Configuring Alert Log Settings and Alert Actions in Dell EMC OpenManage Essentials (OME)

This technical white paper describes the process of configuring alert settings and various alert actions to remotely monitor the data center.

Dell EMC Engineering
August 2017

A Dell EMC Technical White Paper

Revisions

Date	Description
August 2017	Initial release

Contents

Executive summary

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

Introduction

OME provides a powerful framework for monitoring and alerting which can be built upon to automate a variety of common tasks. This technical white paper illustrates several examples and provides complete steps to help you accomplish this. This technical white paper also describes the following supported alert log settings and alert actions in OME, and provides information on how an IT administrator can leverage them:

- Configuring alert logs
- Alert trap forward action
- Alert application launch action
- Alert ignore action

1 Configuring alert logs

OME logs the alerts into its database so that it can be made available in the Alert log screen. OME also allows managing the number of alert logs stored and purging. To go to the Alert Log Configuration page, click **Manage → Alerts → Alert Log Settings**.

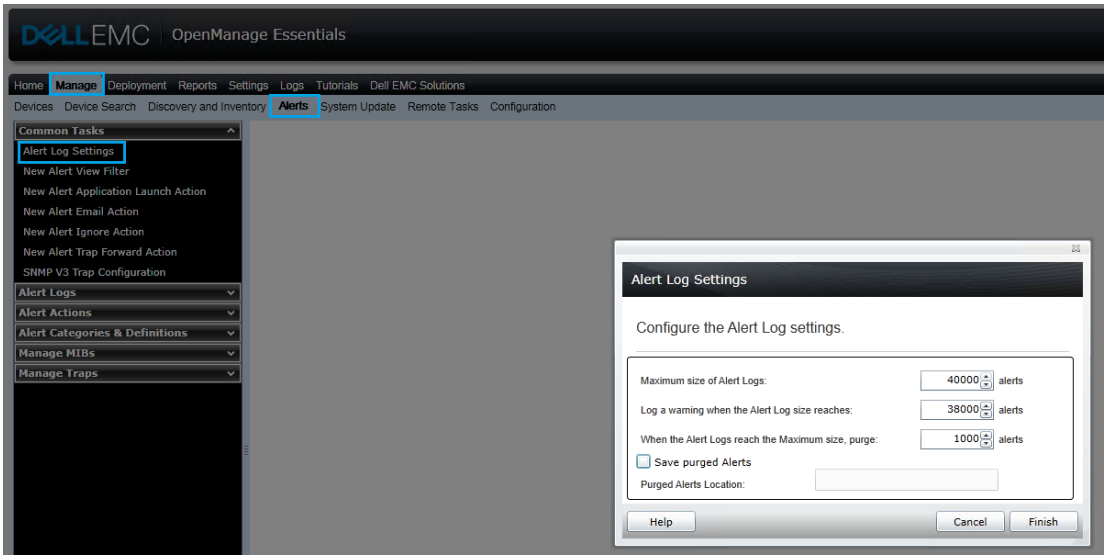

Figure 1 Alert Log Setting navigation

In the Alert Log Settings dialog box:

- Set the maximum number of Alert Logs
- Set an alert message to indicate the alert log has reached its threshold
- Purge logs when the number of logs reaches a particular size
- Save the purged alerts into a file in a specified location

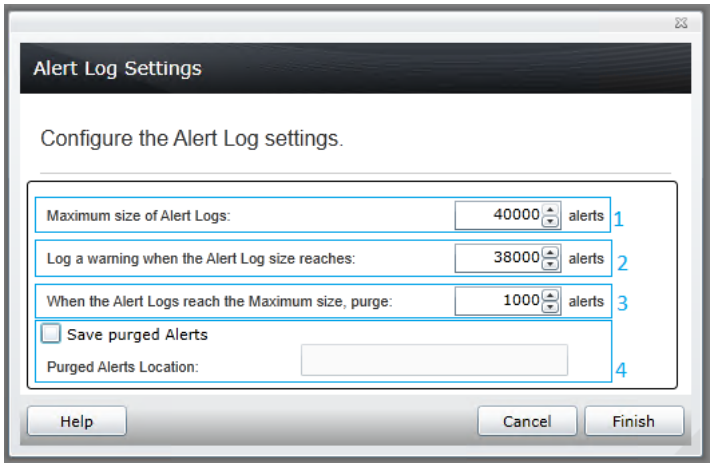

Figure 2 Alert Log Settings Sceen

The file that contains the purged logs will be in the format Alert-<Date and Time in DDMMMYYYY>.csv. The file has the following fields for each alert received,

- Severity
- Acknowledged
- Time
- Device
- Details
- Category
- Source

Severity	Acknowledged	Time	Device	Details	Category	Source
Warning	Not Acknowledged	3/23/2017 13:07	100.96.27.	Message: Login attempt alert for root from 100.....	Other	alertUserTrackingWarning
Unknown	Not Acknowledged	3/23/2017 14:03	936J7C2	Enterprise: .1.3.6.1.4.1.3183.1.1 Trap Ids:Generic:6 Specific:196999; (;0=DELL3;1=100.100.226.199;2=1.3.6.	Unknown	Unknown
Normal	Not Acknowledged	3/23/2017 14:03	936J7C2	Message: The system board Consumption current is within range., System Display Name: System, System	Power	alertAmperageProbeNormal

Figure 3 File format example

2 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 in to the OME 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 4. By default, port 25 is selected. You can customize the port according to your environment. For secured communication, you can enable 'SSL'. Type or select data in the fields as shown in Configuring alert logs.

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 OME console. It is not recommended to enable logging unless it is required, because enabling consumes more storage disk space.

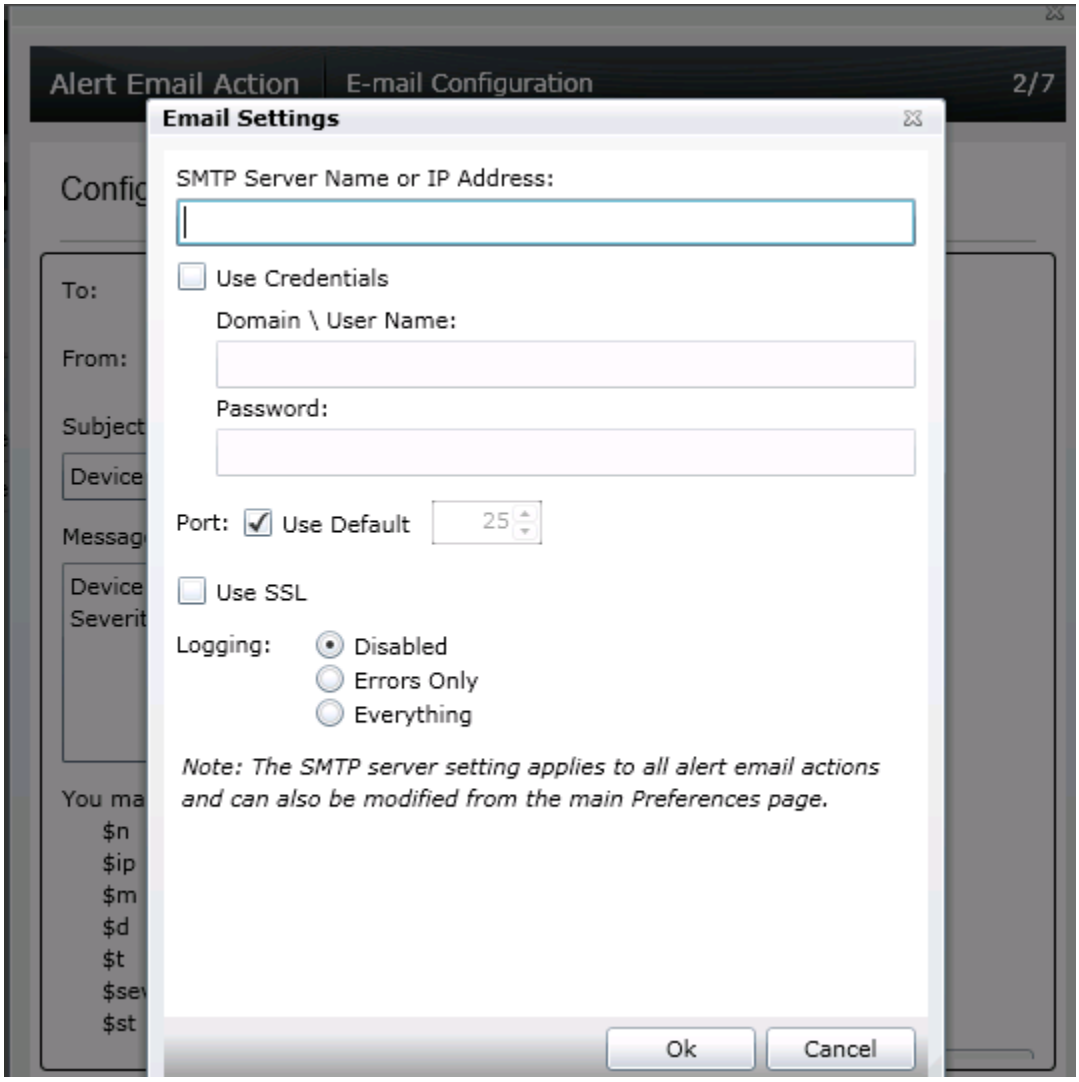

Figure 4 Email Settings

2.1 Creating alert email action

1. Click **New Alert Email Action** as shown in Figure 5 and type a name.

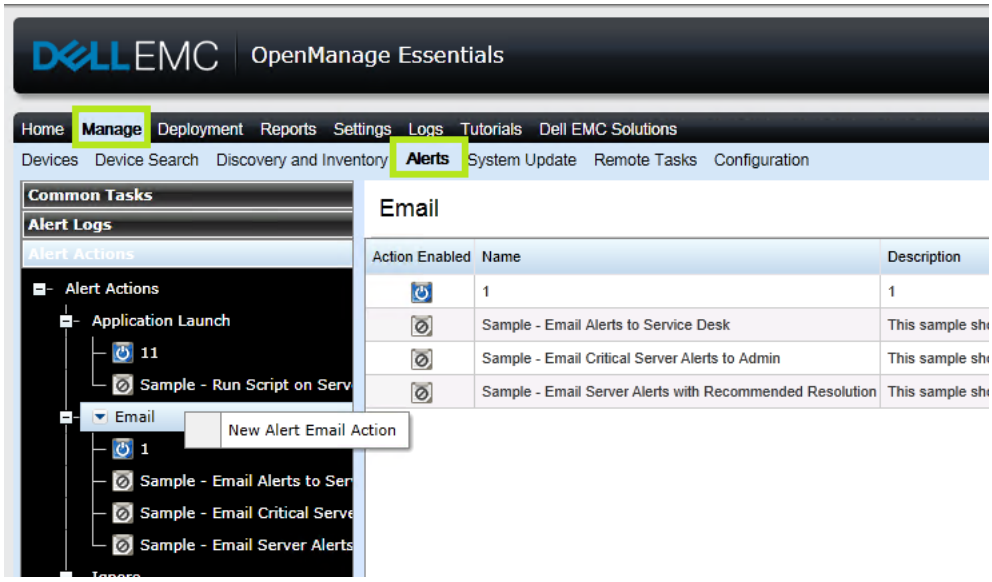

Figure 5 Creating A New Alert Email Action

2. In the **Email Configuration** window, type a valid To and From email address.

3. Customize the Subject and Message of the email based on your preference. See Figure 6.

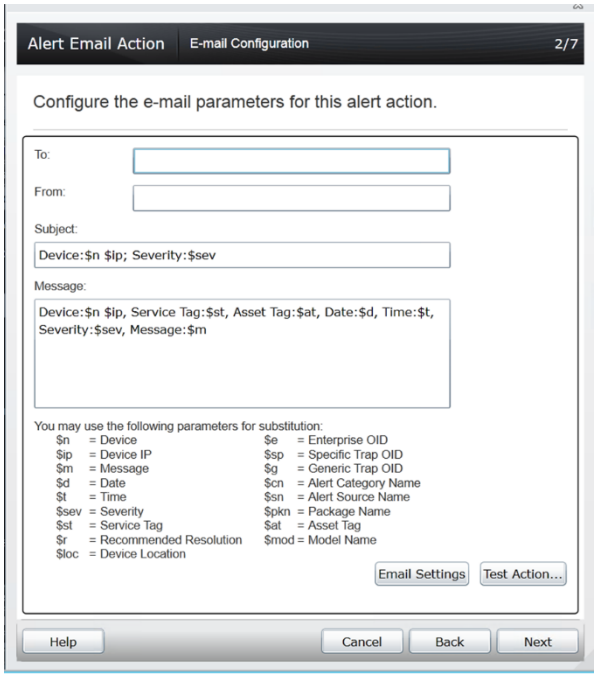

Figure 6 Email Configuration

The various parameters that can be used in the Subject and Message fields are shown in Figure 6. For example, use $m to include the text displayed in the Description field.

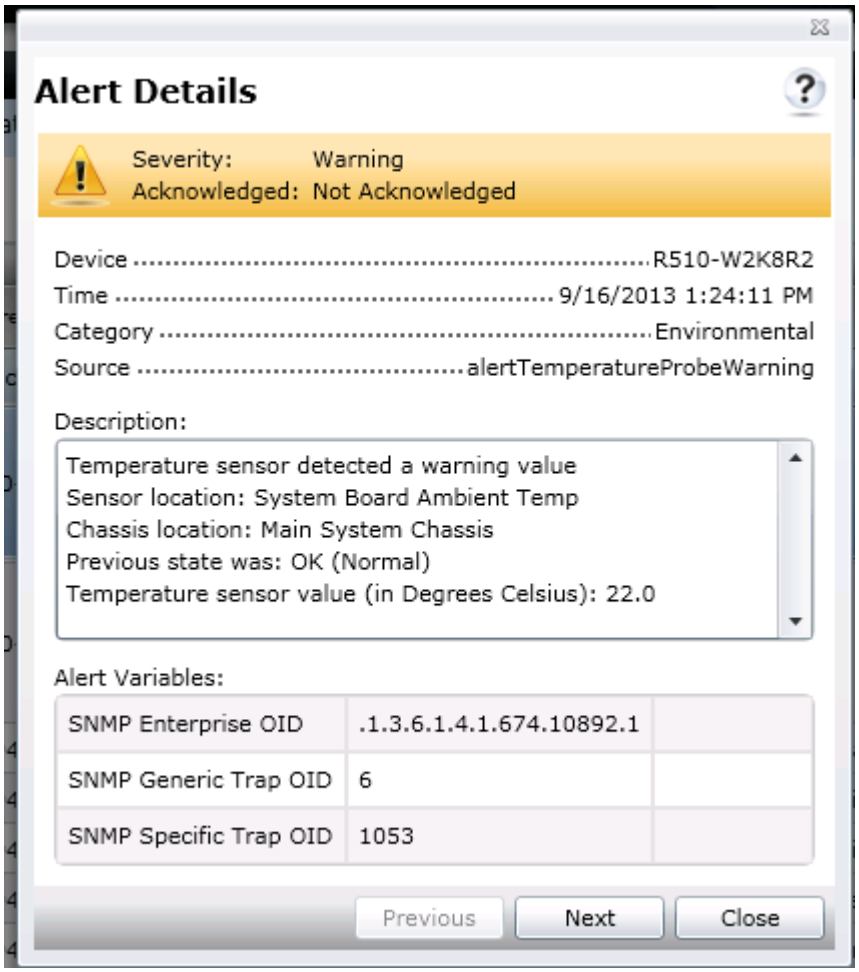

Figure 7 Alert details

4. To receive emails for the alerts that have critical severity, select **Critical** in the **Severity Association** window as shown in Figure 8.

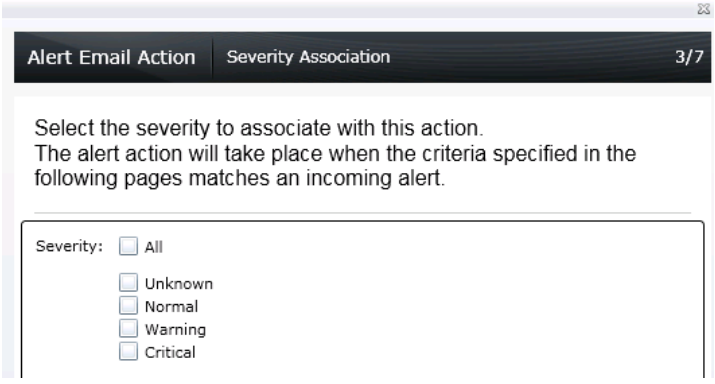

Figure 8 Severity Association

5. To restrict the emails to a specific category, select one or more alert categories or sources as shown in Figure 9.

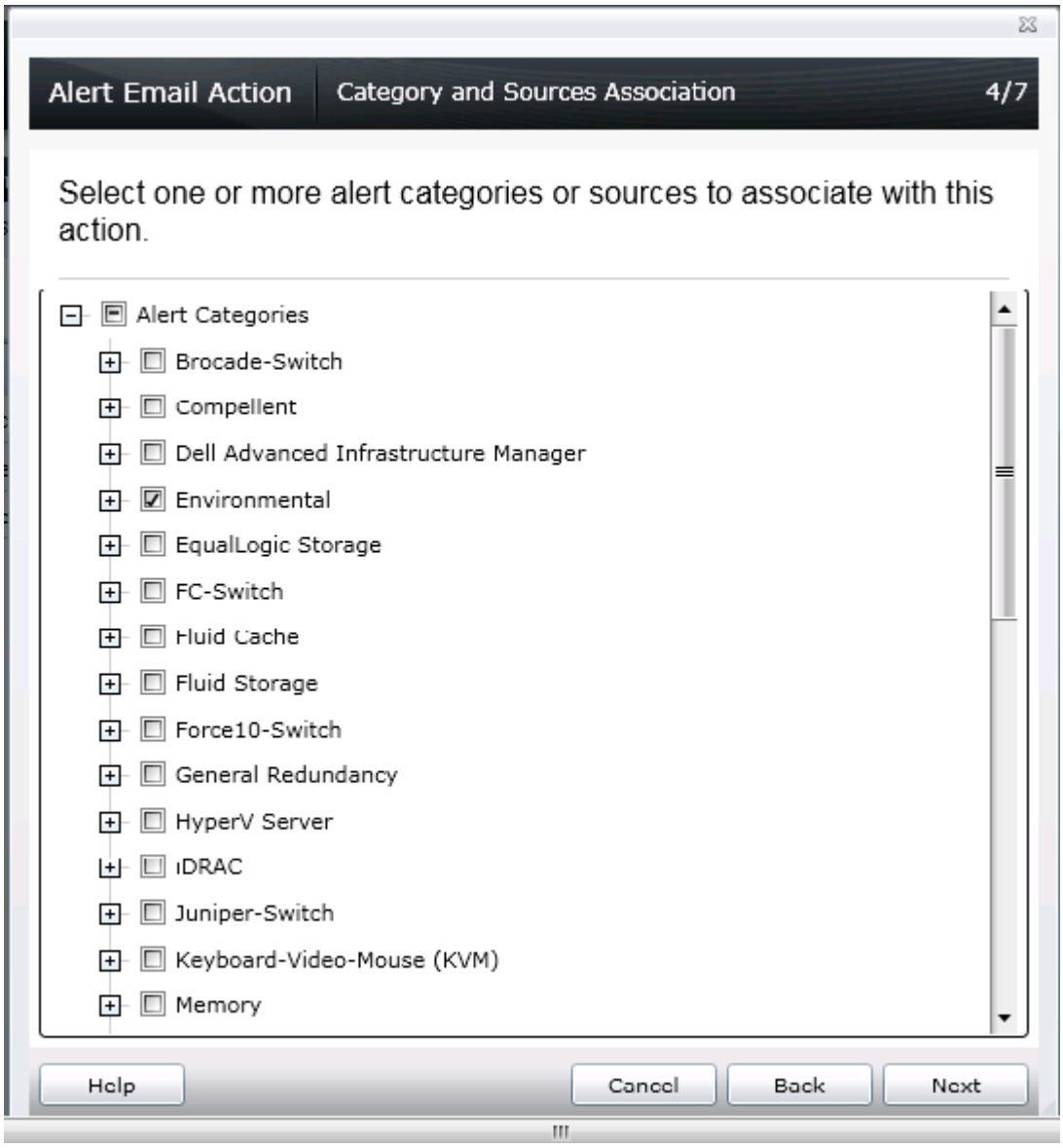

Figure 9 Category and Sources Association

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 10.

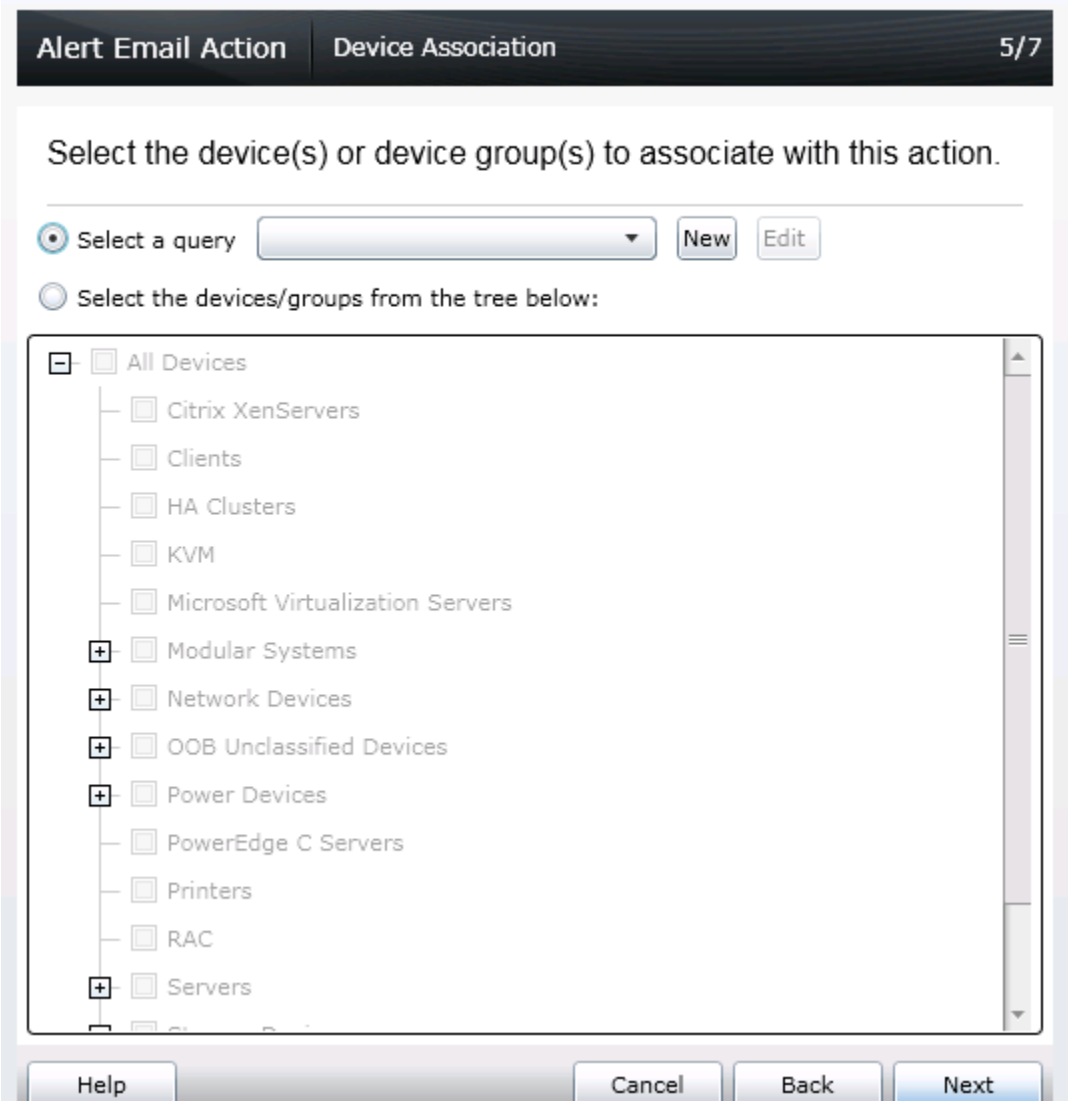

Figure 10 Device Association

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

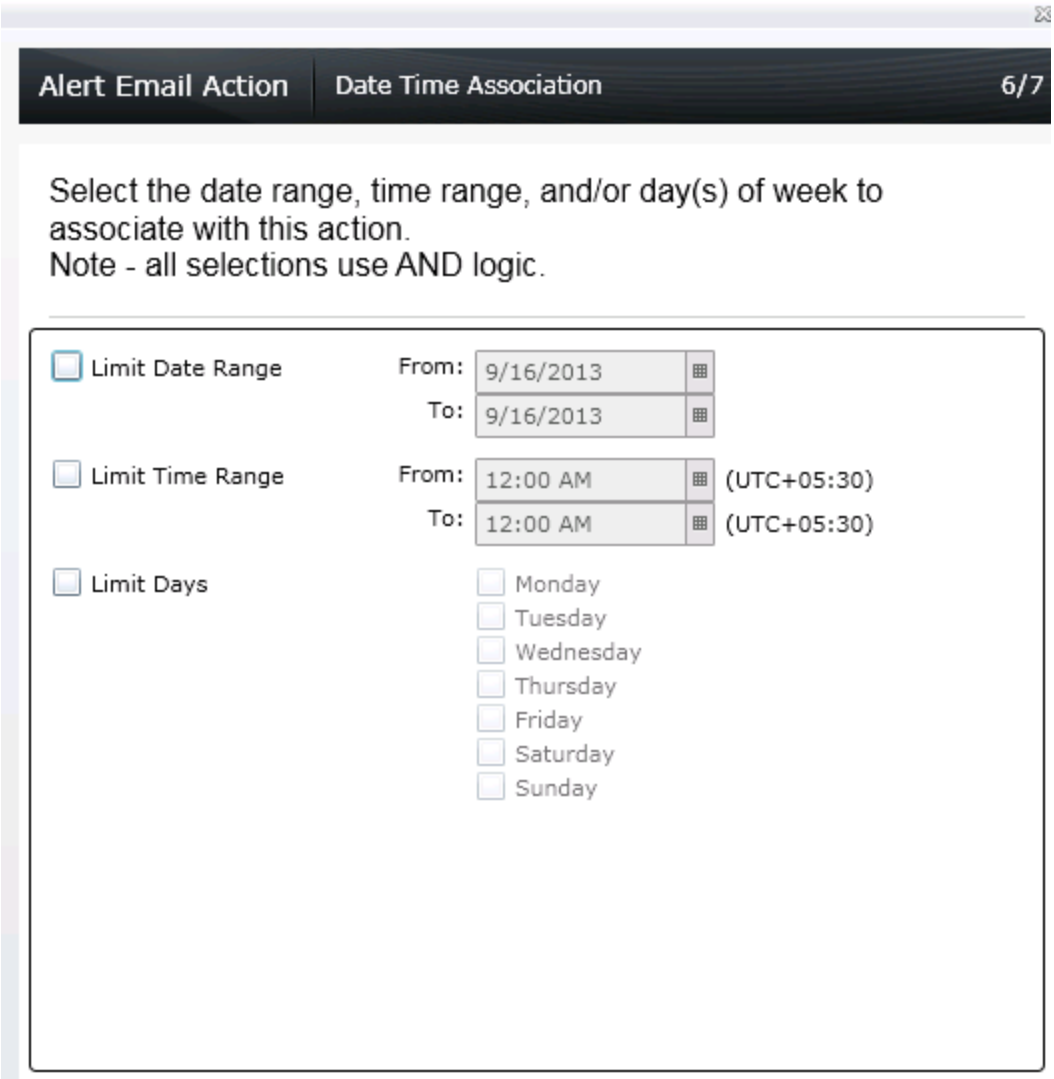

Figure 11 Date Time Association

7. 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 OME.

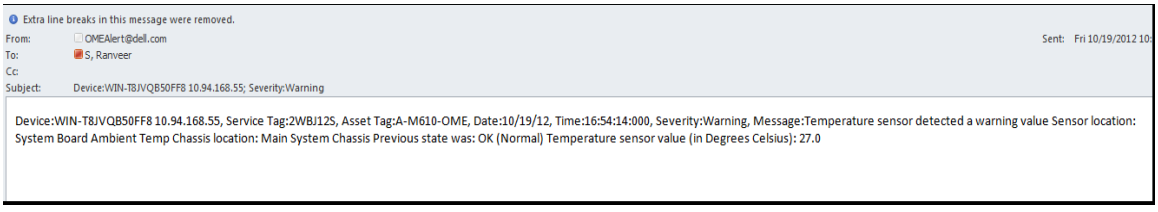

Figure 12 Sample Alert Email

3 Alert trap forward action

OME receives alerts from various SNMP agents and platform event traps (PETs) configured on the network. These traps may be required by another OME instance or other network management systems (NMS) such as Microsoft SCOM, Dell ITA, and Dell DMC. In this scenario, OME 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 OME 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 OME instances for tiered management. Else, the system administrator has to individually check all the OME servers for monitoring the devices. Instead, a system administrator can configure a master OME server to which all the other OME instances will forward the alerts or traps. Instances also 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 OME server.

Note: Only SNMPv1 traps can be forwarded in the original format. OME does not support forwarding SNMPv2 alerts generated by devices such as PDU and KVM in the original format. SNMPv3 alerts are not supported by OME.

3.1 Creating alert trap forward action

1. Click **New Alert Trap Forward Action** as shown in Figure 13, type a name.

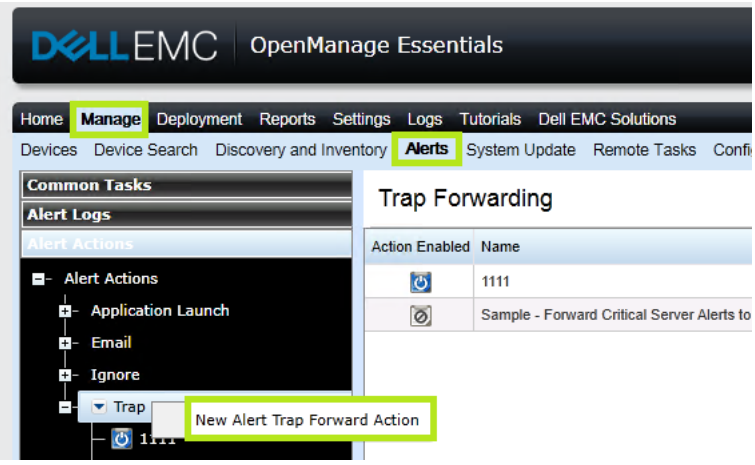

Figure 13 Creating A New Alert Trap Forward Action

2. Type the trap destination to which the alerts must be forwarded. The typed community string must be the same as that of the destination system. See Figure 14.
    - 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 OME console. The alert will have proper severity, enterprise, specific and generic OIDs as the original alert received by OME.

- Forward Trap in Original Format (if disabled): The destination console receives 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.

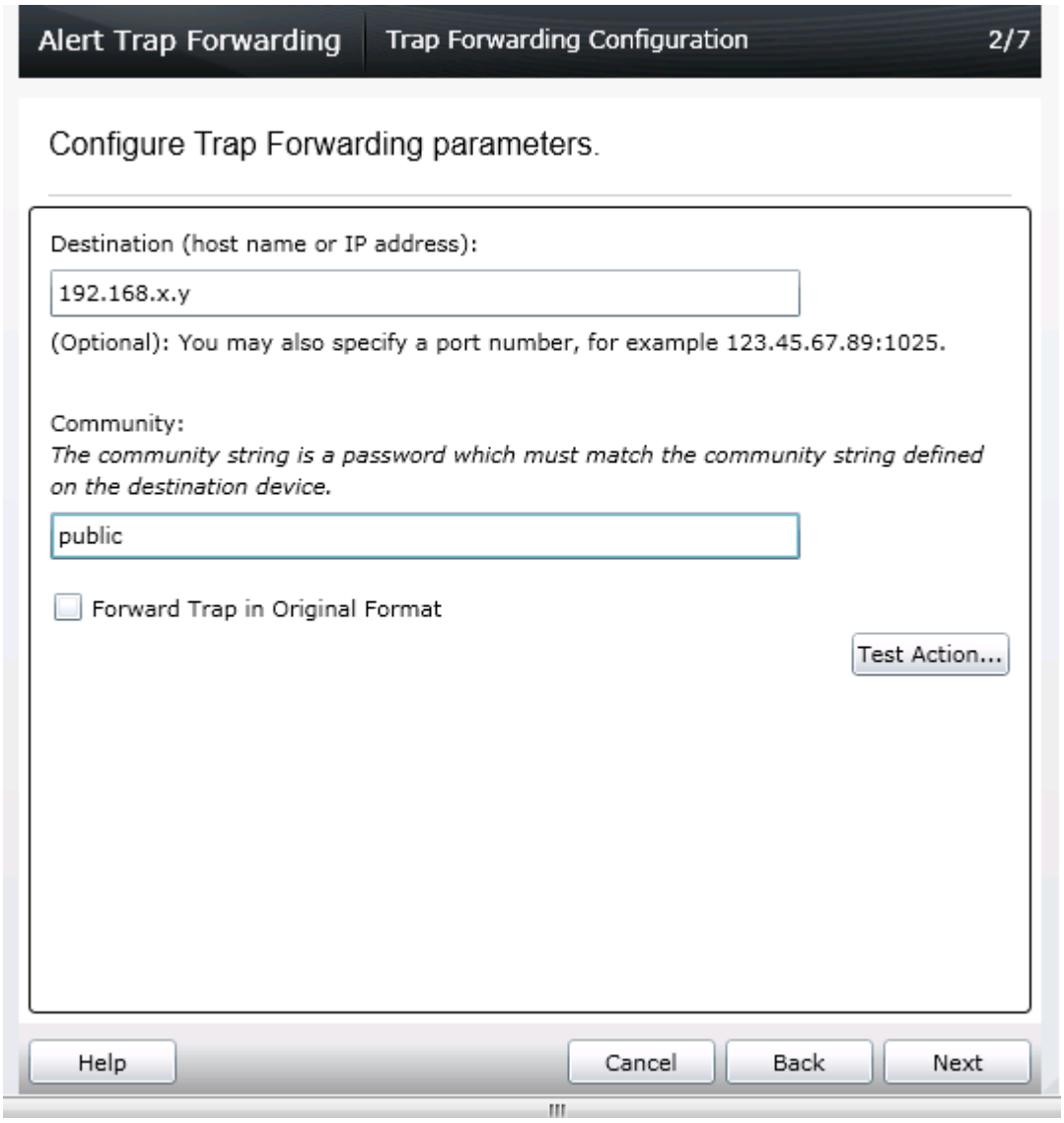

Figure 14 Trap Forwarding Configuration

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

4. The alert is forwarded to the destination OME console if all the conditions configured in the task match. Alert received by the destination console is indicated in Figure 15.

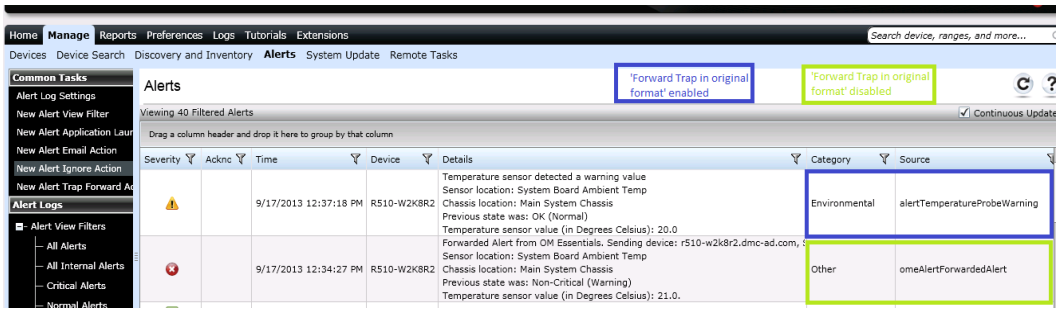

Figure 15 Forwarded Alerts

4 Alert application launch action

Receiving an alert in the OME 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.

4.1 Creating alert application launch action

1. Click **New Application Launch Action** as shown in Figure 16, type a name.

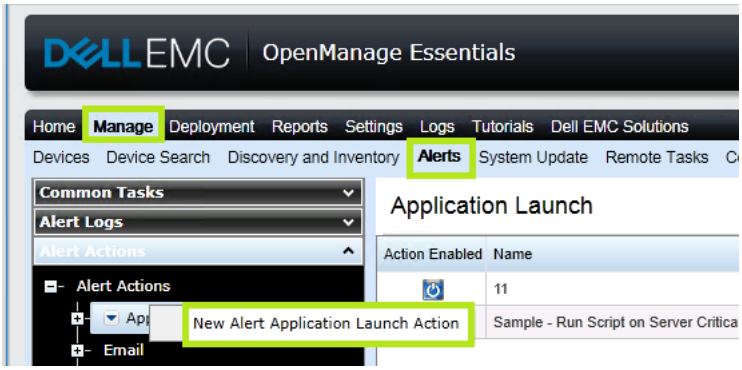

Figure 16 Creating A New Alert Application Launch Action

2. Configure the task by providing the correct path and the name of the script in the **Executable Name** box. The arguments shown in Figure 17 are all configurable.

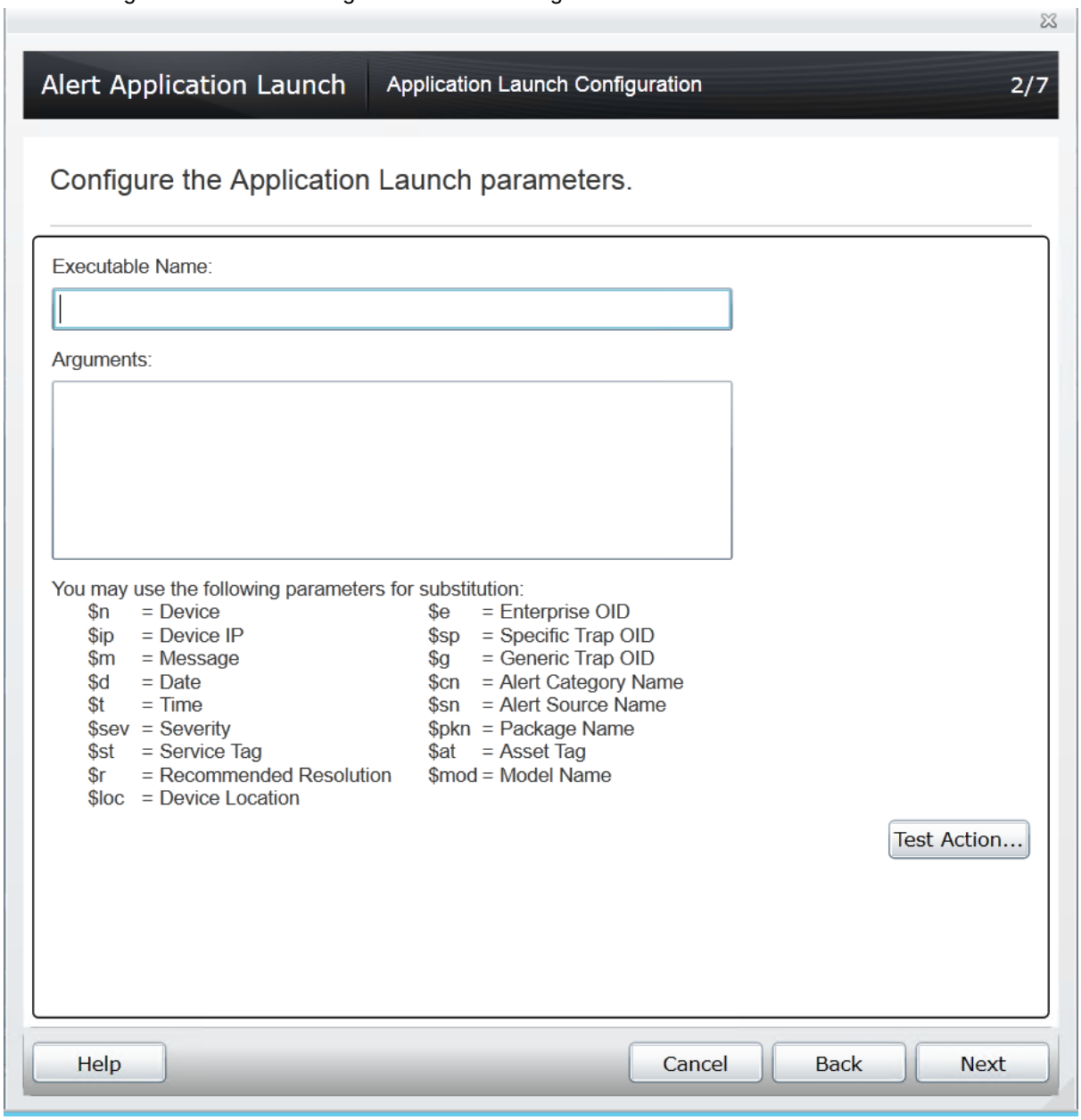

Figure 17 Application Launch Configuration

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

5 Alert ignore action

An IT administrator can choose to ignore alerts for various reasons:

- If a maintenance task is scheduled in a data center, alerts are received in bulk and the alert log is recorded in large numbers in OME. These are known alerts and can be ignored instead of overloading 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.

5.1 Creating alert ignore action

1. Click **New Alert Ignore Action** as shown in Figure 18 and type a name.

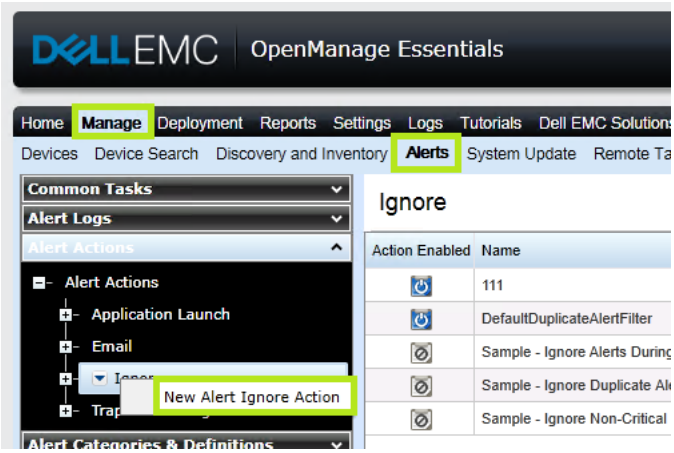

Figure 18 Creating A New Alert Ignore Action

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

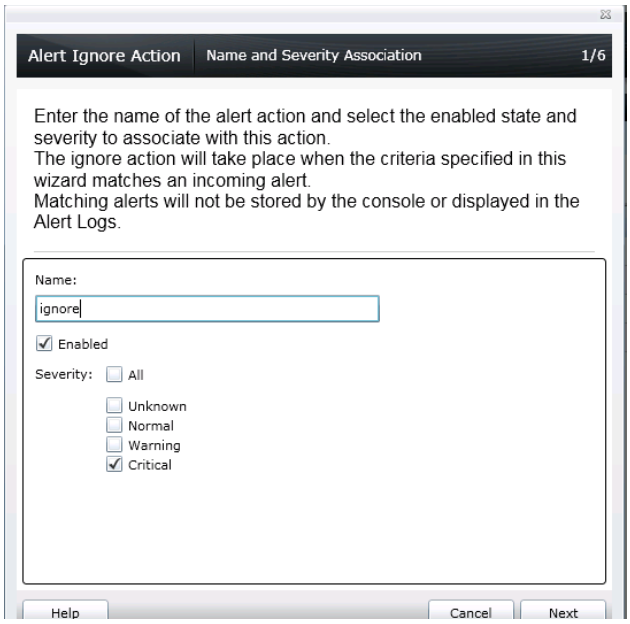

Figure 19 Name and Severity Association

3. Alert category, source, date or range, and time can be customized as described for Alert Email Action.
4. To avoid duplication of alerts, select **Yes** in the **Duplicate Alert Correlation** dialog box. Duplicate alerts received will be deleted within the specified time interval. If you select **No**, the duplicate alerts will be received in the console.

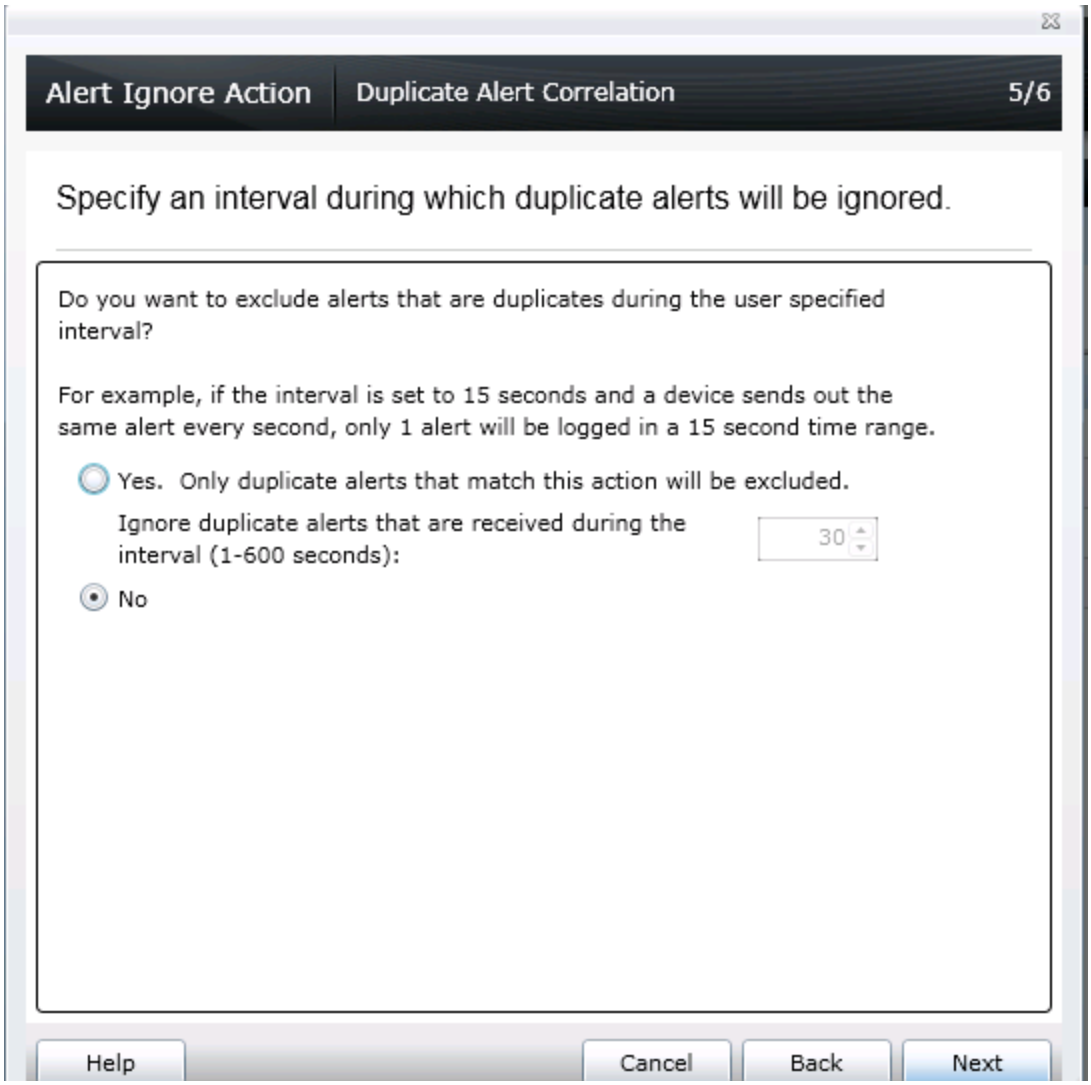

Figure 20 Duplicate Alert Correlation

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

Conclusion

Using OME, an IT administrator can remotely manage business critical servers or devices. 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 to manage the data center from a single master OME console.