DELL Technologies

USING THE DELL POWERMAX CONTENT PACK FOR VMWARE ARIA OPERATIONS FOR LOGS

Monitoring Dell PowerMax log activity with VMware

Abstract

This white paper explains how to setup Dell EMC Solutions Enabler and Unisphere for PowerMax for use with VMware Aria Operations for Logs and the Dell PowerMax content pack.

September 2024

Dell Engineering

Part Number h12138.14

Table of Contents

Executive summary

VMware Aria Operations for Logs (formerly VMware Log Insight), or Operations for Logs, 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 Dell PowerMax content pack, when integrated into VMware Aria Operations for Logs, provides dashboards and user-defined fields specifically for Dell PowerMax arrays to enable administrators to conduct problem analysis and analytics on their array(s).

This paper will explain how Solutions Enabler and Unisphere can be configured to send log files to VMware Aria Operations for Logs and will provide an example of a problem analysis that can be conducted with the Dell PowerMax content pack.

Audience

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

Supported hardware and software versions

As of publication of this paper, VMware Aria Operations for Logs 8.16 is the current GA product version. The content pack covers up to Unisphere for PowerMax and Solutions Enabler 10.x and PowerMaxOS 10.x. Some fields and dashboards may not populate depending on the versions in use. Generally, upgrading to newer versions of Operations for Logs, beyond the documented version here, will not cause any issues with an existing Dell PowerMax content pack, though every effort is made to keep support up to date.

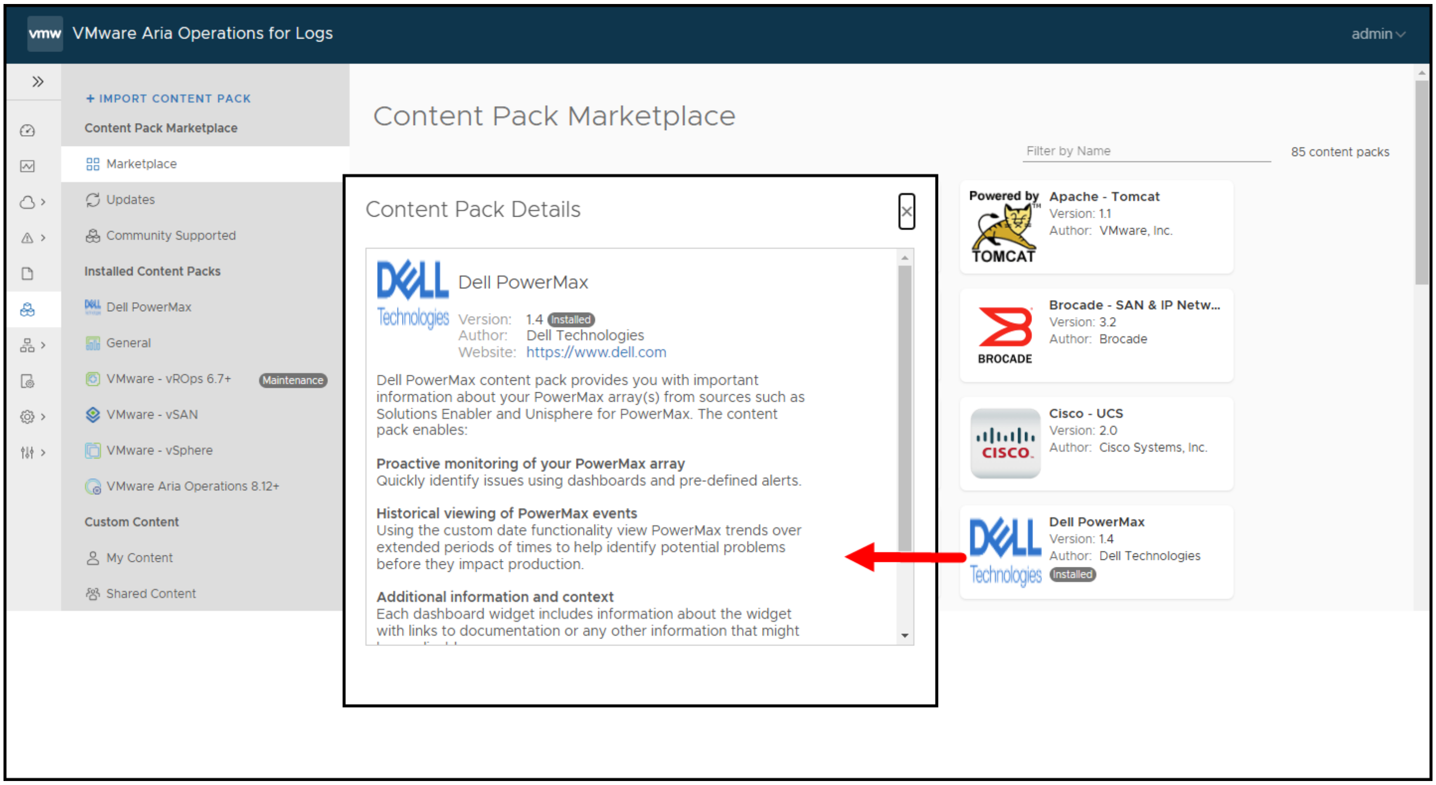
Despite the naming, the Dell PowerMax content pack supports both VMAX and PowerMax arrays. As Unisphere for PowerMax and Solutions Enabler are backward compatible, Dell recommends using these software versions even when monitoring VMAX arrays.

Content

The content of this paper includes information and screenshots from current and previous versions of the content pack. While the technical information is accurate, some naming (e.g., user-defined fields) may reflect a previous content pack. It has no bearing, however, on functionality.

Dell PowerMax content pack

A content pack for VMware Aria Operations for Logs (Operations for Logs) is a special type of dashboard group. It is delivered as a file with a "vlcp" extension and is in XML format. A content pack can be imported into any instance of Operations for Logs. In essence it is a plug-in. VMware delivers a few default content packs with Operations for Logs that are designed for VMware-related log information. Similarly, Dell has developed their own custom content pack for PowerMax log information. As with all content packs, it is available within Operations for Logs in the Marketplace screen. An example of the previous release is shown in Figure 1.



Dell PowerMax

Version: 1.4 Installed
Author: Dell Technologies
Website: https://www.dell.com

Dell PowerMax content pack provides you with important information about your PowerMax array(s) from sources such as Solutions Enabler and Unisphere for PowerMax. The content pack enables:

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

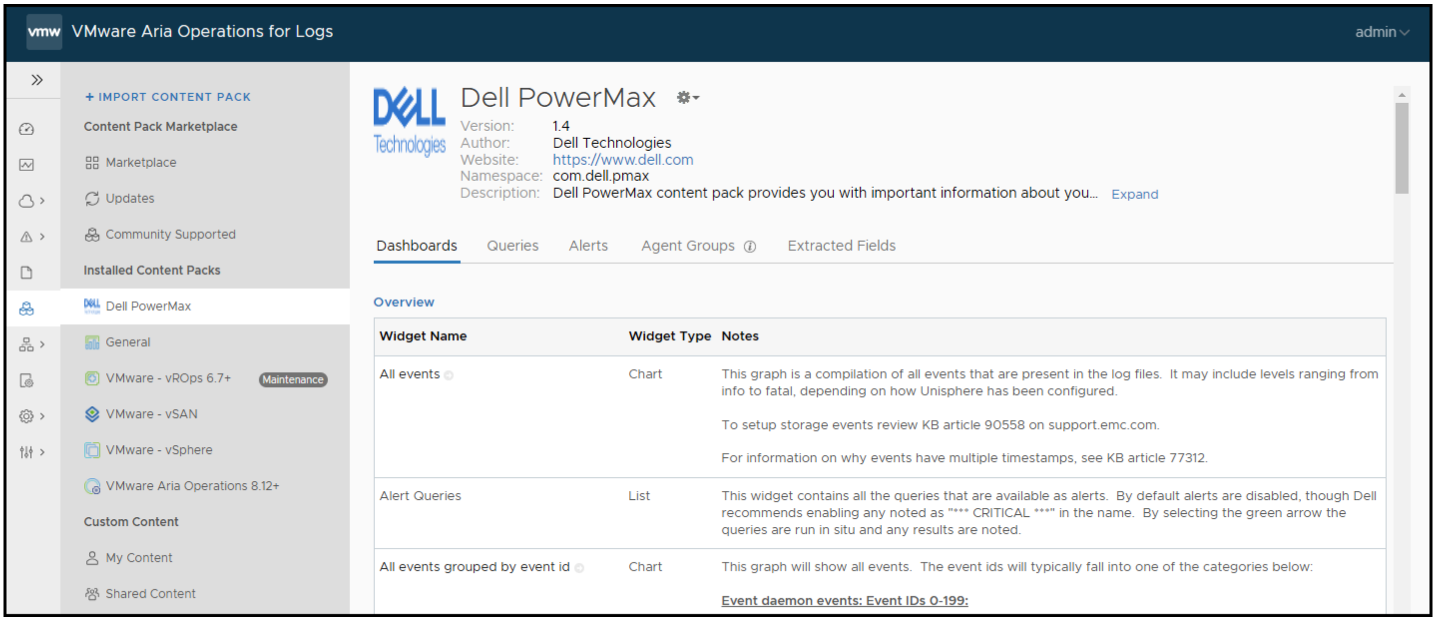
Historical viewing of PowerMax events
Using the custom date functionality view PowerMax trends over extended periods of times to help identify potential problems before they impact production.

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

Figure 1. Operations for Logs Content Pack 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 PowerMax content pack is not required in order to use Operations for Logs with the PowerMax, it is recommended as a good starting point for helping to categorize all the log information coming from the array.

When viewing the PowerMax content pack definition in Operations for Logs, there is a full description of the content pack details. Seen in Figure 2 is the definition of the PowerMax content pack.



Dell PowerMax

Version: 1.4
Author: Dell Technologies
Website: https://www.dell.com
Namespace: com.dell.pmax
Description: Dell PowerMax content pack provides you with important information about you...

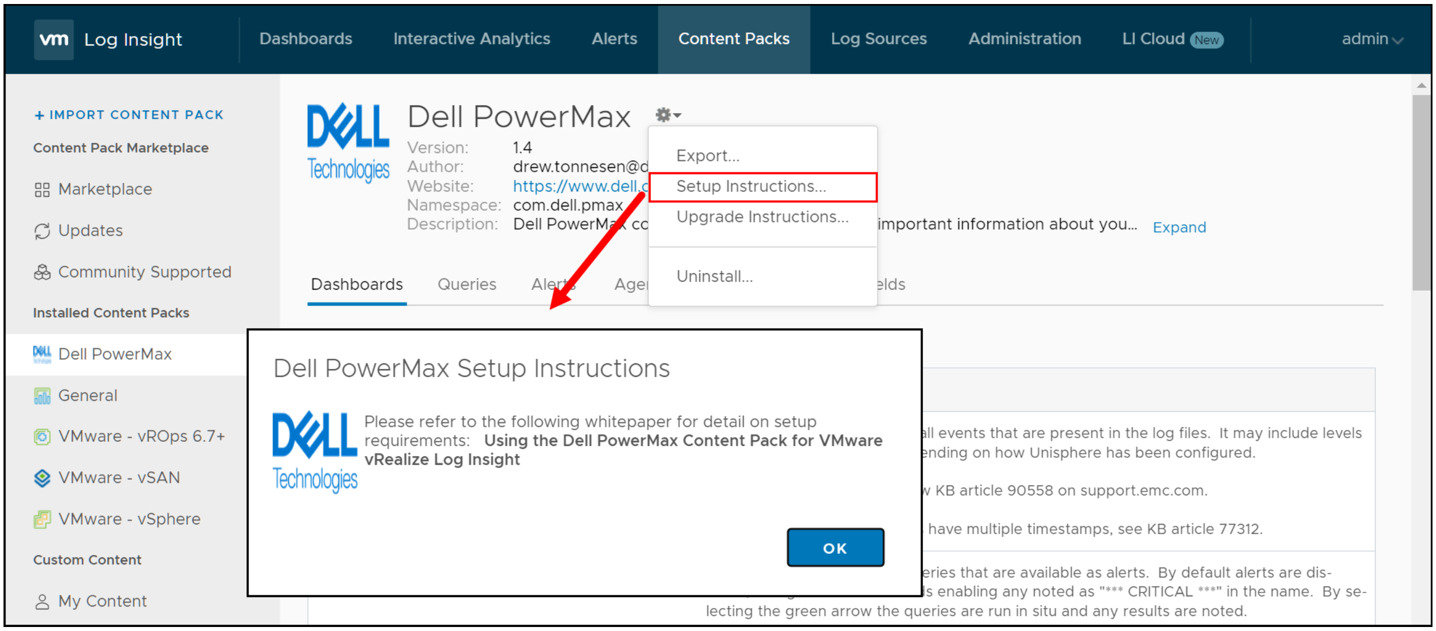
Overview

Widget Name	Widget Type	Notes
All events	Chart	This graph is a compilation of all events that are present in the log files. It may include levels ranging from info to fatal, depending on how Unisphere has been configured. To setup storage events review KB article 90558 on support.emc.com. For information on why events have multiple timestamps, see KB article 77312.
Alert Queries	List	This widget contains all the queries that are available as alerts. By default alerts are disabled, though Dell recommends enabling any noted as "*** CRITICAL ***" in the name. By selecting the green arrow the queries are run in situ and any results are noted.
All events grouped by event id	Chart	This graph will show all events. The event ids will typically fall into one of the categories below: Event daemon events: Event IDs 0-199:

Figure 2. VMware Aria Operations for Logs with the PowerMax content pack

There is also a separate dialog box with a link to the installation instructions. Use the gear icon at the top to access the **Setup Instructions**. This is shown in Figure 3.

Note: The paper referenced below was renamed when Log Insight was renamed. The content pack instructions are awaiting update.



Dell PowerMax

Version: 1.4
Author: drew.tonnesen@d
Website: https://www.dell.c
Namespace: com.dell.pmax
Description: Dell PowerMa cc important information about you...

Dell PowerMax Setup Instructions

Please refer to the following whitepaper for detail on setup requirements: **Using the Dell PowerMax Content Pack for VMware vRealize Log Insight**

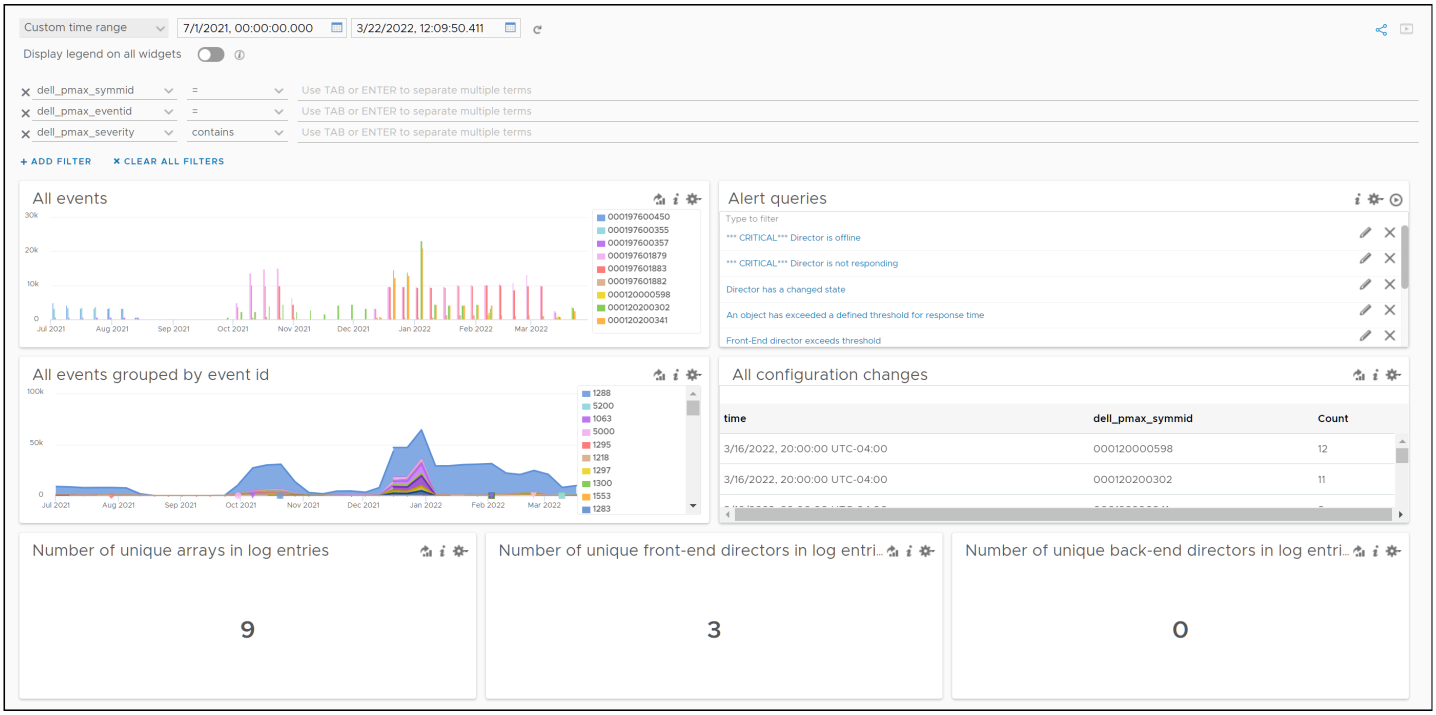
Figure 3. Setup instructions for the PowerMax content pack

Dashboards

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

- **Overview** – Contains widgets with information about all PowerMax data in your Operations for Logs instance.
- **Problems** – Contains widgets with information about potential problems that are recorded in the log files.
- **Service levels** – Contains widgets about Service Level alerts on the PowerMax.
- **Director events** – Contains widgets with information about any front-end or back-end director events on the PowerMax.
- **Local & remote replication** – Contains widgets specific to log messages generated by SRDF™ or TimeFinder™ software.
- **Virtual volumes (vVols)** – Contains widgets with information about vVol storage containers.
- **Auditing** – Contains widgets that display all audit log information.

Examples of the first seven dashboards, in order, are presented in Figure 4, Figure 5, Figure 6, Figure 7, Figure 8, and Figure 9. The auditing dashboard is covered in the Appendix: Dell PowerMax content pack and PowerMax auditing data.



Custom time range: 7/1/2021, 00:00:00.000 – 3/22/2022, 12:09:50.411

Display legend on all widgets: off

dell_pmax_symmid = Use TAB or ENTER to separate multiple terms

dell_pmax_eventid = Use TAB or ENTER to separate multiple terms

dell_pmax_severity contains Use TAB or ENTER to separate multiple terms

*** 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

All configuration changes

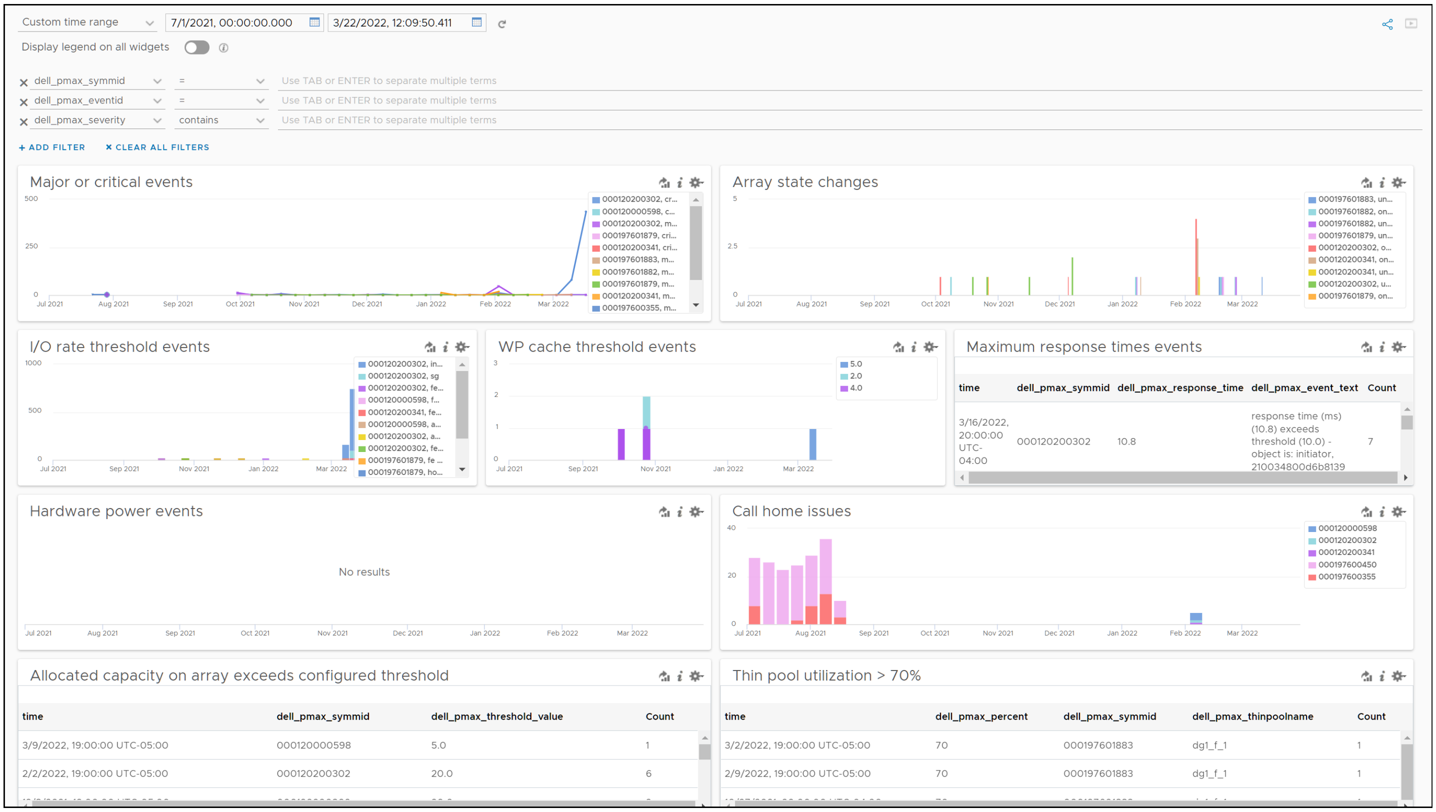
time	dell_pmax_symmid	Count
3/16/2022, 20:00:00 UTC-04:00	000120000598	12
3/16/2022, 20:00:00 UTC-04:00	000120200302	11

Number of unique arrays in log entries: 9

Number of unique front-end directors in log entri…: 3

Number of unique back-end directors in log entri…: 0

Figure 4. PowerMax Content pack - Overview dashboard



Custom time range: 7/1/2021, 00:00:00.000 – 3/22/2022, 12:09:50.411

Display legend on all widgets ○

- dell_pmax_symmid = Use TAB or ENTER to separate multiple terms
- dell_pmax_eventid = Use TAB or ENTER to separate multiple terms
- dell_pmax_severity contains Use TAB or ENTER to separate multiple terms

+ ADD FILTER ✕ CLEAR ALL FILTERS

Maximum response times events

time	dell_pmax_symmid	dell_pmax_response_time	dell_pmax_event_text	Count
3/16/2022, 20:00:00 UTC-04:00	000120200302	10.8	response time (ms) (10.8) exceeds threshold (10.0) - object is: initiator, 210034800d6b8139	7

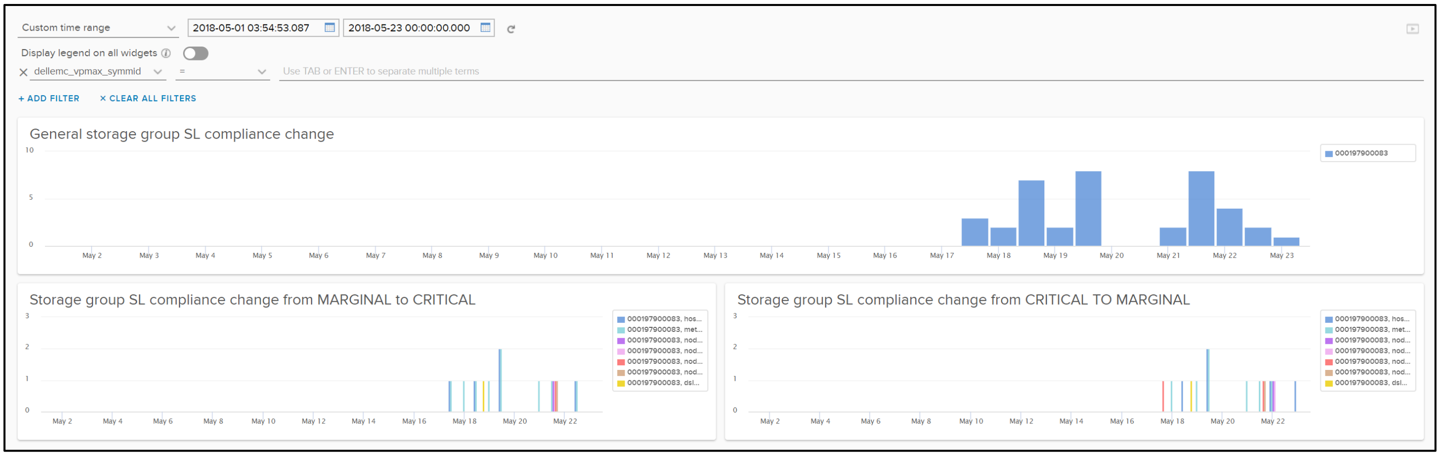
Allocated capacity on array exceeds configured threshold

time	dell_pmax_symmid	dell_pmax_threshold_value	Count
3/9/2022, 19:00:00 UTC-05:00	000120000598	5.0	1
2/2/2022, 19:00:00 UTC-05:00	000120200302	20.0	6

Thin pool utilization > 70%

time	dell_pmax_percent	dell_pmax_symmid	dell_pmax_thinpoolname	Count
3/2/2022, 19:00:00 UTC-05:00	70	000197601883	dg1_f_1	1
2/9/2022, 19:00:00 UTC-05:00	70	000197601883	dg1_f_1	1

Figure 5. PowerMax content pack - Problems dashboard



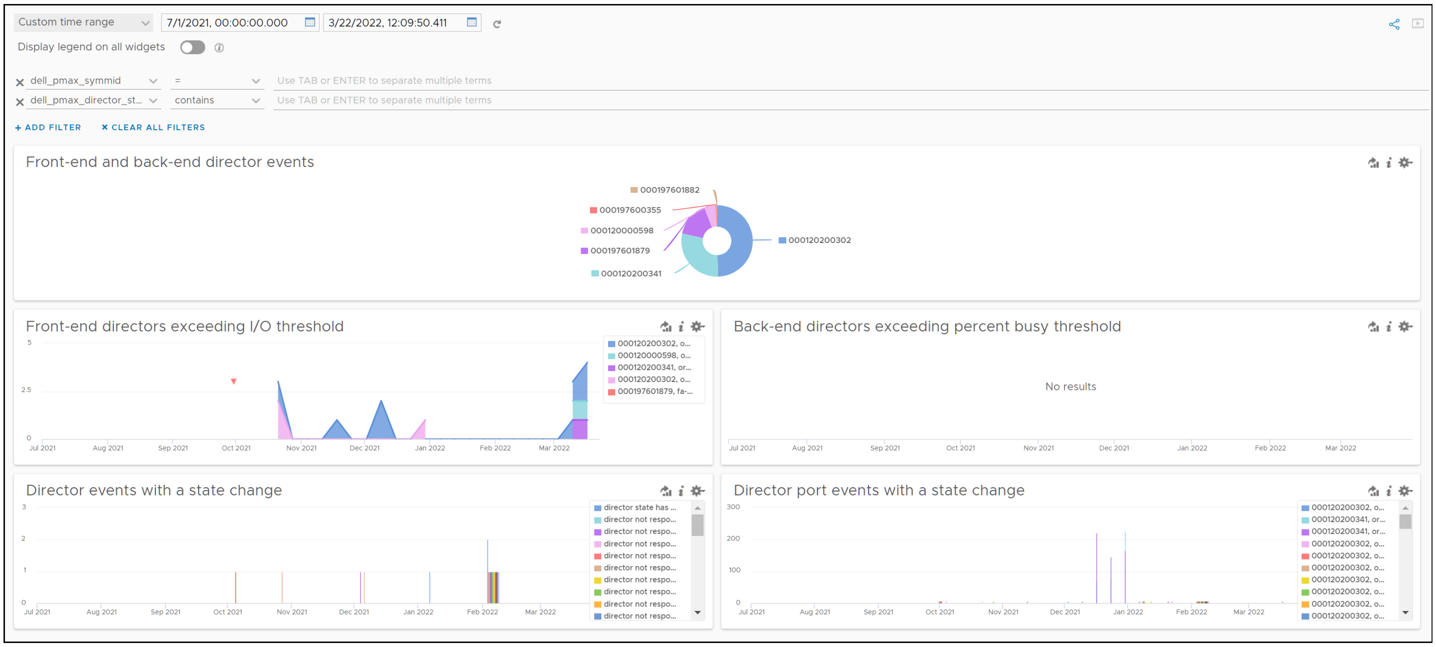
Custom time range: 2018-05-01 03:54:53.087 – 2018-05-23 00:00:00.000

Display legend on all widgets ⓘ ○

- dellemc_vpmax_symmid = Use TAB or ENTER to separate multiple terms

+ ADD FILTER ✕ CLEAR ALL FILTERS

Figure 6. PowerMax content pack – Service levels dashboard



Custom time range | 7/1/2021, 00:00:00.000 | 3/22/2022, 12:09:50.411

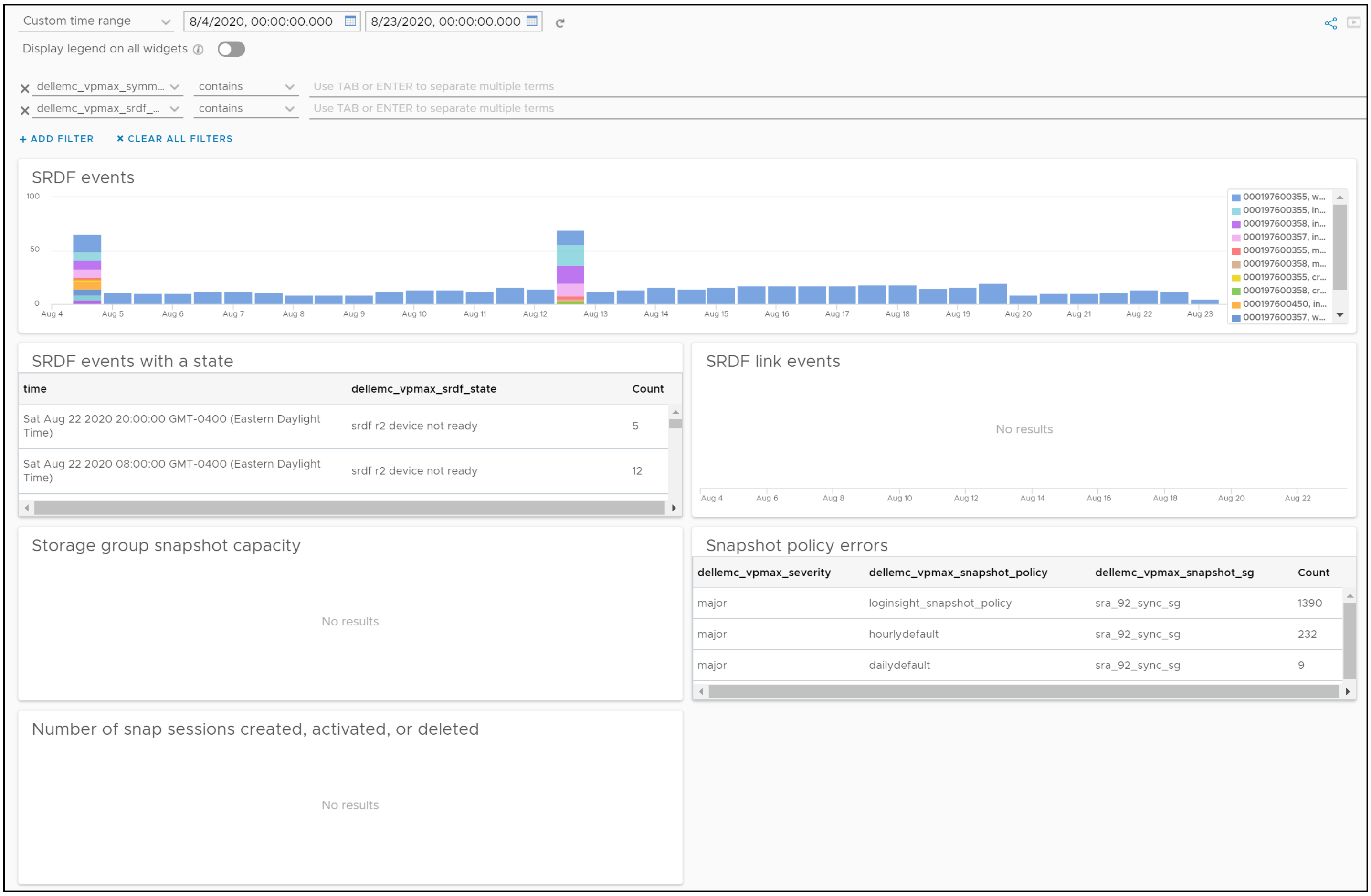
Display legend on all widgets

✕ dell_pmax_symmid | = | Use TAB or ENTER to separate multiple terms

✕ dell_pmax_director_st... | contains | Use TAB or ENTER to separate multiple terms

+ ADD FILTER ✕ CLEAR ALL FILTERS

Figure 7. PowerMax content pack - Director events dashboard



8/4/2020, 00:00:00.000 – 8/23/2020, 00:00:00.000

× dellemc_vpmax_symm... contains Use TAB or ENTER to separate multiple terms

× dellemc_vpmax_srdf_... contains Use TAB or ENTER to separate multiple terms

SRDF events

SRDF events with a state

time	dellemc_vpmax_srdf_state	Count
Sat Aug 22 2020 20:00:00 GMT-0400 (Eastern Daylight Time)	srdf r2 device not ready	5
Sat Aug 22 2020 08:00:00 GMT-0400 (Eastern Daylight Time)	srdf r2 device not ready	12

SRDF link events

No results

Storage group snapshot capacity

No results

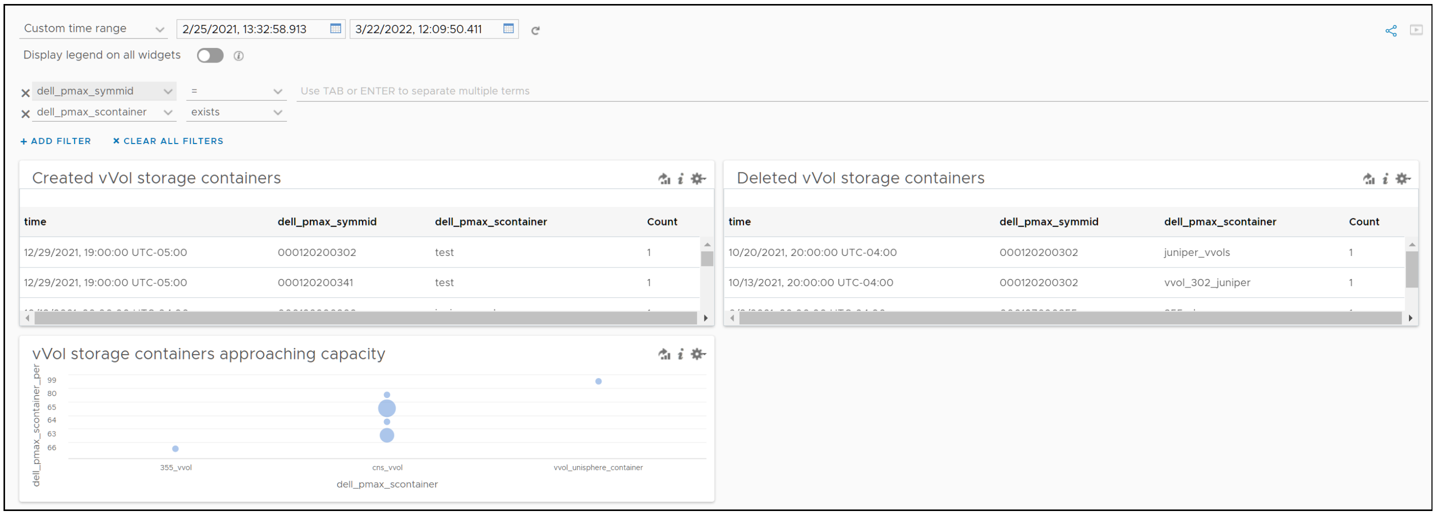
Snapshot policy errors

dellemc_vpmax_severity	dellemc_vpmax_snapshot_policy	dellemc_vpmax_snapshot_sg	Count
major	loginsight_snapshot_policy	sra_92_sync_sg	1390
major	hourlydefault	sra_92_sync_sg	232
major	dailydefault	sra_92_sync_sg	9

Number of snap sessions created, activated, or deleted

No results

Figure 8. PowerMax content pack - Local & remote replication dashboard



2/25/2021, 13:32:58.913 – 3/22/2022, 12:09:50.411

× dell_pmax_symmid = Use TAB or ENTER to separate multiple terms

× dell_pmax_scontainer exists

Created vVol storage containers

time	dell_pmax_symmid	dell_pmax_scontainer	Count
12/29/2021, 19:00:00 UTC-05:00	000120200302	test	1
12/29/2021, 19:00:00 UTC-05:00	000120200341	test	1

Deleted vVol storage containers

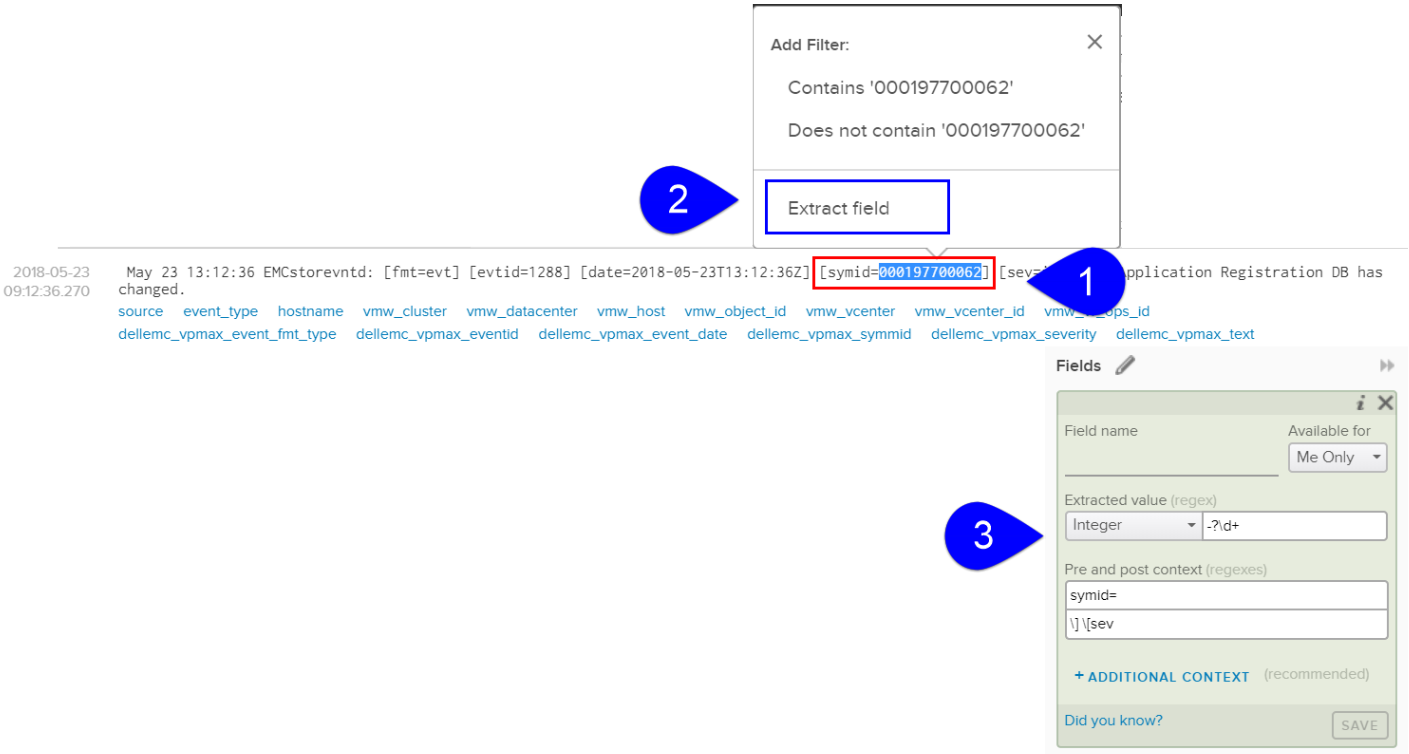
time	dell_pmax_symmid	dell_pmax_scontainer	Count
10/20/2021, 20:00:00 UTC-04:00	000120200302	juniper_vvols	1
10/13/2021, 20:00:00 UTC-04:00	000120200302	vvol_302_juniper	1

vVol storage containers approaching capacity

Figure 9. PowerMax content pack– Virtual volumes (vVols) 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. Operations for Logs 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 10, individual fields can be identified for extraction.



Add Filter:

Contains '000197700062'

Does not contain '000197700062'

Extract field

```
2018-05-23     May 23 13:12:36 EMCstorevntd: [fmt=evt] [evtid=1288] [date=2018-05-23T13:12:36Z] [symid=000197700062] [sev=        pplication Registration DB has
09:12:36.270   changed.
```

source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_ ops_id
dellemc_vpmax_event_fmt_type dellemc_vpmax_eventid dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_severity dellemc_vpmax_text

Fields

Field name

Available for: Me Only

Extracted value (regex): Integer -?\d+

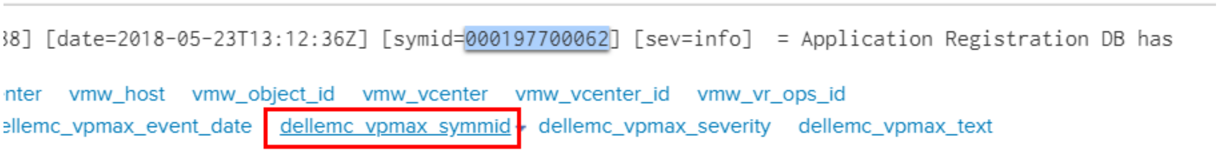
Pre and post context (regexes):
symid=
\] \[sev

+ ADDITIONAL CONTEXT (recommended)

Did you know?

Figure 10. A VMAX log entry - user-defined field extraction

By highlighting the value, an **Extract Field** option appears which can be selected. Once clicked, a regular expression can be applied along with a field name 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 11. By hovering the cursor over the new field, the symid value will be highlighed in blue.



```
38] [date=2018-05-23T13:12:36Z] [symid=000197700062] [sev=info]  = Application Registration DB has
```

nter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id
ellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_severity dellemc_vpmax_text

Figure 11. User-defined field dell_pmax_symmid

Within the PowerMax content pack, Dell has preconfigured user-defined fields for the most commonly appearing objects in the log files. All of the fields have the prefix "dell_pmax_" so they can be easily identified. Note that as some VMAX/PowerMax 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.

- dell_pmax_array_srdf_gp
- dell_pmax_array_state
- dell_pmax_be_director
- dell_pmax_devices
- dell_pmax_director_name
- dell_pmax_director_state
- dell_pmax_egress_tracks
- dell_pmax_event_date
- dell_pmax_event_fmt_type
- dell_pmax_event_text
- dell_pmax_eventid
- dell_pmax_fe_director
- dell_pmax_fe_portname
- dell_pmax_ingress_tracks
- dell_pmax_iorate
- dell_pmax_iscsi_dir_ip
- dell_pmax_objecttype
- dell_pmax_pctbusy
- dell_pmax_pcthit
- dell_pmax_percent
- dell_pmax_port_name
- dell_pmax_port_status
- dell_pmax_portgroup
- dell_pmax_power
- dell_pmax_response_time
- dell_pmax_scontainer
- dell_pmax_scontainer_percent

- dell_pmax_severity
- dell_pmax_sg
- dell_pmax_sg_state
- dell_pmax_sg_state_name
- dell_pmax_sl_sg
- dell_pmax_snapshot_percent
- dell_pmax_snapshot_policy
- dell_pmax_snapshot_sg
- dell_pmax_srdf_group
- dell_pmax_srdf_state
- dell_pmax_srp_name
- dell_pmax_storagegrp
- dell_pmax_storagetier
- dell_pmax_symmid
- dell_pmax_system
- dell_pmax_thinpool_name
- dell_pmax_thinpoolname
- dell_pmax_threshold_value
- dell_pmax_used_capacity
- dell_pmax_volume
- dell_pmax_wp_cache_threshold
- dell_pmax_wp_cache_value

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 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 PowerMax events. While the alerts are named to make their purpose self-explanatory, Dell 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 Dell 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 PowerMax content pack displays existing log information in the database. For the VMAX and PowerMax, both Solutions Enabler and Unisphere for VMAX/PowerMax can be configured to send logs to Operations for Logs. The remainder 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.

Configuring PowerMax for VMware Aria Operations for Logs

In order to effectively make use of the Dell PowerMax content pack, Dell log information is needed. There are two essential products that can be configured to send this log information to Operations for Logs: Solutions Enabler and Unisphere. These products can be installed on an operating system on a VM or physical server, deployed as a virtual appliance, or utilized directly on the array (embedded management).

Solutions Enabler and the Event daemon

A Dell Solutions Enabler install provides your host with SYMAPI and STORAPI shared libraries for use by Solutions Enabler applications, and the PowerMax 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.

Solutions Enabler also has a built-in capability to monitor the PowerMax event log and send all of those event messages to a remote syslog server like Operations for Logs. 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, including the Performance option. A basic setup will be presented herein. For more detailed information please refer to the appropriate Dell Solutions Enabler Installation Guide.

Configuring Solutions Enabler on an operating system

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 Operations for Logs. These are (note the entries will be commented out):

```
#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 Operations for Logs host IP address (the syslog server) and the port of the syslog server on the host. For Operations for Logs 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 Operations for Logs. There are a number of categories to choose from, though the PowerMax content pack takes advantage of all of them. By default, any category will apply to all PowerMax arrays presented to Solutions Enabler unless the array SID is specifically listed. It is also possible to use specific event ids. Both a generic and specific example are below:

Generic

```
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 ;\
```

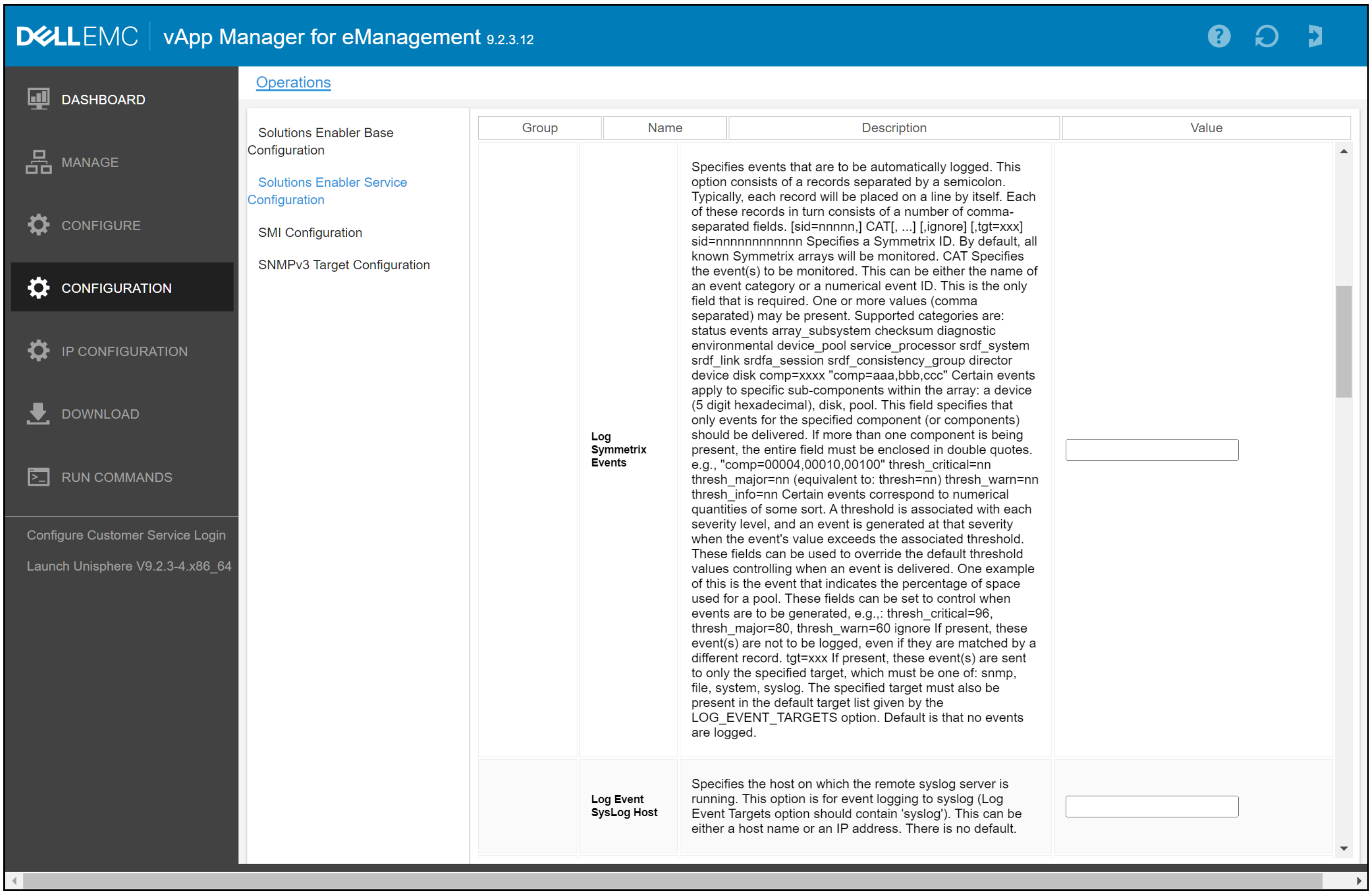
Specific

```
storevntd:LOG_SYMMETRIX_EVENTS = sid=00019570xxxx, 1525, 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 Operations for Logs.

Configuring Solutions Enabler on the vApp or embedded management

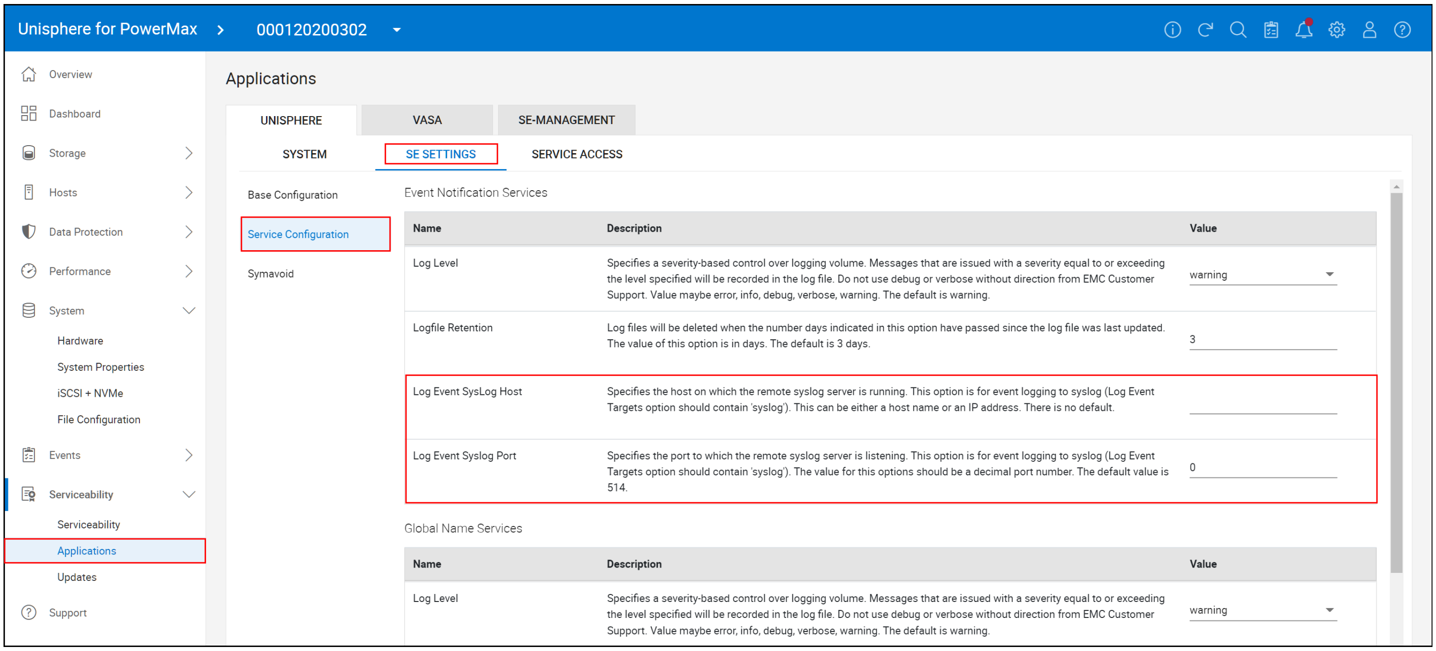
If utilizing a vApp deployment or embedded management (eManagement) with Operations for Logs, modify the previously detailed parameters by accessing the vApp Manager. The configuration screen is seen in Figure 12 for vApp Manager 9.x.


DELLEMC | vApp Manager for eManagement 9.2.3.12
DASHBOARD
MANAGE
CONFIGURE
CONFIGURATION
IP CONFIGURATION
DOWNLOAD
RUN COMMANDS
Configure Customer Service Login
Launch Unisphere V9.2.3-4.x86_64
Operations
Solutions Enabler Base Configuration
Solutions Enabler Service Configuration
SMI Configuration
SNMPv3 Target Configuration

Group	Name	Description	Value
	Log Symmetrix Events	Specifies events that are to be automatically logged. This option consists of a records separated by a semicolon. Typically, each record will be placed on a line by itself. Each of these records in turn consists of a number of comma-separated fields. [sid=nnnnn,] CAT[, ...] [,ignore] [,tgt=xxx] sid=nnnnnnnnnnnn Specifies a Symmetrix ID. By default, all known Symmetrix arrays will be monitored. CAT Specifies the event(s) to be monitored. This can be either the name of an event category or a numerical event ID. This is the only field that is required. One or more values (comma separated) may be present. Supported categories are: status events array_subsystem checksum diagnostic environmental device_pool service_processor srdf_system srdf_link srdfa_session srdf_consistency_group director device disk comp=xxxx "comp=aaa,bbb,ccc" Certain events apply to specific sub-components within the array: a device (5 digit hexadecimal), disk, pool. This field specifies that only events for the specified component (or components) should be delivered. If more than one component is being present, the entire field must be enclosed in double quotes. e.g., "comp=00004,00010,00100" thresh_critical=nn thresh_major=nn (equivalent to: thresh=nn) thresh_warn=nn thresh_info=nn Certain events correspond to numerical quantities of some sort. A threshold is associated with each severity level, and an event is generated at that severity when the event's value exceeds the associated threshold. These fields can be used to override the default threshold values controlling when an event is delivered. One example of this is the event that indicates the percentage of space used for a pool. These fields can be set to control when events are to be generated, e.g.,: thresh_critical=96, thresh_major=80, thresh_warn=60 ignore If present, these event(s) are not to be logged, even if they are matched by a different record. tgt=xxx If present, these event(s) are sent to only the specified target, which must be one of: snmp, file, system, syslog. The specified target must also be present in the default target list given by the LOG_EVENT_TARGETS option. Default is that no events are logged.	
	Log Event SysLog Host	Specifies the host on which the remote syslog server is running. This option is for event logging to syslog (Log Event Targets option should contain 'syslog'). This can be either a host name or an IP address. There is no default.	

Figure 12. Solutions Enabler parameters in vApp Manager 9.x

On the PowerMax 2500/8500, the navigation for modifying the embedded management is shown in Figure 13. Note the parameters are in the **UNISPHERE** section, not **SE-MANAGEMENT** and there is no parameter for Symmetrix events.



Event Notification Services

Name	Description	Value
Log Level	Specifies a severity-based control over logging volume. Messages that are issued with a severity equal to or exceeding the level specified will be recorded in the log file. Do not use debug or verbose without direction from EMC Customer Support. Value maybe error, info, debug, verbose, warning. The default is warning.	warning
Logfile Retention	Log files will be deleted when the number days indicated in this option have passed since the log file was last updated. The value of this option is in days. The default is 3 days.	3
Log Event SysLog Host	Specifies the host on which the remote syslog server is running. This option is for event logging to syslog (Log Event Targets option should contain 'syslog'). This can be either a host name or an IP address. There is no default.	
Log Event Syslog Port	Specifies the port to which the remote syslog server is listening. This option is for event logging to syslog (Log Event Targets option should contain 'syslog'). The value for this options should be a decimal port number. The default value is 514.	0

Global Name Services

Name	Description	Value
Log Level	Specifies a severity-based control over logging volume. Messages that are issued with a severity equal to or exceeding the level specified will be recorded in the log file. Do not use debug or verbose without direction from EMC Customer Support. Value maybe error, info, debug, verbose, warning. The default is warning.	warning

Figure 13. Unisphere parameters in Unisphere for PowerMax 10

Unisphere for PowerMax 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 PowerMax 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.

Syslog event configuration

As the system administrator user (default *smc* user in this example), log in to Unisphere and navigate to the settings gear, then "Alerts" and "Notifications". This is shown in Figure 14.

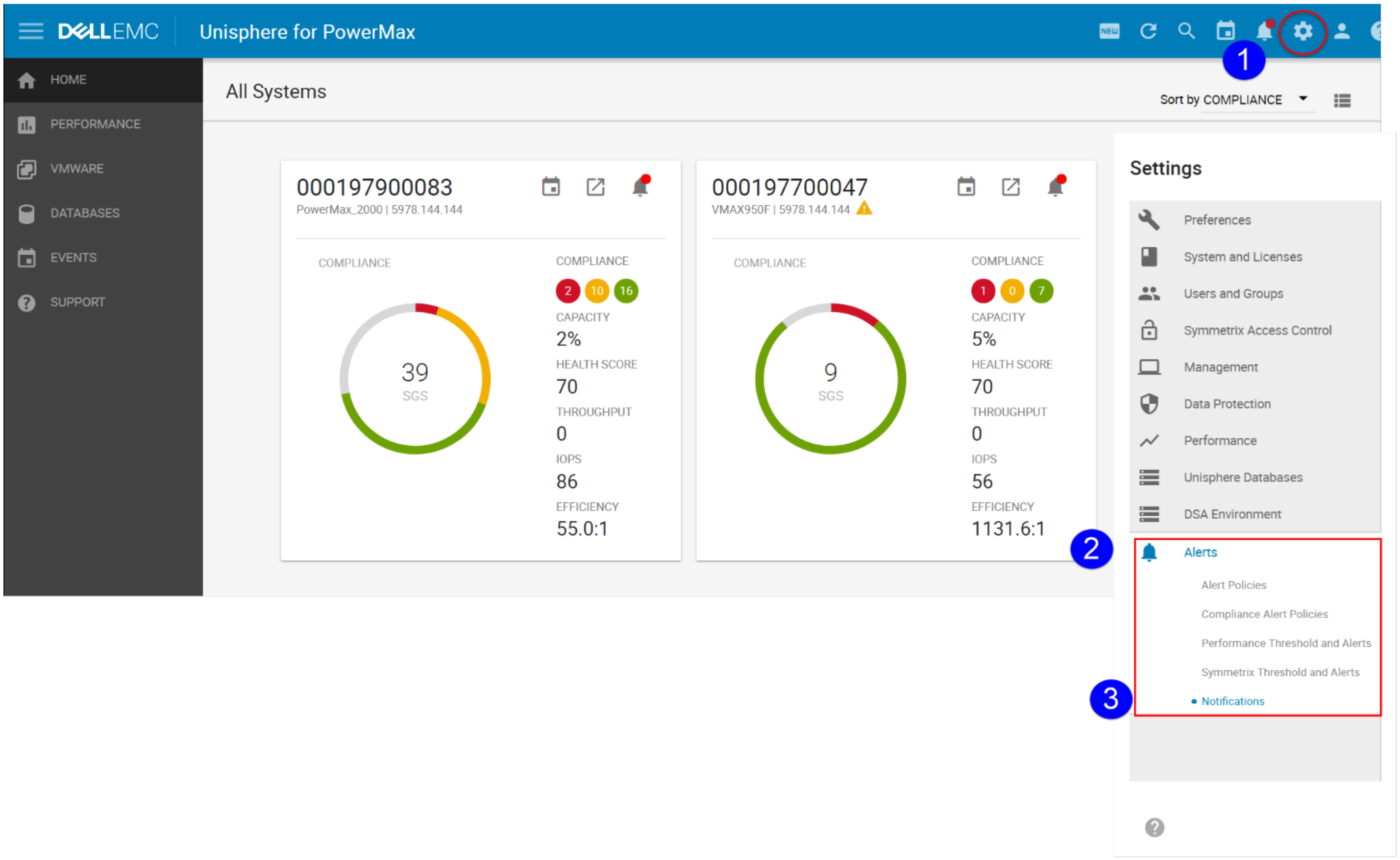
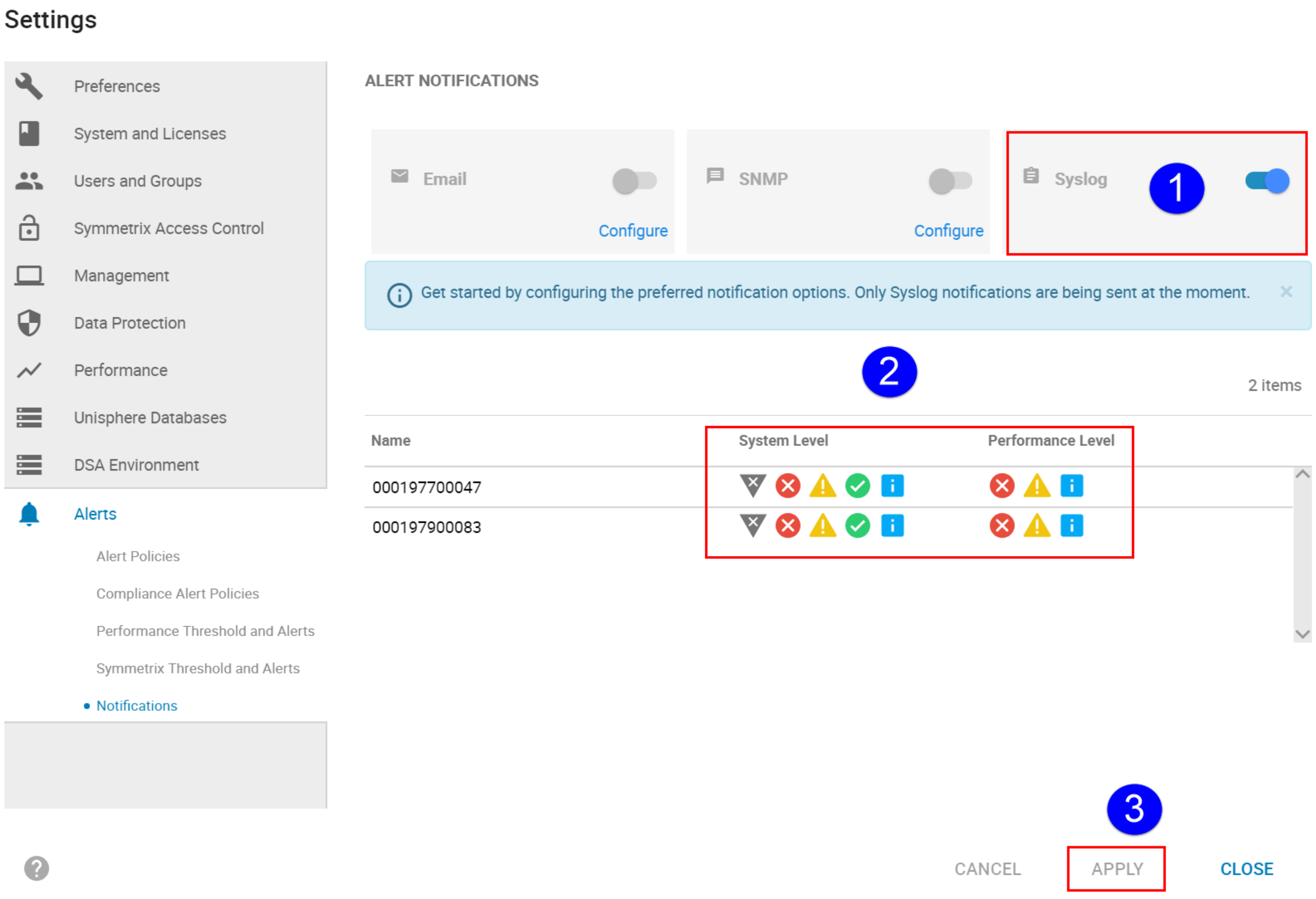


Figure 14. Alert Settings in Unisphere for PowerMax 9.x

Once in the Notifications screen, the user can select the manner in which they wish to be notified, if at all, of events.

First, select “Enable” next to Syslog. 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 step two click on the desired levels which turns on the color of the icon. There are two types of alerts: 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. Once complete, select “Save” in step 3. These steps are shown in Figure 15.


Settings

- Preferences
- System and Licenses
- Users and Groups
- Symmetrix Access Control
- Management
- Data Protection
- Performance
- Unisphere Databases
- DSA Environment
- Alerts
  - Alert Policies
  - Compliance Alert Policies
  - Performance Threshold and Alerts
  - Symmetrix Threshold and Alerts
  - Notifications

ALERT NOTIFICATIONS

Email ○ Configure

SNMP ○ Configure

Syslog ● 1

Get started by configuring the preferred notification options. Only Syslog notifications are being sent at the moment.

2

2 items

Name	System Level	Performance Level
000197700047	▼ ⊗ ⚠ ✓ ℹ	⊗ ⚠ ℹ
000197900083	▼ ⊗ ⚠ ✓ ℹ	⊗ ⚠ ℹ

3

CANCEL APPLY CLOSE

Figure 15. Setting notification type and alert levels in Unisphere for PowerMax 9.x

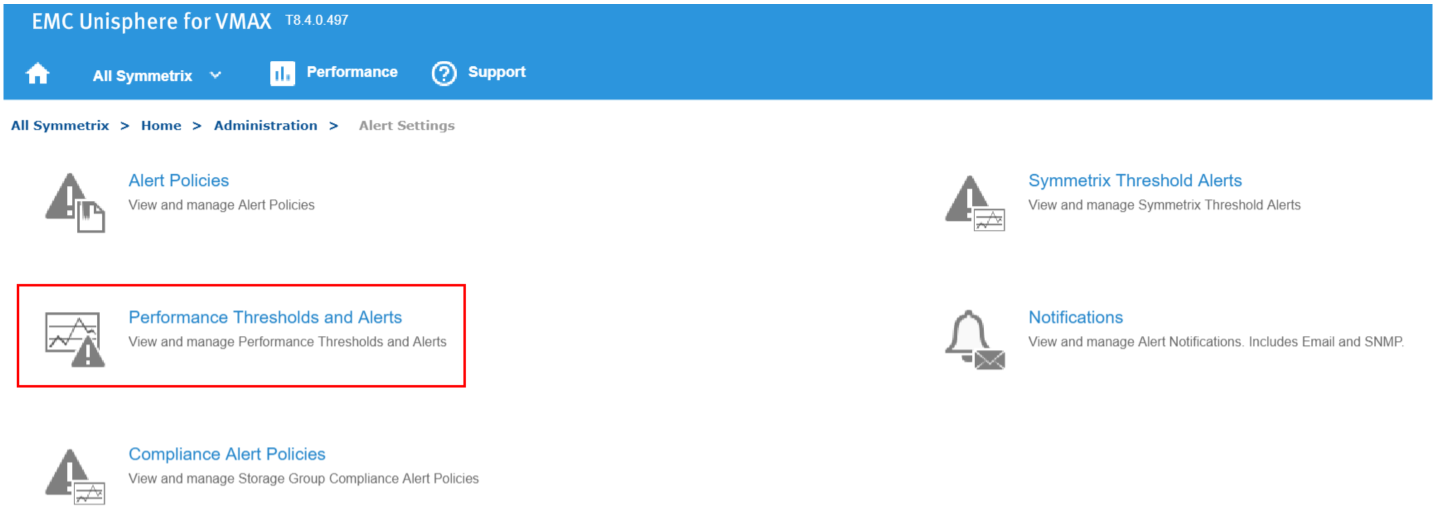
Setting up the events for syslog allows the default alerts to be sent when thresholds are exceeded; however, customers may wish to customize the thresholds at which those events are generated. These can be adjusted in the Alert Settings page under the following categories: Alert Policies (array level)[1], 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.

[1] Note that array level events in Alert Policies must have the notification setup as syslog to receive these alerts in Operations for Logs.

Start by navigating to the previously shown Administration page, and then select Performance Thresholds and Alerts as in Figure 16 or Figure 17 depending on the Unisphere version.


EMC Unisphere for VMAX T8.4.0.497
All Symmetrix
Performance
Support
All Symmetrix > Home > Administration > Alert Settings

Alert Policies
View and manage Alert Policies

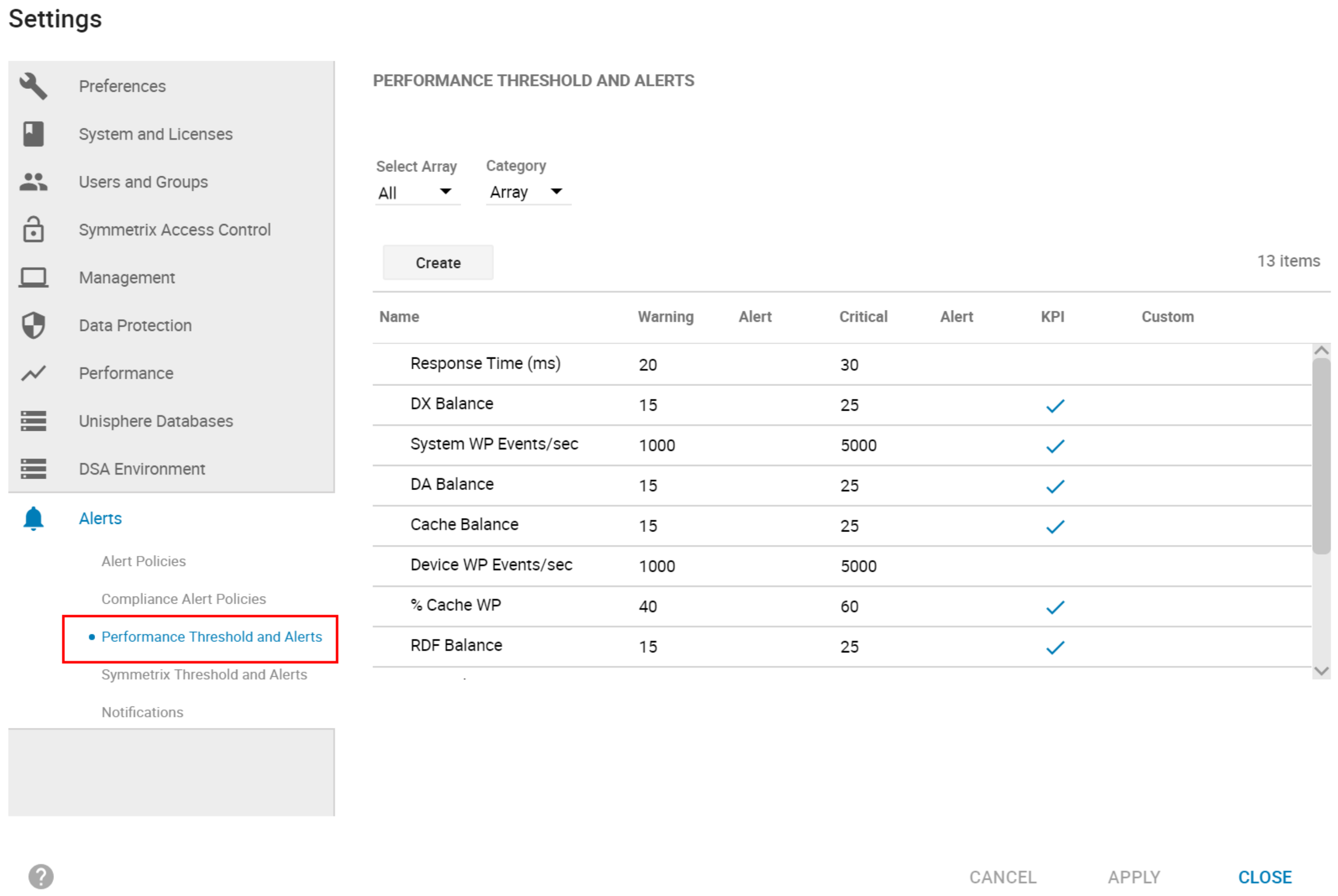
Symmetrix Threshold Alerts
View and manage Symmetrix Threshold Alerts

Performance Thresholds and Alerts
View and manage Performance Thresholds and Alerts

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

Compliance Alert Policies
View and manage Storage Group Compliance Alert Policies

Figure 16. Performance Thresholds and Alerts Unisphere for VMAX 8.x



PERFORMANCE THRESHOLD AND ALERTS

Select Array: All

Category: Array

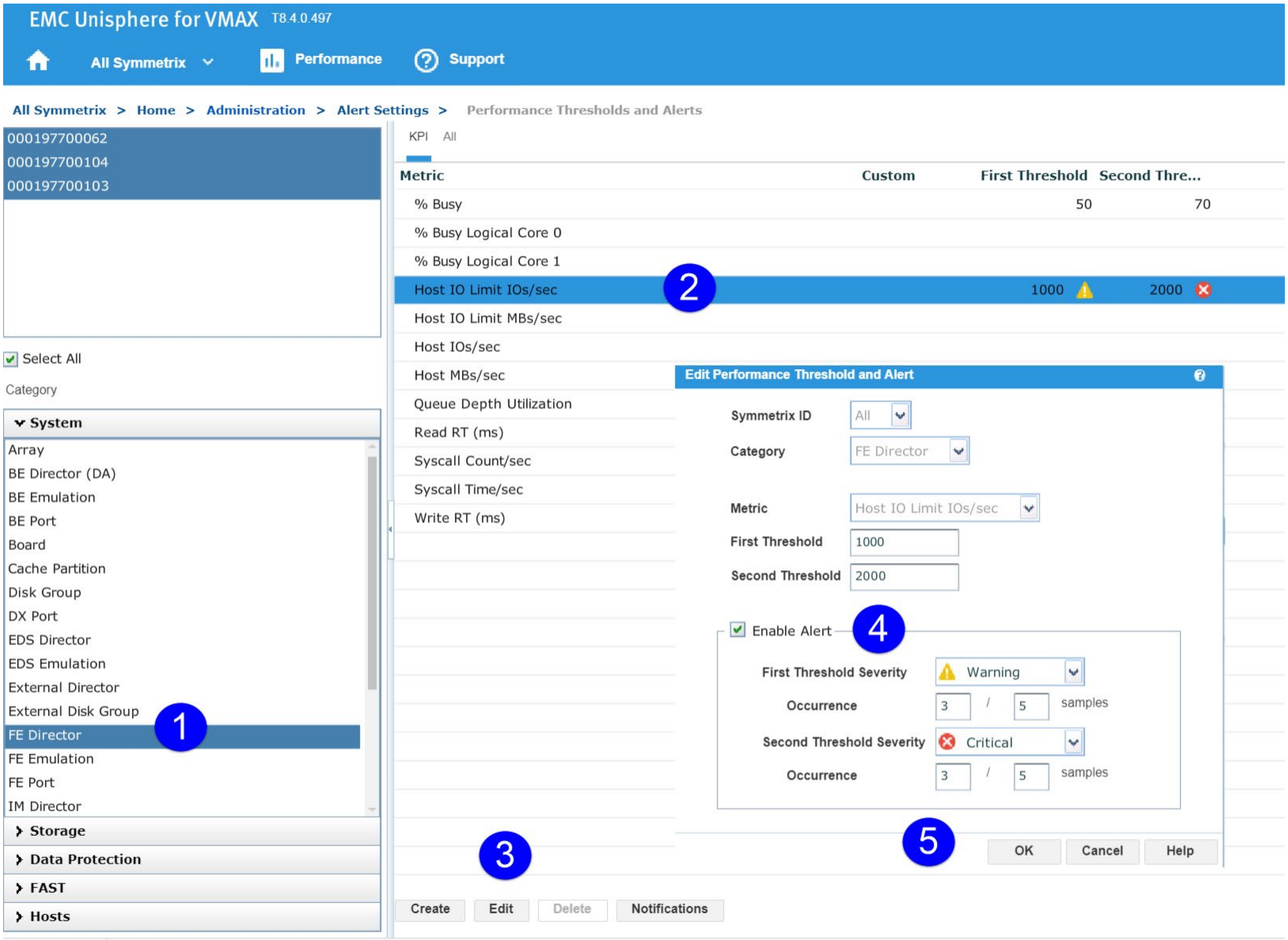
Create

13 items

Name	Warning	Alert	Critical	Alert	KPI	Custom
Response Time (ms)	20		30			
DX Balance	15		25		✓	
System WP Events/sec	1000		5000		✓	
DA Balance	15		25		✓	
Cache Balance	15		25		✓	
Device WP Events/sec	1000		5000			
% Cache WP	40		60		✓	
RDF Balance	15		25		✓	

Figure 17. Performance Thresholds and Alerts Unisphere for PowerMax 9.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 18 walk the user through setting a custom alert on the metric Host IO/sec for an FE Director for Unisphere for VMAX (the procedure is similar in Unisphere for PowerMax). 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.



All Symmetrix > Home > Administration > Alert Settings > Performance Thresholds and Alerts

000197700062
000197700104
000197700103

☑ Select All

Category

System

Array
BE Director (DA)
BE Emulation
BE Port
Board
Cache Partition
Disk Group
DX Port
EDS Director
EDS Emulation
External Director
External Disk Group
FE Director
FE Emulation
FE Port
IM Director

Storage

Data Protection

FAST

Hosts

KPI All

Metric	Custom	First Threshold	Second Thre...
% Busy		50	70
% Busy Logical Core 0			
% Busy Logical Core 1			
Host IO Limit IOs/sec		1000 ⚠	2000 ☒
Host IO Limit MBs/sec			
Host IOs/sec			
Host MBs/sec			
Queue Depth Utilization			
Read RT (ms)			
Syscall Count/sec			
Syscall Time/sec			
Write RT (ms)			

Edit Performance Threshold and Alert

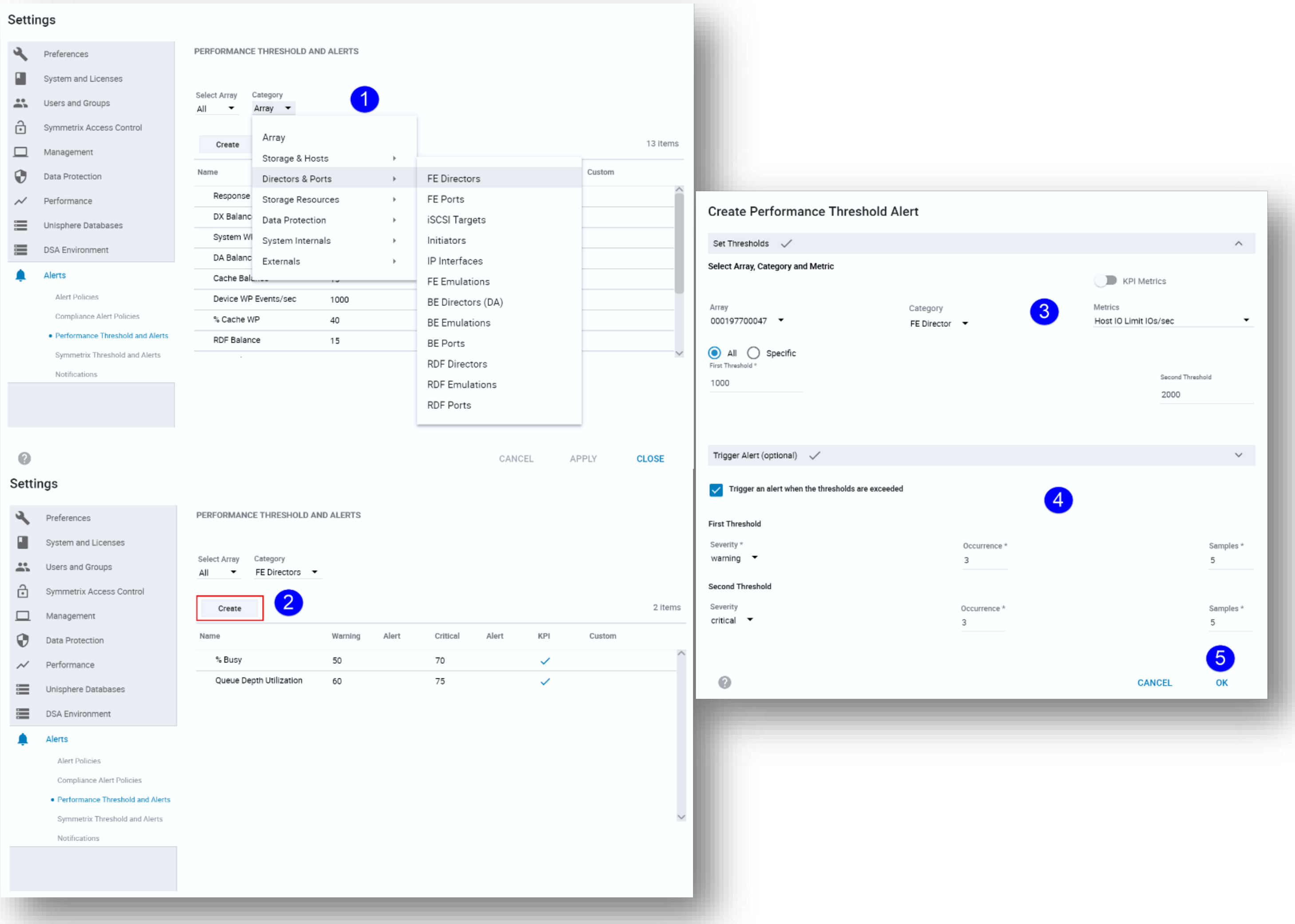
Symmetrix ID: All
Category: FE Director
Metric: Host IO Limit IOs/sec
First Threshold: 1000
Second Threshold: 2000

☑ Enable Alert

First Threshold Severity: ⚠ Warning
Occurrence: 3 / 5 samples
Second Threshold Severity: ☒ Critical
Occurrence: 3 / 5 samples

Figure 18. Setting a custom alert in Unisphere for VMAX 8.x

For Unisphere for PowerMax, it is necessary to create the alert, not simply activate it. The steps are demonstrated in Figure 19.



Select Array: All
Category: Array

Name		Custom
Response		
DX Balanc		
System W		
DA Balanc		
Cache Bal		
Device WP Events/sec	1000	
% Cache WP	40	
RDF Balance	15	

Select Array: All
Category: FE Directors

Name	Warning	Alert	Critical	Alert	KPI	Custom
% Busy	50		70		✓	
Queue Depth Utilization	60		75		✓	

Array: 000197700047
Category: FE Director
Metrics: Host IO Limit IOs/sec

● All ○ Specific

First Threshold *: 1000
Second Threshold: 2000

☑ Trigger an alert when the thresholds are exceeded

First Threshold
Severity *: warning
Occurrence *: 3
Samples *: 5

Second Threshold
Severity: critical
Occurrence *: 3
Samples *: 5

Figure 19. Setting a custom alert in Unisphere for PowerMax 9.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/PowerMax documentation on support.dell.com more detailed information on setting alerts.

Embedded NAS (eNAS)

If eNAS is implemented on the VMAX or PowerMax, a separate setup must be done to send log information to Operations for Logs. Complete the following steps:

1. Log into the Control Station as ***nasadmin*** and then *su* to ***root***.

2. Add an entry to the bottom of /etc/hosts with the IP and hostname of the Operations for Logs environment:

   ```
   ……
   # VMware Operations for Logs
   10.108.100.3 dsib1003.lss.emc.com dsib1003
   ```

3. Modify the /etc/syslog.conf file and add the following entry at the bottom with the short name of the host entered in the /etc/hosts file:

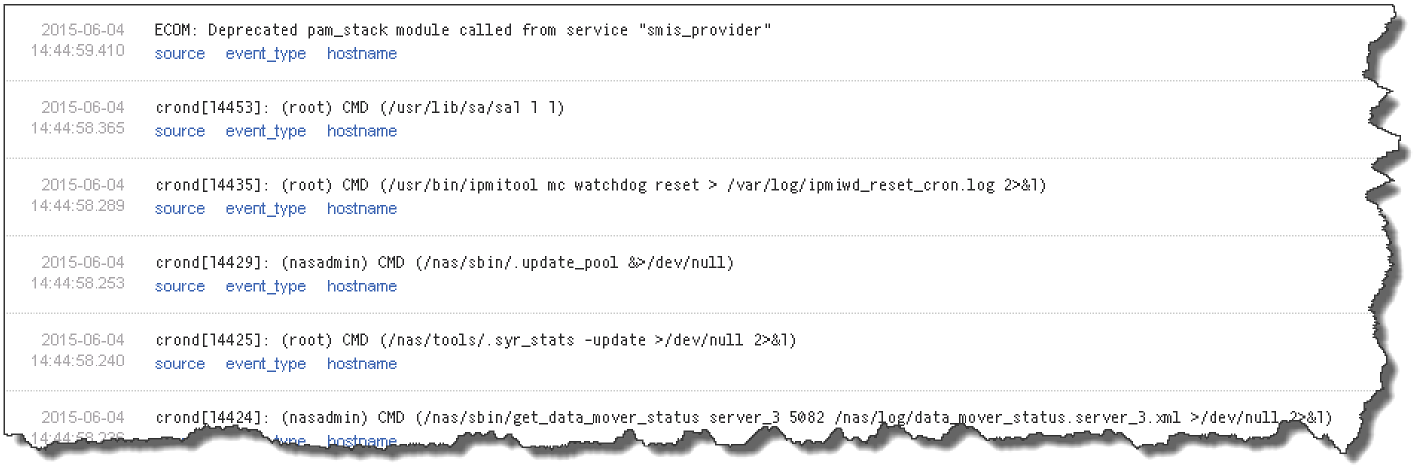
   ```
   ……
   # Entry for VMware Operations for Logs
   *.* @dsib1003
   ```

4. Restart the syslog service to complete the setup:

   ```
   /sbin/service syslog restart
   ```

Once complete, log information will be forwarded to the Operations for Logs instance automatically.

Note that there are no user-defined fields for eNAS as the content of the log information does not lend itself well to extraction. Figure 20 contains a number of sample entries from an eNAS environment.

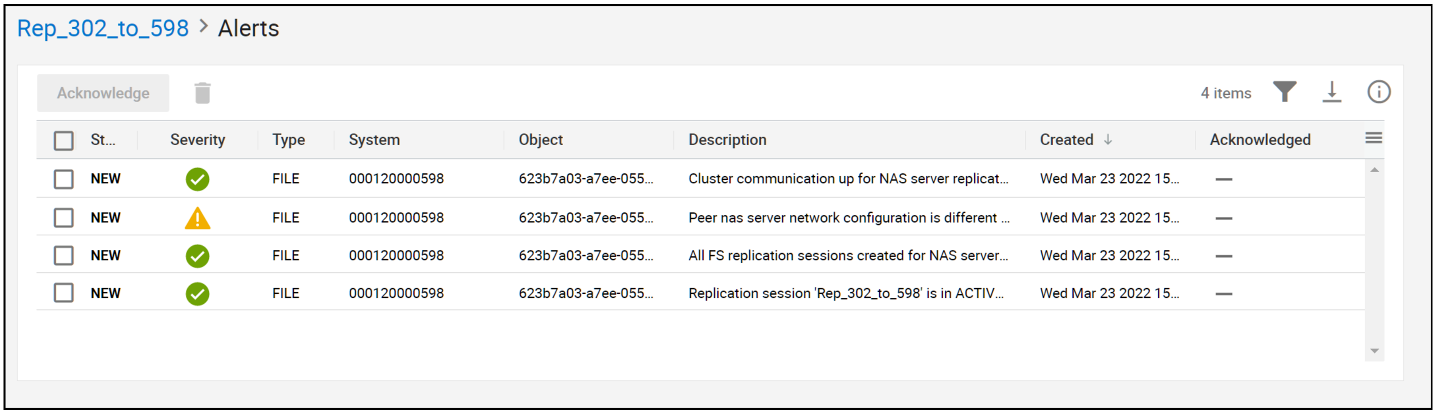


```
  2015-06-04   ECOM: Deprecated pam_stack module called from service "smis_provider"
14:44:59.410   source   event_type   hostname

  2015-06-04   crond[14453]: (root) CMD (/usr/lib/sa/sa1 1 1)
14:44:58.365   source   event_type   hostname

  2015-06-04   crond[14435]: (root) CMD (/usr/bin/ipmitool mc watchdog reset > /var/log/ipmiwd_reset_cron.log 2>&1)
14:44:58.289   source   event_type   hostname

  2015-06-04   crond[14429]: (nasadmin) CMD (/nas/sbin/.update_pool &>/dev/null)
14:44:58.253   source   event_type   hostname

  2015-06-04   crond[14425]: (root) CMD (/nas/tools/.syr_stats -update >/dev/null 2>&1)
14:44:58.240   source   event_type   hostname

  2015-06-04   crond[14424]: (nasadmin) CMD (/nas/sbin/get_data_mover_status server_3 5082 /nas/log/data_mover_status.server_3.xml >/dev/null 2>&1)
14:44:58.236   source   event_type   hostname
```

Figure 20. Log entries generated by eNAS

File

On PowerMaxOS 10, a new implementation of network storage is available called File. File offers new capabilities that were not available with eNAS and is more integrated into the PowerMax array. Therefore, a separate configuration is unnecessary; however, File alerts are only available on embedded management so if using network storage, the embedded Unisphere should be used. An example of these alerts are shown in Figure 21.



Rep_302_to_598 > Alerts

□	St...	Severity	Type	System	Object	Description	Created ↓	Acknowledged
□	NEW	✓	FILE	000120000598	623b7a03-a7ee-055...	Cluster communication up for NAS server replicat...	Wed Mar 23 2022 15...	—
□	NEW	⚠	FILE	000120000598	623b7a03-a7ee-055...	Peer nas server network configuration is different ...	Wed Mar 23 2022 15...	—
□	NEW	✓	FILE	000120000598	623b7a03-a7ee-055...	All FS replication sessions created for NAS server...	Wed Mar 23 2022 15...	—
□	NEW	✓	FILE	000120000598	623b7a03-a7ee-055...	Replication session 'Rep_302_to_598' is in ACTIV...	Wed Mar 23 2022 15...	—

Figure 21. File alerts

Using the Dell PowerMax 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 PowerMax content pack to isolate an issue around FE I/O. Note that various versions of Operations for Logs images are used in this example.

The Problems Dashboard has been designed to make the detailed analysis in this section less necessary as it attempts to show the most common issue areas.

Finding high IO to the FE directors

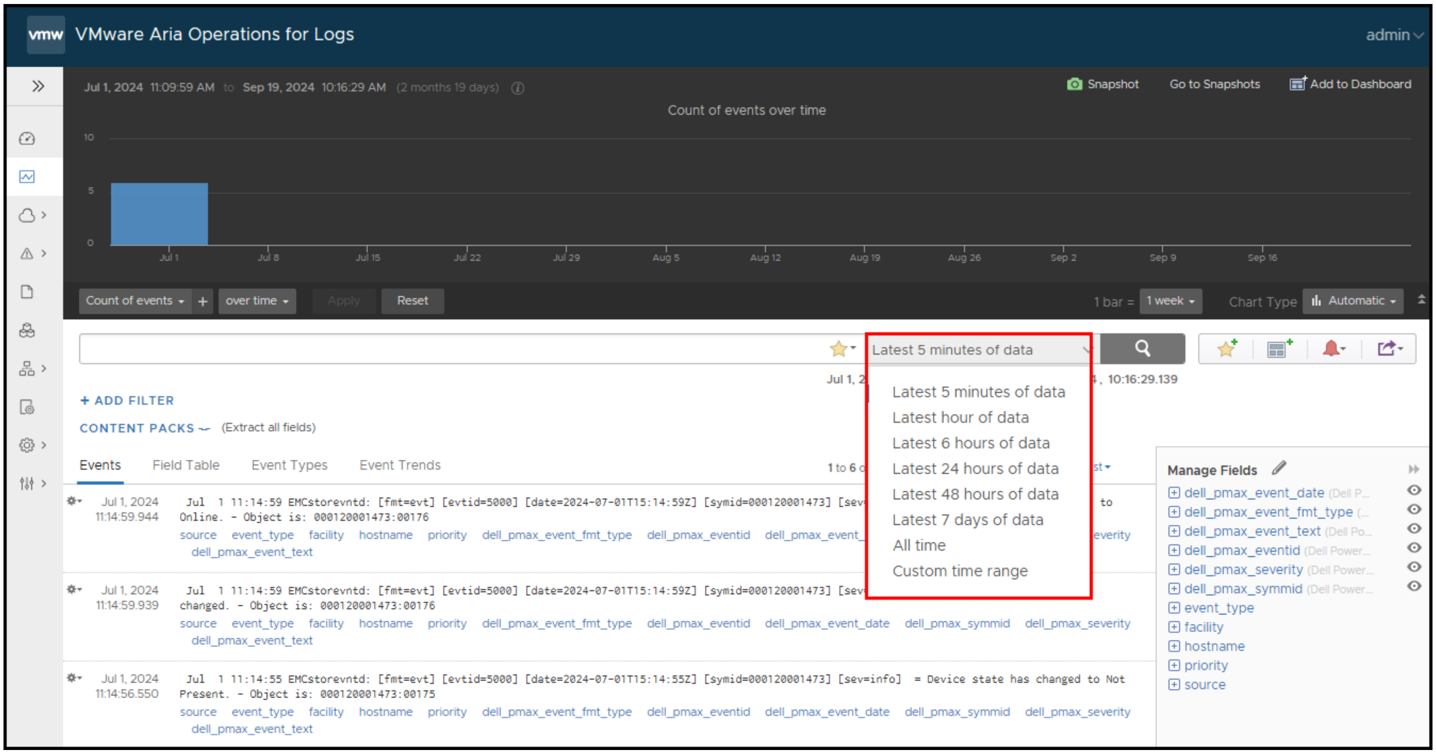
The system administrator (Sysadmin) has noticed that the front-end directors on the PowerMax array that are utilized in the VMware environment have had some heavy activity lately.[2] The Sysadmin asks the VMware administrator (VMAdmin) to determine if there have been any occurrences when an FE director has serviced more than 2500 IOs in the last week. This may indicate that more FE director ports need to be added to the port group.

To investigate, the VMAdmin turns to Operations for Logs which he has previously configured to accept log files from Solutions Enabler and Unisphere for PowerMax. He also has implemented the PowerMax content pack to help make the analysis easier. Within Unisphere for PowerMax he has previously defined two thresholds for FE ports. When IOs reach 1000, a

[2] The IO numbers used in the alert in Unisphere for PowerMax were set low to facilitate triggering in the lab and are not considered "heavy activity" indicating the need for more FE ports. The numbers are arbitrary and simply help elucidate the example.

warning severity will be issued and then if IOs surpass 2000 a critical severity will be issued. Therefore, he can expect two log entries for any FE director servicing more than 2500 IOs since they would breach both these thresholds.

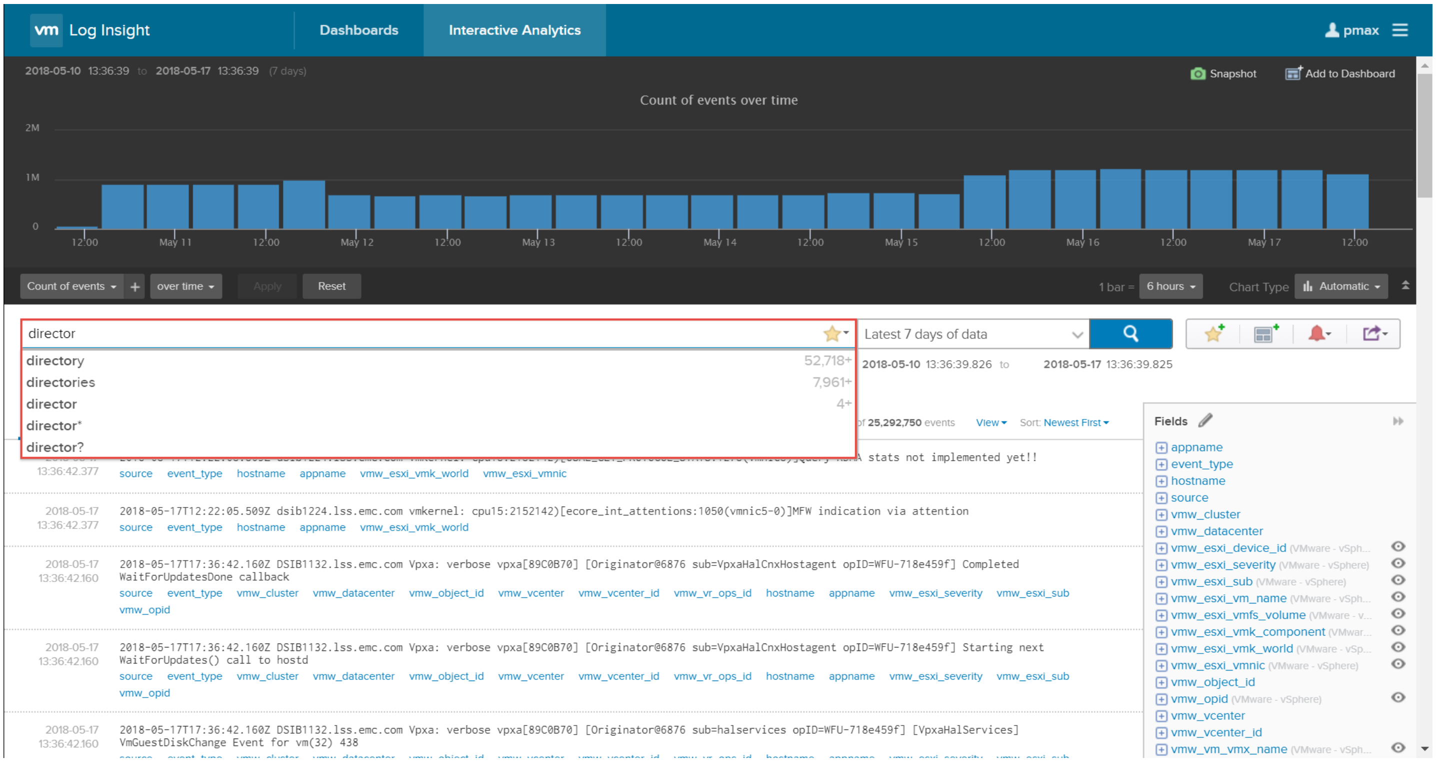
He starts by opening the Interactive Analytics page, seen in Figure 22, which will allow him to make queries into the log files collected.



```
Jul 1, 2024    Jul  1 11:14:59 EMCstorevntd: [fmt=evt] [evtid=5000] [date=2024-07-01T15:14:59Z] [symid=000120001473] [sev
11:14:59.944   Online. - Object is: 000120001473:00176
               source  event_type  facility  hostname  priority  dell_pmax_event_fmt_type  dell_pmax_eventid  dell_pmax_event_
                 dell_pmax_event_text

Jul 1, 2024    Jul  1 11:14:59 EMCstorevntd: [fmt=evt] [evtid=5000] [date=2024-07-01T15:14:59Z] [symid=000120001473] [sev
11:14:59.939   changed. - Object is: 000120001473:00176
               source  event_type  facility  hostname  priority  dell_pmax_event_fmt_type  dell_pmax_eventid  dell_pmax_event_date  dell_pmax_symmid  dell_pmax_severity
                 dell_pmax_event_text

Jul 1, 2024    Jul  1 11:14:55 EMCstorevntd: [fmt=evt] [evtid=5000] [date=2024-07-01T15:14:55Z] [symid=000120001473] [sev=info]  = Device state has changed to Not
11:14:56.550   Present. - Object is: 000120001473:00175
               source  event_type  facility  hostname  priority  dell_pmax_event_fmt_type  dell_pmax_eventid  dell_pmax_event_date  dell_pmax_symmid  dell_pmax_severity
                 dell_pmax_event_text
```

Figure 22. VMware Aria Operations for Logs Interactive Analytics

The first thing he does is to change the Time Range (highlighted in the red box above) to "Latest 7 days of data" to be sure he traverses all the log files for the week. Then he starts with a simple query against the term "director". As he begins typing in the term, Operations for Logs automatically generates options from which to choose. In Figure 23 one can see the first term presented is "director" and that there will be at least 4 entries for that term. He selects that and hits "Search".



director

directory	52,718+
directories	7,961+
director	4+
director*	
director?	

2018-05-10 13:36:39.826 to 2018-05-17 13:36:39.825

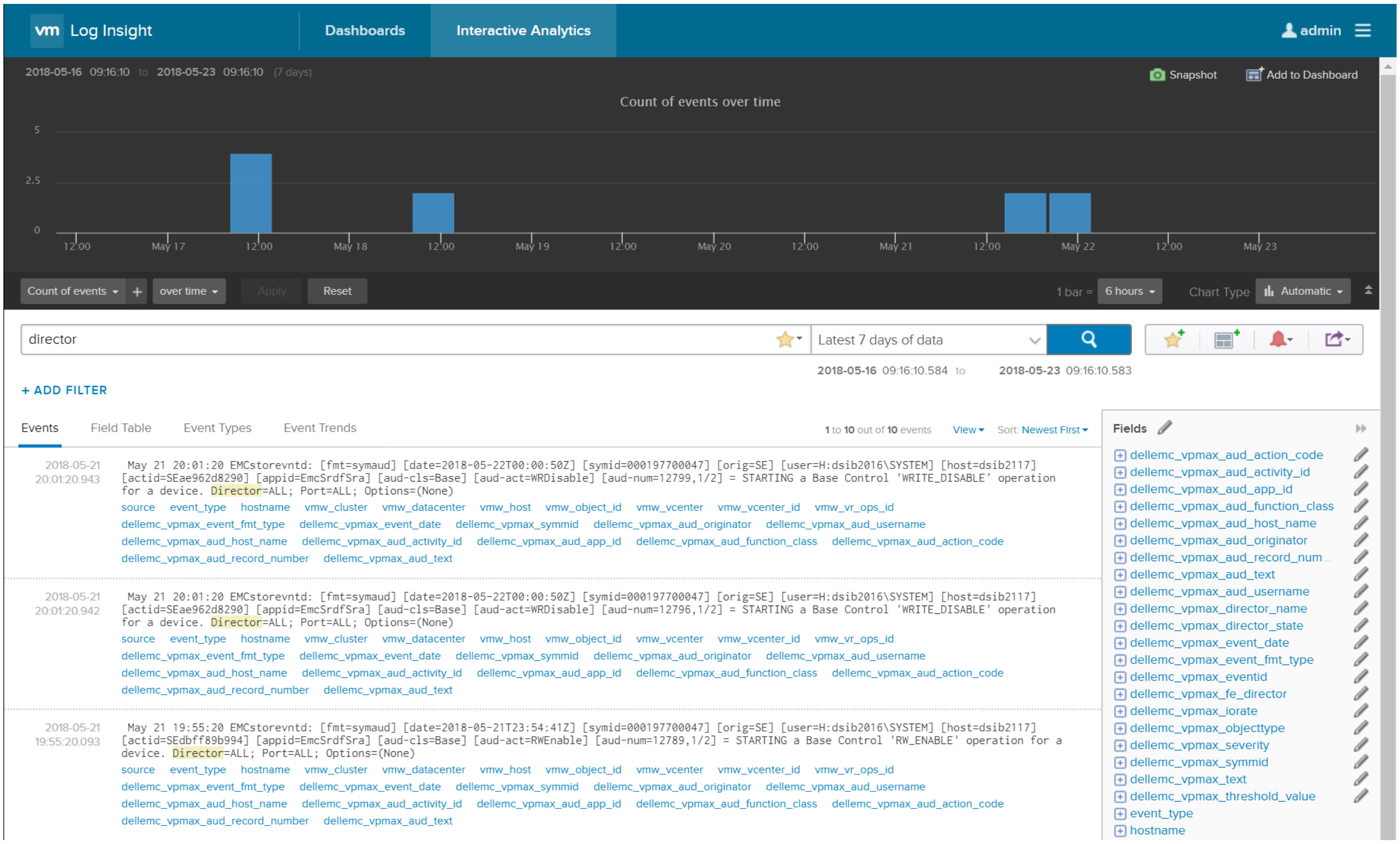
of 25,292,750 events

```
13:36:42.377   stats not implemented yet!!
               source  event_type  hostname  appname  vmw_esxi_vmk_world  vmw_esxi_vmnic

2018-05-17     2018-05-17T12:22:05.509Z dsib1224.lss.emc.com vmkernel: cpu15:2152142)[ecore_int_attentions:1050(vmnic5-0)]MFW indication via attention
13:36:42.377   source  event_type  hostname  appname  vmw_esxi_vmk_world

2018-05-17     2018-05-17T17:36:42.160Z DSIB1132.lss.emc.com Vpxa: verbose vpxa[89C0B70] [Originator@6876 sub=VpxaHalCnxHostagent opID=WFU-718e459f] Completed
13:36:42.160   WaitForUpdatesDone callback
               source  event_type  vmw_cluster  vmw_datacenter  vmw_object_id  vmw_vcenter  vmw_vcenter_id  vmw_vr_ops_id  hostname  appname  vmw_esxi_severity  vmw_esxi_sub
               vmw_opid

2018-05-17     2018-05-17T17:36:42.160Z DSIB1132.lss.emc.com Vpxa: verbose vpxa[89C0B70] [Originator@6876 sub=VpxaHalCnxHostagent opID=WFU-718e459f] Starting next
13:36:42.160   WaitForUpdates() call to hostd
               source  event_type  vmw_cluster  vmw_datacenter  vmw_object_id  vmw_vcenter  vmw_vcenter_id  vmw_vr_ops_id  hostname  appname  vmw_esxi_severity  vmw_esxi_sub
               vmw_opid

2018-05-17     2018-05-17T17:36:42.160Z DSIB1132.lss.emc.com Vpxa: verbose vpxa[89C0B70] [Originator@6876 sub=halservices opID=WFU-718e459f] [VpxaHalServices]
13:36:42.160   VmGuestDiskChange Event for vm(32) 438
```

- appname
- event_type
- hostname
- source
- vmw_cluster
- vmw_datacenter
- vmw_esxi_device_id (VMware - vSph...
- vmw_esxi_severity (VMware - vSphere)
- vmw_esxi_sub (VMware - vSphere)
- vmw_esxi_vm_name (VMware - vSph...
- vmw_esxi_vmfs_volume (VMware - v...
- vmw_esxi_vmk_component (VMwar...
- vmw_esxi_vmk_world (VMware - vSp...
- vmw_esxi_vmnic (VMware - vSphere)
- vmw_object_id
- vmw_opid (VMware - vSphere)
- vmw_vcenter
- vmw_vcenter_id
- vmw_vm_vmx_name (VMware - vSph...

Figure 23. Director term search in Operations for Logs

The result of the query is displayed in Figure 24.



```
2018-05-21     May 21 20:01:20 EMCstorevntd: [fmt=symaud] [date=2018-05-22T00:00:50Z] [symid=000197700047] [orig=SE] [user=H:dsib2016\SYSTEM] [host=dsib2117]
20:01:20.943  [actid=SEae962d8290] [appid=EmcSrdfSra] [aud-cls=Base] [aud-act=WRDisable] [aud-num=12799,1/2] = STARTING a Base Control 'WRITE_DISABLE' operation
              for a device. Director=ALL; Port=ALL; Options=(None)
```

source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id dellemc_vpmax_event_fmt_type dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_aud_originator dellemc_vpmax_aud_username dellemc_vpmax_aud_host_name dellemc_vpmax_aud_activity_id dellemc_vpmax_aud_app_id dellemc_vpmax_aud_function_class dellemc_vpmax_aud_action_code dellemc_vpmax_aud_record_number dellemc_vpmax_aud_text

```
2018-05-21     May 21 20:01:20 EMCstorevntd: [fmt=symaud] [date=2018-05-22T00:00:50Z] [symid=000197700047] [orig=SE] [user=H:dsib2016\SYSTEM] [host=dsib2117]
20:01:20.942  [actid=SEae962d8290] [appid=EmcSrdfSra] [aud-cls=Base] [aud-act=WRDisable] [aud-num=12796,1/2] = STARTING a Base Control 'WRITE_DISABLE' operation
              for a device. Director=ALL; Port=ALL; Options=(None)
```

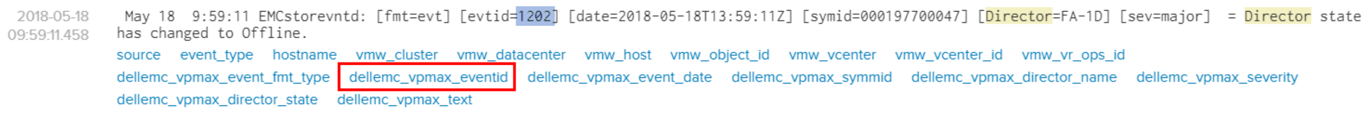
source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id dellemc_vpmax_event_fmt_type dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_aud_originator dellemc_vpmax_aud_username dellemc_vpmax_aud_host_name dellemc_vpmax_aud_activity_id dellemc_vpmax_aud_app_id dellemc_vpmax_aud_function_class dellemc_vpmax_aud_action_code dellemc_vpmax_aud_record_number dellemc_vpmax_aud_text

```
2018-05-21     May 21 19:55:20 EMCstorevntd: [fmt=symaud] [date=2018-05-21T23:54:41Z] [symid=000197700047] [orig=SE] [user=H:dsib2016\SYSTEM] [host=dsib2117]
19:55:20.093  [actid=SEdbff89b994] [appid=EmcSrdfSra] [aud-cls=Base] [aud-act=RWEnable] [aud-num=12789,1/2] = STARTING a Base Control 'RW_ENABLE' operation for a
              device. Director=ALL; Port=ALL; Options=(None)
```

source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id dellemc_vpmax_event_fmt_type dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_aud_originator dellemc_vpmax_aud_username dellemc_vpmax_aud_host_name dellemc_vpmax_aud_activity_id dellemc_vpmax_aud_app_id dellemc_vpmax_aud_function_class dellemc_vpmax_aud_action_code dellemc_vpmax_aud_record_number dellemc_vpmax_aud_text

Figure 24. FE Director entries

Now that he has the director entries, he needs to filter those events further. As auditing is being used, he decides to filter by the event ID as audit records do not have this field. He examines one of the log entries to see what pre-defined fields might assist him. One field that would satisfy the requirement is "dell_pmax_eventid". By putting the cursor over this field, the eventid is highlighted in blue in the entry as in Figure 25.

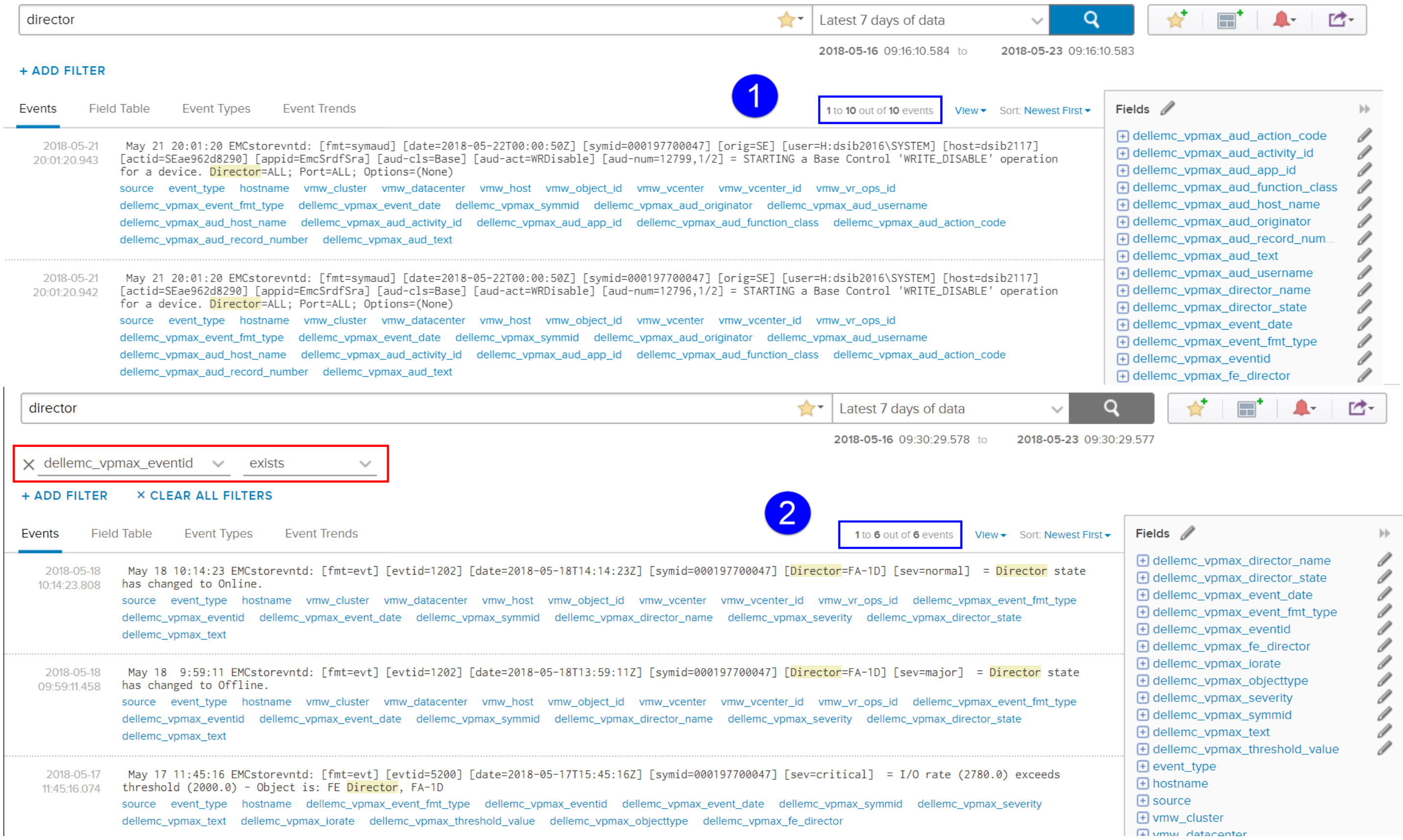


```
2018-05-18     May 18  9:59:11 EMCstorevntd: [fmt=evt] [evtid=1202] [date=2018-05-18T13:59:11Z] [symid=000197700047] [Director=FA-1D] [sev=major]  = Director state
09:59:11.458  has changed to Offline.
```

source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id dellemc_vpmax_event_fmt_type dellemc_vpmax_eventid dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_director_name dellemc_vpmax_severity dellemc_vpmax_director_state dellemc_vpmax_text

Figure 25. dell_pmax_eventid field

He clicks on the "dell_pmax_eventid" field and it is automatically added as a constraint to his query, ensuring only non-auditing director events are shown. He hits Search again and now the entries are reduced from 10 to 6, seen in Figure 26.


director
Latest 7 days of data
2018-05-16 09:16:10.584 to 2018-05-23 09:16:10.583
+ ADD FILTER
Events
Field Table
Event Types
Event Trends
1
1 to 10 out of 10 events
View
Sort: Newest First
Fields
dellemc_vpmax_aud_action_code
dellemc_vpmax_aud_activity_id
dellemc_vpmax_aud_app_id
dellemc_vpmax_aud_function_class
dellemc_vpmax_aud_host_name
dellemc_vpmax_aud_originator
dellemc_vpmax_aud_record_num...
dellemc_vpmax_aud_text
dellemc_vpmax_aud_username
dellemc_vpmax_director_name
dellemc_vpmax_director_state
dellemc_vpmax_event_date
dellemc_vpmax_event_fmt_type
dellemc_vpmax_eventid
dellemc_vpmax_fe_director

```
2018-05-21     May 21 20:01:20 EMCstorevntd: [fmt=symaud] [date=2018-05-22T00:00:50Z] [symid=000197700047] [orig=SE] [user=H:dsib2016\SYSTEM] [host=dsib2117]
20:01:20.943   [actid=SEae962d8290] [appid=EmcSrdfSra] [aud-cls=Base] [aud-act=WRDisable] [aud-num=12799,1/2] = STARTING a Base Control 'WRITE_DISABLE' operation
               for a device. Director=ALL; Port=ALL; Options=(None)
```

source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id
dellemc_vpmax_event_fmt_type dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_aud_originator dellemc_vpmax_aud_username
dellemc_vpmax_aud_host_name dellemc_vpmax_aud_activity_id dellemc_vpmax_aud_app_id dellemc_vpmax_aud_function_class dellemc_vpmax_aud_action_code
dellemc_vpmax_aud_record_number dellemc_vpmax_aud_text

```
2018-05-21     May 21 20:01:20 EMCstorevntd: [fmt=symaud] [date=2018-05-22T00:00:50Z] [symid=000197700047] [orig=SE] [user=H:dsib2016\SYSTEM] [host=dsib2117]
20:01:20.942   [actid=SEae962d8290] [appid=EmcSrdfSra] [aud-cls=Base] [aud-act=WRDisable] [aud-num=12796,1/2] = STARTING a Base Control 'WRITE_DISABLE' operation
               for a device. Director=ALL; Port=ALL; Options=(None)
```

source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id
dellemc_vpmax_event_fmt_type dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_aud_originator dellemc_vpmax_aud_username
dellemc_vpmax_aud_host_name dellemc_vpmax_aud_activity_id dellemc_vpmax_aud_app_id dellemc_vpmax_aud_function_class dellemc_vpmax_aud_action_code
dellemc_vpmax_aud_record_number dellemc_vpmax_aud_text

```
2018-05-18     May 18 10:14:23 EMCstorevntd: [fmt=evt] [evtid=1202] [date=2018-05-18T14:14:23Z] [symid=000197700047] [Director=FA-1D] [sev=normal]  = Director state
10:14:23.808   has changed to Online.
```

source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id dellemc_vpmax_event_fmt_type
dellemc_vpmax_eventid dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_director_name dellemc_vpmax_severity dellemc_vpmax_director_state
dellemc_vpmax_text

```
2018-05-18     May 18  9:59:11 EMCstorevntd: [fmt=evt] [evtid=1202] [date=2018-05-18T13:59:11Z] [symid=000197700047] [Director=FA-1D] [sev=major]  = Director state
09:59:11.458   has changed to Offline.
```

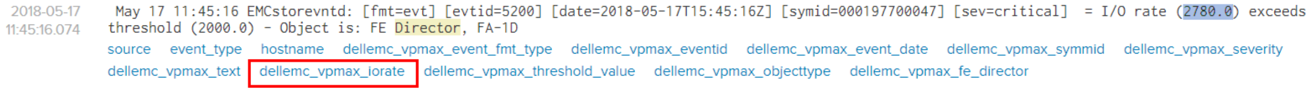
source event_type hostname vmw_cluster vmw_datacenter vmw_host vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id dellemc_vpmax_event_fmt_type
dellemc_vpmax_eventid dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_director_name dellemc_vpmax_severity dellemc_vpmax_director_state
dellemc_vpmax_text

```
2018-05-17     May 17 11:45:16 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=critical]  = I/O rate (2780.0) exceeds
11:45:16.074   threshold (2000.0) - Object is: FE Director, FA-1D
```

source event_type hostname dellemc_vpmax_event_fmt_type dellemc_vpmax_eventid dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_severity
dellemc_vpmax_text dellemc_vpmax_iorate dellemc_vpmax_threshold_value dellemc_vpmax_objecttype dellemc_vpmax_fe_director

Figure 26. Adding a constraint to a query

The VMAdmin sees that a further constraint would be helpful to isolate the desired events. By looking at the first entry he can see an example of what an IO rate event will show. In that entry, in parentheses, is the exact value of the IO that exceeded the threshold. Again, he reviews the available defined fields and finds “dell_pmax_iorate” in Figure 27. Running the cursor over that reveals it is associated with the value in parentheses.

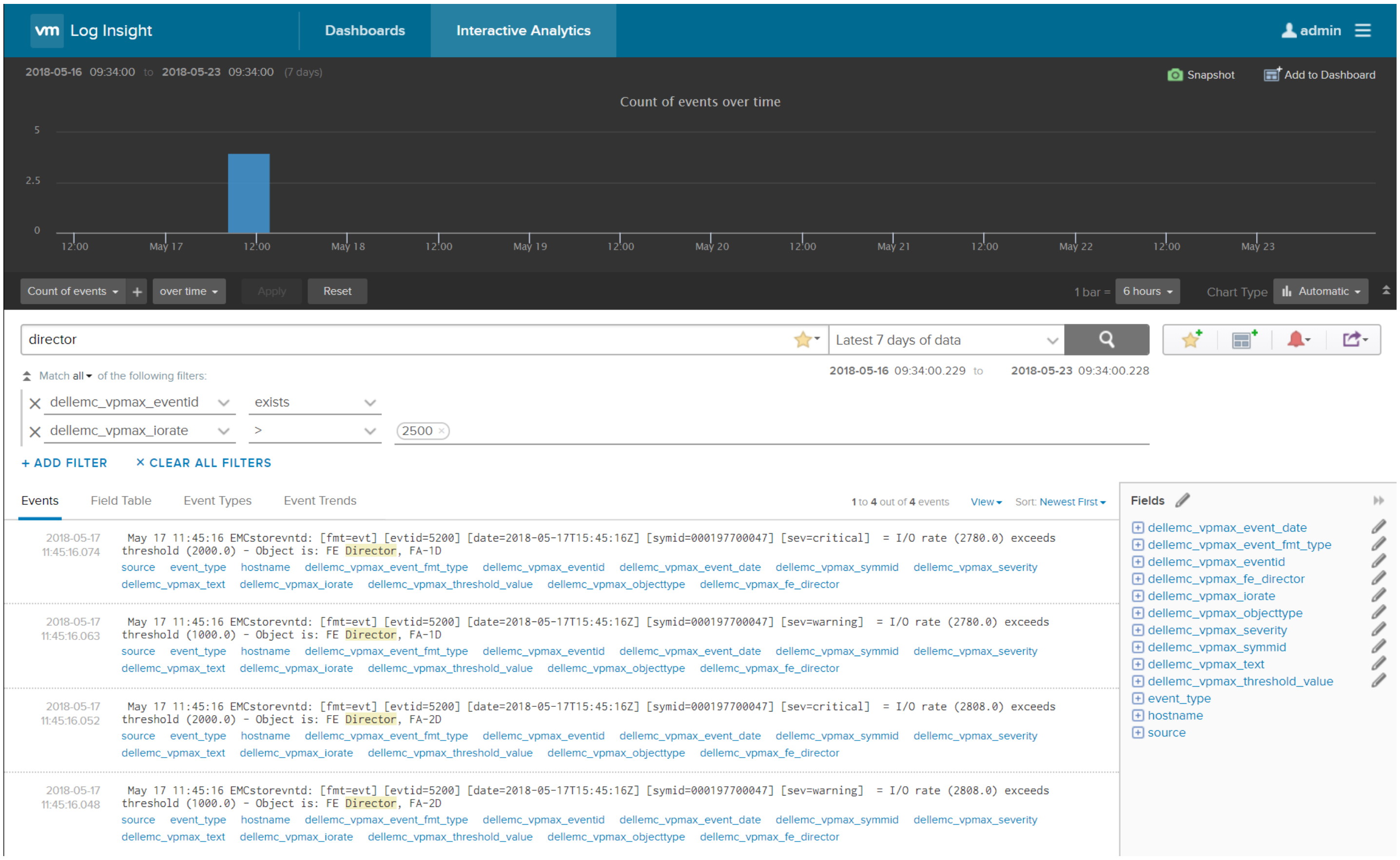


```
2018-05-17     May 17 11:45:16 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=critical]  = I/O rate (2780.0) exceeds
11:45:16.074   threshold (2000.0) - Object is: FE Director, FA-1D
```

source event_type hostname dellemc_vpmax_event_fmt_type dellemc_vpmax_eventid dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_severity
dellemc_vpmax_text dellemc_vpmax_iorate dellemc_vpmax_threshold_value dellemc_vpmax_objecttype dellemc_vpmax_fe_director

Figure 27. dell_pmax_iorate field

To add this field as a filter, he selects “+ ADD FILTER”, then using the drop-down box he chooses the field dell_pmax_iorate, and finally selects the operand greater than and types in 2500. Applying these filters reveals 4 entries that meet the final requirements in Figure 28.



director

2018-05-16 09:34:00.229 to 2018-05-23 09:34:00.228

Match all of the following filters:

- dellemc_vpmax_eventid exists
- dellemc_vpmax_iorate > 2500

+ ADD FILTER ✕ CLEAR ALL FILTERS

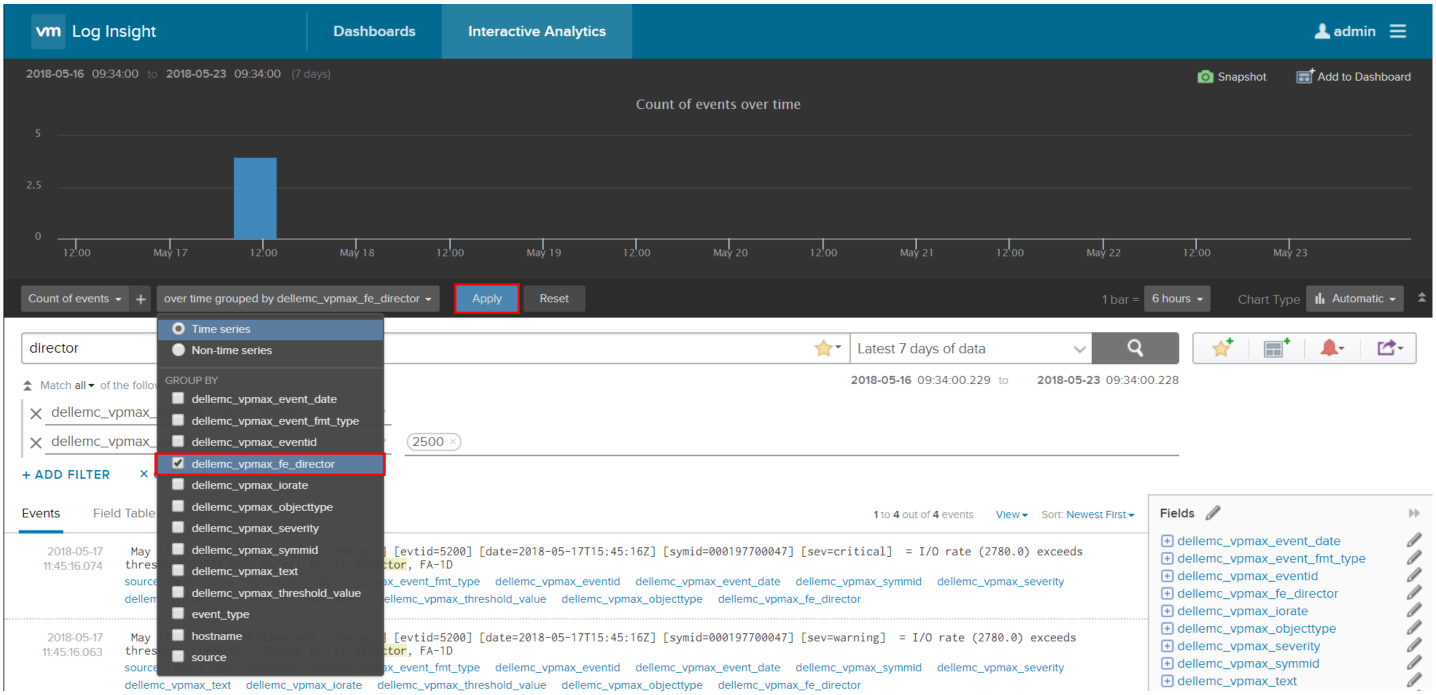
```
2018-05-17    May 17 11:45:16 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=critical]  = I/O rate (2780.0) exceeds
11:45:16.074  threshold (2000.0) - Object is: FE Director, FA-1D

2018-05-17    May 17 11:45:16 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=warning]  = I/O rate (2780.0) exceeds
11:45:16.063  threshold (1000.0) - Object is: FE Director, FA-1D

2018-05-17    May 17 11:45:16 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=critical]  = I/O rate (2808.0) exceeds
11:45:16.052  threshold (2000.0) - Object is: FE Director, FA-2D

2018-05-17    May 17 11:45:16 EMCstorevntd: [fmt=evt] [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=warning]  = I/O rate (2808.0) exceeds
11:45:16.048  threshold (1000.0) - Object is: FE Director, FA-2D
```

source event_type hostname dellemc_vpmax_event_fmt_type dellemc_vpmax_eventid dellemc_vpmax_event_date dellemc_vpmax_symmid dellemc_vpmax_severity dellemc_vpmax_text dellemc_vpmax_iorate dellemc_vpmax_threshold_value dellemc_vpmax_objecttype dellemc_vpmax_fe_director

Figure 28. Applying the 2500 IO limit and the results of investigation

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 29.



2018-05-16 09:34:00 to 2018-05-23 09:34:00 (7 days)

Count of events ▾ | over time grouped by dellemc_vpmax_fe_director ▾ | 1 bar = 6 hours

○ Time series
☑ dellemc_vpmax_fe_director

director | Latest 7 days of data

2018-05-16 09:34:00.229 to 2018-05-23 09:34:00.228

2500

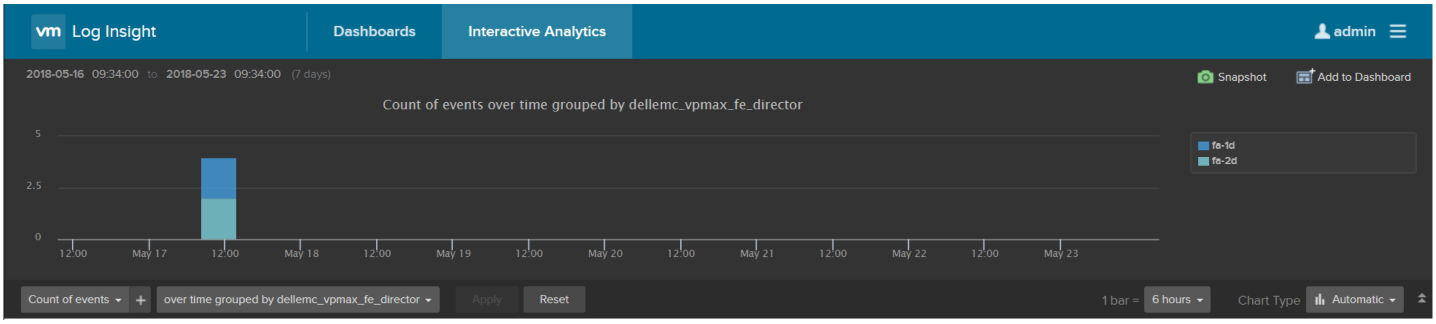
1 to 4 out of 4 events | Sort: Newest First

```
2018-05-17     May  [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=critical]  = I/O rate (2780.0) exceeds
11:45:16.074   thres                  tor, FA-1D

2018-05-17     May  [evtid=5200] [date=2018-05-17T15:45:16Z] [symid=000197700047] [sev=warning]  = I/O rate (2780.0) exceeds
11:45:16.063   thres                  tor, FA-1D
```

- dellemc_vpmax_event_date
- dellemc_vpmax_event_fmt_type
- dellemc_vpmax_eventid
- dellemc_vpmax_fe_director
- dellemc_vpmax_iorate
- dellemc_vpmax_objecttype
- dellemc_vpmax_severity
- dellemc_vpmax_symmid
- dellemc_vpmax_text

Figure 29. Grouping by FE director

After selecting "Apply" the new graph appears in Figure 30.

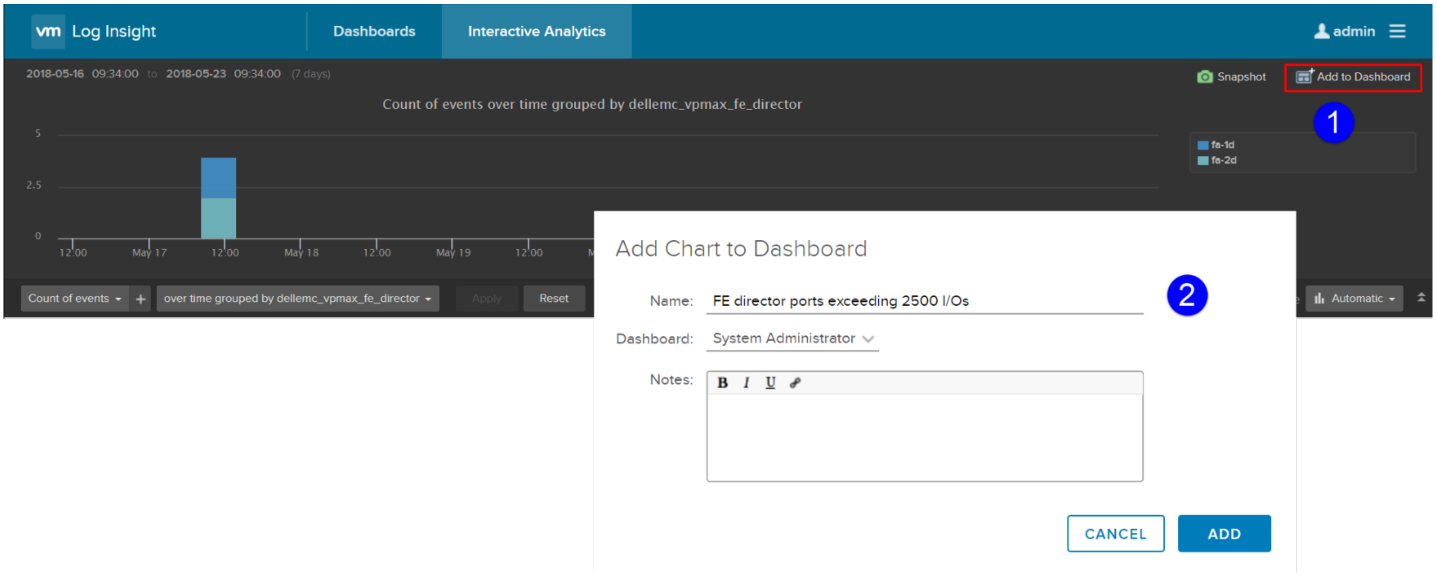


2018-05-16 09:34:00 to 2018-05-23 09:34:00 (7 days)

Count of events ▾ | over time grouped by dellemc_vpmax_fe_director ▾ | 1 bar = 6 hours

Figure 30. Final FE director graph

Finally, the VMAdmin decides to add this graph to the System Administrator's dashboard so that the information is readily available. He selects "Add to Dashboard" and puts it in the dashboard in Figure 31.



2018-05-16 09:34:00 to 2018-05-23 09:34:00 (7 days)

Count of events over time grouped by dellemc_vpmax_fe_director

Count of events · over time grouped by dellemc_vpmax_fe_director

Add Chart to Dashboard

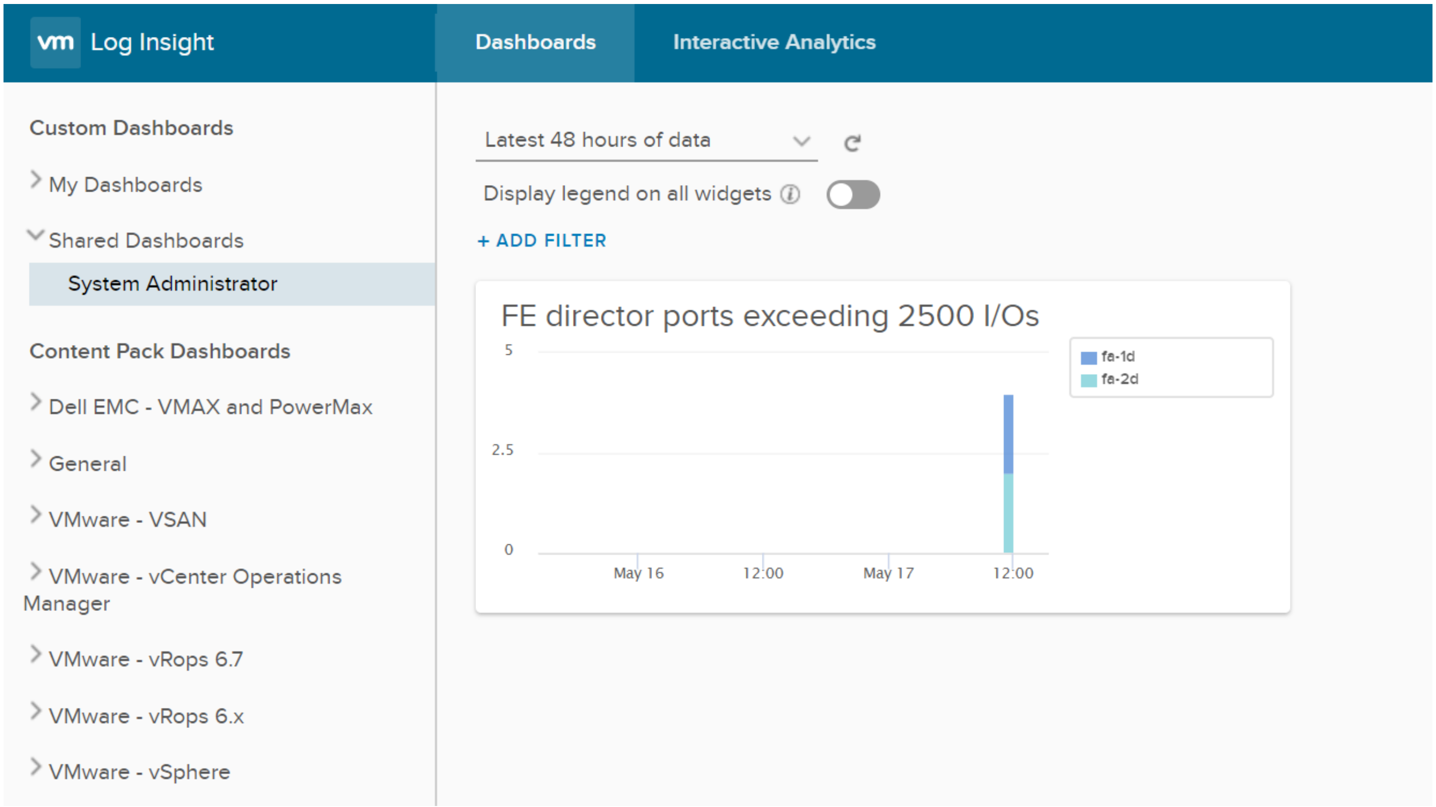
Name: FE director ports exceeding 2500 I/Os

Dashboard: System Administrator

Notes:

Figure 31. Add FE IO graph to dashboard

The final dashboard is shown in Figure 32.



FE director ports exceeding 2500 I/Os

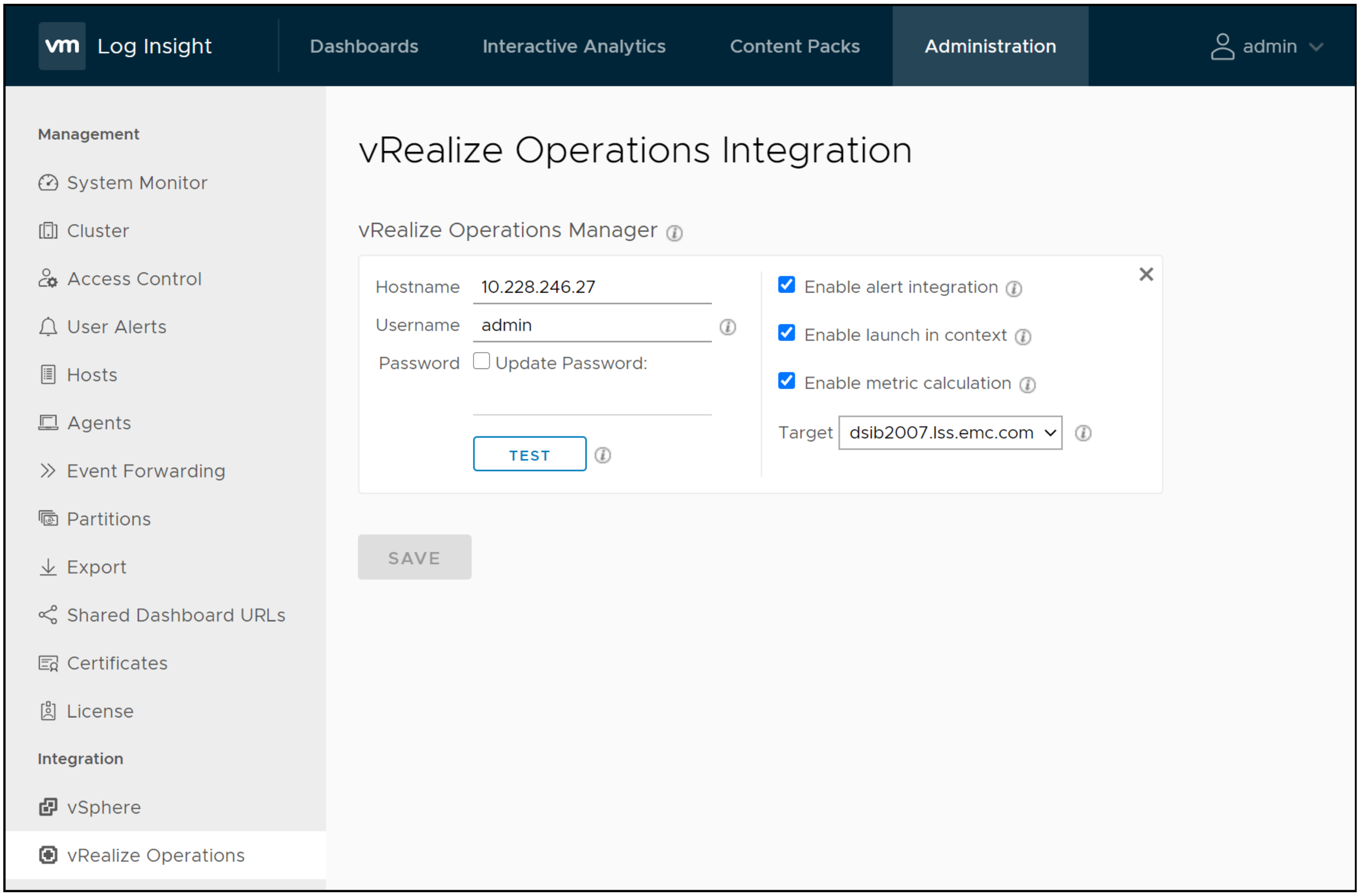
Figure 32. System Administrator dashboard

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

Using the Dell PowerMax content pack with Dell Enterprise Storage Analytics

VMware provides the ability to integrate Operations for Logs 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 Operations for Logs from within vROps. The second is to enable alerts integration which means that it is possible to send alerts from Operations for Logs into vROps and associate them with a resource from Dell Enterprise Storage Analytics (ESA). This second capability allows Operations for Logs customers who also have ESA for VMAX or PowerMax to receive alerts from within ESA. Fortunately, the PowerMax 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 PowerMax content pack.

First, enable the capability by navigating to the Administration page in Operations for Logs and then the vRealize Operations Manager Integration, demonstrated in Figure 33.



vRealize Operations Integration

vRealize Operations Manager

Hostname 10.228.246.27

Username admin

Password □ Update Password:

TEST

☑ Enable alert integration

☑ Enable launch in context

☑ Enable metric calculation

Target dsib2007.lss.emc.com

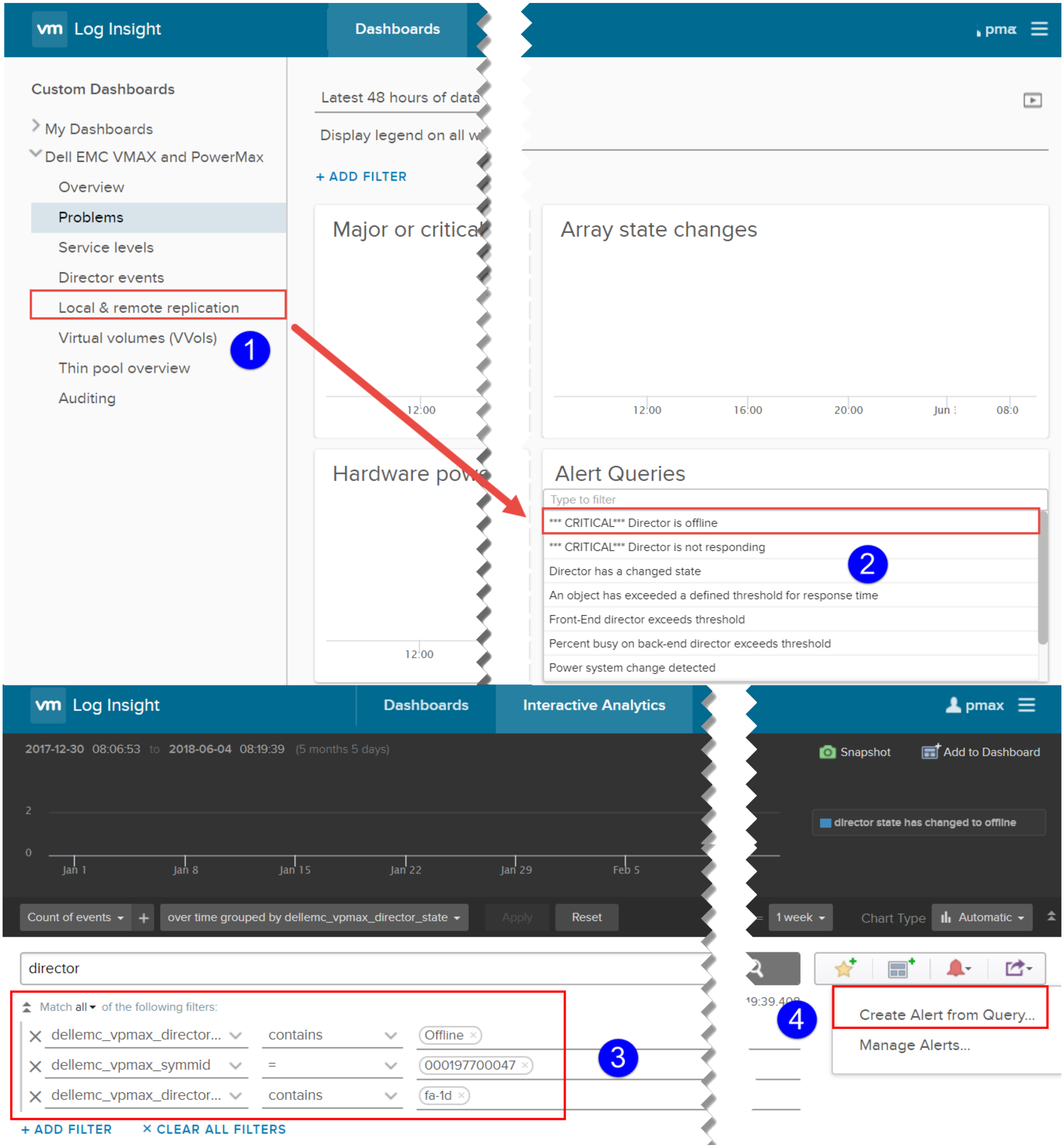
SAVE

Figure 33. 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 PowerMax ID (if more than one is monitored) and a specific FA. Once complete, select “Create Alert from Query…” This is all shown in Figure 34.



*** 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 system change detected

2017-12-30 08:06:53 to 2018-06-04 08:19:39 (5 months 5 days)

director state has changed to offline

Count of events + over time grouped by dellemc_vpmax_director_state

director

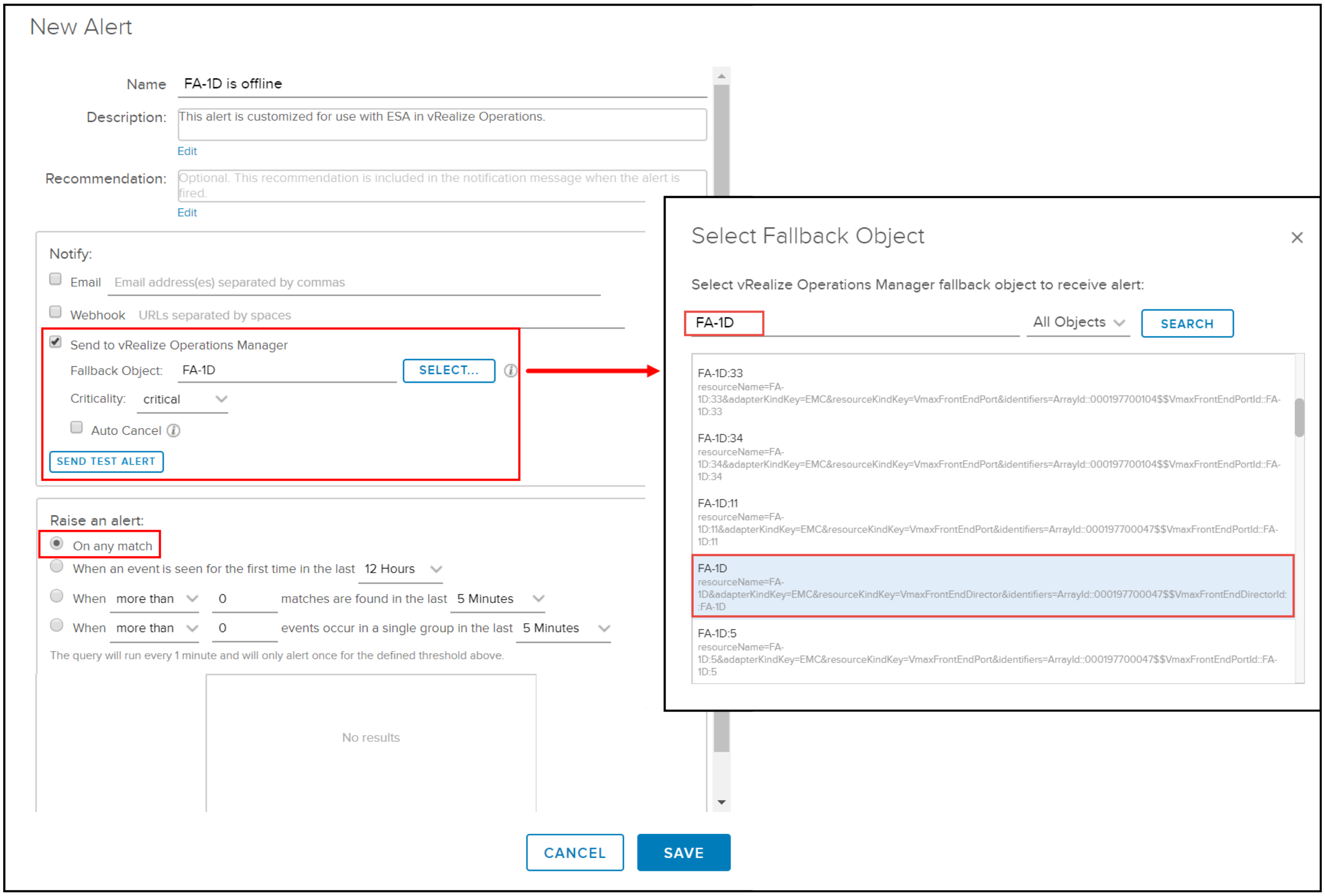
19:39.408

Match all of the following filters:

dellemc_vpmax_director...	contains	Offline
dellemc_vpmax_symmid	=	000197700047
dellemc_vpmax_director...	contains	fa-1d

Figure 34. Selecting, customizing, and creating alert for use in Operations for Logs/ESA

In the separate dialog box for setting up the alert, check the box for "Send to vRealize Operations Manager" (it is optional to unselect the Email as done here), select the correct Failback Object and change the Criticality and then if desired select "SEND TEST ALERT". If successful, change the radio button to "On any match" to ensure you get all alerts and SAVE. This is displayed in Figure 35.


New Alert

Name: FA-1D is offline

Description: This alert is customized for use with ESA in vRealize Operations.

Recommendation: Optional. This recommendation is included in the notification message when the alert is fired.

Notify:

□ Email   Email address(es) separated by commas

□ Webhook   URLs separated by spaces

☑ Send to vRealize Operations Manager

Fallback Object: FA-1D

Criticality: critical

□ Auto Cancel

Raise an alert:

● On any match

○ When an event is seen for the first time in the last 12 Hours

○ When more than 0 matches are found in the last 5 Minutes

○ When more than 0 events occur in a single group in the last 5 Minutes

The query will run every 1 minute and will only alert once for the defined threshold above.

No results

Select Fallback Object

Select vRealize Operations Manager fallback object to receive alert:

FA-1D   All Objects

FA-1D:33
resourceName=FA-1D:33&adapterKindKey=EMC&resourceKindKey=VmaxFrontEndPort&identifiers=ArrayId::000197700104$$VmaxFrontEndPortId::FA-1D:33

FA-1D:34
resourceName=FA-1D:34&adapterKindKey=EMC&resourceKindKey=VmaxFrontEndPort&identifiers=ArrayId::000197700104$$VmaxFrontEndPortId::FA-1D:34

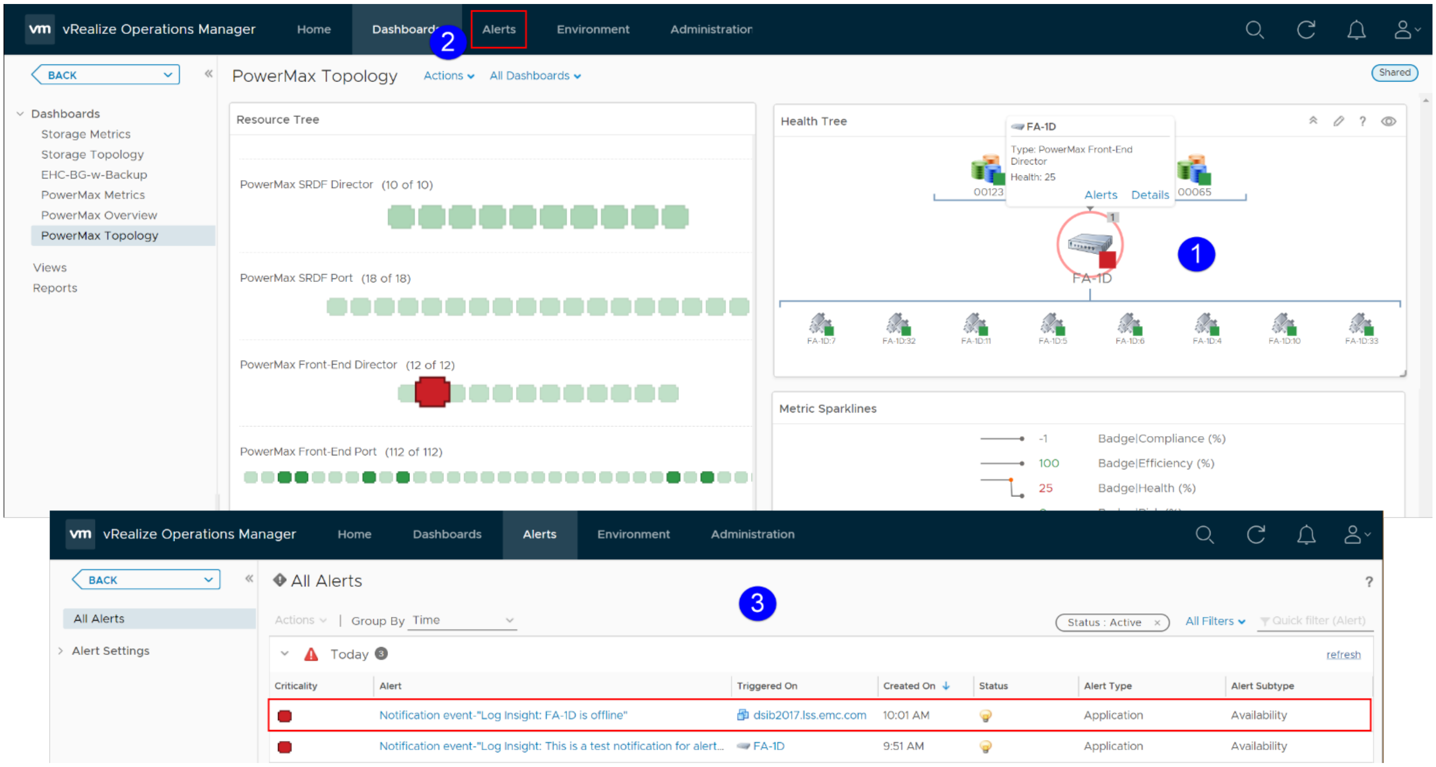
FA-1D:11
resourceName=FA-1D:11&adapterKindKey=EMC&resourceKindKey=VmaxFrontEndPort&identifiers=ArrayId::000197700047$$VmaxFrontEndPortId::FA-1D:11

FA-1D
resourceName=FA-1D&adapterKindKey=EMC&resourceKindKey=VmaxFrontEndDirector&identifiers=ArrayId::000197700047$$VmaxFrontEndDirectorId::FA-1D

FA-1D:5
resourceName=FA-1D:5&adapterKindKey=EMC&resourceKindKey=VmaxFrontEndPort&identifiers=ArrayId::000197700047$$VmaxFrontEndPortId::FA-1D:5

Figure 35. Customizing the alert

Once the alert is in place, it is run every 5 minutes. If there is a match, Operations for Logs 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 select the Alerts page in step 2. Step 3 displays the alert along with the test alert from Figure 35) in Figure 36.



Criticality	Alert	Triggered On	Created On	Status	Alert Type	Alert Subtype
🟥	Notification event-"Log Insight: FA-1D is offline"	dsib2017.lss.emc.com	10:01 AM	💡	Application	Availability
🟥	Notification event-"Log Insight: This is a test notification for alert...	FA-1D	9:51 AM	💡	Application	Availability

Figure 36. Operations for Logs alert generated in ESA

Using the aforementioned process, ESA can receive any alerts generated on the array when the user configures the Operations for Logs integration using the Dell PowerMax content pack.

Conclusion

By utilizing the PowerMax content pack within VMware Aria Operations for Logs, PowerMax 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

Dell

- *PowerMax Technical Documentation*

  https://www.dell.com/support/home/en-us/product-support/product/powermax-os-10/docs
- *Dell Enterprise Storage Analytics for vRealize Operations 7.2 Product Guide*

https://www.dell.com/support/manuals/en-us/storage-analytics/sas_pub_product_guide_version_7_2/references?guid=guid-f48d30dc-9d1e-47ba-8678-1aae8df02767&lang=en-us

VMware

- *VMware Aria Operations for Logs Documentation*

  https://docs.vmware.com/en/VMware-Aria-Operations-for-Logs/index.html

Appendix: Dell PowerMax content pack and PowerMax auditing data

This appendix will discuss how the Dell PowerMax content pack can present PowerMax 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 PowerMax 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 PowerMax array. Records are written to this by Solutions Enabler, software running on the Service Processor, and the Enginuity™ /HYPERMAX OS™/POWERMAXOS™ Operating Environment. There are two ways to present auditing information to Operations for Logs: the event daemon and the *symaudit* command.

There are many types of activities performed on the PowerMax 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

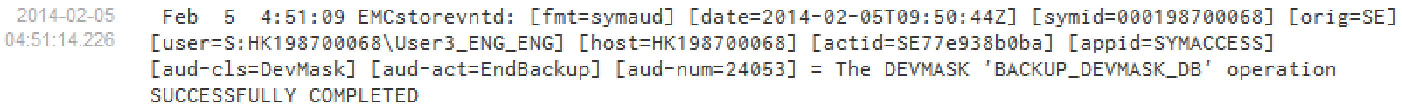
The first, and easiest method to obtain audit records is to use the event daemon. Although not well documented, there is another category that can be added to the daemon_options file as outlined in the Configuring Solutions Enabler section in this document. The category is "audit" and the entry must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

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

If auditing is desired, an entry in the daemon_options file might look like the following:

```
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 37:



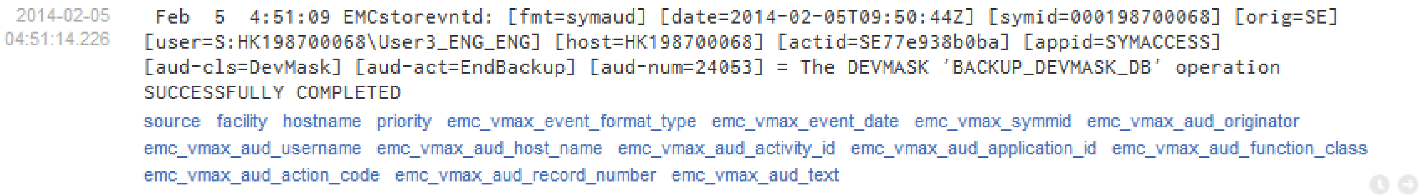
```
2014-02-05    Feb  5  4:51:09 EMCstorevntd: [fmt=symaud] [date=2014-02-05T09:50:44Z] [symid=000198700068] [orig=SE]
04:51:14.226  [user=S:HK198700068\User3_ENG_ENG] [host=HK198700068] [actid=SE77e938b0ba] [appid=SYMACCESS]
              [aud-cls=DevMask] [aud-act=EndBackup] [aud-num=24053] = The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

Figure 37. 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 "dell_pmax_aud_" – the "aud" representing the shortened form of the audit record. The fields are:

- dell_pmax_aud_action_code
- dell_pmax_aud_activity_id
- dell_pmax_aud_app_id
- dell_pmax_aud_function_class
- dell_pmax_aud_host_name
- dell_pmax_aud_originator
- dell_pmax_aud_record_number
- dell_pmax_aud_text
- dell_pmax_aud_username

An entry in Operations for Logs with the fields identified appears in Figure 38.



```
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 38. Audit entry as forwarded by the event daemon with user-defined fields

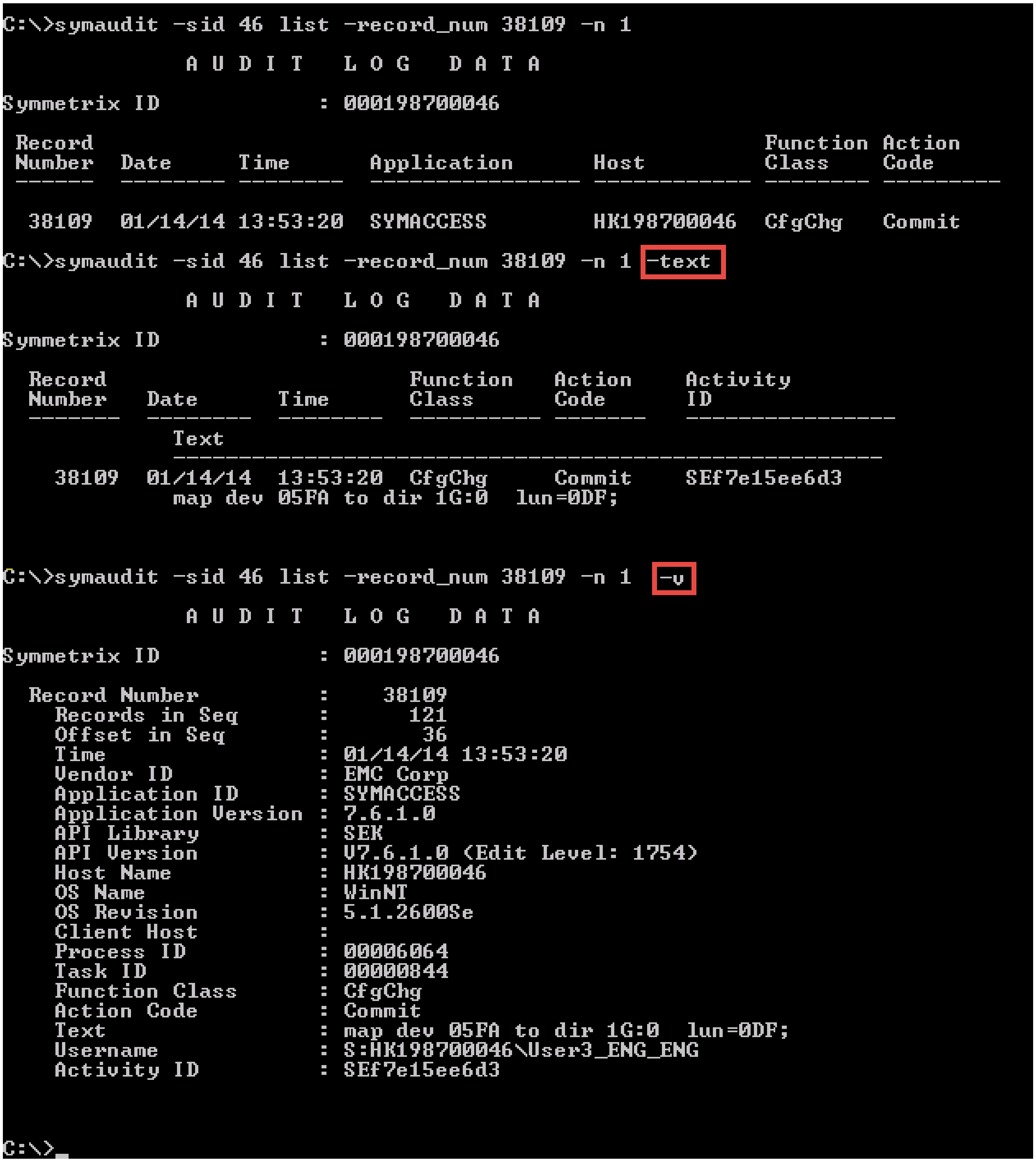
Note that some PowerMax events will generate both a regular log entry as well as an audit log entry in Operations for Logs. Because of the manner in which the PowerMax generates audit entries, however, the date field may not exactly match the associated date field of the non-audit log entry (if any).

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 Operations for Logs.

Symaudit has two modes which could be used in this context: list and monitor[3]. 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 information to Operations for Logs, the more information the better for analysis. Figure 39 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:

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



```
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                       Function   Action    Activity
  Number   Date      Time      Class      Code      ID
  -------  --------  --------  ---------- -------   ----------------
             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 39. The three levels of symaudit detail

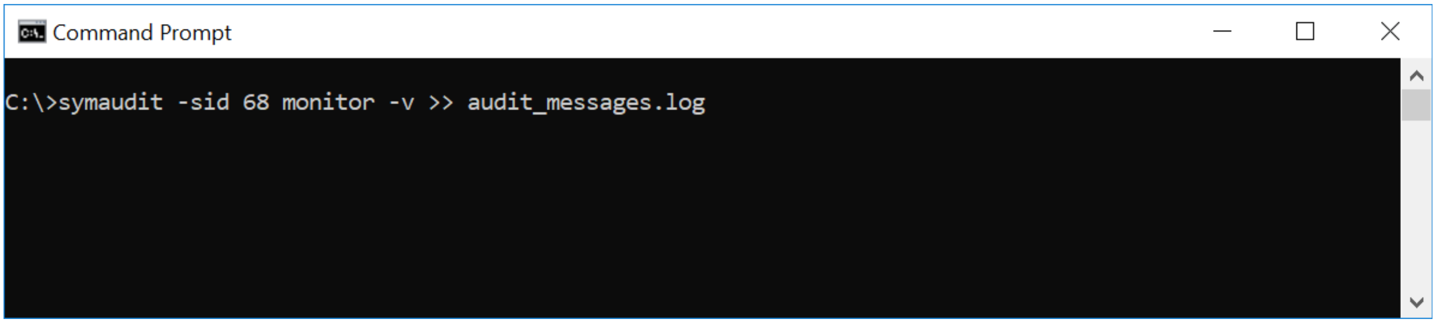
As one can see, the first entry has very basic information. The second adds some text which is more useful but the third includes detail on each field available in the record. Although any of these formats could be sent to Operations for Logs, the PowerMax content pack auditing additions were made based 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 37. Although the event daemon entry contains some of the information, it is not inclusive, nor are the fields self-explanatory.

Sending auditing events to Operations for Logs

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."[4] 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 simple 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 39, is:

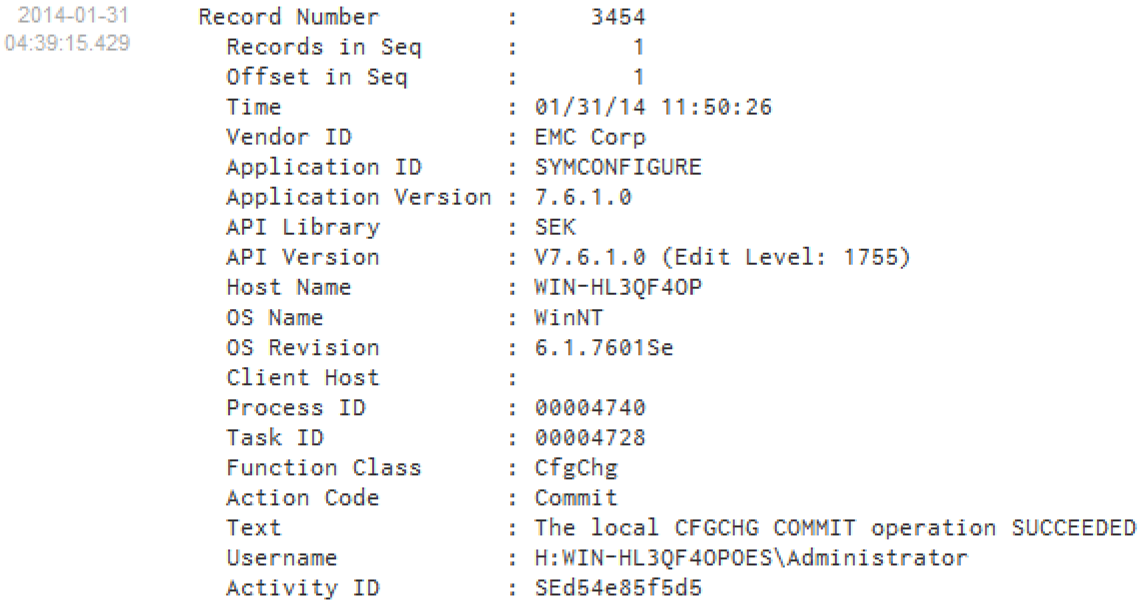


```
C:\>symaudit -sid 68 monitor -v >> audit_messages.log
```

Figure 40. Symaudit monitor command with verbose output

Figure 41 is a typical record that will be sent to Operations for Logs:

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

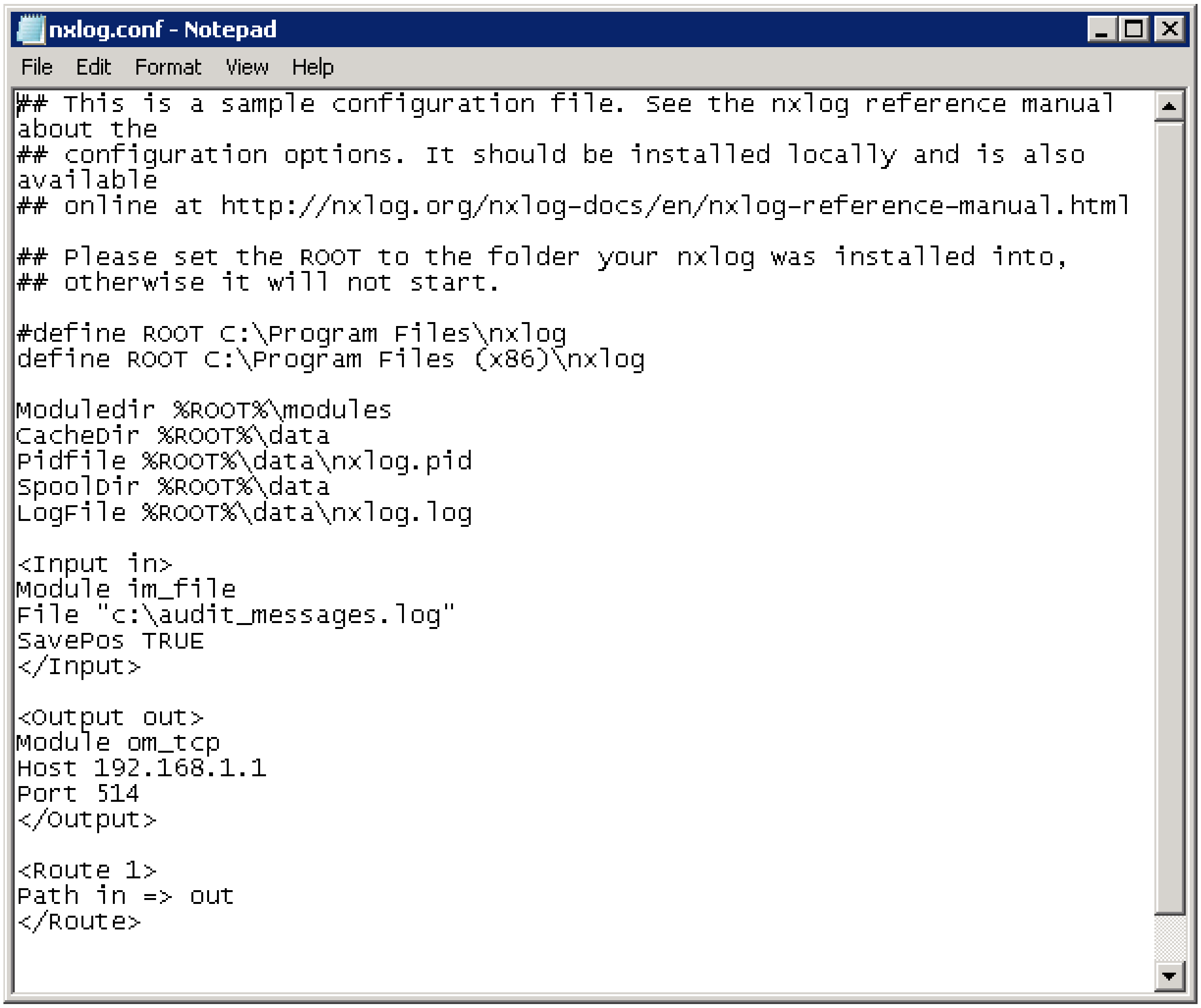


```
2014-01-31    Record Number          :     3454
04:39:15.429    Records in Seq       :        1
                Offset in Seq        :        1
                Time                 : 01/31/14 11:50:26
                Vendor ID            : EMC Corp
                Application ID       : SYMCONFIGURE
                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 41. Audit entry from symaudit

NXLOG configuration

An NXLOG configuration file requires modification to send the audit entries to Operations for Logs. 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 42. 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/PowerMax 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 PowerMax arrays in the environment and audit records are being sent to the same Operations for Logs environment, there is no field in an audit record that lists the VMAX or PowerMax array ID. When records are generated on the array itself, the Host Name will include the array ID (as in Figure 39), 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 41. 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 set 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 Operations for Logs. 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.

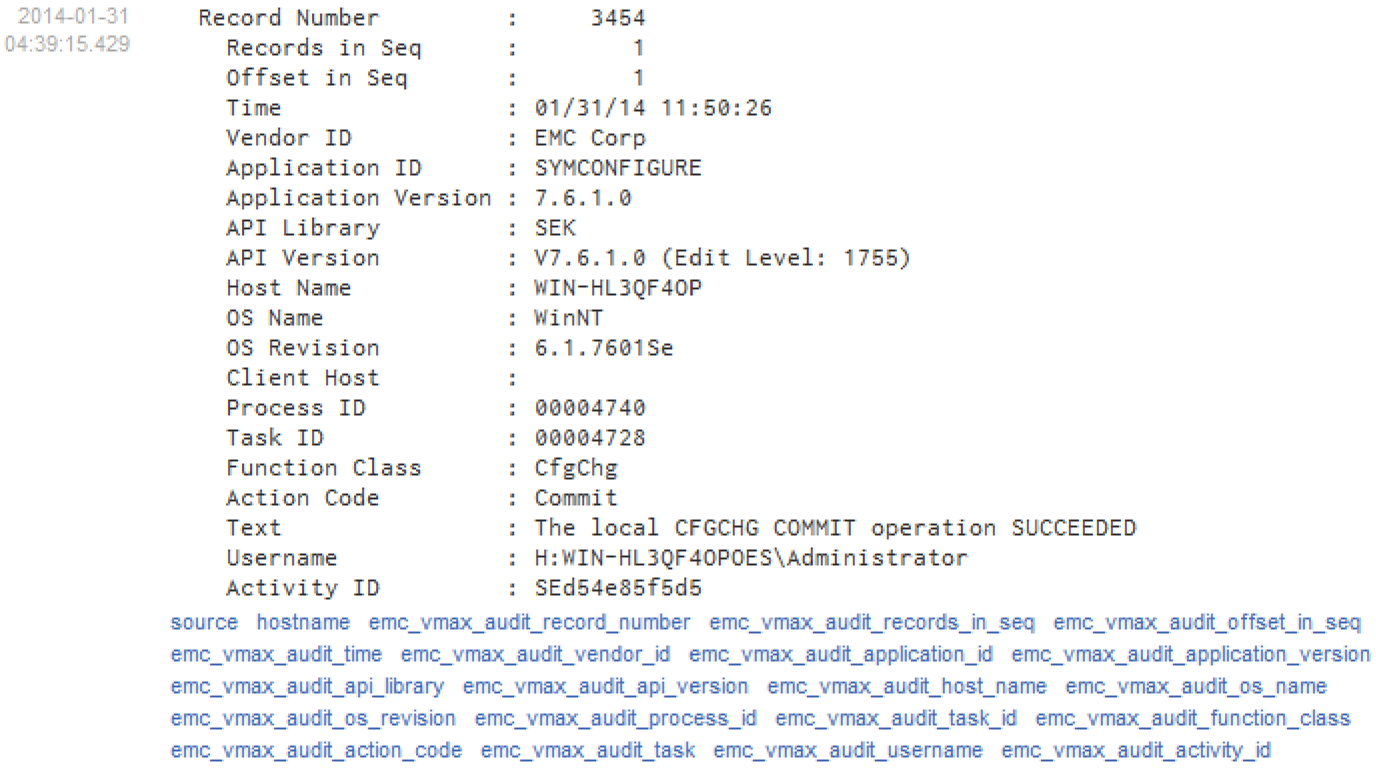
User-defined fields

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 “dell_pmax_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.

- dell_pmax_audit_action_code
- dell_pmax_audit_activity_id
- dell_pmax_audit_api_library
- dell_pmax_audit_api_version
- dell_pmax_audit_application_id
- dell_pmax_audit_application_version
- dell_pmax_audit_client_host
- dell_pmax_audit_function_class

- dell_pmax_audit_host_name
- dell_pmax_audit_offset_in_seq
- dell_pmax_audit_os_name
- dell_pmax_audit_os_revision
- dell_pmax_audit_process_id
- dell_pmax_audit_record_number
- dell_pmax_audit_records_in_seq
- dell_pmax_audit_task_id
- dell_pmax_audit_text
- dell_pmax_audit_time
- dell_pmax_audit_username
- dell_pmax_audit_vendor_id

An entry in Operations for Logs with the fields identified appears in Figure 43.



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
```

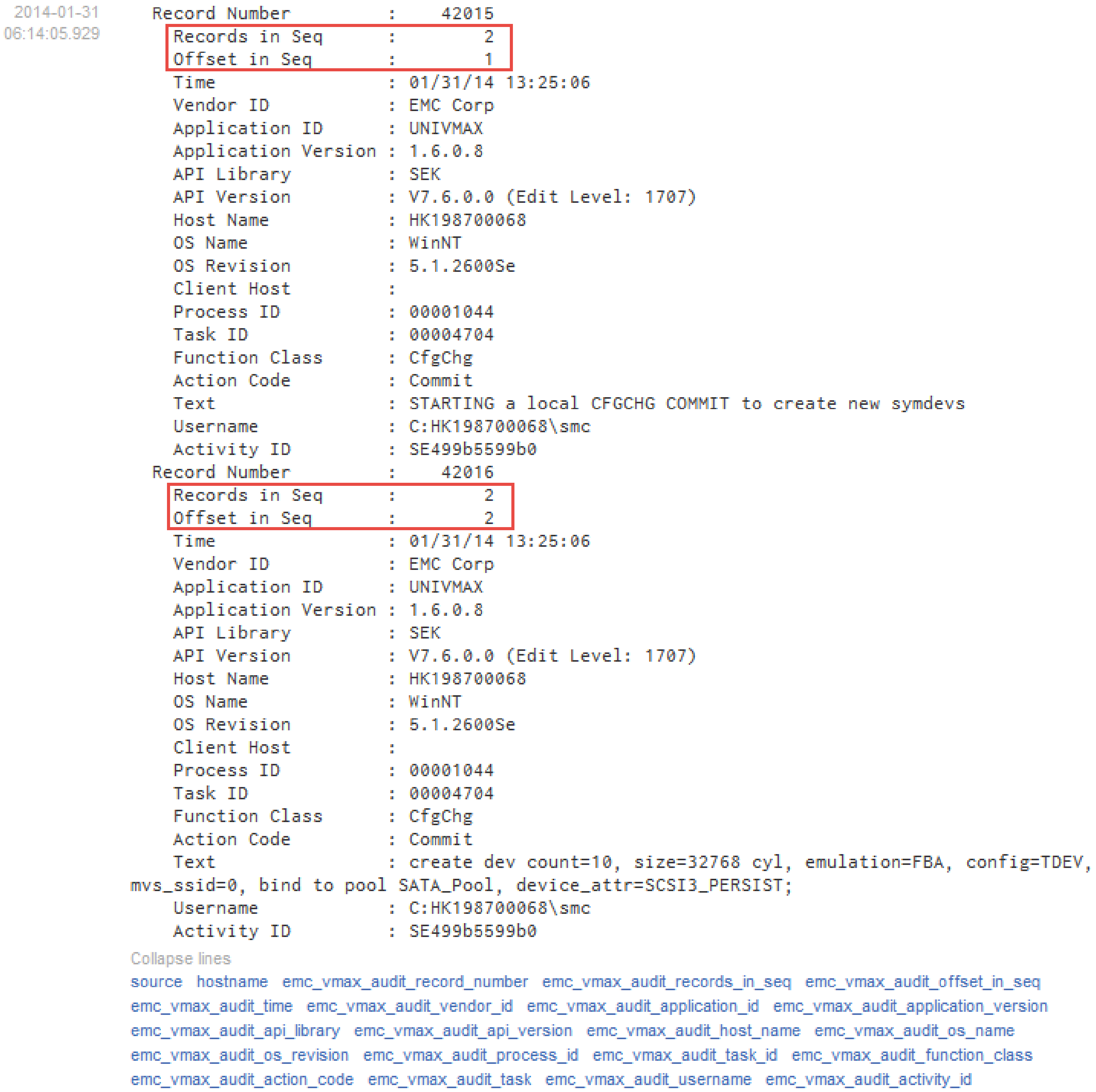
source hostname emc_vmax_audit_record_number emc_vmax_audit_records_in_seq emc_vmax_audit_offset_in_seq
emc_vmax_audit_time emc_vmax_audit_vendor_id emc_vmax_audit_application_id emc_vmax_audit_application_version
emc_vmax_audit_api_library emc_vmax_audit_api_version emc_vmax_audit_host_name emc_vmax_audit_os_name
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 43. 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 Operations for Logs 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 Operations for Logs

There are two noteworthy items to mention concerning the symaudit logs as they appear in Operations for Logs. The first is to understand that audit messages sometimes come in multiples. Because the records get written together, they get sent to Operations for Logs together. For instance, Figure 44 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

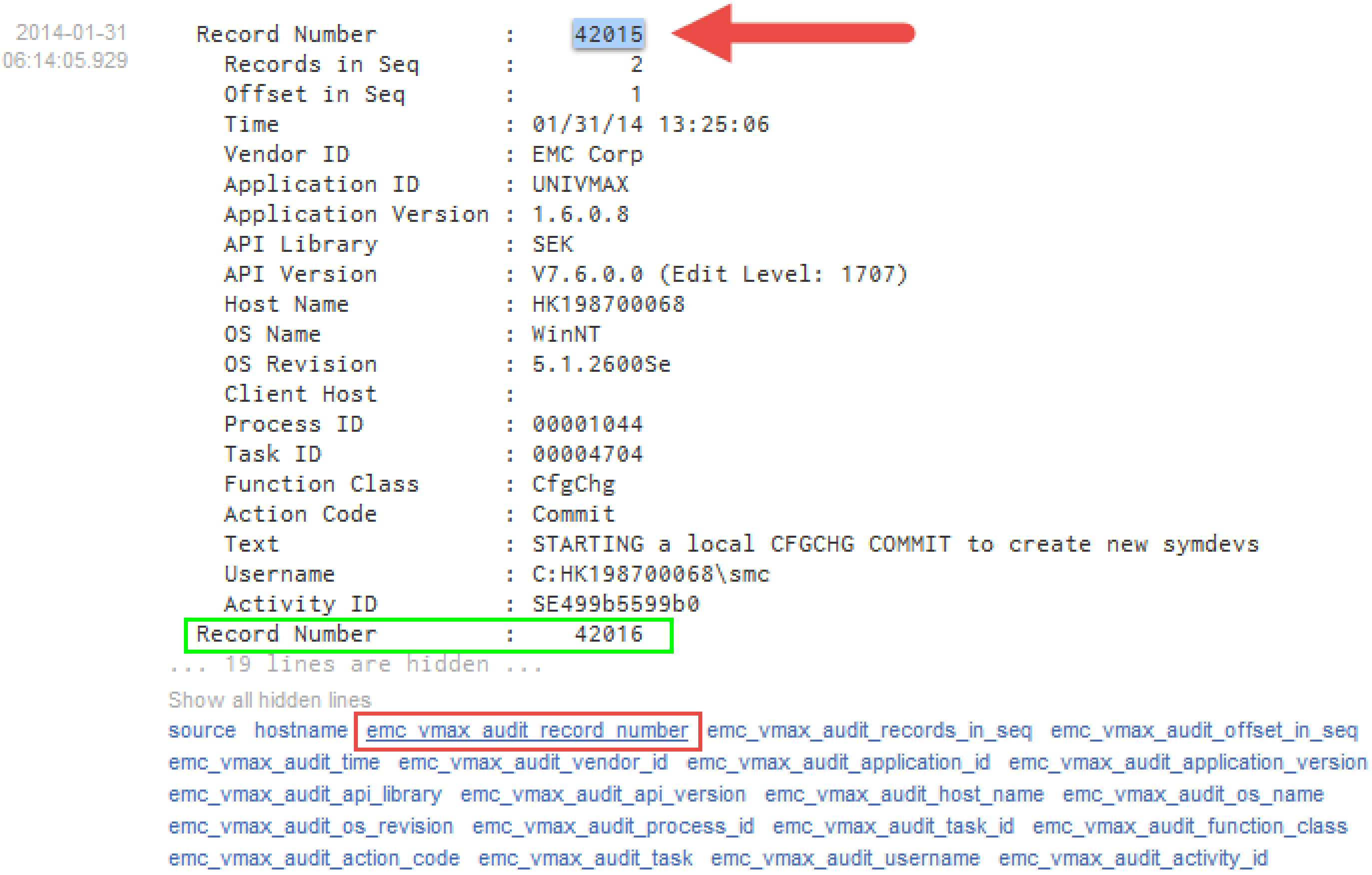
```
  Record Number        :    42015
    Records in Seq     :        2
    Offset in Seq      :        1
    Time               : 01/31/14 13:25:06
    Vendor ID          : EMC Corp
    Application ID     : UNIVMAX
    Application Version : 1.6.0.8
    API Library        : SEK
    API Version        : 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 44. Audit record with multiple entries

The second noteworthy item also relates to multiple records and user-defined fields. Operations for Logs is not capable of recognizing multiple entries of an extracted field in a single event. So, using the previous entry in Figure 44 as an example, if one puts the cursor over the user-defined field, dell_pmax_audit_record_number, only the first occurrence will be highlighted. This is seen in Figure 45.



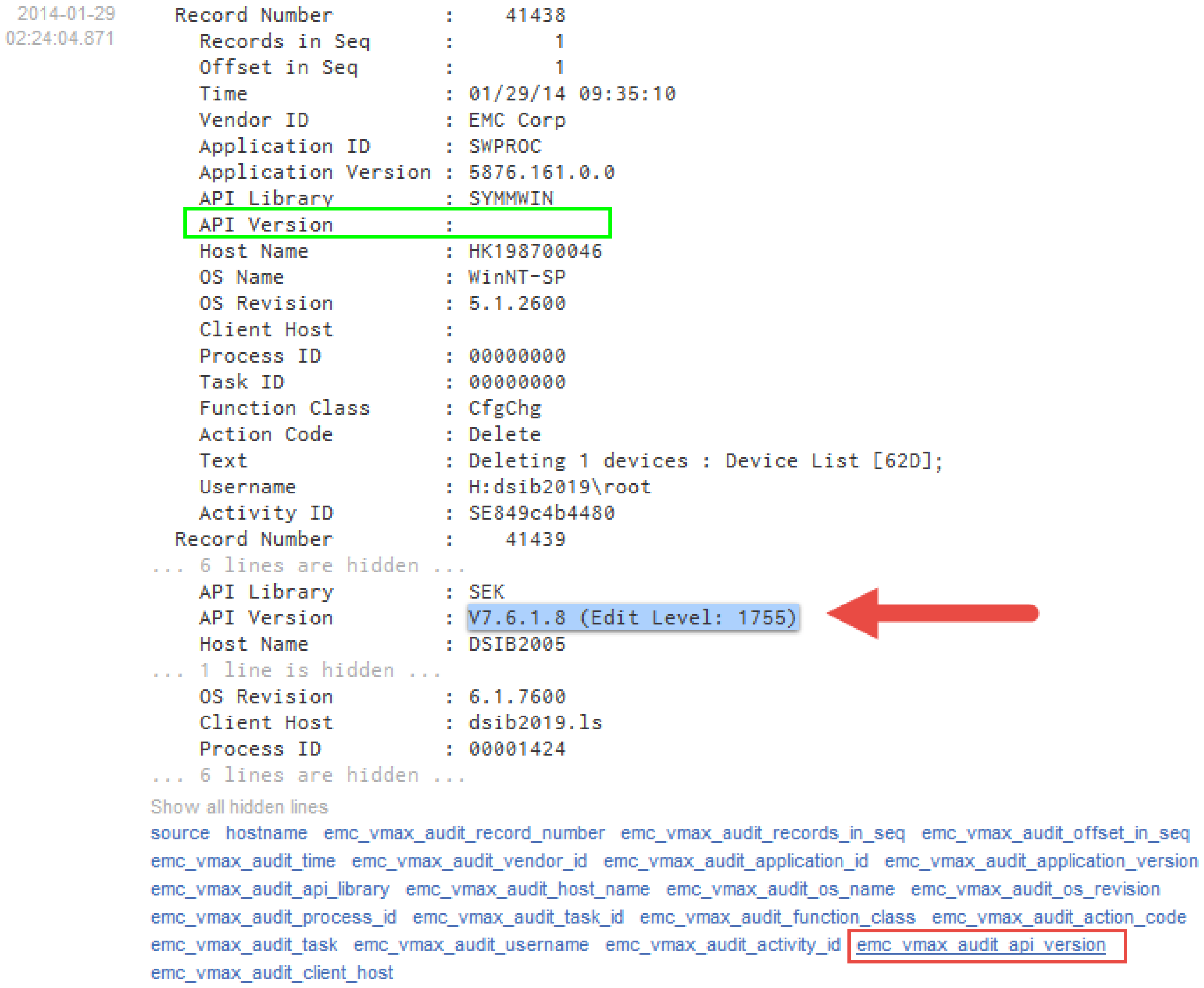
```
2014-01-31     Record Number          :     42015
06:14:05.929     Records in Seq       :         2
                 Offset in Seq        :         1
                 Time                 : 01/31/14 13:25:06
                 Vendor ID            : EMC Corp
                 Application ID       : 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 45. User-defined fields with multiple entries

Similarly, if there are multiple entries but the first occurrence of the field is NULL, Operations for Logs will highlight the next entry as in Figure 46 with the user-defined field dell_pmax_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

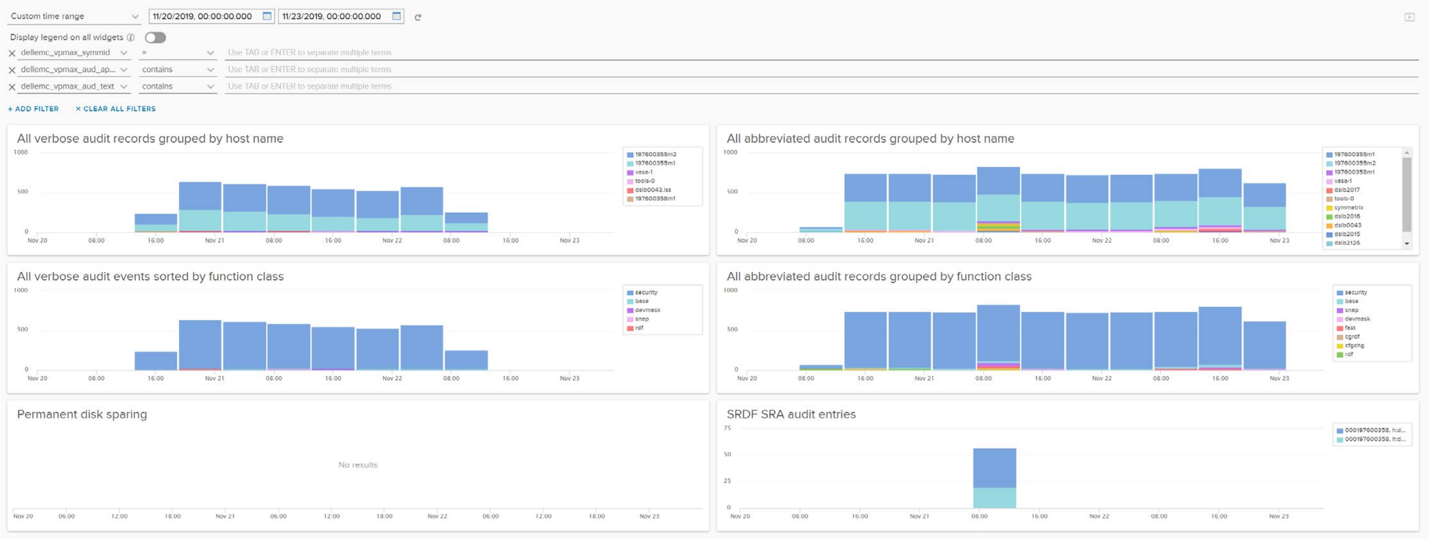
Figure 46. User-defined fields with multiple entries and a NULL value

Dashboard

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 PowerMax audit entries in the Operations for Logs 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 47.



Custom time range | 11/20/2019, 00:00:00.000 | 11/23/2019, 00:00:00.000

Display legend on all widgets

dellemc_vpmax_symmid	=	Use TAB or ENTER to separate multiple terms
dellemc_vpmax_aud_ap...	contains	Use TAB or ENTER to separate multiple terms
dellemc_vpmax_aud_text	contains	Use TAB or ENTER to separate multiple terms

All verbose audit records grouped by host name

All abbreviated audit records grouped by host name

All verbose audit events sorted by function class

All abbreviated audit records grouped by function class

Permanent disk sparing

No results

SRDF SRA audit entries

Figure 47. PowerMax content pack - Auditing dashboard

There are no alerts or queries configured for audit information.