dimensional research

VMware vCenter Log Insight Delivers Immediate Value to IT Operations

Executive Summary

Log analytics is growing increasingly important as the size and complexity of IT environments continues to expand. Add in virtualization, cloud computing, and geographical asset distribution, and it is easy to understand why IT Operations teams are looking for solutions that allow them to more effectively collect, analyze and harness key information hidden in vast amounts of log data.

This paper is based on in-depth interviews with customers who participated in the vCenter Log Insight early access program and investigates the actual benefits achieved during use of the product. All participants in this study stated that they received significant value from VMware's vCenter Log Insight solution. Users report vCenter Log Insight is quick to learn and simple to use, which makes finding and troubleshooting IT issues faster and easier. Users praised the product as easy to setup and use as part of their daily operations to centralize information for issue prevention and remediation.

The paper is organized into individual journal entries chronicling the vCenter Log Insight experiences for each participant.

Project Methodology

VMware commissioned Dimensional Research to interview vCenter Log Insight users and gather in-depth feedback on the actual benefits received from using the product. Dimensional Research conducted five telephone interviews with vCenter Log Insight users, and this report is based on those conversations. All customer quotes were acquired from interview transcripts, although some quotes have been edited slightly for grammar and readability.

VMware compiled a global list of potential participants and then provided their contact information to Dimensional Research. VMware did not participate in the interviews and did not offer input into this report except to clarify certain details of product functionality.

During the interviews, participants were asked about their IT environments, current use of logs, problem resolution techniques, as well as their experiences installing, configuring, and using the vCenter Log Insight product. Users were not compensated for taking part in this research project, although a small donation was made to the charity of their choice as appreciation for their time.

Participant Profile

Interview participants were employed at large companies representing a wide range of industries including:

- A leading shipping and transportation company
- An International telecommunications firm
- A multinational retail chain
- A global travel and hospitality company
- A leading cellular and wireline provider

Each participant personally deployed and used the vCenter Log Insight product. And although their roles varied from virtual environment administrators to senior architects, they were all responsible for hundreds to thousands of devices and virtual machines spanning across multiple data centers. In each case, the deployed solution was used in a subset of every participant's environment.

Users were promised anonymity during the interview process to encourage candid and factual feedback.

Transportation Company Uses Log Analytics to Simplify Troubleshooting

As one of the leading transportation suppliers in North America, this company relies on eight data centers with large virtualization farms. IT runs all of the logistics, business operations, and customer interactions. For this organization, IT uptime is synonymous with business uptime. We spoke with a senior IT architect who manages the entire VMware environment and internal infrastructure as a service (IaaS) cloud for his company.

Reasons for Needing Log Analytics

Given the numerous data centers and geographic diversity, the architect shared that logs were searched several times a week for troubleshooting performance problems. Historically, it was challenging for IT to correlate a server or application alert with correct log data and then find the cause. Often storage was the culprit of performance issues, but the symptoms always appeared somewhere else. The architect noted how they finally attributed these issues to storage after first verifying that the problems were not caused by servers, the virtualization stack, or the network.

> "We use logs several times a week to troubleshoot a wide variety of issues. It is rather difficult and tedious to do this manually."

vCenter Log Insight Experiences

The IT architect explained how vCenter Log Insight was one of the simplest products he has ever deployed. In fact, it only took 20 to 30 minutes to have everything working and required almost no configuration. He recounted how storage issues that were once extremely difficult to identify and resolve are now easy to find with vCenter Log Insight.

> "We love the product, and I don't know how we could go back to operating our environment without it."

> "The learning curve is flat. I watched a one hour video and that was it."

Real-World Benefits

> "Tasks are down from hours to minutes."

> "I can't tell you how much faster and easier vCenter Log Insight is over our old way of searching logs."

The architect recounted how troubleshooting tasks that used to require hours of frustrating work can now be quickly completed by searching for specific entries and then filtering to find the device causing the issue. Not only did vCenter Log Insight help resolve issues faster, it made his team more efficient. To help manage performance issues, the architect built a dashboard that provides access to visualize information and be a starting point for issue resolution. Overall, he cited these benefits that vCenter Log Insight provided to his team:

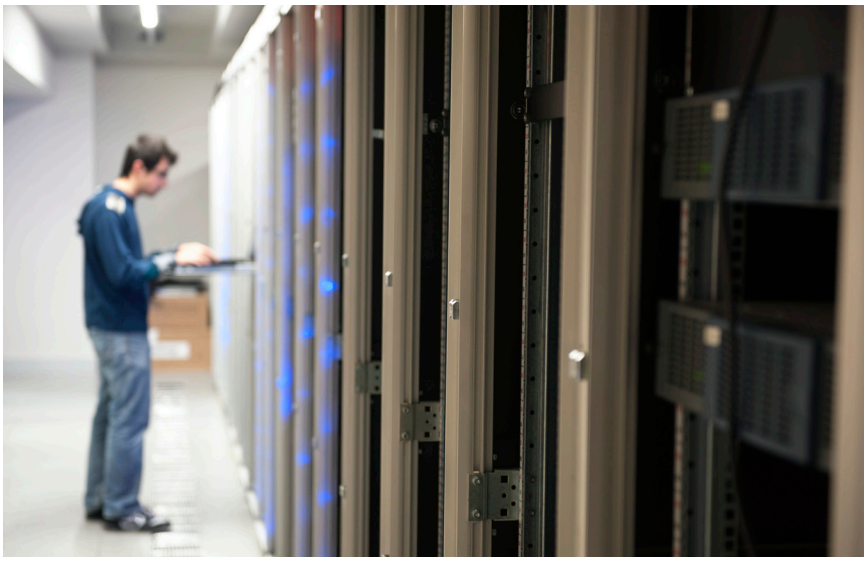
- Faster resolution times
- Improved team efficiency
- Centralized information
- A powerful dashboard for operations

> "We have over 100,000 storage elements, and vCenter Log Insight makes it easy to find the array, path, or device that is causing a problem."

Next Steps

The architect shared that the team was initially using vCenter Log Insight as purely a troubleshooting tool. But now they are creating dashboards and alerts to help proactively resolve issues before they cause any service interruptions.

> "Recently we noticed some odd logs issues when looking vCenter Log Insight dashboard. So we searched on the alert and found three hosts suffering from a corrupted software install. Not only did we resolve that problem, but now we have set an alert for the messages as an early warning system."



VMware vCenter Log Insight

VMware vCenter Log Insight delivers automated log management through log aggregation, analytics and search, extending VMware's leadership in analytics-based IT Operations to include log data. With an integrated and unified approach to IT Operations, vCenter Log Insight provides the operational intelligence and enterprise-wide visibility needed to proactively enable service levels and operational efficiency in dynamic hybrid cloud environments.

Telecommunications Company Needs Log Analytics to Manage Complex Environments

This top U.S. cable entertainment and broadband services provider offers television, Internet, and telephone services to its customers. We interviewed the company's lead virtualization administrator (VI admin) who shared that he manages more than 2,500 virtual machines (VMs) that run software from web servers and databases to the company's accounting and HR applications. Application uptime and performance were key measurements that translated into a heavy focus of problem prevention and fast issue resolution.

Reasons for Needing Log Analytics

The VI admin explained that it was common to search through logs several times a week to find and remediate issues and potential problems. He described the tedious process of checking logs from servers, storage, network gear, and security devices. He told us it could take many hours to find and correlate the data. The company's operations team used Splunk, but the VI admin said that the tool performed poorly when searching the virtualized environment because it couldn't identify all the virtual machines and correlate them to hosts correctly.

> "The Ops team has Splunk, but it just isn't as effective or useful when working in a virtual environment."

vCenter Log Insight Experiences

The VI admin said it only took about an hour to install and configure Log Insight. Unlike other log analytics tools that require a dedicated physical box and a proxy, he could install and run vCenter Log Insight on a virtual machine. He continued to explain how the dashboard and reports were the first advantages he identified. They were better than others he had seen and were usable right out of the box. Furthermore, he could quickly see differences in patterns and then click on the graph to find the devices and logs that were producing the anomalies. In fact, after installation he

"The dashboard and reports out of the box were excellent and useful. You can click on any bar and graph and drill down to the specific log entry on any device."

immediately noticed a different pattern on a few of the hosts. He soon discovered they had a problem with Active Directory and was able to find that the OS installs on those boxes were corrupted. The VI admin expressed how he likes to check the dashboard to look at the patterns of data coming back, which allows him to find issues that haven't even surfaced yet.

"vCenter Log Insight provides links to the Internet with a detailed explanation and possible fixes. With most other tools, you get some cryptic code that you spend hours trying to figure out what it means instead of fixing the issues."

"For a virtual environment vCenter Log Insight is a much better choice than other log search tools."

Real-World Benefits

When asked about the benefits his company receives from using VMware's vCenter Log Insight, he said that vCenter Log Insight allowed him be both proactive and faster in reacting to issues. He articulated the following benefits of vCenter Log Insight:

- A decrease in outage time
- Faster resolution of issues
- Increased visibility of issues
- Prevention of downtime
- All information accessible from a single location

"I can prevent problems from happening and resolve issues faster and easier than with other log search tools."

He also prefers the VMware pricing model based on the number of devices and not the volume of data flowing into the tool. He noted that typical data volume models encourage you to turn off the log feeds unless there is a problem. But with the VMware model you can leave everything on and use that data for monitoring and preventing problems. And when you have a real problem, that data is already in the system so finding the cause of the issue is faster and easier.

"Because of the Splunk data volume model, I was asked to take some of our ESX hosts off because they were too chatty and driving up costs. When you think of it, it's pretty scary when you don't run a tool because of the cost and licensing model."

Next Steps

In the near future, the communication company will be moving to a private cloud and then some hybrid-cloud based operations. The VI admin was emphatic that vCenter Log Insight would be critical for managing and resolving issues in that complex and distributed environment. While the early access product was not packaged with vCenter Operations Management Suite, he thought it would be a very potent combination to marry monitoring and operations with the additional information from vCenter Log Insight.

"I can't wait for vCenter Log Insight to be integrated with vCenter Operations, it would definitely beat any other log analysis and search tool hands down."

Hospitality Company Needed a Single Solution for Log Aggregation, Searching, and Monitoring

This European company offers cloud services to internal clients, business subsidiaries, and external customers. We interviewed the company's cloud architect and the operations manager responsible for day-to-day operations of the cloud and virtualization environment. They indicated that preventing downtime and quickly remediating business issues are extremely critical for both internal and external customer. They measure their team's effectiveness by delivering services that meet SLAs and exceed expectations.

Reasons for Needing Log Analytics

Both the architect and operations manager explained how searching through logs was a daily practice for issue resolution and as an early warning system. However, historically they required several tools to provide monitoring and search functionality. As such, they needed carefully maintained scripts for each tool and all the various devices in their infrastructure.

> "It is part of our standard practice to use log files in both a monitoring capacity and for problem resolution.

vCenter Log Insight Experiences

Both individuals agreed that the vCenter Log Insight product was a surprisingly fast install and very easy to use. They said that their experience with Regular Expression (Regex) made it is easy to understand and perform the most complicated search tasks. But for many day-to-day tasks, Regex was not even necessary in vCenter Log Insight. Both felt the best part of the product was the easy-to-build dashboards that allowed them to track and report on issues proactively. They were impressed with the performance and scalability of the solution as their previous experience with Splunk had led them to believe that log search tools were not fast enough for an infrastructure of their size.

> "If you have any experience with Regex, vCenter Log Insight will be immediately intuitive."

> "vCenter Log Insight allows us to pull log information from many types of devices, such as Cisco and NetApp gear, as well as from servers running Microsoft and Linux."

> "The last time we looked into the log product, Splunk, it was too slow to deal with the million lines of log code we generate daily."

Real-World Benefits

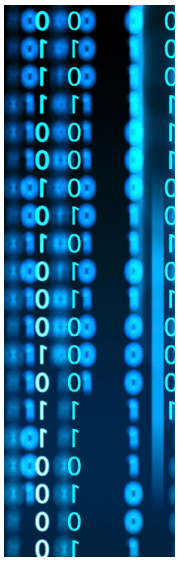
> "I can see the volume of log files in a graph, and, if it spikes, I get an alert and know something is happening or about to happen."

For different reasons, both individuals noted value in the dashboards. For the architect, it provided one location to see the entire infrastructure from numerous vendors. For the operations manager, it offered the ability to track the overall volume of logs and to look for spikes as an early warning system. Both felt that vCenter Log Insight was able to help them find and resolve issues more simply than using multiple log and monitoring tools. Here are the vCenter Log Insight benefits that they cited:

- Faster resolution of issues
- Proactive monitoring and alerting
- A single pane of glass for operations and architecture
- Consolidation of log and monitoring tools

> "vCenter Log Insight would replace a lot of disparate tools that we use today. vCenter Log Insight is easier to manage and it searches better than any tool we have used."

> "The real value is the dashboards, not only to see the information graphically, but to have all of the information in a single place."



Next Steps

The two participants are excited to see the planned integration with vCenter Operations, which will fully integrate monitoring and log data into a single solution. This solution will simplify operations and provide full visibility into their infrastructure. They also indicated that they would prefer a pricing model that focuses on the number of end points and not data.

"We want to see vCenter Log Insight integrated into vCenter Operations. This will mean all of the infrastructure data is in a single location where we can monitor and resolve issues from a single console."

"We like the approach on end points for pricing. It makes pricing predictable for us, and won't penalize us if a log file grows for some reason."

VMware Cloud Operations Management Vision

Highly virtualized infrastructure as the foundation for cloud exceeds the capabilities of traditional management tools and processes. A new approach to IT Operations is needed that is based on analytics, policy-based automation and unified management disciplines across infrastructure and applications. This new approach enables IT Operations to achieve higher service levels, operational efficiency and compliance with IT policies and regulatory requirements.

VMware vCenter Operations and vCenter Log Insight together enable IT organizations to optimize capacity and utilization of infrastructure resources, proactively detect and eliminate performance bottlenecks, and enforce configuration standards. A tight product integration enables seamless transition from monitoring all datacenter activity to troubleshooting and automated remediation of issues in the environment. VMware simplifies and automates cloud operations management and enables IT to focus on delivering business value to their organizations.

Retail Company Requires Effective Root Cause Analysis for a Large Distributed Environment

This company operates over 1,400 grocery stores and retail outlets throughout Europe, making it one of the largest retail chains. We interviewed the lead systems engineer who is responsible for the virtualized infrastructure including over 90 hosts running on more than a 1,000 virtual machines. He shared that although they are a large company they have a very small IT staff. With growing modernization of their stores, they are slowly becoming more reliant on IT for business operations. He told us that they had outages recently and needed better solutions for root cause analysis and trending information to prevent downtime in the future.

Reasons for Needing Log Analytics

> "There is a lot of information in the logs that can give indications of impending issues — trends that show a performance issue is just a few days away. I want to harness that information."

The engineer explained logs were only used for troubleshooting issues and that it was a largely manual process. Searching through logs was primarily conducted to find what actually caused the issues. And, often when a server went down the finger pointing would start. Yet their diligent searching and the log files would inevitably prove a storage, networking, or a bad server configuration. Nevertheless, the engineer believed that logs, and the information within the logs, could be used proactively to provide alerts early enough to prevent future downtime.

> "With a complex private cloud we have to hit the logs to find out what actually caused the problems."

vCenter Log Insight Experiences

The system engineer told us how vCenter Log Insight was up and running in less than 30 minutes, including the configuration of the entire log file feeds from the ESX hosts. From here, he said it only took a few hours to understand the product and set up his own custom dashboard. He stated that the product was very easy to use, and it quickly became a valuable tool for his organization. He noted vCenter Log Insight quickly searches through the logs and can generate an interactive graph from any piece of information. He also explained that the data could also be used to setup future alerts and monitored proactively with the dashboard.

> "I had it (vCenter Log Insight) setup with all of the ESX hosts feeding into it in under 30 minutes."

Real-World Benefits

> "We found a tricky problem in just a couple of hours, and it was with another team's devices. Usually that task would have taken days."

The engineer recounted how they started seeing performance issues within the first week of installing Log Insight. Using the tool, he shared that it only took a few hours to pinpoint the problem to a specific set of SCSI drives in the storage array. In the past, this type of problem was hard to identify because another team owned storage. But with Log Insight, he discovered the drivers' performance was degrading over time. He then used vCenter Log Insight to create a graph that illustrated the problem to his managers and the storage team. Next, he added this metric to his dashboard so they could watch the trending over time and resolve this issue before it created a problem.

> "We are able to move from reactive mode to using the log data to provide very early indications of future issues that we can resolve proactively."

The engineer shared the following benefits that vCenter Log Insight has delivered to his company:

- Faster problem resolution
- The ability to pinpoint exact devices affected by issues and which ones were causing them
- Improved communication with other teams and management
- The prevention of downtime
- Proactive maintenance

> "The graphs are so powerful it makes it very easy to get the teams on the same page and find solutions. We can brief management in minutes."

Next Steps

The team is very interested in adding vCenter Log Insight to its tool bag and looks forward to the vCenter Operations Management Suite integration when it is released. The team members believe that an integrated solution will provide the "single pane of glass" not only for information, but a single place to manage and configure their environment, alerts, and logging.

> "We can't wait for the full integration with vCenter Operations where we can have all the performance, trending, alerts, and log data in a single UI."

Telecommunications Provider Uses Log Analytics to Ensure Compliance

This large international communication service provider is headquartered in Australia and provides cell, wireline, and Internet access to its customers. We spoke with the virtualization (VI) specialist who manages more than 4,000 virtual machines in a private cloud. He shared that the company has been on a virtualization-first initiative for over a year, and they continue to see growth in the cloud environment. While uptime and availability are key, compliance and security are major drivers in their virtual environment.

Reasons for Needing Log Analytics

Today the company uses logs in a traditional manner for troubleshooting issues. Yet the VI specialist expressed that his company wants to generate more intelligent alerts from the log data and move to a proactive posture from a continually reactive mode. Today they manually grep logs, but they know that a log aggregation and search tool would save time. Under their regulation and security strategy they are required to store logs for up to six months; however, the organization currently only stores log data for a few hours.

> "vSphere can only hold its logs up to eight hours before it is overwritten, but we need to store logs for six months due to compliance and security reasons."

> "Troubleshooting is often challenging if a problem occurred in the middle of night or over the weekend. You might not get to the logs fast enough to prevent them from being overwritten."

vCenter Log Insight Experiences

Most of the initial IT problems are resolved by the company's help desk team, so the vCenter Log Insight product was used jointly by the VI specialist and help desk team. The VI specialist stated the product was installed, up and running, and searchable within an hour. He reported it had a clean, easy-to-use UI and was quite fast. And it only took minimal system resources to run it. He also noted that Log Insight only took him an hour to figure out how to build custom dashboards.

Within a few hours of installing vCenter Log Insight, the team was getting alerts for a specific cluster of servers. But they were located outside of the initial deployment. They expanded their vCenter Log Insight coverage to collect logs from that cluster and found the problem within an hour. vCenter Log Insight also provided a way to resolve their log archiving requirements, which allowed them to keep logs for six months.

"It installed and indexed within an hour. vCenter Log Insight only took me minutes to figure out, and the help desk team was doing service-related queries within an hour."

Real-World Benefits

"We used vCenter Log Insight to collect data from a problematic server cluster. Within an hour, we had solved it. This is substantially easier and faster than any other approach."

The VI specialist said it was hard to put a specific value on compliance and security, but vCenter Log Insight helps meet those critical requirements. Shortly after installing vCenter Log Insight, he and the support team were able to solve real problems. They were passionate that vCenter Log Insight was much faster and easier to use than other options. He highlighted how the dashboards and reporting capabilities improved the team's approach to preventing issues and downtime. He also noted that vCenter Log Insight delivered the following benefits to the organization:

- Faster issue resolution
- Compliance adherence
- Security compliance with forensic data
- Proactive warnings and alerts
- Root cause analysis
- Time savings for support desk, engineering, and VI teams

During the discussion about pricing models, the VI specialist was frustrated with price models based only on data volume. When his team considered a product that used the data volume model, they were already having internal debates on what logs to include or exclude. That model was incentivizing him to take risks in order to save money. He stated that VMware's approach of charging for the number of servers generating logs versus the data volume was significantly better.

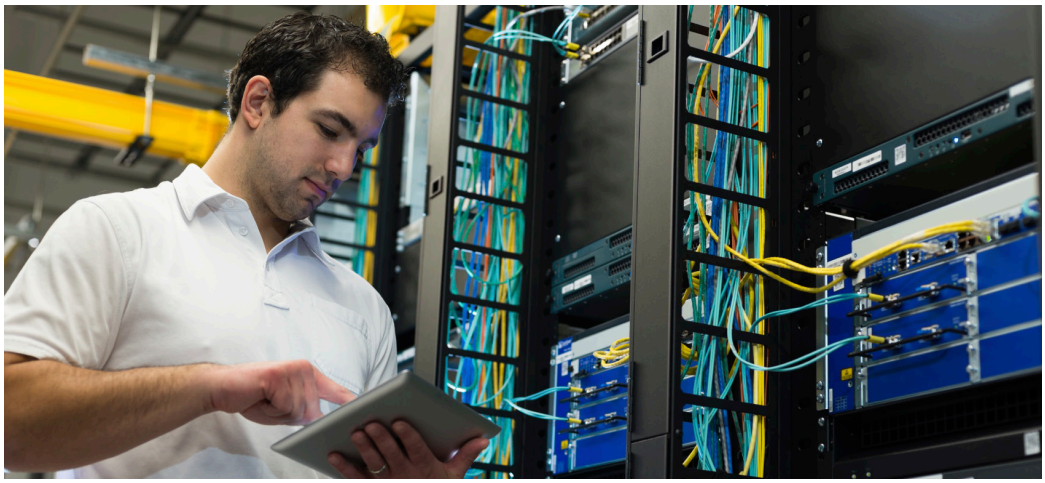
"vCenter Log Insight delivered real value to our team during the initial deployment, not only in finding issues, but providing the information to solve them faster and easier."

"To contain costs with Splunk, we were pondering which logs to not include to keep the price down. That is a bit like taking parts off an airplane and hoping you don't need them."

Next Steps

The communications company is considering migrating a core business application into a hybrid cloud. The VI specialist stated that if the vCenter Log Insight product continues to develop with the potential it shows in the initial deployment, it will be a must have for the company's hybrid cloud environments.

"vCenter Log Insight has a lot of potential already. If it works with vCenter Operations as promised, it will be the single pane of glass that everyone talks about for a hybrid cloud."



Conclusion

All participants interviewed for this study stated that collecting and searching through log files was a critical but time consuming activity for their IT operations. VMware vCenter Log Insight delivered substantial benefits and time savings, while effectively cutting arduous tasks down to minutes.

The product installed quickly, needed little configuration, and provided a very flat learning curve. Many praised the product's intuitive UI and easy to set up dashboards. Most initially used vCenter Log Insight to troubleshoot and remediate problems detected by other management systems; however, over time all participants directly stated that they now wanted to use log data for proactive issue prevention.

Furthermore, they all preferred the pricing model that charges by the number of end points and not by data volume. Users felt this gave budget predictability and did not penalize them when they needed the tool the most.

Finally, the participants believed that log data combined with VMware vCenter Operations would finally provide a complete view of their infrastructures. This would enable users to drill down from an alert to the problem and then to the cause in minutes.

dimensional research

About Dimensional Research

Dimensional Research provides practical market research services that help technology companies make smarter business decisions. Our researchers are experts in technology and understand how corporate IT organizations operate. We partner with every client to deliver actionable information that reduces risk and increases customer satisfaction. Our research services deliver a clear understanding of customer and market dynamics. For more information visit www.dimensionalresearch.com.

About VMware

VMware is the leader in virtualization and cloud infrastructure solutions that enable businesses to thrive in the Cloud Era. Customers rely on VMware to help them transform the way they build, deliver and consume Information Technology resources in a manner that is evolutionary and based on their specific needs. With 2012 revenues of $4.61 billion, VMware has more than 500,000 customers and 55,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.