Using the Pure Storage Content Pack for VMware vRealize Log Insight

Cody Hosterman

Solutions Architect vExpert

purestorage.com

Table of Contents

Executive Summary

This document describes the configuration and use of the Pure Storage FlashArray Content Pack for VMware® vRealize™ Log Insight™. Log Insight is a log aggregator and analysis tool that allows administrators to quickly and easily troubleshoot issues and oversee their infrastructure operations from a single, simple-to-use application. The Pure Storage Content Pack provides a plug-in mechanism that enables Pure Storage-aware descriptions and context to Log Insight and its users.

This document is intended for use by pre-sales consulting engineers, sales engineers and customers who want to deploy the Pure Storage FlashArray in VMware vSphere-based virtualized datacenters utilizing Log Insight.

Pure Storage Introduction

Pure Storage is the leading all-flash enterprise array vendor, committed to enabling companies of all sizes to transform their businesses with flash.

Built on 100% consumer-grade MLC flash, Pure Storage FlashArray delivers all-flash enterprise storage that is 10X faster, more space and power efficient, more reliable, and infinitely simpler, and yet typically costs less than traditional performance disk arrays.

Figure 1. FlashArray 400 Series

The Pure Storage FlashArray FA-400 Series is ideal for:

Accelerating Databases and Applications Speed transactions by 10x with consistent low latency, enable online data analytics across wide datasets, and mix production, analytics, dev/test, and backup workloads without fear.

Virtualizing and Consolidating Workloads Easily accommodate the most IO-hungry Tier 1 workloads, increase consolidation rates (thereby reducing servers), simplify VI administration, and accelerate common administrative tasks.

Delivering the Ultimate Virtual Desktop Experience Support demanding users with better performance than physical desktops, scale without disruption from pilot to >1000's of users, and experience all-flash performance for under $100/desktop.

Protecting and Recovering Vital Data Assets Provide an always-on protection for business-critical data, maintain performance even under failure conditions, and recover instantly with FlashRecover.

Pure Storage FlashArray sets the benchmark for all-flash enterprise storage arrays. It delivers:

Consistent Performance FlashArray delivers consistent <1ms average latency. Performance is optimized for the real-world applications workloads that are dominated by I/O sizes of 32K or larger vs. 4K/8K hero performance benchmarks. Full performance is maintained even under failures/updates.

Less Cost than Disk Inline de-duplication and compression deliver 5 – 10x space savings across a broad set of I/O workloads including Databases, Virtual Machines and Virtual Desktop Infrastructure.

Mission-Critical Resiliency FlashArray delivers >99.999% proven availability, as measured across the Pure Storage installed base and does so with non-disruptive everything without performance impact.

Disaster Recovery Built-In FlashArray offers native, fully-integrated, data reduction-optimized backup and disaster recovery at no additional cost. Setup disaster recovery with policy-based automation within minutes. And, recover instantly from local, space-efficient snapshots or remote replicas.

Simplicity Built-In FlashArray offers game-changing management simplicity that makes storage installation, configuration, provisioning and migration a snap. No more managing performance, RAID, tiers or caching. Achieve optimal application performance without any tuning at any layer. Manage the FlashArray the way you like it: Web-based GUI, CLI, VMware vCenter, Rest API, or OpenStack.

Pure Storage FlashArray FA-400 Series includes FA-405, FA-420, and FA-450. A FlashArray is available for any application, and any budget!

	FA-405	FA-420	FA-450
FRONT VIEW (dual controllers)			
REAR VIEW (dual controllers)			
CAPACITY	• Up to 40+ TBs effective capacity • 2.75-11 TBs raw capacity	• Up to 125+ TBs effective capacity • 11-35 TBs raw capacity	• Up to 250+ TBs effective capacity • 34-70 TBs raw capacity
	Effective capacity assumes HA, RAID, and metadata overhead, GB-to-GiB conversion, and includes benefit of data reduction with always-on inline deduplication, compression & pattern removal. Average data reduction is calculated at 6-to-1. Some customers see data reduction in excess of 20-to-1. Effective capacity has no upper limit and will vary depending on workload.		
PERFORMANCE	• Up to 100,000 **32K** IOPS @ <1ms average latency • Up to 3 GB/s bandwidth	• Up to 150,000 **32K** IOPS @ <1ms average latency • Up to 5 GB/s bandwidth	• Up to 200,000 **32K** IOPS @ <1ms average latency • Up to 7 GB/s bandwidth
	Why does Pure Storage quote 32K, not 4K IOPS? The industry commonly markets 4K IOPS benchmark to make numbers look high, but real-world environments are dominated by IO sizes of 32K or larger. Pure Storage has optimized the FlashArray for the real-world. FlashArray adapts automatically to 512B-32KB IO for superior performance, scalability, and data reduction.		
HOST CONNECTIVITY	• 8 Gb/s Fibre Channel • 10 Gb/s Ethernet iSCSI • Replication ports	• 8 Gb/s Fibre Channel • 10 Gb/s Ethernet iSCSI • Expansion slot (FC or iSCSI) • Replication ports	• 16 Gb/s Fibre Channel • 10 Gb/s Ethernet iSCSI • Expansion slot (FC or iSCSI) • Replication ports

Figure 2. Pure Storage FlashArray 400 Series Specifications

Introduction to VMware vRealize Log Insight

VMware vRealize Log Insight provides real-time log administration for heterogeneous environments that span across physical, virtual and cloud environments. Log Insight provides:

- Universal Log Collection
- Powerful Log Analytics
- Enterprise-class Scalability
- Ease of Use and Deployment
- Built-in vSphere Knowledge

Log Insight collects and analyzes all types of machine-generated log data, including application logs, network traces, configuration files, messages, performance data and system state dumps. Administrators can connect it to everything in their environment—operating systems, applications, storage, firewalls, network devices or something else—for enterprise-wide visibility via log analytics.

Log Insight delivers highly-customizable queries and aggregations that add structure to all types of unstructured log data, so administrators can quickly troubleshoot, without needing to know the data beforehand. These queries are leveraged by dashboards to create stored queries, reports and alerts. With Log Insight administrators can gain a deep understanding by correlating events across massive and complex environments, reducing troubleshooting duration and improving operational efficiency.

Log Insight is easy to deploy due to the virtual appliance deployment scheme. No building, configuring and licensing operating systems to host Log Insight is required. Log Insight offers a GUI-based interface to make simple-to-run, yet powerful, interactive searches, as well as deep analytical queries providing immediate and improved IT operational efficiency. Log Insight automatically chooses the best visualization for your data, saving you valuable time

Log Insight comes with built-in knowledge and native support for VMware vSphere® with vRealize Operations Management™. With this tight integration Log Insight is undoubtedly one of the best solutions for a VMware environment.

The Pure Storage Content Pack for vRealize Log Insight

VMware vRealize Log Insight allows partners to create integration plugins referred to as Content Packs to provide additional intelligence into Log Insight. Content Packs are customized by various partners to be distributed to users of Log Insight that include custom queries, dashboards, alerts and fields. These custom properties are created in context of the source system sending syslog messages (whether it be a storage array, an application or otherwise. By allowing partners to create these Content Packs, customers can easily begin to leverage Log Insight with their source IT objects with little configuration. Content Pack reduce initial configuration because the partner has created them with the most important metrics, events and alerts in mind therefore doing most of the initial legwork for you. The partners know the syntax, fields and the message types their systems send. So the Content Pack can do the heavy lifting and decide what is most important, what should be noted and how they can be displayed. This is achieved by built-in Log Insight objects such as queries and dashboards in the Content Pack. Customers then can just plug-in the Content Pack and begin analyzing their environment.

The Pure Storage Content Pack includes:

- Four dashboard groups including twenty-two dashboard widgets
- Twenty-seven extracted fields
- Six custom alerts
- Two pre-created queries

Pure Storage Content Pack Requirements

The Pure Storage Content Pack requires the following:

- VMware vRealize Log Insight 2.5
- Pure Storage FlashArray 400 series (405, 420 or 450)
- Purity 4.0[1]

Configuring the Pure Storage Content Pack

Configuration of the Pure Storage Content Pack is a three-part process:

1. Download the Content Pack from VMware's Solution Exchange or from within Log Insight in the Marketplace.
2. Install the Content Pack into Log Insight
3. Configure one or more FlashArrays to send syslog messages to Log Insight

[1] Certain functionality requires Purity 4.1.0+, but the content pack functions fine on 4.0.x.

Downloading and Installing the Pure Storage Content Pack

The Pure Storage Content Pack can be downloaded from the VMware Solution Exchange at https://solutionexchange.vmware.com/store/loginsight. They can also be downloaded directly inside of Log Insight from the Marketplace:

Figure 3. Log Insight Marketplace for Content Packs

Or download the Content Pack named "Pure Storage – FlashArray.vlcp". To import the Content Pack into Log Insight navigate to the Content Pack section in the upper-right hand corner of the Log Insight web interface.

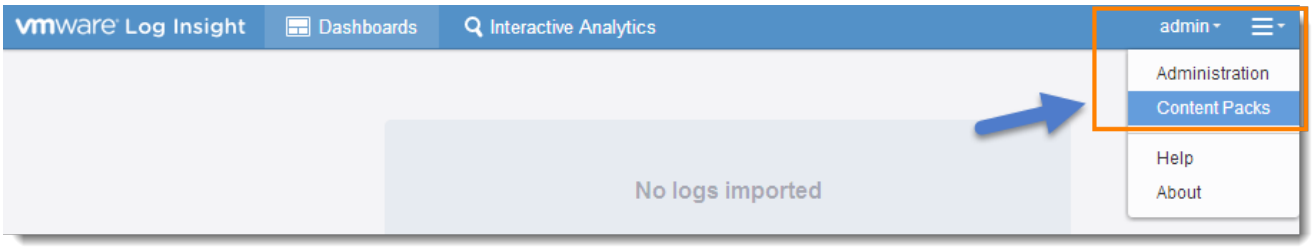
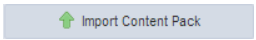


Figure 4. Locating the Content Pack section

In the lower-left hand corner of the screen select the "Import Content Pack" button 

and browse to the Pure Storage vlcp file. The import allows the user to either import it globally or just for their own personal use. Either is fine, but if others would like access to the Content Pack it is best to import it as a Content Pack (globally).

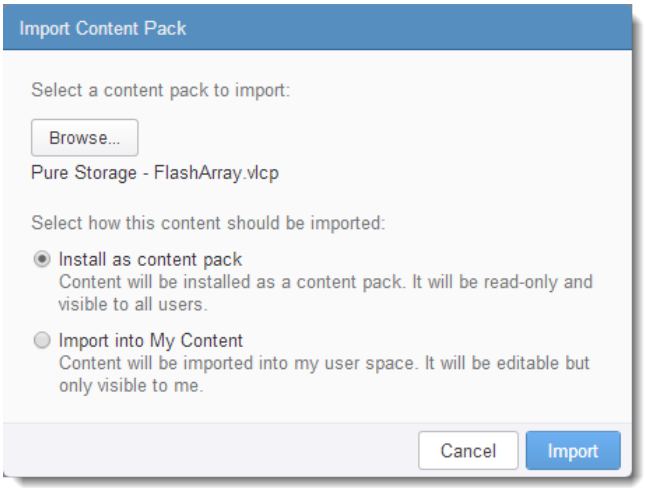


Figure 5. Importing the Pure Storage Content Pack

The Content Pack will automatically appear granting all users access to the built-in dashboards, alerts and extracted fields.

Figure 6. Pure Storage Content Pack successfully imported

Upgrading the Pure Storage Content Pack

For users of the previous (1.0) version of the Pure Storage Content Pack upgrading to the newest version is extremely simple.

If the previous content pack was imported as a content pack and not into the user space, download the content pack in either of the methods described in the previous section and import the new version. Log Insight will recognize the previous content pack was installed and if the “Import as a Content Pack” is chosen, the newer content pack will replace the old version. All of the existing functionality will remain, but with the upgraded dashboards, alerts and extracted fields.

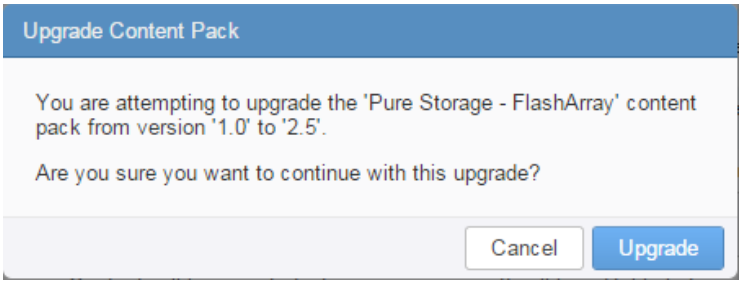


Figure 8. Upgrading the Pure Storage Content Pack

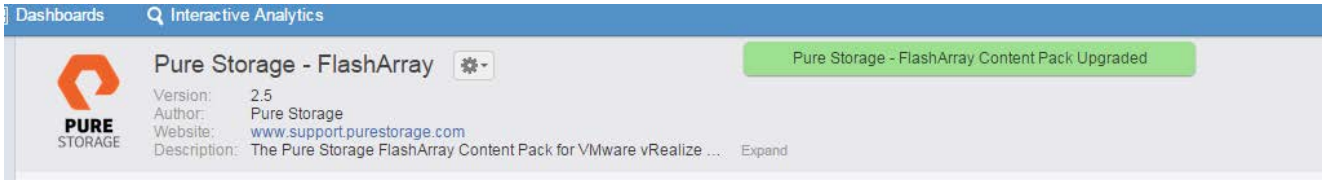


Figure 7. Upgraded Content Pack

If the previous content pack was imported into the user space, Log Insight will not be able to replace previous extracted fields/dashboards/alerts with the newer ones. Instead it will have both co-exist with the newer objects having numbers appended to distinguish them.

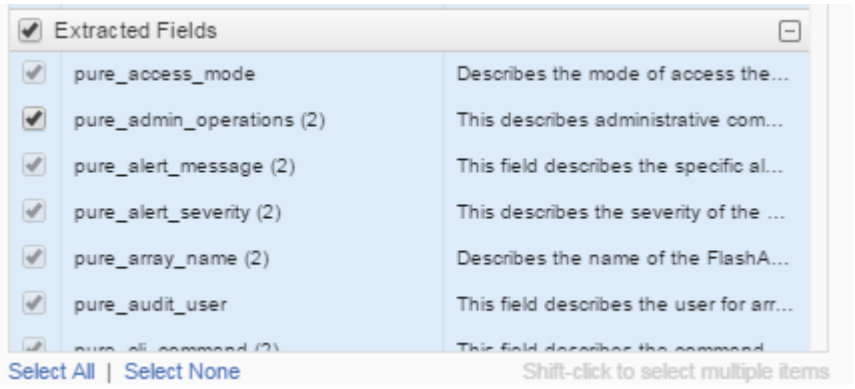


Figure 9. Duplicate extracted fields

It is recommended to delete the older objects first before importing the new content pack to maintain a clean Log Insight instance. Often the newer versions of extracted fields (and the objects using them) are more efficient, faster and/or more accurate.

Configuring a FlashArray to Send Syslog Messages

In order to get FlashArray information into Log Insight, the Log Insight IP or FQDN must be configured into the FlashArray syslog server. The simplest method for this is to use the Pure Graphical User Interface. For instructions on using the Pure CLI refer to the FlashArray User Guide.

First identify the IP address (or FQDN) of the Log Insight instance. For the example in this document, the IP of Log Insight is 10.124.6.27. Once identified, login to the Pure GUI of your FlashArray using the Virtual IP of the array and authorized credentials (using privileges higher than read-only). Navigate to the System tab, followed by the Configuration page and then the Syslog Server sub-entry as seen in the below figure.

Figure 10. Locating the Syslog Server target host entry

Log Insight supports three different port/protocol combinations:

- TCP Port 514
- UDP Port 514
- TCP Port 1514

The FlashArray Syslog Server supports all of these combinations so choose the appropriate one for your environment. For this example TCP Port 514 will be used. Enter the IP or FQDN in the format like below:

tcp://<IP or FQDN>:514

If there is already a syslog target there, append the Log Insight address to the list in a comma-separated fashion. After entering the address in the entry box, click the black check mark to save it and then click the test button that appears below the entry box. This will send a test message to Log Insight immediately. If the message does not appear, check the syntax and accuracy of the address/port/protocol and firewall settings between the FlashArray and the Log Insight Appliance.

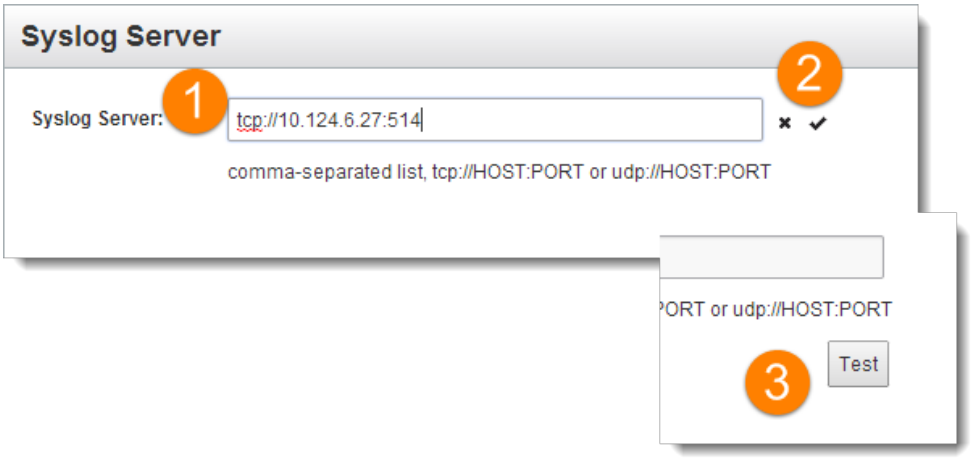


Figure 11. Entering a Log Insight instance as a target syslog client

The test message will look similar to message in the image below:

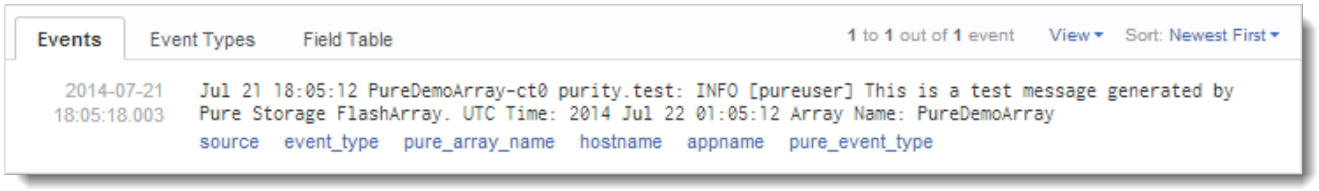


Figure 12. Pure Storage FlashArray Test Syslog Message

Understanding the Pure Storage Content Pack

As mentioned before, the Pure Storage Content Pack offers a variety of queries, dashboards and alerts tailored for the specific information end-users need to know arising from a FlashArray.

Besides the syslog messages themselves, everything within Log Insight is built upon extracted fields. Extracted fields are descriptions of pieces of information that commonly appear inside a syslog message (like an array name or a volume name). Without extraction, Log Insight does not have any assigned relevance to most parts of a syslog message and will see it as just jumbled pieces of text with no meaning. Therefore, various important items must be extracted and Log Insight must be "taught" how to recognize them as something like an array name in order to provide meaning and further analysis. While an end-user does not *need* the Content Pack, the creator of the Content Pack has already extracted all of the important fields, saving valuable time.

A field is extracted like so. Below is a sample syslog message about a volume being created.

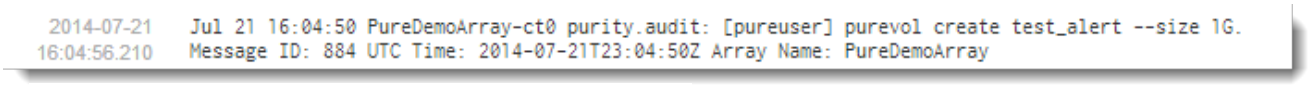


Figure 13. Syslog message about volume creation

It is known that in FlashArray syslog messages the user account running a given operation will always be indicated directly after purity.audit and contained in brackets. To extract the field, highlight the user name (pureuser in this case) and click the "Extract Field" option that appears in the pop-up menu.

Log Insight will attempt to recognize patterns and types of values for you and suggest information that will allow

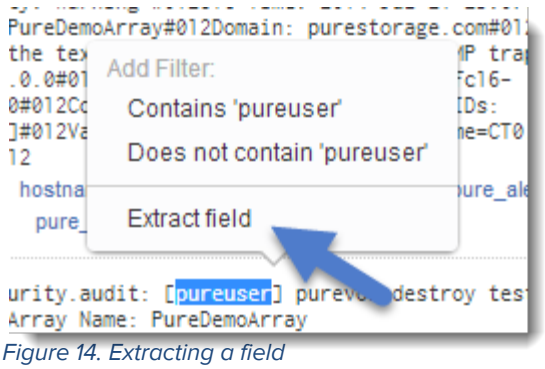


Figure 14. Extracting a field

it to always find the selected field from FlashArray messages. While often accurate, it may need to be improved to make sure nothing is accidentally marked as a user name (a false positive) that could lead to skewed data analysis. Once extract field has been selected an edit screen will appear on the right side of the screen in Log Insight.

Log Insight provides a comprehensive set of indicators to describe a field which are called regular expressions or regex for short. Detailed discussion of these is out of the scope of this document, but refer to VMware documentation for more information. For the above example, it is known that the word "audit" followed by a space and a start bracket will always precede the user name and will be followed by an end bracket. Therefore anything in the middle will be the user name. Assign the field a name and Log Insight will now allow you to easily run queries against Pure Storage FlashArray user names. Note that if you have the Content Pack installed, this has already been done for you.

Pure Storage Content Pack Extracted Fields

The Pure Storage Content Pack contains twenty-seven pre-configured extracted fields that are used by the built-in dashboards and alerts and can be further utilized by users to create their own. These fields are described below.

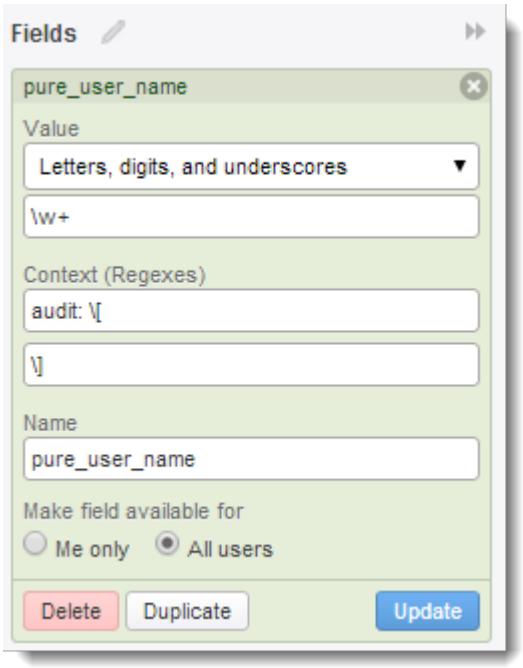


Figure 15. Configuring an extracted field

Extracted Field	Description
• pure_access_mode	Describes the mode of access the user is leveraging to communicate or control the array. Most common options are either through the GUI, CLI or via the REST API.
• pure_admin_operations	This describes administrative commands run against an array. These are configuration changes on the array that do not involve hosts or volumes.
• pure_alert_message	The message from a hardware issue. An example would be “Ethernet failure”.
• pure_alert_severity	This is the severity of a given alert, possibilities are critical, warning or info.
• pure_array_name	The name of the source array for a given message.
• pure_cli_command	The Purity CLI base command that was used in a given operation. This would be purevol, purehgroup etc.
• pure_delayed_pgroup	This field describes the name of a protection group with delayed replication.
• pure_event_type	This is the type of message, possibilities are audit, alert or test. Audit messages are commands run by a user,

	alerts are typically environmental situations such as loss of power.
• pure_failed_hardware	This is the specific hardware component that is experiencing trouble. The component itself may not be bad, but it could be an unplugged cable leading to it or something similar. An example would be “SH0.PWR0”, which would be SSD Shelf 0 Power Supply 0.
• pure_hgroup_name	The name of a host group involved in the syslog message describing a configuration change of a host group such as adding a host or connecting a volume.
• pure_hgroup_operations	The specific command for a configuration change operation executed against a host group such as adding a host or connecting a volume.
• pure_host_name	The name of a host involved in the syslog message describing a configuration change to a host such as deleting a host or connecting a volume.
• pure_host_operations	The specific command for a configuration change operation executed against a host such as deleting a host or connecting a volume.
• pure_hostvol_name	The volume name involved in a host group or host group change. This is typically a connect or disconnect operation.
• pure_percent_full	When the FlashArray begins to exhaust its physical capacity it will syslog a warning with a percent full number. This is typically only reported via syslog when it is at 80% and above.
• pure_pgroup_name	The name of a protection group involved in the syslog message describing a configuration change of a protection group such as creation or replicate now.
• pure_pgroup_objectchange	This field describes the type of object change occurring to a FlashRecover protection group. This can be the removal or addition of one or more volumes, hosts, host groups or FlashArray targets.
• pure_pgroup_objectname	This field describes the name of the FlashRecover protection group object being managed. This could be a volume, a host, a host group or a target FlashArray. This object is either being added or removed. This could represent one object or a space-separated list of them.
• pure_pgroup_operations	The specific command for a configuration change operation executed against a protection group such as changing a replication scheme or deletion of a group.
• pure_purity_version	Version of Purity running on the source array. Note that this will not be included in all syslog messages. An example would be “4.0.0”.
• pure_replicate_frequency	This field describes the remote replication frequency of a FlashRecover protection group.
• pure_setattr_operations	Most Purity CLI commands have a command option

	called setattr that changes advanced the configuration of a given object. This describes the parameter that precedes any use setattr.
• pure_snapshot_frequency	This field describes the local snapshot frequency of a FlashRecover protection group.
• pure_user_name	For any user-initiated operation this field describes the user who executed the command.
• pure_volume_name	The name of the volume in any volume management operation.
• pure_volume_operations	The command parameter that follows any “purevol” command, such as delete, create or eradicate.

These extracted fields comprise the basic building block of the Pure Storage Content Pack and are leveraged to create the remaining Log Insight objects. While these should cover the vast majority of a user’s needs, further fields can be extracted from FlashArray syslog messages for more specific cases.

These fields are used in the Content Pack to create custom queries, alerts and dashboards and will be discussed later in this document.

Using the Pure Storage Content Pack Extracted Fields

A user can leverage the built-in extracted fields (or extract their own in addition to them) to create their own queries, dashboards and alerts. Advanced query, dashboard and alert construction is beyond the scope of this document but a quick example on how to leverage the built-in fields is described below.

Once the Content Pack has been installed in Log Insight the custom extracted fields will be available. It is important to note that the fields will only appear on the right-hand side of the screen if the syslog results currently shown include those fields. If the results do not include anything that matches the extracted fields the fields will be hidden until one does.

Navigate to the Interactive Analysis pane within Log Insight to see the latest syslog messages. By default the screen will only display messages received in the last five minutes. This can be changed via drop-down in the search panel to standard intervals or a custom time period.

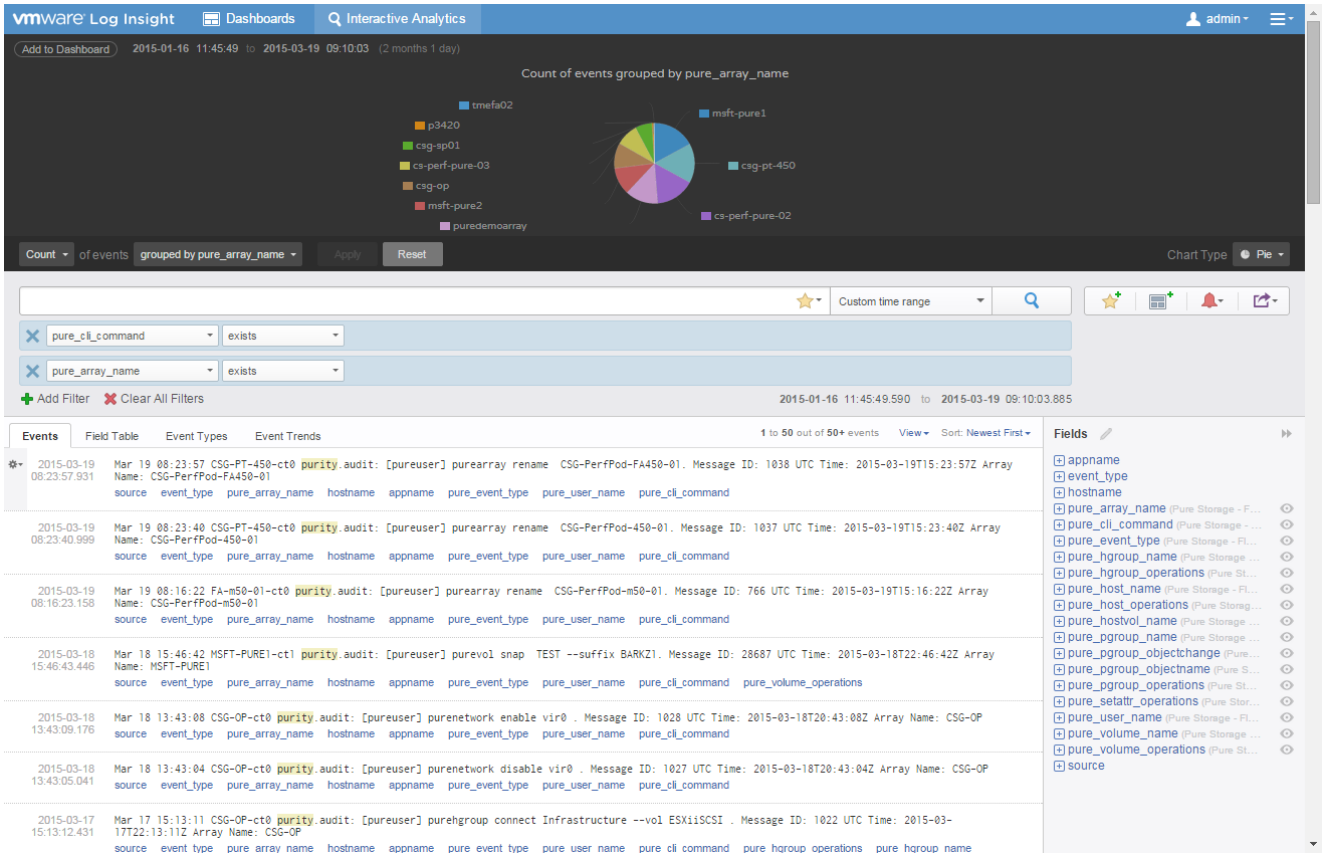


Figure 16. Pure Storage Extracted Fields

In this situation, for example, let's say an administrator wants to know of every time the user "cody" executed a "purevol eradicate" operation on any FlashArray. In order to find this out, the extracted fields built-in to the Content Pack will need to be used via filtering. Under the search box select add filter.

Four filters will need to be created:

1. One that searches for messages only involving a FlashArray.
2. One that searches for a Purity user named “cody”.
3. One that searches for instances of “purevol”
4. One that searches for instances of “eradicate”

When a filter is added, the user can decide what that filter includes (or excludes) in the results. The options in the filter creation line allow for the selection of the Pure Storage extracted fields to be leveraged directly in the filter. The four above filters will be created as described.

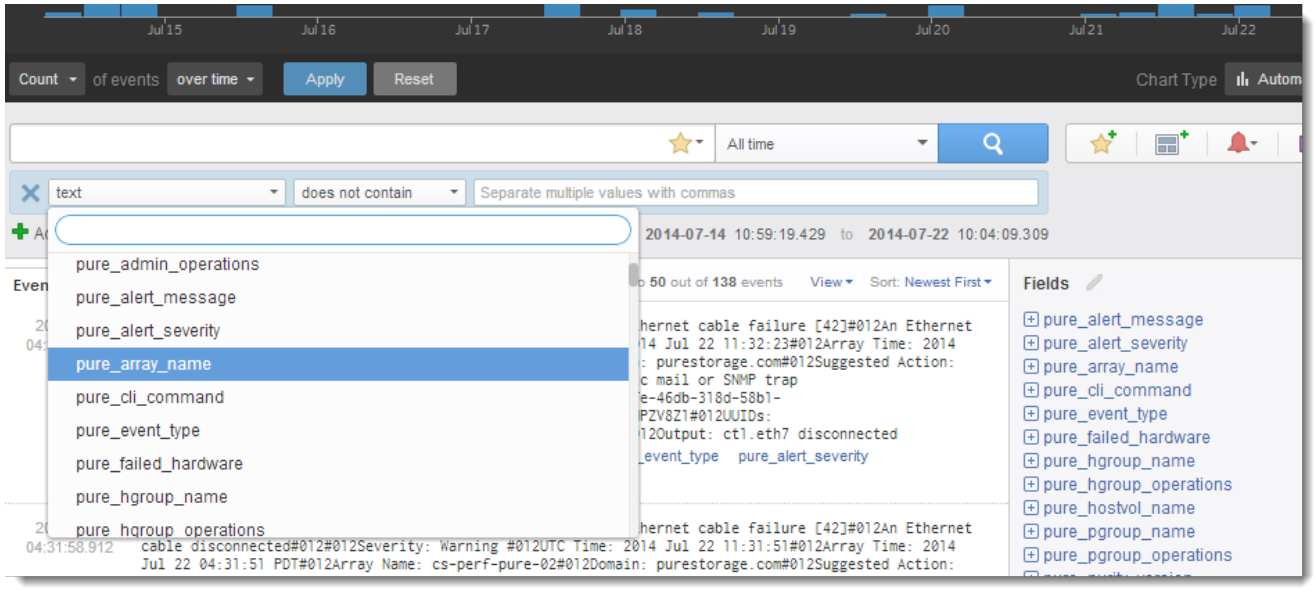


Figure 17. Creating a filter based on Pure Storage Extracted Fields

When selecting an extracted field, Log Insight provides six matching operations for whatever value you provide in the attribute field. These are:

- Contains
- Does not contain
- Starts with
- Does not start with
- Matches regex
- Exists

Detailed descriptions of these options are available in VMware documentation. The following image shows the four filters required to deliver the desired results.

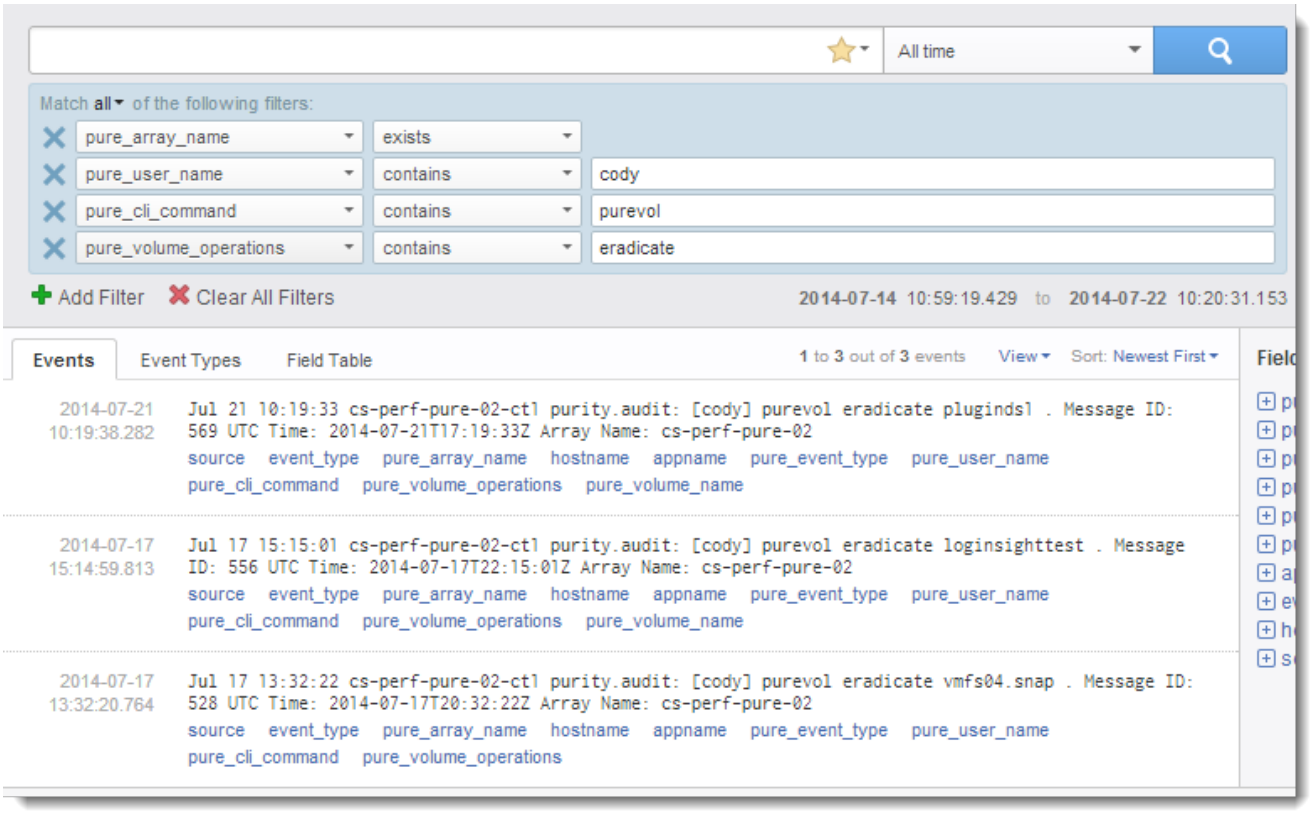


Figure 18. Custom filtering using the Pure Storage Extracted Fields

These results can now be turned into a dashboard or even an alert-triggering event. Once the filters have been created and the search executed, Log Insight automatically lists the matching syslog messages below and creates a graphical view above. If the query/graphical view is something that a user would want to save, they can click the “Add to Dashboard” button in the top left to save it to the dashboard view for repeated viewing (and it will be updated as new matching messages come in).

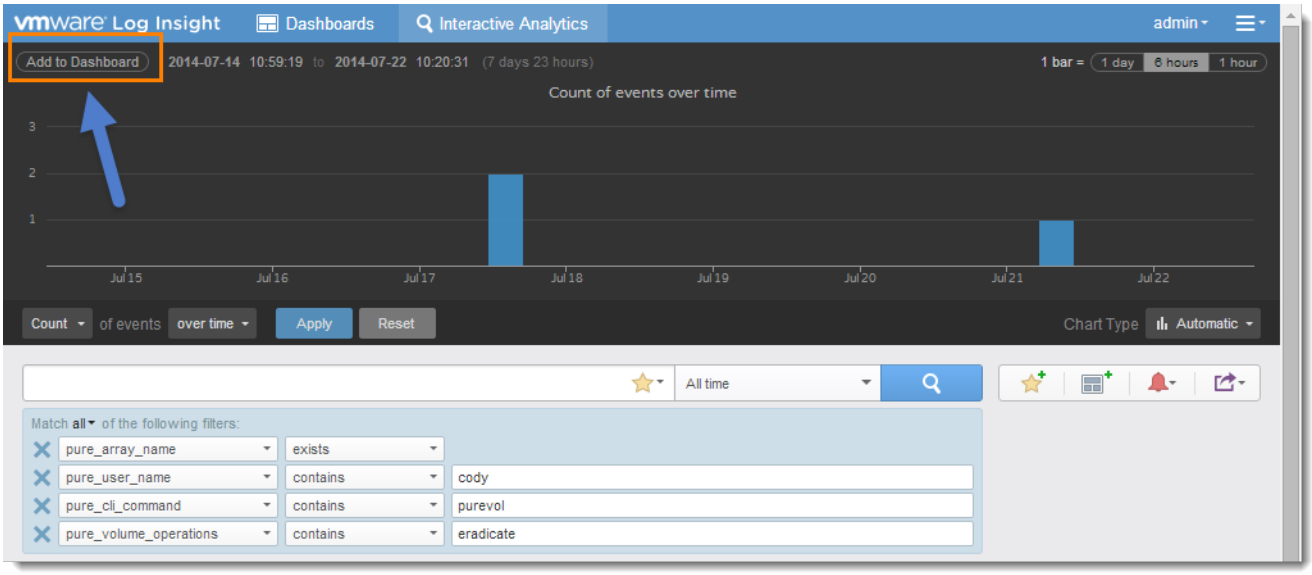


Figure 19. Creating a dashboard from Pure Storage Extracted Fields

Furthermore, an alert can be created so that Log Insight sends an email to an administrator or even a message to VMware Realize Operations Manager whenever a new message comes in that matches the query criteria.

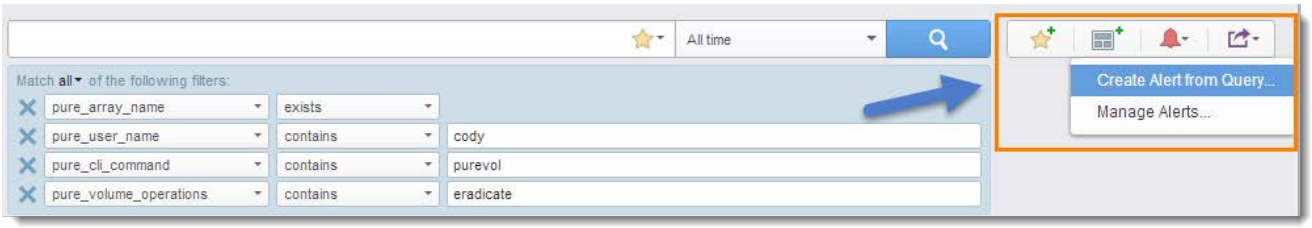


Figure 20. Alert Creating an alert from a query based on Pure Storage Extracted Fields

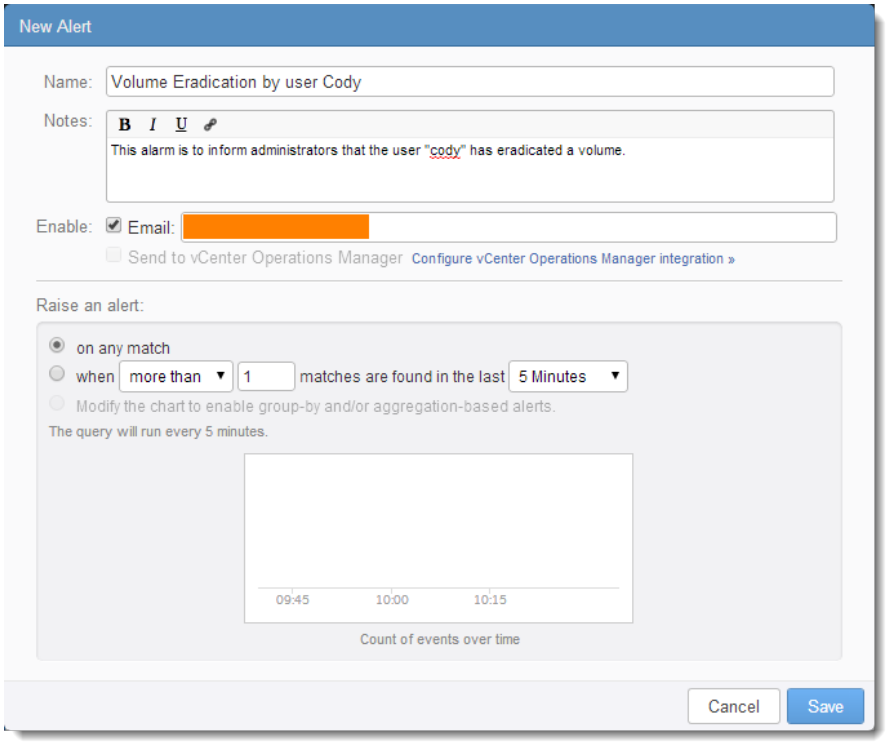


Figure 21. Creating a Log Insight

Once saved an email will be sent (or a message to vROps if selected) to indicate that a new query match has been received. In the example email below it can be see that user “cody” eradicated a volume named “loginsighttest”.

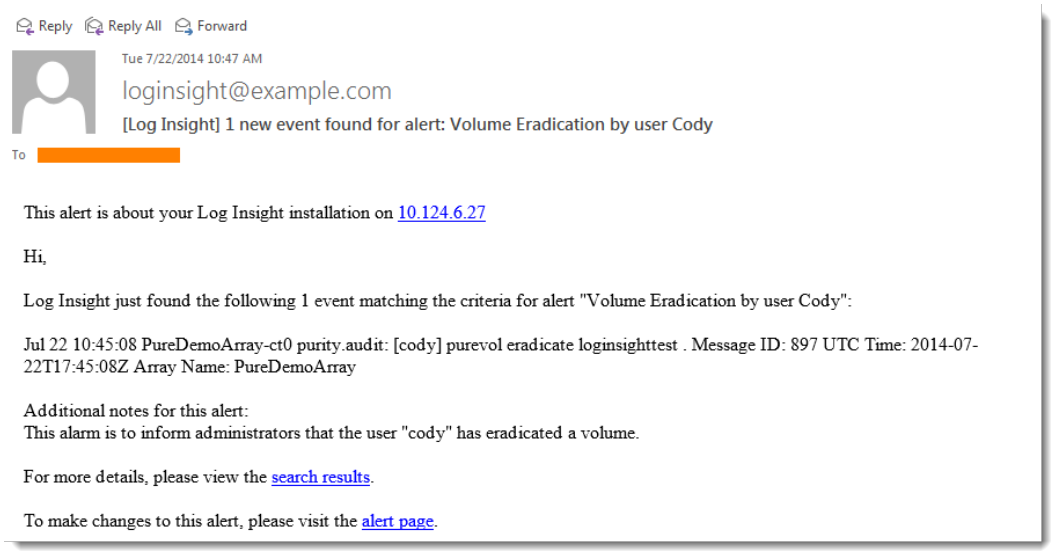


Figure 22. Email alert from Log Insight

Pure Storage Content Pack Dashboards

The Pure Storage Content Pack includes a variety of dashboards specifically tailored for the FlashArray to show important, relevant and useful events by default. The Content Pack includes four dashboard groups:

1. **Overview**— this dashboard group includes chart widgets that describe common and important messages such as number of arrays, alerts and user activity.
2. **Hardware**— this dashboard group includes chart widgets that describe hardware-related events such as cable failure or disconnection and power loss.
3. **FlashRecover**— this dashboard group includes chart widgets that describe replication-related functions such as protection group creation and management, local snap management and remote replication events.
4. **Auditing**— this dashboard group includes chart widgets that display more detailed audit trail information such as volume or host management.

The dashboards can be accessed by navigating to the dashboard screen and choosing the "Pure Storage – FlashArray" dropdown from the list in the upper-left portion of the screen.

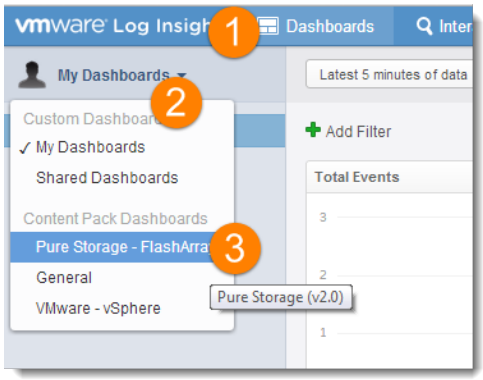


Figure 23. Opening the Pure Storage dashboards

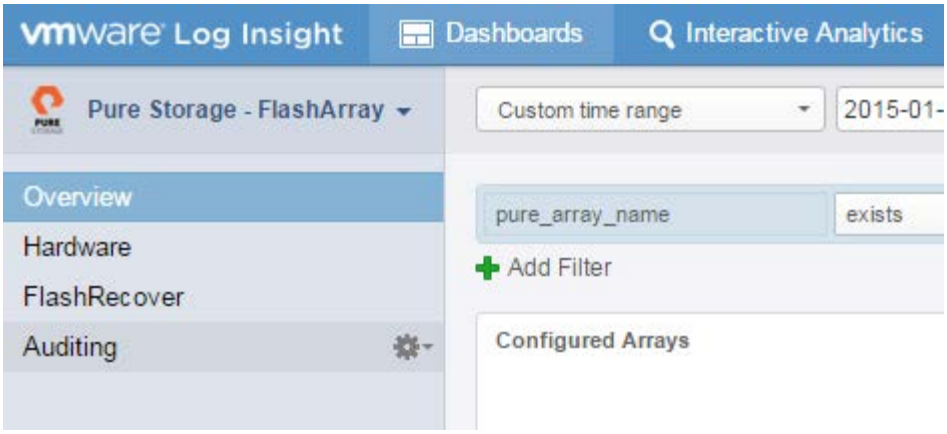


Figure 24. Pure Storage dashboard groups

Each dashboard group has individual chart widgets within them. Each widget is described below.

Overview Dashboard Group

The following section describes the five chart widgets included in the Overview Dashboard Group.

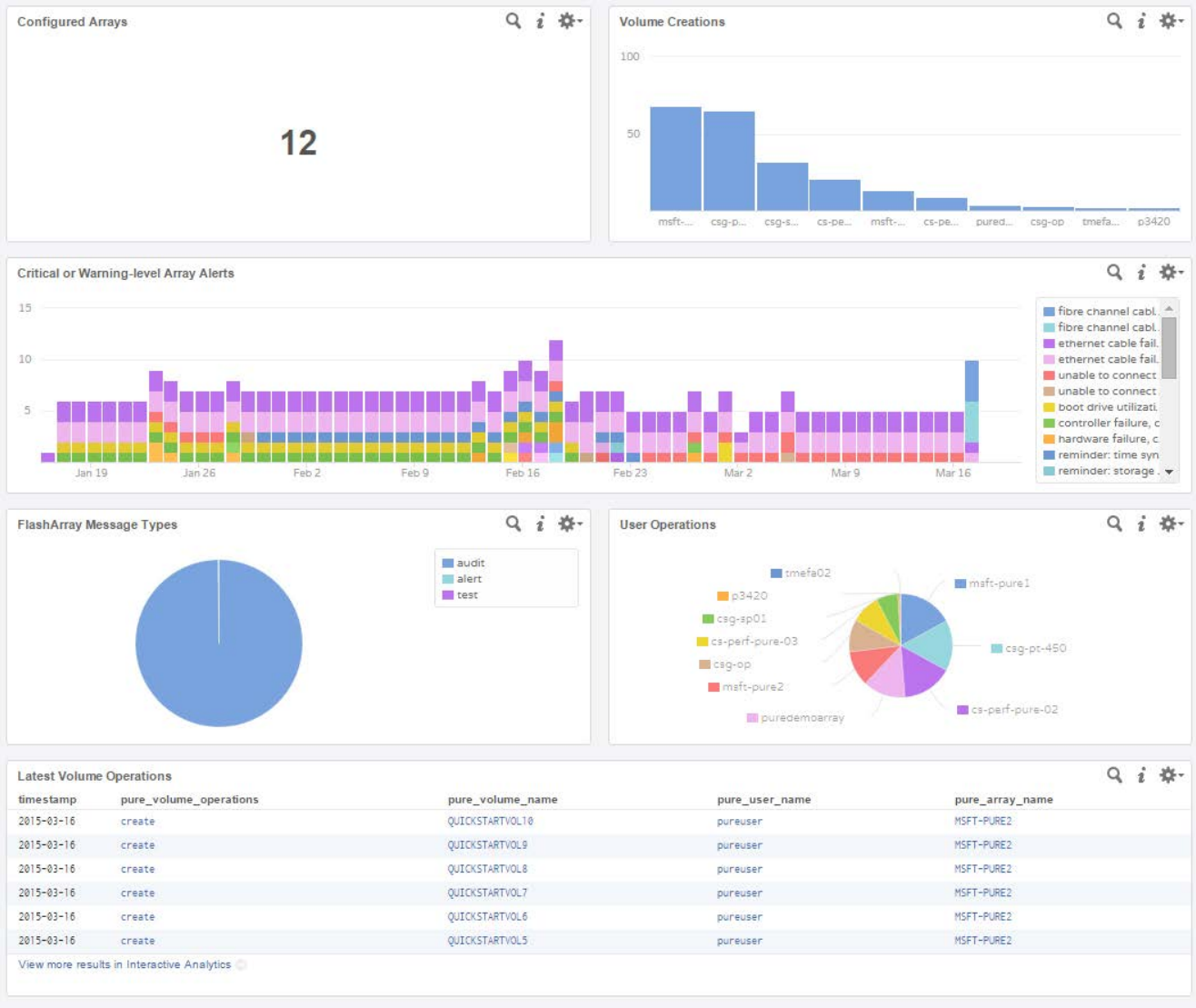


Figure 25. Overview Dashboard Group

Configured Arrays: This dashboard widget shows the number of Pure Storage FlashArrays currently sending syslog messages to this Log Insight instance. If the number is lower than expected it is possible that an array hasn't had anything to syslog let (we recommend always sending a test message when configuring syslog on the FlashArray the first time to prevent this situation) or the syslog feature has not been accurately configured or not all. Drill down further by opening the dashboard widget in Interactive Analysis mode. Find the array that is not present in the Interactive Analysis and ensure proper configuration. Then try a test syslog message from the given array. If no messages appears check firewall settings between the FlashArray controllers and the Log Insight instance. If the number is higher than expected, this means either an array was removed but Log Insight still has its messages or an existing array was renamed. A rename would cause the Content Pack to see this as a new array.

Volume Creations: This dashboard widget shows a count of volume creations across all connected arrays in the selected time period. By clicking on the view in Interactive Analysis mode users can drill down and see when and what volumes were created. This number is not decremented by deletions/eradications and may not reflect the total number of existing arrays if volumes were created prior to syslog configuration to Log Insight.

Critical or Warning-level Array Alerts: This dashboard widget shows all alerts with the severity of “warning” or “critical”. All instances of the alerts should be investigated and resolved immediately. High concentrations of these alerts on a given day or time period indicate a large (usually) environmental issue.

FlashArray Message Types: This dashboard widget shows the counts of the type of messages the FlashArray(s) have sent. These can be audit messages (user actions), alerts (failures) or tests. The large majority (if not all) should be audit messages—a high percentage of alert-type messages usually indicates an on-going environmental problem that has been introducing continuous issues.

User Operations: This dashboard widget shows the user activity of each connected FlashArray as a proportion of the whole in the form of a pie graph.

Latest Volume Operations: This dashboard widget shows a list of the last volume-related operations on the configured FlashArrays. The date, operation, volume name, user name and FlashArray is listed.

Hardware Dashboard Group

The following section describes the five chart widgets included in the Hardware Dashboard Group.

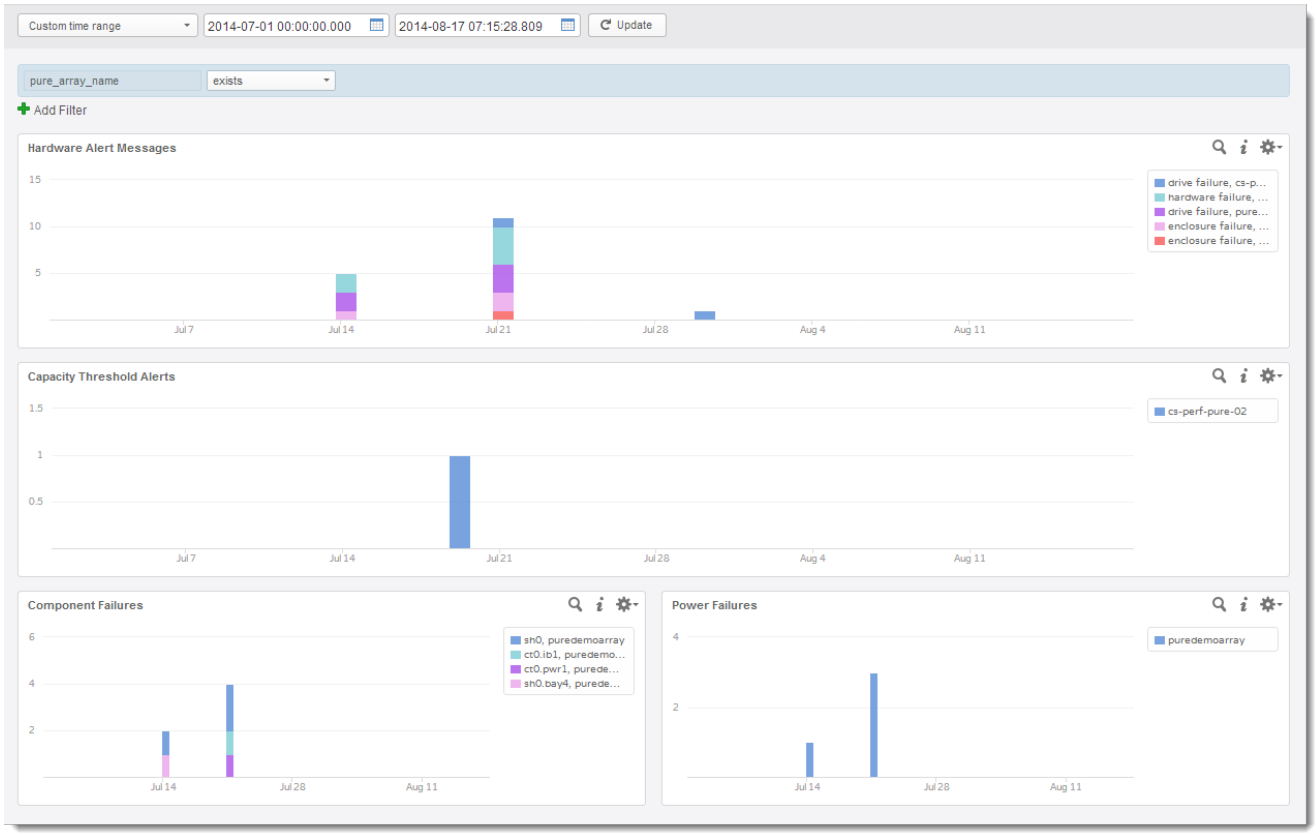


Figure 26. Hardware Dashboard Group

Hardware Alert Message: This dashboard widget shows the count of critical hardware events across all FlashArrays at a certain time. If any of these alerts appear for a given array, immediately take action to resolve them. Which exact component failed may not be known, but this dashboard widget can help diagnose it further. The results are sorted by the failure message and FlashArray name: <failure message, array name>. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Capacity Threshold Alerts: This dashboard widget shows capacity threshold alerts from the FlashArray. If any of these alerts appear for a given array immediately take action to resolve them. Possible remediation options are issuing UNMAP from supported hosts to reclaim dead space or adding physical capacity to the array by adding new SSDs or entire shelves. Refer to your Pure Storage support team for assistance. The results are sorted by FlashArray name. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Component Failures: This dashboard widget shows exact component hardware failures across all FlashArrays at a certain time. If any of these alerts appear for a given array immediately take action to resolve them. This dashboard widget indicates the general location (controller # or shelf #) and specific location (such as ib1 which is Infiniband Connection 1). Refer to the Pure Storage GUI for the physical location of the failure. The results are sorted by failed component and FlashArray name <failed component, array name>. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Power Failures: This dashboard widget shows power component hardware failures across all FlashArrays at a certain time. If any of these alerts appear for a given array immediately take action to resolve them. This dashboard widget indicates the general location (controller # or shelf #) and specific location (such as pwr1 which is Power Connection 1). Refer to the Pure Storage GUI for the physical location of the failure. Failures may be the result of a power supply failure, cord failure/removal or loss of general power. The results are sorted by failed power component and FlashArray name <failed power component, array name>. Drill down further by opening the dashboard widget in Interactive Analysis mode.

FlashRecover Dashboard Group

The following section describes the five chart widgets included in the Replication Dashboard Group.

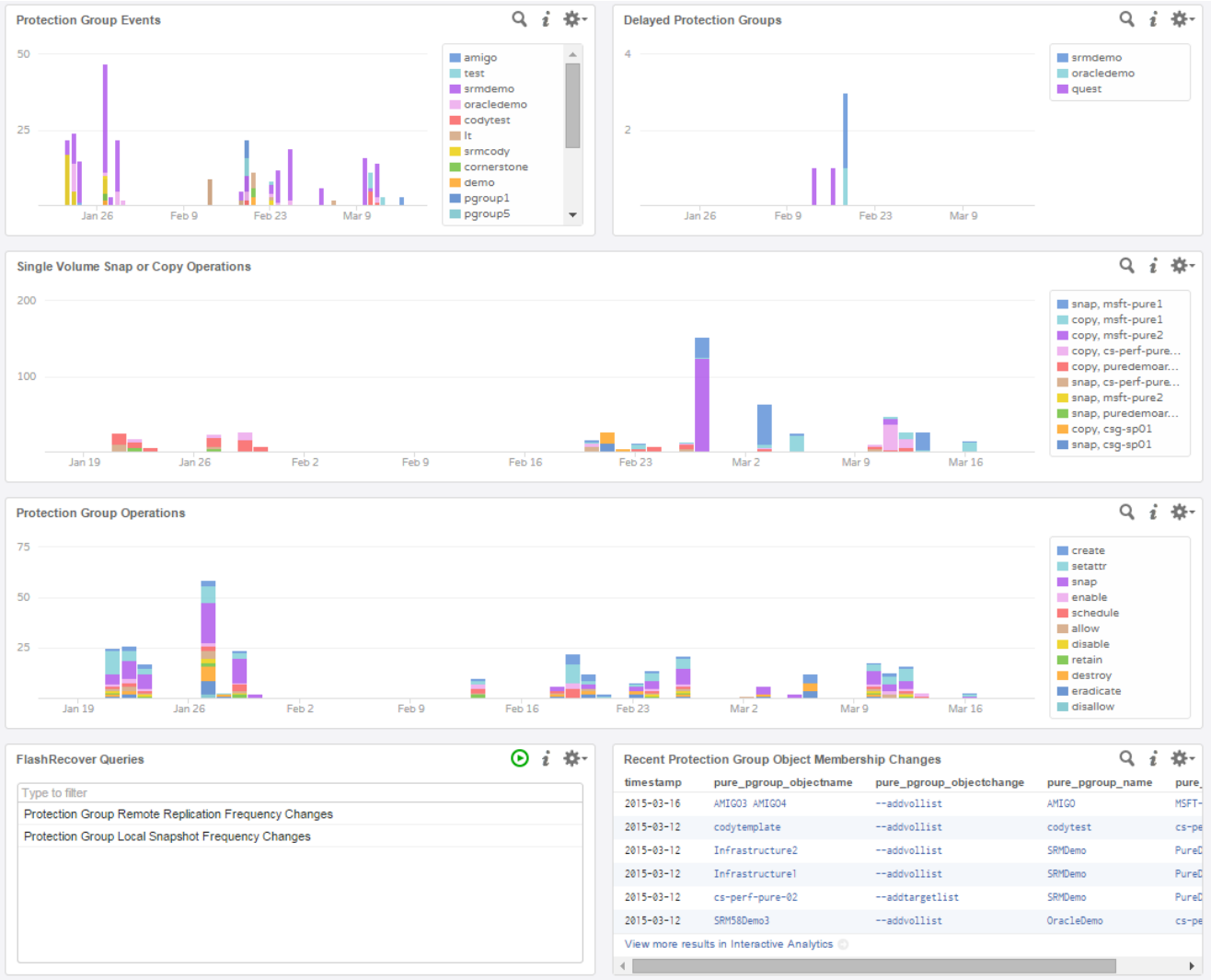


Figure 27. Replication Dashboard Group

Protection Group Events: This dashboard widget shows how many operations were executed on a given protection group at a certain time. Protection groups are groupings of FlashArray volumes that provide a local and remote replication schedule. Analyze this chart for changes to protection groups. The results are sorted by protection group name. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Delayed Protection Group: This dashboard widget shows particular protection groups that, for whatever reason, could not achieve their configured remote replication time interval. This could be due to a too aggressive replication schedule (too frequent replication), disconnected remote array or bandwidth issues. When a protection group is delayed investigate the reason for the delay and remediate as necessary.

Single Volume Snap or Copy Operations: This dashboard widget shows when (if any) single volume local clone or snap operations were executed on a FlashArray at a certain time. Clone operations copy directly from volume to volume and snap operations simply create a Point-In-Time metadata snap of a source volume. The results are

sorted by purevol command (snap or copy) and the FlashArray name <operation, array name>. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Protection Group Operations: This dashboard widget shows what protection group operations were executed across all FlashArrays at a certain time. Protection groups are groupings of FlashArray volumes that provide a local and remote replication schedule. This is a simple chart to allow for analysis of specific protection group operations--it is a more granular view than the Protection Group Events widget. The results are sorted by protection group command operation (enable, create, allow etc.) Drill down further by opening the dashboard widget in Interactive Analysis mode.

FlashRecover Queries: This dashboard widget lists some pre-defined queries one might want to run frequently. These are included in the content pack. The two included queries are for remote replication frequency changes and local snapshot schedule changes. These will report what the new frequency is, what protection group and who made the change.

Recent Protection Group Object Membership Changes: This dashboard widget lists the latest objects that have been added or removed from a protection group. This can include a volume, a host, a host group or a target FlashArray. The list includes, the time, the object name, the type of change, the protection group name and the FlashArray name.

Auditing Dashboard Group

The following section describes the five chart widgets included in the Auditing Dashboard Group.

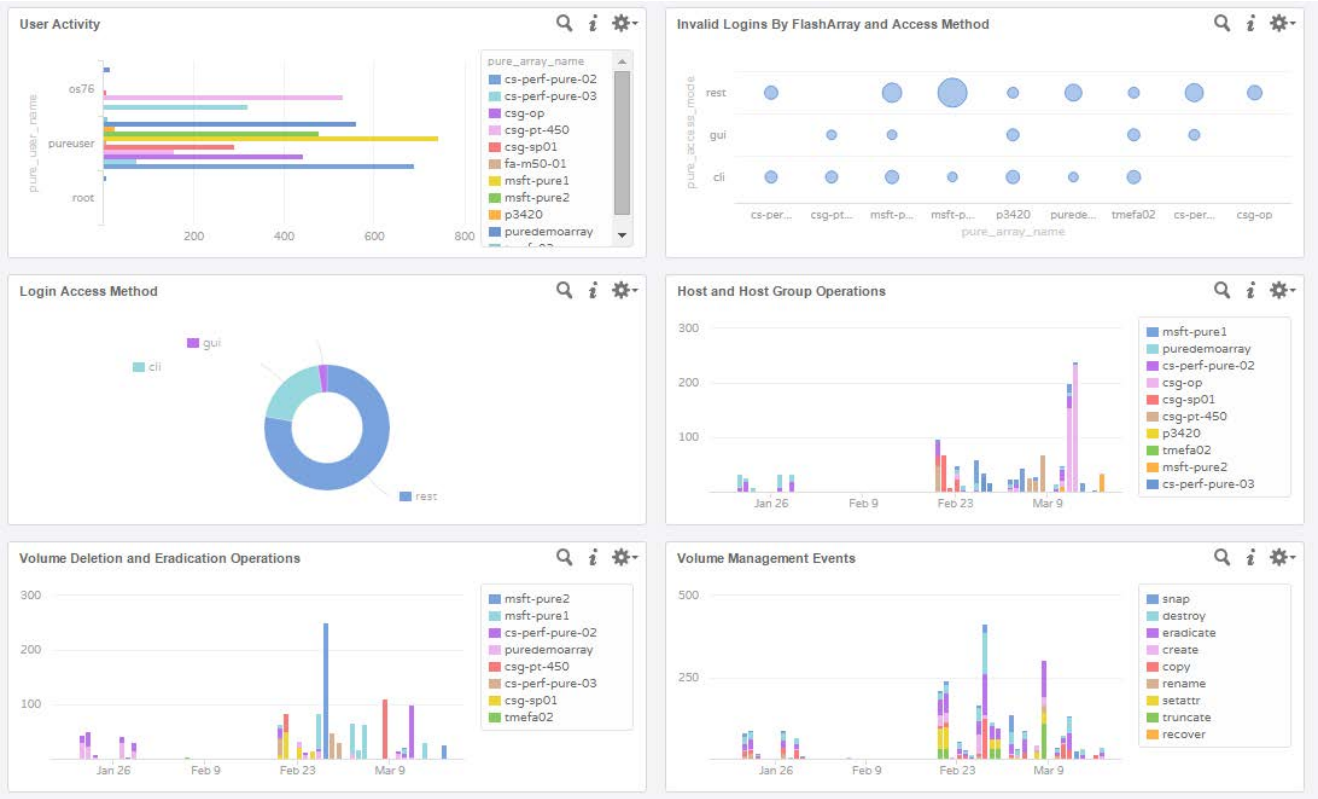


Figure 28. Auditing Dashboard Group

User Activity: This dashboard widget shows user audit activity on the FlashArray. All non-read-only operations by a given user will be logged here and grouped by quantity and command for that specific time. The results are sorted by user account and FlashArray name: <user name, array name>. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Invalid Logins by FlashArray and Access Method: This dashboard widget shows the number of invalid logins (from end-users or applications) sorted by access method (either via REST, GUI or CLI) and the individual target FlashArray. Large increases in this number may represent a pattern of unauthorized access attempts or more likely scripts/applications with outdated credentials. High numbers of REST failures indicates typically a script or application. Drill down further to see specific login information by opening the dashboard widget in the Interactive Analytics page. *NOTE: This requires Purity 4.1 and later to populate.*

Login Access Method: This dashboard widget shows the distribution of access methods (REST, GUI or CLI) by end user or application logins to the configured FlashArrays. This is only for initial logins, not operations or logouts. Drill down further to see specific users by opening the dashboard widget in Interactive Analysis mode. *NOTE: This requires Purity 4.1 and later to populate.*

Host and Host Group Operations: This dashboard widget shows the instances of host group configuration changes. Host groups are the mechanism of logically grouping end hosts and allowing for cluster-based simple provisioning en masse. Operations like creation, deletion, host add, volume add/removal are reported here. The

results are sorted by host group name and FlashArray name: <hgroup name, array name>. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Volume Destroy and Eradicate Operations: This dashboard widget shows the instances of volume deletion and/or eradication. By default when a FlashArray volume is deleted (referred to as destroyed) the data is not permanently lost. Volume data is only completely removed either 24 hours after the initial deletion or by a manual eradication. If a volume is no longer visible, check this dashboard widget and it will tell you if a volume has been destroyed and/or eradicated and when. When opened up, the source array containing the volume and the user who performed the operation will also be listed. The results are sorted by volume name and eradicate/destroy: <volume name, operation>. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Volume Management Events: This dashboard widget shows all instances of volume management. This includes but is not limited to, creation, destruction, expansion, shrinking (truncating), recovering and snapping. The results are sorted by purevol operation. Drill down further by opening the dashboard widget in Interactive Analysis mode.

Pure Storage Content Pack Alerts

The Pure Storage Content Pack includes six standard alerts that can be enabled and used by Log Insight to actively inform administrators of certain messages that match configured queries. Each alert is based on a specific query configured by Pure Storage and when its requirements are met, a message is sent out to either email or vROps. The alert contains the matching syslog message and a description of the alert and what must be done. The name of the alerts and the associated description/next steps are listed below.

Alert name: FlashArray: Protection Group Schedule Change

> **Message**: This alert is generated when the schedule of a FlashRecover protection group has changed. Either the local snapshot policy or the remote replication policy has changed or both. Please ensure that this change is expected and valid.

Alert name: FlashArray: Critical Failure Alert

> **Message**: A component or cable has failed and could lead to data unavailability if not resolved as soon as possible. While all parts are redundant and the array itself can handle multiple SSD failures it is important to resolve any issue immediately. Contact your Pure Storage support team (if they have not already contacted you) to replace or repair the part.

Alert name: FlashArray: Capacity Utilization Warning

> **Message**: Your FlashArray has reached high levels of capacity utilization. Consider adding additional capacity as soon as possible.

Alert name: FlashArray: Volume Destruction Alert

> **Message**: A volume has been destroyed (deleted) on a Pure Storage FlashArray. By default, volume data is preserved for 24 hours following a destroy operation. If this volume should not have been deleted, log into the Pure GUI or CLI and use the purevol recover operation to reclaim the volume. Otherwise this volume will be permanently destroyed in 24 hours (or sooner if a manual eradicate operation is executed).

Alert name: FlashArray: Component Failure Alert

> **Message**: A specific component or cable has failed and could lead to data unavailability if not resolved as soon as possible. While all parts are redundant and the array itself can handle multiple SSD failures it is important to resolve any issue immediately. Contact your Pure Storage support team (if they have not already contacted you) to replace or repair the part.

Alert name: FlashArray: Power Failure Alert

> **Message**: A power component or cable has failed and could lead to data unavailability if not resolved as soon as possible. While all power components are redundant it is important to resolve any issue immediately. This failure could be due to power supply failure, an unplugged or damaged power cord or loss of general power. Contact your Pure Storage support team (if they have not already contacted you) to resolve the issue.

Unlike dashboards and extracted fields, the alerts are **NOT ENABLED BY DEFAULT**—an administrator must configure and enable them first. To do so, navigate to the Interactive Analysis screen and click on the red bell icon and choose “Manage Alerts…”

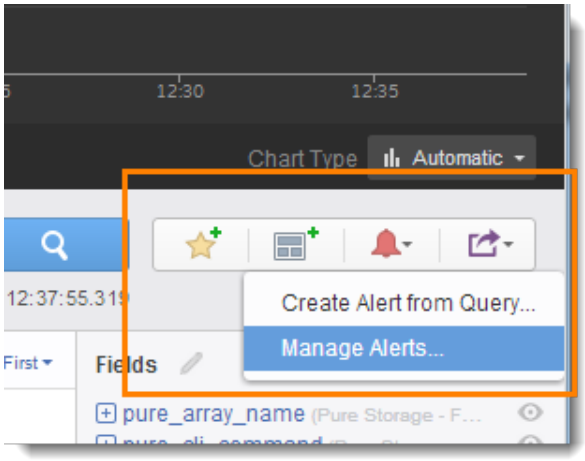


Figure 29. Managing Alerts

The Pure Storage Content Pack Alerts appear under Manage Alerts in a section called “Pure Storage – FlashArray Content Pack. By default, it can be noted the alerts are disabled.

To enable an alert, click on an alert. A screen will pop-up that shows the alert name, the message to be sent and delivery options. Furthermore, the frequency of delivery and sensitivity of the alert can be configured.

A user can change any of these fields that they wish. Once it is configured as desired, click “Save to My Alerts” this will enable the alert. Note that the original alert is not changed or enabled. The enabled alert is copied to the user space instead—this allows the original alerts to be re-used and won’t affect configured alerts if the original ones are changed or replaced due to a Content Pack upgrade.

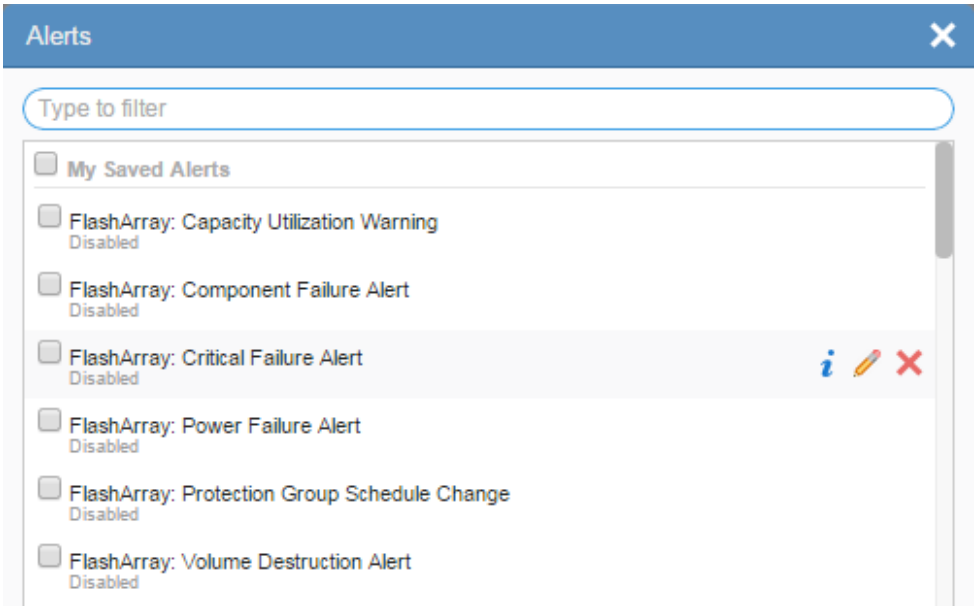


Figure 30. Pure Storage Alerts

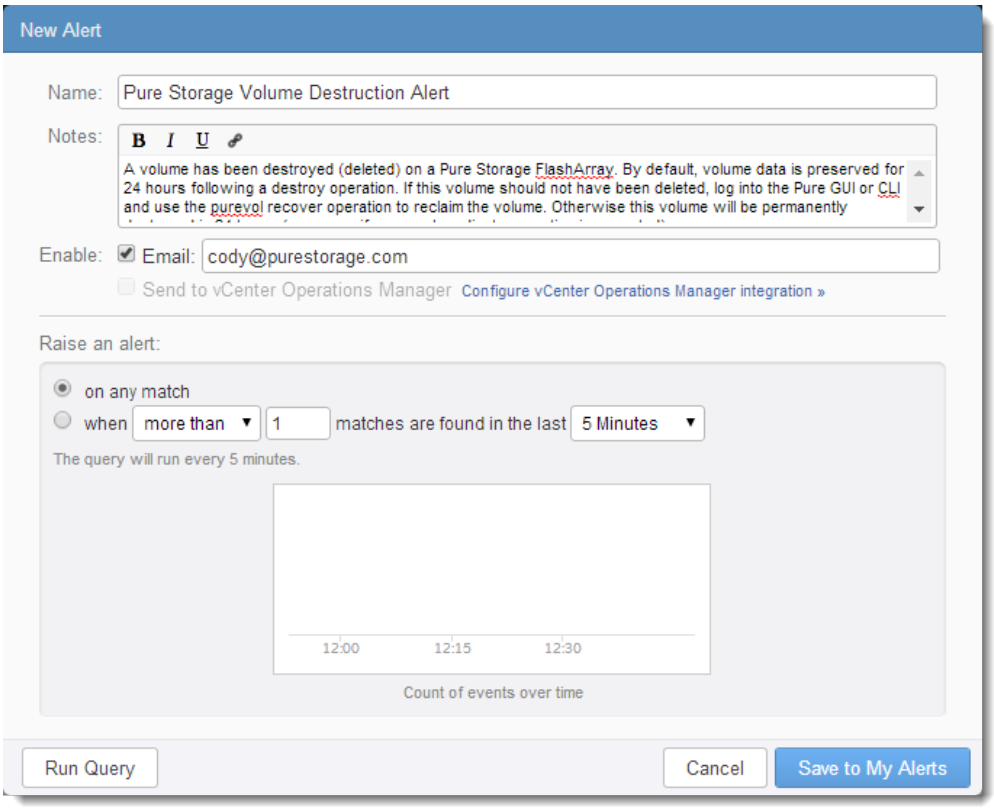


Figure 32. Enabling a Content Pack Alert

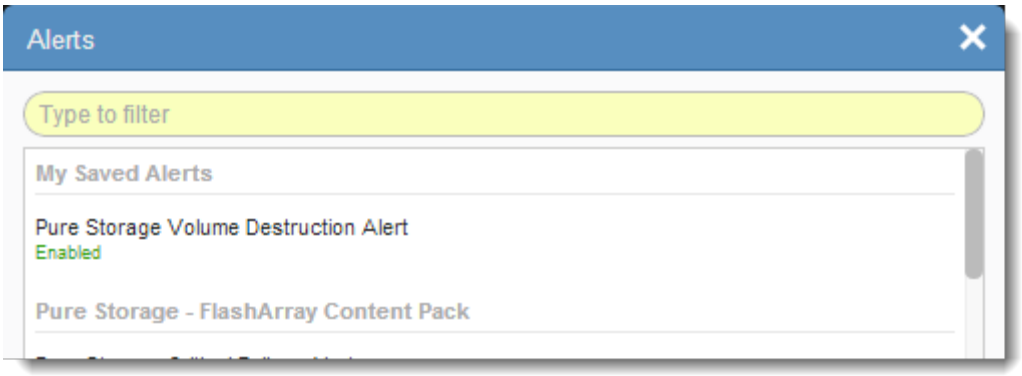


Figure 31. Newly saved alert

Conclusion

The Pure Storage FlashArray Content Pack for VMware vRealize Log Insight is an integral piece for all Pure Storage and Log Insight users. While Log Insight works with the FlashArray without the Content Pack, it is highly encouraged that users deploy and leverage the free Content Pack to simplify configuration and accelerate the time it takes to begin to effectively use Log Insight.

References

Log Insight Documentation— http://pubs.vmware.com/log-insight-25/index.jsp

Pure Storage Documentation— http://support.purestorage.com/

VMware Solution Exchange— https://solutionexchange.vmware.com/store/loginsight

Pure Storage, Inc.
Twitter: @purestorage

650 Castro Street, Suite #400
Mountain View, CA 94041

T: 650-290-6088
F: 650-625-9667

Sales: sales@purestorage.com
Support: support@purestorage.com
Media: pr@purestorage.com
General: info@purestorage.com

