End Your Data Center Logging Chaos with VMware vCenter Log Insight

By David Davis, vExpert

WHITE PAPER

Table of Contents

Many key IT resources—including servers, storage arrays, routers, switches and firewalls—constantly generate log files faster than any human can process them. A VMware ESXi™ host generates 250MB of log files per day on average, and a typical Microsoft Exchange server can generate up to 1GB of log data daily. A large data center can produce hundreds or thousands of log files that over time amount to massive data volumes. If left unattended, those log files can cause problems for their hosts by filling the hosts' available storage. Or, more typically, they overwrite themselves—causing you to lose log entries that are critical for security, compliance and troubleshooting.

Most system administrators try to look through system log files weekly (in some cases using reporting tools)—a task that can take hours. When trouble occurs in the data center, log files can help you track down the root cause. But without log file consolidation, those troubleshooting tasks can be painful.

Running a reliable and secure data center is a continual process of planning, delivering and operating. Without a consolidated view of your infrastructure's system log data, your data center is incomplete and at risk. The risks include

- Increased downtime for applications and servers, because more time is needed to locate and search system log files when trouble occurs
- Security risks such as malicious attacks or unauthorized logins that could be occurring without your knowledge
- Loss of historical system logs, leaving you unprepared to report local authentications or be in compliance

Consolidated system logging is a critical data center feature that is all too commonly left unimplemented because of its complexity. Also, IT professionals rely on data center monitoring tools, most of which focus on raw metrics—such as CPU utilization, memory consumption and storage I/O—but completely ignore log files. When system log files are ignored, valuable diagnostic information is overlooked.

Virtualization makes many things in the data center possible that were previously impossible or impractical. They include the ability to move virtual machines, and improved, simplified approaches to server load balancing, high availability and disaster recovery.

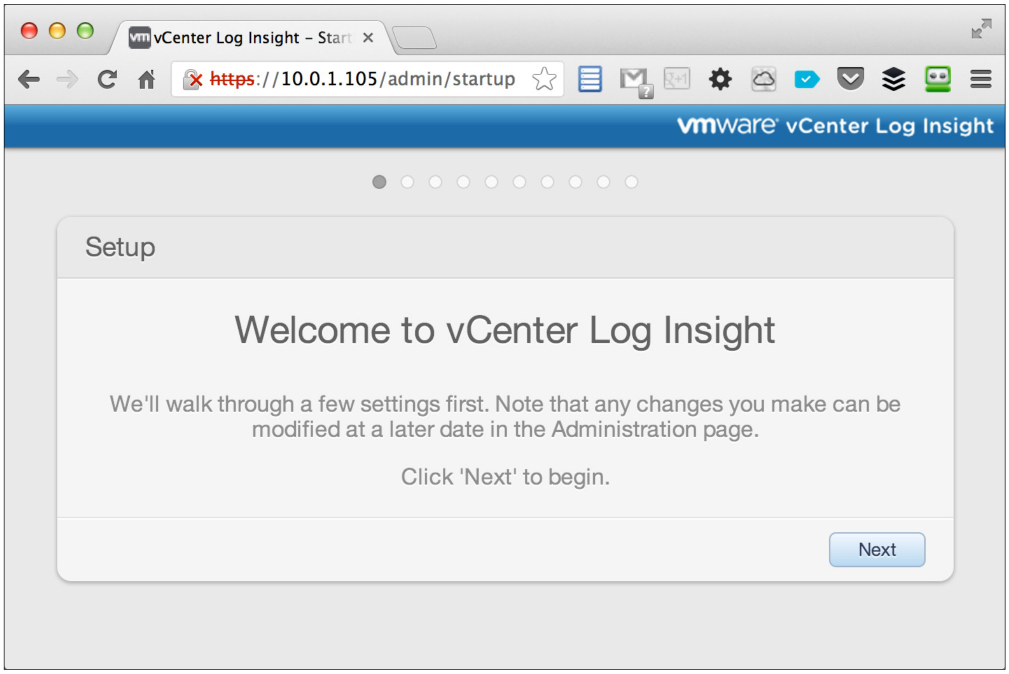
Now, VMware is offering a log analytics solution that is easy to implement and intuitive to use—and that understands your virtual infrastructure. That solution is VMware vCenter™ Log Insight™. Read on to find out how to deploy vCenter Log Insight and use it to solve some of the most common problems affecting today's data centers.

Deploying vCenter Log Insight

Like some other VMware management solutions, vCenter Log Insight is delivered as a virtual appliance. You don't need to install an operating system or set up a database, and no time-consuming updates or patches are required.

After you download the vCenter Log Insight virtual appliance from http://www.vmware.com (available as a 60-day evaluation), you deploy it in VMware vSphere® Client using the **Deploy OVF Template** option. This wizard guides you through the process of accepting the end-user license agreement, selecting a location for the appliance in your virtual infrastructure, specifying the virtual disk format, and configuring the IP address of the virtual machine. The entire deployment process takes about five minutes.

After the virtual appliance is powered on, you need to perform a quick initial configuration of vCenter Log Insight using the Web interface shown in Figure 1.


vCenter Log Insight – Start
~~https~~://10.0.1.105/admin/startup
vmware vCenter Log Insight

Setup

Welcome to vCenter Log Insight

We'll walk through a few settings first. Note that any changes you make can be modified at a later date in the Administration page.

Click 'Next' to begin.

Figure 1. vCenter Log Insight Web Interface

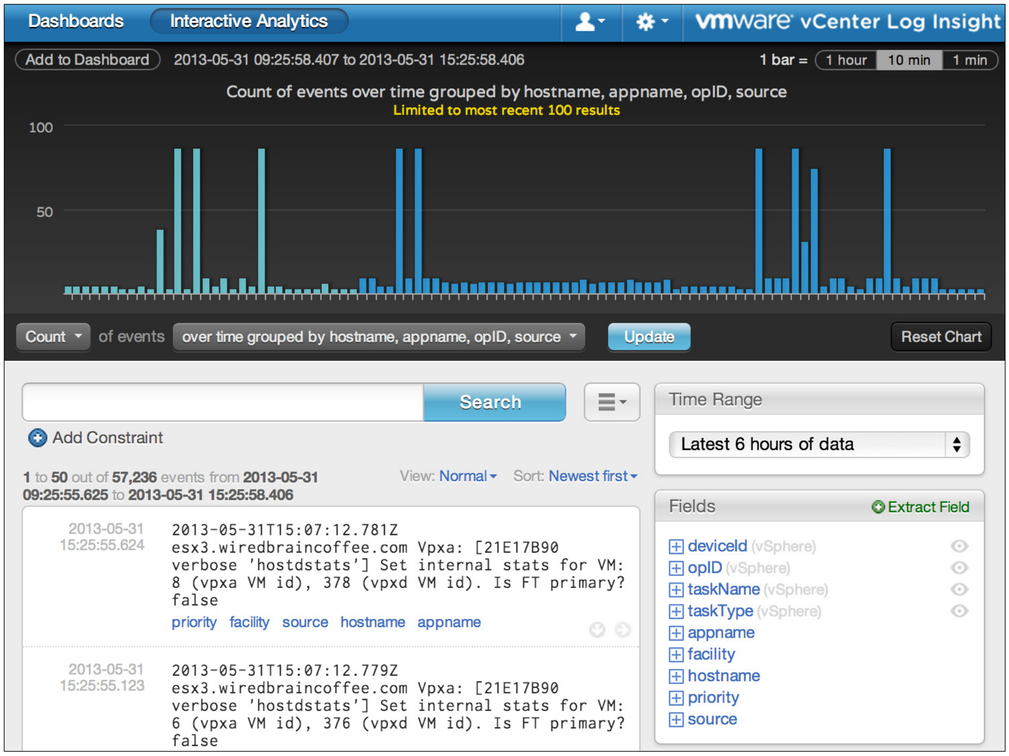
With vCenter Log Insight configured, it's ready to receive syslogs from ESXi hosts and any other data center devices that support syslog.

To configure all ESXi hosts managed by your vCenter Server™ to send their syslogs to vCenter Log Insight, the recommended option is to run the **configure-esx** command from the vCenter Log Insight console. See the vCenter Log Insight Administrator's Guide for information about this script.

vCenter Log Insight Usage Model

With vCenter Log Insight installed and syslog data flowing to it, it's ready for use. Like all applications, vCenter Log Insight has a usage model. For example, as a vSphere administrator you would typically follow this sequence:

- Whether you have an immediate problem to solve or don't know exactly what you're looking for, you start by searching for a keyword, tag, error code or object. vCenter Log Insight autocompletes search strings to help you avoid typos.
- The overhead graph quickly tells you if you have found any results, and the context-sensitive visualization (shown in Figure 2) lets you correlate logs. This is helpful for making a case to your peers and management about trends, system behavior or issues with particular areas in your environment.



2013-05-31 09:25:58.407 to 2013-05-31 15:25:58.406

Count of events over time grouped by hostname, appname, opID, source
Limited to most recent 100 results

Time Range: Latest 6 hours of data

1 to 50 out of 57,236 events from 2013-05-31 09:25:55.625 to 2013-05-31 15:25:58.406

2013-05-31 15:25:55.624

```
2013-05-31T15:07:12.781Z
esx3.wiredbraincoffee.com Vpxa: [21E17B90
verbose 'hostdstats'] Set internal stats for VM:
8 (vpxa VM id), 378 (vpxd VM id). Is FT primary?
false
```

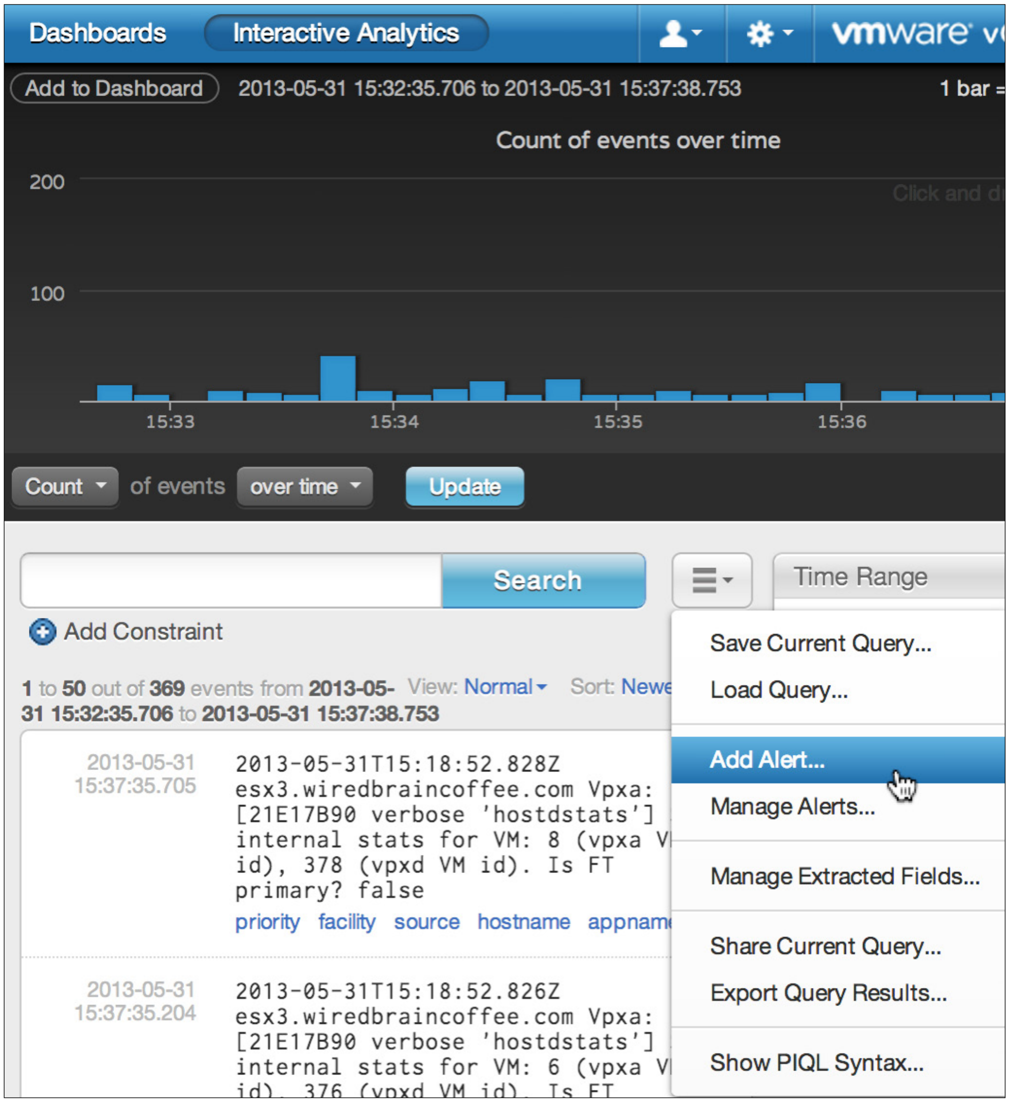
priority facility source hostname appname

2013-05-31 15:25:55.123

```
2013-05-31T15:07:12.779Z
esx3.wiredbraincoffee.com Vpxa: [21E17B90
verbose 'hostdstats'] Set internal stats for VM:
6 (vpxa VM id), 376 (vpxd VM id). Is FT primary?
false
```

Figure 2. vCenter Log Insight Search Visualization

- When you identify critical queries that you want to monitor in the future, you can add those queries to your vCenter Log Insight dashboard screen. The dashboard functionality enables you to monitor a large data set without needing to drill into the details every time. Additionally, you can export dashboards to share them with other vCenter Log Insight users or import dashboards from third parties.
- Finally, you can easily create an alert for any queries that you want continually monitor and receive notifications about, as shown in Figure 3.



1 to 50 out of 369 events from 2013-05-31 15:32:35.706 to 2013-05-31 15:37:38.753

```
2013-05-31     2013-05-31T15:18:52.828Z
15:37:35.705   esx3.wiredbraincoffee.com Vpxa:
               [21E17B90 verbose 'hostdstats']
               internal stats for VM: 8 (vpxa V
               id), 378 (vpxd VM id). Is FT
               primary? false

2013-05-31     2013-05-31T15:18:52.826Z
15:37:35.204   esx3.wiredbraincoffee.com Vpxa:
               [21E17B90 verbose 'hostdstats']
               internal stats for VM: 6 (vpxa V
               id), 376 (vpxd VM id). Is FT
```

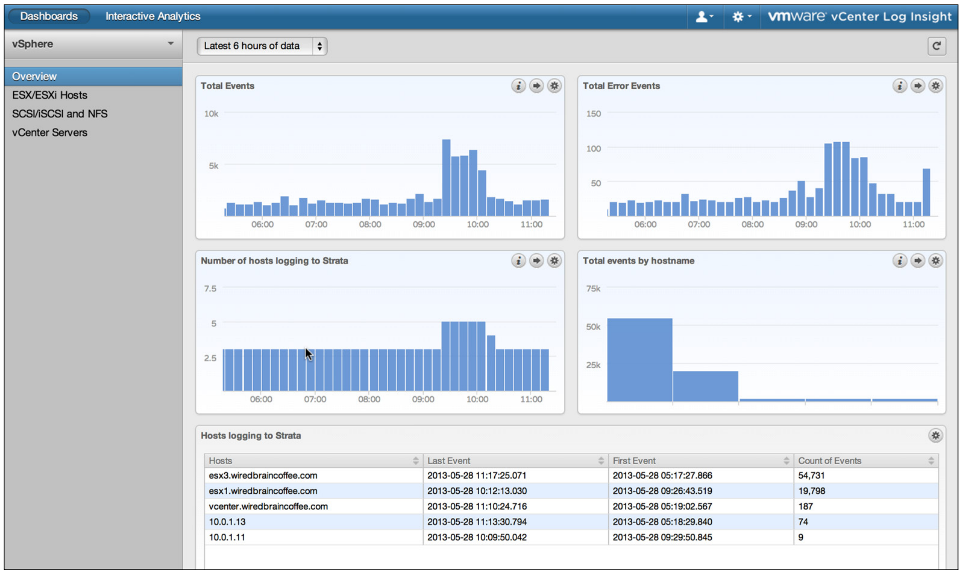
Figure 3. Adding Query Alerts in vCenter Log Insight

Now that you understand the usage model, you're ready to learn about some of the numerous use cases for vCenter Log Insight.

How vCenter Log Insight Helps to Monitor Your Data Center

vCenter Log Insight provides consolidated logging and analytics for any device that supports syslog, but its greatest strength is in vCenter Server and vSphere logging and analytics.

One example of this built-in virtual infrastructure awareness is the included vSphere content pack dashboard, shown in Figure 4. With this dashboard, you can quickly visualize numerous statistics related to ESXi hosts, SCSI, iSCSI, NFS and your vCenter Server instances.



Hosts logging to Strata

Hosts	Last Event	First Event	Count of Events
esx3.wiredbraincoffee.com	2013-05-28 11:17:25.071	2013-05-28 05:17:27.866	54,731
esx1.wiredbraincoffee.com	2013-05-28 10:12:13.030	2013-05-28 09:26:43.519	19,798
vcenter.wiredbraincoffee.com	2013-05-28 11:10:24.716	2013-05-28 05:19:02.567	187
10.0.1.13	2013-05-28 11:13:30.794	2013-05-28 05:18:29.840	74
10.0.1.11	2013-05-28 10:09:50.042	2013-05-28 09:29:50.845	9

Figure 4. vSphere Content Dashboard

By clicking on any point in any of the multiple graphs, you can drill down into the interactive analytics to get more information.

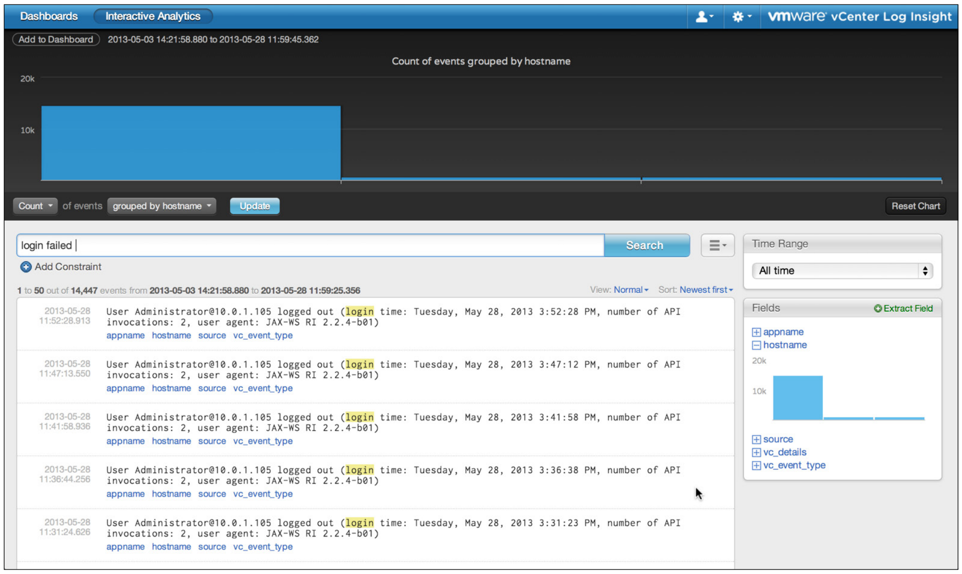
Saved queries in the vSphere content pack include

- Events per host
- vKernel warnings per host
- VMware API calls per host
- Network connectivity lost
- Network uplink redundancy degraded
- SCSI failures per device
- Maximum latency by device
- NFS connection failures
- All paths down
- Storage device performance degraded
- VMFS heartbeat timeout
- SCSI/iSCSI errors and warnings
- NFS errors and warnings
- Failed vs finished vCenter tasks per host (vpxa/vpxd)
- Slow vCenter Operations

How vCenter Log Insight Helps to Secure Your Data Center

vCenter Log Insight works in multiple ways to ensure that your data center is more secure and that it can achieve the security compliance that your company requires.

The first way is to consolidate and archive log data from all the devices in the data center, creating a historical record. Without a log consolidation tool, it's likely that your log files rotate and as a result are being overwritten and lost. Without log files, it can be impossible to track down the source of a security breach.



2013-05-03 14:21:58.880 to 2013-05-28 11:59:45.362

login failed

All time

1 to 50 out of 14,447 events from 2013-05-03 14:21:58.880 to 2013-05-28 11:59:25.356

```
2013-05-28    User Administrator@10.0.1.105 logged out (login time: Tuesday, May 28, 2013 3:52:28 PM, number of API
11:52:28.913  invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
              appname  hostname  source  vc_event_type

2013-05-28    User Administrator@10.0.1.105 logged out (login time: Tuesday, May 28, 2013 3:47:12 PM, number of API
11:47:13.550  invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
              appname  hostname  source  vc_event_type

2013-05-28    User Administrator@10.0.1.105 logged out (login time: Tuesday, May 28, 2013 3:41:58 PM, number of API
11:41:58.936  invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
              appname  hostname  source  vc_event_type

2013-05-28    User Administrator@10.0.1.105 logged out (login time: Tuesday, May 28, 2013 3:36:38 PM, number of API
11:36:44.256  invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
              appname  hostname  source  vc_event_type

2013-05-28    User Administrator@10.0.1.105 logged out (login time: Tuesday, May 28, 2013 3:31:23 PM, number of API
11:31:24.626  invocations: 2, user agent: JAX-WS RI 2.2.4-b01)
              appname  hostname  source  vc_event_type
```

Figure 5. Searching for Security Events with vCenter Log Insight

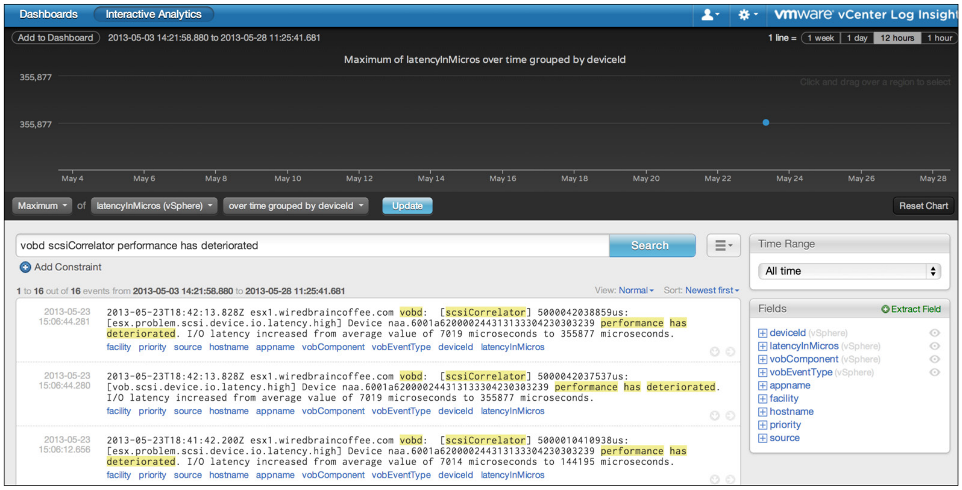
The second way that vCenter Log Insight helps to secure your data center is to take all that consolidated data and allow you to search across it for security events (see Figure 5). For example, suppose that you want to search for failed logins across the infrastructure. You could perform that search across all the various types of devices that make up the data center. That's a powerful security tool that isn't possible without log consolidation and high-speed interactive querying. You could then easily save that query and create your own security dashboard.

How vCenter Log Insight Helps to Troubleshoot Your Datacenter

vCenter Log Insight is a strong troubleshooting tool for your data center (not just for vSphere), because in one place it can correlate the events happening across the entire data center. That enables you to speed up your time to resolution by finding a root cause for a data center problem.

Let's say that your end users are complaining about application performance. Using vCenter Log Insight, you could use the included vSphere SCSI/iSCSI dashboard to perform a saved query showing where storage performance has deteriorated (or quickly search for "SCSI performance deteriorated" in the interactive analytics screen).

Figure 6 shows a number of instances in which storage performance deteriorated from the average, any of which could be the source of end-user application issues.



2013-05-03 14:21:58.880 to 2013-05-28 11:25:41.681

vobd scsiCorrelator performance has deteriorated

1 to 16 out of 16 events from 2013-05-03 14:21:58.880 to 2013-05-28 11:25:41.681

```
2013-05-23   2013-05-23T18:42:13.828Z esx1.wiredbraincoffee.com vobd:  [scsiCorrelator] 5000042038859us:
15:06:44.281 [esx.problem.scsi.device.io.latency.high] Device naa.6001a620000244313133304230303239 performance has
             deteriorated. I/O latency increased from average value of 7019 microseconds to 355877 microseconds.
             facility  priority  source  hostname  appname  vobComponent  vobEventType  deviceId  latencyInMicros

2013-05-23   2013-05-23T18:42:13.828Z esx1.wiredbraincoffee.com vobd:  [scsiCorrelator] 5000042037537us:
15:06:44.280 [vob.scsi.device.io.latency.high] Device naa.6001a620000244313133304230303239 performance has deteriorated.
             I/O latency increased from average value of 7019 microseconds to 355877 microseconds.
             facility  priority  source  hostname  appname  vobComponent  vobEventType  deviceId  latencyInMicros

2013-05-23   2013-05-23T18:41:42.200Z esx1.wiredbraincoffee.com vobd:  [scsiCorrelator] 5000010410938us:
15:06:12.656 [esx.problem.scsi.device.io.latency.high] Device naa.6001a620000244313133304230303239 performance has
             deteriorated. I/O latency increased from average value of 7014 microseconds to 144195 microseconds.
             facility  priority  source  hostname  appname  vobComponent  vobEventType  deviceId  latencyInMicros
```

Figure 6. Troubleshooting with vCenter Log Insight

Yes, you can even have vCenter Log Insight calculate the average latency of all your SCSI devices.

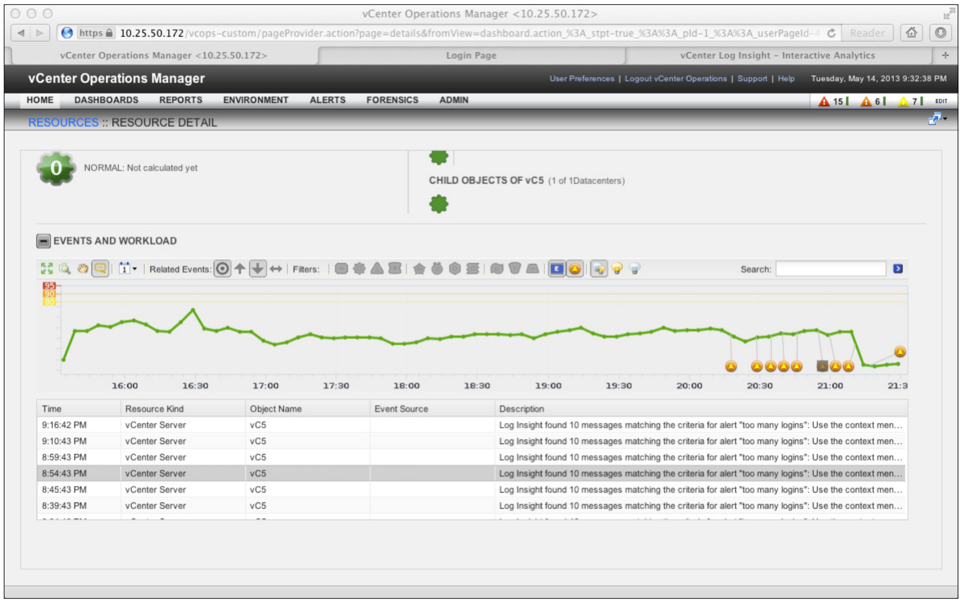
Integrating vCenter Operations Manager with vCenter Log Insight

Although other log analysis and consolidation tools are available, they rarely integrate with existing data center and virtualization management tools. However, integration is a key requirement, because you don't want to use a "silo tool" that is only good for one particular purpose or task.

vCenter Log Insight provides tight integration with VMware vCenter™ Operations Manager™, which is now commonly used to monitor and manage the performance and health of vSphere environments. This integration gives you a comprehensive virtualization management solution with best-of-breed capabilities for monitoring performance metrics, optimizing infrastructure capacity, ensuring configuration compliance and seeing log data in the context of service-level agreements (SLAs).

Because vCenter Log Insight sends events and alerts to vCenter Operations Manager, you can have a single dashboard that proactively notifies you of potential performance bottlenecks and enables you to drill into log data, as needed, to remediate issues.

In Figure 7, you can see vCenter Operations Manager showing that vCenter Log Insight has details about events that are impacting the performance of a workload. You can drill into any one of these events to look at the associated log data.


vCenter Operations Manager <10.25.50.172>
https 10.25.50.172/vcops-custom/pageProvider.action?page=details&fromView=dashboard.action_%3A_stpt-true_%3A%3A_pId-1_%3A%3A_userPageId-4
Reader
vCenter Operations Manager <10.25.50.172>
Login Page
vCenter Log Insight – Interactive Analytics
vCenter Operations Manager
User Preferences | Logout vCenter Operations | Support | Help
Tuesday, May 14, 2013 9:32:38 PM
HOME
DASHBOARDS
REPORTS
ENVIRONMENT
ALERTS
FORENSICS
ADMIN
15
6
7
EDIT
RESOURCES :: RESOURCE DETAIL
0
NORMAL: Not calculated yet
CHILD OBJECTS OF vC5 (1 of 1Datacenters)
EVENTS AND WORKLOAD
Related Events:
Filters:
Search:
90
80
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
20:00
20:30
21:00
21:3

Time	Resource Kind	Object Name	Event Source	Description
9:16:42 PM	vCenter Server	vC5		Log Insight found 10 messages matching the criteria for alert "too many logins": Use the context men...
9:10:43 PM	vCenter Server	vC5		Log Insight found 10 messages matching the criteria for alert "too many logins": Use the context men...
8:59:43 PM	vCenter Server	vC5		Log Insight found 10 messages matching the criteria for alert "too many logins": Use the context men...
8:54:43 PM	vCenter Server	vC5		Log Insight found 10 messages matching the criteria for alert "too many logins": Use the context men...
8:45:43 PM	vCenter Server	vC5		Log Insight found 10 messages matching the criteria for alert "too many logins": Use the context men...
8:39:43 PM	vCenter Server	vC5		Log Insight found 10 messages matching the criteria for alert "too many logins": Use the context men...

Figure 7. Integration of vCenter Operations Manager and vCenter Log Insight

Summary

Although vCenter Log Insight can be used as a standalone log consolidation and analysis tool, it's greatest strength (and biggest differentiator) is its tight integration with vCenter Server, vSphere, and vCenter Operations Manager. No other virtualization-management tool can give you such a complete view of your data center operations by correlating virtualization performance events and system log entries across the vSphere infrastructure.

Another of vCenter Log Insight's great strengths is that it can also manage physical servers, storage, and network devices. vCenter Log Insight is extensible, because you can add third-party content packs (made up of numerous fields) or your own content packs.

Both large enterprises and small and midsized businesses (SMBs) should use vCenter Log Insight to consolidate their log data to gain strong analytics and troubleshooting capabilities.

VMware vCenter Log Insight is useful for monitoring, troubleshooting and securing your data center, and it's quick to set up and enjoyable to use. In addition, vCenter Log Insight offers unique integration with vCenter Operations Manager to give you a complete view of your virtual infrastructure.

For more information about **vCenter Log Insight**, visit http://www.vmware.com.

About the Author

David Davis is the author of the best-selling VMware vSphere video training library from TrainSignal. He has written hundreds of virtualization articles on the Web and is a vExpert, VCP, VCAP-DCA, and CCIE #9369 with more than 18 years of enterprise IT experience. His personal Web site is VMwareVideos.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com