USING THE DELL EMC VMAX AND POWERMAX CONTENT PACK FOR VMWARE VREALIZE LOG INSIGHT
Monitoring Dell EMC VMAX and PowerMax log activity with VMware

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

December 2019

Dell EMC Engineering
Copyright © 2019 Dell Technologies. All Rights Reserved.

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

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

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

VMware, ESXi, vMotion, and vSphere are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks used herein are the property of their respective owners.

Part Number h12138.11
Table of Contents

Executive summary ............................................................................................................. 5
  Audience .......................................................................................................................... 5
  Versions ............................................................................................................................. 5

Dell EMC VMAX and PowerMax Content Pack ................................................................. 6
  Dashboards ....................................................................................................................... 8
  User-defined fields .......................................................................................................... 12
  Alerts ................................................................................................................................. 15
  Queries .............................................................................................................................. 15
  Log event viewing ............................................................................................................ 16

Configuring VMAX and PowerMax for vRealize Log Insight ......................................... 17
  Solutions Enabler and the Event daemon ...................................................................... 17
    Configuring Solutions Enabler ...................................................................................... 17
  Unisphere for VMAX/PowerMax and the Performance option ...................................... 19
    Syslog event configuration .......................................................................................... 19
    Creating a custom alert ............................................................................................... 23
  Embedded NAS (eNAS) ................................................................................................. 26

Using the Dell EMC VMAX and PowerMax Content Pack for Problem Analysis ......... 27
  Finding high I/O to the FE directors ................................................................................ 27
  Creating the dashboard ................................................................................................... 33

Using the Dell EMC VMAX and PowerMax Content Pack with Dell EMC Enterprise
  Storage Analytics ........................................................................................................... 36
  Customized director alert ............................................................................................. 37

Conclusion ......................................................................................................................... 40

References ......................................................................................................................... 40

Dell EMC ............................................................................................................................. 40
VMware ............................................................................................................................... 41

Appendix: Dell EMC VMAX and PowerMax Content Pack and VMAX and PowerMax
  Auditing Data .................................................................................................................... 42
  Auditing ............................................................................................................................ 42
  Audit entries and the event daemon ............................................................................... 42
  Audit entries and symaudit ............................................................................................. 43
  Sending auditing events to Log Insight .......................................................................... 46
  NXLOG configuration ..................................................................................................... 47
User-defined fields..................................................................................................................49
Audit record formatting and Log Insight..................................................................................50
Dashboards..................................................................................................................................54
Executive summary

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

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

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

Audience

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

Versions

As of publication of this paper, VMware vRealize Log Insight 8.0 is the current GA product version. The minimum version required to install the Dell EMC – VMAX and PowerMax Content Pack is version 4.7.
Dell EMC VMAX and PowerMax Content Pack

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

![Log Insight Content Pack Marketplace](image)

**Figure 1. Log Insight 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 VMAX and PowerMax content pack is not required in order to use Log Insight with the VMAX or PowerMax, it is recommended as a good starting point for helping to categorize all the log information coming from the array.

When viewing the VMAX and PowerMax Content Pack definition in Log Insight, there is a full description of the content pack details. Seen in Figure 2 is the definition of the VMAX and PowerMax Content Pack.
Figure 2. VMware Log Insight with the VMAX and 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.
Figure 3. Setup instructions for the VMAX and PowerMax Content Pack

Dashboards

Included below are the seven dashboards that comprise the VMAX and PowerMax Content Pack. They are:

- **Overview** – Contains widgets with information about all VMAX and PowerMax data in your Log Insight 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 VMAX and PowerMax.
- **Director events** – Contains widgets with information about any front-end or back-end director events on the VMAX and PowerMax.
- **Local & remote replication** – Contains widgets specific to log messages generated by SRDF™ or TimeFinder™ software.
- **Virtual volumes (vVols)** – Contains widgets with information about thin pool and device events.
- **Thin pool overview** – Contains widgets with metrics specific to FAST VP on the VMAX2.
- **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, Figure 9, and Figure 10. The auditing dashboard is covered in the Appendix: Dell EMC VMAX and PowerMax Content Pack and VMAX and PowerMax Auditing Data.

Figure 4. VMAX and PowerMax content pack - Overview dashboard

Figure 5. VMAX and PowerMax Content Pack - Problems dashboard
Figure 6. VMAX and PowerMax Content Pack – Service levels dashboard

Figure 7. VMAX and PowerMax Content Pack - Director events dashboard
Figure 8. VMAX and PowerMax Content Pack - Local & remote replication dashboard

Figure 9. VMAX and PowerMax Content Pack– Virtual volumes (vWols) dashboard
User-defined fields

In large environments with numerous log messages, it is difficult to locate instantly the data fields that are important to you. Log Insight provides runtime field extraction to address this problem. You can dynamically extract any field from the data by providing a regular expression. For instance, given the log entry in Figure 11, individual fields can be identified for extraction.
Figure 11. 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 12. By hovering the cursor over the new field, the symid value will be highlighted in blue.

Figure 12. User-defined field dellemc_vpmx_symmid

Within the VMAX and PowerMax Content Pack, Dell EMC has preconfigured user-defined fields for the most commonly appearing objects in the log files. All of the fields have the prefix “dellemc_vpmx_” 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.

- dellemc_vpmx_array_srdf_group
- dellemc_vpmx_array_state
- dellemc_vpmx_be_director
• dellemc_vpmmax_devices
• dellemc_vpmmax_director_name
• dellemc_vpmmax_director_state
• dellemc_vpmmax_egress_tracks
• dellemc_vpmmax_event_date
• dellemc_vpmmax_event_format_type
• dellemc_vpmmax_eventid
• dellemc_vpmmax_fe_director
• dellemc_vpmmax_ingress_tracks
• dellemc_vpmmax_iorate
• dellemc_vpmmax_objecttype
• dellemc_vpmmax_pctbusy
• dellemc_vpmmax_pcthit
• dellemc_vpmmax_percent
• dellemc_vpmmax_port_name
• dellemc_vpmmax_port_status
• dellemc_vpmmax_portgroup
• dellemc_vpmmax_power
• dellemc_vpmmax_response_time
• dellemc_vpmmax_scontainer
• dellemc_vpmmax_scontainer_percent
• dellemc_vpmmax_severity
• dellemc_vpmmax_sg
• dellemc_vpmmax_sg_state
• dellemc_vpmmax_sg_state_name
• dellemc_vpmmax_sl_sg
• dellemc_vpmmax_srdf_group
• dellemc_vpmmax_srdf_state
• dellemc_vpmmax_srp_name
• dellemc_vpmmax_storagegrp
• dellemc_vpmmax_storagetier
• dellemc_vpmax_symmid
• dellemc_vpmax_system
• dellemc_vpmax_text
• dellemc_vpmax_thinpool_name
• dellemc_vpmax_thinpoolname
• dellemc_vpmax_threshold_value
• dellemc_vpmax_used_capacity
• dellemc_vpmax_volume

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

Alerts

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

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

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

Queries

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

• Directors that stopped responding
• Directors that are offline

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

The VMAX and 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 Log Insight. 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 VMAX and PowerMax for vRealize Log Insight

In order to effectively make use of the Dell EMC VMAX and PowerMax Content Pack, Dell EMC log information is needed. There are two essential products that can be configured to send this log information to Log Insight: Solutions Enabler and Unisphere for VMAX/PowerMax.

Solutions Enabler and the Event daemon

A Dell EMC Solutions Enabler install provides your host with SYMAP, CLARAPI, and STORAPI shared libraries for use by Solutions Enabler applications, and the VMAX/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. The target storage environments are typically VMAX or PowerMax arrays.

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

Configuring Solutions Enabler

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

    stord daemon 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\SYMAP\config\.

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

    #storevntd:LOG_EVENT_TARGETS
Each entry is detailed below along with an example.

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

storevntd:LOG_EVENT_TARGETS = syslog

The options “LOG_EVENT_SYSLOG_HOST” and “LOG_EVENT_SYSLOG_PORT” are self-explanatory. Provide the Log Insight host IP address (the syslog server) and the port of the syslog server on the host. For Log Insight this is the default port for syslog of 514.

storevntd:LOG_EVENT_SYSLOG_HOST = 192.168.160.153
storevntd:LOG_EVENT_SYSLOG_PORT = 514

The last option, “LOG_SYMMETRIX_EVENTS” is the one that determines exactly what information will be sent to Log Insight. There are a number of categories to choose from, though the VMAX and PowerMax Content Pack takes advantage of all of them. By default, any category will apply to all VMAX and PowerMax arrays presented to Solutions Enabler unless the array SID is specifically listed. 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, status, groups, optimizer, events, array subsystem, checksum, diagnostic, environmental, device pool, service processor, srdf system, srdf link, srdfa session, srdf consistency group, director, device, disk, smc, spa ;

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

**Unisphere for VMAX/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 for VMAX/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. A basic configuration is shown in the next section for both Unisphere for VMAX and Unisphere for PowerMax. Note that Unisphere for PowerMax screens may alter slightly depending on the version. Only one example is included here.

**Syslog event configuration**

As the system administrator user (default *smc* user in this example), log in to Unisphere and navigate to the home icon then “Administration”. Under that task select “Alert Settings” and then “Notifications”. This is seen in Figure 13 for Unisphere for VMAX 8.x.
Figure 13. Alert Settings in Unisphere for VMAX 8.x

For Unisphere for PowerMax 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 for Unisphere for VMAX and Figure 16 for Unisphere for PowerMax.
Figure 15. Setting notification type and alert levels in Unisphere for VMAX 8.x

Figure 16. 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.

Start by navigating to the previously shown Administration page, and then select Performance Thresholds and Alerts as in Figure 17 or Figure 18 depending on the Unisphere version.

---

\(^{1}\) Note that array level events in Alert Policies must have the notification setup as syslog to receive these alerts in Log Insight.
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 19 walk the user through setting a custom alert on the metric Host I/O/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.
Figure 19. 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 20.
Figure 20. 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.EMC.com for 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 vRealize Log Insight. 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 vRealize Log Insight environment:

   ```
   # VMware Log Insight
   10.108.100.3 dsib1003.1ss.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 Log Insight
.* @dsib1003
```

4. Restart the syslog service to complete the setup:
```
sbin/service syslog restart
```

Once complete, log information will be forwarded to the Log Insight 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 21 contains a number of sample entries from an eNAS environment.

```
2015-06-04 14:44:59:610 EGM: Deprecated pm_stack module called from service "xmit_provider"
   source event:_type hostname

2015-06-04 14:44:59:355 ceph[14451] (root) CMD (lsblk -av /dev/mtl0)
   source event:_type hostname

2015-06-04 14:44:59:289 ceph[14455] (root) CMD (lsblk -av /dev/mtl0 /dev/mtl1)
   source event:_type hostname

   source event:_type hostname

2015-06-04 14:44:59:283 ceph[14495] (root) CMD (/sbin/ceph_mon健/lsblk -av /dev/mtl0)
   source event:_type hostname

   source event:_type hostname

   source event:_type hostname
```

Figure 21. Log entries generated by eNAS

**Using the Dell EMC VMAX and 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 VAdmin could use the VMAX and PowerMax Content Pack to isolate an issue around FE I/O.

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 I/O 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. The Sysadmin asks the VMware administrator (VMAdmin) to
determine if there have been any occurrences when an FE director has serviced more
than 2500 I/Os 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 Log Insight which he has previously configured
to accept log files from Solutions Enabler and Unisphere for PowerMax. He also has
implemented the VMAX and PowerMax Content Pack to help make the analysis
easier. Within Unisphere for PowerMax he has previously defined two thresholds for
FE ports. When I/Os reach 1000, a warning severity will be issued and then if I/Os
surpass 2000 a critical severity will be issued. Therefore he can expect two log entries
for any FE director servicing more than 2500 I/Os 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.

---

² The I/O 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
date example.
Figure 22. vRealize Log Insight 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, Log Insight 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”.

29
**Figure 23. Director term search in vRealize Log Insight**

The result of the query is displayed in Figure 24.
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 EMC_vmax_eventid”. By putting the cursor over this field, the eventid is highlighted in blue in the entry as in Figure 25.

Figure 25. dell EMC_vmax_eventid field

He clicks on the “dell EMC_vmax_eventid” field and it is automatically added as a constraint to his query, ensuring only non-auditing director entries are shown. He hits Search again and now the entries are reduced from 10 to 6, seen in Figure 26.
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 I/O rate event will show. In that entry, in parentheses, is the exact value of the I/O that exceeded the threshold. Again, he reviews the available defined fields and finds “dell EMC_vmax_irorate” in Figure 27. Running the cursor over that reveals it is associated with the value in parentheses.

Figure 27. dell EMC_vmax_irorate field

To add this field as a filter, he selects “+ ADD FILTER”, then using the drop-down box he chooses the field dell EMC_vmax_irorate, 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.
Figure 28. Applying the 2500 I/O 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.
Figure 29. Grouping by FE director

After selecting “Apply” the new graph appears in Figure 30.

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.
Figure 31. Add FE I/O graph to dashboard

The final dashboard is shown in Figure 32.

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 EMC VMAX and PowerMax Content Pack with Dell EMC Enterprise Storage Analytics

VMware provides the ability to integrate vRealize Log Insight with vRealize Operations (vROps) beyond a specialized content pack. There are two integration points which are possible. The first is to enable a launch in context capability of Log Insight from within vROps. The second is to enable alerts integration which means that it is possible to send alerts from Log Insight into vROps and associate them with a resource from Dell EMC Enterprise Storage Analytics (ESA). This second capability allows Log Insight customers who also have ESA for VMAX or PowerMax to receive alerts from within ESA. Fortunately, the VMAX and 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 VMAX and PowerMax Content Pack.

First, enable the capability by navigating to the Administration page in Log Insight and then the vRealize Operations Manager Integration, demonstrated in Figure 33.
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.
Figure 34. Selecting, customizing, and creating alert for use in Log Insight/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.

Figure 35. Customizing the alert

Once the alert is in place, it is run every 5 minutes. If there is a match, Log Insight automatically sends this alert to the defined ESA resource in vROps. There are a number of places to see this alert. In particular any topology view of the resource will include a red triangle indicating an alert. From there select the Alerts page in step 2. Step 3 displays the alert along with the test alert from Figure 35) in Figure 36.
Figure 36. Log Insight alert generated in ESA

Using the aforementioned process, ESA can receive any alerts generated on the array when the user configures the Log Insight integration using the Dell EMC VMAX and PowerMax Content Pack.

Conclusion

By utilizing the VMAX and PowerMax Content Pack within VMware vRealize Log Insight, VMAX and 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 EMC

- PowerMax and VMAX All Flash Technical Documentation
- Dell EMC Enterprise Storage Analytics
  https://support.emc.com/products/30680_Storage-Analytics
VMware

- VMware vRealize Log Insight Documentation
  
Appendix: Dell EMC VMAX and PowerMax Content Pack and VMAX and PowerMax Auditing Data

This appendix will discuss how the Dell EMC VMAX and PowerMax Content Pack can present VMAX and 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 VMAX and 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 VMAX and PowerMax array. Records are written to this by Solutions Enabler, software running on the Service Processor, and the Enginuity™/HYPERMAX OST™/POWERMAX OST™ Operating Environment. There are two ways to present auditing information to Log Insight: the event daemon and the symaudit command.

There are many types of activities performed on the VMAX and 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:
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 EMC_vpmx_aud_” – the “aud” representing the shortened form of the audit record. The fields are:

- dell EMC_vpmx_aud_action_code
- dell EMC_vpmx_aud_activity_id
- dell EMC_vpmx_aud_application_id
- dell EMC_vpmx_aud_function_class
- dell EMC_vpmx_aud_host_name
- dell EMC_vpmx_aud_originator
- dell EMC_vpmx_aud_record_number
- dell EMC_vpmx_aud_text
- dell EMC_vpmx_aud_username

An entry in Log Insight with the fields identified appears in Figure 38.

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

Note that some VMAX and PowerMax events will generate both a regular log entry as well as an audit log entry in Log Insight. Because of the manner in which the VMAX and 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 Log Insight.
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 Log Insight, 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.
As one can see, the first entry has very basic information. The second adds some text which is more useful but the third includes detail on each field available in the record. Although any of these formats could be sent to Log Insight, the VMAX and 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 Log Insight**

As mentioned, the problem with using symaudit is that there is no inherent ability to send the log information to a syslog source. Therefore, a third-party software is necessary. For the most basic functionality, the software needs to be able to send logs to a syslog target. For this example, a product called “NXLOG” was used. It is available as a freeware and touts itself as “…a universal log collector and forwarder supporting different platforms, log sources, and protocols.”

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
```

![Command Prompt](image)

**Figure 40. Symaudit monitor command with verbose output**

Figure 41 is a typical record that will be sent to Log Insight:

---

4 http://www.nxlog.org
Figure 41. Audit entry from symaudit

**NXLOG configuration**

An NXLOG configuration file requires modification to send the audit entries to Log Insight. Here is a sample of the one in this environment:
## This is a sample configuration file. See the nxlog reference manual about the
## configuration options. It should be installed locally and is also available

## 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 VMAX and PowerMax arrays in the environment and audit records are being sent to the same Log Insight environment, there is no field in an audit record that lists the VMAX 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 Log Insight. NXLOG could be configured to even massage the file and remove records that are deemed unnecessary. Such configurations, however, are beyond the scope of this document. See the Solutions Enabler documentation at support.emc.com for more information on symaudit options.

User-defined fields

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

- dellmc_vmax_audit_action_code
- dellmc_vmax_audit_activity_id
- dellmc_vmax_audit_api_library
- dellmc_vmax_audit_api_version
- dellmc_vmax_audit_application_id
- dellmc_vmax_audit_application_version
- dellmc_vmax_audit_client_host
- dellmc_vmax_audit_function_class
- dellmc_vmax_audit_host_name
- dellmc_vmax_audit_offset_in_seq
- dellmc_vmax_audit_os_name
- dellmc_vmax_audit_os_revision
- dellmc_vmax_audit_process_id
- dellmc_vmax_audit_record_number
• dellemc_vmax_audit_records_in_seq
• dellemc_vmax_audit_task
• dellemc_vmax_audit_task_id
• dellemc_vmax_audit_time
• dellemc_vmax_audit_username
• dellemc_vmax_audit_vendor_id

An entry in Log Insight with the fields identified appears in Figure 43.

<table>
<thead>
<tr>
<th>Record Number</th>
<th>: 3454</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records in Seq</td>
<td>: 1</td>
</tr>
<tr>
<td>Offset in Seq</td>
<td>: 1</td>
</tr>
<tr>
<td>Time</td>
<td>: 01/31/14 11:50:26</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>: EMC Corp</td>
</tr>
<tr>
<td>Application ID</td>
<td>: SYMCONFIGURE</td>
</tr>
<tr>
<td>Application Version</td>
<td>: 7.6.1.0</td>
</tr>
<tr>
<td>API Library</td>
<td>: SEK</td>
</tr>
<tr>
<td>API Version</td>
<td>: V7.6.1.0 (Edit Level: 1755)</td>
</tr>
<tr>
<td>Host Name</td>
<td>: WIN-ML3QF40P</td>
</tr>
<tr>
<td>OS Name</td>
<td>: WinNT</td>
</tr>
<tr>
<td>OS Revision</td>
<td>: 6.1.7601Se</td>
</tr>
<tr>
<td>Client Host</td>
<td>:</td>
</tr>
<tr>
<td>Process ID</td>
<td>: 00004740</td>
</tr>
<tr>
<td>Task ID</td>
<td>: 00004728</td>
</tr>
<tr>
<td>Function Class</td>
<td>: CfgChg</td>
</tr>
<tr>
<td>Action Code</td>
<td>: Commit</td>
</tr>
<tr>
<td>Text</td>
<td>: The local CFGCHG COMMIT operation SUCCEEDED</td>
</tr>
<tr>
<td>Username</td>
<td>: H:WIN-ML3QF40POES\Administrator</td>
</tr>
<tr>
<td>Activity ID</td>
<td>: SEd54e85f5d5</td>
</tr>
</tbody>
</table>

source hostname emc_vmax_audit_record_number emc_vmax_audit_records_in_seq emc_vmax_audit_offset_in_seq emc_vmax_audit_task emc_vmax_audit_username 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_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 Log Insight without the --v switch,
e.g. symaudit --sid xx monitor --text, the user-defined fields will not work. User-
defined fields are positional and rely on a pre and post context. As the condensed
versions of the audit log have a different format, the fields cannot be recognized. If a
shorter record is desired, it is best to use the audit entry sent by the event daemon as
explained in the Audit entries and the event daemon section.

Audit record formatting and Log Insight
There are two noteworthy items to mention concerning the symaudit logs as they appear in Log
Insight. The first is to understand that audit messages sometimes come in multiples. Because
the records get written together, they get sent to Log Insight together. For instance, Figure 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.
Figure 44. Audit record with multiple entries

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

Similarly, if there are multiple entries but the first occurrence of the field is NULL, Log Insight will highlight the next entry as in Figure 46 with the user-defined field dell_emc_vmax_audit_api_version.
Figure 46. User-defined fields with multiple entries and a NULL value

**Dashboards**

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

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

An example of this dashboard is shown in Figure 47.
Figure 47. VMAX and PowerMax Content Pack - Auditing dashboard

There are no alerts or queries configured for audit information.