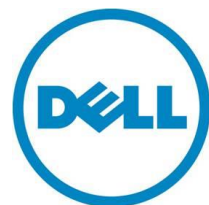

Configuring Alert Actions in OpenManage Essentials

This Dell technical white paper explains how to configure various alert actions in order to monitor the data center remotely.

OME Engineering Team



This document 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.

© 2016 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server 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 disclaims proprietary interest in the marks and names of others.

Contents

Executive Summary.....	4
Introduction	4
Alert Email Action	4
Creating An Alert Email Action.....	6
Alert Trap Forward Action	13
Creating An Alert Trap Forward Action	13
Alert Application Launch Action.....	16
Creating An Alert Application Launch Action	16
Alert Ignore Action	19
Creating An Alert Ignore Action	19
Conclusion	21

Figures

Figure 1. Email Settings.....	5
Figure 2. Creating A New Alert Email Action	6
Figure 3. Email Configuration.....	7
Figure 4. Alert Details.....	8
Figure 5. Severity Association	9
Figure 6. Category and Sources Association	10
Figure 7. Device Association	11
Figure 8. Date Time Association.....	12
Figure 9. Sample Alert Email.....	12
Figure 10. Creating A New Alert Trap Forward Action	14
Figure 11. Trap Forwarding Configuration	15
Figure 12. Forwarded Alerts.....	16
Figure 13. Creating A New Alert Application Launch Action	17
Figure 14. Application Launch Configuration	18
Figure 15. Creating A New Alert Ignore Action	19
Figure 16. Name and Severity Association	20
Figure 17. Duplicate Alert Correlation.....	21

Executive Summary

OpenManage Essentials is a one-to-many systems management tool that helps in monitoring servers, storage devices, printers, KVMs, UPSs, PDUs, chassis, network devices, and so on. OpenManage Essentials provides a framework for monitoring and alerting these devices, which is helpful in managing the data center remotely.

Introduction

OpenManage Essentials provides a powerful framework for monitoring and alerting which can be built upon to automate a variety of common tasks. This white paper illustrates several examples and provides complete steps on how to accomplish this. This white paper also describes the following supported alerts action in OpenManage Essentials and provides information on how an IT administrator can leverage them:

- Alert Email Action
- Alert Trap Forward Action
- Alert Application Launch Action
- Alert Ignore Action

Alert Email Action

The **Alert Email Action** feature helps you know the device status as soon as the device goes into critical state without you having to log on to the OpenManage Essentials console. You can customize alert severity, type, date, device, and days for **Alert Email Action**.

For the IT administrator to receive emails through the support desk, an SMTP server is required. The SMTP settings can be configured when an email alert action task is created. For SMTP settings, see Figure 1. By default, port 25 is selected. You can customize the port according to your environment. For secured communication, you can enable 'SSL'. Fill out all the fields shown in Figure 1.

You can enable **Logging** to help you troubleshoot when there are issues in sending emails to the SMTP server. The logs can be viewed under the **Logs** tab in the OpenManage Essentials console. It is not recommended to enable logging unless it is required as it will consume a large amount of storage space.

Figure 1. Email Settings

The screenshot shows the 'Email Settings' dialog box overlaid on the 'Alert Email Action' configuration page. The dialog box has a title bar with 'Email Settings' and a close button. It contains the following fields and options:

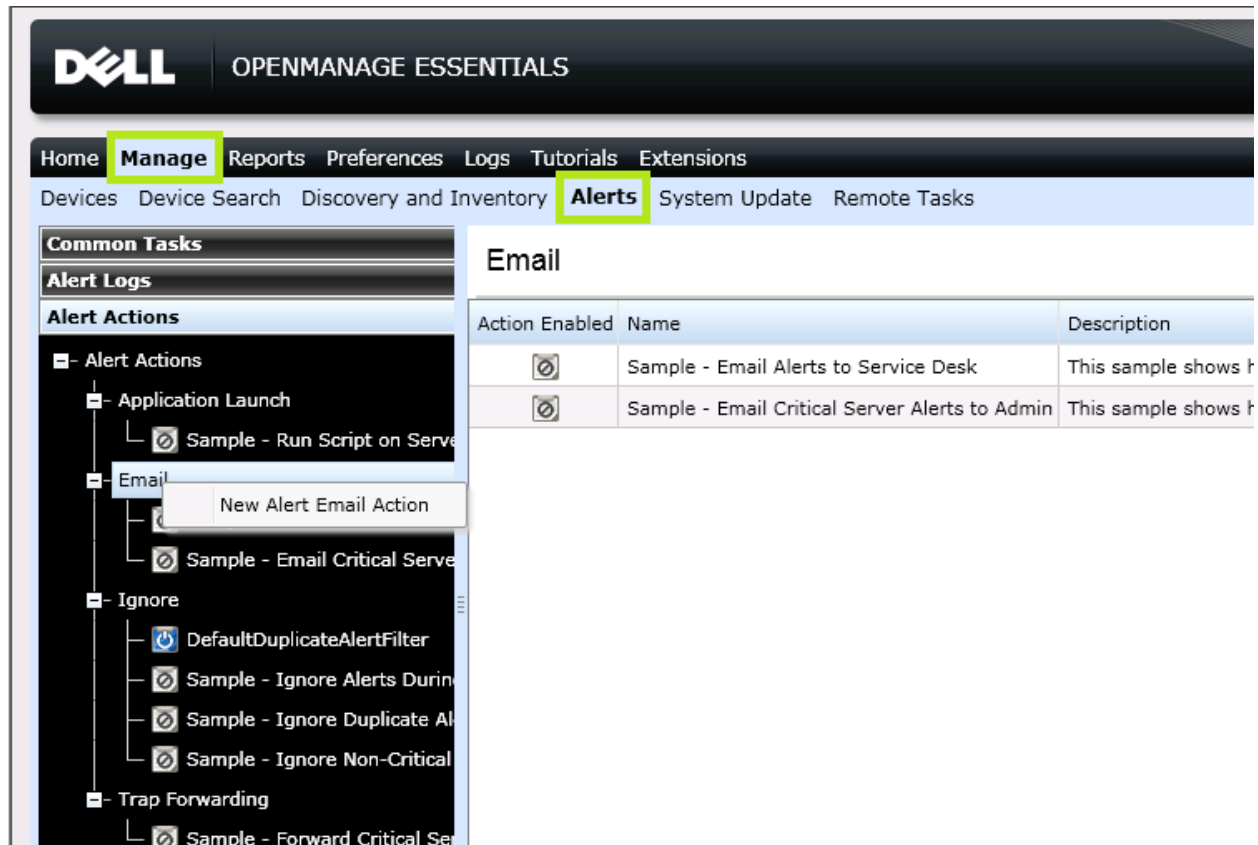
- SMTP Server Name or IP Address:** A text input field.
- Use Credentials:** A checkbox that is currently unchecked.
- Domain \ User Name:** A text input field, visible only if 'Use Credentials' is checked.
- Password:** A text input field, visible only if 'Use Credentials' is checked.
- Port:** A section with a checked 'Use Default' checkbox and a spinner box set to '25'.
- Use SSL:** A checkbox that is currently unchecked.
- Logging:** Three radio button options: 'Disabled' (selected), 'Errors Only', and 'Everything'.
- Note:** A text note stating: 'Note: The SMTP server setting applies to all alert email actions and can also be modified from the main Preferences page.'
- Buttons:** 'Ok' and 'Cancel' buttons at the bottom right.

The background window shows the 'Alert Email Action' configuration page with tabs for 'Alert Email Action' and 'E-mail Configuration'. The 'E-mail Configuration' tab is active, showing fields for 'To:', 'From:', 'Subject:', 'Device', 'Message', 'Device', and 'Severity'. A list of severity levels is visible on the left: '\$n', '\$ip', '\$m', '\$d', '\$t', '\$sev', '\$st'.

Creating An Alert Email Action

1. Click **New Alert Email Action** as shown in Figure 2, provide a name and proceed.

Figure 2. Creating A New Alert Email Action



2. In the **Email Configuration** window, provide a valid **To** and **From** email address.
3. Customize the **Subject** and **Message** of the email based on your preference. See 0.

Figure 3. Email Configuration

Alert Email Action | E-mail Configuration 2/7

Configure the e-mail parameters for this alert action.

To:

From:

Subject:

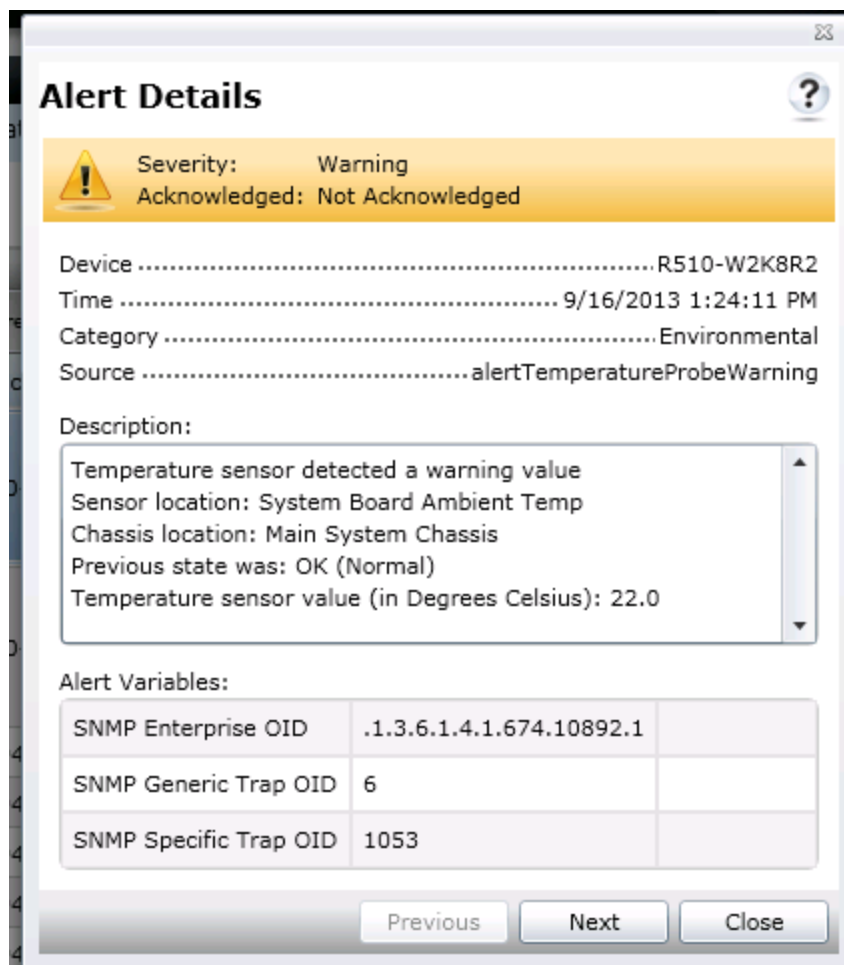
Message:

You may use the following parameters for substitution:

\$n = Device	\$e = Enterprise OID
\$ip = Device IP	\$sp = Specific Trap OID
\$m = Message	\$g = Generic Trap OID
\$d = Date	\$cn = Alert Category Name
\$t = Time	\$sn = Alert Source Name
\$sev = Severity	\$pkn = Package Name
\$st = Service Tag	\$at = Asset Tag
\$r = Recommended Resolution	\$mod = Model Name
\$loc = Device Location	

The various parameters that can be used in the **Subject** and **Message** fields are shown in Figure 4. For example, use \$m to include the text displayed in the **Description** field.

Figure 4. Alert Details



Alert Details

Severity: Warning
Acknowledged: Not Acknowledged

Device R510-W2K8R2
Time 9/16/2013 1:24:11 PM
Category Environmental
Source alertTemperatureProbeWarning

Description:

Temperature sensor detected a warning value
Sensor location: System Board Ambient Temp
Chassis location: Main System Chassis
Previous state was: OK (Normal)
Temperature sensor value (in Degrees Celsius): 22.0

Alert Variables:

SNMP Enterprise OID	.1.3.6.1.4.1.674.10892.1	
SNMP Generic Trap OID	6	
SNMP Specific Trap OID	1053	

Previous Next Close

- To receive emails for the alerts with critical severity, select **Critical** in the **Severity Association** window as shown in Figure 5.

Figure 5. Severity Association

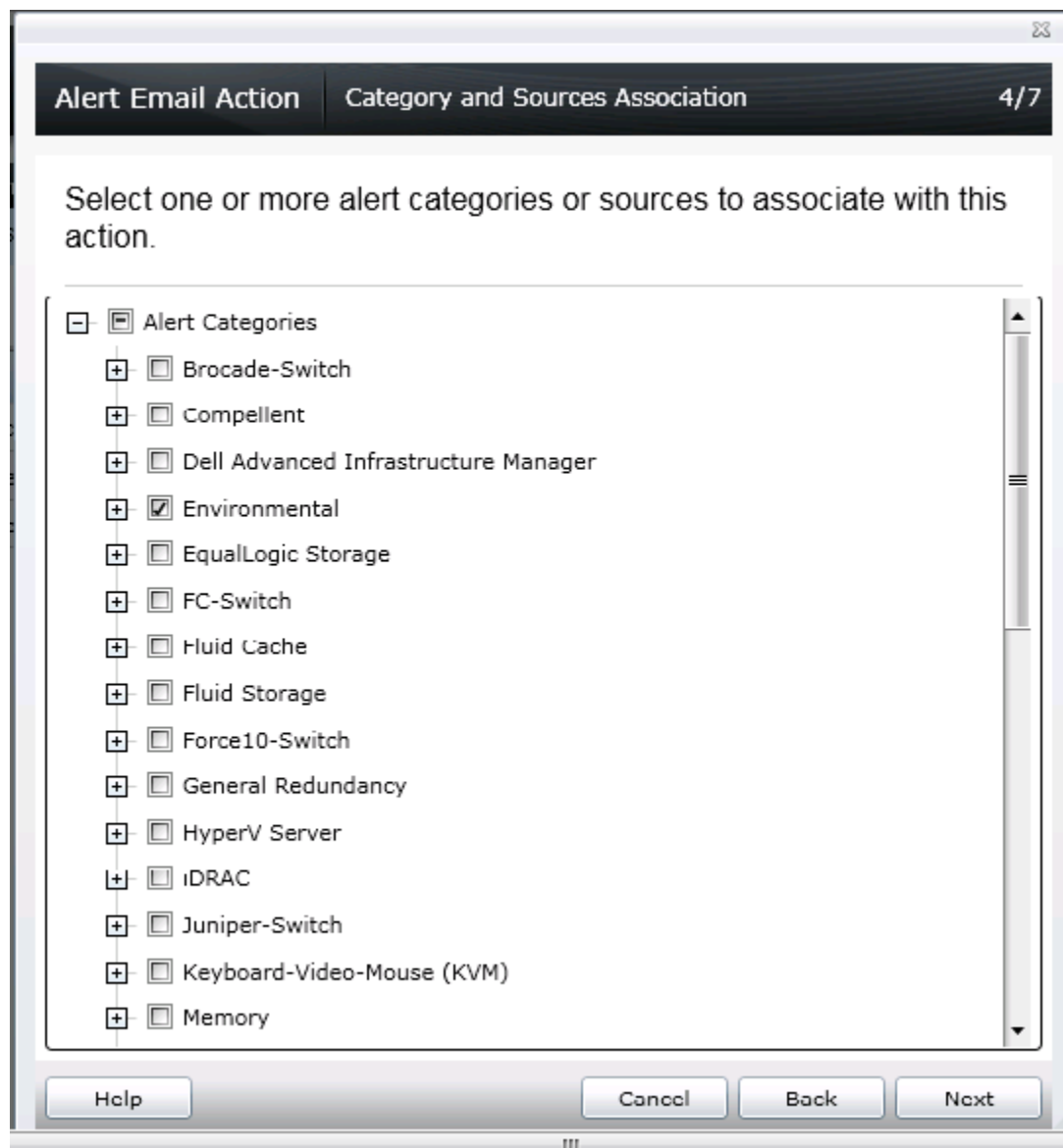
Alert Email Action | Severity Association 3/7

Select the severity to associate with this action.
The alert action will take place when the criteria specified in the following pages matches an incoming alert.

Severity: ☐ All
☐ Unknown
☐ Normal
☐ Warning
☐ Critical

5. To restrict the emails to a specific category, select one or more alert categories or sources as shown in Figure 6.

Figure 6. Category and Sources Association



6. A specific device(s) that needs to be monitored can only be selected through a query or from the device tree as shown in Figure 7.

Figure 7. Device Association

Alert Email Action Device Association 5/7

Select the device(s) or device group(s) to associate with this action.

☒ Select a query

☐ Select the devices/groups from the tree below:

- ☐ All Devices
 - ☐ Citrix XenServers
 - ☐ Clients
 - ☐ HA Clusters
 - ☐ KVM
 - ☐ Microsoft Virtualization Servers
 - ☒ Modular Systems
 - ☒ Network Devices
 - ☒ OOB Unclassified Devices
 - ☒ Power Devices
 - ☐ PowerEdge C Servers
 - ☐ Printers
 - ☐ RAC
 - ☒ Servers

7. Emails can be configured to be sent during a specific date/range. If none of the options are selected in this wizard, emails will be sent without any time restriction.

Figure 8. Date Time Association

Alert Email Action | **Date Time Association** 6/7

Select the date range, time range, and/or day(s) of week to associate with this action.
Note - all selections use AND logic.

☐ Limit Date Range

From: 9/16/2013

To: 9/16/2013

☐ Limit Time Range

From: 12:00 AM (UTC+05:30)

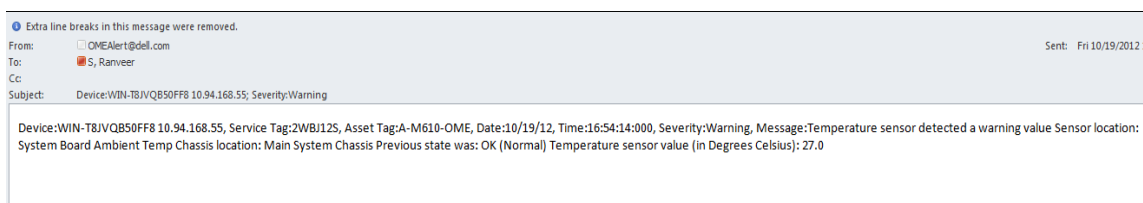
To: 12:00 AM (UTC+05:30)

☐ Limit Days

- ☐ Monday
- ☐ Tuesday
- ☐ Wednesday
- ☐ Thursday
- ☐ Friday
- ☐ Saturday
- ☐ Sunday

8. On receiving an alert that matches all the conditions configured in the **Alert Email Action** task, an email as shown in Figure 9 is sent from OpenManage Essentials.

Figure 9. Sample Alert Email



Alert Trap Forward Action

OpenManage Essential receives alerts from various SNMP agents and platform event traps (PETs) configured on the network. These traps may be required by another OpenManage Essentials instance or other network management systems (NMS) such as Microsoft SCOM, Dell ITA, Dell DMC, and so on. In this scenario, OpenManage Essentials can reproduce the traps and send them to other NMS for consolidation of the traps.

The system administrator can set the rules to define which traps will be forwarded based on the traps severity, traps categories, and devices/device groups.

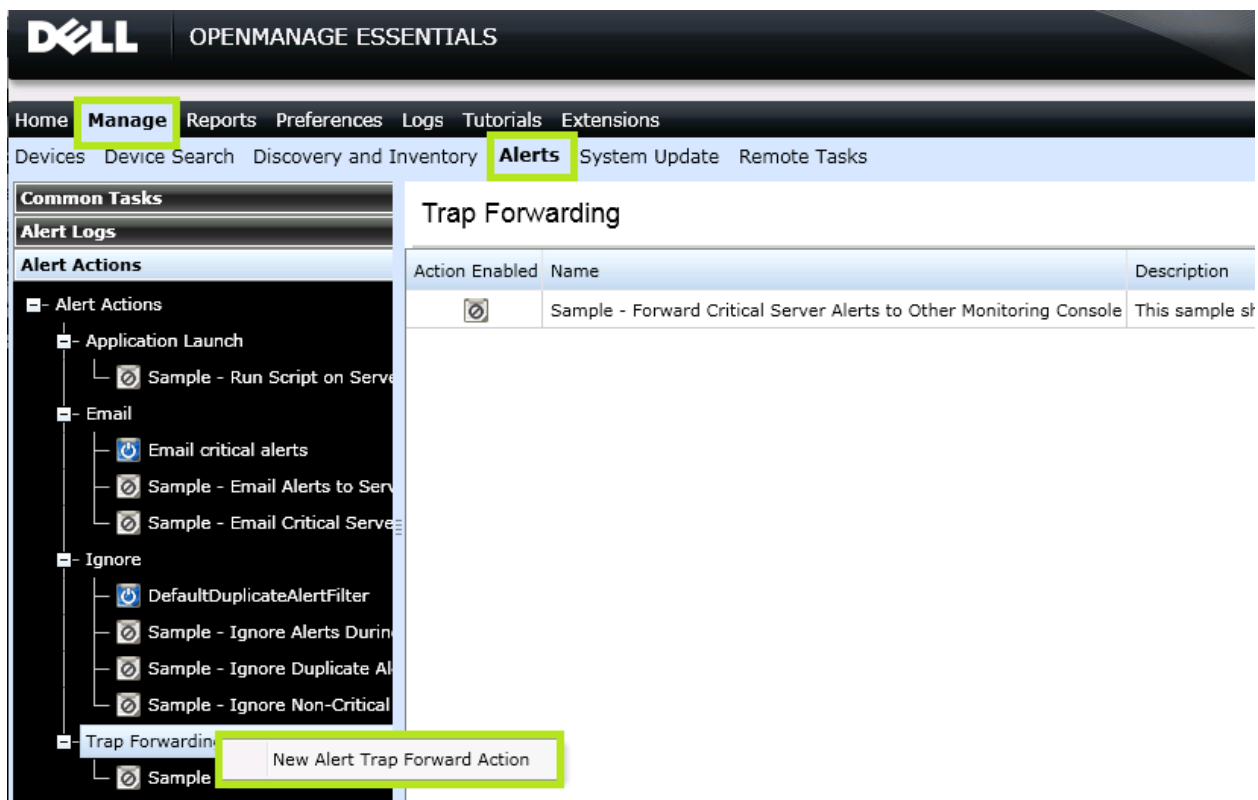
When there are multiple instances of OpenManage Essentials configured where each instance is monitoring a subset of devices in a data center, a system administrator may want to consolidate the alerts from multiple OpenManage Essential instances for tiered management. Otherwise, the system administrator will have to individually check all the OpenManage Essentials servers for monitoring the devices. Instead a system administrator can configure a master OpenManage Essentials server to which all the other OpenManage Essentials instances will forward the alerts/traps. It will then provide the system administrator a consolidated view of all the alerts and enable the system administrator to manage the data center from a single master OpenManage Essentials server.

NOTE: Only SNMPv1 traps can be forwarded in the original format. OpenManage Essentials does not support forwarding SNMP v2 alerts generated by devices such as PDU, KVM, and so on in the original format. SNMP v3 alerts are not supported by OpenManage Essentials.

Creating An Alert Trap Forward Action

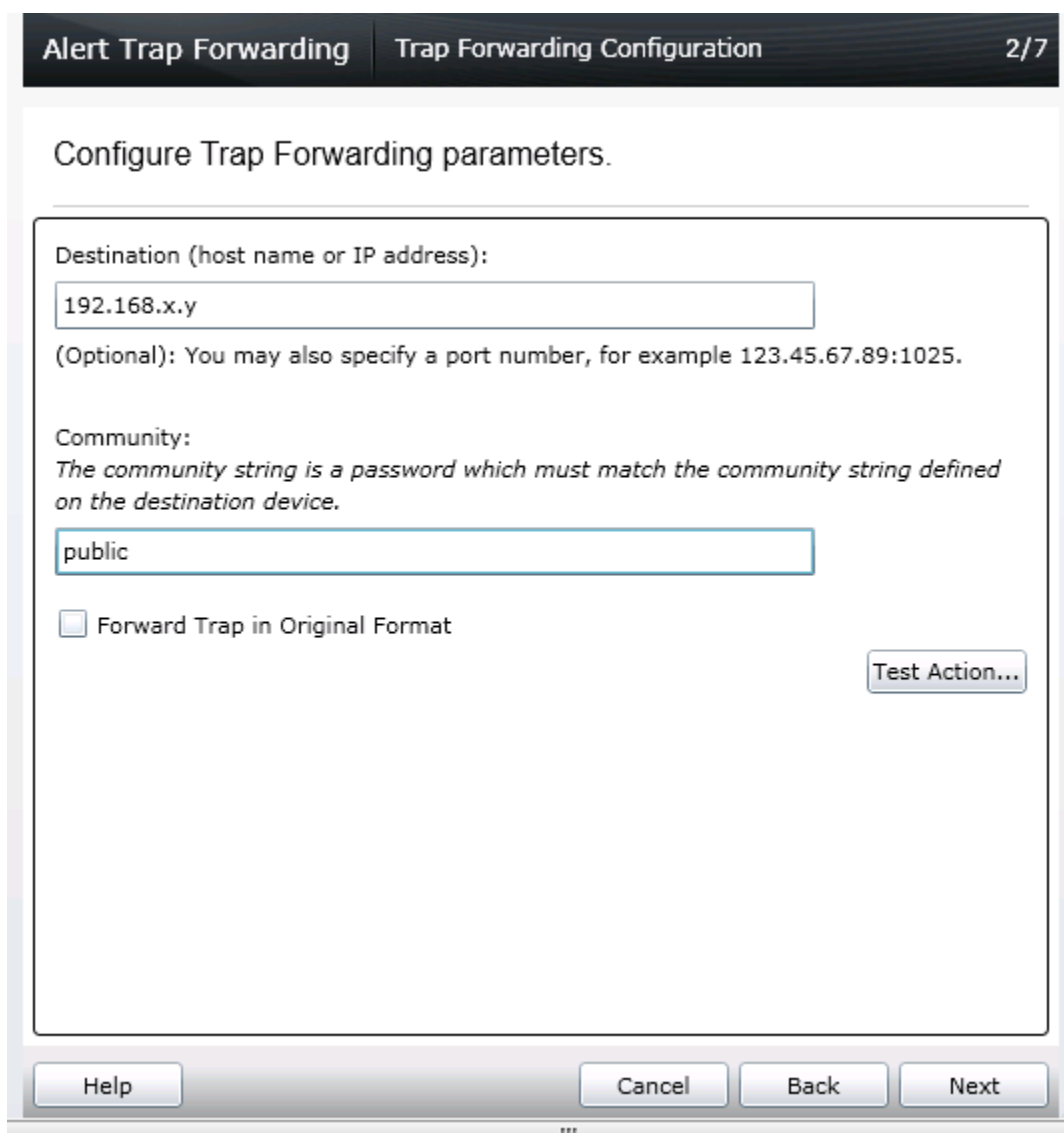
1. Click **New Alert Trap Forward Action** as shown in Figure 10, provide a name and proceed.

Figure 10. Creating A New Alert Trap Forward Action



2. Provide the trap destination to which the alerts need to be forwarded. The community string provided should be the same as that of the destination system. See **Error! Reference source not found.**
 - **Forward Trap in Original Format** (if enabled): The destination console will receive the alerts in the same format as the original alert that was received in the OpenManage Essentials console. The alert will have proper severity, enterprise, specific and generic OIDs as the original alert received by OpenManage Essentials.
 - **Forward Trap in Original Format** (if disabled): The destination console will receive the alert with 'other' category and source as 'OMEalertforwardedalert'. The Enterprise OID alert will always be 1.3.6.1.4.1.674.11000.1000.100.1 irrespective of the original alert.

Figure 11. Trap Forwarding Configuration



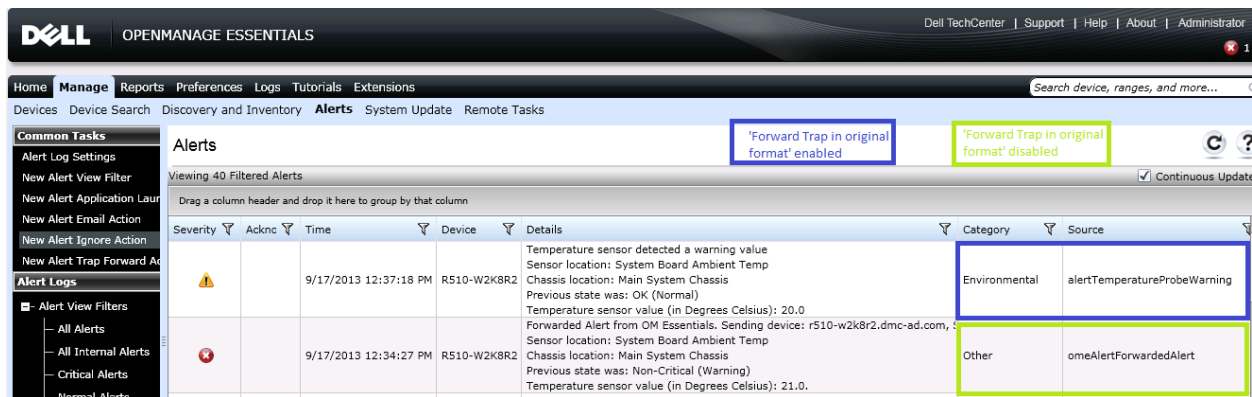
The image shows a 'Trap Forwarding Configuration' dialog box. At the top, there is a dark header bar with 'Alert Trap Forwarding' on the left and 'Trap Forwarding Configuration' on the right, followed by a page indicator '2/7'. Below the header, the main area is titled 'Configure Trap Forwarding parameters.' and contains the following fields and controls:

- Destination (host name or IP address):** A text input field containing '192.168.x.y'.
- (Optional):** A note stating 'You may also specify a port number, for example 123.45.67.89:1025.'
- Community:** A text input field containing 'public'. Below this field is a note: 'The community string is a password which must match the community string defined on the destination device.'
- Forward Trap in Original Format:** A checkbox that is currently unchecked.
- Test Action...:** A button located to the right of the checkbox.

At the bottom of the dialog, there are four buttons: 'Help', 'Cancel', 'Back', and 'Next'.

3. Severity, Category, Device, date and time can be customized according to the requirement as described for **Alert Email Action**.
4. The alert is forwarded to the destination OpenManage Essentials console if all the conditions configured in the task match. Alert received by the destination console is represented in **Error! eference source not found..**

Figure 12. Forwarded Alerts



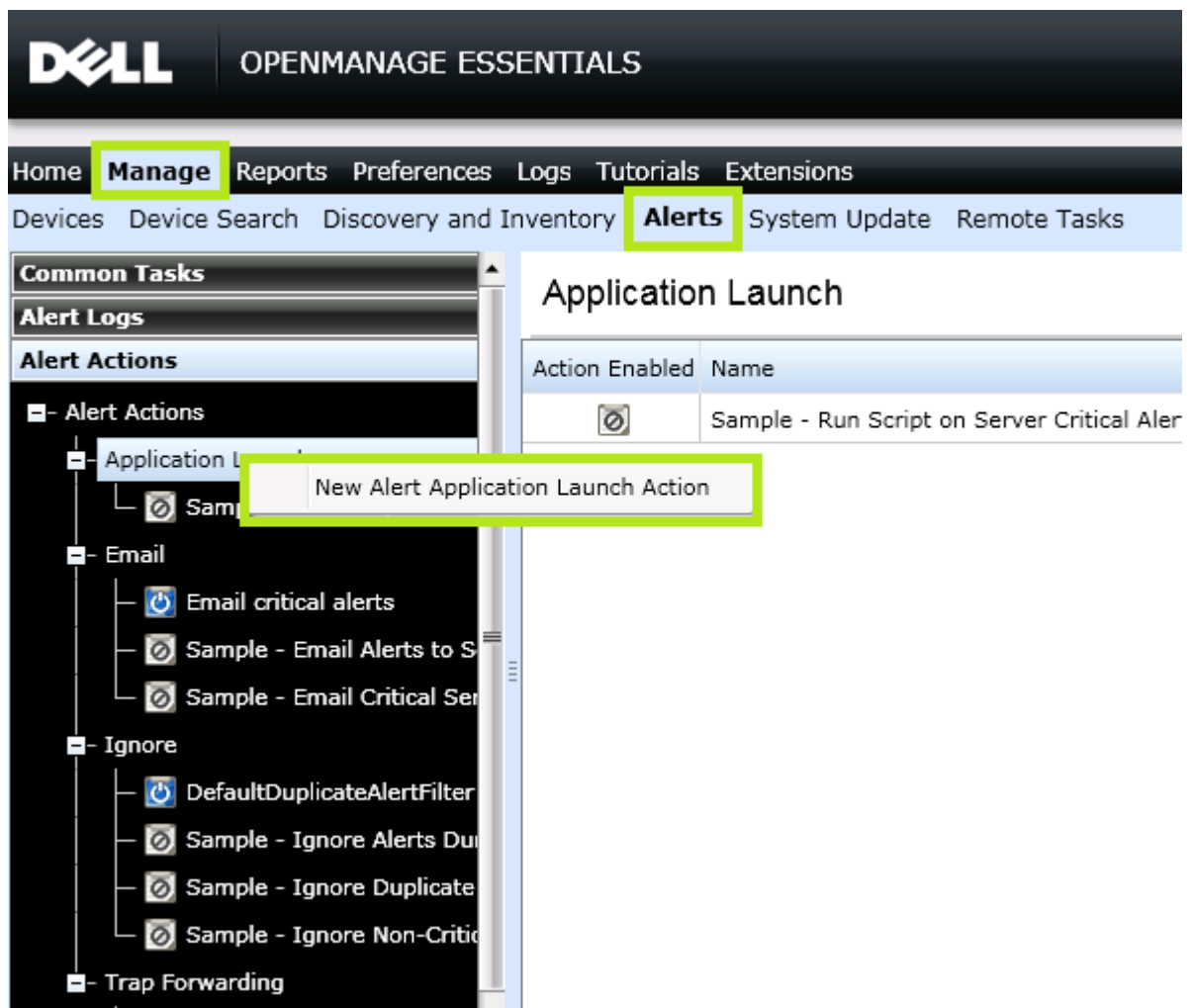
Alert Application Launch Action

On receiving an alert in the OpenManage Essentials console, an IT administrator can automate to run scripts. Scripts can be used to log a trouble ticket or run any diagnostic tool. An executable VBScript or a batch file can be configured to run when an alert is received.

Creating An Alert Application Launch Action

1. Click **New Application Launch Action** as shown in Figure 13, provide a name and proceed.

Figure 13. Creating A New Alert Application Launch Action



2. Configure the task by providing the correct path and the name of the script in the **Executable Name** field. The arguments shown in Figure 14 are all configurable.

Figure 14. Application Launch Configuration

Alert Application Launch | Application Launch Configuration 2/7

Configure the Application Launch parameters.

Executable Name:

Arguments:

You may use the following parameters for substitution:

\$n = Device	\$e = Enterprise OID
\$ip = Device IP	\$sp = Specific Trap OID
\$m = Message	\$g = Generic Trap OID
\$d = Date	\$cn = Alert Category Name
\$t = Time	\$sn = Alert Source Name
\$sev = Severity	\$pkn = Package Name
\$st = Service Tag	\$at = Asset Tag
\$r = Recommended Resolution	\$mod = Model Name
\$loc = Device Location	

- Severity, Category, Device, date and time can be customized according to the requirement as described for **Alert Email Action**.

Alert Ignore Action

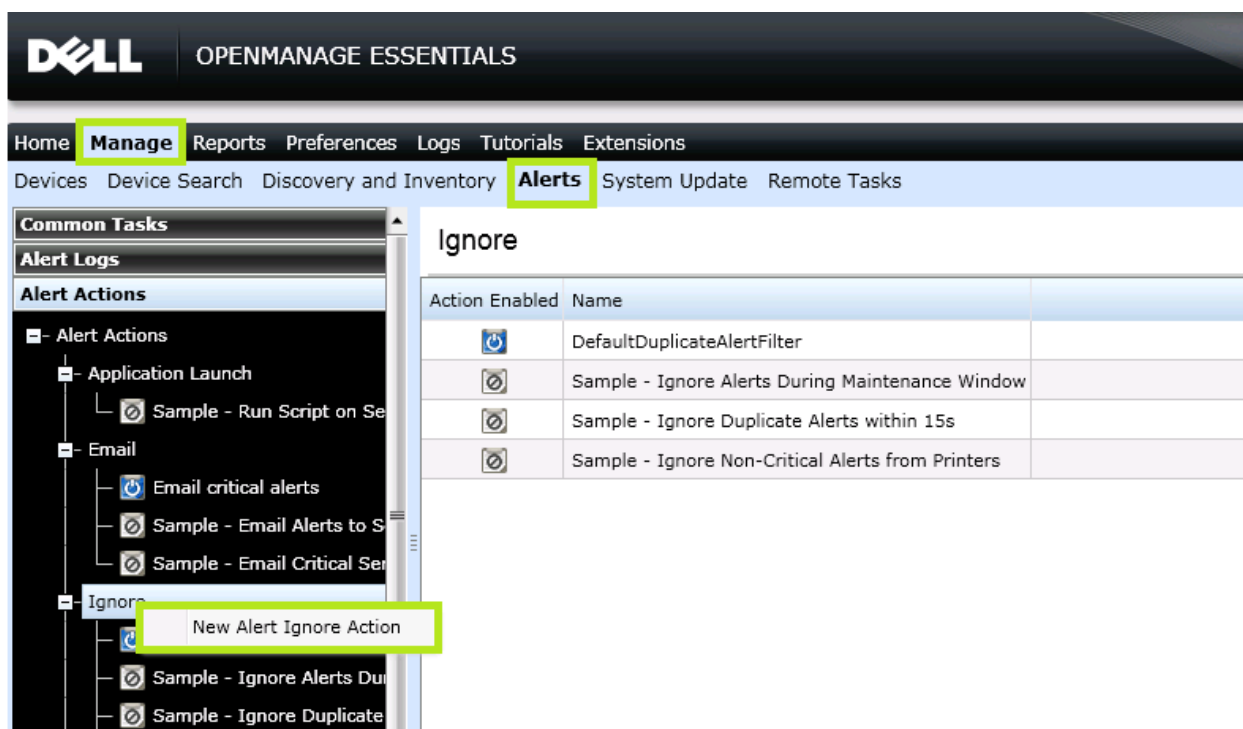
An IT administrator can choose to ignore alerts for different reasons.

- If a maintenance task is scheduled in a data center, alerts are received in bulk and the alert log is flooded in OpenManage Essentials. These alerts are known and can be ignored instead of flooding the database.
- When you are aware that there are a few fault devices in the data center that keep generating alerts frequently. Alerts from those devices can be ignored.
- In case of devices sending similar alerts continuously, you can choose to avoid receiving duplicate alerts in the console.

Creating An Alert Ignore Action

1. Click **New Alert Ignore Action** as shown in Figure 15, provide a name and proceed.

Figure 15. Creating A New Alert Ignore Action



2. Select the alert severity in the **Name and Severity Association** wizard.

Figure 16. Name and Severity Association

The screenshot shows a wizard window titled 'Alert Ignore Action' with a sub-tab 'Name and Severity Association' and a progress indicator '1/6'. The main text area contains instructions: 'Enter the name of the alert action and select the enabled state and severity to associate with this action. The ignore action will take place when the criteria specified in this wizard matches an incoming alert. Matching alerts will not be stored by the console or displayed in the Alert Logs.'

Below the text, there is a form with the following fields:

- Name:** A text box containing the word 'ignore'.
- Enabled:** A checkbox that is checked.
- Severity:** A group of five checkboxes:
 - ☐ All
 - ☐ Unknown
 - ☐ Normal
 - ☐ Warning
 - ☒ Critical

At the bottom of the window, there are three buttons: 'Help', 'Cancel', and 'Next'.

- Alert category, source, date/Range and time can be customized as described for **Alert Email Action**.
- In order to avoid duplication of alerts, select **Yes** in the **Duplicate Alert Correlation** wizard. Duplicate alerts received will be discarded within the specified time interval. If you select **No**, the duplicate alerts will be received in the console.

Figure 17. Duplicate Alert Correlation

Alert Ignore Action Duplicate Alert Correlation 5/6

Specify an interval during which duplicate alerts will be ignored.

Do you want to exclude alerts that are duplicates during the user specified interval?

For example, if the interval is set to 15 seconds and a device sends out the same alert every second, only 1 alert will be logged in a 15 second time range.

☐ Yes. Only duplicate alerts that match this action will be excluded.

Ignore duplicate alerts that are received during the interval (1-600 seconds):

☒ No

Help Cancel Back Next

Alerts that match the ignore alerts criteria will neither be stored in DB nor be displayed in the console, as they are discarded. By default, 'Default duplicate alert filter' is enabled to avoid getting duplicate alerts within 15 seconds.

Conclusion

Using OpenManage Essentials, An IT administrator can manage business critical servers/devices remotely. Corrective action can be taken even before the devices stop working and cause interruption to the business by being aware of the problem as soon as it occurs. Using the Application Launch actions a trouble ticket can be automatically logged. Through the Trap Forward Alert Action, all the alerts can be consolidated at one place to manage the data center from a single master OpenManage Essentials console.