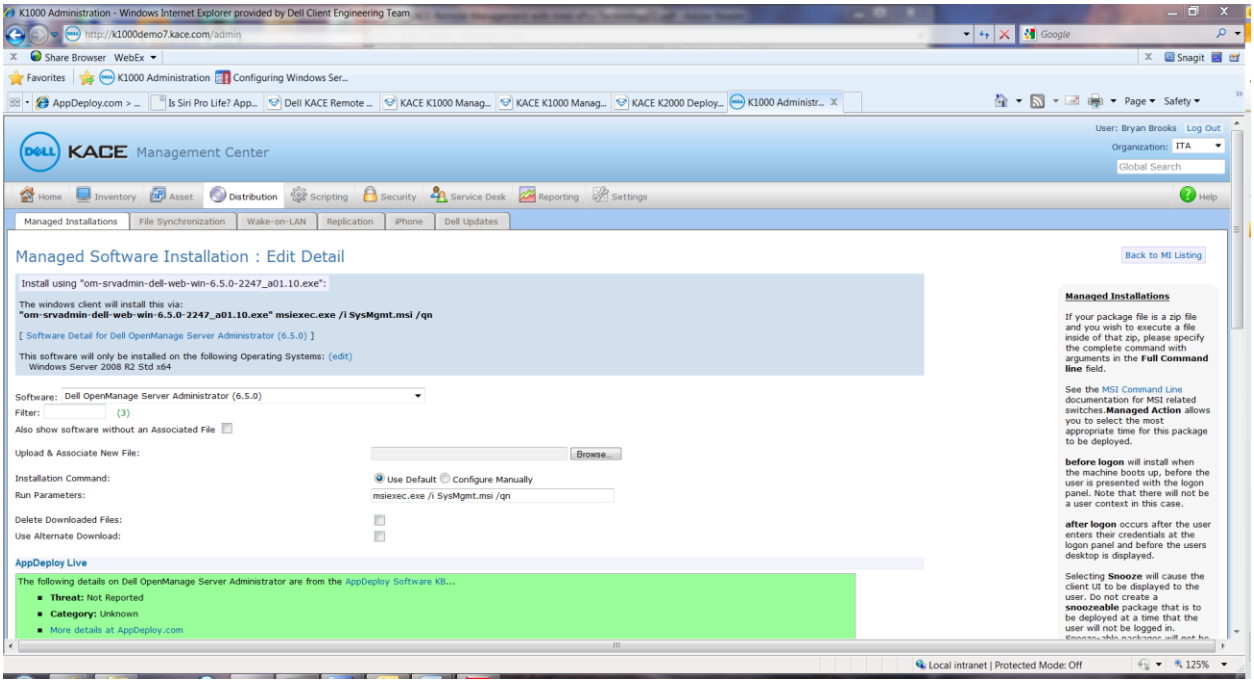


Figure 4: K1000 Software Inventory

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:



Copyright © 2011 Dell | KACE. All rights reserved.

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.

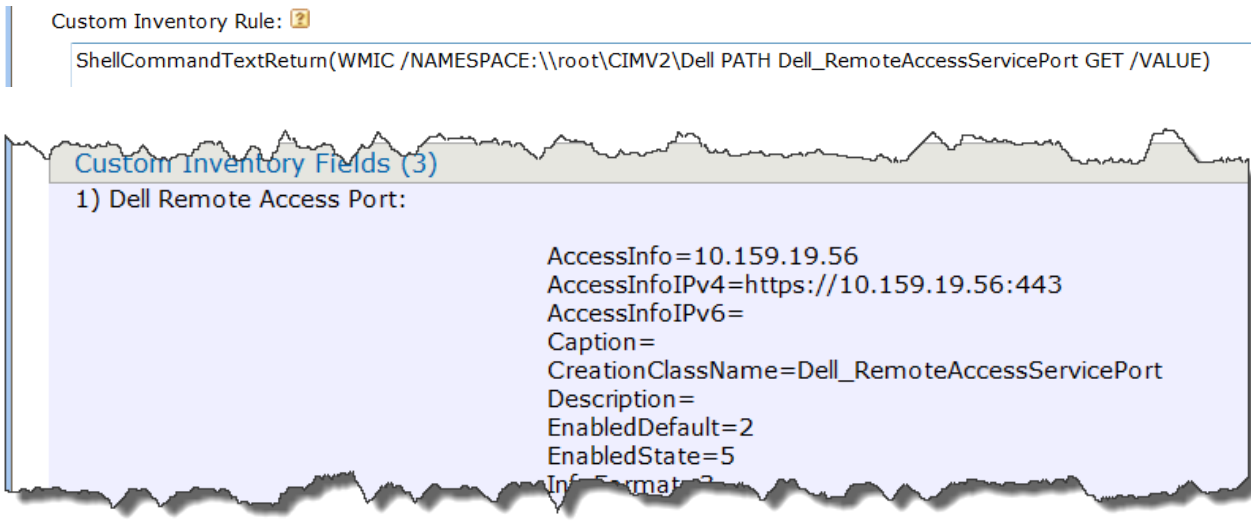
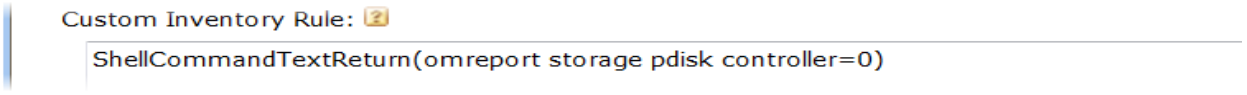


Figure 5: Custom Inventory with Dell CIM

In the above example, the Dell WMI namespace is accessed to retrieve information about the out-of-band 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.



Copyright © 2011 Dell | KACE. All rights reserved.

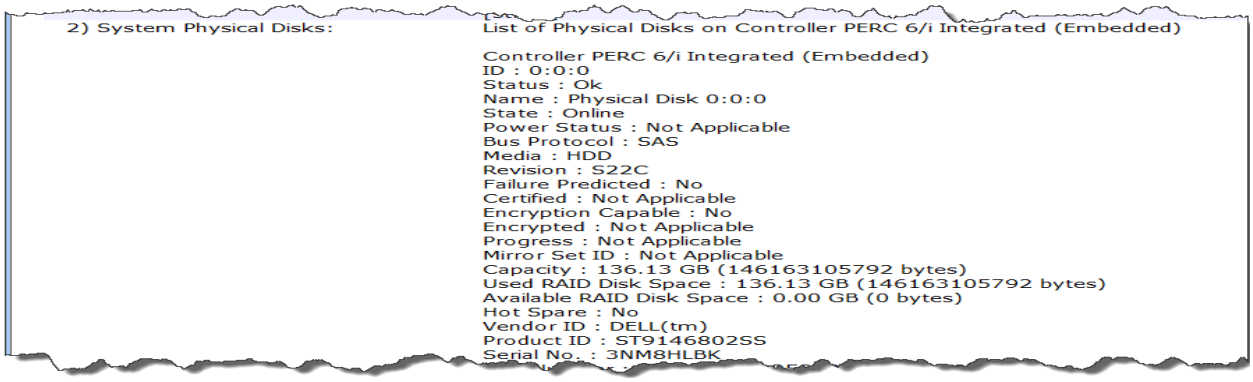


Figure 6: Custom Inventory with OMSA OMREPORT

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.

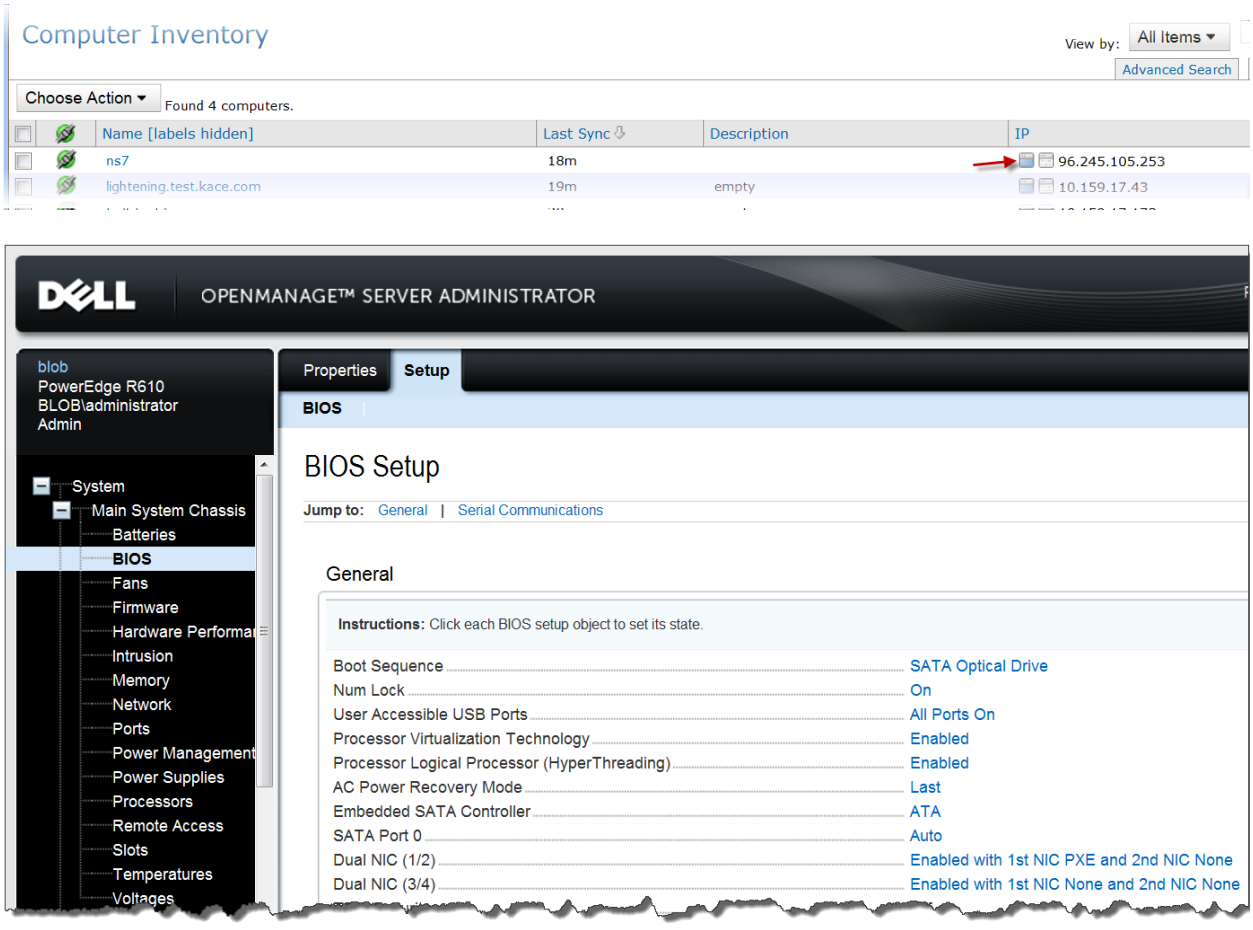
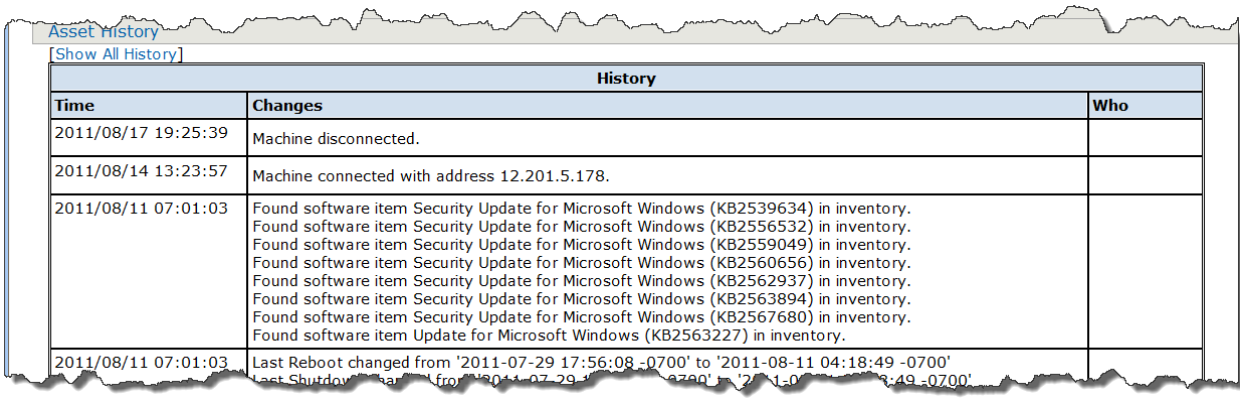


Figure 7: Attaching a Machine Action to enable OMSA or DRAC

Copyright © 2011 Dell | KACE. All rights reserved.

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.



Asset History

[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 (KB2556532) in inventory. Found software item Security Update for Microsoft Windows (KB2559049) in inventory. Found software item Security Update for Microsoft Windows (KB2560656) in inventory. Found software item Security Update for Microsoft Windows (KB2562937) in inventory. Found software item Security Update for Microsoft Windows (KB2563894) in inventory. Found software item Security Update for Microsoft Windows (KB2567680) in inventory. Found software item Update for Microsoft Windows (KB2563227) in inventory.	
2011/08/11 07:01:03	Last Reboot changed from '2011-07-29 17:56:08 -0700' to '2011-08-11 04:18:49 -0700'	

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

Copyright © 2011 Dell | KACE. All rights reserved.

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,

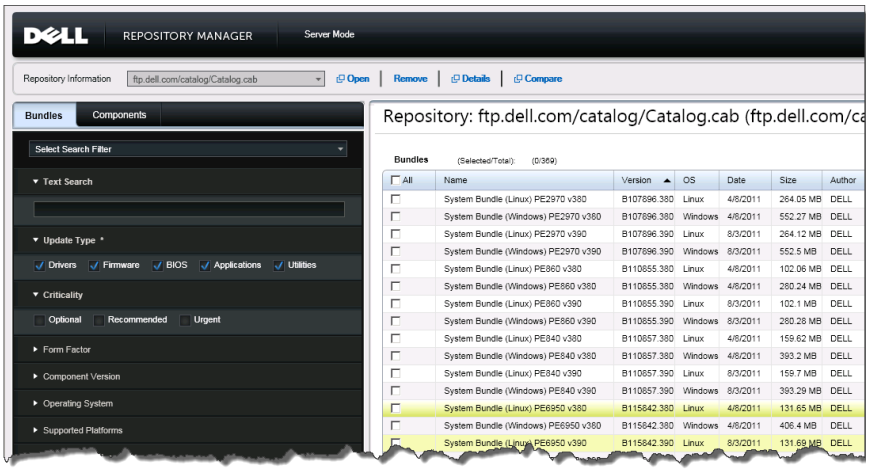
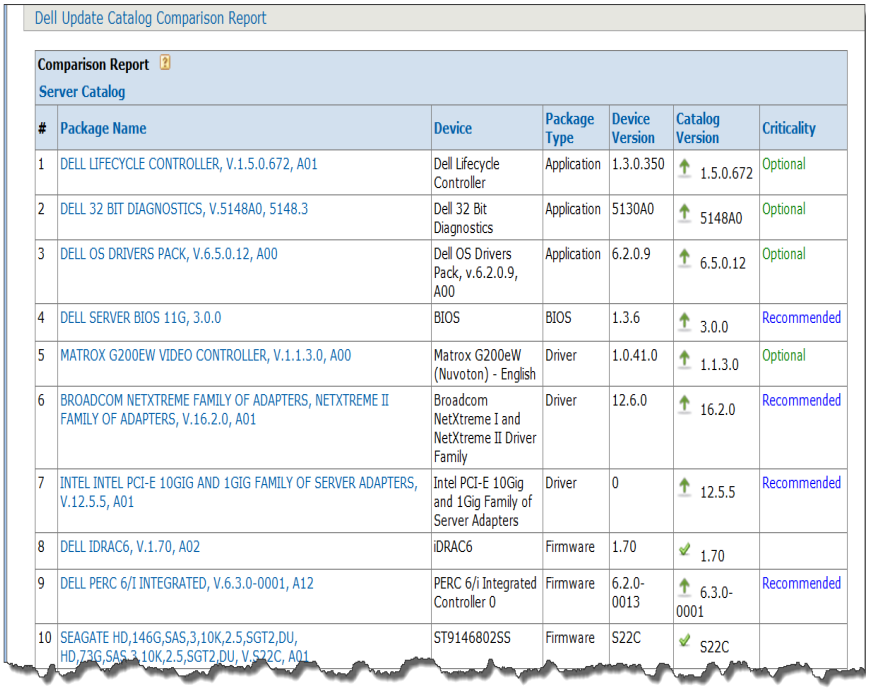


Figure 9: OME Dell Update Repository

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.

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



#	Package Name	Device	Package Type	Device Version	Catalog Version	Criticality
1	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	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	6.5.0.12	Optional
4	DELL SERVER BIOS 11G, 3.0.0	BIOS	BIOS	1.3.6	3.0.0	Recommended
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
6	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	Recommended
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	12.5.5	Recommended
8	DELL IDRAC6, V.1.70, A02	iDRAC6	Firmware	1.70	1.70	
9	DELL PERC 6/I INTEGRATED, V.6.3.0-0001, A12	PERC 6/i Integrated Controller 0	Firmware	6.2.0-0013	6.3.0-0001	Recommended
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	S22C	

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.

Copyright © 2011 Dell | KACE. All rights reserved.

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.

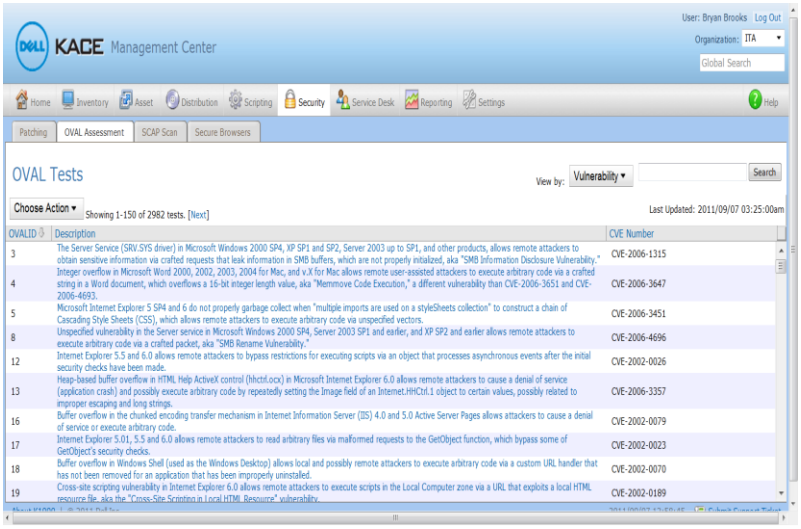


Figure 11: OVAL Vulnerability Assessment Tests

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.

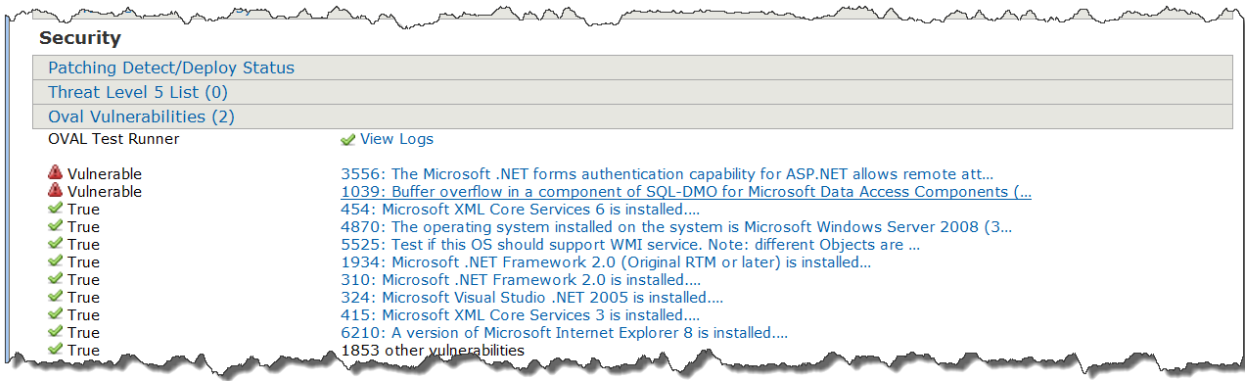


Figure 12: OVAL Test as Applied to a Machine in Inventory

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.

Copyright © 2011 Dell | KACE. All rights reserved.

64	?	Sun Java JRE 1.6.0_25 for Windows (64Bit) (Full/Upgrade) (All Languages) (See Notes)	NOTPATCHED	2011-06-14T17:08:00-07:00		0000-00-00 00:00:00	0		0000-00-00 00:00:00	0
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 00:00:00	0		0000-00-00 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 00:00:00	0		0000-00-00 00:00:00	0
67	✓	2443685 Update for Windows Server 2008 R2 x64 (KB2443685)	PATCHED	2011-06-14T17:08:00-07:00		0000-00-00 00:00:00	0		0000-00-00 00:00:00	0
68	✓	974431 Update for Windows Server 2008 R2 x64 Edition (KB974431)	PATCHED	2011-06-14T17:08:00-07:00		0000-00-00 00:00:00	0		0000-00-00 00:00:00	0
69	✓	977074 Update for Windows Server 2008 R2 x64 Edition (KB977074)	PATCHED	2011-06-14T17:08:00		0000-00-00	0		0000-00-00	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.

Copyright © 2011 Dell | KACE. All rights reserved.

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.

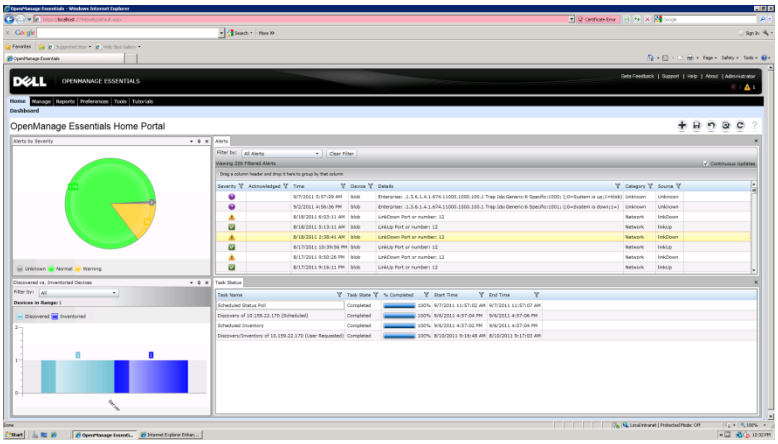


Figure 14: Monitoring and Filtering Alerts in OME

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.

Figure 15: Delivering Alerts to the K1000

When configuring the Alert Action in OME, 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

Copyright © 2011 Dell | KACE. All rights reserved.

- 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.

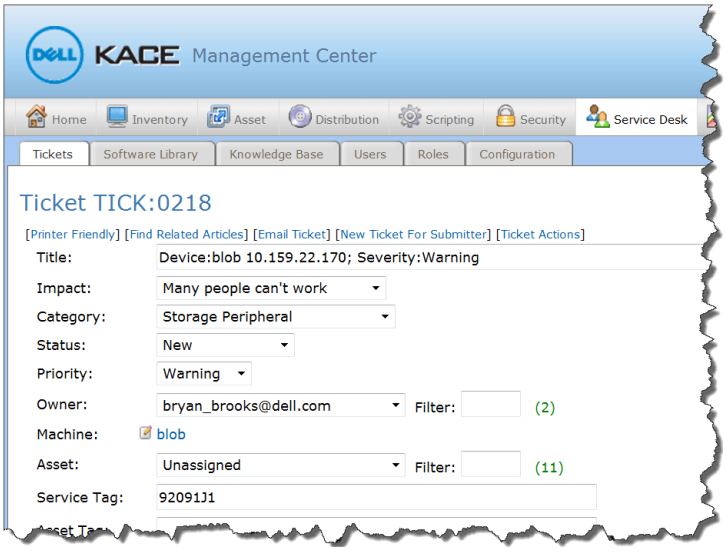


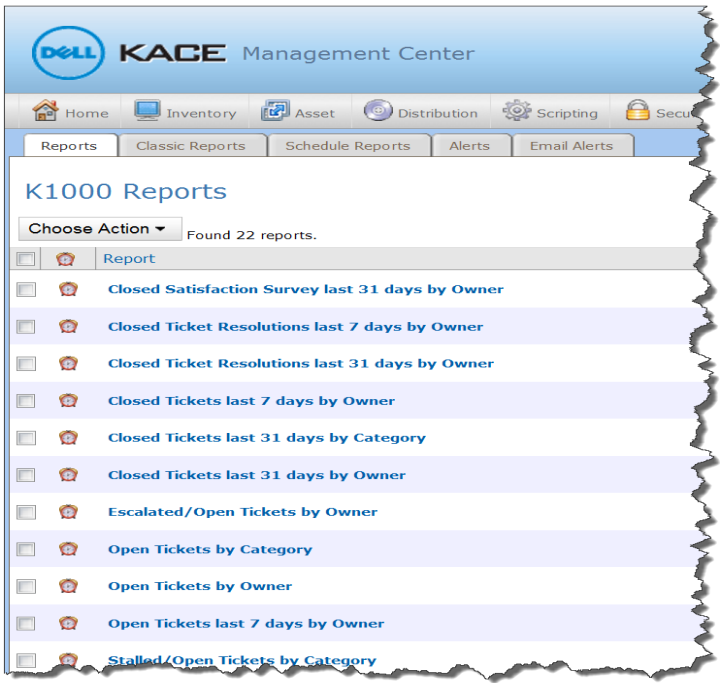
Figure 16: Ticket for an Alert in the K1000 Service Desk

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

Copyright © 2011 Dell | KACE. All rights reserved.

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.



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.

Figure 17: K1000 Service Desk Reports

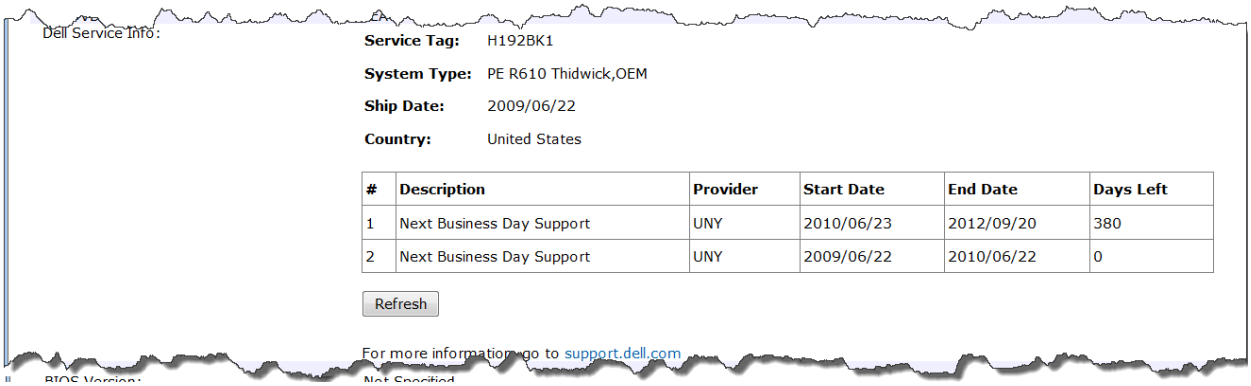


Figure 18: Dell Warranty Information in K1000 Inventory

Copyright © 2011 Dell | KACE. All rights reserved.

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.

Copyright © 2011 Dell | KACE. All rights reserved.

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 http://delltechcenter.com/ome

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.

Copyright © 2011 Dell | KACE. All rights reserved.