VRTX Chassis Alert Management Techniques

This White paper addresses the various logging and alerting mechanism in the Chassis, which the administrator rely on monitoring and controlling a VRTX Chassis.

Author(s)

Anto Jesurajan

Arun Muthaiyan

Michael Brundridge

Sheshadri P.R. Rao

Executive summary

This white paper explains the various logging and alerting features available in the VRTX Chassis Management Controller (CMC). The CMC logs the events on Chassis Log, SEL Log, Remote syslog, and LCD. It can also be configured for email and SNMP alerts. With the Remote System Logging feature, CMC has the capability to remote logging and alerting, which is more essential for Administrators to easily debug and to monitor the events without being physically present in front of the system.

This white paper explains the format of different logging techniques such as SEL format and Chassis Log format, and the recommended action to assist in troubleshooting.

Contents

Introduction

Logging is a technique to inform and alert administrators about any Chassis events, which is not normal and requires attention. Logging or alerting can occur through one or more of the following:

- CMC non-volatile memory, which in turn, reflects on the health of a chassis, on the basis of severity of an event.
- LCD (where the messages appear on the LCD Display)
- Remote management station on the basis of configuration such as the Remote System Logging (Syslog).
- Remote Alert management, which can be either by email, Remote Syslog, or Simple Network Management Protocol (SNMP).

Terminology

SNMP: Simple Network Management Protocol is an Internet-standard protocol for managing devices on IP networks.

SMTP: Simple Mail Transfer Protocol is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol networks.

SEL: System event log is logging standard based on IPMI Specification.

LCD: A Liquid-crystal display is a flat panel display, electronic visual display, or video display that uses the light modulating properties of liquid crystals. Liquid crystals do not emit light directly.

SYSLOG: Syslog is a standard for computer data logging. It separates the software that generates messages from the system that stores them, and the software that reports and analyzes them.

WSMAN: Web Services-Management (WS–Management) is a DMTF open standard defining a SOAP–based protocol for the management of servers.

RACADM: Dell Remote Access Controller Admin Tool is a command line utility for Chassis configuration and monitoring.

Logging Types

The CMC has the following logging techniques as described in VRTX Logging Techniques. In Addition to the logging, it supports the alerting techniques such as SNMP and email.

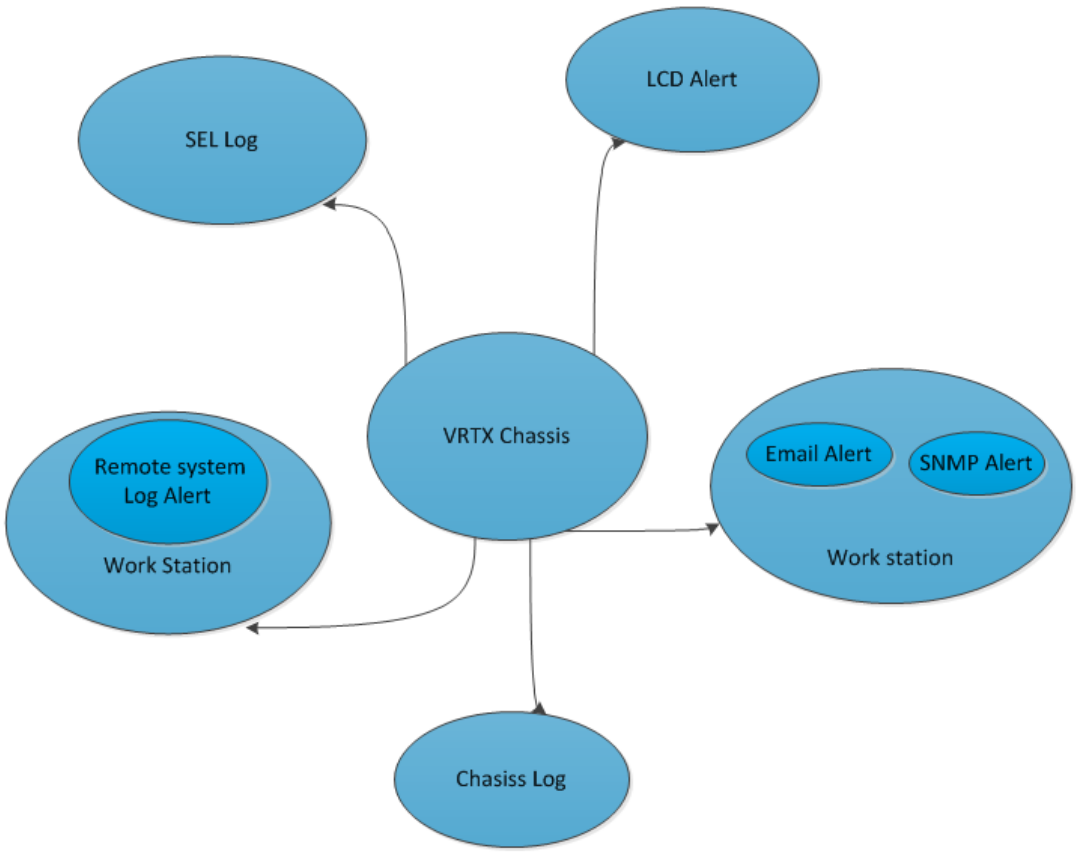

Figure 1. VRTX Logging Techniques

Chassis Events

The Critical, Warning, and Informational events are monitored by the VRTX Chassis Management Controller (CMC) firmware and logged through Chassis Log and SEL log, and can be filtered for sending email Alert, SNMP, Remote Syslog. The CMC monitors the chassis events, filters the events, generates alerts, or specifies actions when an event occurs. An event occurs when the status of a system component is outside the predefined or normal condition. If an event matches an event filter, and if the filter is configured to generate an alert (email or SNMP trap), an alert is sent to one or more of the configured destinations. To change a setting, click **Chassis Overview > Alerts > Chassis Events.** To perform this task, you must have the **Chassis Configuration Administrator** privileges.

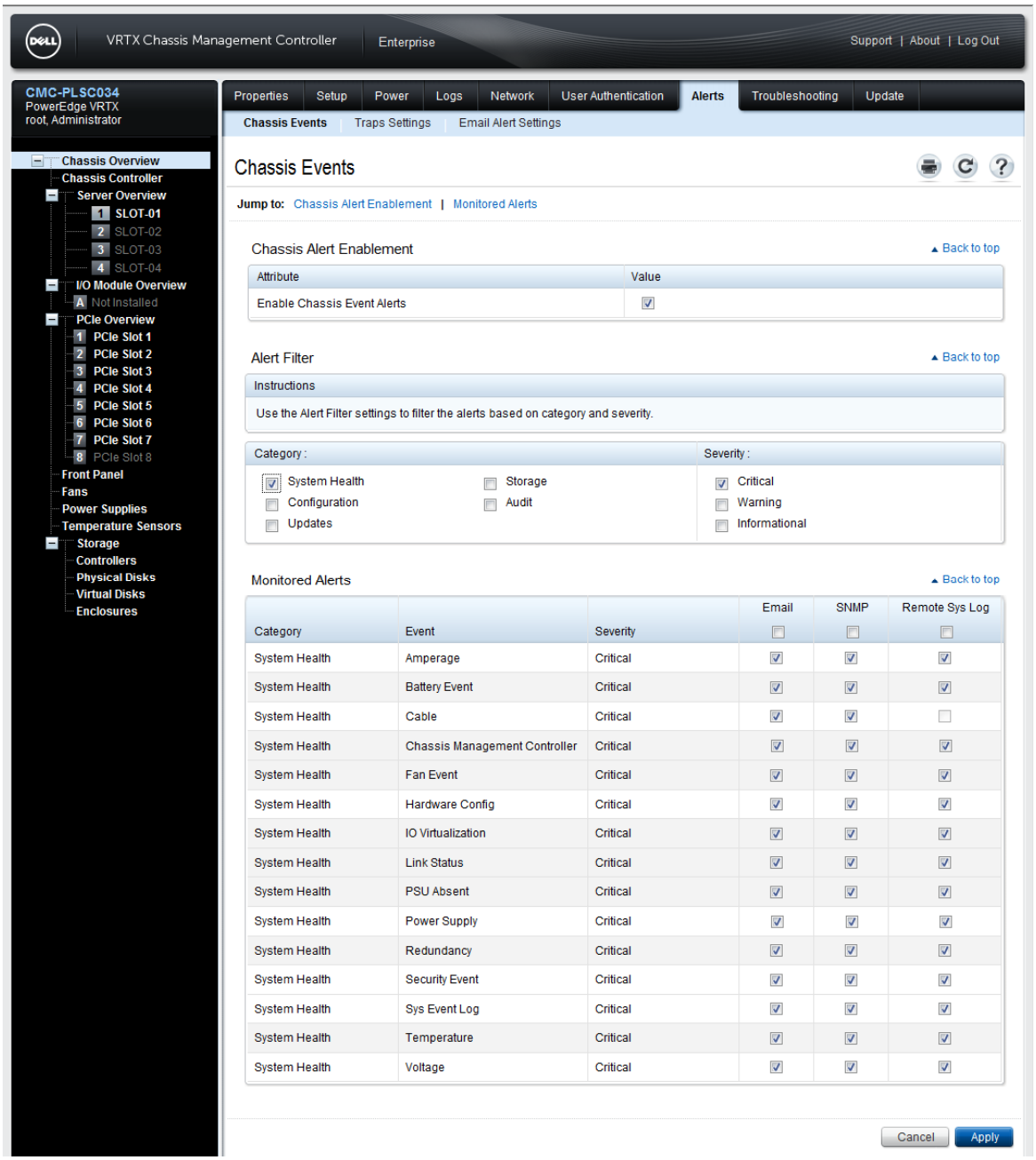

Figure 2. Example of Chassis Event Page

Chassis Alert Enablement

Enable Chassis Event Alerts can be configured using the Web interface (see Figure 2), RACADM Command Life Interface (CLI), or WS-MAN to send an alert for any registered event.

Events can be configured to send alerts through email, SNMP trap, or Remote Syslog option. Events are not enabled until the **Enable Chassis Event Alerts** option is enabled. After **Enable Chassis Event Alerts** is enabled, any monitored event that has been configured will send an alert using the configured interfaces after its threshold is reached.

The alert message has various categories; **System Health** (monitors the overall system health of the VRTX Chassis and the components of a), **Storage** (Monitored Storage Components HDD, Expander, Storage Adapters, and Backplane), **Updates** (related to all chassis updates), **Configuration** (IO virtualization), **Audit** (Events for Chassis Administrators**).** The events have three severity levels**; Critical, Warning** and **Informational.**

Types of Logging

Chassis Log

Chassis log events are logged with the following categories: System Health, Storage Configuration, Audit, Updates, with severities of Critical, Warning, and Informational. Chassis log is stored in a non-volatile storage area in the chassis and retained on the chassis AC cycle.

Chassis Log Format

```
-----------------------------------------------------------------------------------------------
    1. SeqNumber        =
    2. Message ID       =
    3. Category         =
    4. AgentID          =
    5. Severity         =
    6. Timestamp        =
    7. Message Arg   1  =
    8. Message          =
---------------------------------------------------------------------------------------------
```

Format	Description
SeqNumber	The chassis log index.
Message ID	This is the combination of Agent ID and Message Number which is unique for an Agent ID.
Severity	Critical, Informational and Warning.
Timestamp	Indicates the time of the event.
Message Arg 1 …. Message Arg N	Arguments passed to the message.
Message	Message String

The chassis events can be configured to alert using SNMP, email, and Remote Syslog:

- **Email**: Configure the event to send an email to the configured email address when an event occurs. Configure the email server settings (SMTP Server).
- **SNMP Trap:** Configure the event to send a SNMP trap to the configured destination IP address when an event occurs. Configure the SNMP trap settings in the chassis to send SNMP trap.
- **Remote Syslog**: Configure the event to send an alert to an external server. Configure the Remote Syslog settings in the chassis to send Remote Syslog.

SEL Log

The System Event Log is a non-volatile repository for system events and certain system configuration information. The device that receives the commands to access the SEL is referred to as the System Event Log Device or SEL device. Event message information is normally written into the SEL after being received by the Event Receiver functionality in the Event Receiver device.

SEL Entries have a unique 'Record ID' field. This field is used for retrieving log entries from the SEL. SEL reading can be done in a random access—manner. That is, SEL Entries can be read in any order assuming that the Record ID is known.

SEL Record IDs **0000h** and **FFFFh** are reserved for functional use and are not legal ID values. Record IDs are handles. They are not required to be sequential or consecutive. Applications should not assume that SEL Record IDs will follow any particular numeric ordering. SEL Records are kept as an ordered list.

Table 1 – SEL Record Format lists the format of the SEL. For more information about SEL format, refer to the IPMI Specification.

Byte	Field	Description
1 2	Record ID	ID used for SEL Record access. The Record ID values 0000h and FFFFh have special meaning in the Event Access commands and must not be used as Record ID values for stored SEL Event Records.
3	Record Type	[7:0] - Record Type 02h = system event record C0h-DFh = OEM timestamped, bytes 8–16 OEM defined E0h-FFh = OEM non-timestamped, bytes 4–16 OEM defined
4 5 6 7	Timestamp	Time when an event was logged. LS byte first.
8 9	Generator ID	RqSA & LUN, if event was generated from IPMB. Software ID, if event was generated from a system software. Byte1 [7:1] - 7-bit I^2C. Slave Address, or 7–bit system software ID [0] 0b = ID is IPMB Slave Address 1b = system software ID Byte2 [7:4] - Channel number. Channel over which an event message was received. 0h, if the event message was received through the system interface, primary IPMB, or internally generated by the BMC. (New for IPMI v1.5. These bits were reserved in IPMI v1.0) [3:2] - reserved. Write as 00b. [1:0] - IPMB device LUN if byte 1 holds Slave Address. 00b otherwise.
10	EvM Rev	Event Message format version (=**04h** for events in this specification, 03h for IPMI v1.0 Event Messages.) *Note: the BMC must accept Platform Event request messages that are in IPMI v1.0 format (EvMRev=03h) and log them as IPMI v1.5 | v2.0 Records by setting the EvMRev field to 04h and setting the Channel Number in the Generator ID field appropriately for the channel that the event was received from.*
11	Sensor Type	Sensor Type Code for sensor that generated the event
12	Sensor #	Number of sensor that generated the event

13	Event Dir | Event Type	EventDir [7] - 0b = Assertion event. 1b = Deassertion event. EventType Type of trigger for the event. For example, critical threshold going high, state asserted, and so on. Also indicates *class* of the event. For example, discrete, threshold, or OEM. The Event Type field is encoded using the Event/Reading Type Code. See section 42.1 *Event/Reading Type Codes*. [6:0] - Event Type Code
14	Event Data 1	Per *Table 2,* Event Data Field Contents
15	Event Data 2	Per *Table 2,* Event Data Field Contents
16	Event Data 3	Per *Table 2,* Event Data Field Contents

Table 1 – SEL Record Format

The contents of the Event Data field (see Table 2 - Event Data Field Contents) in an Event Request Message (Event Message) depends on the sensor class. The sensor class obtained from the Event/Reading Type Code specifies whether or not the sensor event is threshold-based, discrete, or OEM–defined. Each event type is associated with a sensor class.

SEL logs are parsed and displayed in a user-readable format.

Sensor Class	Event Data
threshold	EventData1 [7:6] - 00b = unspecified byte 2 01b = trigger reading in byte 2 10b = OEM code in byte 2 11b = sensor-specific event extension code in byte 2 [5:4] - 00b = unspecified byte 3 01b = trigger threshold value in byte 3 10b = OEM code in byte 3 11b = sensor-specific event extension code in byte 3 [3:0] - Offset from Event/Reading Code for threshold event. EventData2 reading that triggered event, FFh or not present if unspecified. EventData3 threshold value that triggered event, FFh or not present if unspecified. If present, byte 2 must be present.
discrete	EventData1 [7:6] - 00b = unspecified byte 2 01b = previous state and/or severity in byte 2 10b = OEM code in byte 2 11b = sensor-specific event extension code in byte 2 [5:4] - 00b = unspecified byte 3 01b = reserved 10b = OEM code in byte 3 11b = sensor-specific event extension code in byte 3 [3:0] - Offset from Event/Reading Code for discrete event state EventData2 [7:4] - Optional offset from 'Severity' Event/Reading Code. (0Fh if unspecified). [3:0] - Optional offset from Event/Reading Type Code for previous discrete event state. (0Fh if unspecified.) EventData3 Optional OEM code. FFh or not present if unspecified.

OEM	EventData1 [7:6] - 00b = unspecified in byte 2 01b = previous state and/or severity in byte 2 10b = OEM code in byte 2 11b = reserved [5:4] - 00b = unspecified byte 3 01b = reserved 10b = OEM code in byte 3 11b = reserved [3:0] - Offset from Event/Reading Type Code EventData2 [7:4] - Optional OEM code bits or offset from 'Severity' Event/Reading Type Code. (0Fh if unspecified). [3:0] - Optional OEM code or offset from Event/Reading Type Code for previous event state. (0Fh if unspecified). EventData3 Optional OEM code. FFh or not present or unspecified.

Table 2 - Event Data Field Contents

Types of Alerting Techniques

CMC has the following Alert Management interfaces Email, SNMP, and Remote Syslog.

Email Alert

SMTP is a protocol and set of requirements that allows CMC to transmit email over the Internet. CMC is designed to use SMTP for communication purposes when sending email, and is only used for outgoing messages. When chassis events have been configured to send Email based alerts, the corresponding **SMTP (Email) Server** address has to be configured in the **Chassis Overview > Alerts > Email Alert Settings** page. There are two other protocols—POP3 and IMAP, which are used for retrieving emails on the Management station.

SMTP is the protocol defined for email communication between systems. The protocol has a defined format of sending messages across a network, which comprises of a sender, recipient, message body, and title. The message is broken down to the standard format which the receiver understands. The message format is transformed into key value pairs, which can be decoded by the receiver on the basis of encoding, and can be separated to different sections before sending. The email server at the receiving end is designed to receive the message, decode, and reorganize based on each recipient's *n*.

POP3 is an acronym for Post Office Protocol, version 3, which is used on the mail server. This protocol helps retain the email on the receiving end, till it is read by the recipient. POP3 can be used by administrators to receive the mail from the CMC.

IMAP is another popular email retrieval protocol which can also be used. Administrators can also use other email retrieval programs on mail servers other than POP3/IMAP.

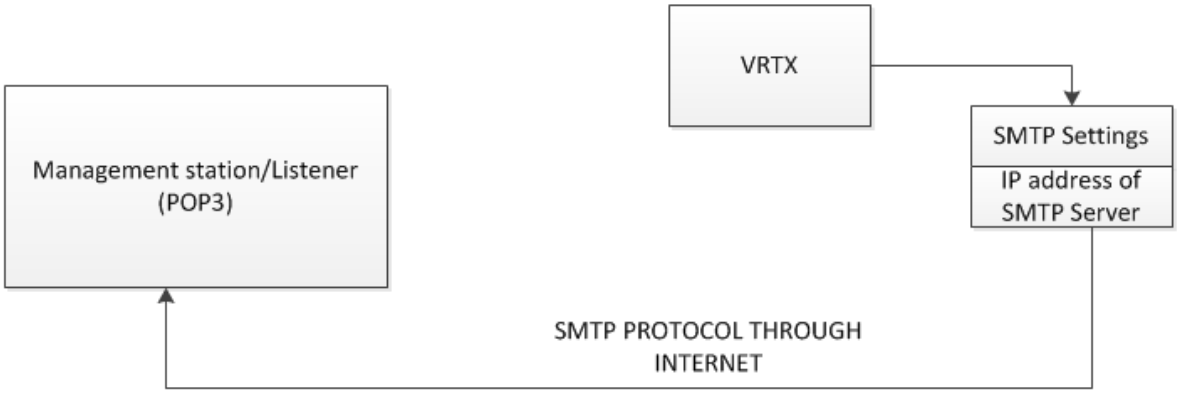

Figure 3. SMTP Flow Diagram

Email Alert Settings

CMC has the facility to set the email alert destinations. More than one email alert destinations can be set and CMC currently supports four alert email destinations. When an event occurs, which could be either a component issue or environmental issue, CMC sends an alert to all the destinations configured in the email alert destination of the chassis. The alert destination can be changed or removed any time, provided the user has the configuration privilege. For correct usage of email alerts, the SMTP settings must be configured.

SMTP settings is the mail server or Management Station IP address. The CMC has the provision to configure the sender information which can be used to set the chassis name so the alert on the management station can be identified by the administrator on the basis of a chassis. Administrators are free to configure any valid name as the source email name.

SMTP (Email) Server Settings

An SMTP server can only be changed if the user has the Chassis Configuration Administrator privilege. From the CMC Web interface:

1. For the SMTP (Email) Server configuration, enter the SMTP server details using either the dot-separated format (for example, 140.25.122.31) or the DNS name.

2. For the Modify Source Email Name, configure the desired originator email for the alert, or leave it blank to use the default email originator. The default value is `cmc@[IP_address]`, where [IP_address] is the IP address of a CMC. If administrators decide to input an email address, then the syntax of the email name is `emailname[@domain]`, an email domain can be optionally specified. If @domain is not specified and there is an active CMC network domain, then the email address of emailname@cmc.domain is used as the source email. If @domain is not specified and CMC has no active network domain, then the IP address of CMC is used (for example, emailname@[IP_address]).

   NOTE: SMTP IP addresses are supported. If your network has an SMTP server that releases and renews IP Address periodically, and the addresses are different, then there is a duration when this property setting does not work due to change in the specified SMTP server IP address. In such cases, it is suggested to use the DNS name.

3. Email Alert Number displays the sequential number that denotes four configurable email addresses. Email alert numbers identify a particular alert configuration while configuring through RACADM and are also used in CLI scripting. To enable the email alert, destination corresponding to the destination number has to be enabled. This option is enabled by default.

4. Destination Email Address in the configuration in the email address to which email alerts are sent. The address must be valid, containing an 'at' (@) symbol, and a 'period' (.) For example, **name@domain.com** or **name@domain.com.uk**. Name (Optional) is the name of the entity receiving an email. This field is optional. If a name is entered for an invalid email address, it is not considered. Then click Apply.

5. The (**Test Email**) **Send** button is to send a test email to the specified destination email address. Make sure that the SMTP (email) server IP address is configured on the Network Configuration before sending the test email.

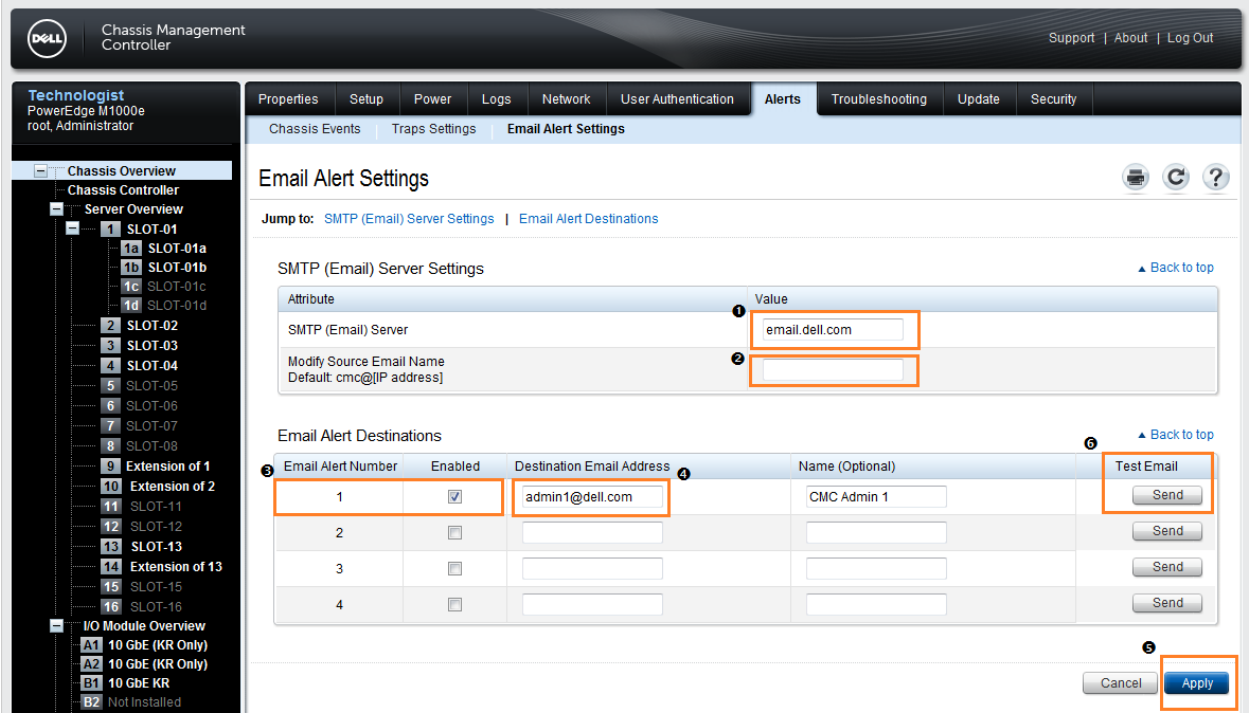

Figure 4. Email Alert Settings

The SMTP (Email) Server Settings can also be set using the RACADM command line as follows:

1. To set the SMTP (Email) Server address, run the command `racadm config –g cfgRemoteHosts –o cfgRhostsSmtpServerIpAddr` *`192.168.0.152`* **OR** `racadm config –g cfgRemoteHosts –o cfgRhostsSmtpServerIpAddr` *`domain.name`*
2. To set Modify Source Email Name, run the command `racadm config –g cfgAlerting –o cfgAlertingSourceEmailName` *`user@home.com`*
3. To set Email Alert Destinations, run the command
   a. `racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <`*`index`*`>`
   b. `racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <`*`email address`*`> -i <`*`index`*`>`
   c. `racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName "John Doe" -i <`*`index`*`>`
4. To send a test email, run the command `racadm testemail –i <`*`index`*`>,` where index is the configured Email Alert Number.

SNMP Trap

SNMP trap is a type of alert similar to an email alert, which complies with the SNMP Protocol. The SNMP trap is received by a management station or console.

SNMP components

- SNMP Manager
- SNMP Managed devices
- SNMP agent
- Management Information Database referred to as Management Information Base (MIB)

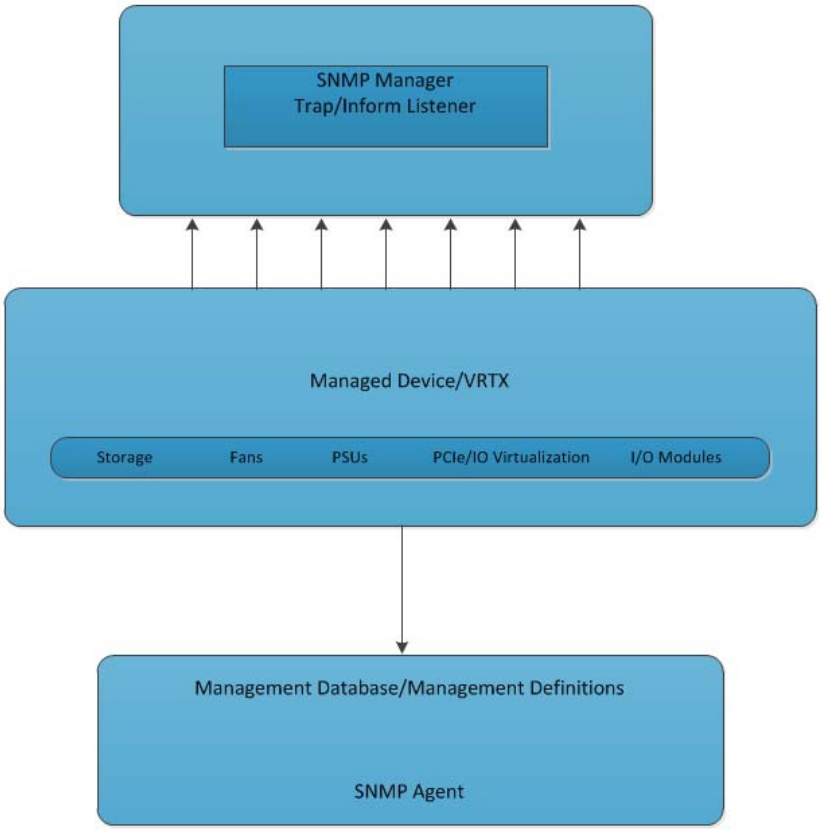

Figure 5. SNMP Flow Diagram

SNMP Manager

A manager or management system is a separate entity that is responsible for communicating with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager does the following functions:

- Walks agents
- Gets response from the agents
- Sets data in agents
- Acknowledges asynchronous events from the agents

SNMP–Managed Devices

A managed device or the network element is a part of the network/VRTX Chassis components that requires some form of monitoring and management. For example, storage components, fan components, IO components, PCIe components, and PSUs.

SNMP Agent

An agent is a program tied to the managed element. Enabling an agent allows it to collect the management information database from the managed device locally, and makes it available to the SNMP manager through the queries it gets through the manger. These agents could be standard (for example, Net-SNMP).

SNMP agents do the following:

- Gathers management information about its local environment
- Saves and broadcasts the management information as defined in the MIB
- Alerts an event to the SNMP manager
- Acts as a substitute for some non–SNMP—manageable nodes

Management Information Base (MIB)

The managed device properties are described in the information database and is tracked by an SNMP agent. The database is shared by the manager and the agent. The manager gets the properties of the managed device through the agent with the help of a shared database known as MIB (Management Information Base).

MIB contains the configuration values and statistical values defined for the managed devices, which could be standard or private. The Agent helps get the data through the queries by the Manager using the MIB.

MIB files are the set of queries that a SNMP Manager can query the agent. Agent collects these data locally and stores it, as defined in the MIB. So, the SNMP Manager is aware of these standard and private questions for every type of agent.

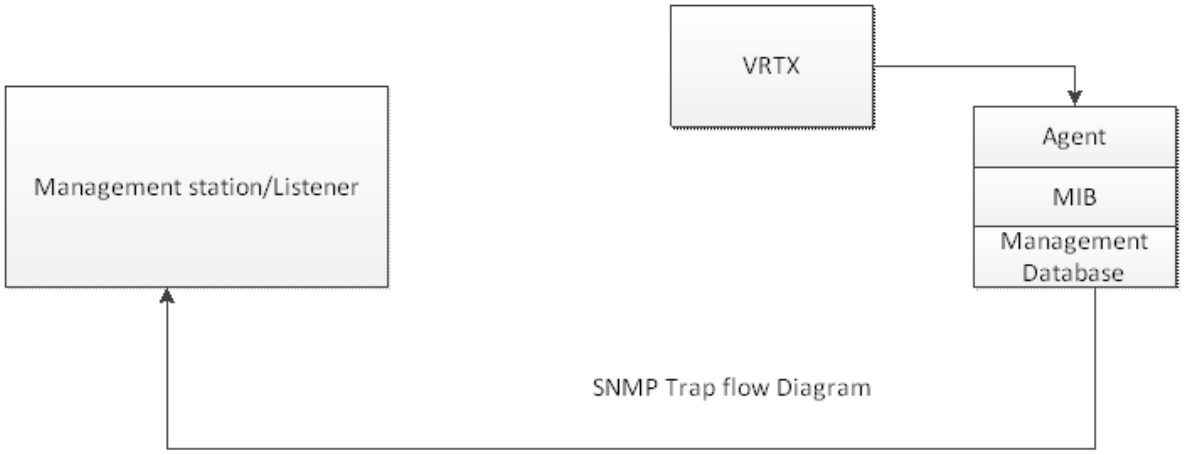

Figure 6. SNMP Flow Diagram

SNMP trap destinations and Agent settings can be set got through RACADM command line interface as follows:

1. To set the SNMP Trap Destination address, run the command

   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIpAddr 143.169.25.1 -i 1
   ```

   where i is the index of the Destination Address. CMC supports up to index 4 (i.e. CMC allows up to 4 destinations).

2. To set the SNMP Community string for a specific index, run the command

   ```
   racadm config -g cfgTraps  -o cfgTrapsCommunityName public -i 1
   ```

3. To get the SNMP settings, run the command

   ```
   racadm getconfig -g cfgTraps -i 1
   ```

4. The SNMP agent can be enabled through, run the command

   ```
   racadm config -g cfgOobSnmp –o cfgOobSnmpAgentEnable 1
   ```

5. To Set SNMP Agent community String, run the command

   ```
   racadm config –g cfgOobSnmp –o cfgOobSnmpAgentCommunity public
   ```

6. To get SNMP Agent configuration, run the command

```
racadm getconfig –g cfgOobSnmp
```

To change any of the settings on the Web page, click **Chassis Overview > Alerts > Traps Settings**. (Example of Chassis Event Page). To perform this task, you must have the **Chassis Configuration Administrator** privileges.

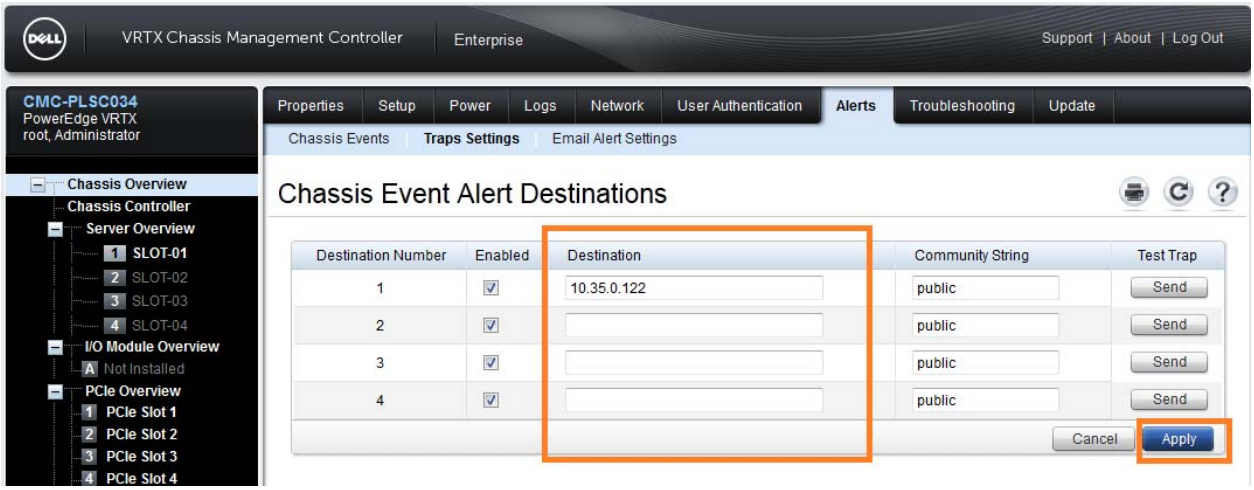

Figure 7. SNMP Trap Settings Remote Syslog

Remote Syslog Logging is a standard for computer data logging. It separates the chassis that generates messages from the management station that stores them, and the software that reports and analyzes them. Remote Syslog can be used for chassis system management, security auditing, generalized information, analysis, and debugging purposes. Messages are added with a facility code (auth, kern, mail, news, syslog, user, local0, …, local7) indicating the type of event that generated the messages, and are assigned a severity as configured in the messages (Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug). Implementations are available for many operating systems. Specific configuration may permit directing messages to remote syslog servers.

Enable Remote Syslog in the management station and configure the remote system IP addresses in CMC Remote Syslog configuration. The port(s) a remote management station is listening for syslog messages should match the configuration in CMC.

To change any of the Remote syslog settings on the Web page, click **Chassis Overview > Network > Services** page (Example of Chassis Event Page), To perform this task, you must have the **Chassis Configuration Administrator** privileges.

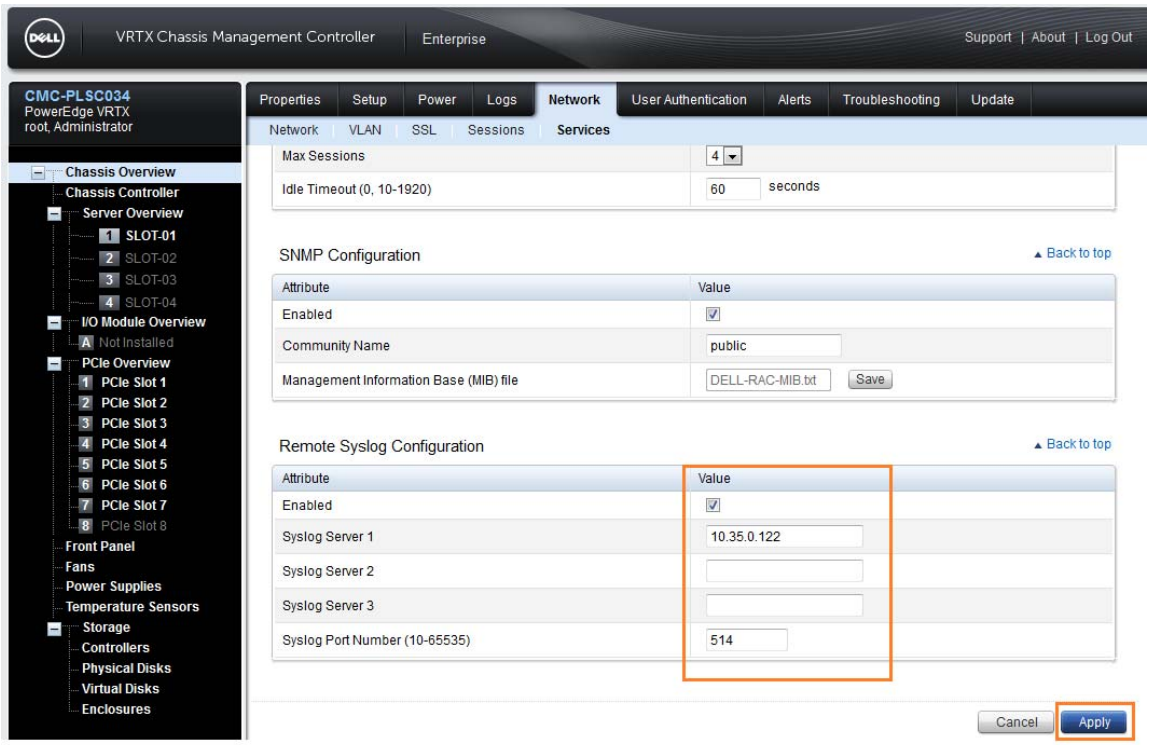

Figure 8. Remote Syslog Settings

Remote Syslog settings can be set or got through RACADM command line interface as follows:

1. To enable remote syslog, run the command

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSyslogEnable 1
   ```

2. To set the remote syslog port, run the command

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPort 514
   ```

3. To set the remote syslog host, run the command

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer1
   10.35.0.122
   ```

4. The enable remote syslog for power subsystem in CMC, run the command

   ```
   racadm config -g cfgRemoteHosts –o
   cfgRhostsSyslogPowerLoggingEnabled  1
   ```

5. To get remote syslog settings, run the command

   ```
   racadm getconfig -g cfgRemoteHosts
   ```

Enabling the r-syslog in Linux

Remote Syslog can be enabled in Linux management station by adding an `–r` option in `the syslog configuration` file. The configuration file has to be reloaded after the change, so it requires a restart of syslog service. The syslog server listens on the port configured on the management station or any syslog messages, and then logs on the storage repository configured on the syslog server configuration file.

Learn more

Visit Dell.com/PowerEdge for more information about Dell's enterprise-class servers.

http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-specifications.html
http://en.community.dell.com/techcenter/extras/m/white_papers/20097170.aspx

June 2013 | Rev 1.0