White Paper

USING THE EMC VMAX CONTENT PACK FOR VMWARE VREALIZE LOG INSIGHT

Monitoring EMC Symmetrix log activity with VMware

Abstract

This white paper explains how to setup EMC Solutions Enabler™ and Unisphere for VMAX™ for use with VMware vRealize™ Log Insight™ and the VMAX Content Pack.

December 2014

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

The information in this publication is provided “as is”. EMC Corporation 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.

Part Number h12138.6

Table of Contents

Executive summary

VMware vRealize Log Insight delivers automated log management through log analytics, aggregation and search. With an integrated cloud operations management approach, it provides the operational intelligence and enterprise-wide visibility needed to proactively enable service levels and operational efficiency in dynamic hybrid cloud environments.

The EMC VMAX Content Pack, when integrated into VMware vRealize Log Insight, provides dashboards and user-defined fields specifically for EMC Symmetrix® VMAX arrays to enable administrators to conduct problem analysis and analytics on their array(s).

This paper will explain how Solutions Enabler and Unisphere for VMAX can be configured to send log files to VMware vRealize Log Insight and will provide an example of a problem analysis that can be conducted with the EMC VMAX Content Pack.

Audience

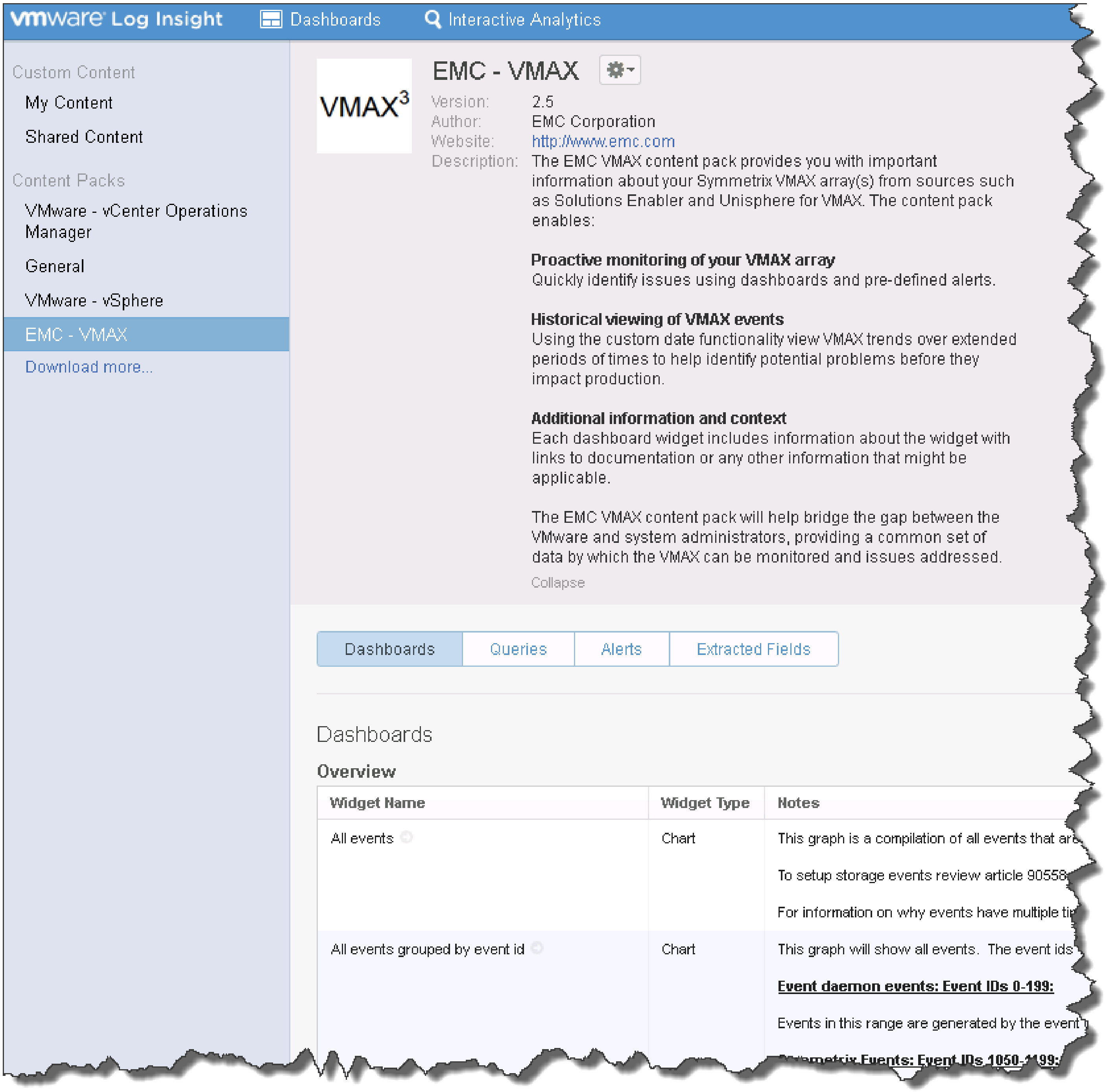
This technical white paper is intended for VMware administrators and storage administrators responsible for deploying VMware vRealize Log Insight with EMC Symmetrix VMAX. This document assumes a general understanding of VMware vRealize Log Insight and the components that make it up, including the Dashboards and Interactive Analytics page. The reader should also be familiar with EMC Solutions Enabler and EMC Unisphere for VMAX.

EMC VMAX Content Pack

A content pack for VMware vRealize Log Insight (Log Insight) is a special type of dashboard group. It is delivered as a file with a “vlcp” extension. A content pack can be imported into any instance of Log Insight. In essence it is a plug-in. VMware delivers a default content pack with Log Insight that is designed for VMware-related log information. Similarly, EMC has developed their own custom content pack for VMAX log information. It can be downloaded at the VMware Solution Exchange in the Cloud Management Marketplace. This content pack contains both dashboards and user-defined fields. All of the widgets that make up the dashboards contain an information field that explains the purpose of the graph. Though the VMAX content pack is not required in order to use Log Insight with the VMAX, it is recommended as a good starting point for helping to categorize all the log information coming from the array.

This document will serve to cover the Log Insight versions v2.0 and higher.

When viewing the VMAX content pack definition in Log Insight, there is a full description of the content pack details. Seen in Figure 1 is the definition of the VMAX content pack.



EMC - VMAX

Version: 2.5
Author: EMC Corporation
Website: http://www.emc.com
Description: The EMC VMAX content pack provides you with important information about your Symmetrix VMAX array(s) from sources such as Solutions Enabler and Unisphere for VMAX. The content pack enables:

Proactive monitoring of your VMAX array
Quickly identify issues using dashboards and pre-defined alerts.

Historical viewing of VMAX events
Using the custom date functionality view VMAX trends over extended periods of times to help identify potential problems before they impact production.

Additional information and context
Each dashboard widget includes information about the widget with links to documentation or any other information that might be applicable.

The EMC VMAX content pack will help bridge the gap between the VMware and system administrators, providing a common set of data by which the VMAX can be monitored and issues addressed.

Dashboards

Overview

Widget Name	Widget Type	Notes
All events	Chart	This graph is a compilation of all events that ar To setup storage events review article 90558 For information on why events have multiple ti
All events grouped by event id	Chart	This graph will show all events. The event ids **Event daemon events: Event IDs 0-199:** Events in this range are generated by the event **Symmetrix Events: Event IDs 1050-1199:**

Figure 1. VMware Log Insight v2.5 with the VMAX content pack

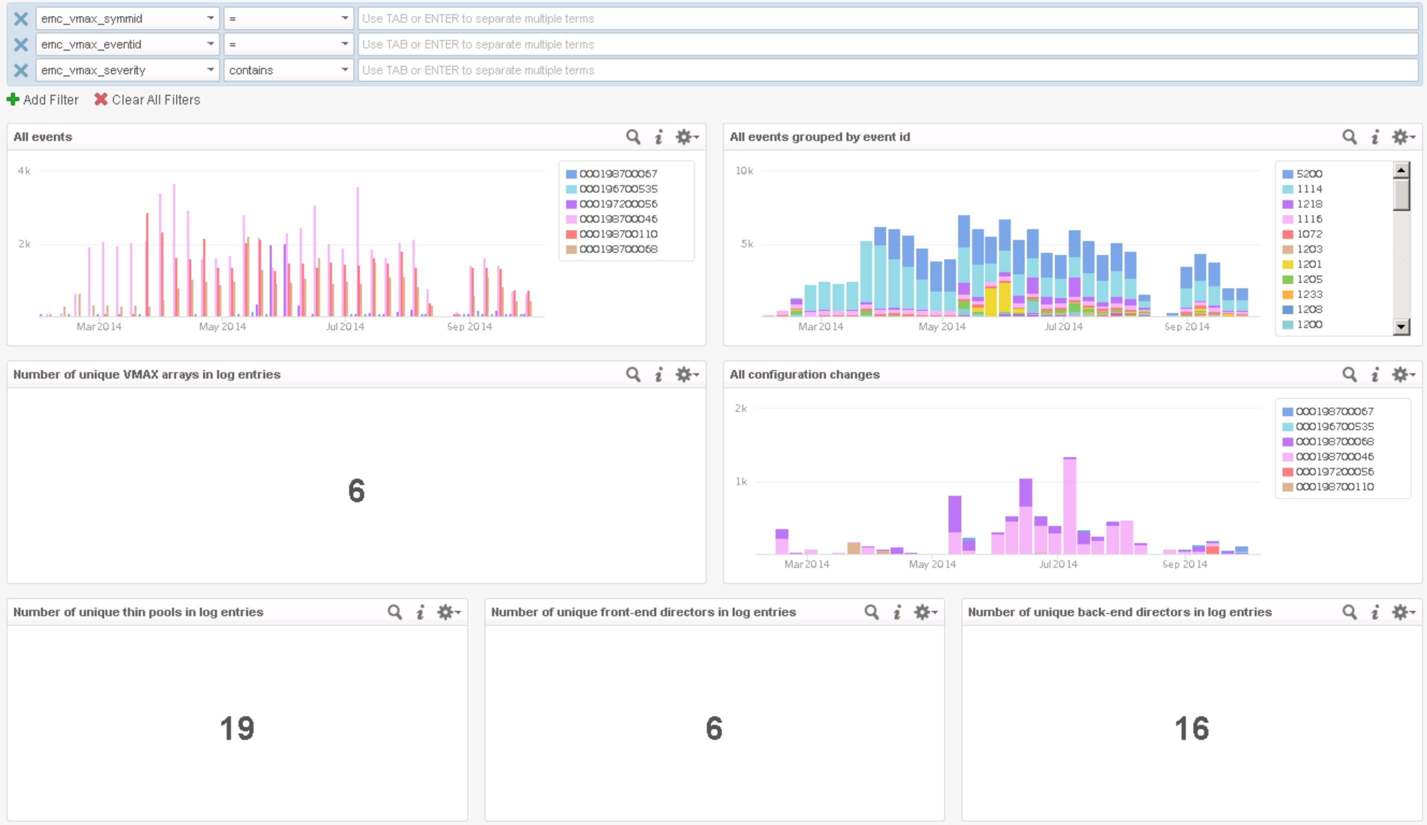
Dashboards

Included below are the seven dashboards that comprise the VMAX content pack. They are:

- **Overview** – Contains widgets with information about all VMAX data in your Log Insight instance.

- **Problems** – Contains widgets with information about potential problems that are recorded in the log files.
- **Local & remote replication** – Contains widgets specific to log messages generated by SRDF™ or TimeFinder™ software.
- **Virtual provisioning overview** – Contains widgets with information about thin pool and device events.
- **Director events** – Contains widgets with information about any front-end or back-end director events on the VMAX.
- **FAST VP** – Contains widgets with metrics specific to FAST VP.
- **Auditing** – Contains widgets that display all audit log information.

Examples of the first five dashboards, in order, are presented in Figure 2, Figure 3, Figure 4, Figure 5, Figure 6, and Figure 7. The auditing dashboard is covered in the Appendix: EMC VMAX Content Pack and VMAX Auditing Data.



emc_vmax_symmid = Use TAB or ENTER to separate multiple terms

emc_vmax_eventid = Use TAB or ENTER to separate multiple terms

emc_vmax_severity contains Use TAB or ENTER to separate multiple terms

All events

All events grouped by event id

Number of unique VMAX arrays in log entries: 6

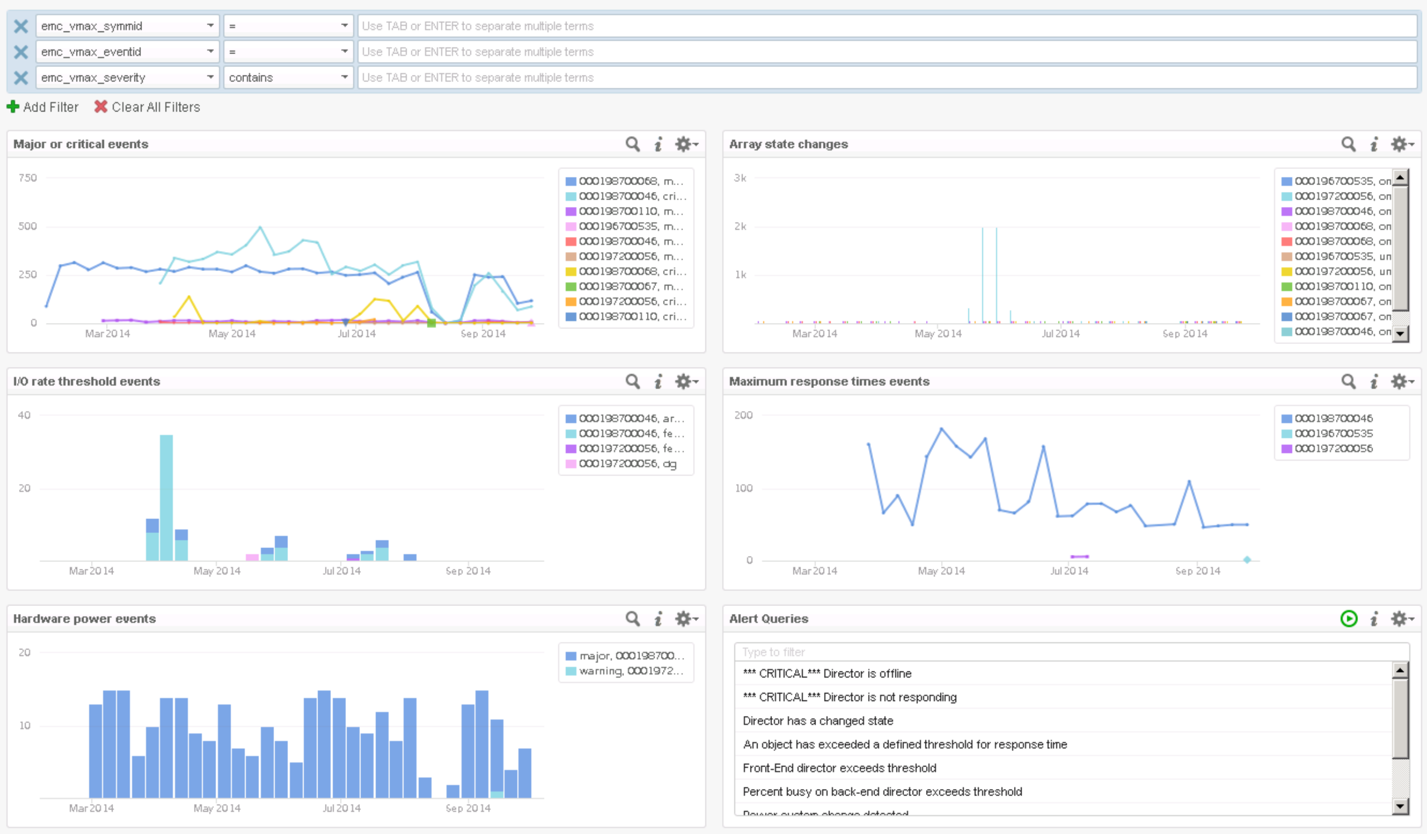
All configuration changes

Number of unique thin pools in log entries: 19

Number of unique front-end directors in log entries: 6

Number of unique back-end directors in log entries: 16

Figure 2. VMAX content pack - Overview dashboard



emc_vmax_symmid = Use TAB or ENTER to separate multiple terms

emc_vmax_eventid = Use TAB or ENTER to separate multiple terms

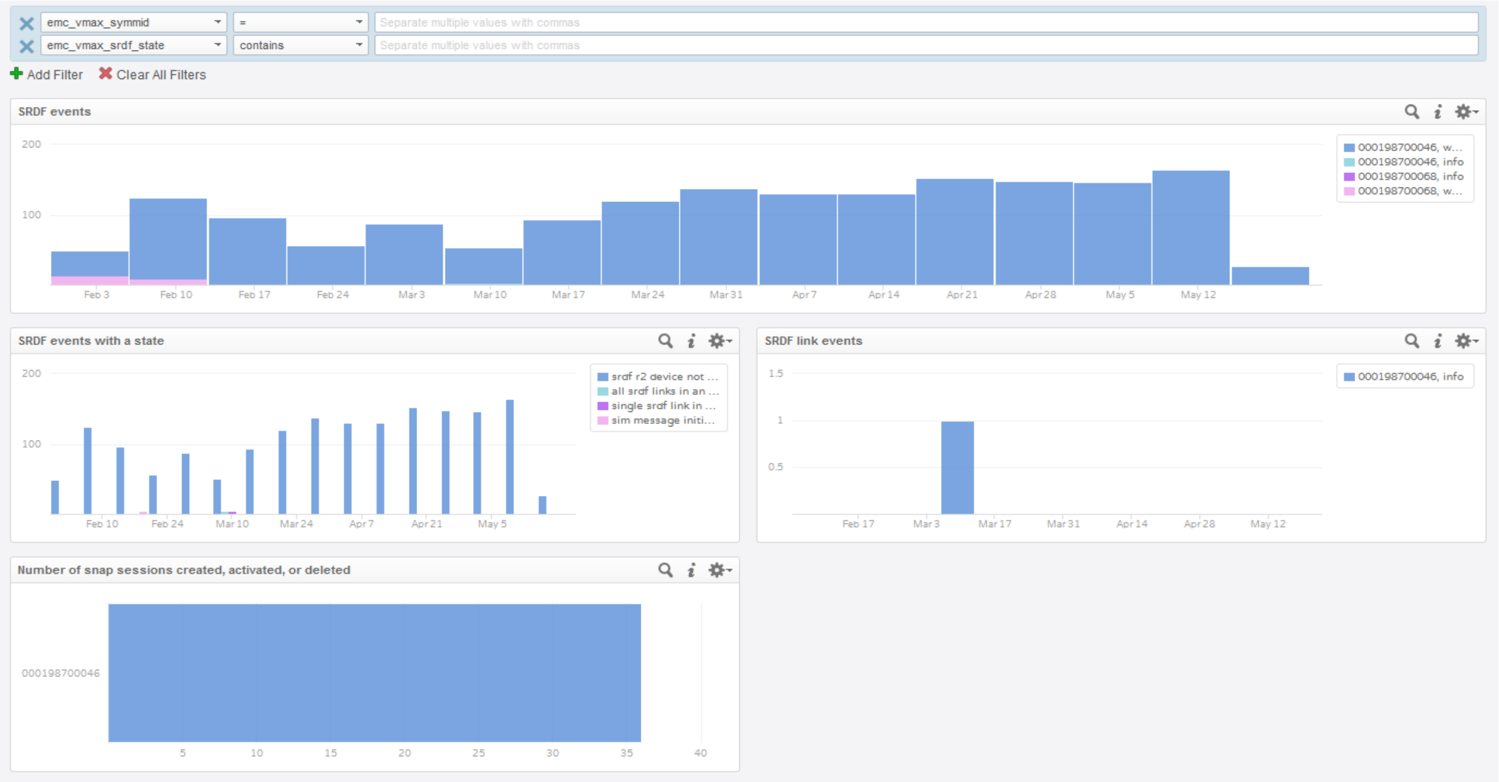
emc_vmax_severity contains Use TAB or ENTER to separate multiple terms

Alert Queries

Type to filter

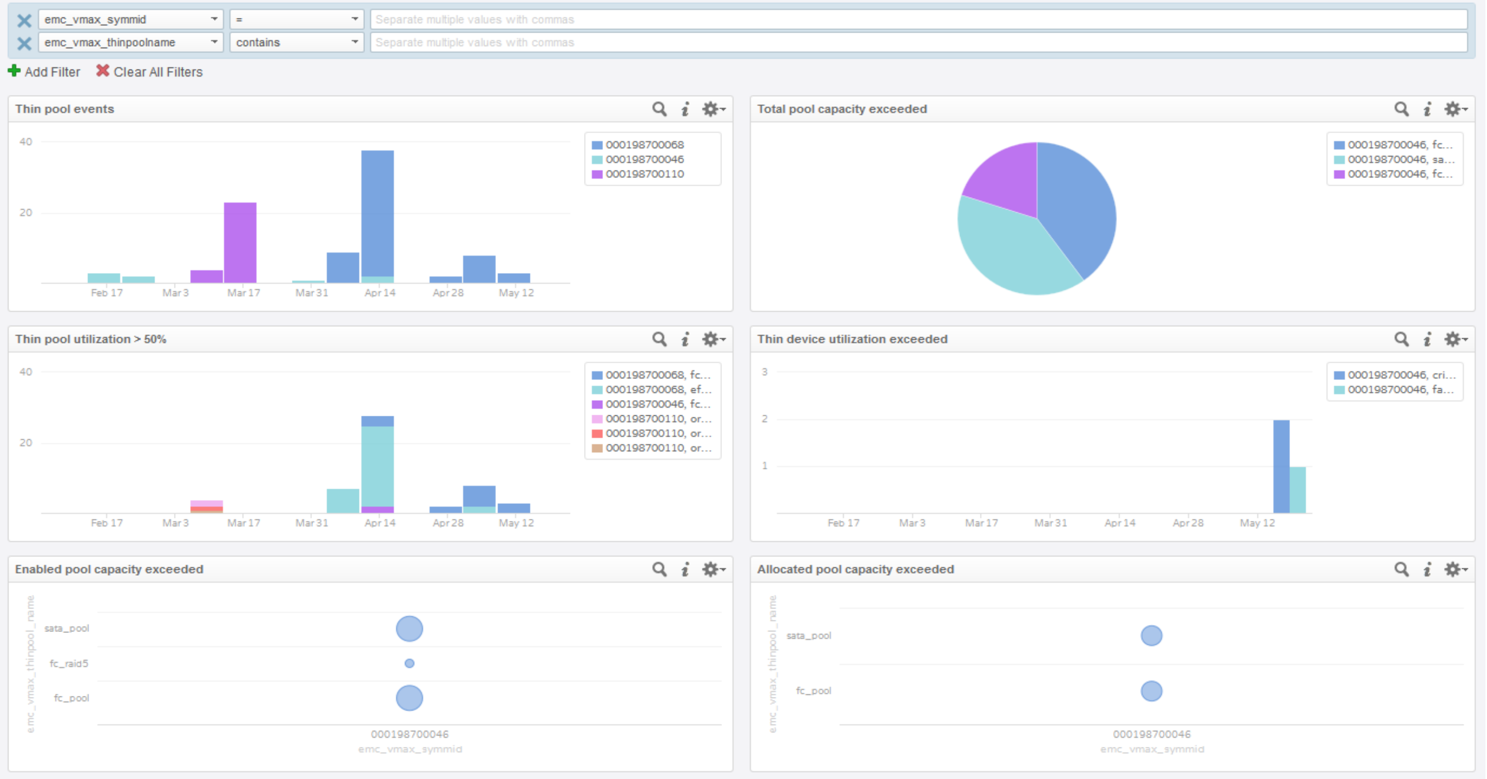
- *** CRITICAL*** Director is offline
- *** CRITICAL*** Director is not responding
- Director has a changed state
- An object has exceeded a defined threshold for response time
- Front-End director exceeds threshold
- Percent busy on back-end director exceeds threshold
- Power custom change detected

Figure 3. VMAX content pack - Problems dashboard


emc_vmax_symmid = Separate multiple values with commas

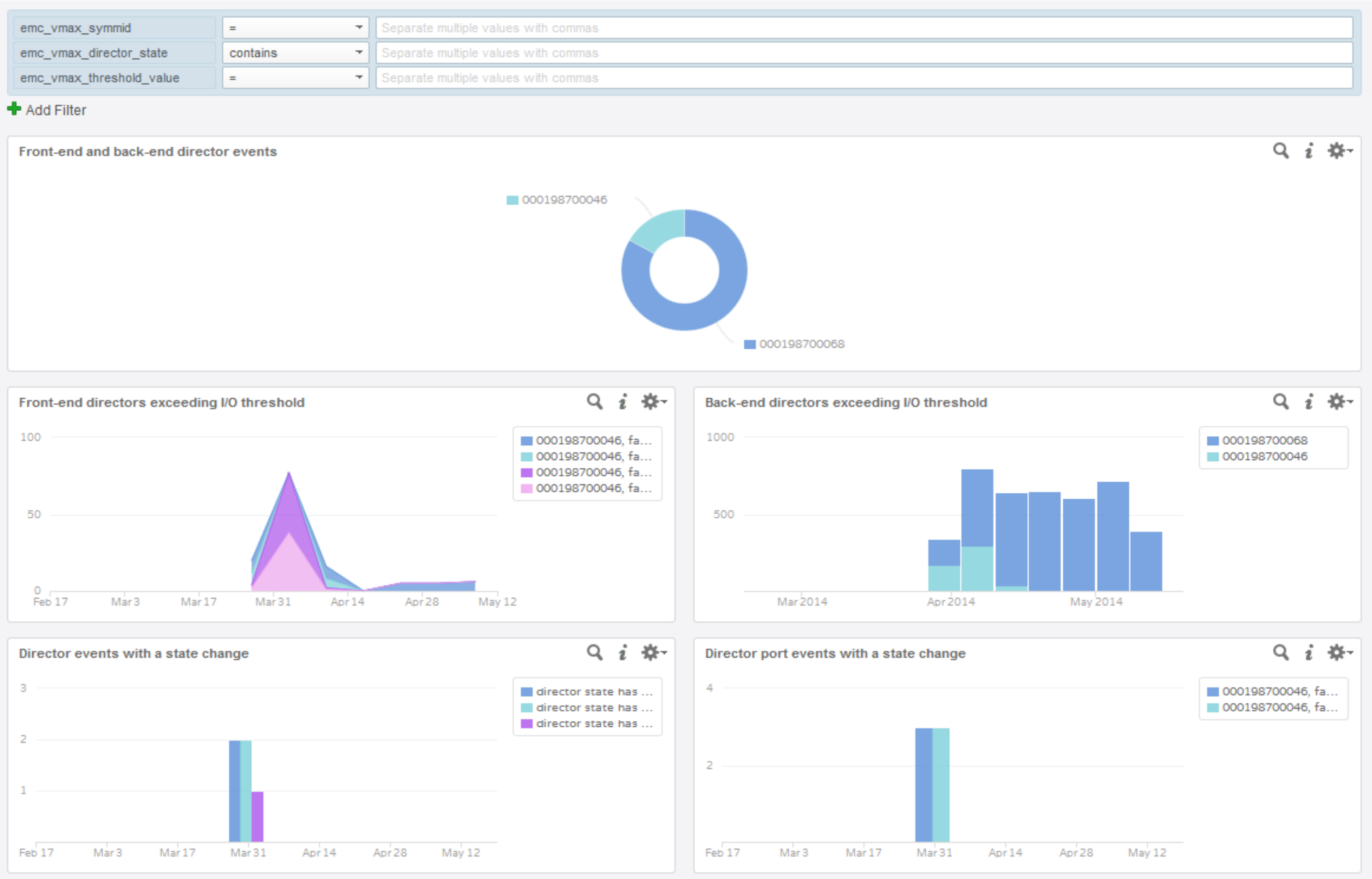
emc_vmax_srdf_state contains Separate multiple values with commas

Figure 4. VMAX content pack - Local & remote replication dashboard


emc_vmax_symmid = Separate multiple values with commas

emc_vmax_thinpoolname contains Separate multiple values with commas

Figure 5. VMAX content pack - Virtual provisioning overview dashboard

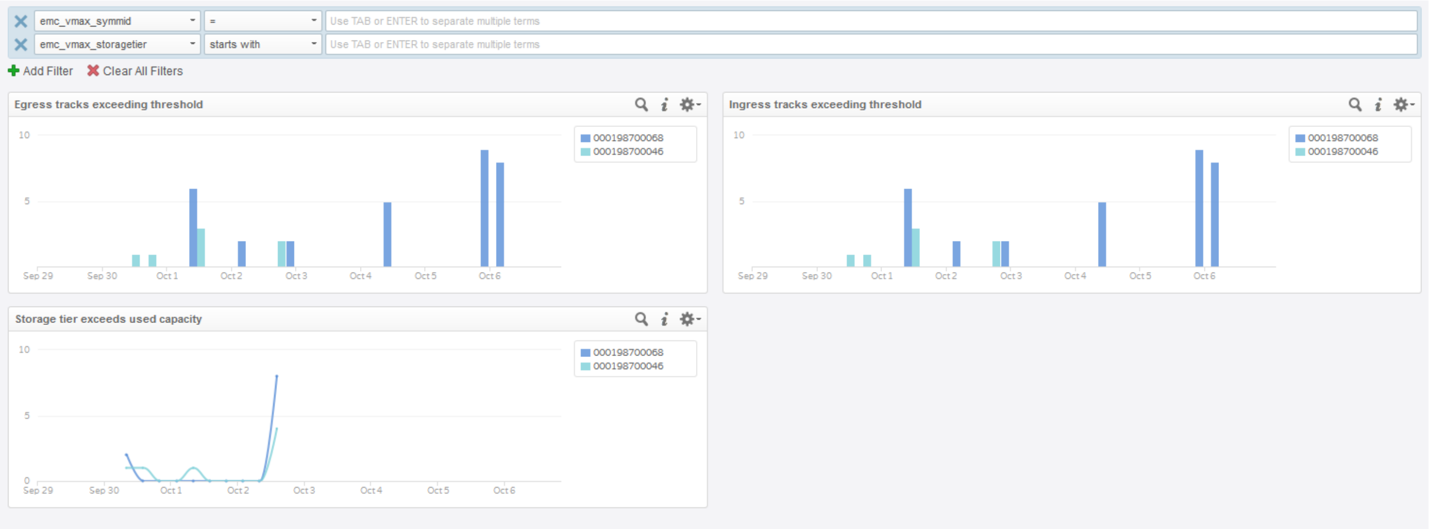


emc_vmax_symmid = Separate multiple values with commas

emc_vmax_director_state contains Separate multiple values with commas

emc_vmax_threshold_value = Separate multiple values with commas

Figure 6. VMAX content pack - Director events dashboard



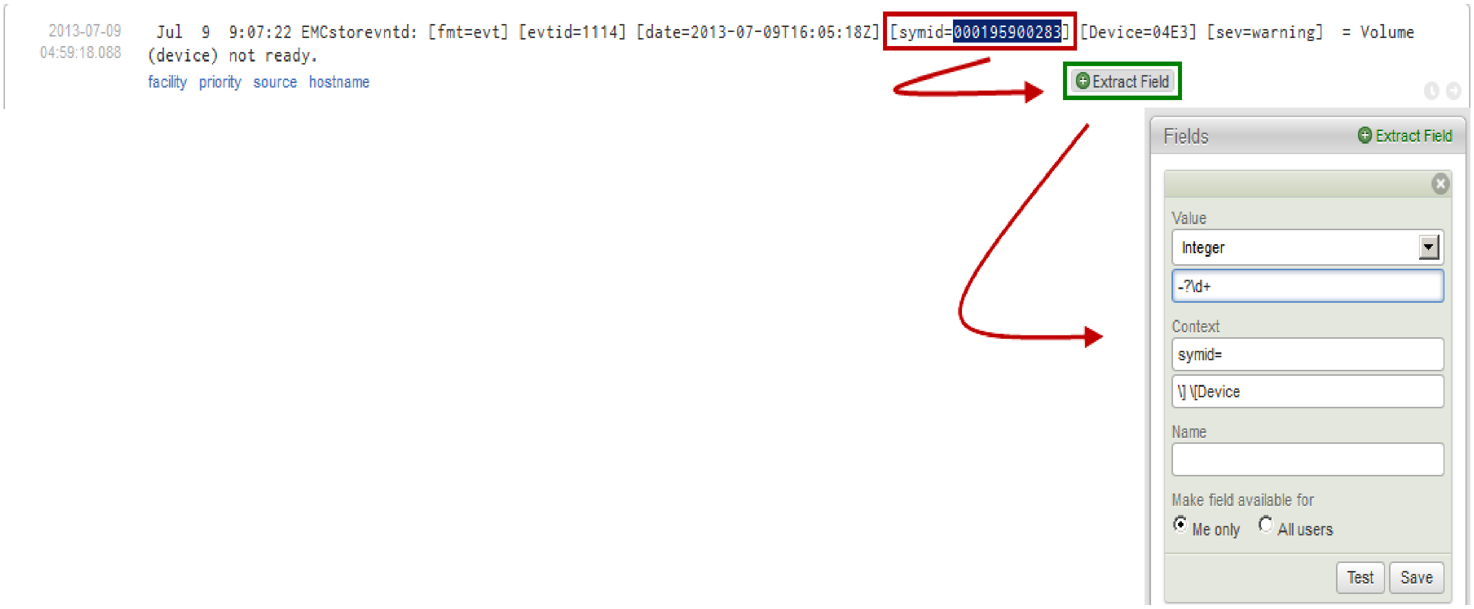
emc_vmax_symmid = Use TAB or ENTER to separate multiple terms

emc_vmax_storagetier starts with Use TAB or ENTER to separate multiple terms

Figure 7. VMAX content pack - FAST VP dashboard

User-defined fields

In large environment with numerous log messages, it is difficult to locate instantly the data fields that are important to you. Log Insight provides runtime field extraction to address this problem. You can dynamically extract any field from the data by providing a regular expression. For instance, given the log entry in Figure 8, individual fields can be identified for extraction.



```
2013-07-09    Jul  9  9:07:22 EMCstorevntd: [fmt=evt] [evtid=1114] [date=2013-07-09T16:05:18Z] [symid=000195900283] [Device=04E3] [sev=warning]  = Volume
04:59:18.088  (device) not ready.
              facility  priority  source  hostname
```

Fields

Value

Integer

-?\d+

Context

symid=

\] \[Device

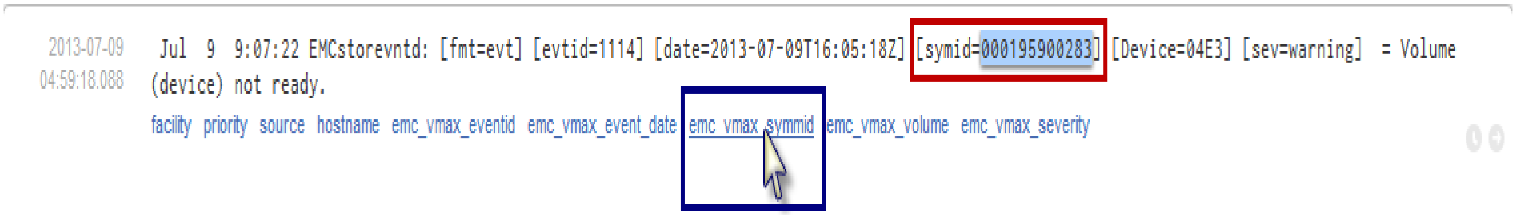
Name

Make field available for

● Me only ○ All users

Figure 8. A VMAX log entry - user-defined field extraction

By highlighting the value, an Extract Field icon appears which can be selected. Once clicked, a regular expression can be applied so that every time the *symid* term appears in a log, the newly created user-defined field will appear in the list of terms below the log entry as in Figure 9. By hovering the cursor over the new field, the symid value will be highlighted in blue.



```
2013-07-09    Jul  9  9:07:22 EMCstorevntd: [fmt=evt] [evtid=1114] [date=2013-07-09T16:05:18Z] [symid=000195900283] [Device=04E3] [sev=warning]  = Volume
04:59:18.088  (device) not ready.
              facility  priority  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_volume  emc_vmax_severity
```

Figure 9. User-defined field emc_vmax_symmid

Within the VMAX content pack, EMC has preconfigured user-defined fields for the most commonly appearing objects in the log files. All of the fields have the prefix “emc_vmax_” so they can be easily identified. Note that as some VMAX logs present data differently, more than one user-defined field is required to represent an object, e.g. thin pool. The fields are generally self-explanatory.

- emc_vmax_array_state
- emc_vmax_be_director
- emc_vmax_devices
- emc_vmax_director_name
- emc_vmax_director_state
- emc_vmax_egress_tracks
- emc_vmax_event_date
- emc_vmax_event_format_type
- emc_vmax_eventid
- emc_vmax_fe_director
- emc_vmax_ingress_tracks
- emc_vmax_iorate
- emc_vmax_objecttype
- emc_vmax_pctbusy
- emc_vmax_pcthit
- emc_vmax_percent
- emc_vmax_port_name
- emc_vmax_port_status
- emc_vmax_portgroup
- emc_vmax_power
- emc_vmax_response_time
- emc_vmax_severity
- emc_vmax_srdf_group
- emc_vmax_srdf_state
- emc_vmax_storagegrp
- emc_vmax_storagetier
- emc_vmax_symmid
- emc_vmax_system
- emc_vmax_text
- emc_vmax_thinpool_name
- emc_vmax_thinpoolname

- emc_vmax_threshold_value
- emc_vmax_used_capacity
- emc_vmax_volume

The content pack can be imported into the user space, if desired, so it can be edited. If it is installed as a content pack, however, it will be read-only; however both the widgets and dashboards can be cloned so that users can customize to their own environments

Alerts

The content pack contains a selection of default alerts for VMAX events. While the alerts are named to make their purpose self-explanatory, EMC provides detailed notes for each one in the content pack, just as it does with the dashboard widgets and queries. There are 9 alerts:

- Front-End director exceeds threshold
- Thin Pool utilization exceeds 80%
- Total thin pool capacity exceeded
- Director is not responding
- Director is offline
- A front-end or back-end director has changed state
- An object has exceeded a defined threshold for response time
- Power system change detected
- Percent busy on back-end director exceeds threshold

Content pack alerts are always set to disabled and must be manually activated. For those alerts that EMC strongly recommends enablement, they are prefixed with *** CRITICAL ***. Note that these alerts are incorporated into a widget in the Problems dashboard and can be executed as queries.

Queries

The content pack also contains a couple queries. These queries are:

- Directors that stopped responding
- Directors that are offline

The two included queries are for specific conditions of the back-end directors.

Log event viewing

The VMAX content pack displays existing log information in the database. For the VMAX, both Solutions Enabler and Unisphere for VMAX can be configured to send logs to Log Insight. The rest of this paper explains how to setup those products to do that, as well as an example of how to use the content pack once configured.

EMC VMAX Content Pack Configuration for VMware vRealize Log Insight

Solutions Enabler and the Event daemon

In order to use the EMC VMAX Content Pack, it is necessary to configure EMC Solutions Enabler to send log information to the VMware vRealize Log Insight syslog server.[1] An EMC Solutions Enabler install provides your host with SYMAPI, CLARAPI, and STORAPI shared libraries for use by Solutions Enabler applications, and the Symmetrix Command Line Interface (SYMCLI) for use by storage administrators and systems engineers.

SYMCLI is a specialized library of UNIX-formatted commands that can be invoked one at a time. It supports single command line entries and scripts to map and perform control operations on devices and data objects toward the management of your storage complex. It also monitors device configuration and status of devices that make up the storage environment. The target storage environments are typically Symmetrix arrays.

Solutions Enabler also has a built-in capability to monitor the Symmetrix event log and send all of those event messages to a remote syslog server (or a file, or SNMP etc.). It accomplishes this through one of its daemons, the Event daemon or "storevntd". By default, the Event daemon does not issue events to a remote syslog server. This has to be configured first. Storevntd can be customized to send events in a number of categories, as well as sending events from Unisphere for VMAX, including the Performance option. A basic setup will be presented herein. This setup should be sufficient for both VMAX and VMAX^3 arrays. For more detailed information please refer to the appropriate EMC Solutions Enabler Installation Guide.

Configuring Solutions Enabler

Once Solutions Enabler is installed (and gatekeepers presented per the Install Guide) the Event daemon can be configured to use syslog. First install the storevntd if not already done. It is best to enable autostart so the daemon will start back up automatically when/if the server is rebooted. To install the daemon and enable autostart, issue the following command:

```
stordaemon install storevntd -autostart
```

The behavior of the storevntd (like all daemons) is controlled by the file "daemon_options". The location of this file changes according to operating system. The SE Install Guide will have this information. In this Windows example, the location is: C:\Program Files\EMC\SYMAPI\config\.

Within the file there are sections for each daemon, including storevntd. There are many options for storevntd, but only a few are pertinent to the setup for Log Insight. These are (note the entries will be commented out):

[1] EMC suggests using Solutions Enabler 7.5 and higher with the VMAX content pack when using VMAX arrays.

```
#storevntd:LOG_EVENT_TARGETS

#storevntd:LOG_EVENT_SYSLOG_HOST

#storevntd:LOG_EVENT_SYSLOG_PORT

#storevntd:LOG_SYMMETRIX_EVENTS
```

Each entry is detailed below along with an example.

The "`LOG_EVENT_TARGETS`" option indicates to storevntd which type of message it should issue. To use syslog, simply set it to "syslog". Note that multiple entries are acceptable for this option, for instance if a file is required in addition to syslog it would simply be "syslog,file" (other options are needed for file).

```
storevntd:LOG_EVENT_TARGETS = syslog
```

The options "`LOG_EVENT_SYSLOG_HOST`" and "`LOG_EVENT_SYSLOG_PORT`" are self-explanatory. Provide the Log Insight host IP and the port of the syslog server on the host. For Log Insight this is the default port for syslog of 514.

```
storevntd:LOG_EVENT_SYSLOG_HOST = 192.168.160.153

storevntd:LOG_EVENT_SYSLOG_PORT = 514
```

The last option, "`LOG_SYMMETRIX_EVENTS`" is the one that determines exactly what information will be sent to Log Insight. There are a number of categories to choose from, though the VMAX Content Pack takes advantage of all of them. By default, any category will apply to all VMAX arrays presented to Solutions Enabler unless the array SID is specifically listed. Both a generic and specific example are below:

```
storevntd:LOG_SYMMETRIX_EVENTS = status, groups, optimizer, events,
array subsystem, checksum, diagnostic, environmental, device pool,
service processor, srdf system, srdf link, srdfa session, srdf
consistency group, director, device, disk, smc, spa ;\
```

```
storevntd:LOG_SYMMETRIX_EVENTS = sid=00019570xxxx, status, groups,
optimizer, events, array subsystem, checksum, diagnostic, environmental,
device pool, service processor, srdf system, srdf link, srdfa session,
srdf consistency group, director, device, disk, smc, spa ;\
```

There are many different filters that can be applied to each category to reduce or increase the amount of data sent. It may be preferable to start with everything in a test environment and then tweak the categories until just the messages of interest are sent to Log Insight.

Unisphere for VMAX and the Performance option

The last two entries in the "`LOG_SYMMETRIX_EVENTS`" are "smc" and "spa". These two categories refer to the alerts that Unisphere for VMAX and the Performance option generate. Unlike the other categories, however, these alerts are not enabled by default. Configuration within Unisphere requires enabling the events to be sent to the syslog server. A basic configuration is shown in the next section for both Unisphere for VMAX version 1.6 and 8.x.

Syslog event configuration

As the system administrator user (default *smc* user in this example), log in to Unisphere and navigate to the Common Task "Administration". Under that task select "Alert Settings" and then "Notifications". This is seen in Figure 10 for Unisphere for VMAX 1.6.x and Figure 11 for version 8.x.

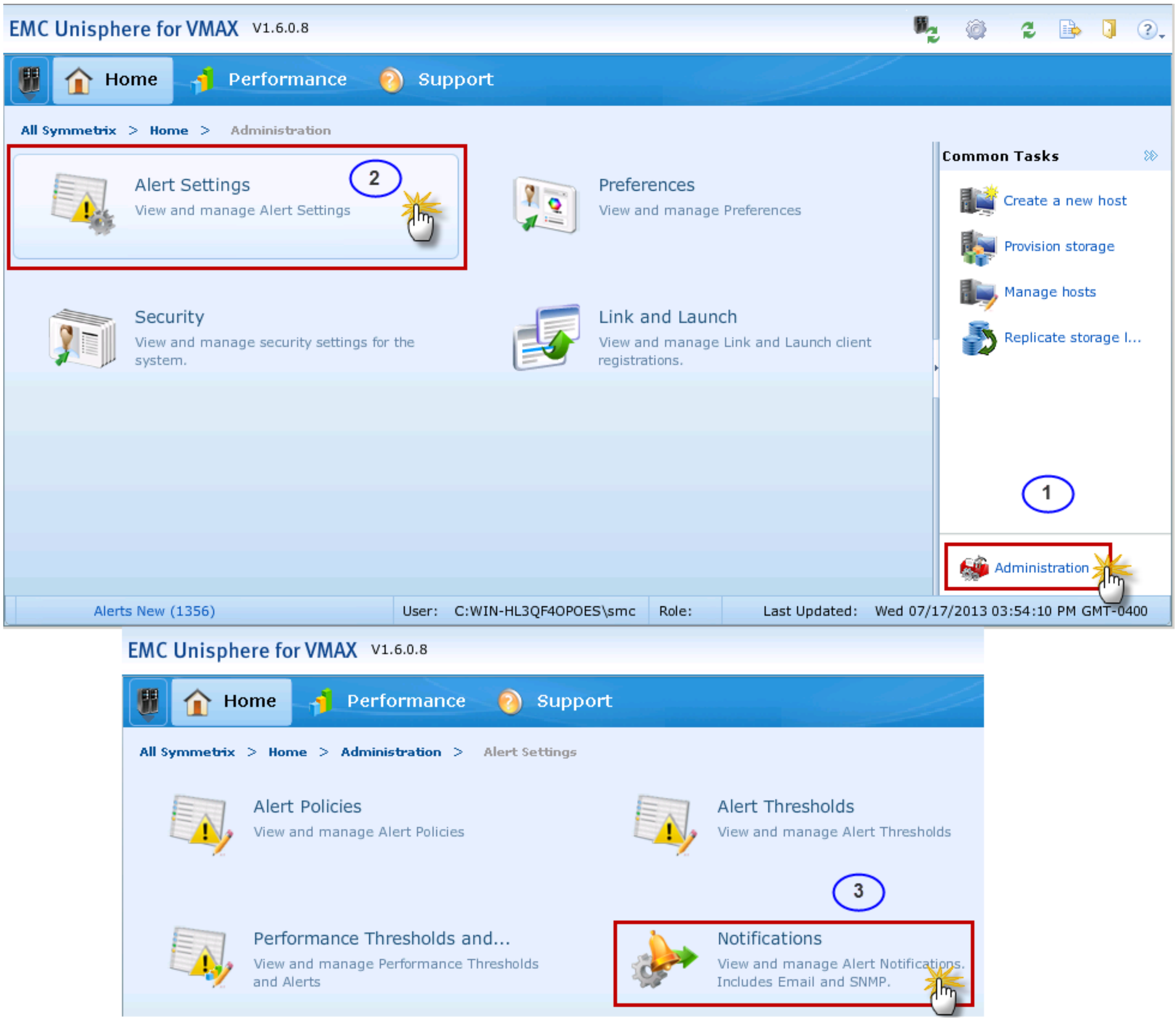
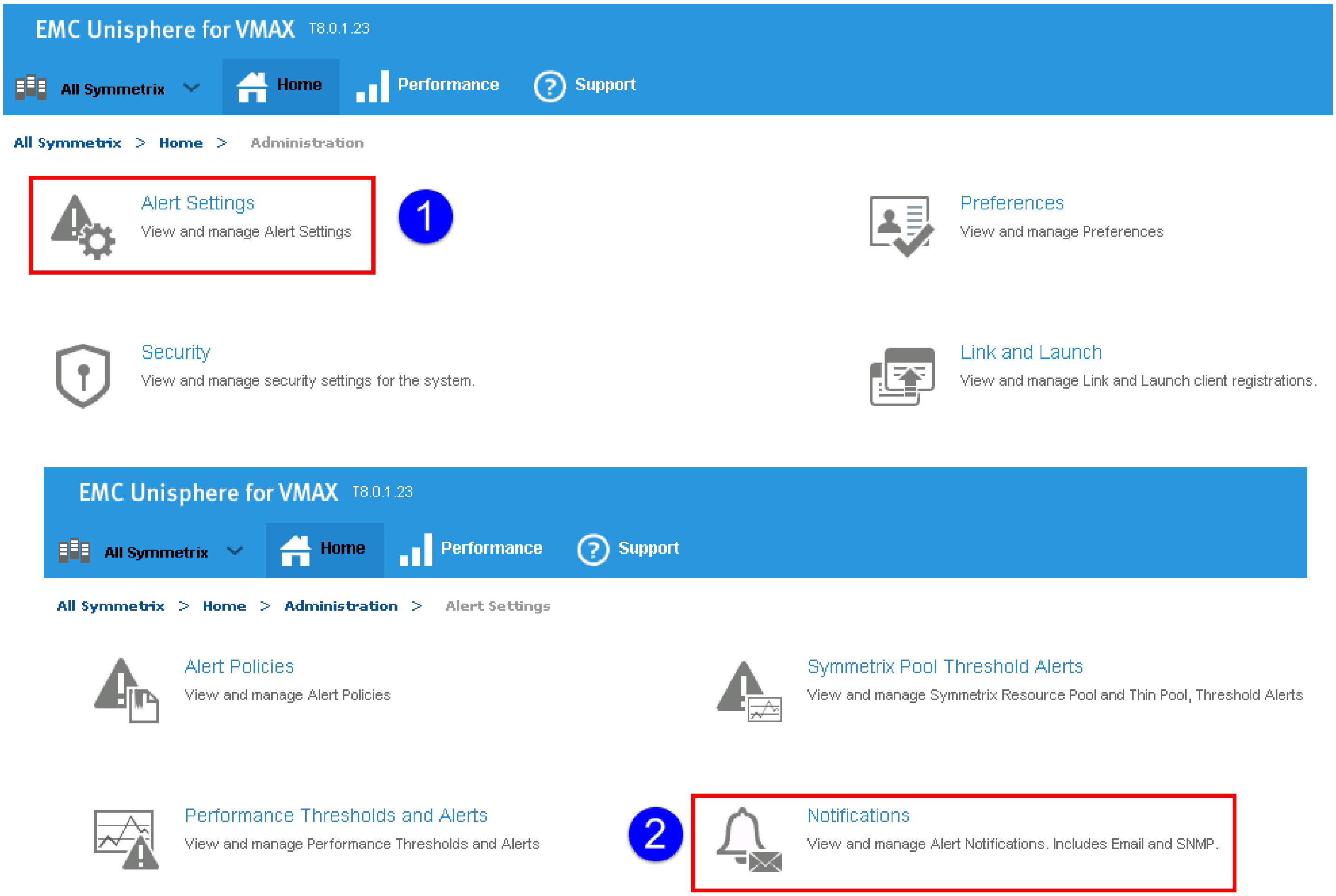

EMC Unisphere for VMAX V1.6.0.8
Home
Performance
Support
All Symmetrix > Home > Administration
Alert Settings
View and manage Alert Settings
2
Preferences
View and manage Preferences
Security
View and manage security settings for the system.
Link and Launch
View and manage Link and Launch client registrations.
Common Tasks
Create a new host
Provision storage
Manage hosts
Replicate storage l...
1
Administration
Alerts New (1356)
User: C:WIN-HL3QF4OPOES\smc
Role:
Last Updated: Wed 07/17/2013 03:54:10 PM GMT-0400
EMC Unisphere for VMAX V1.6.0.8
Home
Performance
Support
All Symmetrix > Home > Administration > Alert Settings
Alert Policies
View and manage Alert Policies
Alert Thresholds
View and manage Alert Thresholds
3
Performance Thresholds and...
View and manage Performance Thresholds and Alerts
Notifications
View and manage Alert Notifications. Includes Email and SNMP.

Figure 10. Alert Settings in Unisphere for VMAX v1.6



EMC Unisphere for VMAX T8.0.1.23

All Symmetrix > Home > Administration

1

Alert Settings
View and manage Alert Settings

Preferences
View and manage Preferences

Security
View and manage security settings for the system.

Link and Launch
View and manage Link and Launch client registrations.

EMC Unisphere for VMAX T8.0.1.23

All Symmetrix > Home > Administration > Alert Settings

Alert Policies
View and manage Alert Policies

Symmetrix Pool Threshold Alerts
View and manage Symmetrix Resource Pool and Thin Pool, Threshold Alerts

Performance Thresholds and Alerts
View and manage Performance Thresholds and Alerts

2

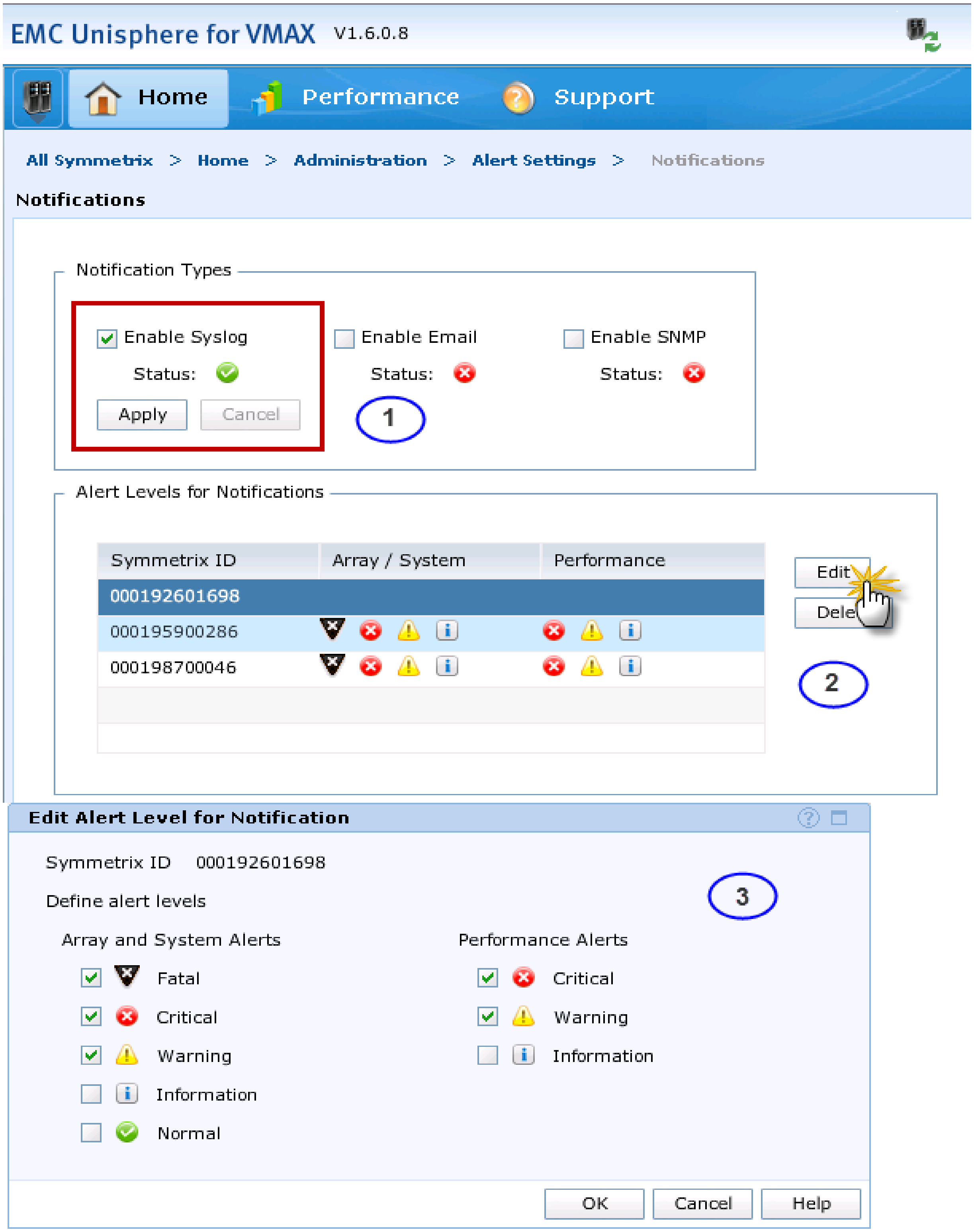
Notifications
View and manage Alert Notifications. Includes Email and SNMP.

Figure 11. Alert Settings in Unisphere for VMAX v8.x

Once in the Notifications screen, the user can select the manner in which they wish to be notified, if at all, of events. Figure 12 demonstrates the three steps required to setup the alerts in Unisphere for VMAX 1.6.

First, check the box to enable syslog and select “Apply”. This allows Unisphere to send its alerts to the syslog server that is configured in Solutions Enabler. Unisphere relies upon the configuration in Solutions Enabler as previously explained in Configuring Solutions Enabler. Unisphere has no capability to configure syslog settings for server or port in the GUI interface.

Once syslog is enabled, in steps two and three assign each array alert levels by highlighting the array and selecting “Edit”. The alert level dialog appears upon editing. There are two types of alerts: Array and System Alerts and Performance Alerts. The former alert is for Unisphere in general and the latter is for the performance option of Unisphere. Check the boxes for the level(s) for which you wish to receive alerts.


EMC Unisphere for VMAX V1.6.0.8
Home
Performance
Support
All Symmetrix > Home > Administration > Alert Settings > Notifications
Apply
Cancel
1
Edit
Dele
2
3
OK
Cancel
Help

Notifications

Notification Types

☑ Enable Syslog Status: ✓

☐ Enable Email Status: ✗

☐ Enable SNMP Status: ✗

Alert Levels for Notifications

Symmetrix ID	Array / System	Performance
000192601698		
000195900286	▼ ✗ ⚠ ℹ	✗ ⚠ ℹ
000198700046	▼ ✗ ⚠ ℹ	✗ ⚠ ℹ

Edit Alert Level for Notification

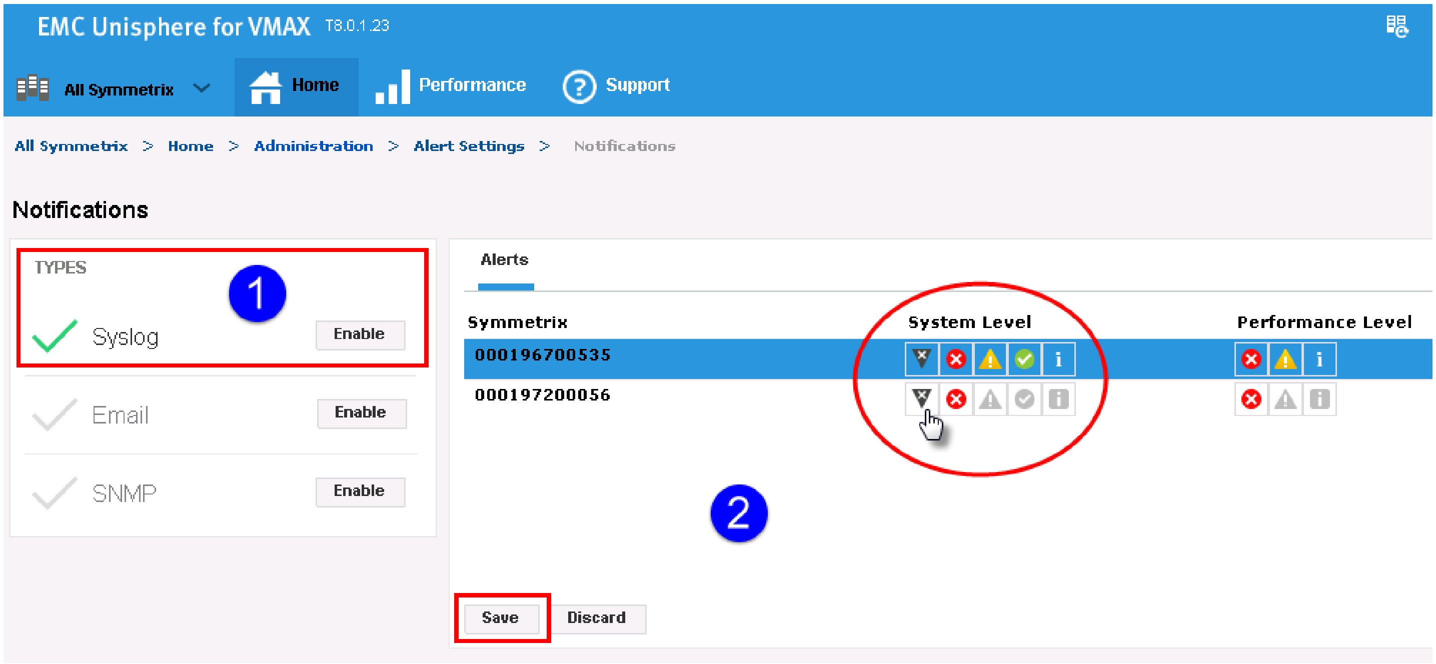
Symmetrix ID 000192601698

Define alert levels

Array and System Alerts	Performance Alerts
☑ ▼ Fatal	☑ ✗ Critical
☑ ✗ Critical	☑ ⚠ Warning
☑ ⚠ Warning	☐ ℹ Information
☐ ℹ Information	
☐ ✓ Normal	

Figure 12. Setting notification type and alert levels in Unisphere for VMAX v1.6

In Unisphere for VMAX 8.x these two screens have been merged into one, seen in Figure 13. First simply enable syslog by selecting the “Enable” button. Then on the right-hand side click the desired levels for System and Performance and select “Save’.



Symmetrix	System Level	Performance Level
000196700535	✗ ⚠ ✓ i	✗ ⚠ i
000197200056	✗ ⚠ ✓ i	✗ ⚠ i

Figure 13. Setting notification type and alert levels in Unisphere for VMAX v8.x

Setting up the events for syslog allows the default alerts to be sent when thresholds are exceeded; however, customers may wish to customize the thresholds at which those events are generated. These can be adjusted in the Alert Settings page under the following categories: Alert Policies (array level)[2], Alert Thresholds (v1.6) or Symmetrix Pool Threshold Alerts (v8.x), and Performance Thresholds and Alerts.

Creating a custom alert

The following is an example of how to set a custom alert within Unisphere.

Start by navigating to the previously shown Administration page, and then select Performance Thresholds and Alerts as in Figure 14 or Figure 15.

[2] Note that array level events in Alert Policies must have the notification setup as syslog to receive these alerts in Log Insight.

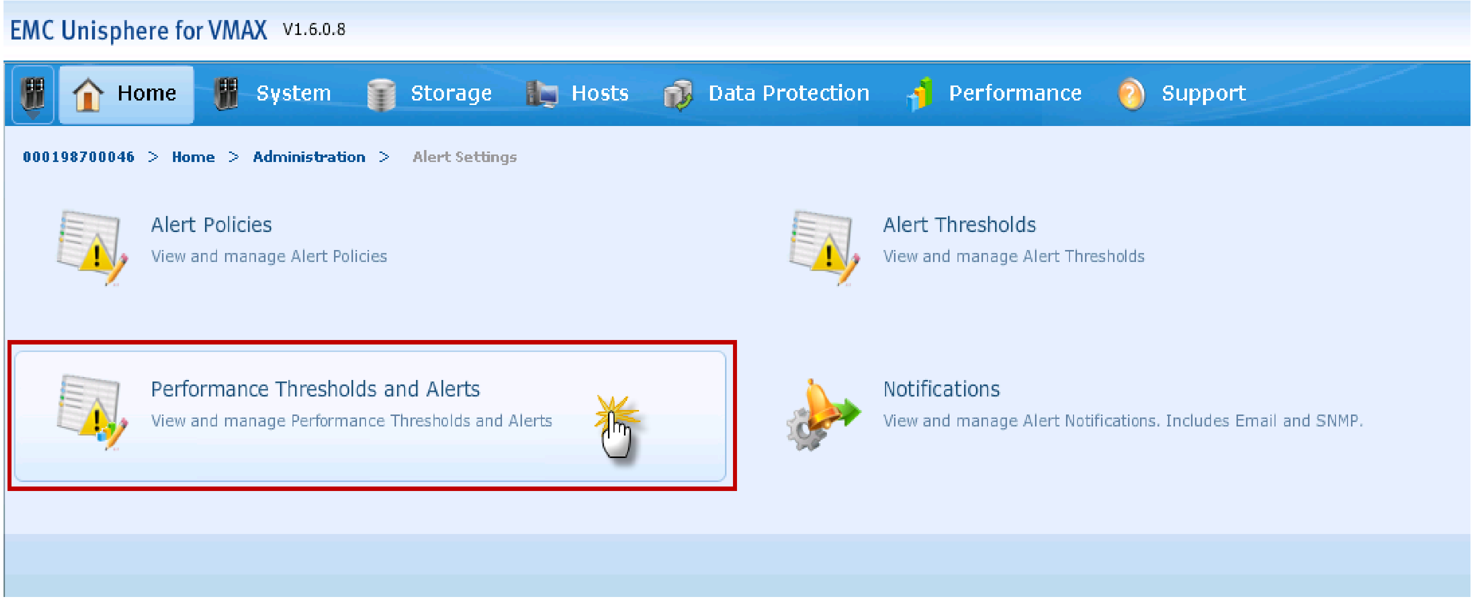

EMC Unisphere for VMAX V1.6.0.8
Home
System
Storage
Hosts
Data Protection
Performance
Support
000198700046 > Home > Administration > Alert Settings
Alert Policies
View and manage Alert Policies
Alert Thresholds
View and manage Alert Thresholds
Performance Thresholds and Alerts
View and manage Performance Thresholds and Alerts
Notifications
View and manage Alert Notifications. Includes Email and SNMP.

Figure 14. Performance Thresholds and Alerts Unisphere for VMAX v1.6

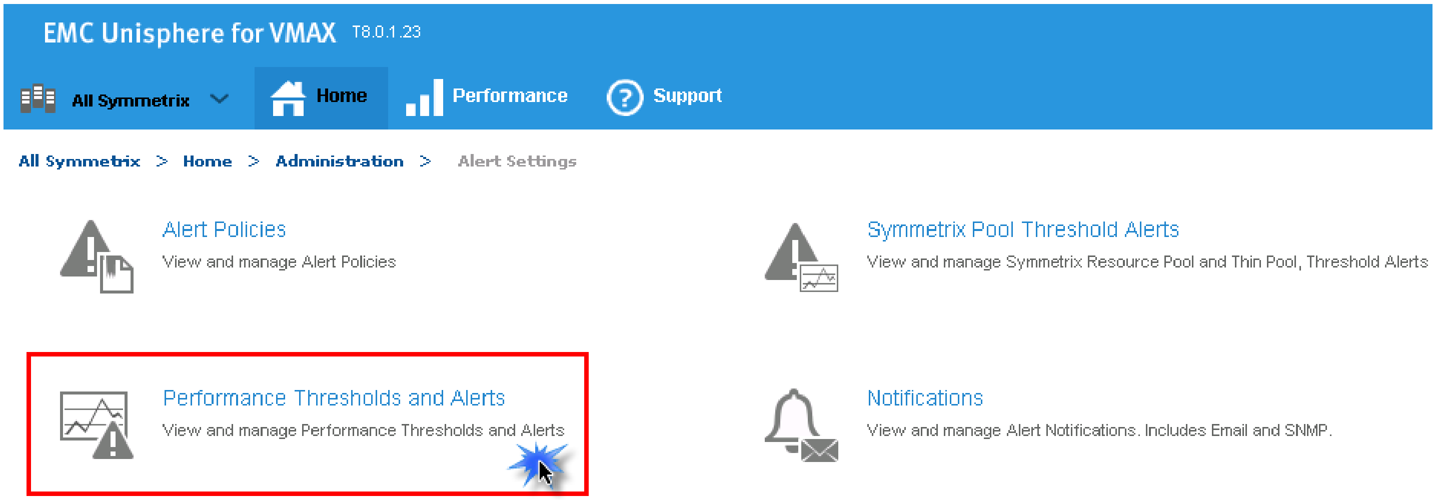
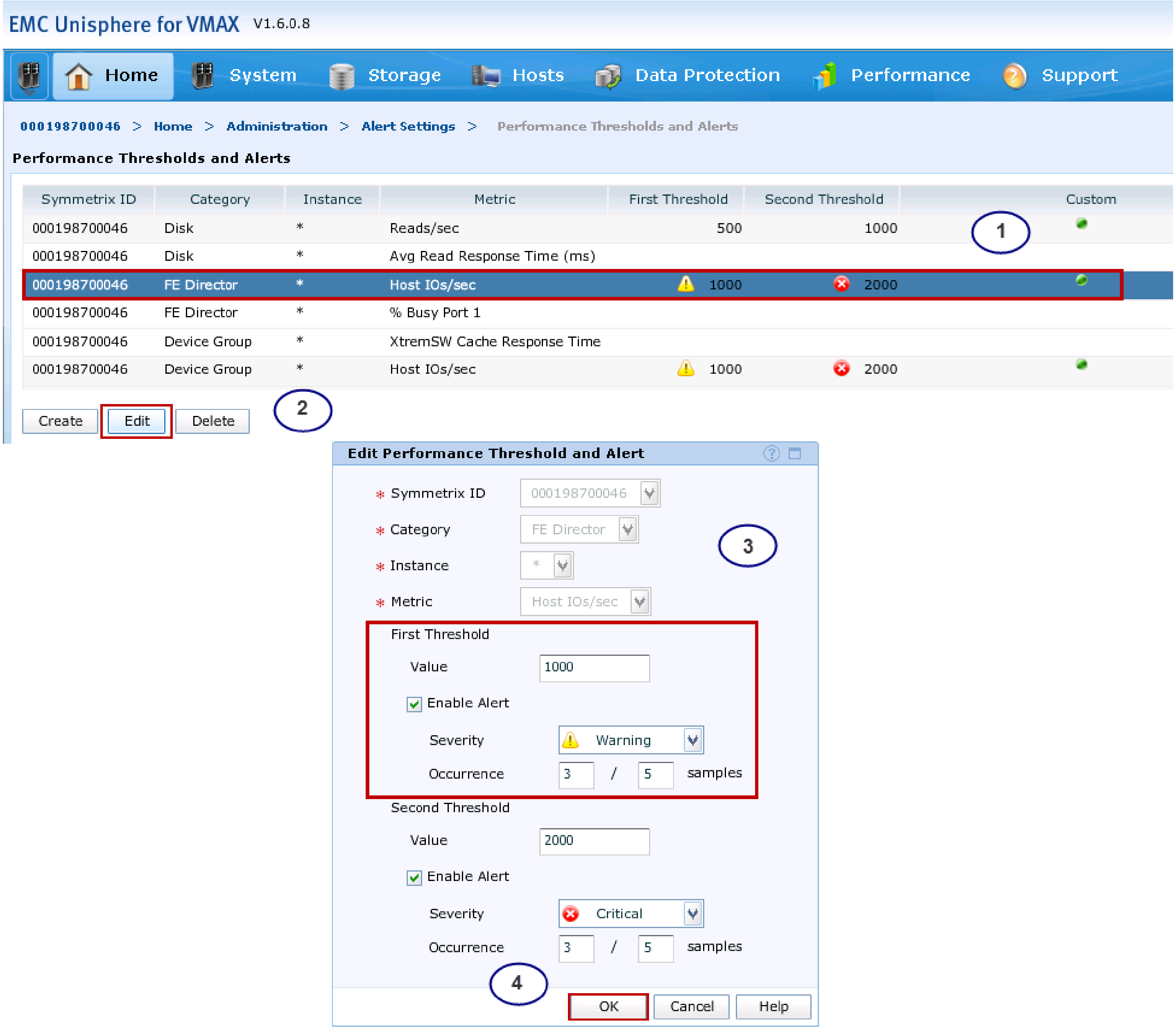

EMC Unisphere for VMAX T8.0.1.23
All Symmetrix
Home
Performance
Support
All Symmetrix > Home > Administration > Alert Settings
Alert Policies
View and manage Alert Policies
Symmetrix Pool Threshold Alerts
View and manage Symmetrix Resource Pool and Thin Pool, Threshold Alerts
Performance Thresholds and Alerts
View and manage Performance Thresholds and Alerts
Notifications
View and manage Alert Notifications. Includes Email and SNMP.

Figure 15. Performance Thresholds and Alerts Unisphere for VMAX v8.x

This now brings up the different metrics that can be customized and have alerts set upon them. Since the alerting mechanism, syslog, has already been configured, the alerts can be customized and simply activated. Figure 16 and Figure 15 walk the user through setting a custom alert on the metric Host IO/sec for an FE Director. In this example, both a Warning and Critical alert value are set. The user can enable whatever alert levels are preferable at the desired metric value limit.



000198700046 > Home > Administration > Alert Settings > Performance Thresholds and Alerts

Performance Thresholds and Alerts

Symmetrix ID	Category	Instance	Metric	First Threshold	Second Threshold	Custom
000198700046	Disk	*	Reads/sec	500	1000	●
000198700046	Disk	*	Avg Read Response Time (ms)			
000198700046	FE Director	*	Host IOs/sec	⚠ 1000	✖ 2000	●
000198700046	FE Director	*	% Busy Port 1			
000198700046	Device Group	*	XtremSW Cache Response Time			
000198700046	Device Group	*	Host IOs/sec	⚠ 1000	✖ 2000	●

Edit Performance Threshold and Alert

* Symmetrix ID	000198700046
* Category	FE Director
* Instance	*
* Metric	Host IOs/sec

First Threshold

Value 1000

☑ Enable Alert

Severity ⚠ Warning

Occurrence 3 / 5 samples

Second Threshold

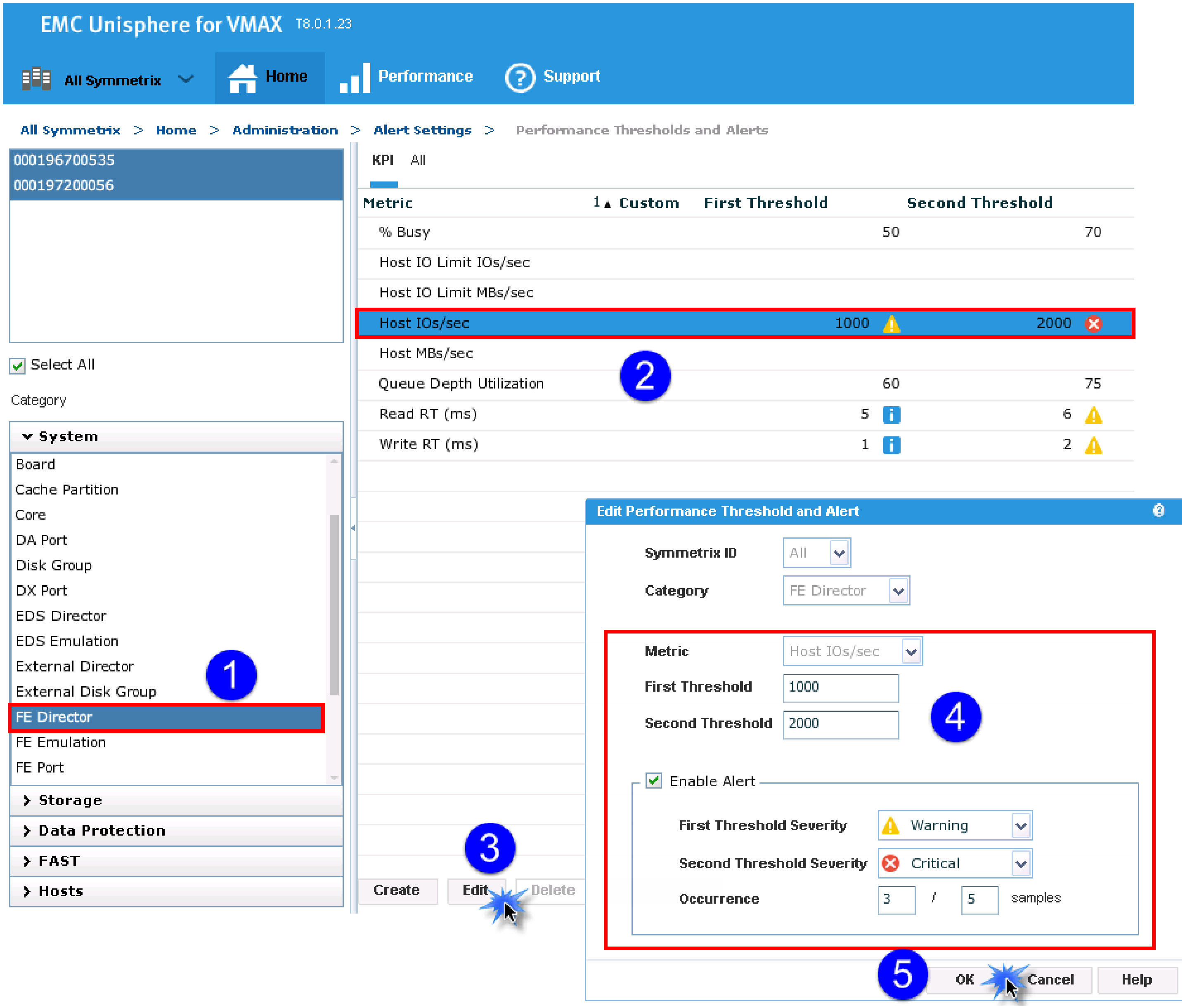
Value 2000

☑ Enable Alert

Severity ✖ Critical

Occurrence 3 / 5 samples

Figure 16. Setting a custom alert in Unisphere for VMAX v1.6



Metric	1▲ Custom	First Threshold	Second Threshold
% Busy		50	70
Host IO Limit IOs/sec			
Host IO Limit MBs/sec			
Host IOs/sec		1000 ⚠	2000 ☒
Host MBs/sec			
Queue Depth Utilization		60	75
Read RT (ms)		5 ℹ	6 ⚠
Write RT (ms)		1 ℹ	2 ⚠

Symmetrix ID: All

Category: FE Director

Metric: Host IOs/sec

First Threshold: 1000

Second Threshold: 2000

☑ Enable Alert

First Threshold Severity: ⚠ Warning

Second Threshold Severity: ☒ Critical

Occurrence: 3 / 5 samples

Figure 17. Setting a custom alert in Unisphere for VMAX v8.x

Once the alert is enabled, whenever the conditions of the alert are met, a log entry will be issued to the syslog server as well as recorded locally within Unisphere.

Please see the Unisphere for VMAX documentation on support.EMC.com more detailed information on setting alerts.

Using the VMAX Content Pack for Problem Analysis

The following sections walk a user through what could be a typical problem analysis situation. It explains how a Sysadmin and VMAdmin could use the VMAX Content

Pack to isolate an issue. Although the screenshots are from v1.0 of Log Insight, the process is essentially the same v2.x.

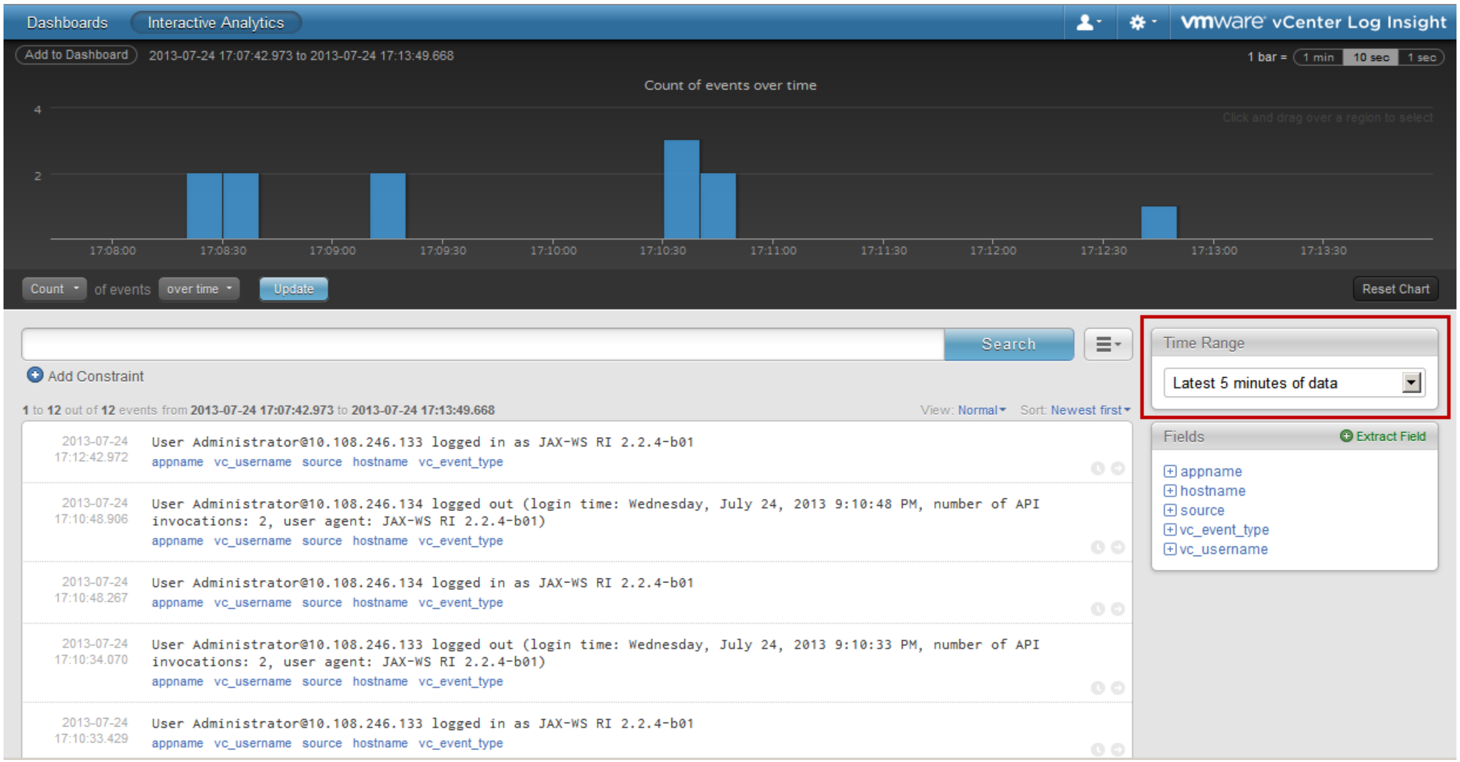
Finding high I/O to the FE directors[3]

The system administrator (Sysadmin) has noticed that the front-end directors on the VMAX array that is utilized in the VMware environment have had some heavy activity lately. The Sysadmin asks the VMware administrator (VMAdmin) to determine if there have been any occurrences when an FE director has serviced more than 6000 I/Os. This may indicate that more FE director ports need to be added to the port group.

To investigate, the VMAdmin turns to Log Insight which he has previously configured to accept log files from Solutions Enabler and Unisphere for VMAX. He also has implemented the VMAX content pack to help make the analysis easier. Within Unisphere for VMAX he has previously defined two thresholds for FE ports. When I/Os reach 1000, a warning severity will be issued and then if I/Os surpass 2000 a critical severity will be issued. Therefore he can expect two log entries for any FE director servicing more than 6000 I/Os since they would breach both these thresholds.

He starts by opening the Interactive Analytics page, seen in Figure 18, which will allow him to make queries into the log files collected.

[3] The I/O numbers used in this example are entirely arbitrary.



2013-07-24 17:07:42.973 to 2013-07-24 17:13:49.668

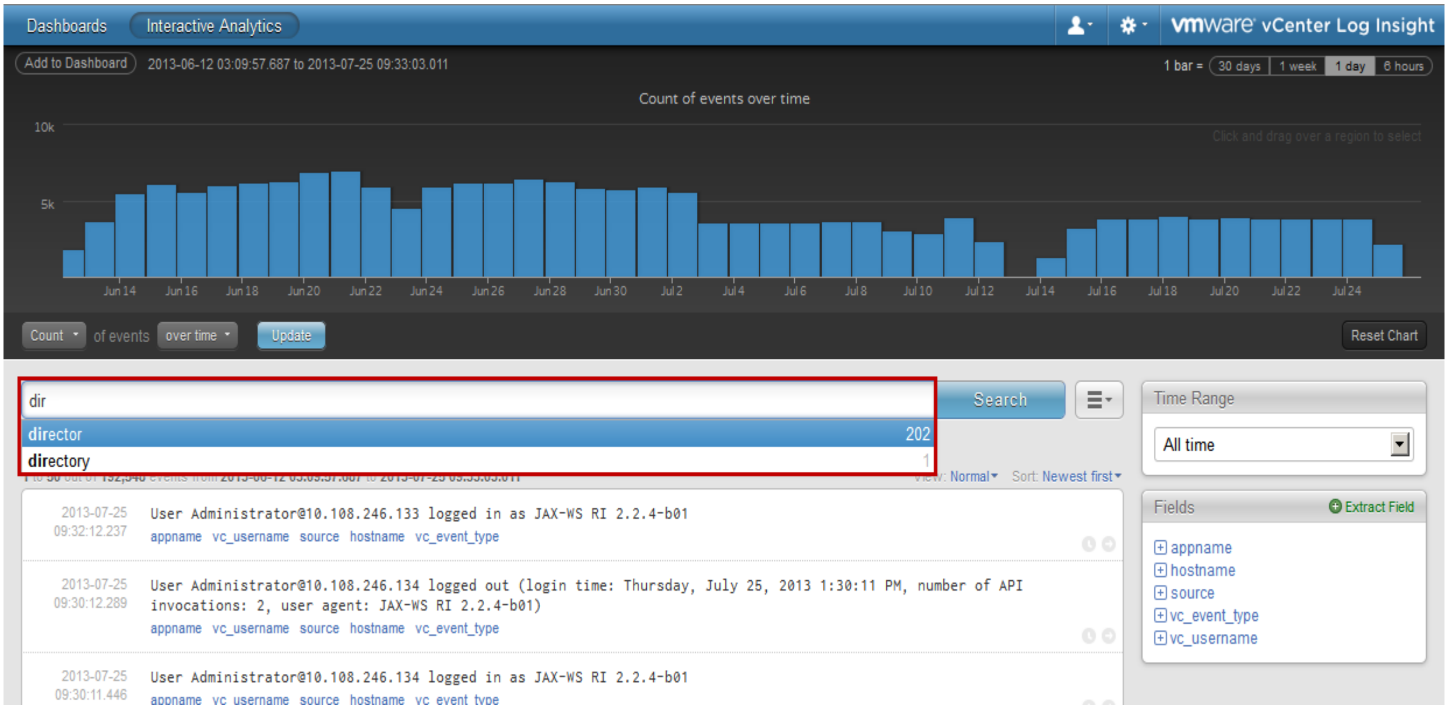
Time Range: Latest 5 minutes of data

1 to 12 out of 12 events from 2013-07-24 17:07:42.973 to 2013-07-24 17:13:49.668

```
2013-07-24     User Administrator@10.108.246.133 logged in as JAX-WS RI 2.2.4-b01
17:12:42.972   appname  vc_username  source  hostname  vc_event_type

2013-07-24     User Administrator@10.108.246.134 logged out (login time: Wednesday, July 24, 2013 9:10:48 PM, number of API
17:10:48.906   invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
               appname  vc_username  source  hostname  vc_event_type

2013-07-24     User Administrator@10.108.246.134 logged in as JAX-WS RI 2.2.4-b01
17:10:48.267   appname  vc_username  source  hostname  vc_event_type

2013-07-24     User Administrator@10.108.246.133 logged out (login time: Wednesday, July 24, 2013 9:10:33 PM, number of API
17:10:34.070   invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
               appname  vc_username  source  hostname  vc_event_type

2013-07-24     User Administrator@10.108.246.133 logged in as JAX-WS RI 2.2.4-b01
17:10:33.429   appname  vc_username  source  hostname  vc_event_type
```

Figure 18. vRealize Log Insight Interactive Analytics

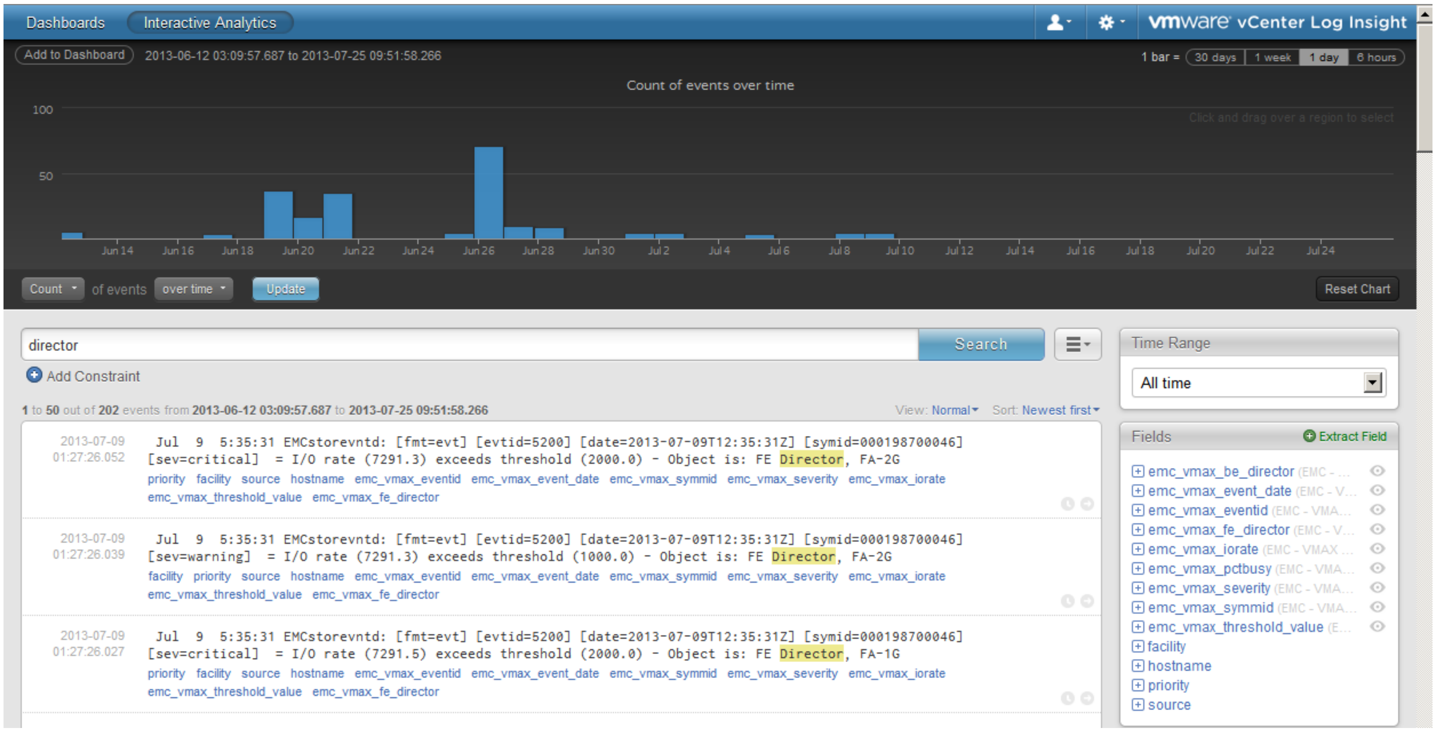
The first thing he does is to change the Time Range (highlighted in red above) to “All time” to be sure he traverses all the log files with his queries. Then he starts with a simple query against the term “director”. As he begins typing in the term, Log Insight automatically generates options from which to choose. In Figure 19 one can see the first term presented is “director” and that there will be 202 entries for that term. He selects that and hits “Search”.


Dashboards
Interactive Analytics
vmware vCenter Log Insight
Add to Dashboard
2013-06-12 03:09:57.687 to 2013-07-25 09:33:03.011
1 bar = 30 days 1 week 1 day 6 hours
Count of events over time
10k
5k
Click and drag over a region to select
Jun 14 Jun 16 Jun 18 Jun 20 Jun 22 Jun 24 Jun 26 Jun 28 Jun 30 Jul 2 Jul 4 Jul 6 Jul 8 Jul 10 Jul 12 Jul 14 Jul 16 Jul 18 Jul 20 Jul 22 Jul 24
Count of events over time
Update
Reset Chart
dir
Search
director 202
directory 1
View: Normal
Sort: Newest first
Time Range
All time
Fields
Extract Field
appname
hostname
source
vc_event_type
vc_username

```
2013-07-25    User Administrator@10.108.246.133 logged in as JAX-WS RI 2.2.4-b01
09:32:12.237  appname  vc_username  source  hostname  vc_event_type

2013-07-25    User Administrator@10.108.246.134 logged out (login time: Thursday, July 25, 2013 1:30:11 PM, number of API
09:30:12.289  invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
              appname  vc_username  source  hostname  vc_event_type

2013-07-25    User Administrator@10.108.246.134 logged in as JAX-WS RI 2.2.4-b01
09:30:11.446  appname  vc_username  source  hostname  vc_event_type
```

Figure 19. Director term search in vRealize Log Insight

The result of the query is displayed in Figure 20.

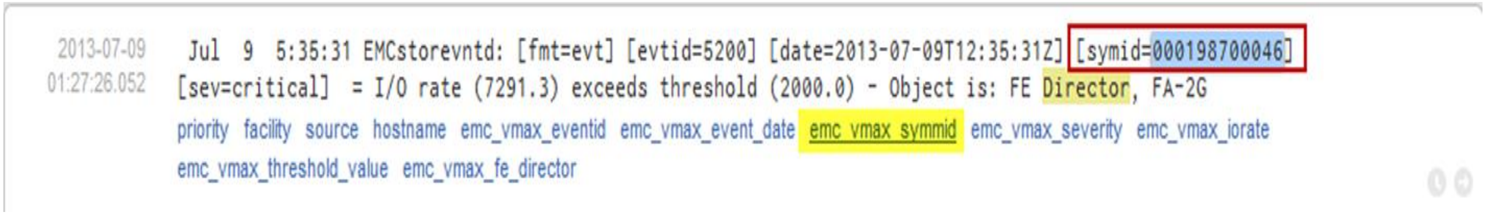

Dashboards
Interactive Analytics
vmware vCenter Log Insight
Add to Dashboard
2013-06-12 03:09:57.687 to 2013-07-25 09:51:58.266
1 bar = 30 days 1 week 1 day 6 hours
Count of events over time
100
50
Click and drag over a region to select
Jun 14 Jun 16 Jun 18 Jun 20 Jun 22 Jun 24 Jun 26 Jun 28 Jun 30 Jul 2 Jul 4 Jul 6 Jul 8 Jul 10 Jul 12 Jul 14 Jul 16 Jul 18 Jul 20 Jul 22 Jul 24
Count of events over time
Update
Reset Chart
director
Search
Add Constraint
View: Normal
Sort: Newest first
Time Range
All time
Fields
Extract Field
emc_vmax_be_director (EMC - ...
emc_vmax_event_date (EMC - V...
emc_vmax_eventid (EMC - VMA...
emc_vmax_fe_director (EMC - V...
emc_vmax_iorate (EMC - VMAX ...
emc_vmax_pctbusy (EMC - VMA...
emc_vmax_severity (EMC - VMA...
emc_vmax_symmid (EMC - VMA...
emc_vmax_threshold_value (E...
facility
hostname
priority
source

1 to 50 out of 202 events from 2013-06-12 03:09:57.687 to 2013-07-25 09:51:58.266

```
2013-07-09    Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.052  [sev=critical]  = I/O rate (7291.3) exceeds threshold (2000.0) - Object is: FE Director, FA-2G
              priority  facility  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
              emc_vmax_threshold_value  emc_vmax_fe_director

2013-07-09    Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.039  [sev=warning]  = I/O rate (7291.3) exceeds threshold (1000.0) - Object is: FE Director, FA-2G
              facility  priority  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
              emc_vmax_threshold_value  emc_vmax_fe_director

2013-07-09    Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.027  [sev=critical]  = I/O rate (7291.5) exceeds threshold (2000.0) - Object is: FE Director, FA-1G
              priority  facility  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
              emc_vmax_threshold_value  emc_vmax_fe_director
```

Figure 20. FE Director entries

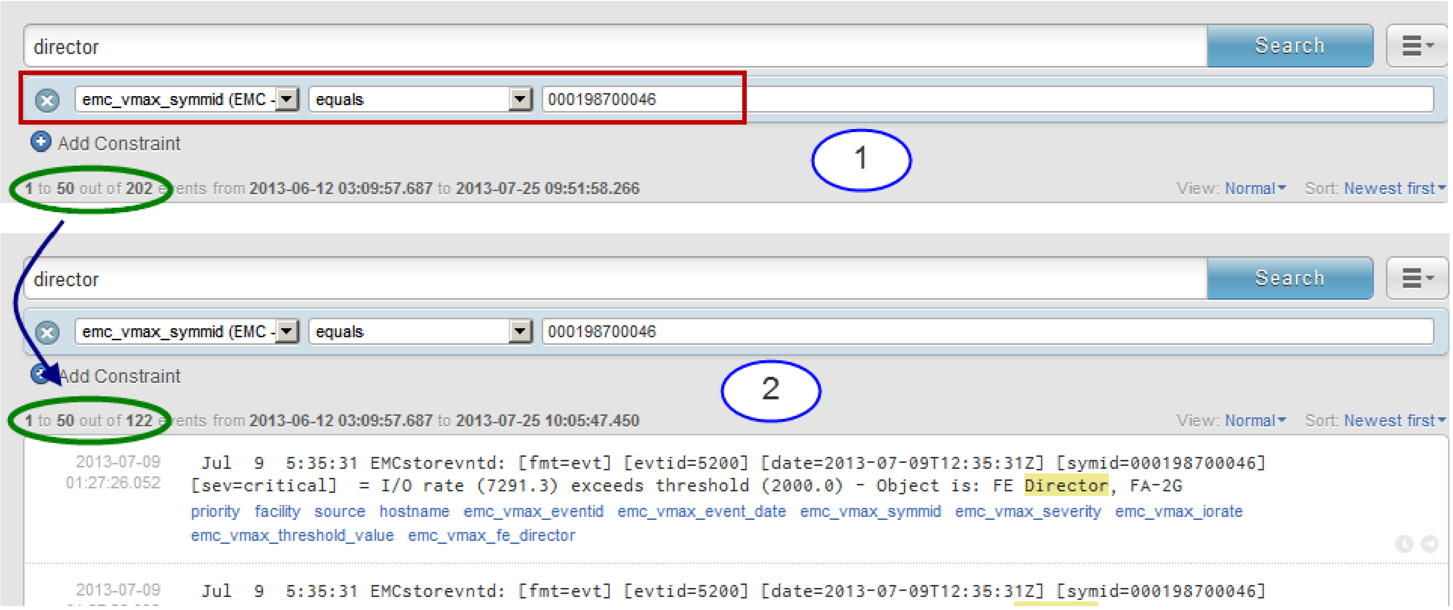
Now that he has the director entries, he needs to filter those events further to the VMAX array he uses. He examines one of the log entries to see what pre-defined fields might assist him. One field that would satisfy the requirement is "emc_vmax_symid". By putting the cursor over this field, the VMAX id is highlighted in the entry as in Figure 21.



```
2013-07-09     Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.052   [sev=critical]  = I/O rate (7291.3) exceeds threshold (2000.0) - Object is: FE Director, FA-2G
               priority  facility  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
               emc_vmax_threshold_value  emc_vmax_fe_director
```

Figure 21. emc_vmax_symid field

As the entry contains the VMAX id he needs, he clicks on the "emc_vmax_symid" field and it is automatically added as a constraint to his query, ensuring only director events related to his VMAX are shown. He hits Search again and now the entries are reduced from 202 to 122, seen in Figure 22.



director

emc_vmax_symmid (EMC - | equals | 000198700046

1 to 50 out of 202 events from 2013-06-12 03:09:57.687 to 2013-07-25 09:51:58.266   View: Normal   Sort: Newest first

director

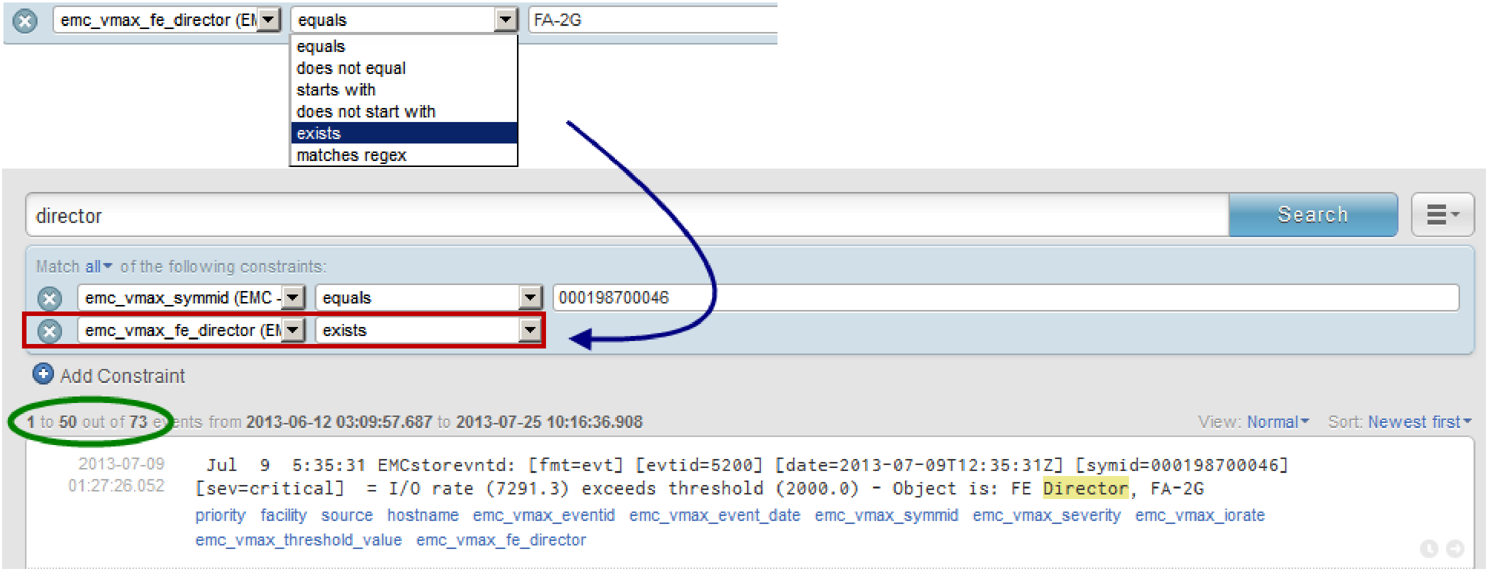
emc_vmax_symmid (EMC - | equals | 000198700046

1 to 50 out of 122 events from 2013-06-12 03:09:57.687 to 2013-07-25 10:05:47.450   View: Normal   Sort: Newest first

```
2013-07-09     Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.052   [sev=critical]  = I/O rate (7291.3) exceeds threshold (2000.0) - Object is: FE Director, FA-2G
               priority  facility  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
               emc_vmax_threshold_value  emc_vmax_fe_director

2013-07-09     Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
```

Figure 22. Adding a constraint to a query

The VMAdmin sees that two further constraints will be necessary to achieve his goal. First, he needs to see only FE director events, not back-end director events. This might be achieved in two ways. Based on the log entries he might add "FE" to his director query or he could use another defined field. He chooses the latter, and adds "emc_vmax_fe_director". For this constraint, however, if he clicks on the field associated with an entry, it will associate it with that specific FE. Once added, therefore, he changes the condition to “exists” so he will see all FEs. His count is now reduced to 73 seen in Figure 23.



emc_vmax_fe_director (EM | equals | FA-2G

director

Match all of the following constraints:

emc_vmax_symmid (EMC - | equals | 000198700046

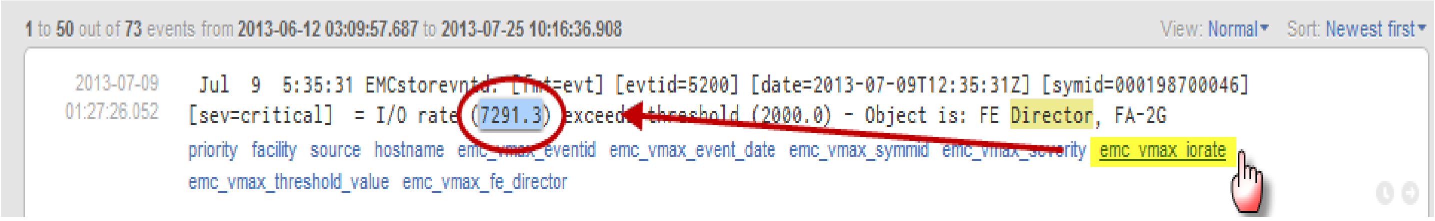
emc_vmax_fe_director (EM | exists

1 to 50 out of 73 events from 2013-06-12 03:09:57.687 to 2013-07-25 10:16:36.908

```
2013-07-09     Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.052   [sev=critical]  = I/O rate (7291.3) exceeds threshold (2000.0) - Object is: FE Director, FA-2G
               priority  facility  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
               emc_vmax_threshold_value  emc_vmax_fe_director
```

Figure 23. Adding emc_vmax_fe_director field constraint

With all FE director events accounted for, the final condition needs to be applied. By looking at the first entry he can see an example of what an I/O rate event will show. In that entry, in parentheses, is the exact value that exceeded the threshold. Again, he reviews the available defined fields and finds “emc_vmax_iorate” in Figure 24. Running the cursor over that reveals it is associated with the value in parentheses.

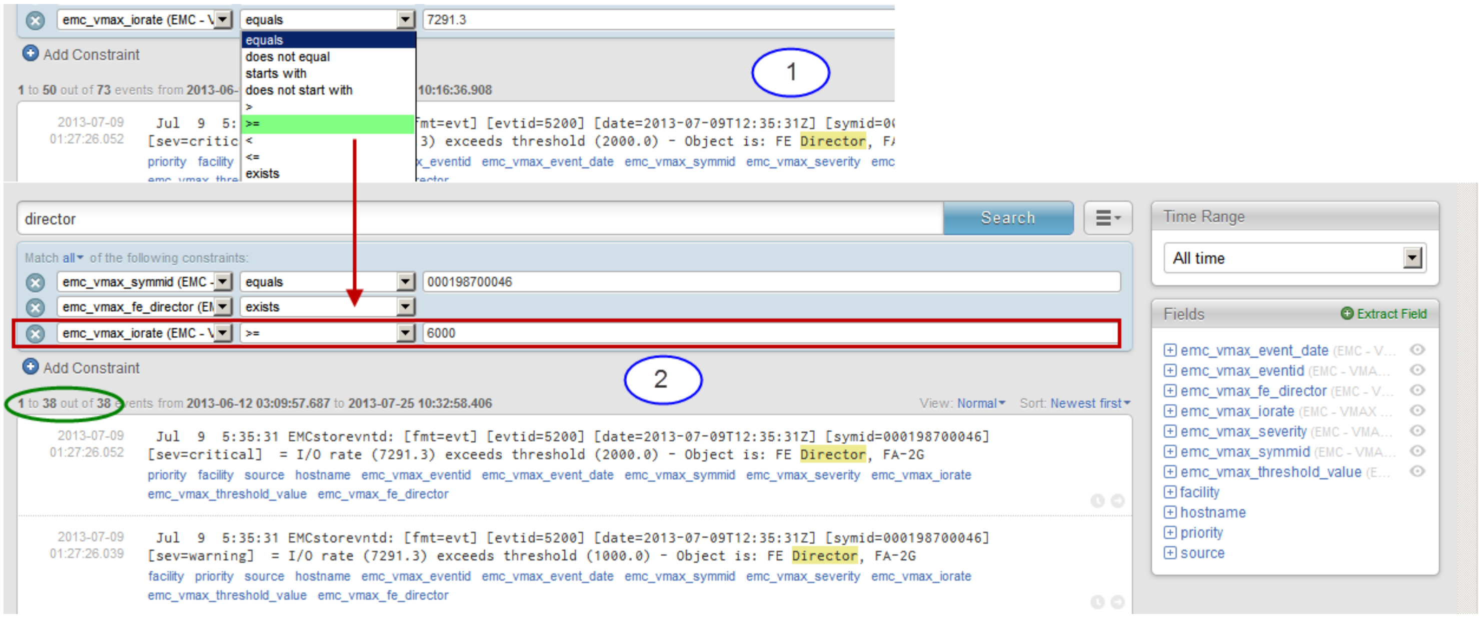


1 to 50 out of 73 events from 2013-06-12 03:09:57.687 to 2013-07-25 10:16:36.908

```
2013-07-09     Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.052   [sev=critical]  = I/O rate (7291.3) exceeds threshold (2000.0) - Object is: FE Director, FA-2G
               priority  facility  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
               emc_vmax_threshold_value  emc_vmax_fe_director
```

Figure 24. emc_vmax_iorate field

He reviews the other operands that can be used since the field is an integer and finds greater than or equal to. Now he can apply that to the field and use the “6000” number that the Sysadmin required. This is displayed in Figure 25.



emc_vmax_iorate (EMC - V equals 7291.3

1 to 50 out of 73 events from 2013-06- … 10:16:36.908

director

Match all of the following constraints:

- emc_vmax_symmid (EMC - equals 000198700046
- emc_vmax_fe_director (EM exists
- emc_vmax_iorate (EMC - V >= 6000

1 to 38 out of 38 events from 2013-06-12 03:09:57.687 to 2013-07-25 10:32:58.406

Time Range: All time

Fields: emc_vmax_event_date (EMC - V…, emc_vmax_eventid (EMC - VMA…, emc_vmax_fe_director (EMC - V…, emc_vmax_iorate (EMC - VMAX …, emc_vmax_severity (EMC - VMA…, emc_vmax_symmid (EMC - VMA…, emc_vmax_threshold_value (E…, facility, hostname, priority, source

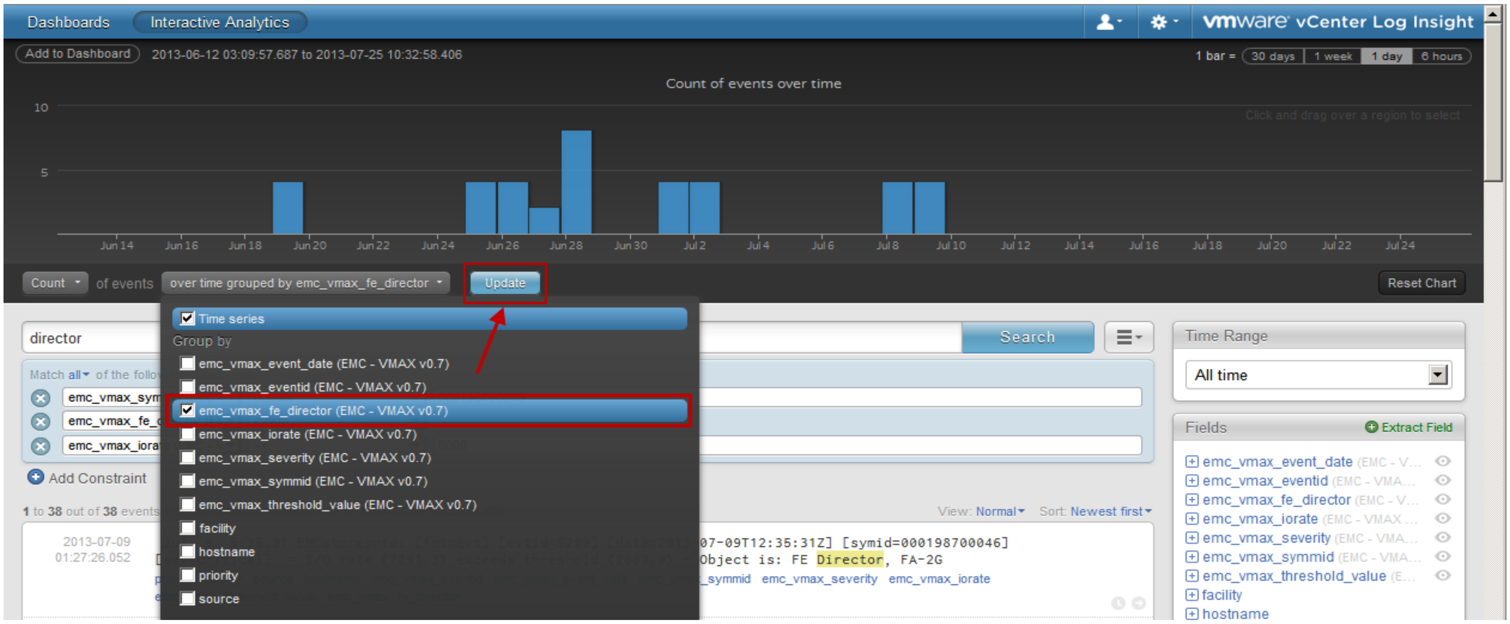
```
2013-07-09     Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.052   [sev=critical]  = I/O rate (7291.3) exceeds threshold (2000.0) - Object is: FE Director, FA-2G
               priority  facility  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
               emc_vmax_threshold_value  emc_vmax_fe_director

2013-07-09     Jul  9  5:35:31 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2013-07-09T12:35:31Z] [symid=000198700046]
01:27:26.039   [sev=warning]  = I/O rate (7291.3) exceeds threshold (1000.0) - Object is: FE Director, FA-2G
               facility  priority  source  hostname  emc_vmax_eventid  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_severity  emc_vmax_iorate
               emc_vmax_threshold_value  emc_vmax_fe_director
```

Figure 25. Applying the 6000 I/O limit

Within a short time, the VMAdmin has found the 38 entries that meet the requirements.

Creating the dashboard

Although all the entries are listed, it would be far easier if it was put in a graphical display. The graph at the top of the Interactive Analytics page can now be updated using all the conditions supplied by the VMAdmin. Furthermore, by utilizing the group by function, he can sort by the FE director as in Figure 26.



2013-06-12 03:09:57.687 to 2013-07-25 10:32:58.406

Count of events over time grouped by emc_vmax_fe_director

☑ Time series

Group by

- ☐ emc_vmax_event_date (EMC - VMAX v0.7)
- ☐ emc_vmax_eventid (EMC - VMAX v0.7)
- ☑ emc_vmax_fe_director (EMC - VMAX v0.7)
- ☐ emc_vmax_iorate (EMC - VMAX v0.7)
- ☐ emc_vmax_severity (EMC - VMAX v0.7)
- ☐ emc_vmax_symmid (EMC - VMAX v0.7)
- ☐ emc_vmax_threshold_value (EMC - VMAX v0.7)
- ☐ facility
- ☐ hostname
- ☐ priority
- ☐ source

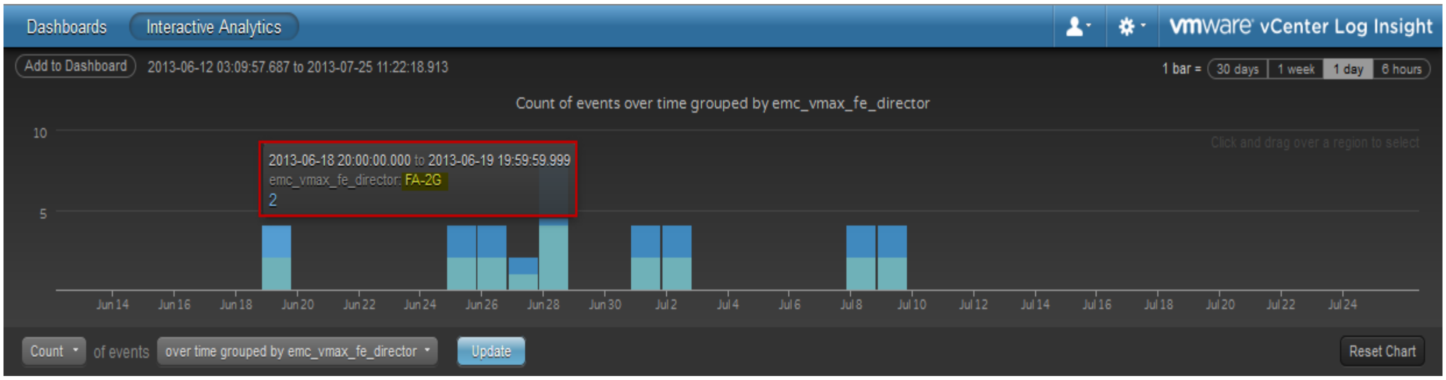
director

1 to 38 out of 38 events

Time Range: All time

Figure 26. Grouping by FE director

After selecting “Update” the new graph appears, and by hovering the cursor over a bar, the FE director is seen in Figure 27.

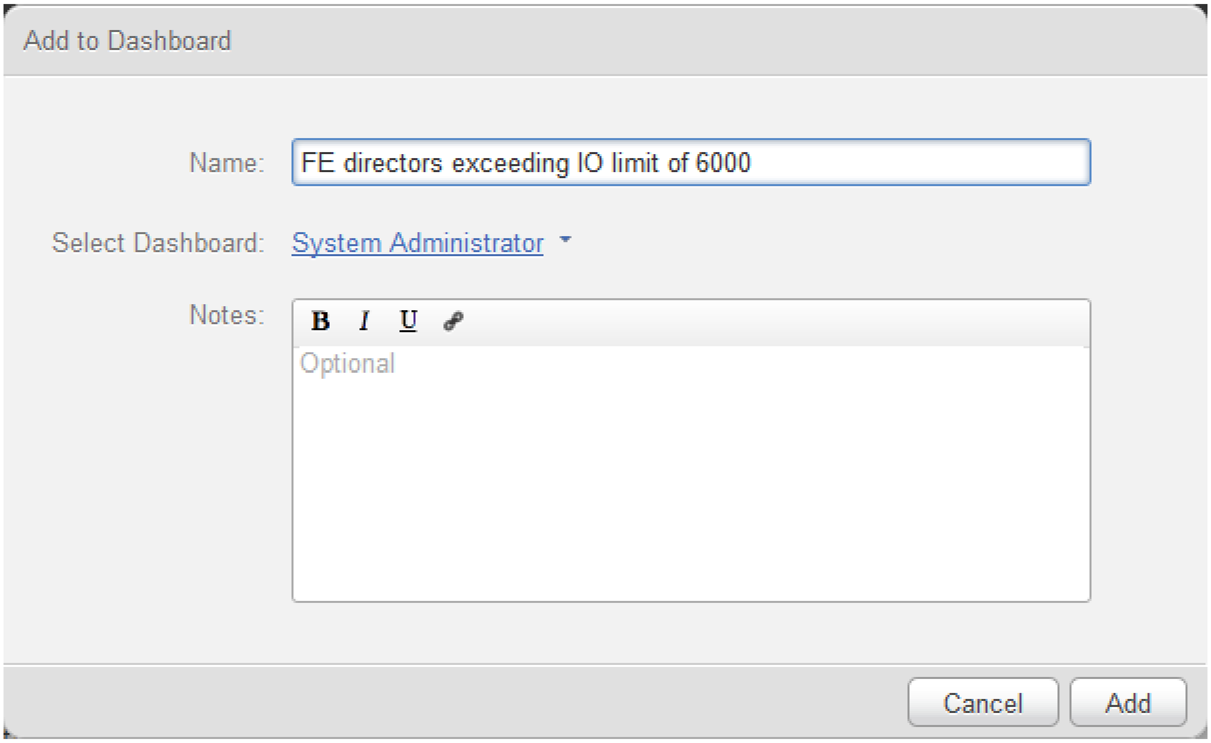


2013-06-12 03:09:57.687 to 2013-07-25 11:22:18.913

2013-06-18 20:00:00.000 to 2013-06-19 19:59:59.999
emc_vmax_fe_director: FA-2G
2

Figure 27. Final FE director graph

Finally, the VMAdmin decides to add this graph to the System Administrator’s dashboard so that the information can be correlated with other information from the VMAX. He selects “Add to Dashboard” and puts it in the dashboard in Figure 28.



Name: FE directors exceeding IO limit of 6000

Select Dashboard: System Administrator

Notes:

Figure 28. Add FE I/O graph to dashboard

The final dashboard is shown in Figure 29.

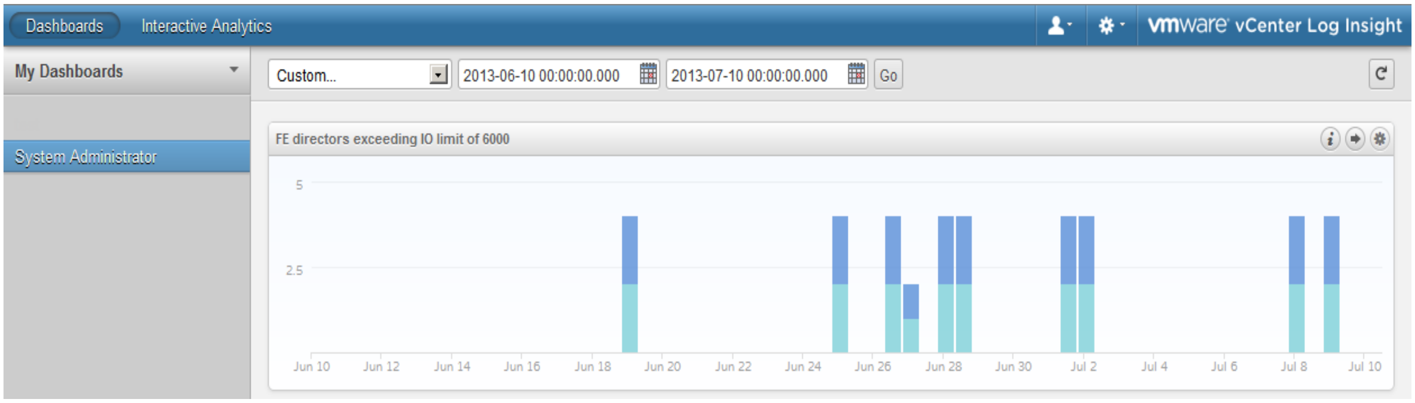


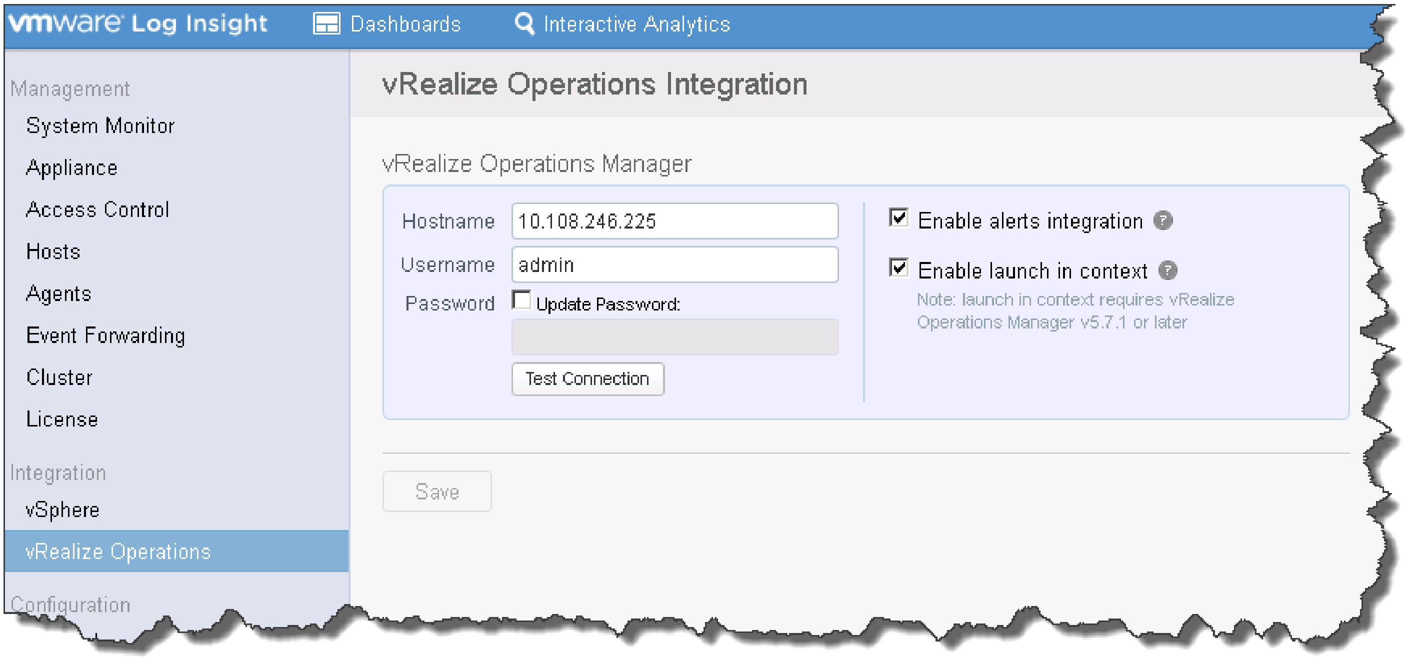
Figure 29. System Administrator dashboard

The problem resolution is now complete and the Sysadmin can use this piece of information to make an informed decision and implement the necessary changes.

Using the VMAX Content Pack with EMC Storage Analytics

VMware provides the ability to integrate vRealize Log Insight with vRealize Operations (vROps) beyond a specialized content pack. There are two integration points which are possible. The first is to enable a launch in context capability of Log Insight from within vROps. The second is to enable alerts integration which means that it is possible to send alerts from Log Insight into vROps and associate them with a resource from EMC Storage Analytics (ESA). This second capability allows Log Insight customers who also have ESA for VMAX to receive alerts from within ESA. Fortunately the VMAX content pack makes this very simple to setup since there are many alerts preconfigured that can be used in this capacity. The following will provide an example of how to setup this integration using one of the alerts from the VMAX content pack.

To enable the capability, navigate to the Administration page in Log Insight and then the vRealize Operations Manager Integration, demonstrated in Figure 30.



vRealize Operations Integration

vRealize Operations Manager

Hostname 10.108.246.225

Username admin

Password □ Update Password:

☑ Enable alerts integration

☑ Enable launch in context

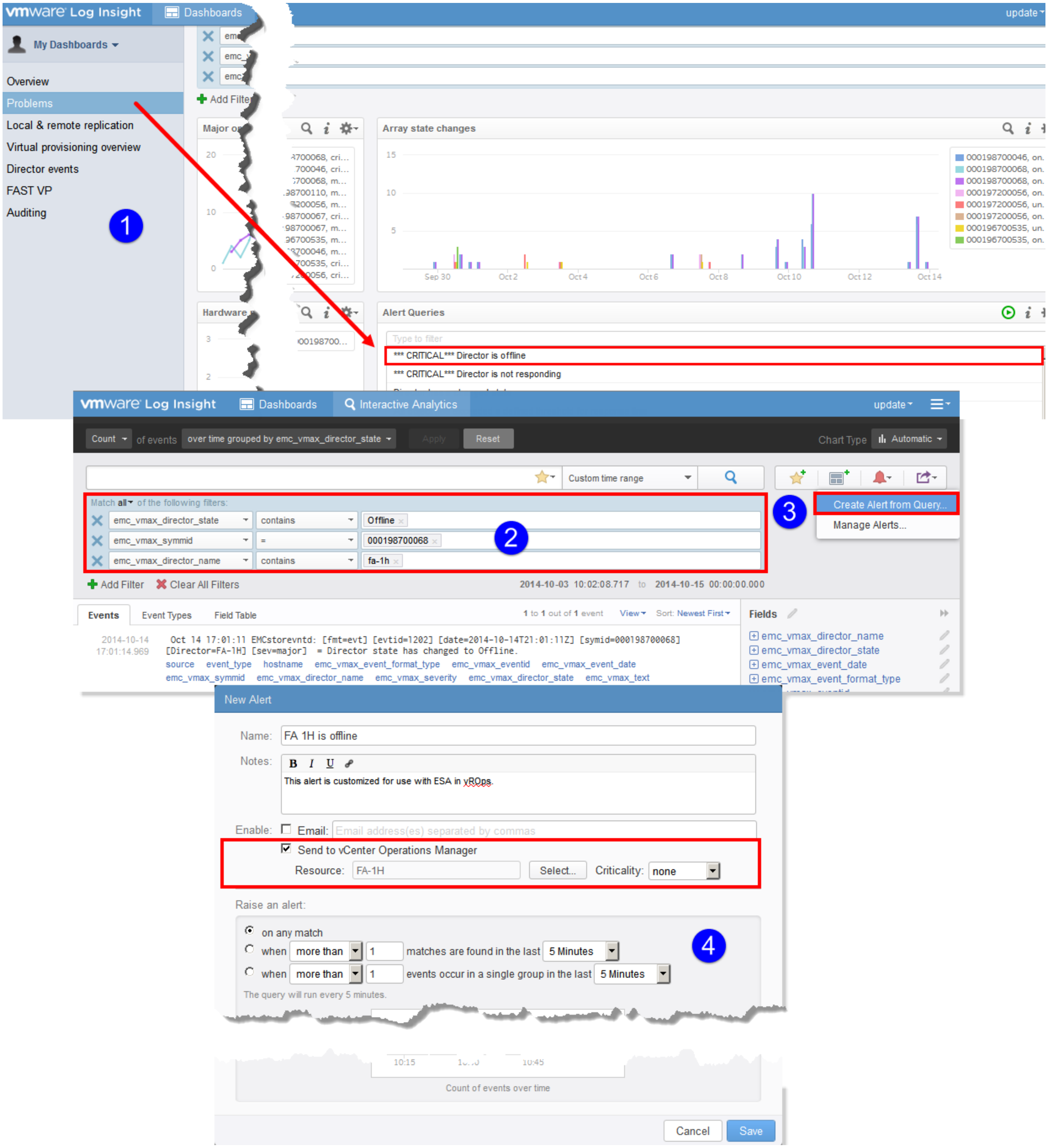
Note: launch in context requires vRealize Operations Manager v5.7.1 or later

Figure 30. vRealize Operations integration

Once enabled, alerts can be tied to vROps ESA resources. What follows is an example of how that is done.

Customized director alert

Within the VMAX CP, navigate to the Problems dashboard and click the ***** CRITICAL *** Director is offline** alert. This will bring up the Interactive Analytics page. From here, using the user-defined fields, customize the alert with a specific VMAX ID (if more than one is monitored) and a specific FA. Once complete, create an alert from the query and tie it to the correct FA resource in ESA. In Figure 31 these 4 steps are shown.



Alert Queries:

- *** CRITICAL*** Director is offline
- *** CRITICAL*** Director is not responding

Match all of the following filters:

emc_vmax_director_state	contains	Offline
emc_vmax_symmid	=	000198700068
emc_vmax_director_name	contains	fa-1h

2014-10-03 10:02:08.717 to 2014-10-15 00:00:00.000

1 to 1 out of 1 event

```
2014-10-14    Oct 14 17:01:11 EMCstorevntd: [fmt=evt] [evtid=1202] [date=2014-10-14T21:01:11Z] [symid=000198700068]
17:01:14.969  [Director=FA-1H] [sev=major]  = Director state has changed to Offline.
              source  event_type  hostname  emc_vmax_event_format_type  emc_vmax_eventid  emc_vmax_event_date
              emc_vmax_symmid  emc_vmax_director_name  emc_vmax_severity  emc_vmax_director_state  emc_vmax_text
```

New Alert

Name: FA 1H is offline

Notes: This alert is customized for use with ESA in vROps.

Enable: □ Email: Email address(es) separated by commas

☑ Send to vCenter Operations Manager

Resource: FA-1H Select... Criticality: none

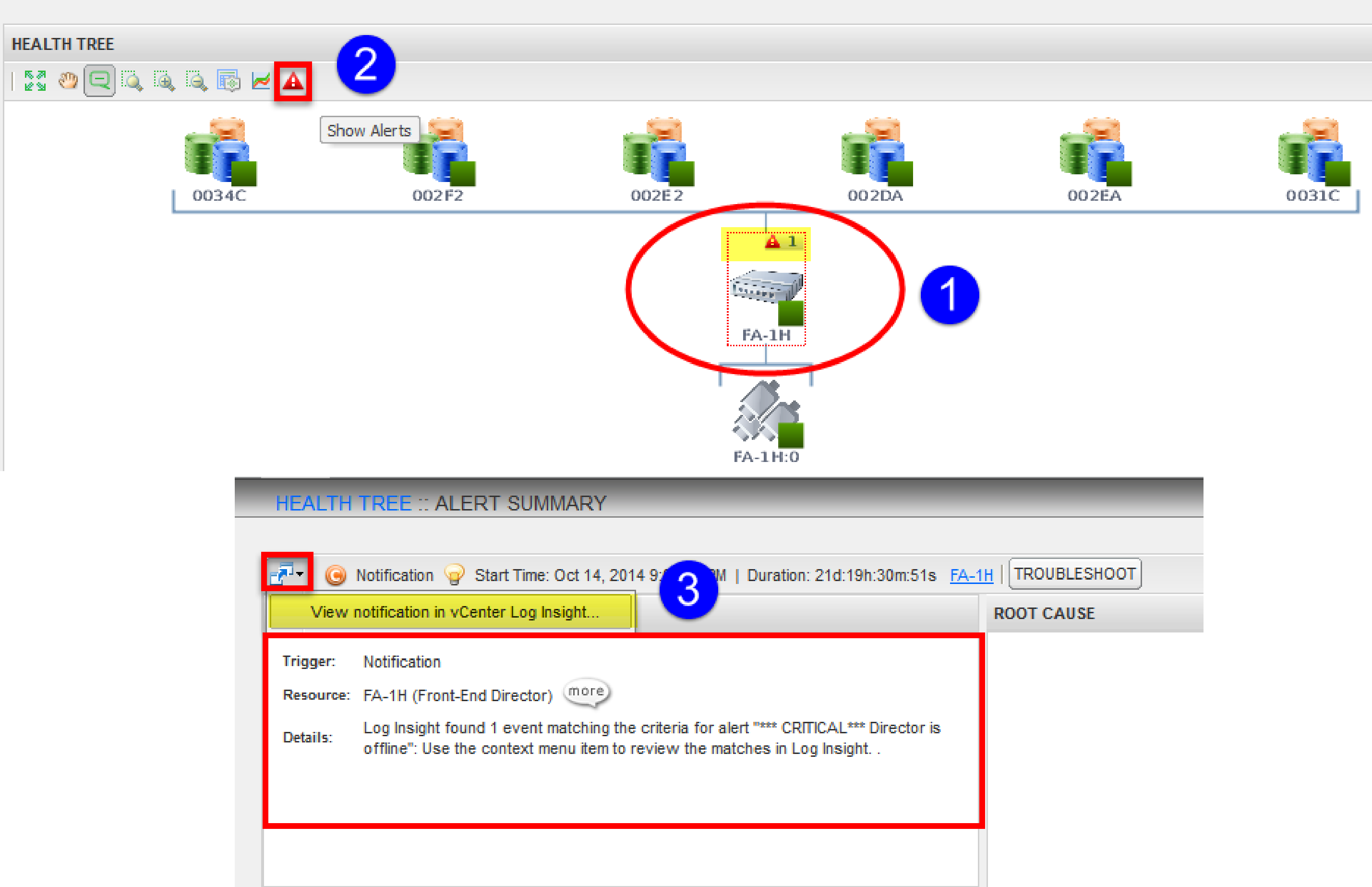
Raise an alert:

- ● on any match
- ○ when more than 1 matches are found in the last 5 Minutes
- ○ when more than 1 events occur in a single group in the last 5 Minutes

The query will run every 5 minutes.

Figure 31. Selecting, customizing, and creating alert for use in Log Insight/ESA

Once the alert is in place, it is run every 5 minutes. If there is a match, Log Insight automatically sends this alert to the defined ESA resource in vROps. There are a number of places to see this alert. In particular any topology view of the resource will include a red triangle indicating an alert. From there the alert icon can be selected and the detail page will appear. After reviewing the notification, the user can select a drop-down box which will launch Log Insight in-context so the log entry itself can be viewed in that application. These steps are seen in Figure 32.


HEALTH TREE
2
Show Alerts
0034C
002F2
002E2
002DA
002EA
0031C
1
1
FA-1H
FA-1H:0
HEALTH TREE :: ALERT SUMMARY
3
Notification
Start Time: Oct 14, 2014 9:
M
Duration: 21d:19h:30m:51s
FA-1H
TROUBLESHOOT
View notification in vCenter Log Insight...
ROOT CAUSE
more

Trigger: Notification

Resource: FA-1H (Front-End Director)

Details: Log Insight found 1 event matching the criteria for alert "*** CRITICAL*** Director is offline": Use the context menu item to review the matches in Log Insight. .

Figure 32. Log Insight alert generated in ESA

Using the aforementioned process, ESA for VMAX can receive any alerts generated on the array when the user configures the Log Insight integration using the EMC VMAX content pack.

Conclusion

By utilizing the VMAX Content Pack within VMware vRealize Log Insight, Symmetrix customers can have access to dashboards and user-defined fields that categorize the log information coming from the array, presenting it in a graphical format that helps in troubleshooting issues.

References

EMC

- *Unisphere for VMAX 1.6 Installation Guide*
  https://support.emc.com/docu47001_Unisphere_for_VMAX_1.6_Installation_Guide.pdf

- *Unisphere for VMAX 1.6 Product Guide*

  https://support.emc.com/docu46997_Unisphere_for_VMAX_1.6_Product_Guide.pdf

- *Unisphere for VMAX Documentation Set*

  https://support.emc.com/docu55521_Unisphere_for_VMAX_8.0_Documentation_Set.pdf

- *Solutions Enabler 7.6 Installation Guide*

  https://support.emc.com/docu46992_Solutions_Enabler_7.6__Installation_Guide.pdf

- *Solutions Enabler 8.0 Documentation Set*

  https://support.emc.com/docu55498_Solutions_Enabler_8.0_Documentation_Set.pdf

- *ESA for VMAX*

  https://support.emc.com/products/32027_Storage-Analytics-SW-for-VMAX

VMware

- *VMware vRealize Log Insight Release Notes*

  http://www.vmware.com/support/log-insight/doc/log-insight-20-release-notes.html

  vRealize Log Insight Installation and Administration Guides

  http://www.vmware.com/pdf/log-insight-20-install-admin-guide.pdf

Appendix: EMC VMAX Content Pack and VMAX Auditing Data

This appendix will discuss how the EMC VMAX Content Pack can present VMAX auditing information.

Auditing

In addition to the event daemon and Unisphere options previously discussed, there is another area where log entries are generated: auditing. Every action made on the VMAX is recorded on the array in a special internal location. The secure audit log contains a record of configuration changes, security alarms, service operations, and security-relevant actions maintained on each Symmetrix array. Records are written to this by Solutions Enabler, software running on the Service Processor, and the Enginuity™ /HYPERMAX Operating Environment. There are two ways to present auditing information to Log Insight: the event daemon and the *symaudit* command.

There are many types of activities performed on the VMAX which are only recorded in the auditing logs. For instance, if a user wants to see whether there has been any disk sparing on the array, the audit log is the only place which contains this information.

Audit entries and the event daemon

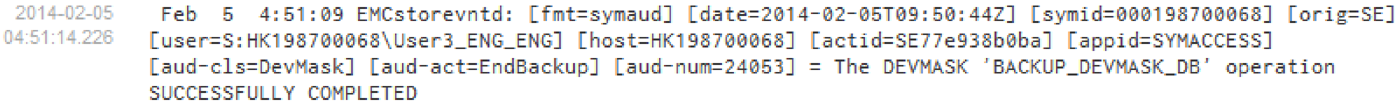
The first, and easiest method to obtain audit records is to use the event daemon. Although not well documented, there is another category that can be added to the daemon_options file as outlined in the Configuring Solutions Enabler section in this document. The category is “audit” and the entry needs to include the Symmetrix array even if the array is not being specified for the other categories:

```
sid=0001987000xx,audit;
```

So an entry in the daemon_options file might look like this if auditing is desired:

```
storevntd:LOG_SYMMETRIX_EVENTS = status, groups, optimizer, events,
array subsystem, checksum, diagnostic, environmental, device pool,
service processor, srdf system, srdf link, srdfa session, srdf
consistency group, director, device, disk, smc, spa,
sid=0001987000xx,audit;\
```

An audit entry when forwarded by the event daemon takes the following form in Figure 33:



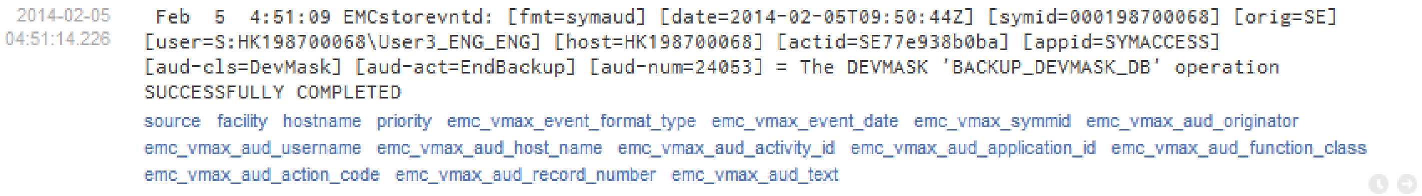
```
2014-02-05     Feb  5  4:51:09 EMCstorevntd: [fmt=symaud] [date=2014-02-05T09:50:44Z] [symid=000198700068] [orig=SE]
04:51:14.226  [user=S:HK198700068\User3_ENG_ENG] [host=HK198700068] [actid=SE77e938b0ba] [appid=SYMACCESS]
              [aud-cls=DevMask] [aud-act=EndBackup] [aud-num=24053] = The DEVMASK 'BACKUP_DEVMASK_DB' operation
              SUCCESSFULLY COMPLETED
```

Figure 33. Audit entry as forwarded by the event daemon

Each of the fields in the audit entry have been extracted into user-defined fields. As there are two different types of audit records that are addressed in this document, these fields are identified by the prefix “emc_vmax_aud_” – the “aud” representing the shortened form of the audit record. The fields are:

- emc_vmax_aud_action_code
- emc_vmax_aud_activity_id
- emc_vmax_aud_application_id
- emc_vmax_aud_function_class
- emc_vmax_aud_host_name
- emc_vmax_aud_originator
- emc_vmax_aud_record_number
- emc_vmax_aud_text
- emc_vmax_aud_username

An entry in Log Insight with the fields identified appears in Figure 34.



```
2014-02-05     Feb  5  4:51:09 EMCstorevntd: [fmt=symaud] [date=2014-02-05T09:50:44Z] [symid=000198700068] [orig=SE]
04:51:14.226  [user=S:HK198700068\User3_ENG_ENG] [host=HK198700068] [actid=SE77e938b0ba] [appid=SYMACCESS]
              [aud-cls=DevMask] [aud-act=EndBackup] [aud-num=24053] = The DEVMASK 'BACKUP_DEVMASK_DB' operation
              SUCCESSFULLY COMPLETED
              source  facility  hostname  priority  emc_vmax_event_format_type  emc_vmax_event_date  emc_vmax_symmid  emc_vmax_aud_originator
              emc_vmax_aud_username  emc_vmax_aud_host_name  emc_vmax_aud_activity_id  emc_vmax_aud_application_id  emc_vmax_aud_function_class
              emc_vmax_aud_action_code  emc_vmax_aud_record_number  emc_vmax_aud_text
```

Figure 34. Audit entry as forwarded by the event daemon with user-defined fields

Note that some VMAX events will generate both a regular log entry as well as an audit log entry in Log Insight. Because of the manner in which the VMAX generates audit entries, however, the date field may not exactly match the associated date field of the non-audit log entry (if any).

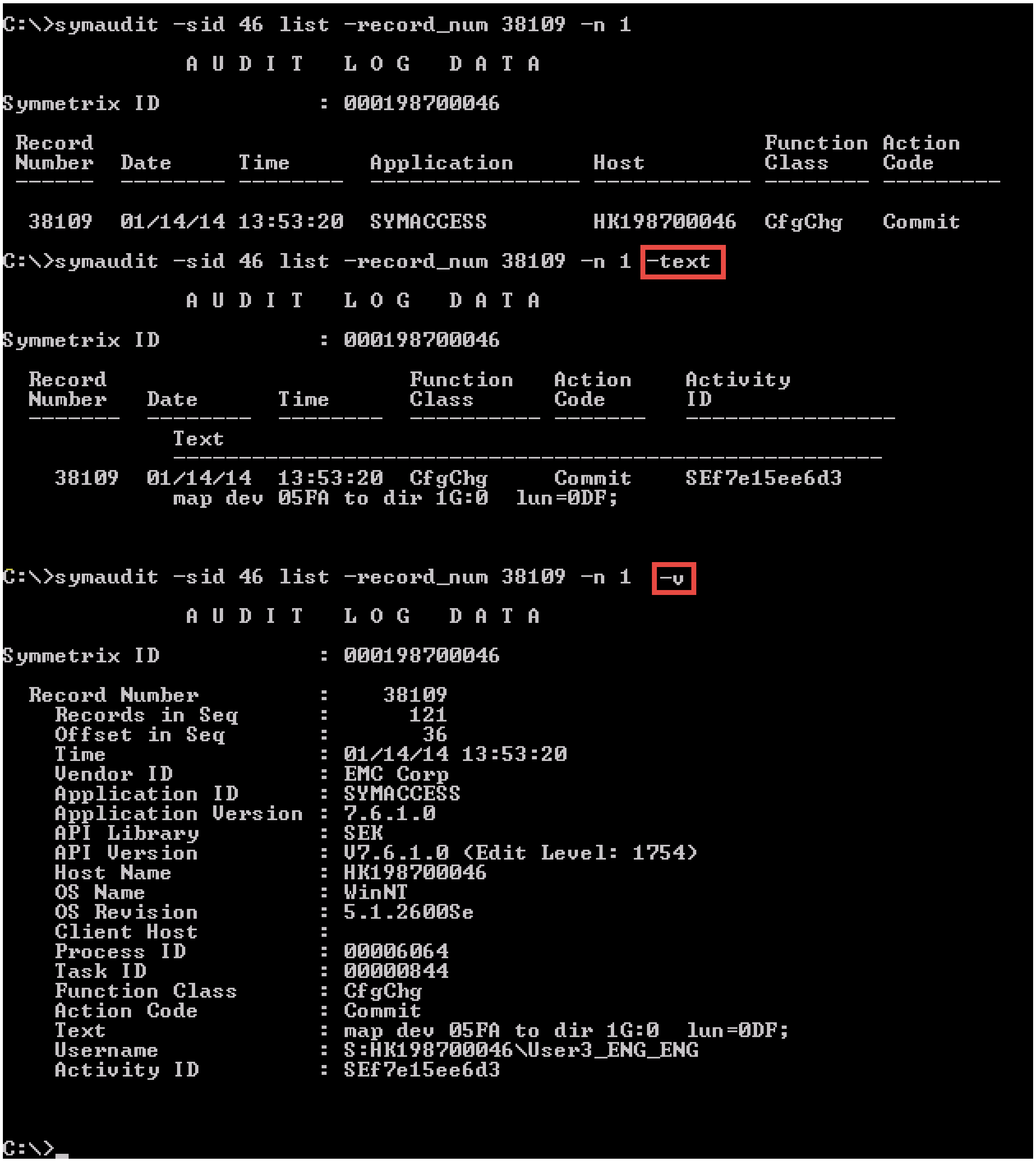
Audit entries and symaudit

The second method to obtain auditing records is to use the SYMCLI command symaudit. Unlike the event daemon, however, there is no configuration file that can be changed to capture the more detailed auditing entries and send them to Log Insight.

Symaudit has two modes which could be used in this context: list and monitor[4]. The list functionality allows querying against the information stored on the array. There are a variety of ways to qualify that listing, from function class, to user, to timestamp. They can be found in the Solutions Enabler command reference guide. The other use of symaudit is to monitor the entries in real-time. The monitor switch also takes the same qualifiers as list to access specific records, but for the purposes of pushing the

[4] A third mode is “show” which will provide a synopsis of the start and end date of the log history and the record numbers.

information to Log Insight, the more information the better for analysis. Figure 35 show how a single record entry appears using symaudit with different amounts of detail. The first command asks for a particular record. The second command asks for that record with text; and the final command expands the information by using verbose (-text is implied). Note that some of the switches here are the same whether monitor or list is used, but list allows the same entry to be queried multiple times using the record number while monitor cannot be used in that manner as it is real-time:



```
C:\>symaudit -sid 46 list -record_num 38109 -n 1

              A U D I T   L O G   D A T A

Symmetrix ID            : 000198700046

 Record                                                  Function Action
 Number  Date     Time      Application      Host         Class    Code
 ------  -------- --------  ---------------- ------------ -------- ---------

  38109  01/14/14 13:53:20  SYMACCESS        HK198700046  CfgChg   Commit

C:\>symaudit -sid 46 list -record_num 38109 -n 1 -text

              A U D I T   L O G   D A T A

Symmetrix ID            : 000198700046

  Record   Date      Time      Function   Action    Activity
  Number   --------  --------  ---------- -------   ----------------
  -------    Text
             ------------------------------------------------------

    38109  01/14/14  13:53:20  CfgChg     Commit    SEf7e15ee6d3
             map dev 05FA to dir 1G:0  lun=0DF;


C:\>symaudit -sid 46 list -record_num 38109 -n 1 -v

              A U D I T   L O G   D A T A

Symmetrix ID            : 000198700046

  Record Number         :    38109
    Records in Seq      :      121
    Offset in Seq       :       36
    Time                : 01/14/14 13:53:20
    Vendor ID           : EMC Corp
    Application ID      : SYMACCESS
    Application Version : 7.6.1.0
    API Library         : SEK
    API Version         : V7.6.1.0 (Edit Level: 1754)
    Host Name           : HK198700046
    OS Name             : WinNT
    OS Revision         : 5.1.2600Se
    Client Host         :
    Process ID          : 00006064
    Task ID             : 00000844
    Function Class      : CfgChg
    Action Code         : Commit
    Text                : map dev 05FA to dir 1G:0  lun=0DF;
    Username            : S:HK198700046\User3_ENG_ENG
    Activity ID         : SEf7e15ee6d3


C:\>_
```

Figure 35. The three levels of symaudit detail

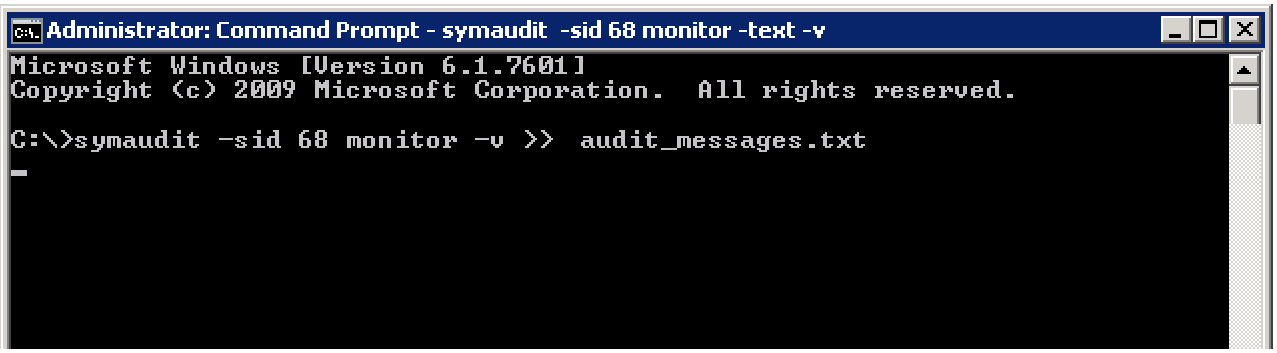
As one can see, the first entry has very basic information. The second adds some text which is more useful but the third includes detail on each field available in the record. Although any of these formats could be sent to Log Insight, the VMAX content pack auditing additions were made based upon the verbose output since that is the most detailed. Note the difference in detail between the verbose log entry and the entry sent by the event daemon in Figure 33. Although the event daemon entry contains some of the information, it is not inclusive, nor are the fields self-explanatory.

Sending auditing events to Log Insight

As mentioned, the problem with using symaudit is that there is no inherent ability to send the log information to a syslog source. Therefore a third-party software is necessary. For the most basic functionality, the software needs to be able to send logs to a syslog target. For this example, a product called "NXLOG" was used. It is available as a freeware and touts itself as "…a universal log collector and forwarder supporting different platforms, log sources, and protocols."[5] There are countless other software packages that could be used in this configuration so there is no requirement that NXLOG be that package.

As the Solutions Enabler environment was installed on Windows in this environment that is also where the Windows version of NXLOG was installed. The installation of NXLOG is straightforward. It runs as a service on Windows and requires a fairly simply modification of a configuration file.

In order to have NXLOG act upon something, a log will be necessary. Since issuing the *symaudit monitor* command is only going to stream the events to the screen as they occur, it needs to be re-directed to a file. NXLOG is intelligent enough to remember position in that file and only grab the newest entries so even if the box reboots, for example, you can restart the symaudit command and use the append ("››") redirector. The command to ensure the highest level of detail as shown in Figure 35, is:



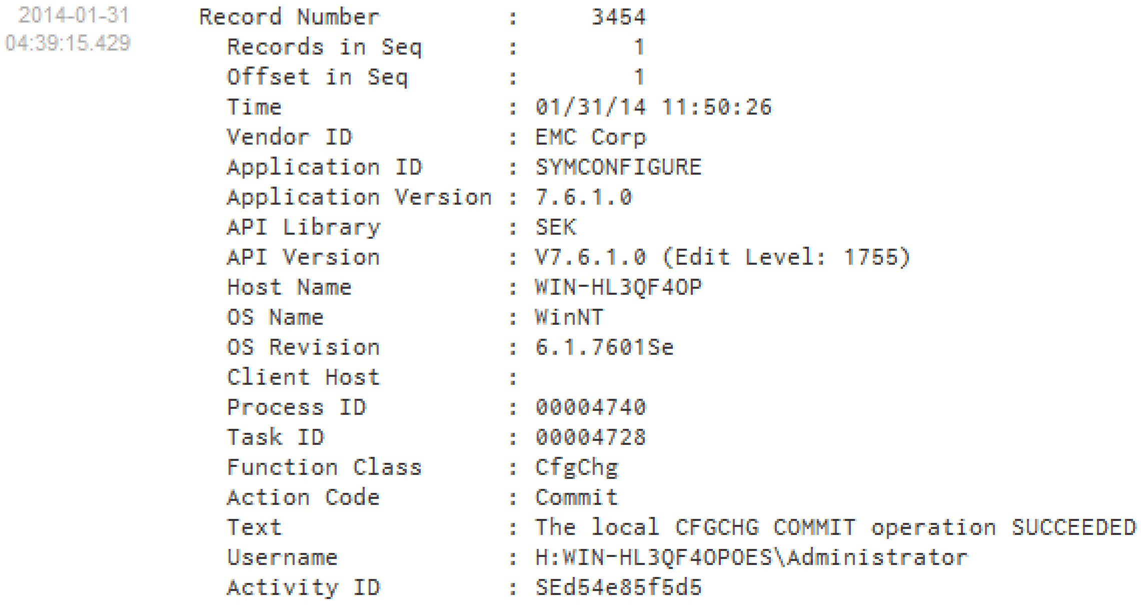
Administrator: Command Prompt - symaudit -sid 68 monitor -text -v

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>symaudit -sid 68 monitor -v >>  audit_messages.txt
_
```

Figure 36. Symaudit monitor command with verbose output

Figure 37 is a typical record that will be sent to Log Insight:

[5] http://www.nxlog.org

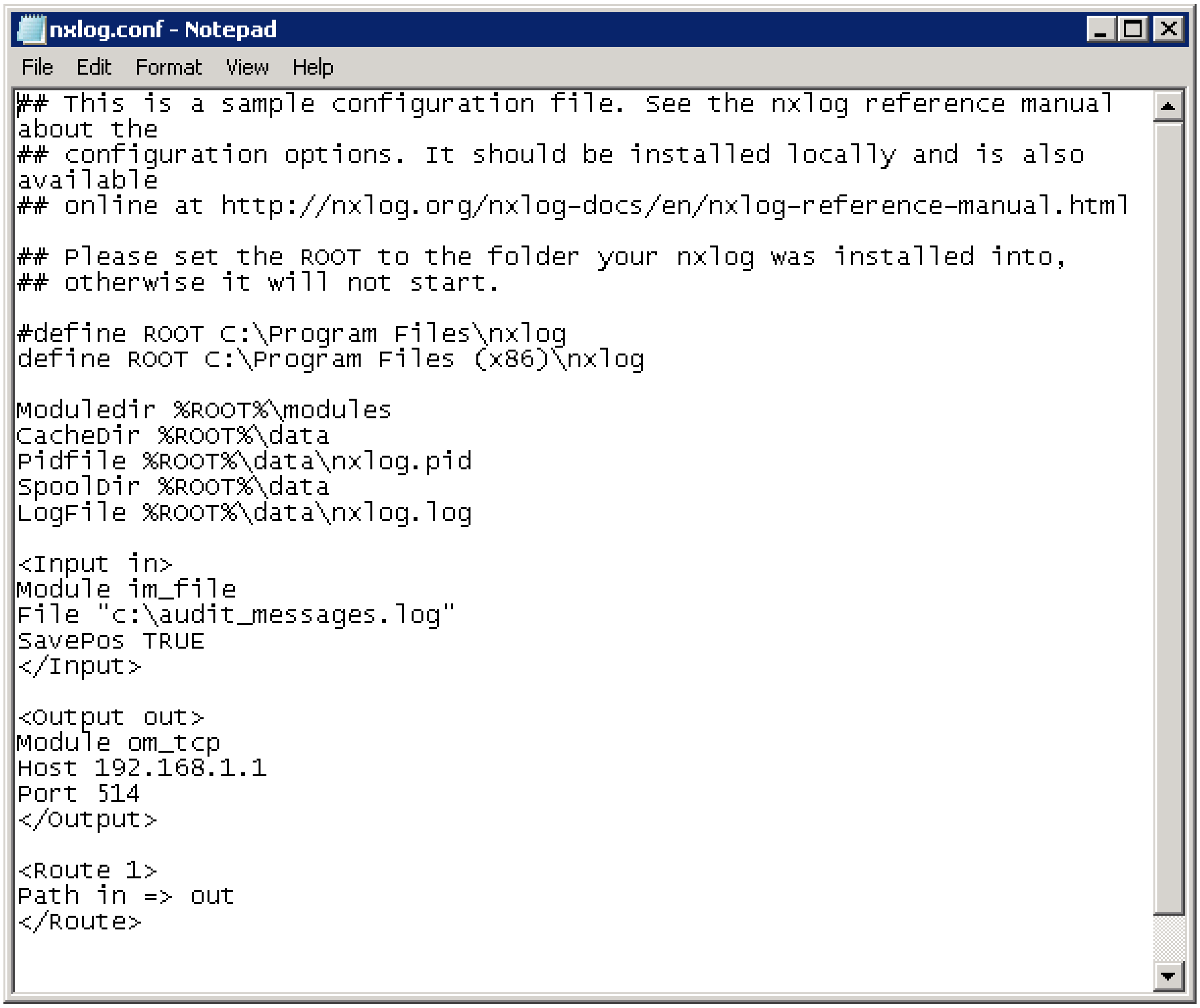


```
  2014-01-31      Record Number          :     3454
04:39:15.429        Records in Seq       :        1
                    Offset in Seq        :        1
                    Time                 : 01/31/14 11:50:26
                    Vendor ID            : EMC Corp
                    Application ID       : SYMCONFIGURE
                    Application Version  : 7.6.1.0
                    API Library          : SEK
                    API Version          : V7.6.1.0 (Edit Level: 1755)
                    Host Name            : WIN-HL3QF4OP
                    OS Name              : WinNT
                    OS Revision          : 6.1.7601Se
                    Client Host          :
                    Process ID           : 00004740
                    Task ID              : 00004728
                    Function Class       : CfgChg
                    Action Code          : Commit
                    Text                 : The local CFGCHG COMMIT operation SUCCEEDED
                    Username             : H:WIN-HL3QF4OPOES\Administrator
                    Activity ID          : SEd54e85f5d5
```

Figure 37. Audit entry from symaudit

NXLOG configuration

An NXLOG configuration file requires modification to send the audit entries to Log Insight. Here is a sample of the one in this environment:



```
## This is a sample configuration file. See the nxlog reference manual
about the
## configuration options. It should be installed locally and is also
available
## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html

## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Input in>
Module im_file
File "c:\audit_messages.log"
SavePos TRUE
</Input>

<Output out>
Module om_tcp
Host 192.168.1.1
Port 514
</Output>

<Route 1>
Path in => out
</Route>
```

Figure 38. NXLOG configuration file

Basically the content tells NXLOG to look for a file called "audit_messages.log" in the C drive and then send entries in that file to the syslog server at the IP and port in the output section. Note the "SavePos" entry which when set to TRUE ensures that NXLOG will not send duplicate entries if the symaudit command is interrupted. If there are multiple VMAX arrays in the environment, and they are all presented to this environment, it is possible to run multiple symaudit monitor sessions, one for each array. In that case, the NXLOG configuration file would be changed to include a wildcard (*) in the File entry. For instance, each symaudit could write to its own file called *"audit_messages_<sid>.log"*. Therefore the File entry would be changed to: *File "c:\audit_messages_*.log"* which would allow NXLOG to pick up the audit entries from each array.

Note if there are multiple VMAX arrays in the environment and audit records are being sent to the same Log Insight environment, there is no field in an audit record that lists the VMAX array ID. When records are generated on the array itself, the Host Name will include the array ID (as in Figure 35), but if the task that generated the audit record is run on another box, the Host Name would reflect that box, such as WIN-HL3QF4OP in Figure 37. In such cases, using the Record Number field from other entries with the VMAX ID in the Host Name will help identify the arrays.

By default NXLOG will run continuously, checking the log file every 1 second. Another option to using the continuous *monitor* command is to use the *list* command with symaudit, specifying a particular time period, or perhaps activity code and redirecting that to a file. NXLOG could then be run manually against the file which will put the information into Log Insight. NXLOG could be configured to even massage the file and remove records that are deemed unnecessary. Such configurations, however, are beyond the scope of this document. See the Solutions Enabler documentation at support.EMC.com for more information on symaudit options.

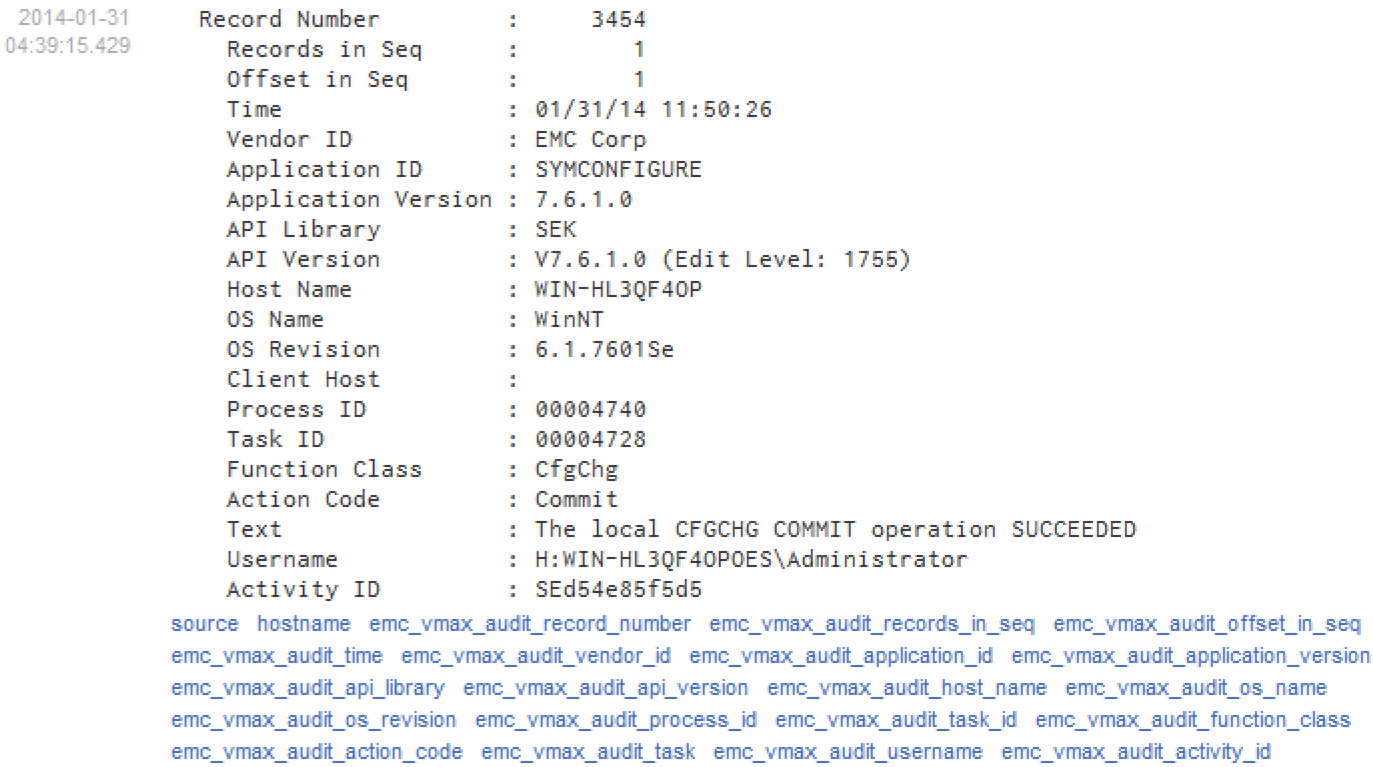
User-defined fields

The following are the user-defined fields that have been extracted for the detailed auditing logs. There are 20 fields in a single audit record and they have all been defined. The field names for the long auditing records all have the same suffix "emc_vmax_audit_" – the "audit" representing the long form of the audit record as opposed to the "aud" for the short form. Both suffixes also serve to differentiate them from the user-defined fields in the base content pack.

- emc_vmax_audit_action_code
- emc_vmax_audit_activity_id
- emc_vmax_audit_api_library
- emc_vmax_audit_api_version
- emc_vmax_audit_application_id
- emc_vmax_audit_application_version
- emc_vmax_audit_client_host
- emc_vmax_audit_function_class
- emc_vmax_audit_host_name
- emc_vmax_audit_offset_in_seq
- emc_vmax_audit_os_name
- emc_vmax_audit_os_revision
- emc_vmax_audit_process_id
- emc_vmax_audit_record_number

- emc_vmax_audit_records_in_seq
- emc_vmax_audit_task
- emc_vmax_audit_task_id
- emc_vmax_audit_time
- emc_vmax_audit_username
- emc_vmax_audit_vendor_id

An entry in Log Insight with the fields identified appears in Figure 39.



```
2014-01-31
04:39:15.429
```

```
Record Number          :     3454
  Records in Seq       :        1
  Offset in Seq        :        1
  Time                 : 01/31/14 11:50:26
  Vendor ID            : EMC Corp
  Application ID       : SYMCONFIGURE
  Application Version  : 7.6.1.0
  API Library          : SEK
  API Version          : V7.6.1.0 (Edit Level: 1755)
  Host Name            : WIN-HL3QF4OP
  OS Name              : WinNT
  OS Revision          : 6.1.7601Se
  Client Host          :
  Process ID           : 00004740
  Task ID              : 00004728
  Function Class       : CfgChg
  Action Code          : Commit
  Text                 : The local CFGCHG COMMIT operation SUCCEEDED
  Username             : H:WIN-HL3QF4OPOES\Administrator
  Activity ID          : SEd54e85f5d5
```

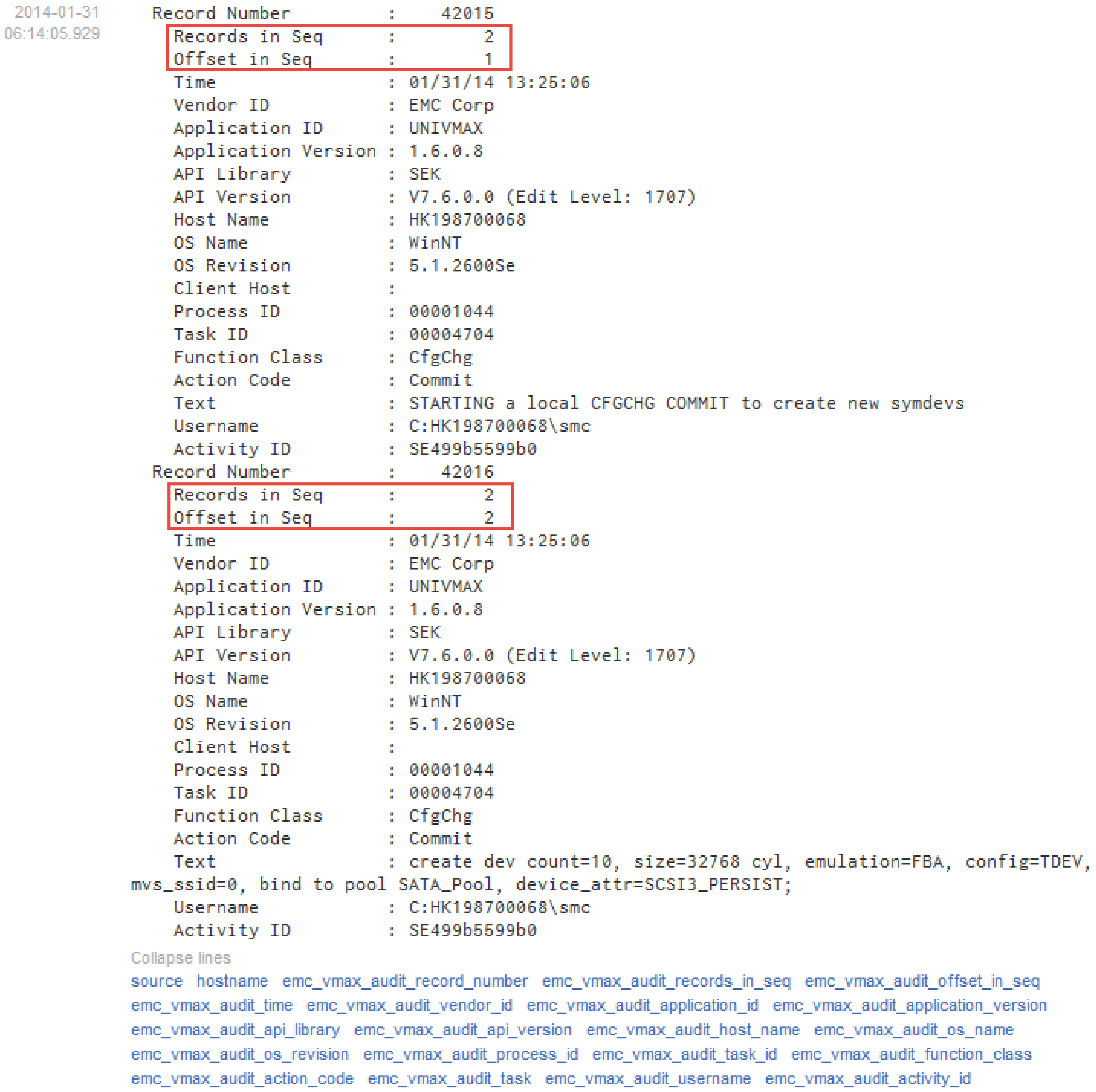
source
hostname
emc_vmax_audit_record_number
emc_vmax_audit_records_in_seq
emc_vmax_audit_offset_in_seq
emc_vmax_audit_time
emc_vmax_audit_vendor_id
emc_vmax_audit_application_id
emc_vmax_audit_application_version
emc_vmax_audit_api_library
emc_vmax_audit_api_version
emc_vmax_audit_host_name
emc_vmax_audit_os_name
emc_vmax_audit_os_revision
emc_vmax_audit_process_id
emc_vmax_audit_task_id
emc_vmax_audit_function_class
emc_vmax_audit_action_code
emc_vmax_audit_task
emc_vmax_audit_username
emc_vmax_audit_activity_id

Figure 39. Audit entry from symaudit with user-defined fields

Note that the user-defined fields are based on a verbose auditing record. If a more condensed version of the audit record is sent to Log Insight without the –v switch, e.g. *symaudit –sid xx monitor –text*, the user-defined fields will not work. User-defined fields are positional and rely on a pre and post context. As the condensed versions of the audit log have a different format, the fields cannot be recognized. If a shorter record is desired, it is best to use the audit entry sent by the event daemon as explained in the Audit entries and the event daemon section.

Audit record formatting and Log Insight

There are two noteworthy items to mention concerning the symaudit logs as they appear in Log Insight. The first is to understand that audit messages sometimes come in multiples. Because the records get written together, they get sent to Log Insight together. For instance, Figure 40 is showing the creation of a device. Highlighted in the figure are the fields “Records in Seq” and “Offset in Seq” which demonstrate how the two entries are tied together. In the first record listed, 42015, the “Records in Seq” field indicates that there are 2 entries for this event while the “Offset in Seq” field designates it as the first of the two. Similarly the second record, 42016, also shows 2 records but the “Offset in Seq” field is now 2, indicating it is the second record. Note that in related messages, the Process ID and the Task ID will be the same too.



2014-01-31
06:14:05.929

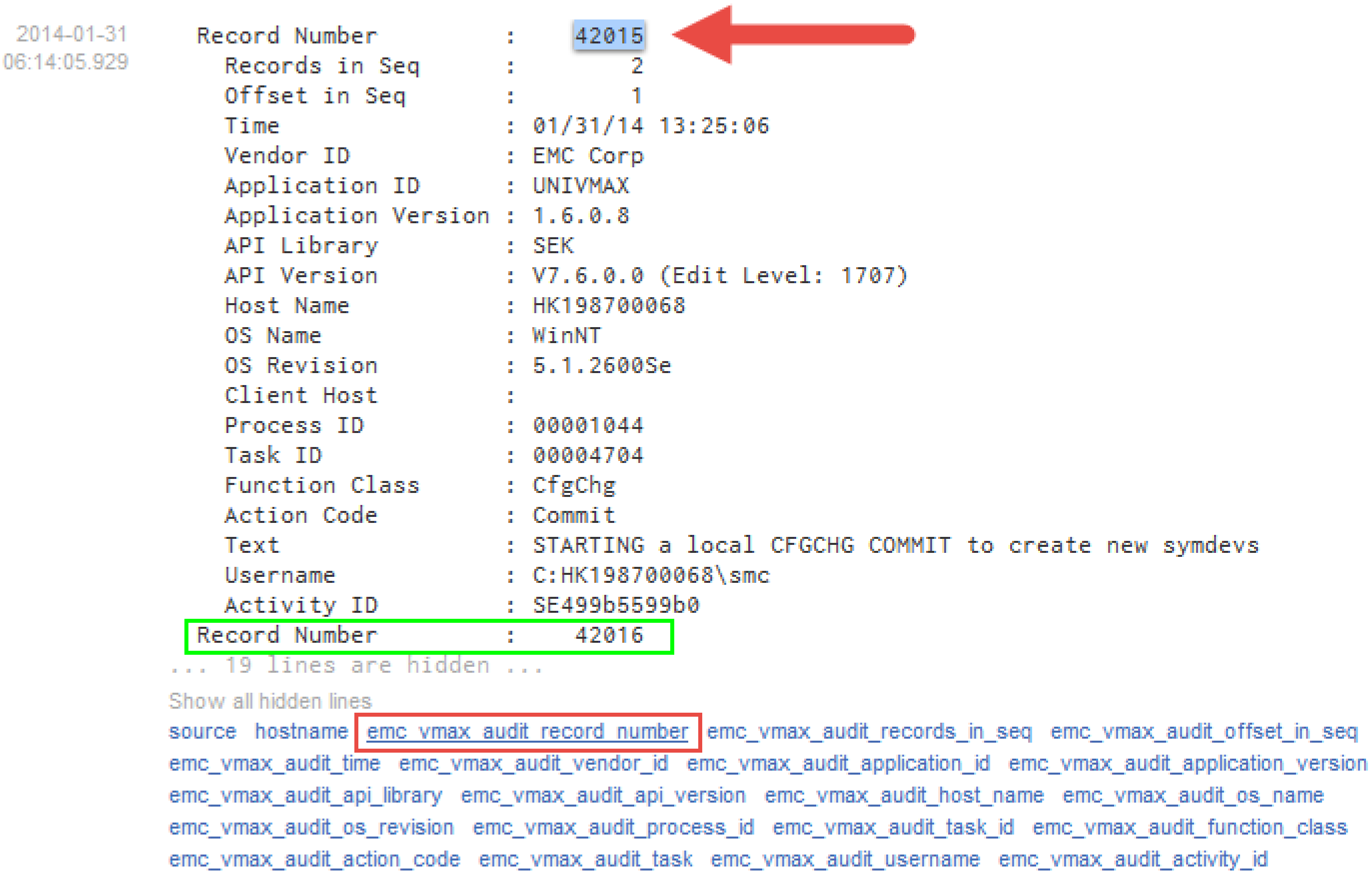
```
  Record Number         :    42015
    Records in Seq      :        2
    Offset in Seq       :        1
    Time                : 01/31/14 13:25:06
    Vendor ID           : EMC Corp
    Application ID      : UNIVMAX
    Application Version : 1.6.0.8
    API Library         : SEK
    API Version         : V7.6.0.0 (Edit Level: 1707)
    Host Name           : HK198700068
    OS Name             : WinNT
    OS Revision         : 5.1.2600Se
    Client Host         :
    Process ID          : 00001044
    Task ID             : 00004704
    Function Class      : CfgChg
    Action Code         : Commit
    Text                : STARTING a local CFGCHG COMMIT to create new symdevs
    Username            : C:HK198700068\smc
    Activity ID         : SE499b5599b0
  Record Number         :    42016
    Records in Seq      :        2
    Offset in Seq       :        2
    Time                : 01/31/14 13:25:06
    Vendor ID           : EMC Corp
    Application ID      : UNIVMAX
    Application Version : 1.6.0.8
    API Library         : SEK
    API Version         : V7.6.0.0 (Edit Level: 1707)
    Host Name           : HK198700068
    OS Name             : WinNT
    OS Revision         : 5.1.2600Se
    Client Host         :
    Process ID          : 00001044
    Task ID             : 00004704
    Function Class      : CfgChg
    Action Code         : Commit
    Text                : create dev count=10, size=32768 cyl, emulation=FBA, config=TDEV,
mvs_ssid=0, bind to pool SATA_Pool, device_attr=SCSI3_PERSIST;
    Username            : C:HK198700068\smc
    Activity ID         : SE499b5599b0
```

Collapse lines

source hostname emc_vmax_audit_record_number emc_vmax_audit_records_in_seq emc_vmax_audit_offset_in_seq emc_vmax_audit_time emc_vmax_audit_vendor_id emc_vmax_audit_application_id emc_vmax_audit_application_version emc_vmax_audit_api_library emc_vmax_audit_api_version emc_vmax_audit_host_name emc_vmax_audit_os_name emc_vmax_audit_os_revision emc_vmax_audit_process_id emc_vmax_audit_task_id emc_vmax_audit_function_class emc_vmax_audit_action_code emc_vmax_audit_task emc_vmax_audit_username emc_vmax_audit_activity_id

Figure 40. Audit record with multiple entries

The second noteworthy item also relates to multiple records and user-defined fields. Log Insight is not capable of recognizing multiple entries of an extracted field in a single event. So using the previous entry in Figure 40 as an example, if one puts the cursor over the user-defined field, emc_vmax_audit_record_number, only the first occurrence will be highlighted. This is seen in Figure 41.



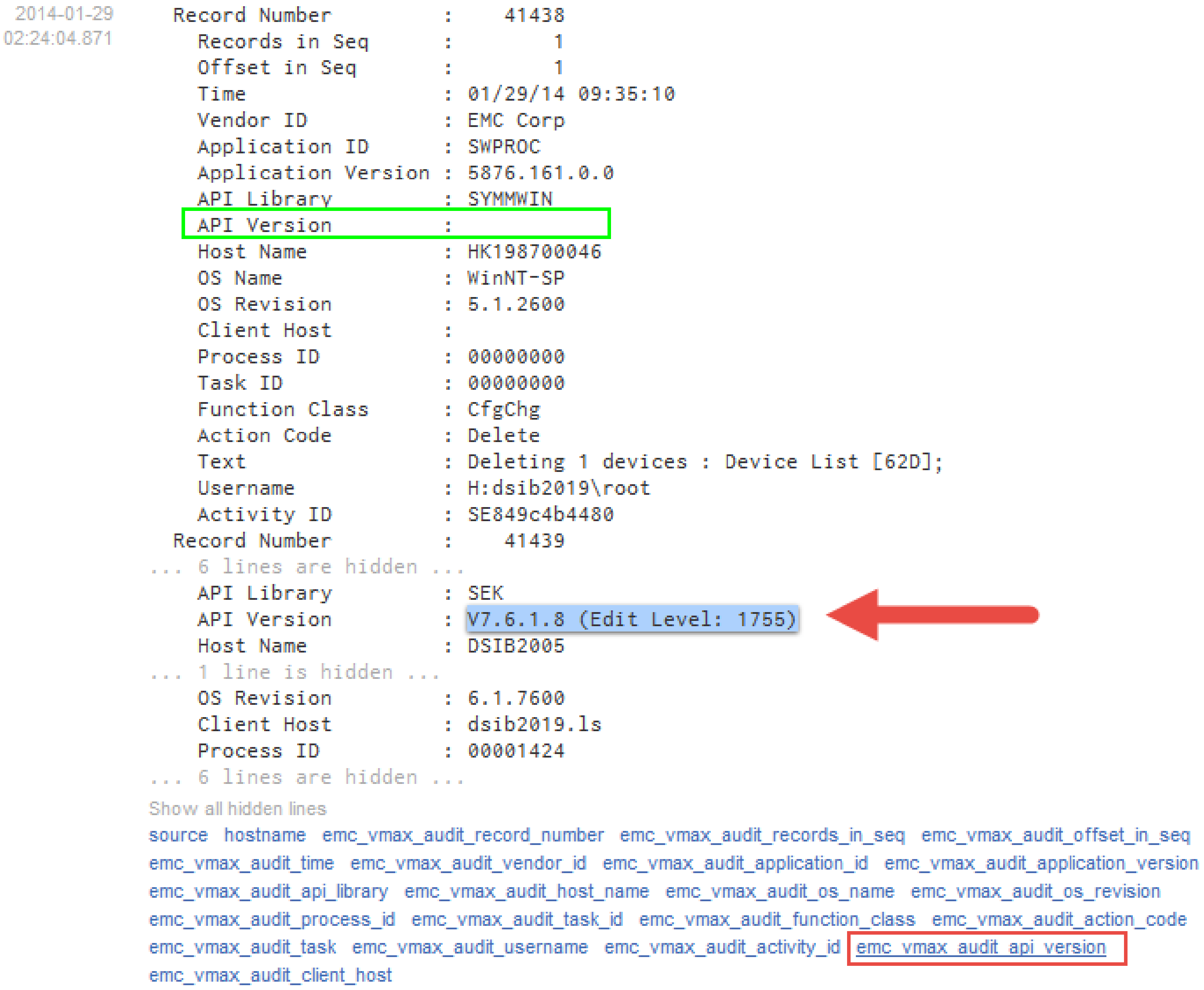
```
2014-01-31    Record Number           :     42015
06:14:05.929    Records in Seq        :         2
                Offset in Seq         :         1
                Time                  : 01/31/14 13:25:06
                Vendor ID             : EMC Corp
                Application ID        : UNIVMAX
                Application Version   : 1.6.0.8
                API Library           : SEK
                API Version           : V7.6.0.0 (Edit Level: 1707)
                Host Name             : HK198700068
                OS Name               : WinNT
                OS Revision           : 5.1.2600Se
                Client Host           :
                Process ID            : 00001044
                Task ID               : 00004704
                Function Class        : CfgChg
              Action Code           : Commit
                Text                  : STARTING a local CFGCHG COMMIT to create new symdevs
                Username              : C:HK198700068\smc
                Activity ID           : SE499b5599b0
              Record Number           :     42016
            ... 19 lines are hidden ...
```

Show all hidden lines

source hostname emc_vmax_audit_record_number emc_vmax_audit_records_in_seq emc_vmax_audit_offset_in_seq emc_vmax_audit_time emc_vmax_audit_vendor_id emc_vmax_audit_application_id emc_vmax_audit_application_version emc_vmax_audit_api_library emc_vmax_audit_api_version emc_vmax_audit_host_name emc_vmax_audit_os_name emc_vmax_audit_os_revision emc_vmax_audit_process_id emc_vmax_audit_task_id emc_vmax_audit_function_class emc_vmax_audit_action_code emc_vmax_audit_task emc_vmax_audit_username emc_vmax_audit_activity_id

Figure 41. User-defined fields with multiple entries

Similarly, if there are multiple entries but the first occurrence of the field is NULL, Log Insight will highlight the next entry as in Figure 42 with the user-defined field emc_vmax_audit_api_version.



```
2014-01-29     Record Number          :     41438
02:24:04.871     Records in Seq       :         1
                 Offset in Seq        :         1
                 Time                 : 01/29/14 09:35:10
                 Vendor ID            : EMC Corp
                 Application ID       : SWPROC
                 Application Version  : 5876.161.0.0
                 API Library          : SYMMWIN
                 API Version          :
                 Host Name            : HK198700046
                 OS Name              : WinNT-SP
                 OS Revision          : 5.1.2600
                 Client Host          :
                 Process ID           : 00000000
                 Task ID              : 00000000
                 Function Class       : CfgChg
                 Action Code          : Delete
                 Text                 : Deleting 1 devices : Device List [62D];
                 Username             : H:dsib2019\root
                 Activity ID          : SE849c4b4480
               Record Number          :     41439
             ... 6 lines are hidden ...
                 API Library          : SEK
                 API Version          : V7.6.1.8 (Edit Level: 1755)
                 Host Name            : DSIB2005
             ... 1 line is hidden ...
                 OS Revision          : 6.1.7600
                 Client Host          : dsib2019.ls
                 Process ID           : 00001424
             ... 6 lines are hidden ...
```

Show all hidden lines

source hostname emc_vmax_audit_record_number emc_vmax_audit_records_in_seq emc_vmax_audit_offset_in_seq emc_vmax_audit_time emc_vmax_audit_vendor_id emc_vmax_audit_application_id emc_vmax_audit_application_version emc_vmax_audit_api_library emc_vmax_audit_host_name emc_vmax_audit_os_name emc_vmax_audit_os_revision emc_vmax_audit_process_id emc_vmax_audit_task_id emc_vmax_audit_function_class emc_vmax_audit_action_code emc_vmax_audit_task emc_vmax_audit_username emc_vmax_audit_activity_id emc_vmax_audit_api_version emc_vmax_audit_client_host

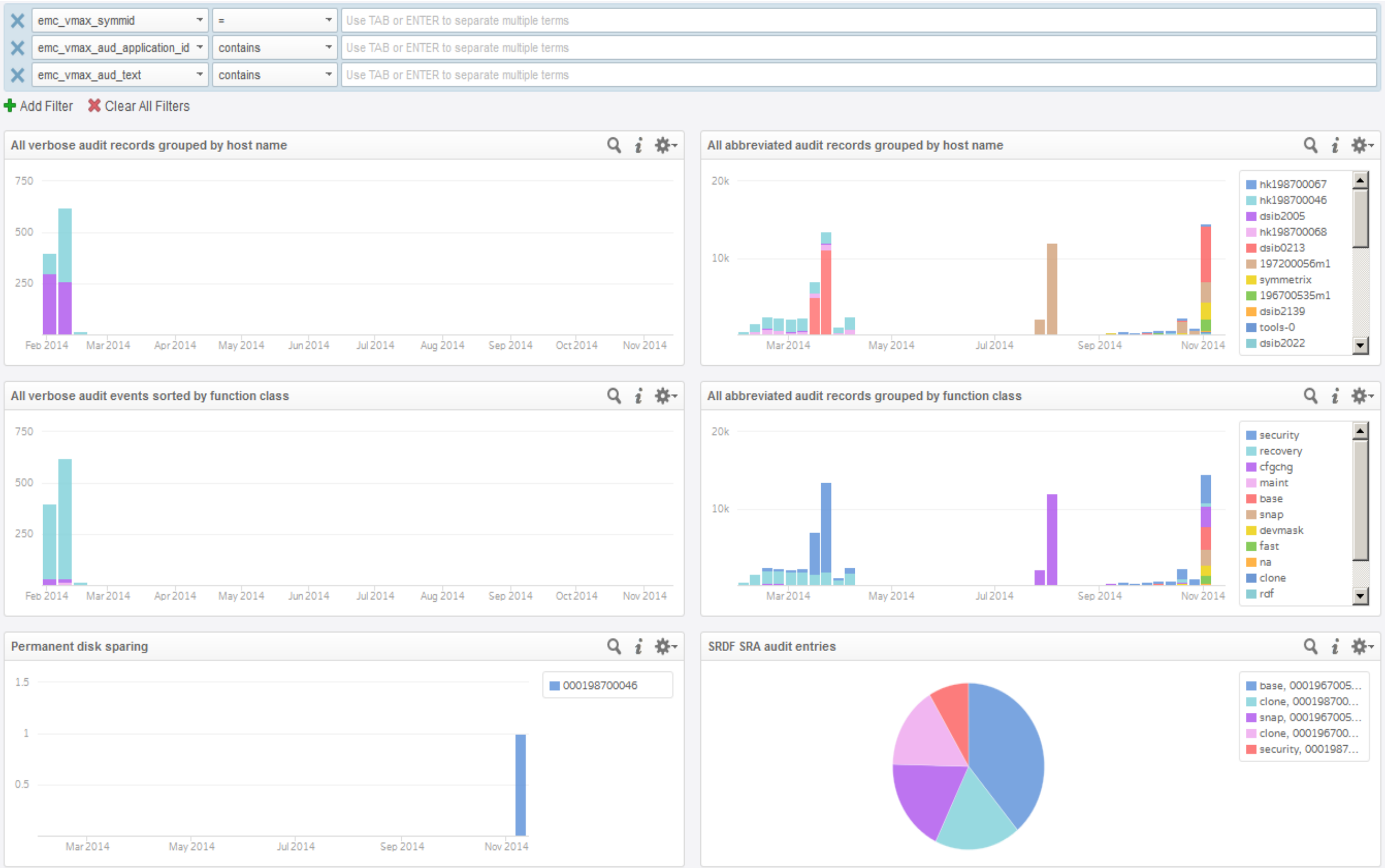
Figure 42. User-defined fields with multiple entries and a NULL value

Dashboards

Currently there is a single dashboard for auditing information. Unlike the base content pack and the information it displays, auditing information does not lend itself well to many different kinds of widgets. The single dashboard is:

- **Auditing** – Contains widgets with information about all VMAX audit entries in the Log Insight instance. This includes 2 widgets for event daemon audit entries, 2 widgets for symaudit entries, one for disk sparing and one for SRDF SRA for vRealize Site Recovery Manager entries.

An example of this dashboard is shown in Figure 43.



emc_vmax_symmid | = | Use TAB or ENTER to separate multiple terms

emc_vmax_aud_application_id | contains | Use TAB or ENTER to separate multiple terms

emc_vmax_aud_text | contains | Use TAB or ENTER to separate multiple terms

Figure 43. VMAX content pack - Auditing dashboard

There are no alerts or queries configured for audit information.