HYTRUST
Cloud Under Control

Solution Brief

Enterprise-class logging for virtual infrastructure

With HyTrust you can:

- VMware virtual infrastructure (vSphere) does not provide suf cient native logging for compliance, security forensics, or rapid troubleshooting.
- SIEMs and Log Management systems do not solve this problem, because they are dependent on the log data produced by vSphere.
- HyTrust CloudControl™ provides the industry's leading solution for privileged account logging on VMware virtual infrastructure, providing compliance quality logs with no impact to admin experience.
- Integrates with all leading logging systems and SIEMs (ArcSight, Splunk, Log Insight and more)

Detailed, comprehensive event logging is critical for security incident response, compliance, and operations. A good log must tell you exactly what was done — or attempted — by whom, and when. A solid forensic trail of activity is mandatory to understand infrastructure change, implement numerous compliance control activities, and to detect and remediate security incidents.

Logging of administrative activity is of particular interest. Administrative accounts have far greater capabilities than other accounts and can perform a wide variety of potentially risky activities:

- Shutting down or otherwise disrupting critical applications
- Bypassing access controls to copy or corrupt sensitive data
- Creating or modifying user accounts or system services to create unauthorized back doors
- Tampering with or deleting log data

For all these reasons, admin accounts are very commonly the target of malware and advanced persistent threats. An attacker that can obtain admin credentials through session hijacking or spear phishing immediately has the perfect vector to deposit a malware payload and pivot deeper into the infrastructure. It should be clear therefore that not only does administrative activity need to be logged, it needs to be logged in such a way that the admin credentials cannot be used to tamper with the logs.

Defending against sophisticated APTs is all about effective response. There is general acknowledgement that attacks will penetrate your network—so what's needed is timely detection to enable rapid, appropriate response. And effective response depends on granular knowledge about what has happened, knowledge that will be unavailable unless strong logging was in place at the time of the incident.

Because the risks are so clear, compliance regimens such as PCI DSS, NIST SP 800-53, and HIPAA/ HITECH always include controls on administrative accounts and information system activity. Administrative actions typically must be logged, reviewed on a daily basis, and reconciled with approval tickets that justify the activity. In some cases further policy validation is required, for example to confirm

that the change was done within an approved change control window, or from an allowed location. Without complete, granular logging, such controls are impossible to implement.

Inadequate logging creates operational and security risks

Despite the clear need for robust logging, many IT systems do not provide it. Often the system does not log all events that may be important or required for compliance. For example, a system may log administrator logins, but not failed login attempts. In some cases the data within the log entry may be lacking. The entry may contain the obvious elements like the system name and address and the timestamp, but not other critical information such exactly which change was performed on what object.

It should be noted that log collection systems and SIEMs do not help solve this problem. Such products consume log data, they do not create it on behalf of the monitored system. If an IT system does not send the SIEM sufficient log information, the SIEM cannot possibly compensate for that deficiency, because it has no insight about what is going on within the IT system. It's only as good as the log data being sent to it.

A number of third party solutions have been developed to try to solve the problem of insufficient native logging in IT systems. Some solutions attempt to solve the problem by recording the complete, real time activity of the administrator. This "VCR style" logging can be useful for forensics, but only in very limited situations. The problem is that someone has to watch the replay of potentially hours of recording to pick out the specific admin actions one by one. This approach is neither scalable nor reliable. A sports analogy would be to compare a three-hour video of an entire baseball game to the box score, which clearly shows what each player did at a glance. Other solutions are able to capture admin activity if it is text based (that is, command line), but have no way of creating an event log from GUI-based administration. This clearly is insufficient given the prevalence of GUI-based administration for systems such as VMware vCenter.

HyTrust CloudControl: industry leading controls & logging For vmware administration

To meet security and compliance requirements for their virtualized data centers and private clouds, enterprises rely on HyTrust. HyTrust CloudControlTM was designed to be the most complete solution available for administrator and configuration controls on VMware vSphere infrastructure (with NSX virtual networking support available soon). CloudControl supports an industry leading feature set that spans all four key functional areas:

- Strong Two-Factor Authentication
- Role-Based Authorization & Access Controls
- Forensic-quality Logging
- Configuration Hardening for Platform Integrity

Available as a virtual, highly-available appliance, CloudControl has no impact on application availability or performance. With CloudControl, organizations can define policies to automate what administrators—or those who gain their credentials—can and can't do. These controls better protect sensitive data, help guarantee uptime, and meet compliance requirements by controlling and monitoring all aspects of the VMware system administration. With CloudControl, administrators stay within their "swim lanes", sensitive data is protected, and VMware operations staff can more efficiently troubleshoot and maintain the virtual infrastructure.

HYTRUST
Cloud Under Control

"Perfect defenses are not achievable – better detection is also required."

Gartner [1]

Complete logging for VMware infrastructure

HyTrust CloudControl produces the complete, detailed activity logs that VMware vSphere and vCenter do not provide. Although VMware infrastructure is a critical component of most modern data centers and private clouds, it does not provide sufficient native logging for compliance or security. CloudControl sits between vCenter/vSphere and the client PCs used to administer them, where it can monitor and log all administrator activity. CloudControl provides the logging needed for compliance, security forensics, and availability troubleshooting:

Log Parameter	VMware vSphere	HyTrust CloudControl
Time/date	•	•
Target object	•	•
Action	•	•
User ID		•
Source IP address		•
Configuration parameters		•
Secondary approval ID		•
Denied operation event		•

Integration and alerting

HyTrust CloudControl goes beyond logging to support alerting on suspicious or abnormal admin activity. Threshold-based alerts can be generated when the volume of a particular type of action is greater than normal. This is a common occurrence when admin accounts are compromised (Edward Snowden provides the ideal example). Programmable thresholds allow organizations to tune the system to eliminate false positives. And CloudControl integrates with leading SIEMs such as HP ArcSight, Splunk, VMware Log Insight and RSA Envision to support secure log retention, event correlation, and consolidated report generation.

Summary

As organizations place more and more critical and sensitive workloads on VMware virtual infrastructure, it becomes ever more important to generate and maintain robust logging on administrative activity. Indeed, it is impossible to support many compliance objectives or adequately protect sensitive data

1 Reference: www.gartner.com/technology/topics/information-security.jsp

from cyber threats without proper logging. However, VMware virtual infrastructure does not provide sufficient native logging for compliance or security forensics. HyTrust CloudControl solves this problem, without affecting application availability or performance, and without changing admin procedures. It also seamlessly integrates with leading SIEMs and log collection systems to drive efficient compliance and security reporting, and to increase up time. CloudControl should therefore be deployed by default for all virtual infrastructure hosting sensitive or regulated data or applications.

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100