Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers

This technical white paper describes the Lifecycle log and Alerts capabilities of iDRAC9 in Dell EMC PowerEdge servers.

Dell EMC Engineering
June 2017

Authors

Sreenivasula Reddy

Rochak Gupta

Kalyani Korubilli

A Dell EMC Technical White paper

Revisions

Date	Description
June 2017	Initial release

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Revisions....2

Executive summary....4

Introduction....5

1 Lifecycle log....6

1.1 Lifecycle Log categories....9

1.1.1 System Health....10

1.1.2 Storage....10

1.1.3 Configuration....10

1.1.4 Audit....11

1.1.5 Updates....11

1.1.6 Work Notes....12

2 Alert configuration....13

2.1 Email alert....14

2.2 SNMP and IPMI trap alert....16

2.3 Remote System Log....17

2.4 WS-Eventing....17

2.5 OS Log....18

2.6 Redfish Event....20

2.7 Action....20

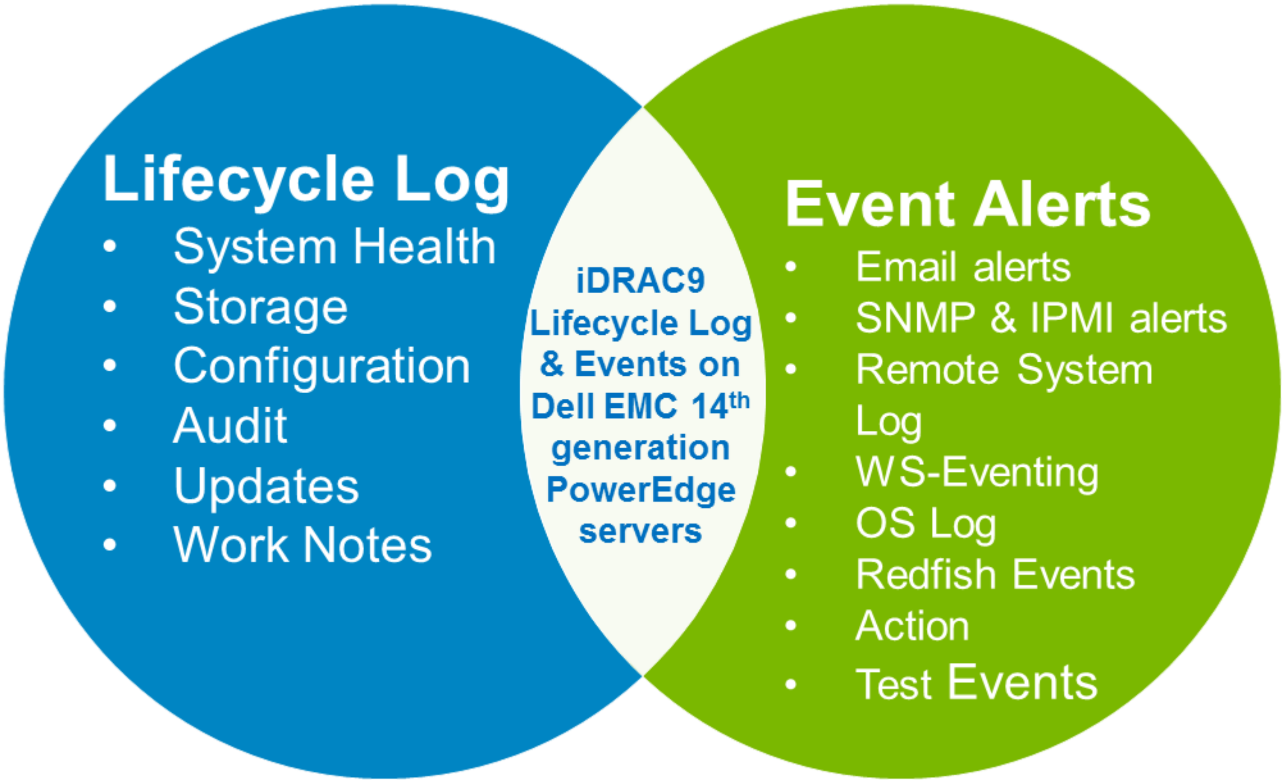
2.8 Test Event....21

2.9 Alert Configuration prerequisites....21

Conclusion....23

Executive summary

In a data center where multiple servers are located, it is difficult to troubleshoot failures in any of the systems. The iDRAC9 with Lifecycle Controller provides the Lifecycle Logs feature that records every action performed and any failures occurred on the server. System administrators and Dell technical support can make use of iDRAC Lifecycle log feature provided in the PowerEdge servers to remotely monitor the server. When a Lifecycle Log is generated, iDRAC9 enables you to configure and forward event alerts to destinations by using various ways such as email, SNMP, Redfish, and WS-Eventing.



Introduction

The Lifecycle Logs feature:

- Records events generated for any real-time software or hardware changes occurred in the server.
- Enables you to view Lifecycle log information locally or remotely by using GUI-based consoles and iDRAC supported command line interface (CLIs).
- Provides various options such as view lifecycle log, export lifecycle log, add work note, and add comments.

Alerts provide information about events with recommended action when any failure occurs. iDRAC9 supports more types of alerts and offers an improved and user-friendly web GUI to configure them. There are various Alert types such as email, SNMP, and IPMI, supported by each events. User can subscribe to any of the supported Alert types to get the event notifications to the predefined destinations. User can also configure multiple alerts for each event.

This technical white paper discusses about Lifecycle Log and different types of alerts and actions supported by iDRAC9.

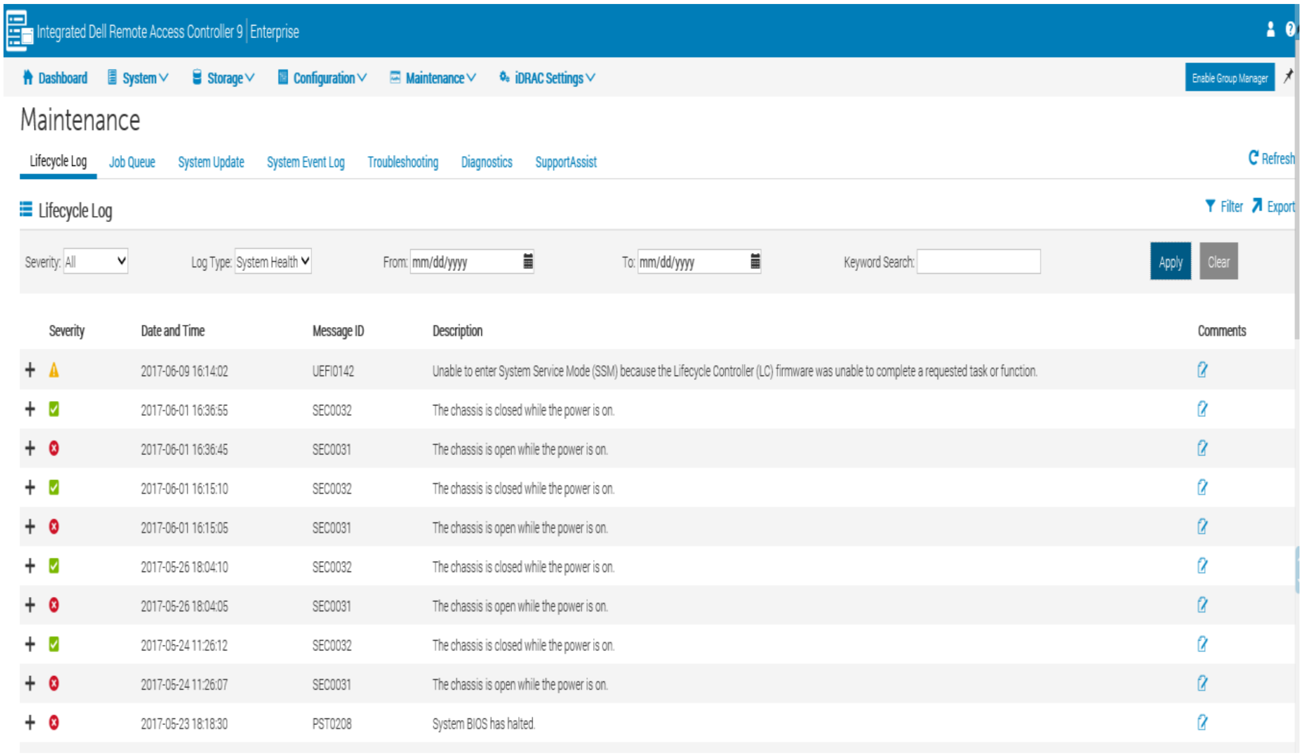
1 Lifecycle log

Lifecycle log is a collection of events and their details corresponding to events occurred in the server over a period of time. Lifecycle log provides description of events occurred with timestamps, severity, recommended actions, and other technical information that could come very handy for tracking or alert purposes.

Following are the various types of information recorded in lifecycle logs.

- Configuration Changes on the system hardware components
- iDRAC, BIOS, NIC, and RAID configuration changes
- Logs of all the remote operations
- Firmware update history based on device, version, and date
- Information about replaced parts
- Information about failed parts
- Event and error message IDs
- Host power-related events
- POST errors
- User login events
- Sensor state change events

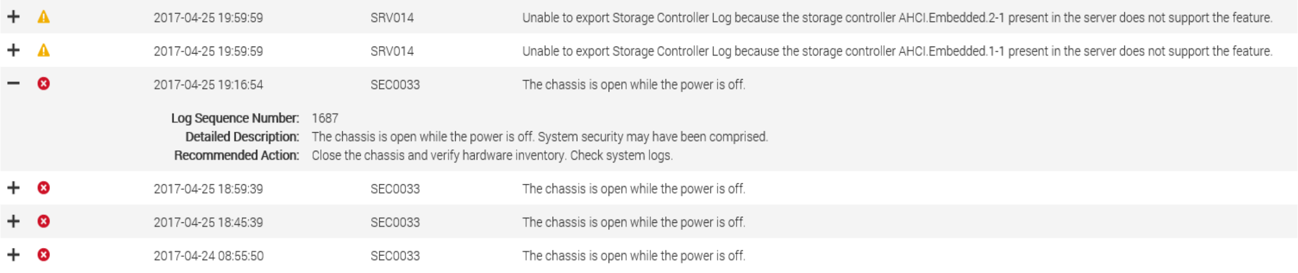
You can view the Lifecycle logs from iDRAC web GUI. To view Lifecycle Log, log in to iDRAC and click **Maintenance → Lifecycle Log**.



Severity: All
Log Type: System Health
From: mm/dd/yyyy
To: mm/dd/yyyy
Keyword Search:

	Severity	Date and Time	Message ID	Description	Comments
+	⚠	2017-06-09 16:14:02	UEFI0142	Unable to enter System Service Mode (SSM) because the Lifecycle Controller (LC) firmware was unable to complete a requested task or function.	
+	✓	2017-06-01 16:36:55	SEC0032	The chassis is closed while the power is on.	
+	✖	2017-06-01 16:36:45	SEC0031	The chassis is open while the power is on.	
+	✓	2017-06-01 16:15:10	SEC0032	The chassis is closed while the power is on.	
+	✖	2017-06-01 16:15:05	SEC0031	The chassis is open while the power is on.	
+	✓	2017-05-26 18:04:10	SEC0032	The chassis is closed while the power is on.	
+	✖	2017-05-26 18:04:05	SEC0031	The chassis is open while the power is on.	
+	✓	2017-05-24 11:26:12	SEC0032	The chassis is closed while the power is on.	
+	✖	2017-05-24 11:26:07	SEC0031	The chassis is open while the power is on.	
+	✖	2017-05-23 18:18:30	PST0208	System BIOS has halted.	

Detailed information about the log can be viewed by expanding the listed Logs.



+	⚠	2017-04-25 19:59:59	SRV014	Unable to export Storage Controller Log because the storage controller AHCI.Embedded.2-1 present in the server does not support the feature.
+	⚠	2017-04-25 19:59:59	SRV014	Unable to export Storage Controller Log because the storage controller AHCI.Embedded.1-1 present in the server does not support the feature.
−	⊗	2017-04-25 19:16:54	SEC0033	The chassis is open while the power is off.
		Log Sequence Number:	1687	
		Detailed Description:	The chassis is open while the power is off. System security may have been comprised.	
		Recommended Action:	Close the chassis and verify hardware inventory. Check system logs.	
+	⊗	2017-04-25 18:59:39	SEC0033	The chassis is open while the power is off.
+	⊗	2017-04-25 18:45:39	SEC0033	The chassis is open while the power is off.
+	⊗	2017-04-24 08:55:50	SEC0033	The chassis is open while the power is off.

Following are the details provided as part of each Lifecycle Log entry:

Severity	Each event is classified based on the impact to the system. The severity can be: **Severity 1 (Critical)** A catastrophic production problem that may severely impact production systems, or in which production systems are down or not functioning. Production data is lost and no procedural work around exists. Severity 1 problems also include issues that result in an emergency condition that causes a serious security breach. **Severity 2 (Warning)** A high-impact problem in which system operation is disrupted but there is capacity to remain productive and maintain necessary business-level operations. Severity 2 also applies to minor security breach situations. **Severity 3 (Information)** A medium-to-low impact problem that involves partial, non-critical loss of functionality. A problem that impairs some operations but allows continued function. This category includes documentation errors, and issues for which there is an easy circumvention or avoidance by the user.
Timestamp	Indicates the date and time when the event occurred.
Message ID	A unique alphanumeric identifier for the event. This identifier can be up to 8 characters long and consists of two parts: **Message ID Prefix** - Up to four alphabetic characters. **Message ID Sequence** - Up to four numeric digits
Message/ Description	The message text that is displayed to the user or logged as a result of the event.
Log Sequence Number	Indicates a sequence number for the log entry.
Detailed Description	Provides additional detailed description for the action or event.
Recommended Action	The description of the recommended action to be taken by the user to resolve the situation after having been notified of exception, error or event.
Category/ Log type	Provides the domain or the agent name from where the message is Logged. Lifecycle Log messages are categorized based on the operations it belong to. Below are the list of categories: • System Health • Storage

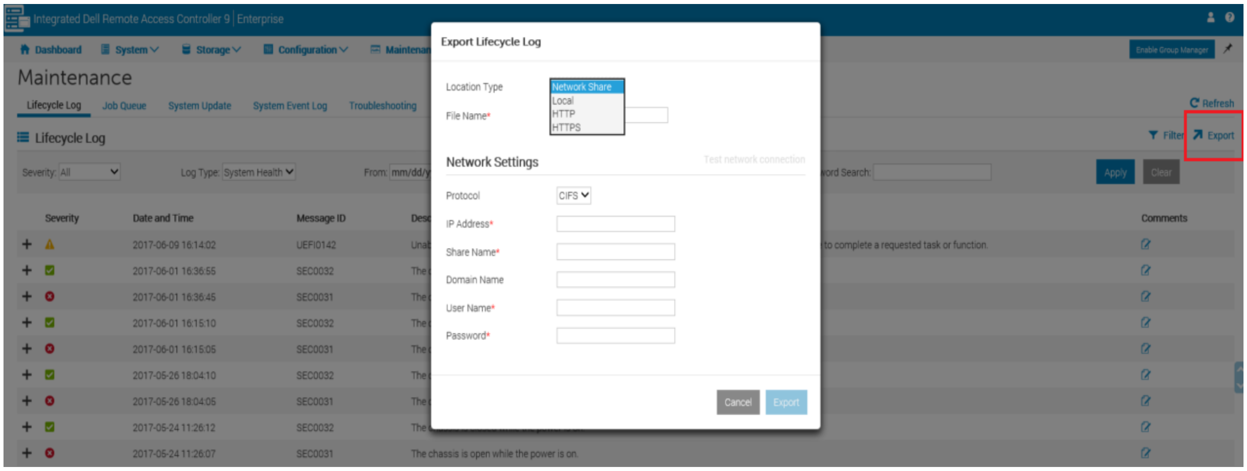
	• Configuration • Audit • Updates • Work Notes

The Lifecycle Log contains events related to system, storage devices, network devices, firmware updates, configuration changes, license messages, and so on. However, the system events are also available as a separate log called the System Event Log (SEL). When a system event occurs on a managed system, it is recorded in the SEL. The storage capacity of SEL events are limited and hence they get overwritten beyond 1024 entries. In order to ensure no event is lost the same SEL entries are replicated in the Lifecycle Log.

iDRAC stores up to 1 MB of active Lifecycle Log data. If the size of active logs exceed 90% of the space, the data is compressed and moved to archive partition. 10 MB is the size limit of archive partition. After the log data exceeds 10 MB size, the oldest archived data file is deleted to make storage space for the new archived data.

You can view only active logs from the iDRAC GUI. You can transfer the complete log data including archived logs to remote or local location by using the Export Lifecycle Log feature.

1. To export the Lifecycle Log data, on the **Maintenance** page, click **Export** in the upper-right corner.
2. In the **Export Lifeycle Log** dialog box, type or select data to transfer the logs to the local or remote share.



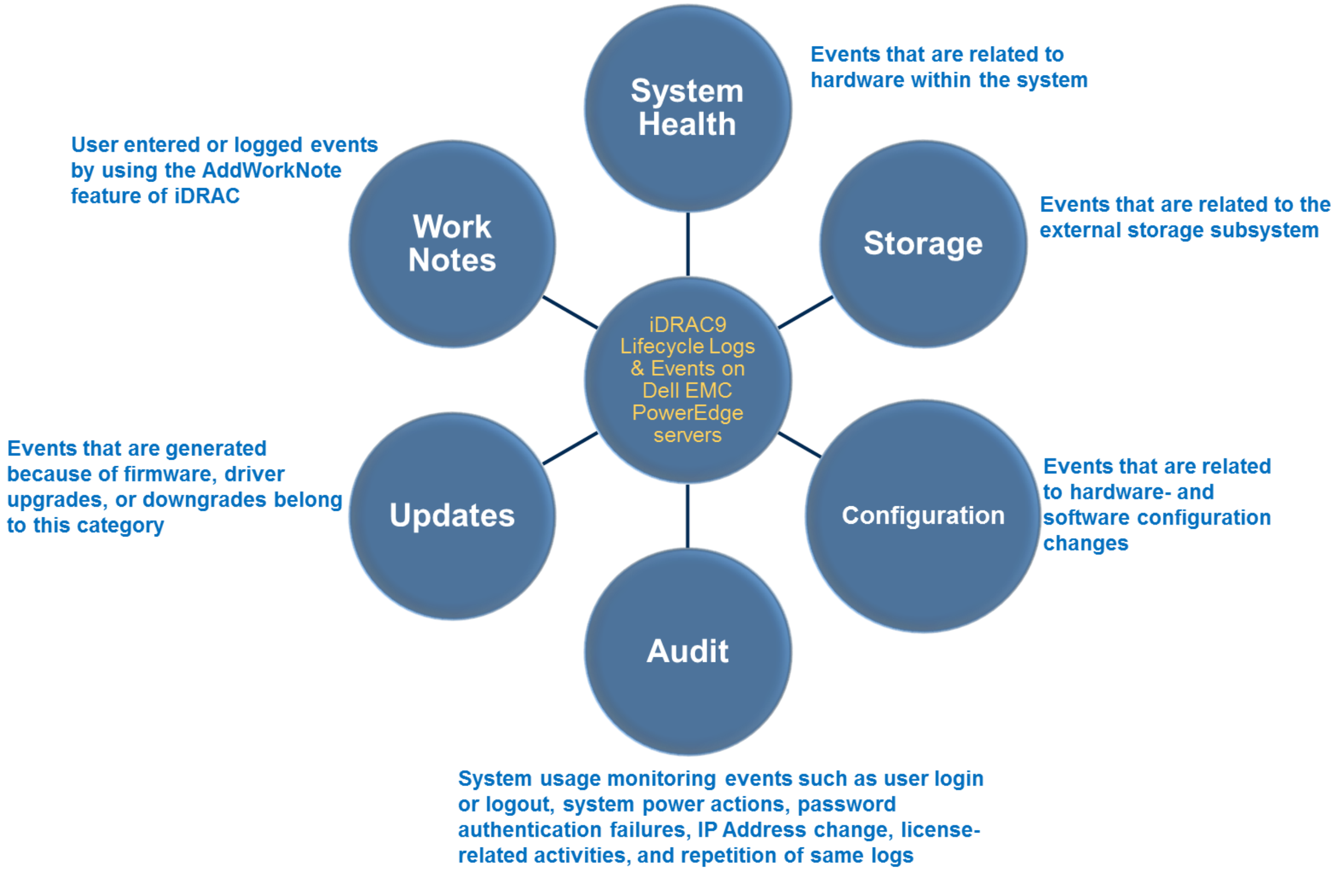
Severity	Date and Time	Message ID	Desc	Comments
⚠	2017-06-09 16:14:02	UEFI0142	Unab … to complete a requested task or function.	
✓	2017-06-01 16:36:55	SEC0032	The	
⊗	2017-06-01 16:36:45	SEC0031	The	
✓	2017-06-01 16:15:10	SEC0032	The	
⊗	2017-06-01 16:15:05	SEC0031	The	
✓	2017-05-26 18:04:10	SEC0032	The	
⊗	2017-05-26 18:04:05	SEC0031	The	
✓	2017-05-24 11:26:12	SEC0032	The	
⊗	2017-05-24 11:26:07	SEC0031	The chassis is open while the power is on.	

3. Click **Export**.
   The Lifecycle Log data is exported to the specified destination folder.
   Using the Alert Configuration feature of iDRAC, you can configure event alerts to be forwarded, and set up actions to be performed when a Lifecycle Log event occurs. Various types of alert filters and alert configuration are described in the later sections of this technical white paper.

1.1 Lifecycle Log categories

Lifecycle Logs are categorized into different groups based on domain or the agent from where event is logged. Following are the list of the categories and their details.

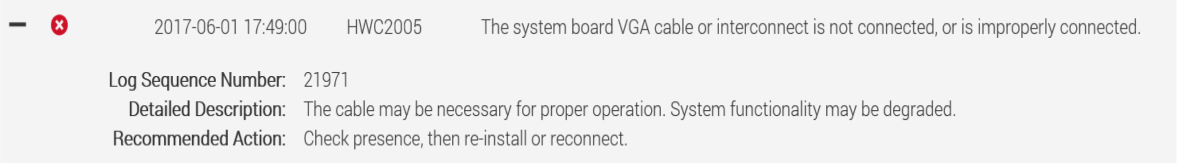
- System Health
- Storage
- Configuration
- Audit
- Updates
- Work Notes



System Health
Events that are related to hardware within the system
Work Notes
User entered or logged events by using the AddWorkNote feature of iDRAC
Storage
Events that are related to the external storage subsystem
iDRAC9 Lifecycle Logs & Events on Dell EMC PowerEdge servers
Updates
Events that are generated because of firmware, driver upgrades, or downgrades belong to this category
Configuration
Events that are related to hardware- and software configuration changes
Audit
System usage monitoring events such as user login or logout, system power actions, password authentication failures, IP Address change, license-related activities, and repetition of same logs

1.1.1 System Health

This category represents the events that are related to hardware within the system. For example, logs related to Power Supply Units (PSUs), Chassis, vFlash, battery, processor, and network adapters. Screen shot shows a sample event log related to System Health.

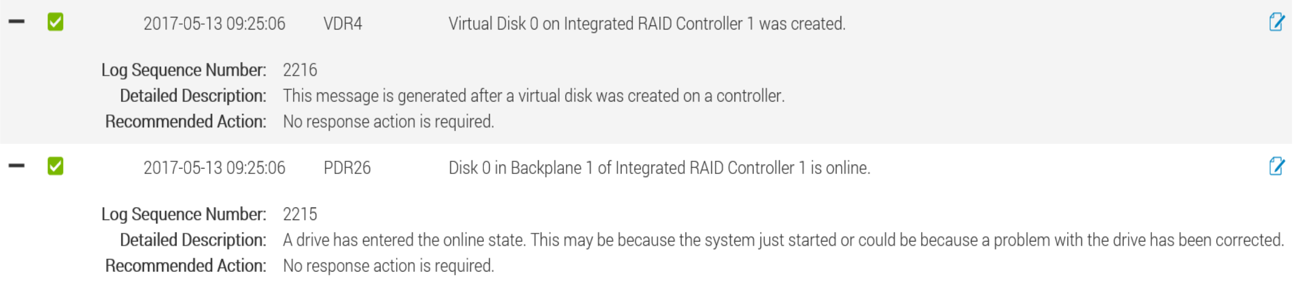


− ✗ 2017-06-01 17:49:00 HWC2005 The system board VGA cable or interconnect is not connected, or is improperly connected.

Log Sequence Number: 21971
Detailed Description: The cable may be necessary for proper operation. System functionality may be degraded.
Recommended Action: Check presence, then re-install or reconnect.

1.1.2 Storage

The storage category represents events that are related to the external storage subsystem. For example, logs related to storage controller, enclosure, hard drives, virtual drives, and SWRAID. Screen shot shows a sample event log related to Storage.



− ✓ 2017-05-13 09:25:06 VDR4 Virtual Disk 0 on Integrated RAID Controller 1 was created.

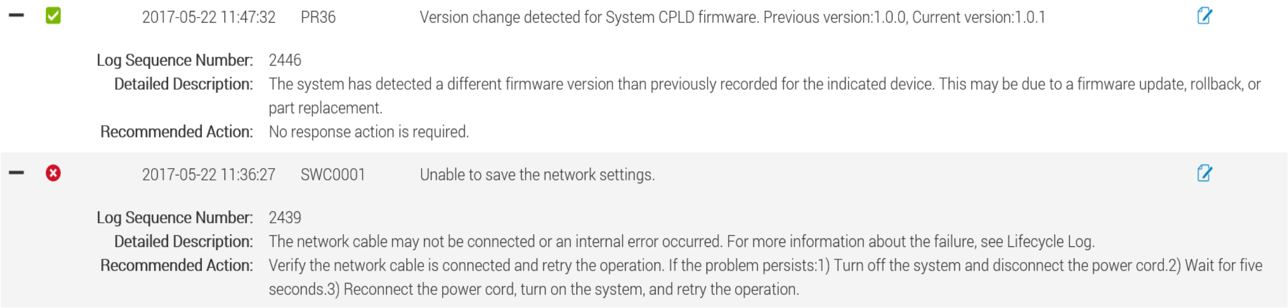
Log Sequence Number: 2216
Detailed Description: This message is generated after a virtual disk was created on a controller.
Recommended Action: No response action is required.

− ✓ 2017-05-13 09:25:06 PDR26 Disk 0 in Backplane 1 of Integrated RAID Controller 1 is online.

Log Sequence Number: 2215
Detailed Description: A drive has entered the online state. This may be because the system just started or could be because a problem with the drive has been corrected.
Recommended Action: No response action is required.

1.1.3 Configuration

This category mainly represents events that are related to hardware- and software configuration changes. The hardware configuration changes include any new additions or removal of hardware from the system. For example, CPU, Memory, and PCI-e card. The software configuration information includes any configuration changes in the system. Screen shot shows a sample event log related to Configuration.



− ✓ 2017-05-22 11:47:32 PR36 Version change detected for System CPLD firmware. Previous version:1.0.0, Current version:1.0.1

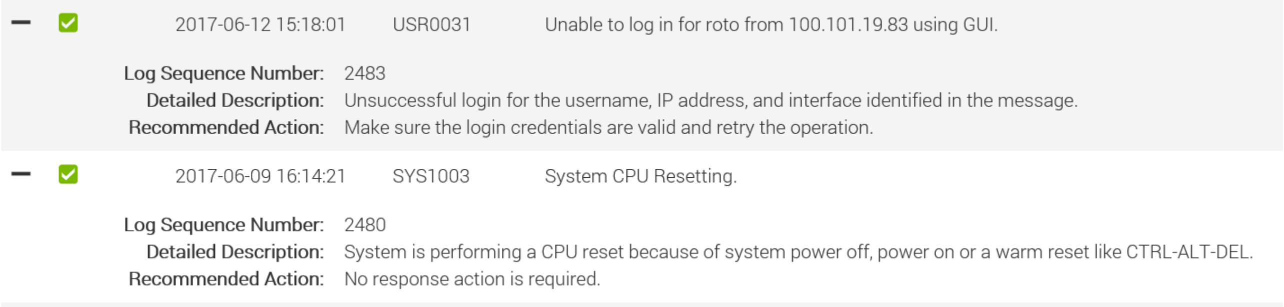
Log Sequence Number: 2446
Detailed Description: The system has detected a different firmware version than previously recorded for the indicated device. This may be due to a firmware update, rollback, or part replacement.
Recommended Action: No response action is required.

− ✗ 2017-05-22 11:36:27 SWC0001 Unable to save the network settings.

Log Sequence Number: 2439
Detailed Description: The network cable may not be connected or an internal error occurred. For more information about the failure, see Lifecycle Log.
Recommended Action: Verify the network cable is connected and retry the operation. If the problem persists:1) Turn off the system and disconnect the power cord.2) Wait for five seconds.3) Reconnect the power cord, turn on the system, and retry the operation.

1.1.4 Audit

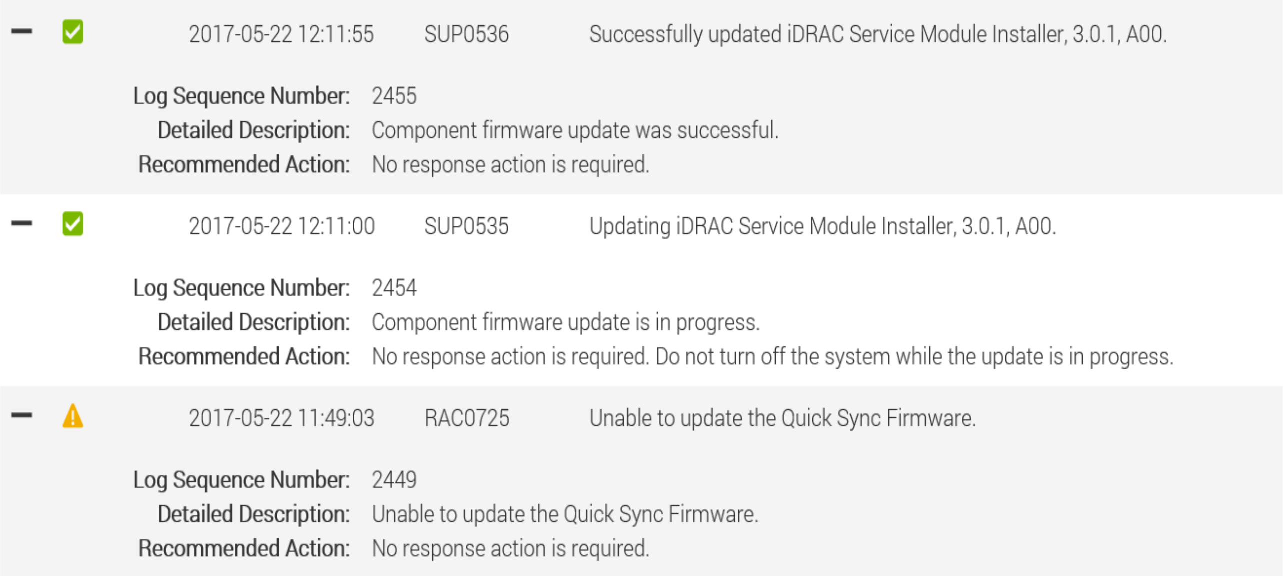
Audit category of events are used to represent system usage monitoring events such as user login or logout, system power actions, password authentication failures, IP Address change, license-related activities, and repetition of same logs. Screen shot shows a sample event log related to Audit.



```
−  ✓   2017-06-12 15:18:01   USR0031   Unable to log in for roto from 100.101.19.83 using GUI.

       Log Sequence Number:  2483
       Detailed Description: Unsuccessful login for the username, IP address, and interface identified in the message.
        Recommended Action:  Make sure the login credentials are valid and retry the operation.

−  ✓   2017-06-09 16:14:21   SYS1003   System CPU Resetting.

       Log Sequence Number:  2480
       Detailed Description: System is performing a CPU reset because of system power off, power on or a warm reset like CTRL-ALT-DEL.
        Recommended Action:  No response action is required.
```

1.1.5 Updates

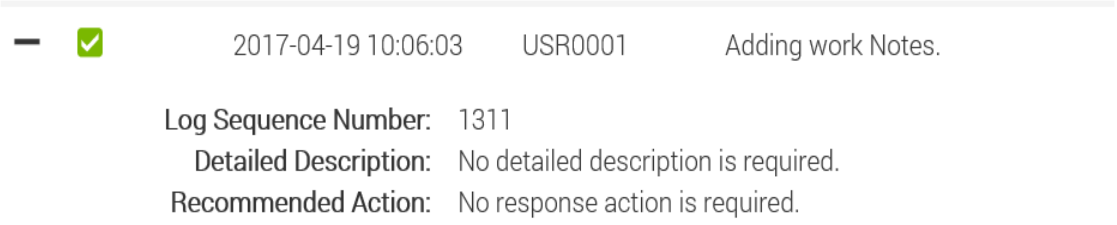
All events that are generated because of firmware, driver upgrades, or downgrades belong to this category. Screen shot shows a sample event log related to Updates.



```
−  ✓   2017-05-22 12:11:55   SUP0536   Successfully updated iDRAC Service Module Installer, 3.0.1, A00.

       Log Sequence Number:  2455
       Detailed Description: Component firmware update was successful.
        Recommended Action:  No response action is required.

−  ✓   2017-05-22 12:11:00   SUP0535   Updating iDRAC Service Module Installer, 3.0.1, A00.

       Log Sequence Number:  2454
       Detailed Description: Component firmware update is in progress.
        Recommended Action:  No response action is required. Do not turn off the system while the update is in progress.

−  ⚠   2017-05-22 11:49:03   RAC0725   Unable to update the Quick Sync Firmware.

       Log Sequence Number:  2449
       Detailed Description: Unable to update the Quick Sync Firmware.
        Recommended Action:  No response action is required.
```

1.1.6 Work Notes

User entered or logged events by using the AddWorkNote feature of iDRAC. Severity of theses logs will be always informational (Severity 3). Screen shot shows a sample event log related to Work Notes.



− ☑ 2017-04-19 10:06:03 USR0001 Adding work Notes.

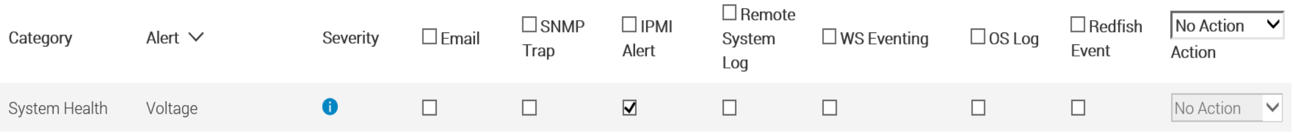
Log Sequence Number: 1311

Detailed Description: No detailed description is required.

Recommended Action: No response action is required.

2 Alert configuration

Alert Configuration feature in iDRAC provides capability to configure different types of Event Alerts to be forwarded and set up actions to be performed when a Lifecycle Logs event occurs. Event Alert filters are combination of category, sub-category, and severity. For example, event messages that belong to the System Health category, Voltage sub-category, and severity 3 (information) are grouped in to one alert filter. For this event type, if user configures IPMI alert type, an event will be forwarded from iDRAC to destination address by using IPMI alert mechanism when an event of this filter category is generated.



Category	Alert ∨	Severity	□ Email	□ SNMP Trap	□ IPMI Alert	□ Remote System Log	□ WS Eventing	□ OS Log	□ Redfish Event	No Action ∨ Action
System Health	Voltage	ℹ	□	□	☑	□	□	□	□	No Action ∨

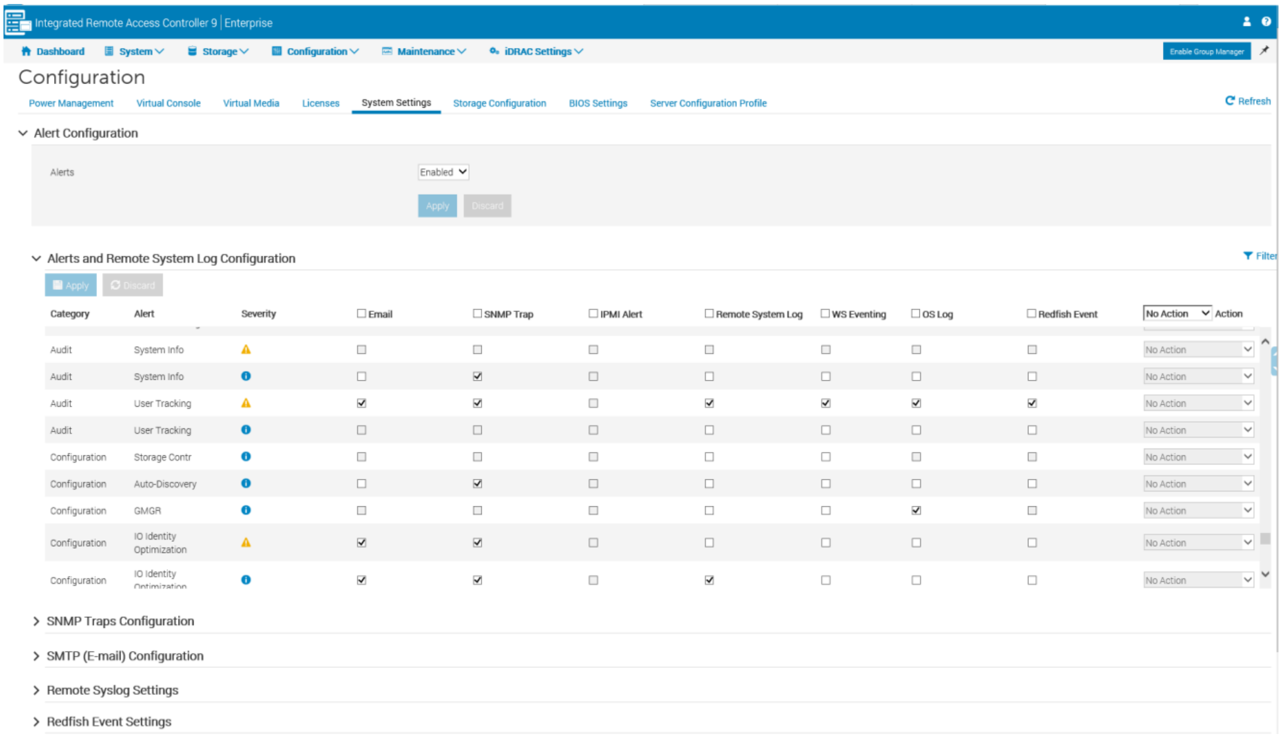
When an event is generated, it is forwarded to the configured destinations by using the selected alert type mechanisms. iDRAC supports different types of alerts such as:

- Email alert
- SNMP and IPMI trap alert
- Remote System Log
- WS-Eventing
- OS Log
- Redfish Event
- Action
- Test Event

To go to the Alert and Remote System Log Configuration section, click **Configuration → System Setting → Alert and Remote System Log Configuration**. On this page, you can configure alerts for any alert category by selecting the check box of particular alert type for the event category.

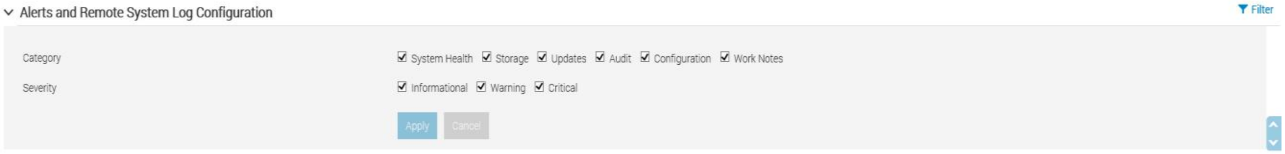
There are permitted and non-permitted alert types for each filters. Not all Alert types can be configured for all the Alert filters. By default, there are default alert types enabled for the few filters. User is allowed to disable the default selection of Alert type.

Note: A check box is greyed out if the alert type is not permitted for the particular alert filter.



Category	Alert	Severity	□ Email	□ SNMP Trap	□ IPMI Alert	□ Remote System Log	□ WS Eventing	□ OS Log	□ Redfish Event	No Action Action
Audit	System Info	⚠	□	□	□	□	□	□	□	No Action
Audit	System Info	ℹ	□	☑	□	□	□	□	□	No Action
Audit	User Tracking	⚠	☑	☑	□	☑	☑	☑	☑	No Action
Audit	User Tracking	ℹ	□	□	□	□	□	□	□	No Action
Configuration	Storage Contr	ℹ	□	□	□	□	□	□	□	No Action
Configuration	Auto-Discovery	ℹ	□	☑	□	□	□	□	□	No Action
Configuration	GMGR	ℹ	□	□	□	□	□	☑	□	No Action
Configuration	IO Identity Optimization	⚠	☑	☑	□	□	□	□	□	No Action
Configuration	IO Identity Optimization	ℹ	☑	☑	□	☑	□	□	□	No Action

You can sort and search for alerts by either category or severity using iDRAC9 GUI.



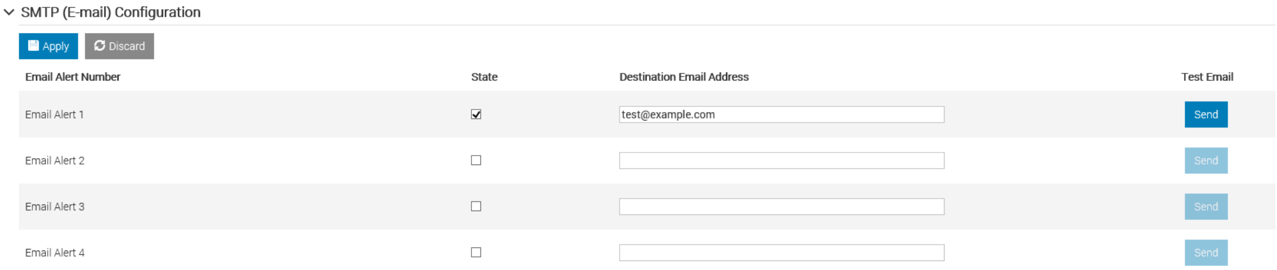
Category ☑ System Health ☑ Storage ☑ Updates ☑ Audit ☑ Configuration ☑ Work Notes

Severity ☑ Informational ☑ Warning ☑ Critical

2.1 Email alert

To configure email alerts:

1. Log in to the iDRAC Web GUI.
2. Click **Configuration → System Setting → Alert Configuration → SMTP (E-mail) Configuration**.
3. Type the destination email address and select the corresponding **State** check box to indicate that the SMTP email alert is enabled by default. You can configure up to four email address.
4. To test connection between the host and destination, click **Send** corresponding to the alert.
5. Click **Apply**.

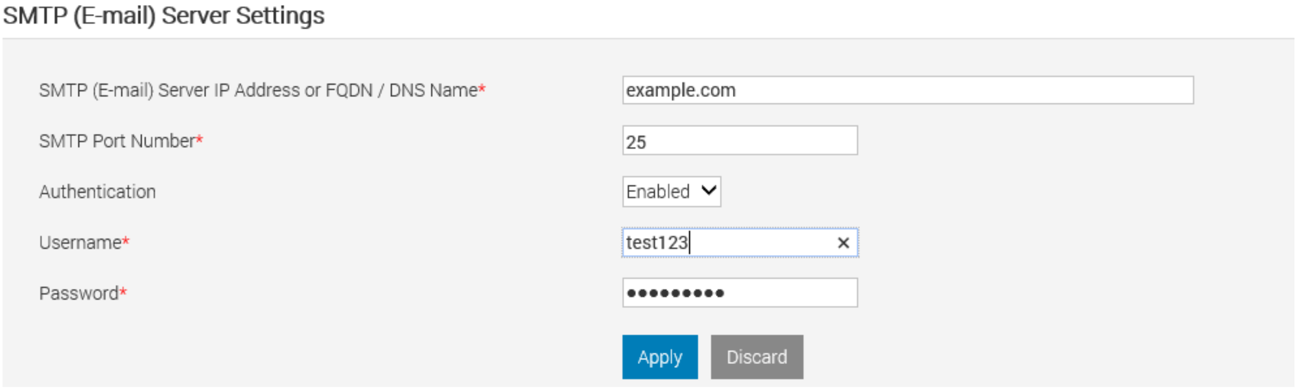

SMTP (E-mail) Configuration

Email Alert Number	State	Destination Email Address	Test Email
Email Alert 1	☑	test@example.com	Send
Email Alert 2	□		Send
Email Alert 3	□		Send
Email Alert 4	□		Send

To configure SMTP Server Settings for additional authentication:

1. Log in to the iDRAC GUI.
2. Click **Configuration → System Setting → Alert Configuration → SMTP (E-mail) Configuration**.
3. Type a valid IP Address or a Fully Qualified Domain Name (FQDN) of the SMTP.
4. Type a valid SMTP port number. The SMTP default port number is 25. Permitted port range is 1–65535.
5. If authentication is enabled, type credentials of the user who can access the SMTP.
6. Click **Apply**.

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.

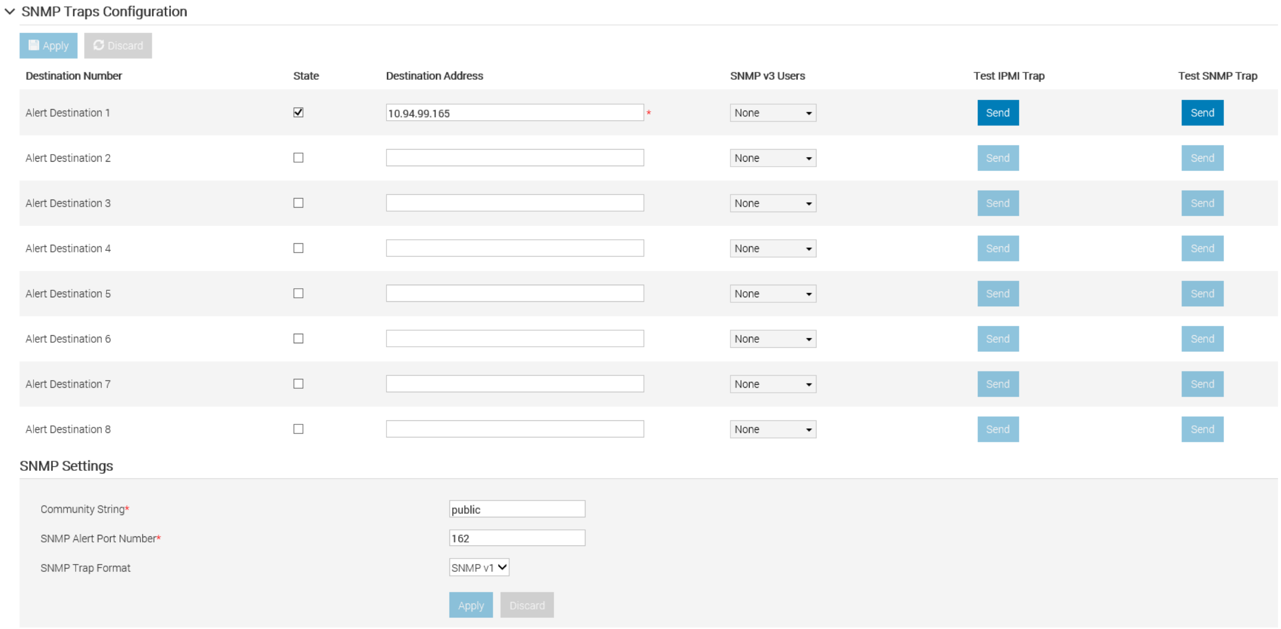

SMTP (E-mail) Server Settings

SMTP (E-mail) Server IP Address or FQDN / DNS Name*	example.com
SMTP Port Number*	25
Authentication	Enabled
Username*	test123
Password*	●●●●●●●●●

2.2 SNMP and IPMI trap alert

1. Log in to the iDRAC web GUI.
2. Click **Configuration → System Setting → Alert Configuration → SNMP Traps Configuration**.
3. Type the destination email address and select the corresponding **State** check box to indicate that the SNMP email alert is enabled by default. You can configure up to eight destination addresses for SNMP (or) IPMI Alert. IPv4 address, IPv6 address, or a FQDN are the supported destination address formats.
4. To test connection between the host and destination, click **Send** corresponding to the alert.
5. Select the Check box under **State** option.
6. Select the SNMPv3 user name by using which you want to send the SNMP v3 formats.
7. Click **Apply**.
8. Enter the iDRAC SNMP community name.
   This is used by iDRAC when sending SNMP and IPMI traps. The destination trap receiver must check for this community name in the traps it receives. To receive the SNMP alert, the community string for iDRAC needs to be same as the destination trap receiver community string. By default, the value of the iDRAC community string is set to **public**.
9. Enter the SNMP Alert Port Number. By default, the value is 162.
10. Select the SNMP trap format. SNMPv1, SNMPv2, and SNMPv3 are currently supported. By default, SNMPv1 is selected.

Note: You can send the test SNMP or IPMI traps to the alert destination address by clicking **Send** button under **Test IPMI Trap or Test SNMP Trap.** You can send the test traps even if the state option is disabled.



Destination Number	State	Destination Address	SNMP v3 Users	Test IPMI Trap	Test SNMP Trap
Alert Destination 1	☑	10.94.99.165 *	None	Send	Send
Alert Destination 2	□		None	Send	Send
Alert Destination 3	□		None	Send	Send
Alert Destination 4	□		None	Send	Send
Alert Destination 5	□		None	Send	Send
Alert Destination 6	□		None	Send	Send
Alert Destination 7	□		None	Send	Send
Alert Destination 8	□		None	Send	Send

SNMP Settings

Community String*	public
SNMP Alert Port Number*	162
SNMP Trap Format	SNMP v1

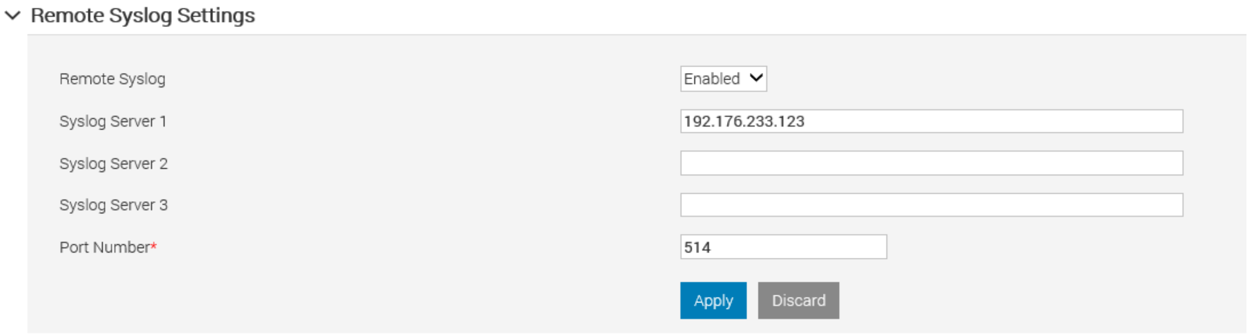
2.3 Remote System Log

This feature is used to configure the remote server settings to remotely write the RAC log and System Event Log (SEL) entries to an external server. To send the logs to the remote server, ensure that:

- There is network connection between iDRAC and the remote server
- The remote server is running on the same network as iDRAC

To configure Remote Syslog Settings by using iDRAC GUI:

1. Log in to the iDRAC web GUI.
2. Click **Configuration → System Setting → Alert Configuration → Remote Syslog Settings**.
3. To enable the transmission and remote capture of the system logs to an external server, from the **Remote Syslog** drop-down menu, select **Enabled**.
   When enabled, new log entries are sent to the specified servers.
   Select **Disabled** to enable the transmission and remote capture of the system logs to an external server.
4. Type information about the Syslog servers 1–3.
5. Type the remote server's name, IPv4 address, or IPv6 address to log iDRAC messages. You can type information about up to 3 servers.
6. Type the port number of the remote server that iDRAC must connect to. The valid values are 1–65535. Default value=514.



Remote Syslog Settings

Remote Syslog	Enabled
Syslog Server 1	192.176.233.123
Syslog Server 2	
Syslog Server 3	
Port Number*	514

2.4 WS-Eventing

The WS-Eventing protocol is used for a client service (subscriber) to register interest (subscription) with a server (event source) for receiving messages containing the server events (notifications or event messages). Clients interested in receiving the WS Eventing messages can subscribe with iDRAC and receive Lifecycle Controller job related events.

To enable WS Eventing from iDRAC web GUI:

1. Click **Configuration → System Setting → Alert Configuration**.
2. Select the **WS Eventing** check box in the **Alert and Remote System Log Configuration** wizard for the required LC log categories.

2.5 OS Log

Replicates the Lifecycle Controller (LC) logs to the OS logs. All events that have the OS Log option as the target replicated in the OS log using the iDRAC Service Module. This process is similar to the System Event Log (SEL) replication performed by the Server Administrator. The default set of logs to be included in the OS logs are the same as the logs configured for SNMP traps SNMP alerts. Only the events logged in the LC log after the iDRAC Service Module (iSM) was installed are replicated to the OS Log. If the Server Administrator is installed, the monitoring feature is disabled to avoid duplicate SEL entries in the OS log.

Starting iDRAC Service Module 2.1, you can customize the location to replicate the LC logs. By default, the Lifecycle Controller logs are replicated in the System group of the Windows logs folder in the Windows Event Viewer. You can replicate the Lifecycle Controller logs to an existing group or create a new folder in the `Application` and `Services Logs` folder in the Windows Event Viewer.

Note: You can choose the location to replicate the Lifecycle Controller logs only during the custom installation or modification of the iSM application.

Note: The source name of the iSM Lifecycle Controller has been changed from iDRAC Service Module to Lifecycle Controller Log.

To enable OS Log Alert from iDRAC web GUI:

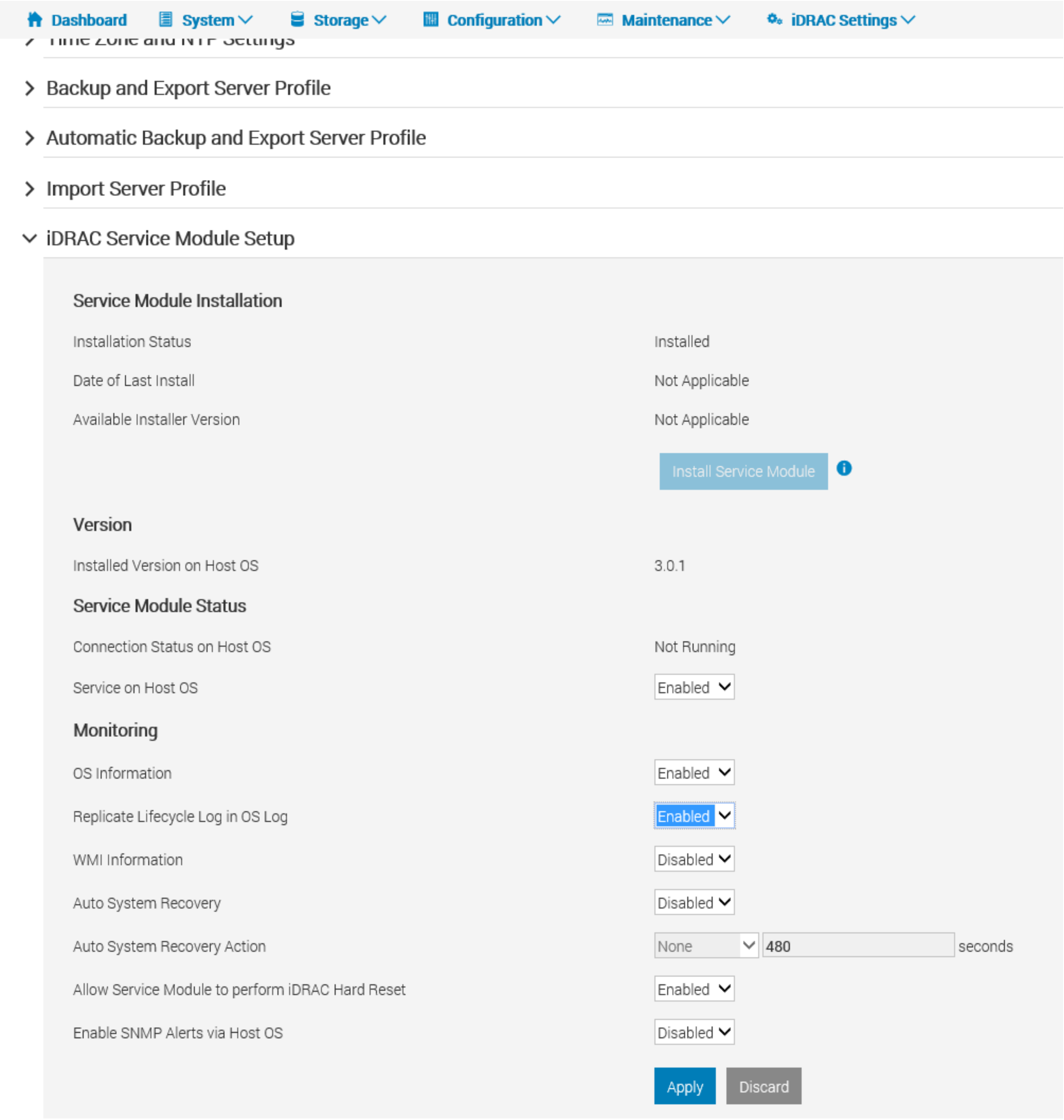
1. Click **Configuration → System Setting → Alert Configuration**.
2. Select the **OS Log** check box in the **Alert and Remote System Log Configuration** wizard for the required LC log categories.

Prerequisites:

- The iSM service must be running on the host.
- Lifecycle Controller logs replication property must be enabled.

To configure the iSM feature by using the iDRAC web GUI:

1. Click **iDRAC Settings → Setting → iDRAC Service Module Setup**.
2. Select the **Replicate Lifecycle Log in OS Log** option.



Time Zone and NTP Settings

Backup and Export Server Profile

Automatic Backup and Export Server Profile

Import Server Profile

iDRAC Service Module Setup

Service Module Installation

Installation Status	Installed
Date of Last Install	Not Applicable
Available Installer Version	Not Applicable

Version

Installed Version on Host OS	3.0.1

Service Module Status

Connection Status on Host OS	Not Running
Service on Host OS	Enabled

Monitoring

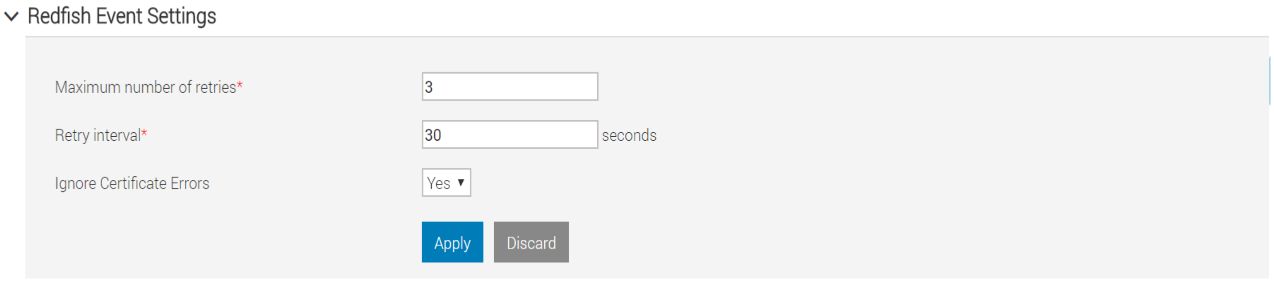
OS Information	Enabled
Replicate Lifecycle Log in OS Log	Enabled
WMI Information	Disabled
Auto System Recovery	Disabled
Auto System Recovery Action	None 480 seconds
Allow Service Module to perform iDRAC Hard Reset	Enabled
Enable SNMP Alerts via Host OS	Disabled

2.6 Redfish Event

Redfish specification includes support for eventing that enables the notification of important events occurring in a server to a management client. Redfish provides push-style event notifications to an event listener, defined as a Redfish-compliant HTTPS server. The listener subscribes to the events of interest based on the event types defined in the Redfish specification. Event subscriptions remain in place until specifically deleted or until the Redfish manager such as iDRAC is reset to its default configuration.

You can perform redfish event settings by using iDRAC web GUI.

1. Log in to the iDRAC web GUI.
2. Click **Configuration → System Setting → Alert Configuration → Redfish Event Settings**.
3. Type or select data in the fields.
   You can set up the maximum number of retries to attempt before failing the operation. The default value is 3. The allowed range is 0–5.
   The allowed range for retry interval is 5–60.
4. To ignore the certificate errors, leave **Yes** as-is. The certificate validation will not happen over HTTPs. Else, if **No** is selected, certificates are validated.



Redfish Event Settings

Maximum number of retries* 3

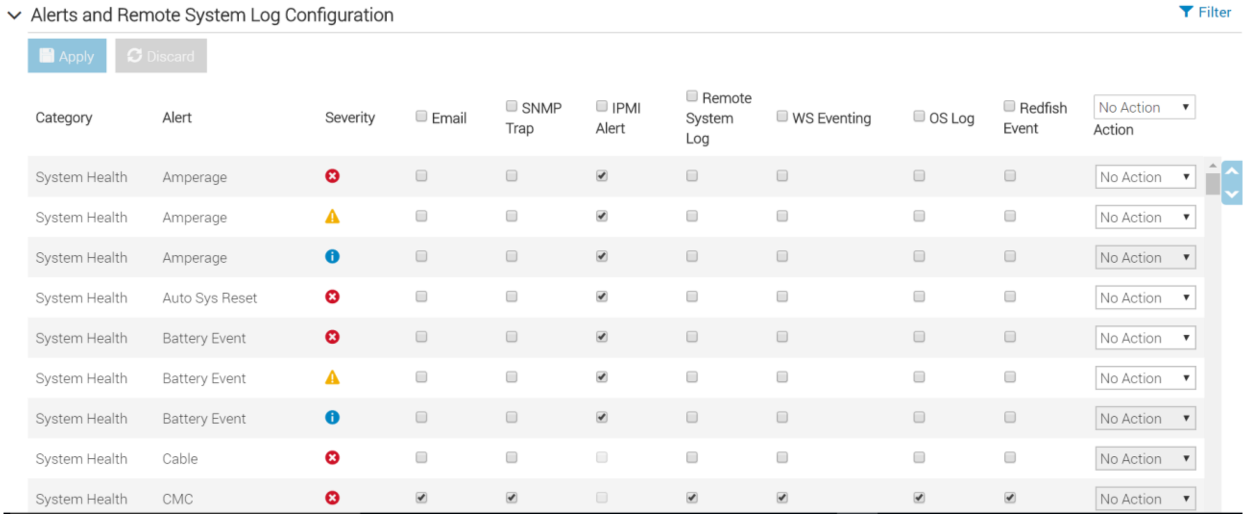
Retry interval* 30 seconds

Ignore Certificate Errors Yes

2.7 Action

You can associate an action with every Lifecycle Log event. Actions can be set on the **Configuration → System Setting → Alert Configuration → Alert and Remote System Log Configuration** page for each event by using the **Action** column. You can select one of the following:

- **No Action** — No action is required to be performed when an event occurs.
- **Reboot** — Restarts (warm boot) the system when an event occurs.
- **Power Cycle** — Power cycle the system (cold boot) when an event occurs.
- **Power off** — Powers off the system when an event occurs.



Alerts and Remote System Log Configuration

Filter

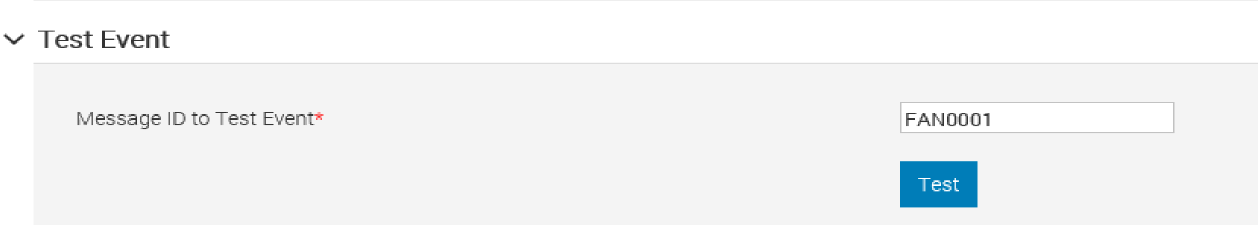
Apply | Discard

Category	Alert	Severity	□ Email	□ SNMP Trap	□ IPMI Alert	□ Remote System Log	□ WS Eventing	□ OS Log	□ Redfish Event	No Action ▾ Action
System Health	Amperage	☒	□	□	☑	□	□	□	□	No Action ▾
System Health	Amperage	⚠	□	□	☑	□	□	□	□	No Action ▾
System Health	Amperage	ℹ	□	□	☑	□	□	□	□	No Action ▾
System Health	Auto Sys Reset	☒	□	□	☑	□	□	□	□	No Action ▾
System Health	Battery Event	☒	□	□	☑	□	□	□	□	No Action ▾
System Health	Battery Event	⚠	□	□	☑	□	□	□	□	No Action ▾
System Health	Battery Event	ℹ	□	□	☑	□	□	□	□	No Action ▾
System Health	Cable	☒	□	□	□	□	□	□	□	No Action ▾
System Health	CMC	☒	☑	☑	□	☑	☑	☑	☑	No Action ▾

2.8 Test Event

After configuring alerts, you can test the configuration of each event. On the IDRAC9 web GUI, you can test configured events by using the Test event feature.

1. Click **Configuration → System Setting → Alert Configuration → Test Event**.
2. Type the message ID of an alert. For a list of valid message IDs, see the *Event and Error Message Reference Guide for 14th Generation Dell EMC PowerEdge Servers* available on http://dell.com/idracmanuals.
3. To send the configured event to the respective SNMP, IPMI, email, remote syslog, WS-Eventing, OS Log, and Redfish Event alerts, click **Test**.



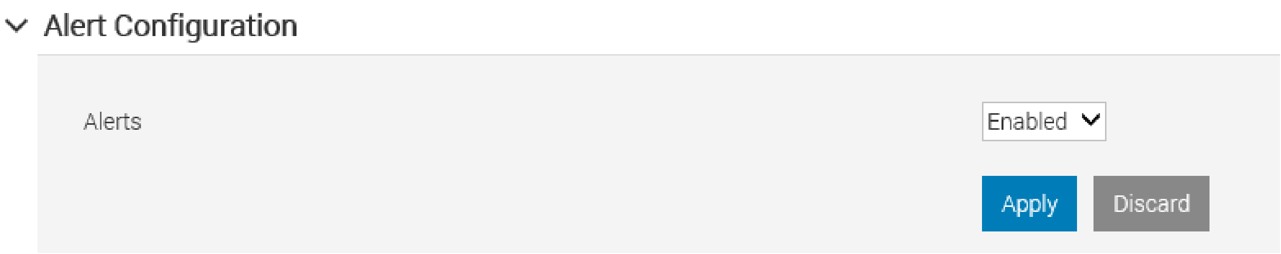
Test Event

Message ID to Test Event*: FAN0001

Test

2.9 Alert Configuration prerequisites

1. To configure an alert, log in to the iDRAC web GUI.
    a. Click **Configuration → System Setting → Alert Configuration**.
    b. Under **Alert Configuration**, select **Enabled** for from the **Alerts** drop-down menu, and then click **Apply**.



Alerts: Enabled

2. Configure the network settings. You must configure iDRAC9 network settings for DNS server and domain name.
   a. Click **iDRAC Settings → Connectivity → Network**.
   b. Under **Common Settings**, select the **Register iDRAC on DNS** check box.
   c. Either select **Auto Config Domain Name**, or type a static DNS Domain Name.
   d. Under **IPv4 Settings**, either select the **Use DHCP to obtain DNS server addresses** check box, or manually enter the IP address of your DNS server.
   e. For IPv6, you can use the Auto configuration 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.

Note: To receive any alerts, Configuration mentioned above are the perquisites, apart from alert settings specific to alert type (covered in Alert configuration section).

Conclusion

The alert settings in iDRAC9 firmware release provides IT administrators with more options, methods, and granularity to manage PowerEdge servers. Key features 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
- Types of alerts such as SNMP, WS-Events, authenticated email, and remote syslog

Also, you can receive alerts for servers that have no OS installed. Therefore, there is no need for installing an OS agent such as OMSA. You can configure alert destinations by using a FQDN instead of an IP address. You now have the ability to search for and view the newly standardized message database by using the iDRAC9 web interface.