
Enhancements to iDRAC7 Alert Notification

This Dell white paper discusses the improvements made to the iDRAC7 version 1.30.30 alerting capabilities

Kareem Fazal

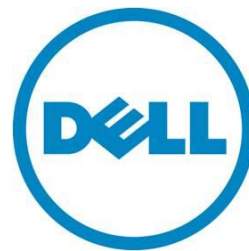
Test Engineer
Enterprise Software Validation

Cori Rizzo

Test Engineer
Enterprise Software Validation

Sanjeev Singh

Firmware Engineer
Enterprise Firmware



Contents

Executive summary	3
Introduction	3
Feature enhancements	3
Filtering alerts by category and severity levels	4
Setting event alerts	5
Email alerts	6
SNMP Trap alerts	8
IPMI PET alerts	10
Remote System Log alerts	12
WS Eventing alerts	13
Testing configured events	14
Configuring network settings for alerts	14
Summary	15

Figures

Figure 1. Alert categories and severity levels	4
Figure 2. Alert types	5
Figure 3. Email alert configuration	6
Figure 4. Authenticated email alert configuration	6
Figure 5. Configuring SNMP Trap alerts	8
Figure 6. Setting a destination address	9
Figure 7. Sample alert for a chassis intrusion event	11
Figure 8. Configuring Remote System Log alerts	12
Figure 9. Remote Syslog Settings	12
Figure 10. Configuring WS Eventing alerts	13
Figure 11. Testing a configured event	14

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.

© 2013 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, OpenManage, and PowerEdge are trademarks of Dell Inc. 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.

Executive summary

Alerts and actions can be set for certain events that occur on Dell™ PowerEdge™ servers. Event alerts provide immediate notification about an event, plus information about the action the system requires to address the event.

The newest version of the Integrated Dell Remote Access Controller (iDRAC7 version 1.30.30) for Dell PowerEdge 12th generation servers support more types of alert mechanisms and improves the user experience through an updated web interface. With the latest enhancements, all of the alert features now focus more on out-of-band support without the need to install additional host software.

Introduction

The iDRAC7 with Lifecycle Controller is a Dell systems management solution for Dell PowerEdge servers. These controllers provide a way of proactively notifying IT administrators of abnormalities, called events, that may cause interruptions or system failure.

Events occur when the status of a component is outside the range of a predefined condition. An event notification occurs when alerts and actions are set. If an event matches a filter, and the filter is configured to generate an alert, an alert is sent to a preconfigured destination.

Alerts can take the form of an email alert, Simple Network Management Protocol (SNMP) alert, Intelligent Platform Management Interface (IPMI) alert, remote system log (syslog) alert, or Web Services (WS) Events alert. Each individual event can also be set with a different system action including power cycle, reboot, and power off.

To arrange immediate notification in the case of an event, you can set alerts and actions using the iDRAC7 web interface or command-line interface (CLI). Alerts provide information about events and allow you or the system to take the necessary action to remedy an event before a system failure occurs causing costly downtime in the data center. iDRAC7 now supports more types of alerts and offers an improved, user-friendly web interface.

Feature enhancements

Management controllers on previous generation Dell servers—early DRAC and iDRAC versions, and the baseboard management controller (BMC)—supported only Platform Event Trap (PET) alerts. These IPMI alerts were confined to events generated by IPMI sensors, and did not include events generated by subsystems such as storage or memory.

Additionally, only servers with Dell OpenManage™ Server Administrator (OMSA) could send SNMPv1 alerts. With the latest version of iDRAC7, SNMP alerts no longer require an operating system or agent such as OMSA. With the latest enhancements to the alert notification feature in iDRAC7, monitoring your PowerEdge systems is easier than ever. These feature enhancements include:

- [Out-of-band SNMP alerts](#)
- [Authenticated email alerts](#)
- [Events logging to remote syslog](#)

- [Additional alert subsystem categories](#)
- Column-separated information, such as severity type (info, warning, and critical), category type, and action type
- Recommended actions specified for each alert
- [Support for SNMPv1 and SNMPv2 alerts](#)
- No requirement for an operating system agent for SNMP alerts, meaning no additional software installations for the host operating system
- Fully qualified domain name supported for email, SNMP, and IPMI alert destinations
- [Capability for testing configured events](#)

Filtering alerts by category and severity levels

You can sort and search for alerts by either category or severity using the iDRAC7 web interface. Supported alert category types include:

- System Health
- Storage
- Configuration
- Audit
- Updates
- Work Notes

Supported alert severity types include:

- Critical
- Warning
- Informational

You can select as many alert categories or severity levels as you need when searching for alerts. See Figure 1.

Figure 1. Alert categories and severity levels

Alerts Filter		▲ Back to Top
Category:		Severity:
<input checked="" type="checkbox"/> System Health	<input checked="" type="checkbox"/> Audit	<input checked="" type="checkbox"/> Informational
<input checked="" type="checkbox"/> Storage	<input checked="" type="checkbox"/> Updates	<input checked="" type="checkbox"/> Warning
<input checked="" type="checkbox"/> Configuration	<input checked="" type="checkbox"/> Work Notes	<input checked="" type="checkbox"/> Critical
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>		

Note: Alert filters are session based. The selected alert filters will revert to the default state once you refresh the page or end the session.

Setting event alerts

You can configure iDRAC7 to send alerts to configured destinations for a variety of events. The types of event alerts, as shown in Figure 2, include the following:

- Email
- SNMP Trap
- IPMI
- Remote System Log
- WS Eventing

Figure 2. Alert types

[Back to Top](#)

Alerts and Remote System Log Configuration								
Category	Alert	Severity	Email	SNMP Trap	IPMI Alert	Remote System Log	WS Eventing	Action
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Voltage		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Reboot
System Health	Voltage		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Power Cycle
Storage	Battery Event		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
Storage	Battery Event		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
Storage	Battery Event		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
Storage	Storage Contr		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
Storage	Storage Contr		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
Storage	Storage Contr		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action

Page 9 of 13

You can configure alerts using the iDRAC7 web interface or the Remote Access Controller Admin utility (RACADM) CLI. For more information on the web interface, see the online help or the [Integrated Dell Remote Access Controller 7 \(iDRAC7\) Version 1.30.30 User's Guide](#). For more information on the CLI, see the [RACADM Command Line Reference Guide for iDRAC7 1.30.30 and CMC 4.3](#).

Email alerts

Configuring email alerts using the iDRAC7 web interface

1. Select **Overview > Server > Alerts > SNMP Traps and Email Settings**.
2. Select **State** and enter the destination email address and the email server address.
3. Click **Send** under **Test Email** to test the configured email alert settings.
4. Click **Apply**.

Figure 3. Email alert configuration

Destination E-mail Addresses

E-mail Alert Number	State	Destination E-mail Address	Test E-mail
E-mail Alert 1	<input checked="" type="checkbox"/>	<input type="text" value="test@delllab"/>	<input type="button" value="Send"/>
E-mail Alert 2	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Send"/>
E-mail Alert 3	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Send"/>
E-mail Alert 4	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Send"/>

To use the new authenticated email alert option:

1. Select **Enable Authentication**.
2. Enter the **Username** and **Password** for the user who has access to SMTP server.
3. Enter a valid IP address or the fully qualified domain name (FQDN) of the SMTP server in the **SMTP (Email) Server IP Address or FQDN/DNS Name** field.

Authenticated email alerts require a username and password to access the domain where the mail server is located. Transport Layer Security (TLS) is used and credentials are verified before emails are delivered.

Figure 4. Authenticated email alert configuration

SMTP (E-Mail) Server Address Settings

Attribute	Value
Enable Authentication	<input checked="" type="checkbox"/>
Username	<input type="text" value="test"/>
Password	<input type="password" value="•••••"/>
SMTP (E-mail) Server IP Address or FQDN / DNS Name	<input type="text" value="172.17.0.4"/>

Configuring email alerts using RACADM commands

To configure the SMTP email server:

set command

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP Email Server IP Address>
```

config command

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr <SMTP Email Server IP Address>
```

To enable email alerts:

config command

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i [index] [0|1]
```

where [index] is the email destination index and 0 disables the email alert or 1 enables the alert

The email destination index can be a value from 1 through 4. For example, to enable email with index 4, use the following command:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

set command

```
racadm set iDRAC.EmailAlert.Enable.[index] 1
```

where [index] is the email destination index and 0 disables the email alert or 1 enables the alert

The email destination index can be a value from 1 through 4. For example, to enable email with index 4, enter the following command:

```
racadm set iDRAC.EmailAlert.Enable.4 1
```

To configure email settings:

config command

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 [email-address]
```

where 1 is the email destination index and [email-address] is the destination email address that receives the platform event alerts

set command

```
racadm set iDRAC.EmailAlert.Address.1 [email-address]
```

where 1 is the email destination index and [email-address] is the destination email address that receives the platform event alerts

To configure a custom message:

config command

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i [index]
[custom-message]
```

where [index] is the email destination index and [custom-message] is the custom message

set command

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

where [index] is the email destination index and [custom-message] is the custom message

To test the configured email alert, if required:

```
racadm testemail -i [index]
```

where [index] is the email destination index to test

SNMP Trap alerts

In previous generations of Dell PowerEdge servers, SNMP alerts were supported only for in-band through OMSA. The Dell PowerEdge 12th generation servers with iDRAC7 support SNMP out-of-band alerts. SNMP trap alerts are currently supported in two different types of formats: SNMPv1 and SNMPv2.

Configuring SNMP trap alerts using the iDRAC7 web interface

You can configure SNMP alerts for any alert category by selecting the check box under **SNMP Trap** to enable an SNMP alert for the event category. See Figure 5.

Figure 5. Configuring SNMP Trap alerts

Alerts and Remote System Log Configuration ▲ Back to Top

Page 5 of 13

Category	Alert	Severity	Email	SNMP Trap	IPMI Alert	Remote System Log	WS Eventing	Action
System Health	Power Supply		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Power Supply		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Power Supply		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	PSU Absent		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Power Usage		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Power Usage		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Power Usage		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Redundancy		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action

Page 5 of 13 Apply

You can then configure up to eight destination addresses for delivery of any SNMP alert. You can configure the destination address using IPv4 address, IPv6 address, or a FQDN. See Figure 6.

To receive the SNMP alert, the community string for iDRAC needs to be the same as the destination community string. By default, the value of the iDRAC community string is set to **public**. See Figure 6.

Figure 6. Setting a destination address

The screenshot shows the 'SNMP Traps and E-mail Settings' configuration page. At the top, there are tabs for 'Alerts', 'SNMP and E-mail Settings', and 'Alert Recurrence'. The main heading is 'SNMP Traps and E-mail Settings'. Below this is the 'IP Destination List' section, which contains a table with the following columns: Destination Number, State, Destination Address, Test IPMI Trap, and Test SNMP Trap. The table has 8 rows, each representing an alert destination. The first three rows are checked in the State column and have their respective Destination Address fields populated with 'idrac-4N9BBBB', 'fe80::d6ae:52ff:fea0:af51', and '172.17.0.50'. The remaining five rows are unchecked and have empty Destination Address fields. Below the table is a 'Community String' field with the value 'public'. An 'Apply' button is located at the bottom right of the IP Destination List section. Below this is the 'SNMP Trap Format' section, which has two radio button options: 'SNMP v1' (selected) and 'SNMP v2'. An 'Apply' button is also present at the bottom right of this section.

Destination Number	State	Destination Address	Test IPMI Trap	Test SNMP Trap
Alert Destination1	<input checked="" type="checkbox"/>	idrac-4N9BBBB	Send	Send
Alert Destination2	<input checked="" type="checkbox"/>	fe80::d6ae:52ff:fea0:af51	Send	Send
Alert Destination3	<input checked="" type="checkbox"/>	172.17.0.50	Send	Send
Alert Destination4	<input type="checkbox"/>		Send	Send
Alert Destination5	<input type="checkbox"/>	::	Send	Send
Alert Destination6	<input type="checkbox"/>	::	Send	Send
Alert Destination7	<input type="checkbox"/>	::	Send	Send
Alert Destination8	<input type="checkbox"/>	::	Send	Send

Community String: public

SNMP Trap Format:

- SNMP v1
- SNMP v2

Configuring SNMP trap alerts using RACADM commands

To configure the trap destination address for IPv4:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i [index]
[IP-address]
```

where [index] is the trap destination index and [IP-address] is the destination IP address of the system that receives the platform event alerts

To configure the trap destination address for IPv6:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i
[index] [IP-address]
```

where [index] is the trap destination index and [IP-address] is the destination IP address of the system that receives the platform event alerts

To configure the SNMP community name string:

config command

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName [name]
where [name] is the SNMP Community Name
```

set command

```
racadm set iDRAC.SNMP.AgentCommunity [name]
where [name] is the SNMP Community Name
```

To test the trap, if required:

```
racadm testtrap -i [index]
where [index] is the trap destination index
```

To configure the trap format:

```
racadm set iDRAC.SNMP.TrapFormat [format]
where [format] is the SNMP v1 or SNMP v2 format; the value can either be set to 0 or 1
```

IPMI PET alerts

Most Dell PowerEdge servers with iDRAC7 support IPMI PET alerts. The IPMI trap event format is specified in the PET specification (see <http://download.intel.com/design/servers/ipmi/PET100.pdf>). To help decode IPMI trap information, Dell provides a Management Information Base (MIB) file (DcAsfSrv.mib) on the OpenManage DVD and on Support.Dell.com.

IPMI alerts are more difficult to decode than SNMP alerts. You need to correlate events with the MIB file and/or sensor information to decode an IPMI alert. You can retrieve sensor information from iDRAC7 using a standard IPMI utility, such as ipmitool, which is also located on the OpenManage DVD and on Support.Dell.com.

To demonstrate decoding an IPMI PET alert, see the sample in Figure 7 of an alert caused by a chassis intrusion event.

Figure 7. Sample alert for a chassis intrusion event

TimeStamp	61 days, 15 hours, 40 minutes, 53 seconds.
Enterprise	.iso.org.dod.internet.private.enterprises.wiredformgmt.pet.asfPetEvts
Generic Type	Enterprise Specific
Specific Type	356096
Message	.iso.org.dod.internet.private.enterprises.wiredformgmt.pet.asfPetEvts.1: 44 45 4c 4c 50 00 10 47 80 31 68 6f 73 74 2e 6e 6f 63 61 6c 64 6f 6d 61 69 6e 00 c1:
Severity	Clear
Entity	10.210.136.169

In the trap details, note the contents of the **Specific Type** field, which are 356096 in this sample. Match 356096 to the DcAsfSrv.mib file, which has the following information for a chassis intrusion event:

```
-- Intrusion --
-- Intrusion
asfTrapCaseIntrusion TRAP-TYPE
ENTERPRISE asfPetEvts
DESCRIPTION
"Chassis Intrusion - Physical Security Violation"
--#SUMMARY    "Chassis Intrusion - Physical Security Violation"
--#ARGUMENTS  {}
--#SEVERITY   CRITICAL
::= 356096
```

You can also decode the contents of the **Message** field using the PET specification, which indicates a number of items such as the sensor number and the event severity.

Remote System Log alerts

Using iDRAC7 for Dell PowerEdge 12th generation servers, you can configure alerts to be send to a remote syslog. To send an event alert to a remote syslog sever, select the corresponding check box under **Remote System Log**. See Figure 8.

Figure 8. Configuring Remote System Log alerts

Alerts and Remote System Log Configuration ▲ Back to Top

Page 3 of 13

Category	Alert	Severity	Email	SNMP Trap	IPMI Alert	Remote System Log	WS Eventing	Action
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Hardware Config		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Hardware Config		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Memory		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Memory		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Memory		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	NIC Config		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	NIC Config		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	OS Event		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action

Page 3 of 13 Apply

Note: Remote syslog is an Enterprise level license feature, and is not available at the Express level.

Configuring remote syslog in the iDRAC7 web interface

1. Select **Overview > Server > Logs > Settings**.
2. Select the **Remote Syslog Enabled** check box.
3. To define the server location, enter the destination server address in the **Syslog Server** field and enter the **Port Number**.
4. Click **Apply**.

Figure 9. Remote Syslog Settings

Properties Console Attached Media vFlash Logs Job Queue

Logs Settings Lifecycle Log

Remote Syslog Settings

Remote Syslog Enabled	<input checked="" type="checkbox"/>
Syslog Server1	<input type="text" value="192.168.201.62"/>
Syslog Server2	<input type="text"/>
Syslog Server3	<input type="text"/>
Port Number	<input type="text" value="514"/>

Apply

Configuring remote syslog using RACADM commands

To enable remote syslog:

config command

```
racadm config -g cfgRemotehosts -o cfgRhostsSyslogEnable [number] -
where [number] is to disable [0] or enable [1] the remote syslog
```

set command

```
racadm set iDRAC.Syslog.SyslogEnable [number]
where [number] is to disable [0] or enable [1] the remote syslog
```

To set a destination address for a remote syslog:

config command

```
racadm config -g cfgRemotehosts -o cfgRhostsSyslogServer[#] {address}
where [#] is number of the syslog server, user can configure up to 3 servers and {address} is
the IP address of the destination server
```

set command

```
racadm set iDRAC.Syslog.Server[#] {address}
where [#] is number of the syslog server, user can configure up to 3 servers and {address} is
the IP address of the destination server
```

WS Eventing alerts

For Dell PowerEdge 12th generation servers, you can set WS Eventing to receive WS Eventing notifications. In iDRAC7 1.30.30, WS Eventing only supports job control events that are found in the configuration category. WS Eventing defines a protocol for a client service (subscriber) to register interest (a subscription) with a server web service (event source) to receive the messages containing the server events (notifications or event messages).

To set WS Eventing for a configuration event, select the corresponding check box under **WS Eventing**. See Figure 10.

Figure 10. Configuring WS Eventing alerts

Alerts and Remote System Log Configuration [▲ Back to Top](#)

Page 1 of 1

Category	Alert	Severity	Email	SNMP Trap	IPMI Alert	Remote System Log	WS Eventing	Action
Configuration	DRAC IP Address		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
Configuration	Job Control		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No Action
Configuration	RAC Event		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
Configuration	Security Event		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action

Page 1 of 1

Testing configured events

After configuring alerts, you can test the configuration of each event.

1. In the iDRAC7 web interface, enter the message ID of an alert in the **Message ID to Test Event** field. See Figure 11.
For a list of valid message IDs, see the [Dell Event Message Reference](#) or the [Dell Event/Error Message Reference 2.0](#) on [Dell.com](#).
Each alert message starts with a three- or four-character code to identify the problem area. This code is followed by a three- or four-digit number that specifies the actual error.
2. Click **Test** to send the configured event to the respective SNMP, IPMI, email, remote syslog, and WS Eventing alerts.

Figure 11. Testing a configured event

The screenshot shows a web form titled "Test Event" with a "Back to Top" link in the top right corner. The form contains a single text input field labeled "Message ID to Test Event:" with the value "LIC204" entered. A "Test" button is positioned at the bottom right of the form.

Configuring network settings for alerts

For alerts to work correctly, you must configure the iDRAC7 network settings for a DNS server and a domain name. You can configure the iDRAC7 network settings using either the iDRAC7 web interface or RACADM CLI.

Configuring networks settings in the iDRAC7 web interface

1. Select **Overview > iDRAC Settings > Network**.
2. Under **Common Settings** select **Register DRAC on DNS**.
3. In the same section, either select **Auto Config Domain Name**, or enter a static **DNS Domain Name**.
4. Under **IPv4 Settings**, either select **Use DHCP to obtain DNS server addresses**, or manually enter the IP address of your DNS server.
5. For IPv6, you can use the **Autoconfiguration Enable** feature, or manually enter the IP and DNS information. When using IPv6, make sure you specify the iDRAC DNS domain name under **Common Settings**.

Configuring networks settings using RACADM commands

For instructions, see the [RACADM Command Line Reference Guide for iDRAC7 1.30.30 and CMC 4.3](#).

Summary

The alert enhancements in the iDRAC7 1.30.30 firmware release provide IT administrators with more options, methods, and granularity to manage Dell PowerEdge servers. Key improvements include:

- Improved web interface that is more user friendly
- Individual alert messages with recommended actions for resolving events
- Alerts for more subsystem categories such as storage and configuration
- Additional types of alerts including SNMP, WS Events, authenticated email, and remote syslog

Additionally, you can receive alerts for servers that have no operating system installed, and therefore, no need for installing an operating system agent such as OMSA. You can configure alert destinations using a fully qualified domain name instead of an IP address. Plus you now have the ability to search and view the newly standardized message database using the iDRAC7 web interface.

Dell continues to listen to our customers and provide features that meet the needs of the ever-changing IT world. By adding these enhancements to the alerting feature, administrators have much more flexibility to configure alerts for their specific environment.

[More information on iDRAC7 version 1.30.30](#)

For more information on iDRAC7 version 1.30.30, see [Support for Integrated Dell Remote Access Controller 7 Version 1.30.30](#) on [Dell.com](#).