Managing and Monitoring Data Center Assets with Dell KACE and OpenManage Essentials

This Dell Technical White Paper addresses integration of Dell KACE K1000 appliance with OpenManage Essentials (OME) and how Dell KACE and OME can play an important role of managing and monitoring data center assets in a simple, cost-effective solution to bring fault resolution in a quick and proactive manner.

Dell | KACE

Bryan Brooks

Dell Open Manage Essentials

Rajaneesh Shresta

Sean Kim

November 2012| Version 1.0

Contents

Executive summary 3
Introduction 4
Inventorying and managing data center assets 6
Managing system updates 11
Assessing and resolving security vulnerabilities 12
Integrating Dell K1000 with OME 19
Configuring OME and K1000 19
Customizing service desk ticket related parameters 22
Sample workflow of OME/KACE integration 34
Conclusion 36
Additional resources 37

Executive summary

Customers already using Dell™|KACE™ K1000 Systems Management Appliance to manage their client environment (workstations, desktops, laptops etc.) can leverage OpenManage™ Essentials (OME), a free Dell application, to manage their server environment. Integrating KACE and OME allows customers to extend KACE service desk for server fault management without adding cost to their balance sheet.

As part of OME and KACE K1000 Service Desk integration, users need to:

- Configure e-mail alert action in OME that gets triggered when an alert is received (based on filters set, including Alert Severity, Alert Category, Device/Device group).
- Configure Service Desk in the KACE K1000 appliance to parse the e-mail received from OME and create a trouble ticket.
- Validate the configuration by sending a test e-mail from OME.

Introduction

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

This is especially true of managing change within a server environment. Servers are typically housed in secured, air conditioned environments and thus 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?

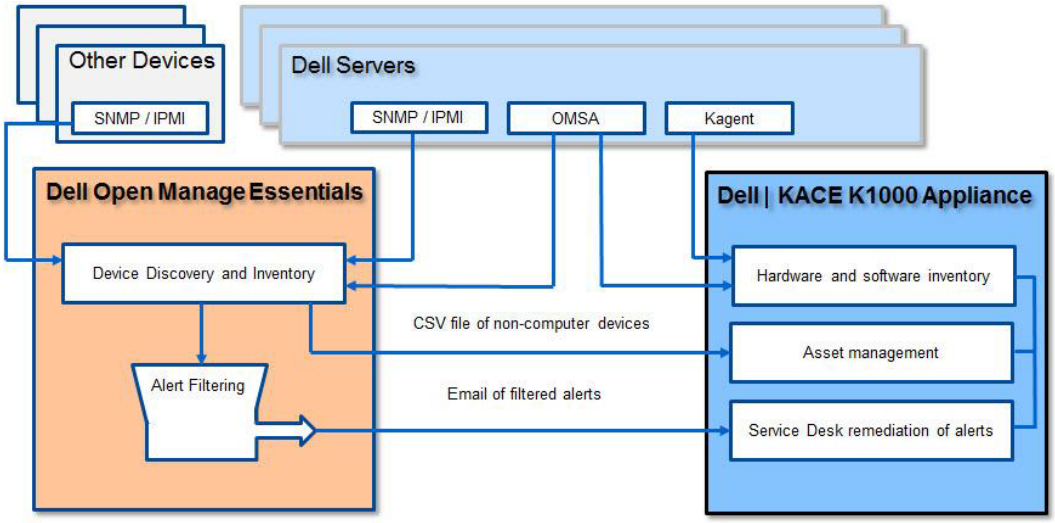
To answer these questions effectively, we need a comprehensive view of the systems under management and the necessary tools to assess and update these systems before issues arise. Of course, this needs to be accomplished with minimal impact on the IT budget. So the tools need to be easy to

acquire and easily adopted by 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 Essentials and Dell|KACE



- Inventorying and Managing Data Center Assets—Computer 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 essential as you work to protect your Dell computing investment. Both OME and the K1000 offer fully integrated Dell system update capabilities to provide you with 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.

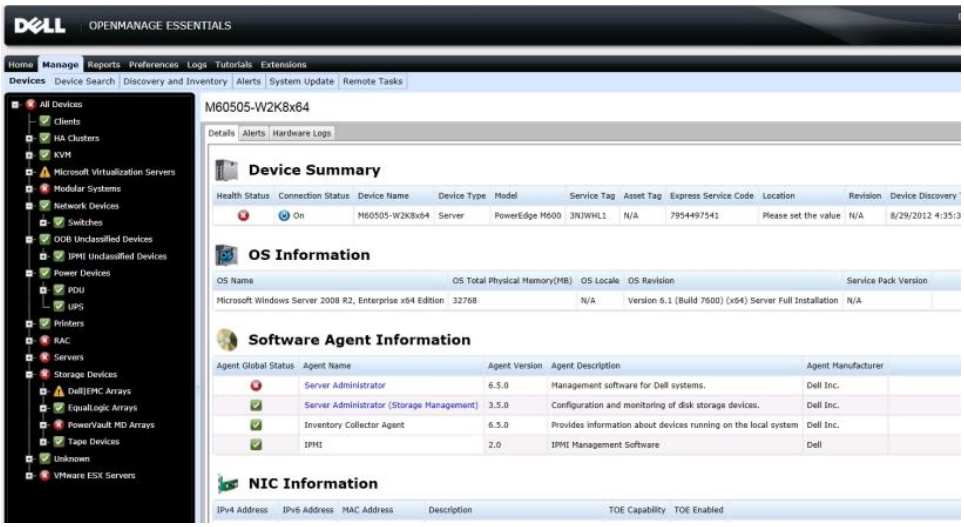
- System Monitoring and Fault Resolution—The Dell OpenManage Essentials toolset provides active system monitoring via SNMP and IPMI, and delivers issues that have been identified for remediation to the Dell|KACE service desk for ownership assignment and resolution.
- Reporting on Data Center Assets and Activities—Extensive reporting capabilities are provided to track progress and validate processes.

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 (OMSA) 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. OpenManage Essentials inventory



For the Dell|KACE K1000 Appliance, 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. Dell|KACE K1000 system inventory

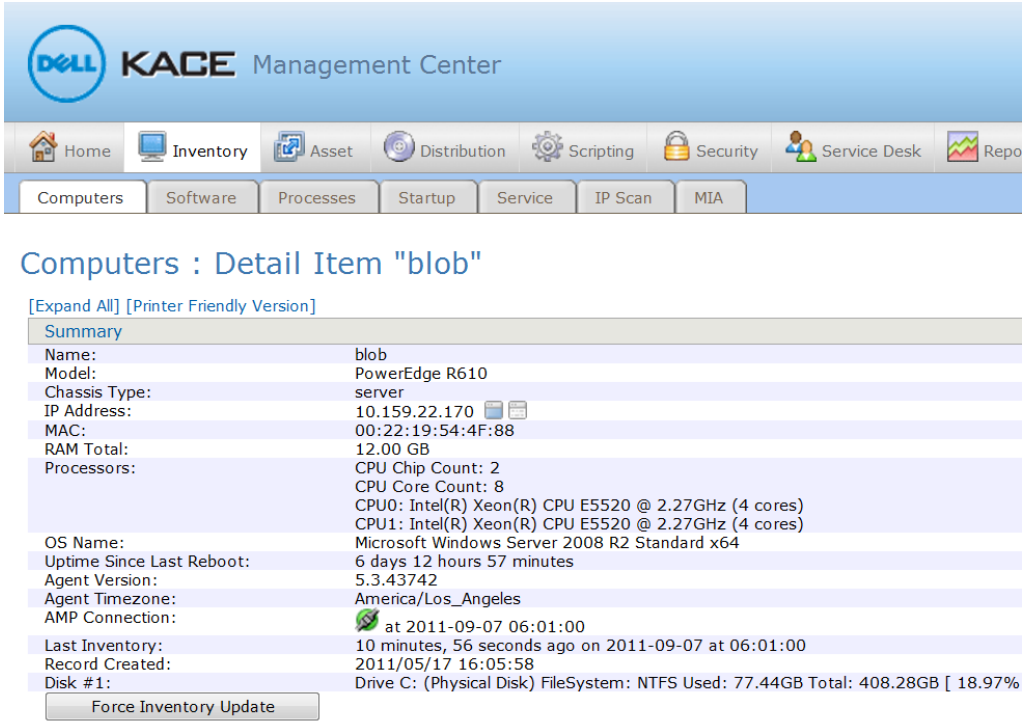
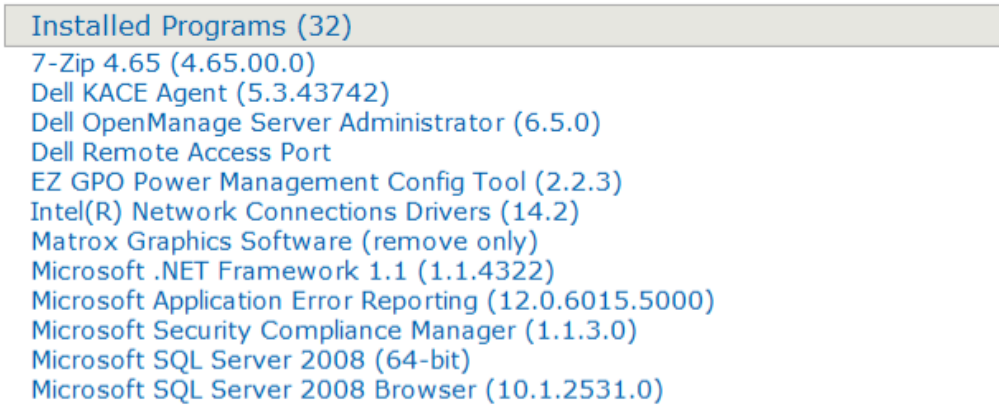


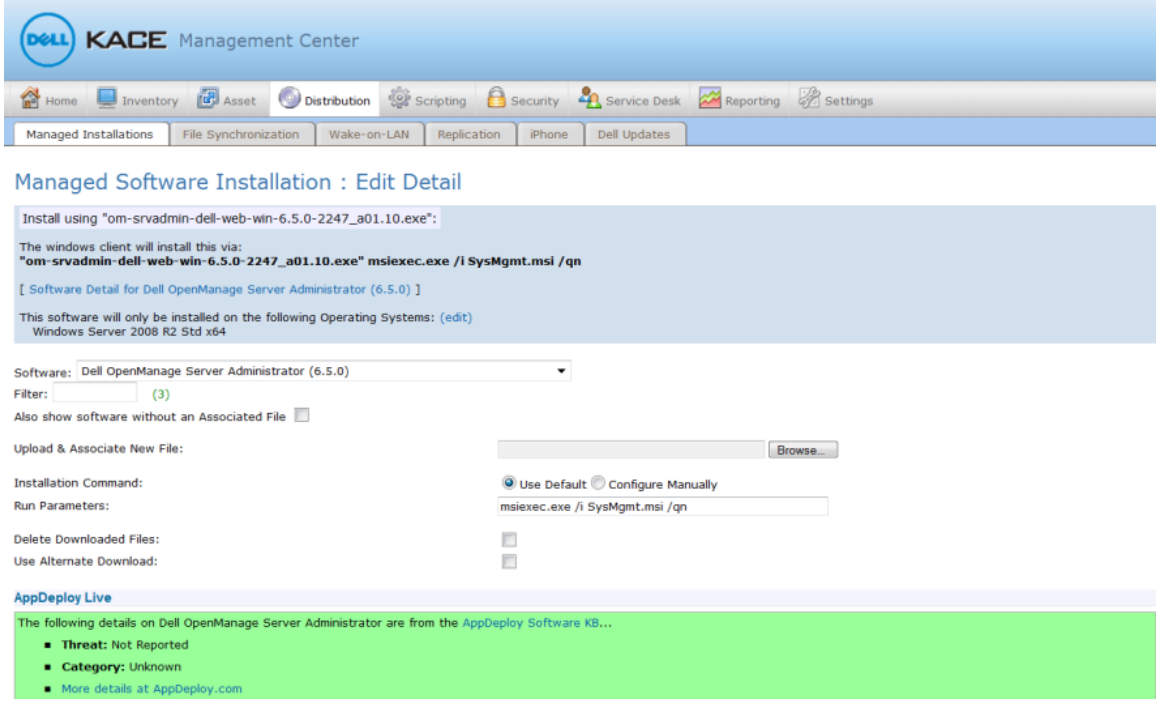
Figure 4. K1000 software inventory



The K1000 Appliance 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:

Figure 5. K1000 managed installations



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 6. Custom inventory with Dell CIM

Custom Inventory Rule:

```
ShellCommandTextReturn(WMIC /NAMESPACE:\\root\CIMV2\Dell PATH Dell_RemoteAccessServicePort GET /VALUE)
```

Custom Inventory Fields (3)

1) Dell Remote Access Port:

```
AccessInfo=10.159.19.56
AccessInfoIPv4=https://10.159.19.56:443
AccessInfoIPv6=
Caption=
CreationClassName=Dell_RemoteAccessServicePort
Description=
EnabledDefault=2
EnabledState=5
```

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 (DRAC), 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 is not 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.

Figure 7. Custom inventory with OMSA OMREPORT

Custom Inventory Rule:

```
ShellCommandTextReturn(omreport storage pdisk controller=0)
```

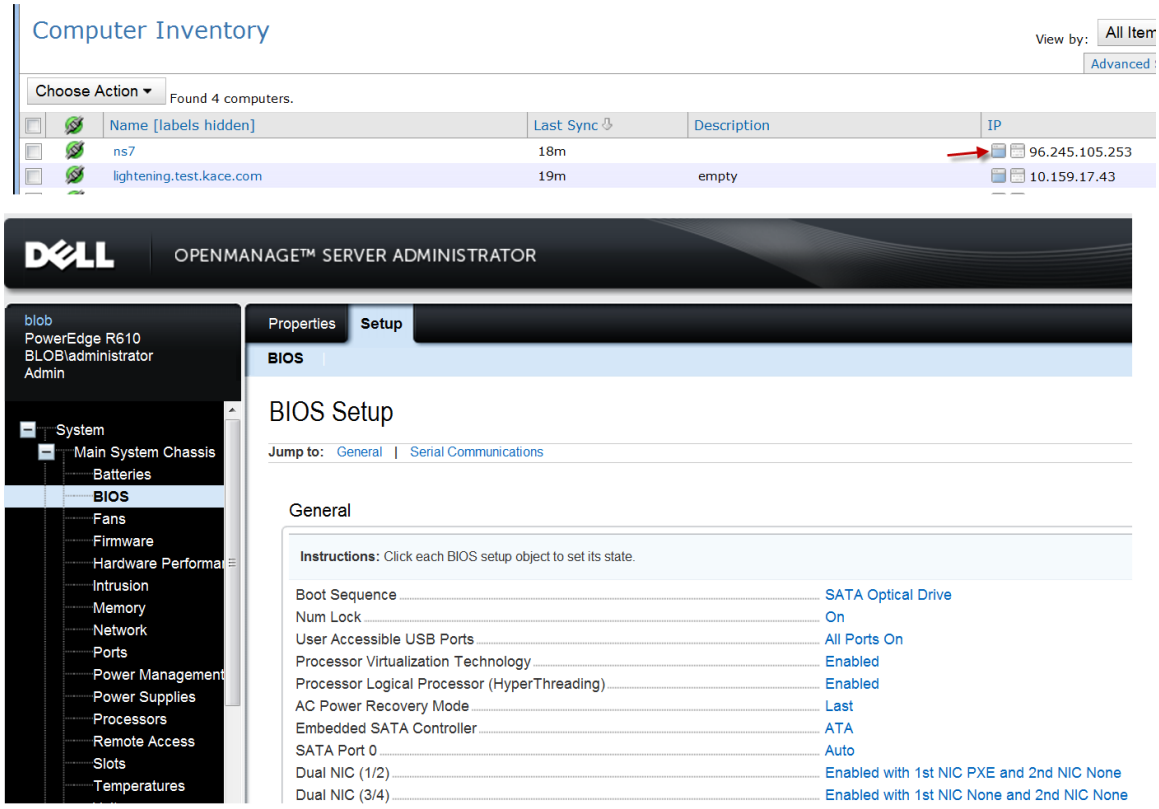
2) System Physical Disks:

```
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
```

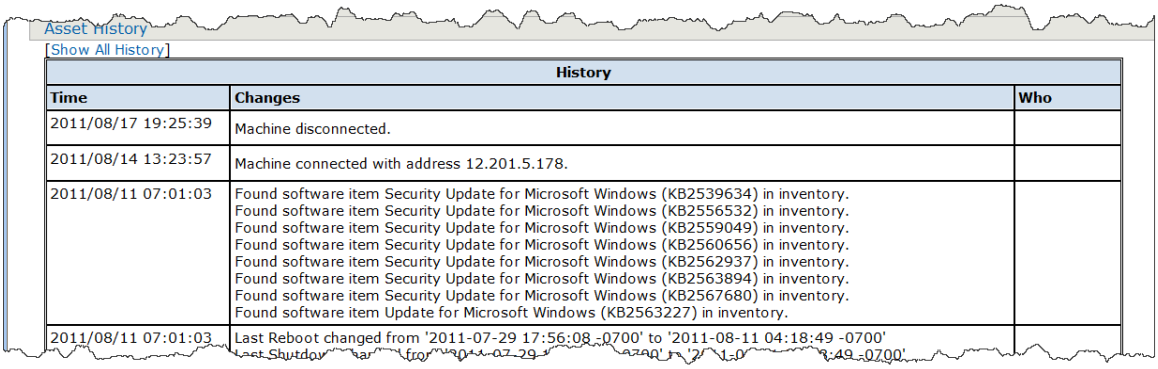
Actions may be enabled within the K1000 inventory that direct the administrator to the OMSA and DRAC web interfaces, conveniently placing remote control access to the server directly within the system management interface.

Figure 8. 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.

Figure 9. Tracking change history with the K1000 asset history



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'	

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>
```

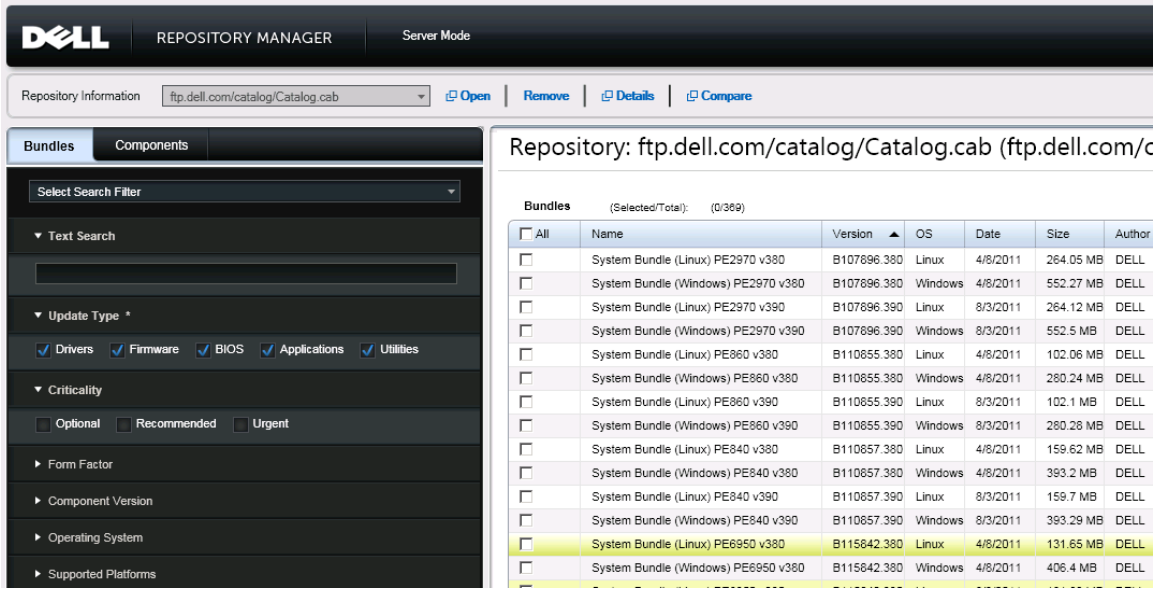
Detailed documentation for the OMCONFIG command set can be found in the OMSA manual. http://support.dell.com/support/edocs/software/svradmin

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.

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 10. 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

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.

Figure 11. K1000 Dell update comparison per machine

Dell Update Catalog Comparison Report

Comparison Report

Server Catalog

#	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

Assessing and resolving security vulnerabilities

Because the K1000 Appliance extends systems management to include the operating system and software applications, it is able 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 (OVAL) and the Security Content Automation Protocol (SCAP). Use of OVAL and SCAP ensures a reliable and reproducible set of metrics that are constantly updated as new threats are identified.

Figure 12. OVAL vulnerability assessment tests

KACE Management Center

User: Bryan Brooks Log Out
Organization: ITA
Global Search

Home | Inventory | Asset | Distribution | Scripting | Security | Service Desk | Reporting | Settings | Help

Patching | OVAL Assessment | SCAP Scan | Secure Browsers

OVAL Tests

View by: Vulnerability Search

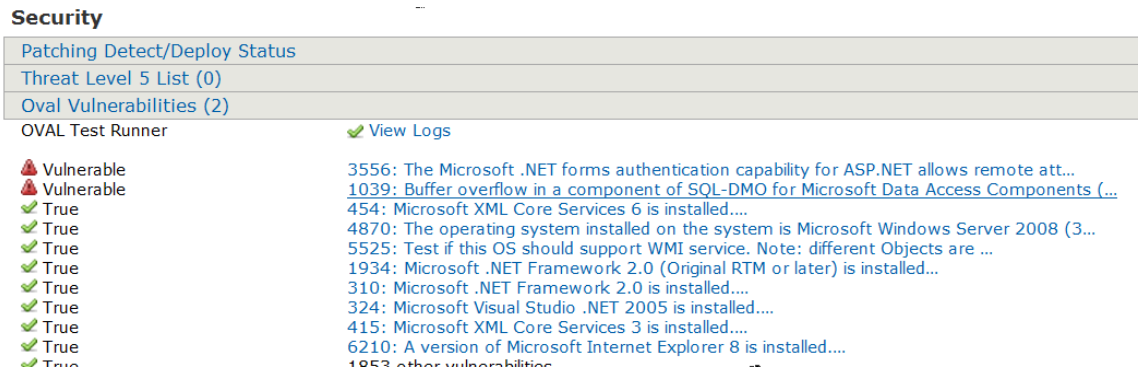
Choose Action Showing 1-150 of 2982 tests. [Next]

Last Updated: 2011/09/07 03:25:00am

OVALID	Description	CVE Number
3	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
4	Integer overflow in Microsoft Word 2000, 2002, 2003, 2004 for Mac, and v.X for Mac allows remote user-asssisted 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
5	Microsoft Internet Explorer 5 SP4 and 6 do not properly garbage collect when "multiple imports are used on a styleSheets collection" to construct a chain of Cascading Style Sheets (CSS), which allows remote attackers to execute arbitrary code via unspecified vectors.	CVE-2006-3451
8	Unspecified vulnerability in the Server service in Microsoft Windows 2000 SP4, Server 2003 SP1 and earlier, and XP SP2 and earlier allows remote attackers to execute arbitrary code via a crafted packet, aka "SMB Rename Vulnerability."	CVE-2006-4696
12	Internet Explorer 5.5 and 6.0 allows remote attackers to bypass restrictions for executing scripts via an object that processes asynchronous events after the initial security checks have been made.	CVE-2002-0026
13	Heap-based buffer overflow in HTML Help ActiveX control (hhctrl.ocx) in Microsoft Internet Explorer 6.0 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code by repeatedly setting the Image field of an Internet.HHCtrl.1 object to certain values, possibly related to improper escaping and long strings.	CVE-2006-3357
16	Buffer overflow in the chunked encoding transfer mechanism in Internet Information Server (IIS) 4.0 and 5.0 Active Server Pages allows attackers to cause a denial of service or execute arbitrary code.	CVE-2002-0079
17	Internet Explorer 5.01, 5.5 and 6.0 allows remote attackers to read arbitrary files via malformed requests to the GetObject function, which bypass some of GetObject's security checks.	CVE-2002-0023
18	Buffer overflow in Windows Shell (used as the Windows Desktop) allows local and possibly remote attackers to execute arbitrary code via a custom URL handler that has not been removed for an application that has been improperly uninstalled.	CVE-2002-0070
19	Cross-site scripting vulnerability in Internet Explorer 6.0 allows remote attackers to execute scripts in the Local Computer zone via a URL that exploits a local HTML	CVE-2002-0189

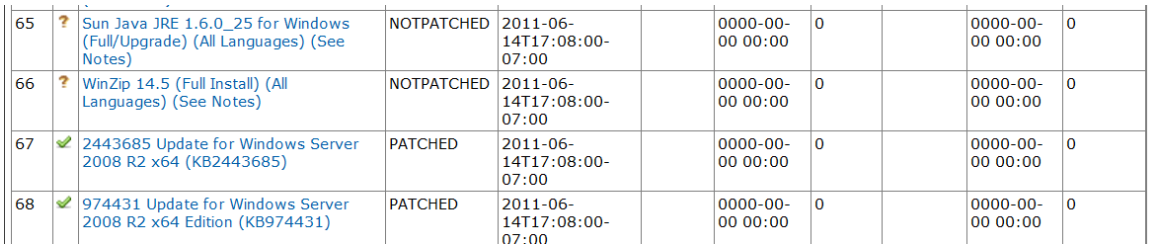
Assessments may be applied across multiple machines using the same dynamic grouping mechanism available to all features of the K1000, allowing scanning schedules to account more frequently for those systems that are of highest concern. When vulnerabilities are identified, patching and system configuration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

Figure 13. 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.

Figure 14. Patching status for a machine in inventory



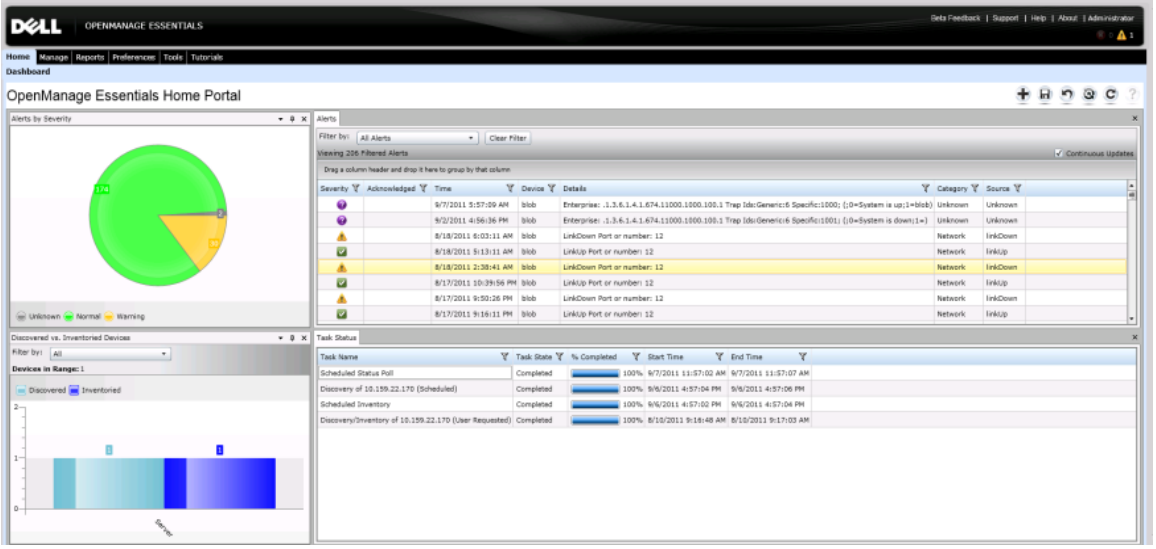
65	?	Sun Java JRE 1.6.0_25 for Windows (Full/Upgrade) (All Languages) (See Notes)	NOTPATCHED	2011-06-14T17:08:00-07:00		0000-00-00 00:00	0		0000-00-00 00:00	0
66	?	WinZip 14.5 (Full Install) (All Languages) (See Notes)	NOTPATCHED	2011-06-14T17:08:00-07:00		0000-00-00 00:00	0		0000-00-00 00:00	0
67	✓	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	✓	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

The 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 proof that system weaknesses have been addressed via the compliance reports.

System monitoring and fault resolution

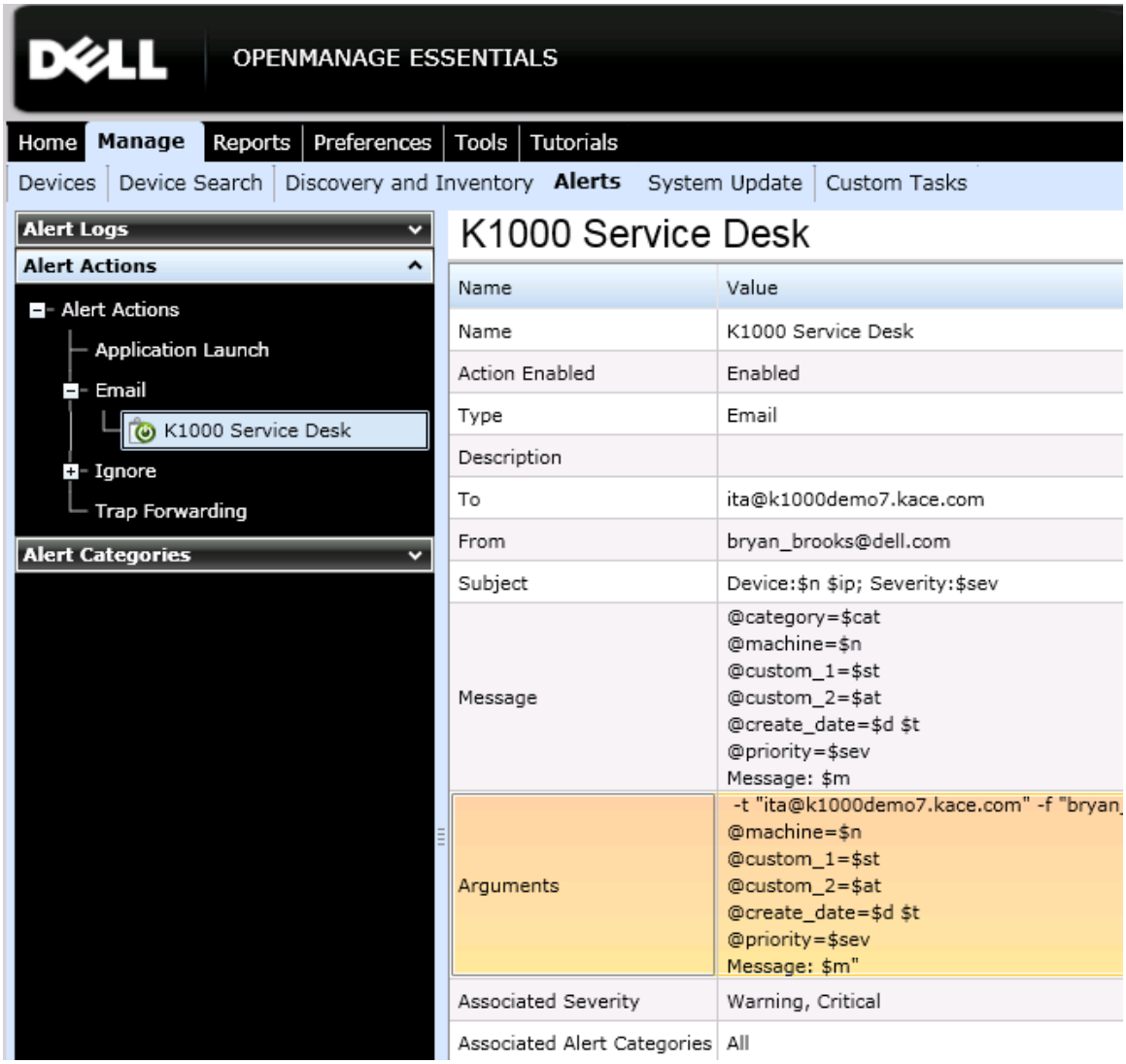
Possibly the most important task to be automated is proactive identification of faults within the systems being monitored, and tracking of the fault remediation to its conclusion. OME provides active monitoring of Dell and non-Dell computer systems and other devices via industry-standard SNMP and IPMI 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 15. 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 16. Delivering alerts to the K1000 appliance



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 ($st)—The Dell Service Tag assigned to the device.
- Asset Tag ($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 a @ 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:

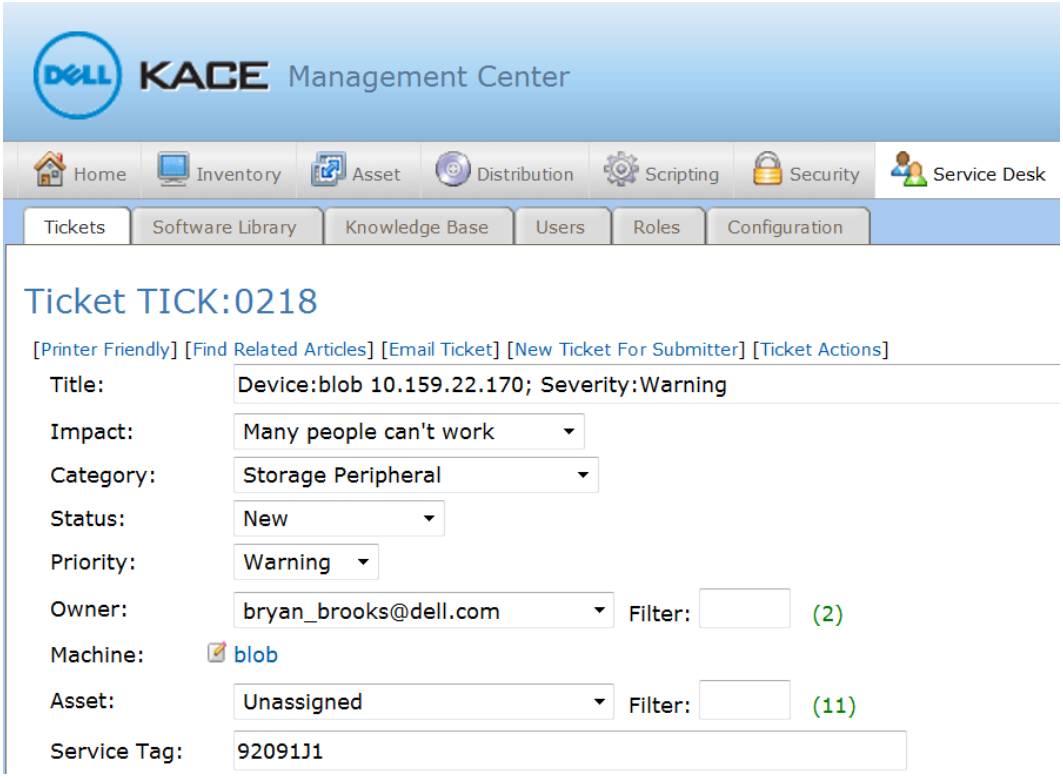
- `@custom_n=$at (where „n" is the custom field in the ticket being used for asset tag)`

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 17. 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.

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 18. K1000 service desk reports

Figure 19. Dell warranty information in K1000 inventory

Service Tag: H192BK1

System Type: PE R610 Thidwick,OEM

Ship Date: 2009/06/22

Country: United States

#	Description	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

Refresh

Integrating Dell K1000 with OME

The features of the Dell|KACE K1000 Systems Management Appliance are exceptionally well suited to manage a distributed desktop environment. But what about managing the servers in your environment? Obviously, most of the K1000 features such as automated inventory and machine labeling, server operating system patching, Dell driver and firmware updates for servers, OVAL and SCAP vulnerability assessment, scripted configuration management, and reporting also work well for managing servers. A key feature that's often a requirement for server management that you may also need is active system monitoring based on protocols like SNMP or IPMI. While the K1000 can perform SNMP scans to assist in device discovery, it doesn't receive SNMP traps to assist in identifying issues with those servers.

In any IT environment, 24/7 accessibility to the data center is essential in order to proactively monitor system health, identify faults, and automatically notify IT administrators for immediate resolution of these faults. Dell OpenManage Essentials (OME) allows IT organizations to actively monitor Dell servers, non-Dell Servers[1], and other devices via industry standard SNMP and IPMI protocols. By configuring devices to send SNMP traps/alerts and IPMI Platform Event Traps (PET) to an OME management station, OME acts as a centralized monitoring application.

Many IT organizations have implemented a centralized mechanism for tracking and handling these server faults such as hard drive failure, loss of network connection etc. These server faults are typically managed through a service desk or a help desk. KACE 1000 Service Desk can receive alerts information from OME, then open a trouble ticket and assign it to an IT administrator for remediation. 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.

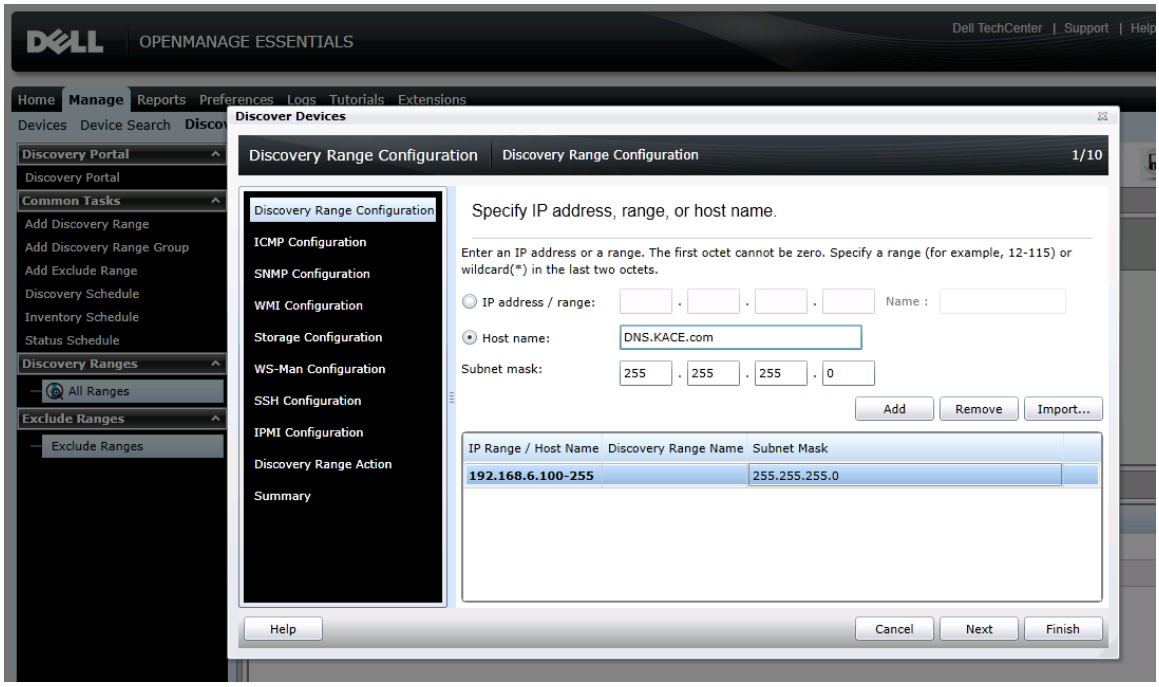
Configuring OME and K1000

Dell OpenManage Essentials is a Windows-based systems management console that replaces Dell IT Assistant. A physical or virtual server running Windows Server 2008 will be required to run OME. This installation is quite simple and largely self-contained. OME includes Microsoft SQL Server® Express for small deployments. If you plan to manage a large environment, however, OME supports use of Microsoft SQL Server Enterprise.

1. Install OME
2. Launch the OME console and select **Manage → Discovery and Inventory.**
3. In the left pane, select **Discovery Ranges → Add Discovery Ranges** to define an IP range for discovering your servers.
4. Enter the **IP address / range** or a list of **DNS hostnames** for the machines you want to monitor, and select an applicable protocol, provide credentials then click **Finish**.

[1] Supported only if the corresponding MIB is imported into OME.

Figure 20. OpenManage Essentials discovery range configuration wizard



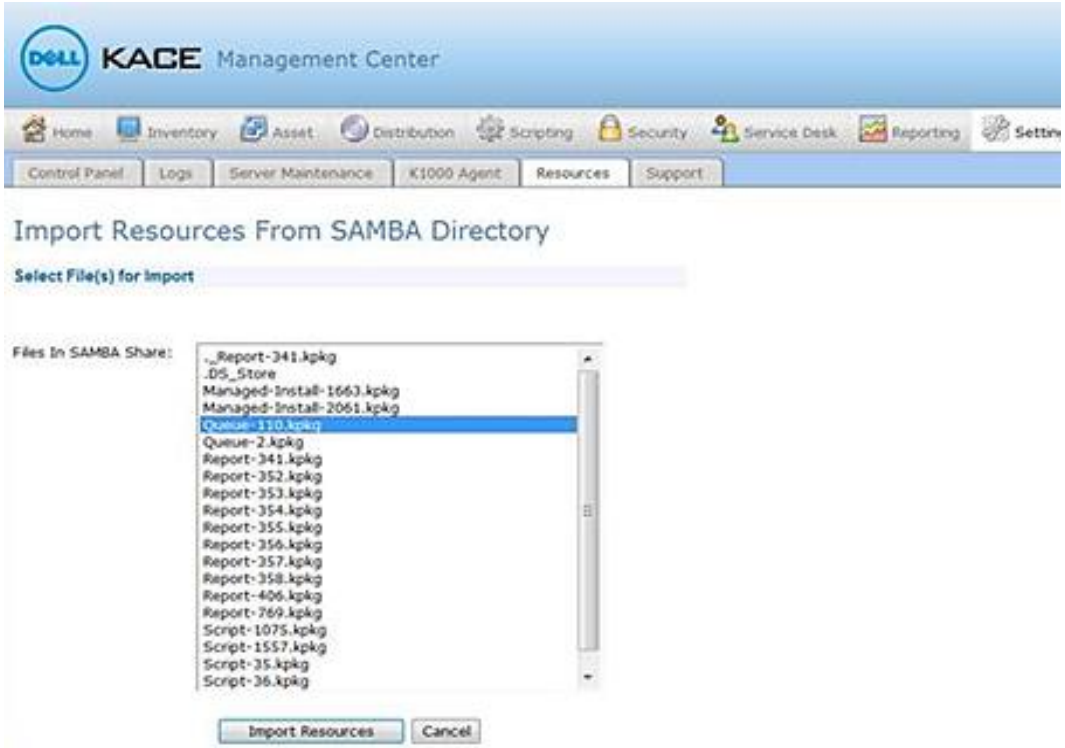
Configure service desk and service queue in KACE

The next step is to create your K1000 service desk queue so it can receive emails from OME. We'll set this up before configuring the email alert in OME since we need the email address for the service desk queue to complete the OME configuration. To simplify this task you can download a sample queue as a kpkg here[2] and upload it to your K1000 Appliance as follows:

1. Connect to the clientdrop network share on your K1000 and navigate to **\\<your_K1000_host>\clientdrop** and log into the share using the credentials configured in the K1000 Appliance for the network share.
2. Copy the downloaded **Queue-110.kpkg** file to the clientdrop share.
3. Log into your K1000 Appliance and go **to Settings → Resources → Import K1000 Resources**.
4. From the dropdown field on the left, select **Choose Action → Import Resources(s)** from SAMBA Share.

[2] If the sample queue package becomes unavailable for download, Google search for *Queue-110.kpkg*.

Figure 21. Import resources from SAMBA share directory

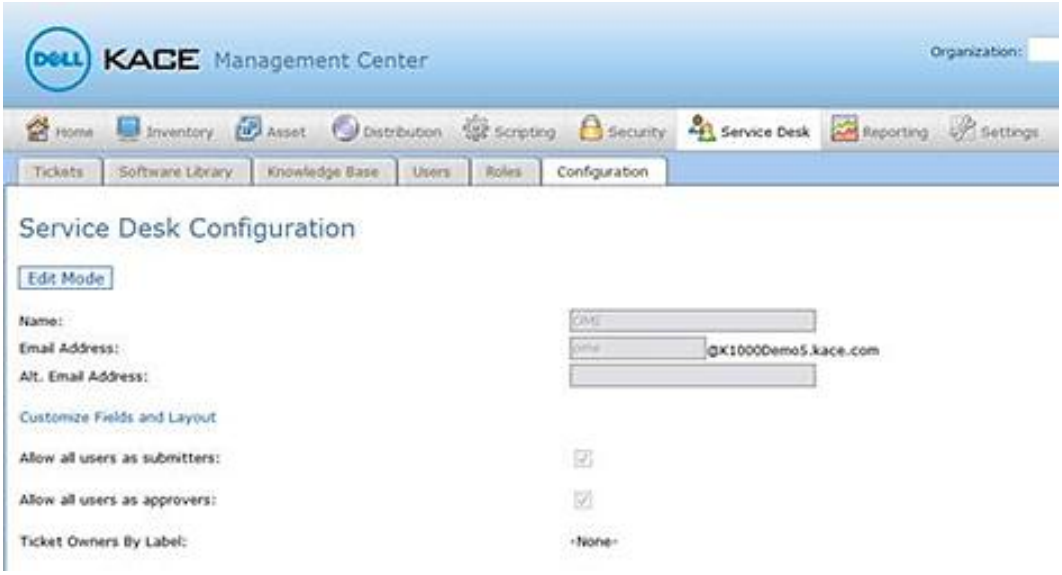


1. Select **Queue-110.kpkg** from the list of files, and then select **Import Resources**.

   You'll now see a queue resource listed called OME that is imported into your K1000 Appliance.

2. Navigate to **Service Desk → Configuration → Queues**. Click on the OME queue.

Figure 22. Service desk configuration



Note the email address of the queue. This is the email address that will be recognized within the K1000 Appliance as the queue to receive email tickets from OME. If you wish to use a different email address that is first externally defined in your email environment and then forwarded to this address, you may specify that in the **Alt. Email Address** field. Here, though, we'll assume that the queues **Email Address** is being used. When you configure the email alert in OME, this email address will be the **TO:** address in the OME Email alert action.

Also note that there is no specification for **Ticket Owners by Label**. This is simply because user labels and the assigned users will be specific to your environment and cannot be assumed for the imported queue. Everything within the imported queue may be customized to meet your requirements.

From the Ticket Layout section of the Service Desk Customization page you can customize the way tickets are displayed in the Tickets tab for each queue. For example, you

- can create different ticket views and set read/write access for users, ticket owners, and administrators.
- Refer to KACE K1000 Service Desk Administrator Guide for more information on customizing service desk tickets.

Customizing service desk ticket related parameters

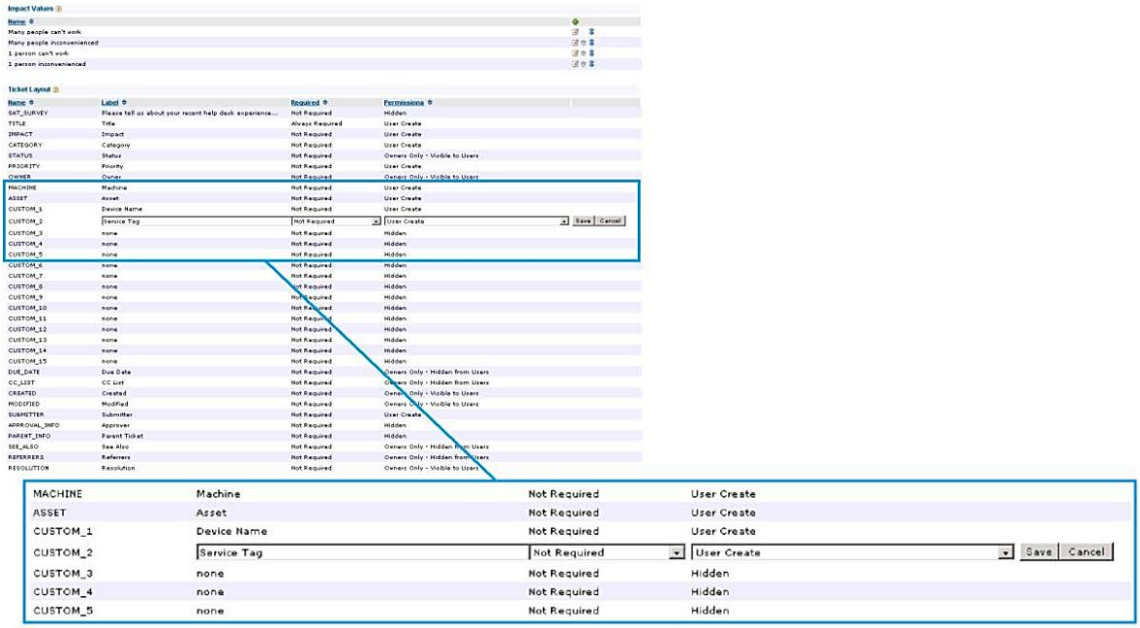
1. Select **Service Desk** → **Configuration** → **Queues** → <***Queue name***> → **Customize Fields and Layout** link.
2. Select the **Name** you want to customize and set the label and permissions from the dropdown list.

   Example:
   Name: CUSTOM_2
   Label: Service Tag
   Required: Not Required
   Permissions: User Create

3. You can also define the **Name type**, assign default value to a **Name**, and etc. under the **Custom Fields** section.

   Example:
   Name: CUSTOM_2
   Type: Text
   Default: Unknown

Figure 23. Define custom fields and parameters on the service desk configuration page



You can configure a new Alert Category in K1000 to match alert categories supported by OME. *Alert category* identifies the type of device, component, or application that generated the alert. For example, temperature-related alerts will be under the Environmental alert category.

- To configure the Alert Category, select **Service Desk → Configuration → Queues →** *<Queue name>* **→ Ticket.** Defaults: **Customize These Values** link.
- To add a new alert category, select the + icon on the top right under the **Category Values** section, then provide the **Name** and **Label** properties, and set the **Default Owner**, **User Settable** properties.

  Example:
  Name: Environmental
  Label: Environmental
  Default Owner: OMEAdmin
  User Settable: True

Create an e-mail alert action in OME

1. Launch the OME console and select Manage → Alerts then in the left pane, select Alert Actions → Email
2. Right-click on Email and select New Email Alert Action OR right-click a pre-canned sample alert action and select Clone then provide a new name and select Edit from the right-click menu of the cloned alert action.

Figure 24. Launching an e-mail alert action wizard

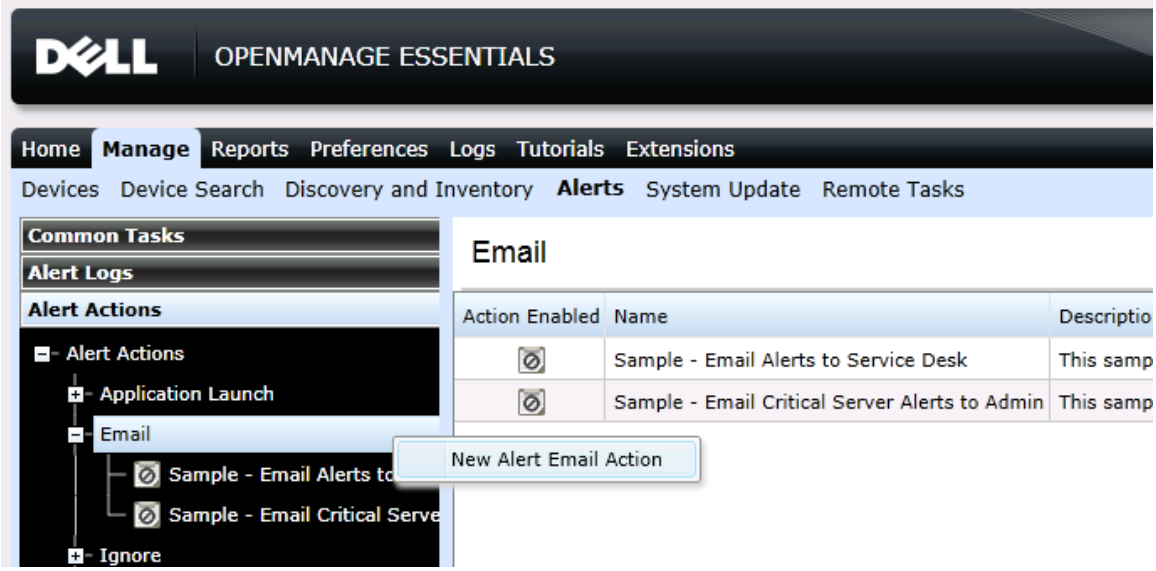


Figure 25. Clone a pre-canned sample e-mail alert action

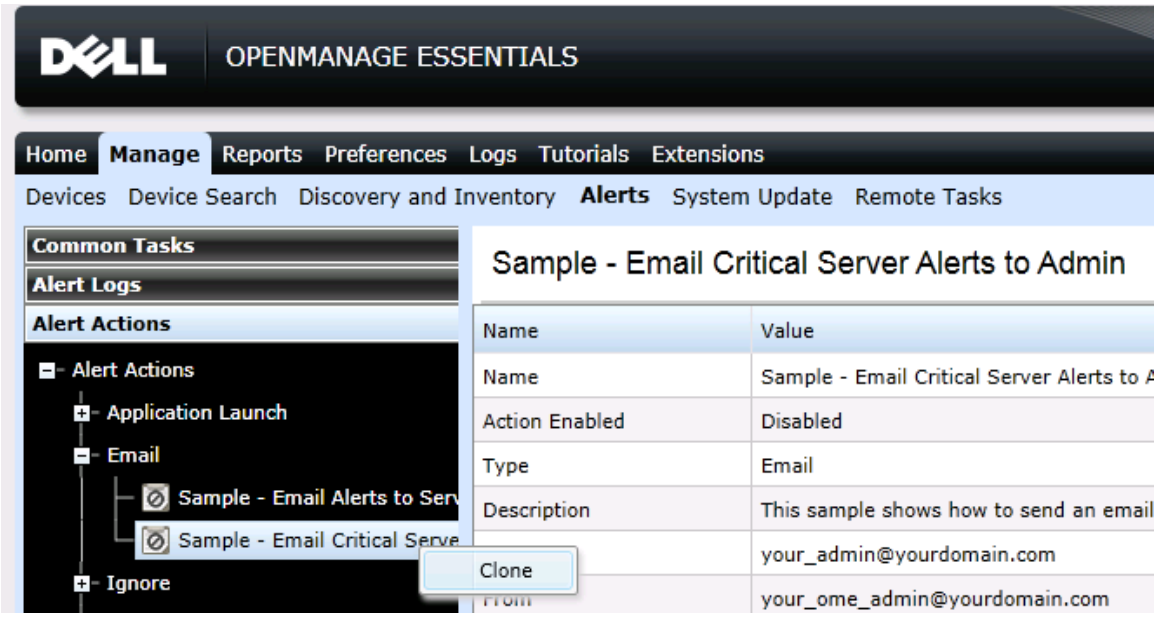
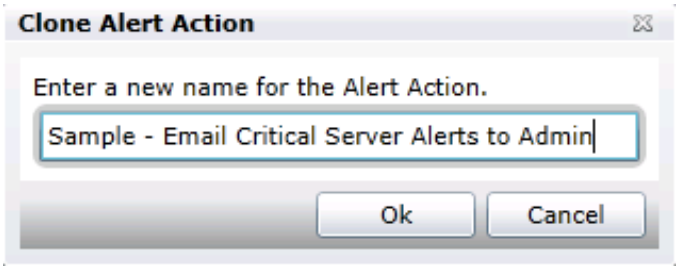
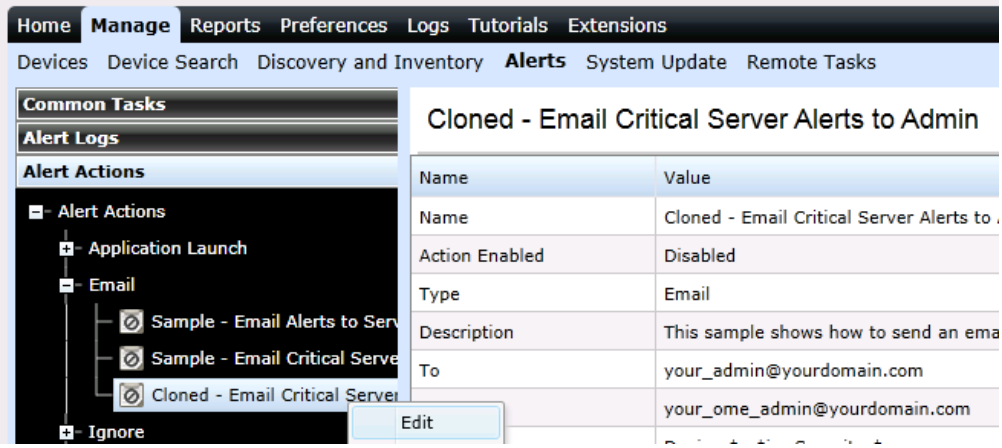


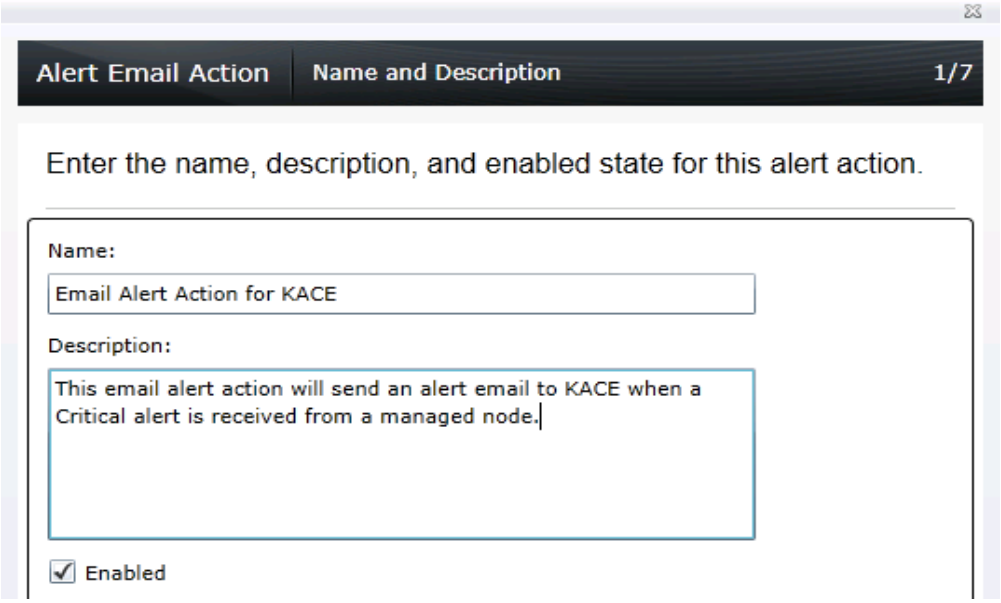
Figure 26. Enter and edit a new name for the cloned e-mail alert action





3. In **Name and Description**, provide e-mail alert action name and description.
4. Check **Enabled** checkbox and Click **Next**.

Figure 27. Name and description in e-mail alert action wizard



5. In the e-mail configuration screen, provide the recipients of this e-mail and sender in To: and **From:** address fields.

   NOTE: Make sure the **To** e-mail address in OME matches the e-mail address in KACE Service Desk configuration.

   NOTE: Verify that the e-mail address in the **From** field in OME (user sending the ticket into the K1000 service queue) matches exactly the e-mail address defined for that user in the KACE appliance.

   NOTE: Separate each recipient or distribution list with a semi-colon.

6. Provide a **Subject**.
7. In the **Message** field, create a map of the KACE service desk and OME pre-defined alert substitution parameters. For each of the supported parameters the e-mail alert action fetches alert data and assigns it to the corresponding parameters on the KACE service desk trouble ticket.
8. Refer to the KACE K1000 Service Desk Administrator Guide for more information on customizing service desk tickets.

   Example:

   ```
   @machine=$n

   @custom_1=$st

   @create_date=$d $t

   @priority=$sev

   @category=$cn
   ```

   NOTE: Parameters prefixed with "@" are defined in the KACE service desk.

   NOTE: Parameters prefixed with "@" must be defined first in the message section of the Alert Email Action wizard and each parameter has to be in a new line.

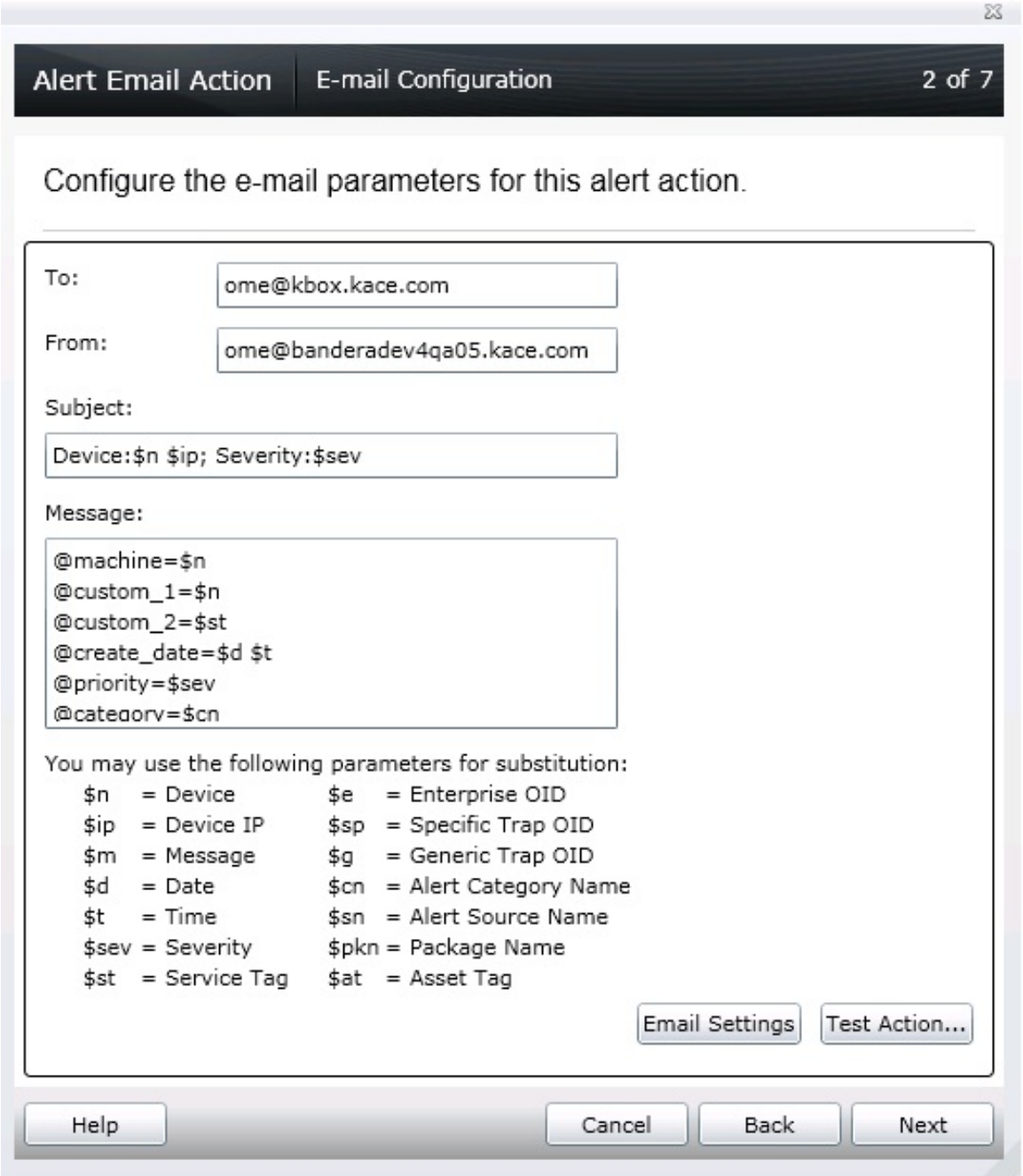
   NOTE: Parameters prefixed with "$" are defined in OME and are substituted with actual value when E-mail alert action is triggered.

9. Click **Email Settings** and provide an SMTP server name or IP Address.

   NOTE: Make sure KBOX and OME are using the same SMTP server name/address.

10. Validate the configuration using the **Test Action** button. This should send a sample e-mail to the all the recipients. Click **Next**.

Figure 28. E-mail configuration in e-mail alert action wizard



Note: The address in the **To:** field will be the e-mail address of the service queue in the K1000 Appliance where the service desk tickets will be logged.

Figure 29. Email settings

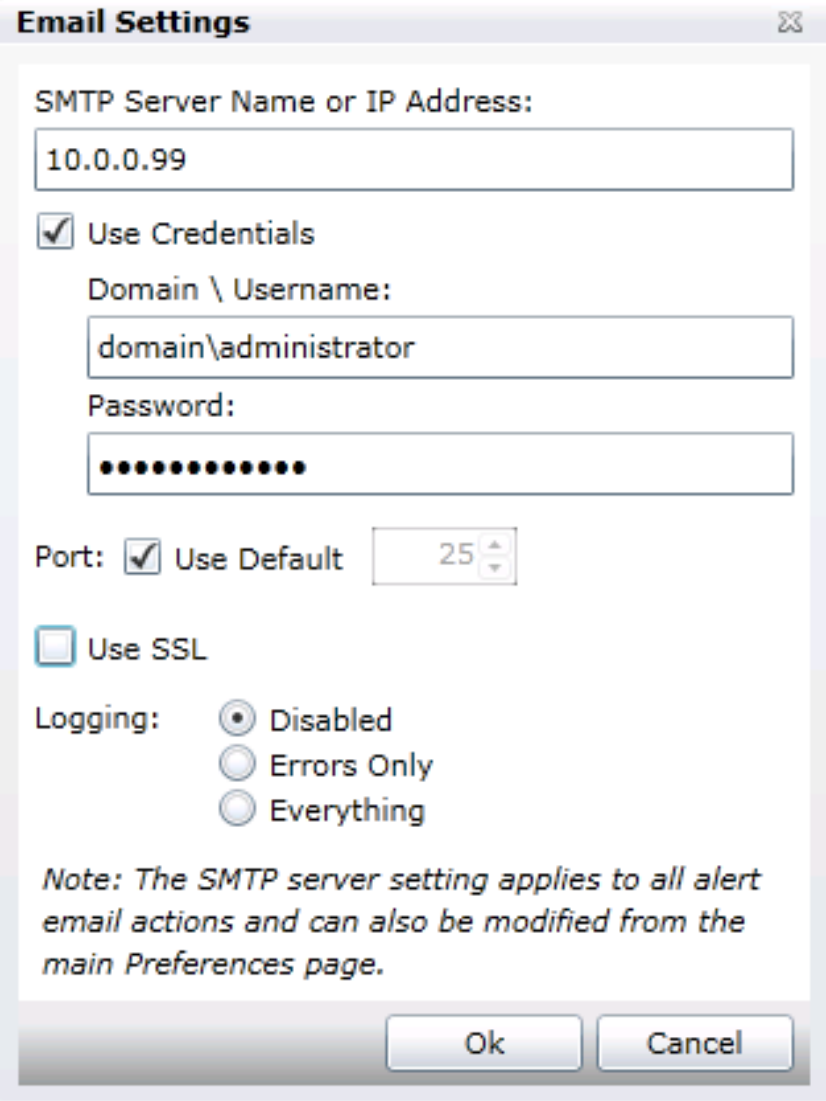
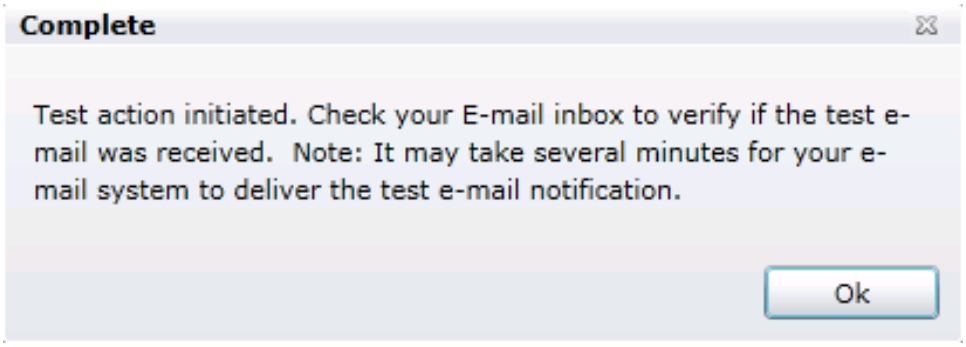
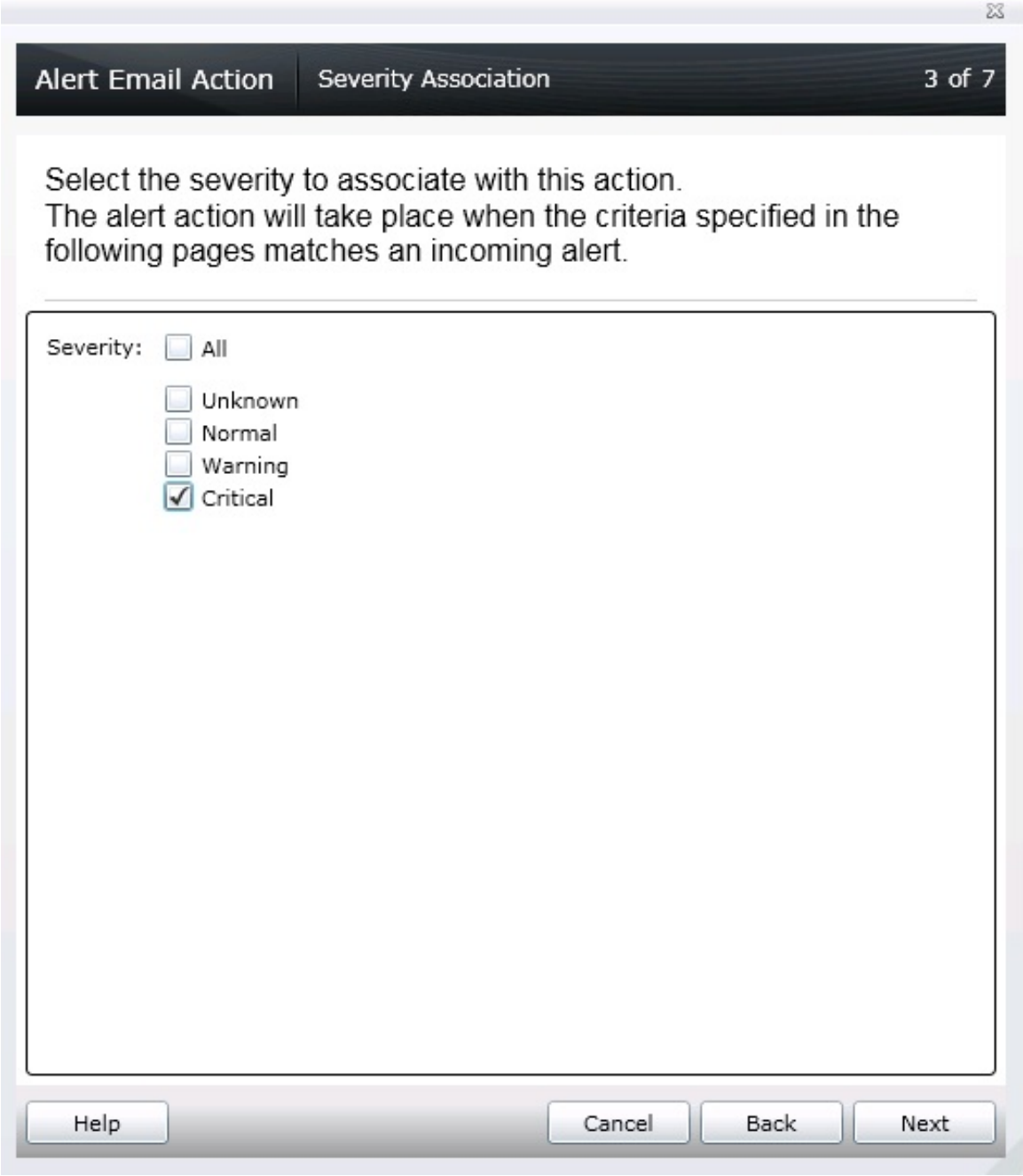


Figure 30. Test email confirmation dialog box



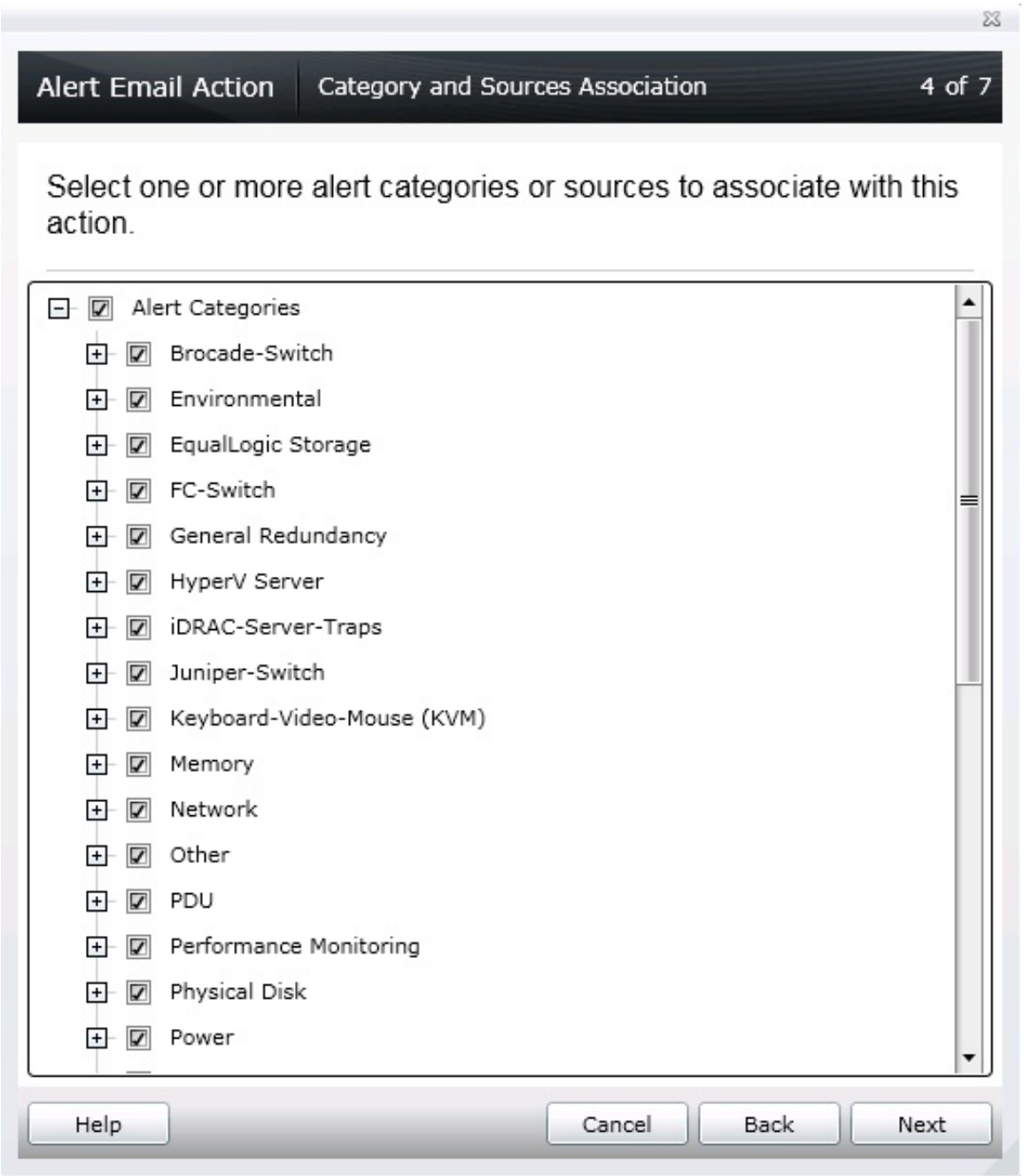
11. In **Severity Association**, assign the alert severity to which you want to associate this e-mail alert and then click **Next**.

Figure 31. Select sevierty association in e-mail alert action wizard



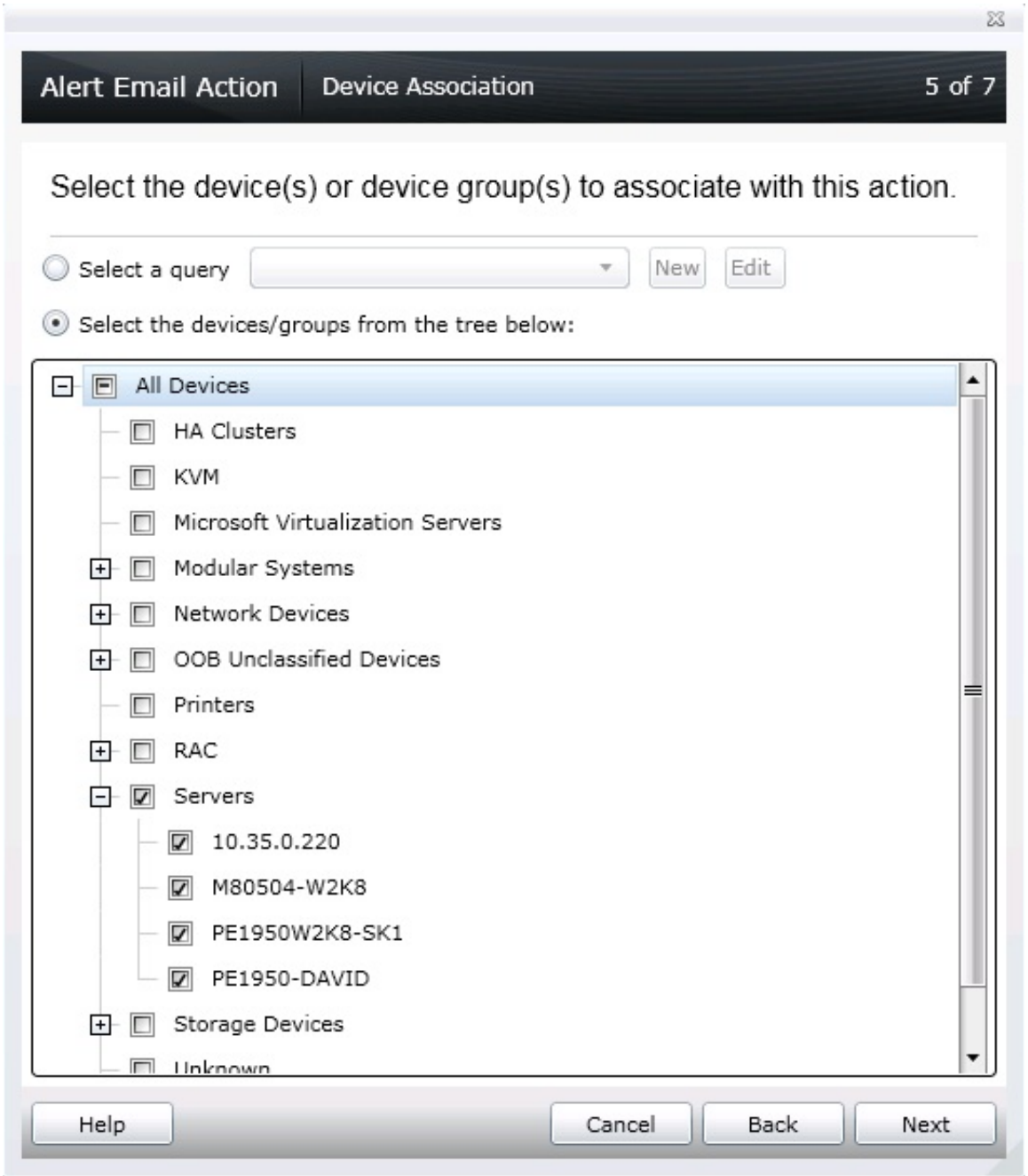
12. In **Categories and Sources Association**, assign the alert categories source to which you want to associate this e-mail alert and then click **Next**.

Figure 32. Select alert categories in e-mail alert action wizard



13. In **Device Association**, assign the device or device groups to which you want to associate this e-mail alert and then click **Next**.

Figure 33. Select devices in e-mail alert action wizard



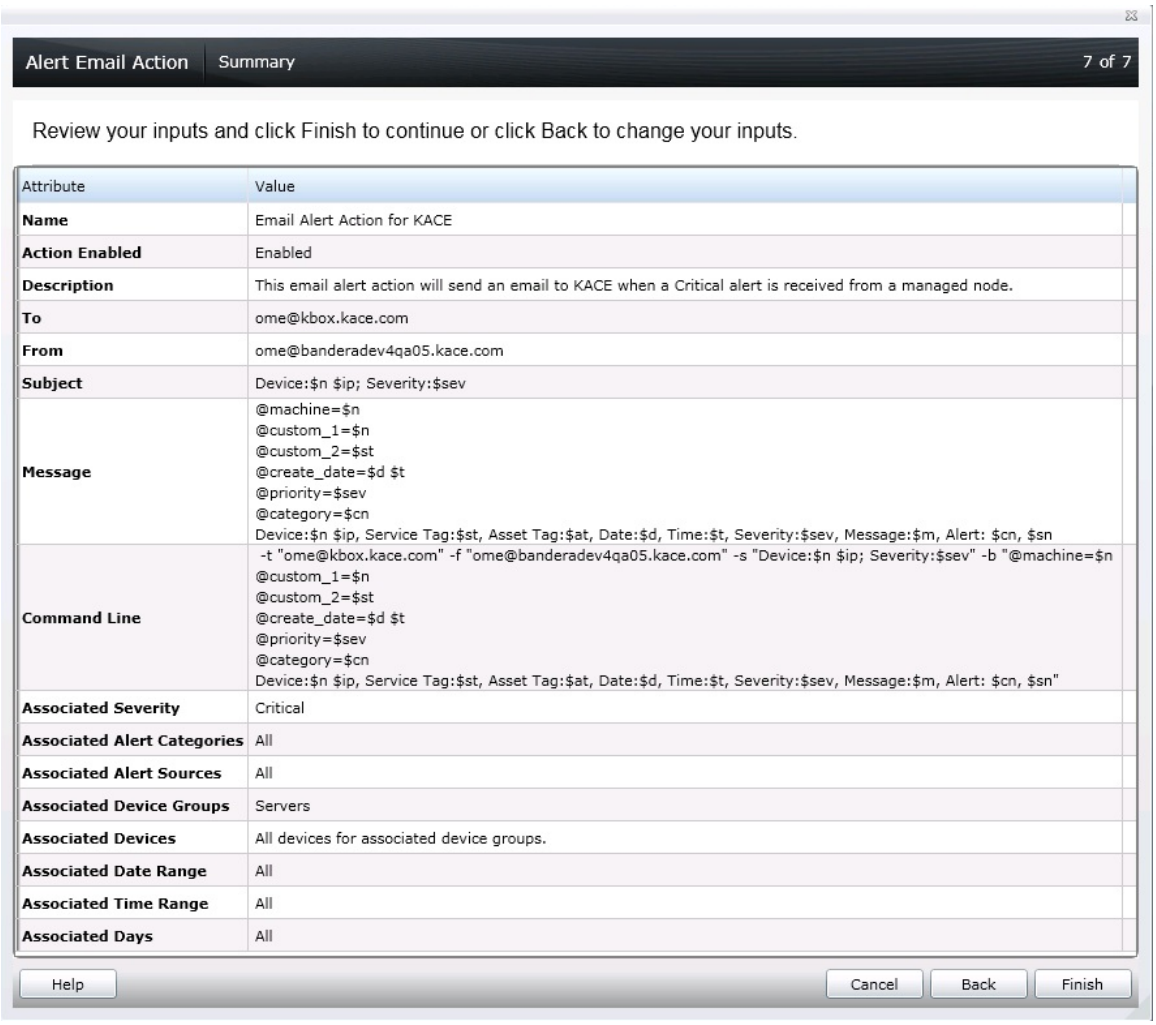
14. In **Date Time Association**, enter the date or time range on when this e-mail alert action is active, and then click **Next.**

    By default, the e-mail alert action created is active at all times.

Figure 34. Date time association in e-mail alert action wizard

15. In the **Summary** window, review inputs and click **Finish**.

Figure 35. Review configuration in e-mail alert action summary



Alert Email Action | Summary | 7 of 7

Review your inputs and click Finish to continue or click Back to change your inputs.

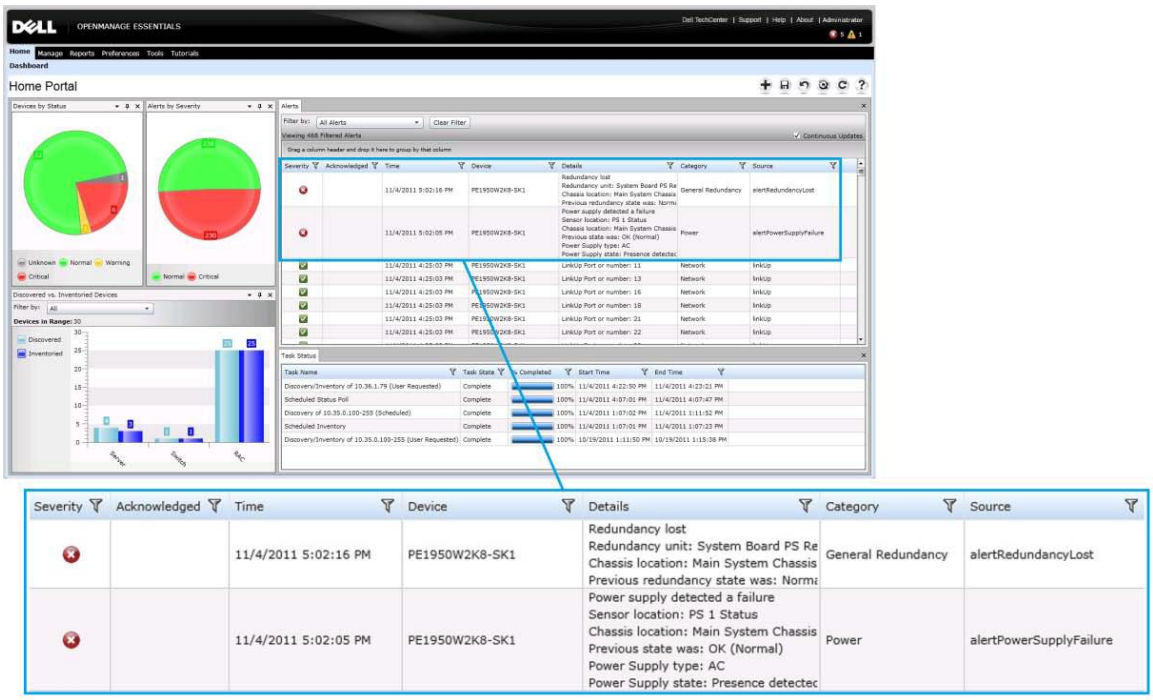
Attribute	Value
Name	Email Alert Action for KACE
Action Enabled	Enabled
Description	This email alert action will send an email to KACE when a Critical alert is received from a managed node.
To	ome@kbox.kace.com
From	ome@banderadev4qa05.kace.com
Subject	Device:$n $ip; Severity:$sev
Message	@machine=$n @custom_1=$n @custom_2=$st @create_date=$d $t @priority=$sev @category=$cn Device:$n $ip, Service Tag:$st, Asset Tag:$at, Date:$d, Time:$t, Severity:$sev, Message:$m, Alert: $cn, $sn
Command Line	-t "ome@kbox.kace.com" -f "ome@banderadev4qa05.kace.com" -s "Device:$n $ip; Severity:$sev" -b "@machine=$n @custom_1=$n @custom_2=$st @create_date=$d $t @priority=$sev @category=$cn Device:$n $ip, Service Tag:$st, Asset Tag:$at, Date:$d, Time:$t, Severity:$sev, Message:$m, Alert: $cn, $sn"
Associated Severity	Critical
Associated Alert Categories	All
Associated Alert Sources	All
Associated Device Groups	Servers
Associated Devices	All devices for associated device groups.
Associated Date Range	All
Associated Time Range	All
Associated Days	All

Help | Cancel | Back | Finish

Sample workflow of OME/KACE integration

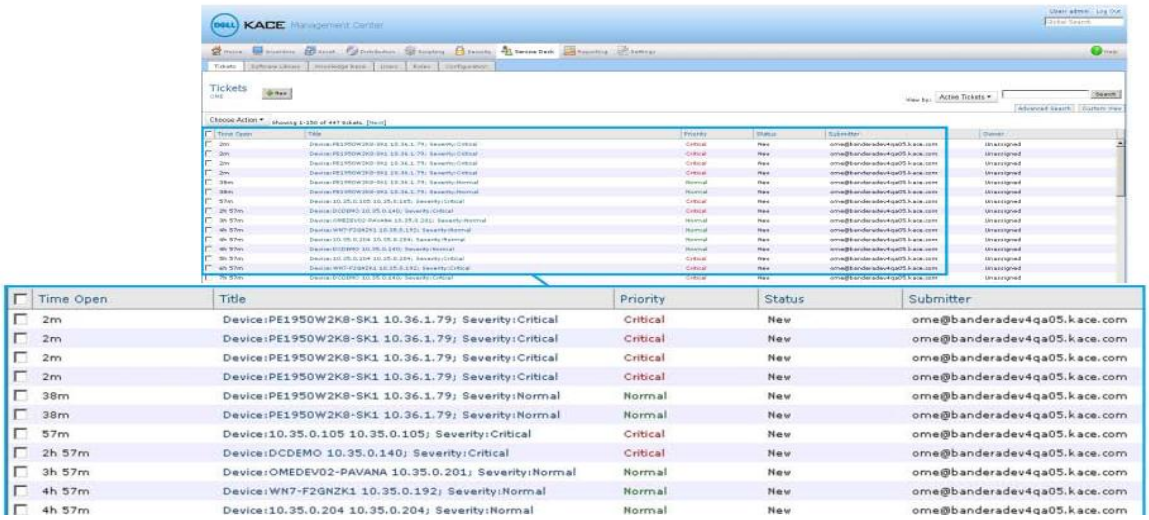
1. OME receives a critical alert from a monitored server and triggers the E-mail alert action, which in turn collects alert data and sends an e-mail to KACE service desk.

Figure 36. Alerts received in OME Home Portal dashboard



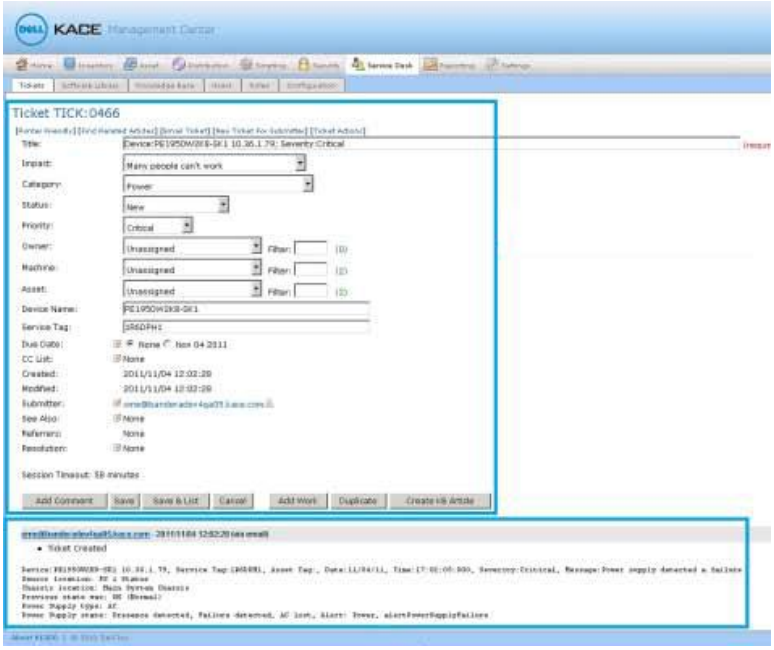
2. The E-mail received is parsed by KACE Service Desk. It then creates a Service Desk ticket under OME service queue based on the criteria set.

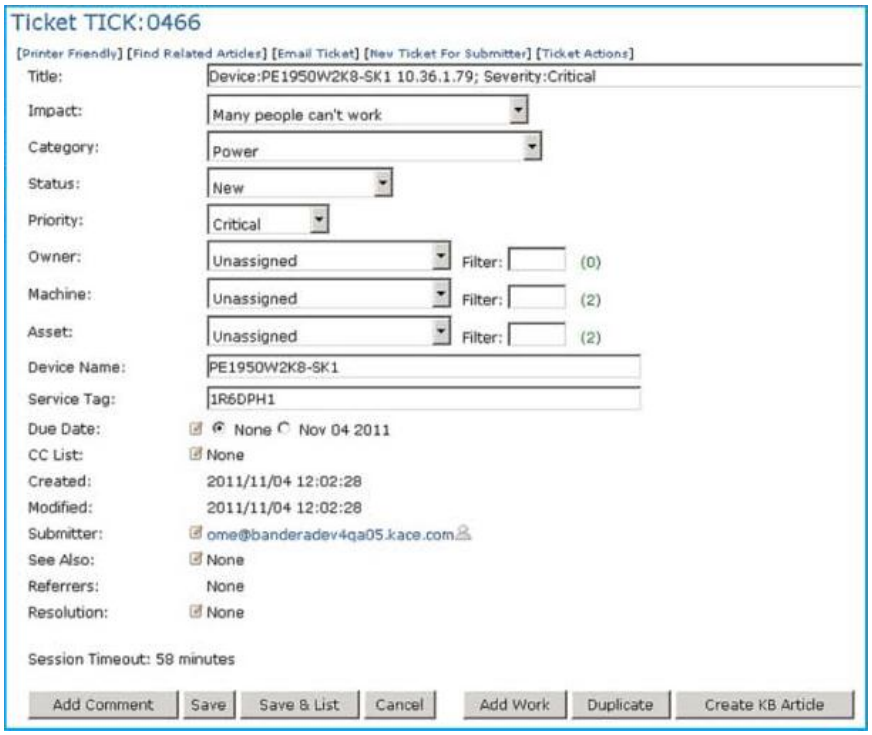
Figure 37. List of service desk tickets in K1000 Appliance

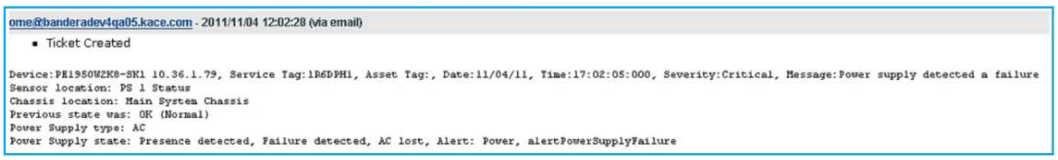


3. Click on the service desk ticket to view the details.

Figure 38. Details of a service desk ticket in K1000 Appliance







Conclusion

Users can have both OME and the KACE K1000 Appliance running on the same physical machine. This can be achieved by having multiple virtual machines (VMs) on the same physical hypervisor system, where one of the VMs will have OME installed and the other VM houses the K1000 virtual appliance. By adding OME—a simple free solution to your environment—you can provide hardware monitoring within your KACE environment without impacting your budget.

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 be able to review all aspects of the hardware and software you have deployed in your data center and their update status. They will be able to track changes that have taken place over time and by whom they have been implemented. When vulnerabilities are identified, service contracts are nearing expiration, or components fail, your 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.

Additional resources

Dell OpenManage Essentials

For more information on Dell OpenMange Essentials visit www.dell.com/ome or www.delltechcenter.com/ome

Dell OpenManage Administrator

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

Helpful Links:
KACE Systems Management Appliances
KACE Systems Deployment Appliances