Monitoring VMware virtualization infrastructure

You work in the IT department for a large software development company that makes heavy use of virtual machines for testing during development.

It is crucial that the virtual machines that rely on the VMware ESXi hypervisor and vSphere remain available so that the software release cycle isn't disrupted. Part of your job is to monitor all VMware infrastructure and respond to any issues that might arise.

You can use Splunk software to monitor virtual machine and virtual machine host resource usage, watch for key events that might require troubleshooting, and obtain useful inventories of your VMware environment.

Data required

Technologies:

- IT Essentials Work
- Splunk Add-on for VMware ESXi Logs
- Splunk Add-on for vCenter Logs
- Splunk Add-on for VMware Metrics

Data:

- Virtualization data
- System log data

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor VMware virtual machine performance. Depending on what information you have available, you might find it useful to identify some or all of the following.

ESXi hosts

- ESXi hosts with sustained high ballooning
- ESXi hosts with sustained high swapping
- ESXi hosts with high CPU Ready summation value
- Virtual machines currently running on ESXi host
- ESXi host version identification

vSphere

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
• vSphere configuration changes
• Recently triggered vSphere alarms

Other

• VMotion events for a specific virtual machine
• Virtual machines with high CPU Ready summation value
• Virtual machines with large file size utilization
• vCenter console logins
• VMware datastores with highest utilization
• Topology of a VMware environment

Next steps

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

• Capacity planning, compute hardware, storage, and network
• Native monitoring tools integrated with Splunk for cross-domain visibility
• Tooling for software provisioning and configuration management
• Backups, security, and compliance

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

• Mean time to problem resolution
• Mean time to root cause analysis
• Reduction in system degradation, such as underperformance or unplanned downtime

This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

• Blog: Splunk Stream in VMware environments
• Blog: VM Monitoring and capacity management
• Blog: What can you do with Splunk, VMware and AWS?
• Conf Talk: Monitoring your VMWare vSphere environment with Splunk

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.