

# Setting up a Splunk Server to Monitor a VMware Environment

---

## Introduction

Gathering and maintaining log files is an important part of a server administrator's duties. Using a centralized logging server, such as a syslog server offers several benefits. The log files become useful for troubleshooting purposes, if needed. Also, keeping an unaltered set of logs in a different location can aid in forensic activities after an attack.

This document explains how to set up Splunk for monitoring a VMware Environment. This includes monitoring the ESX/ESXi Server logs, the vCenter Server Logs and some of the add-on services to vCenter. It also includes generic event logging for Windows and Linux guest operating systems.

## Intended Audience

VMware Certified Professionals, System Management / Sysadmin / Operations

## Outline

1. Requirements
2. Preparing the Splunk Server
3. Installing Splunk Server
4. Setting up ESX Servers and Linux VMs for Monitoring
5. Setting up ESXi Servers for Monitoring
6. Setting up vCenter Servers and Windows VMs for Monitoring
7. Adding Miscellaneous Log Files to Splunk for Monitoring

## Resources

- This document on the web @ <http://viops.vmware.com/home/docs/DOC-1563>
- See attached document for content
- [VI:OPS Logging Zone](#) [[http://www.vmware.com/support/vi3/doc/vi3\\_vcb15\\_rel\\_notes.html](http://www.vmware.com/support/vi3/doc/vi3_vcb15_rel_notes.html) ]
- [Splunk](#)
- [Snare on Sourceforge](#) [[http://www.vmware.com/pdf/vi3\\_systems\\_guide.pdf](http://www.vmware.com/pdf/vi3_systems_guide.pdf) ]
- [Ubuntu Server Guide](#) [[http://www.vmware.com/pdf/vi3\\_io\\_guide.pdf](http://www.vmware.com/pdf/vi3_io_guide.pdf) ]
- [Ubuntu VMware Tools Guide](#) [[http://www.vmware.com/pdf/vi3\\_san\\_guide.pdf](http://www.vmware.com/pdf/vi3_san_guide.pdf) ]

- [VMO Logs KB](#) [  
[http://www.vmware.com/pdf/vi3\\_35/esx\\_3/r35u2/vi3\\_35\\_25\\_u2\\_config\\_max.pdf](http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_config_max.pdf) ]
- [VMware KB for Collecting Diagnostic Data](#)

## Author

[David Convery](#), VMware vExpert 2009



Also check out <http://www.dailyhypervisor.com/> |

## Disclaimer

You use this proven practice at your discretion. VMware, <http://www.dailyhypervisor.com> and the author do not guarantee any results from the use of this proven practice. This proven practice is provided on an as-is basis and is for demonstration purposes only.