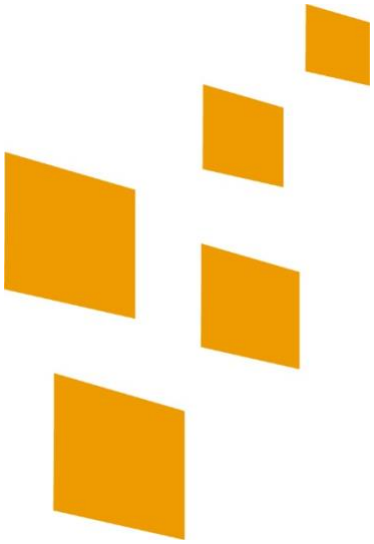

Reducing Operational Complexity with Runecast Analyzer

Achieving vSphere Optimal Performance and Minimal Downtime

White Paper

By Alastair Cooke
Technical Consultant
Demitasse Ltd

Runecast
Software-defined expertise

Contents

Executive Summary

Operating an Enterprise vSphere environment is a complex undertaking, and maintaining such environments is a critical activity for many IT departments. Business units that have applications on these vSphere platforms require optimal performance and minimal downtime. System outages cost businesses money and can be a significant risk to the overall health of the business. The average cost of downtime is estimated at $300,000 per hour[1]. Every time there is an outage, there is not simply a financial loss; the business may also lose confidence in the IT department. No matter how good the operations team is, reactive fault resolution results in downtime or performance problems. To add insult to injury, most of the problems are caused by known issues with known resolutions. To escape the break-fix cycle, a different approach is required.

Runecast provides proactive fault avoidance to minimize the risk of downtime. The Runecast solution is a patent pending automated system that compares vSphere configuration and logs with a repository of known issues and best practices. By identifying known potential issues, Runecast allows IT operations teams to get in front of faults and prevent outages. Downtime is reduced, as known faults can be corrected before they cause outages. Ensuring ongoing consistent adherence to best practices further reduces the risk of downtime and the associated business costs.

For many IT departments, security auditing and compliance are a continuous challenge. The Runecast repository includes security guidance from VMware's Security Hardening Guide. The same scanning and log analysis are validated against the security guidelines to provide immediate feedback on security compliance. The virtualization infrastructure is more secure as a result. The risk of a breach is reduced by hardening the infrastructure layer. In addition, security audits are simpler, as there is an audit log of compliance.

[1] http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

The Problem with Enterprise Virtualization

There are many challenges to address in operating a virtualized infrastructure. Many of them are caused by the complexity of enterprise IT. Others are related to how operations teams resolve issues with that infrastructure. There are seven specific areas that cause pain to the infrastructure team:

1. Technology complexity
2. Interdependence
3. Aggregated rate of change
4. Volume of Knowledge Base articles
5. Ad-hoc changes from troubleshooting
6. Long time to resolution
7. Reactive fault resolution

1. Technology complexity

Enterprise IT infrastructure has become more and more complex as new technologies are added to existing ones. Blade servers were added alongside rack servers. IP storage has been added alongside Fiber Channel and local storage. Disk-based backups were added to tape systems, and now converged backup is being added to many data centers. Servers are virtualized, adding another layer to the compute section. Storage is virtualized, bringing more complexity. Lately, network teams have started adding Software Defined Networking (SDN) which brings yet more complexity.

Often point solutions are added to address specific shortcomings. A cache may be layered in front of a storage array that is not performing adequately but not yet due for replacement. Enterprise IT teams look enviously at pictures of cloud-scale data centers with rows of identical racks, full of identical servers. This is not what we see in Enterprise data centers, where there is usually a collection of different technologies. It is much easier to add new technologies than retire old ones. All these pieces of technology require management and monitoring to ensure availability and performance. As we add different components that require management, we cannot simply add more staff. IT needs better operations software. The additional complexity that virtualization brings to a data center has been well documented. A DCIG study [2] from 2012 highlighted the complexity of virtualized environments as the cause of reduced agility and slower provisioning.

2. Interdependence

Virtualization has broken down technology silos and sped up the adoption of new technologies. At the same time, virtualization has created a lot of dependencies between different parts of the IT infrastructure. Before virtualization, each server was an island and only the network was shared by these islands. Each server had its own CPU, RAM, storage, and network cards. In a virtualized infrastructure, everything is shared and everything is connected. Each VM is dependent on a hypervisor host, which it shares with other VMs, so a misconfiguration on the hypervisor can affect tens of VMs. Many VMs on many hypervisor hosts will access the same shared storage, and the link between a VM and its storage passes through many layers. From the VM it passes through the hypervisor, then over the storage network before arriving at the storage array. Each of these layers must be optimally configured, as a misconfiguration at any layer can lead to widespread performance or availability problems. A virtualized data center is a stacked tower of technologies. Any layer in the tower can cause instability for the entire data center. IT teams need operations software that stabilizes the whole tower.

3. Aggregated rate of change

Enterprise environments strive to control change, however there is always change and in a large environment there is near continuous change. This month the backup team may deploy a new disk backup target. Next week the virtualization team may add six VLANs across 20 switches. While each item is slow to change, the number of items in an enterprise data center mean that change is constant. Each change has dependencies through that stacked tower of IT infrastructure. Every change can destabilize the entire stack, and each is

[2] https://www.dcig.com/2012/09/virtualization-gets-complexity-reality-check.html

a chance for something to go wrong or for a latent issue to cause a problem.

It is not always possible to predict the impact of a change. Every IT operations team needs ways to rapidly identify any negative effects of change. They also need to identify any latent issues in the environment that may trigger problems when updates or changes are applied.

4. Volume of Knowledge Base articles

The VMware Knowledge Base has hundreds of articles documenting potential issues with different versions or combinations of VMware and third party products. To minimize the risk of outage and to optimize performance, the recommendations of all relevant Knowledge Base articles should be applied. Being familiar with the relevant articles at any point in time is a significant challenge. An even more significant challenge is keeping up with change. Not just changes in the virtualization environment but also weekly additions to VMware's Knowledge Base articles and updates to existing ones. It is impractical to keep up to date by reading the articles as they are released or searching the Knowledge Base before any change is made. Some sort of automated system is required to get the full benefit from the VMware Knowledge Base.

5. Ad-hoc changes from troubleshooting

Planned activities are not the only cause of change in Enterprise data centers. Often change happens because of a fault. An ESXi server that experiences a recurrent system crash may have its firmware updated. Now this one server is different from our other servers. Often the troubleshooting process involves making multiple changes during a crisis. Most of the changes are ineffective and should be backed out, but often they are left in place.

A lack of consistency will lead to further support requirements. Inconsistency increases the risk of outages and increases the time to resolution. But re-establishing consistency will require further change. Either the server must be remediated to the standard configuration, or the other servers must have the same change applied. Most often the change is forgotten, and slowly every server's configuration becomes unique.

The operations team is usually required to prioritize uptime and fault resolution. They may not even have a way to track uniqueness, let alone remediate back to consistency. Every enterprise IT team needs an automated system that identifies consistency and compliance with appropriate standards.

6. Long Time to resolution

Due to the complexity of these virtualization platforms, fault resolution may be delayed, even when the fault and corrective action have been identified. It can take days for a trouble ticket to be seen by a technical resource. Once investigations begin it can take some time for data gathering, log collection and configuration analysis. Once the fault is identified and a resolution formulated, it can take some time to test the resolution process. Change management often demands that changes for performance and availability are delayed until they can be approved. This can take several weeks for large organizations and exposes the business to extended risk or performance issues. Slow resolution of IT issues has a direct link to satisfaction with IT systems. A study by the technical support industry group, HDI[3], shows a direct link between slow resolution and low satisfaction. Identifying known issues before they cause problems enables the change management process to begin before there is a business impact.

7. Reactive fault resolution

Most fault resolution requires an impact to production before any action can be taken. A server must fail or an application's performance must degrade before any action is taken. These failures have significant costs for businesses; some outages cost millions of dollars[4].

This point strikes at the heart of why Runecast was created. Most times, when an outage occurs in a well-managed data center, the cause is a fault that was known to the system vendor. It might be a bug

[3] http://www.thinkhdi.com/~/media/HDICorp/Files/Library-Archive/Insider%20Articles/mean-time-to-resolve.pdf
[4] http://datacenterpost.com/wp-content/uploads/2015/10/State-of-the-data-center.pdf

that is patched in a later software release or it might be a default configuration that doesn't work for a specific combination of components. The engineer who is resolving the fault will use Google to discover the known issue and apply its known resolution. There are thousands of known issues with various combinations of components. VMware documents new issues in the Knowledge Base articles every week. Some operations teams review every new article for relevance to their environment, but few teams can also track the articles that relate to their environment as it changes. The impracticality of identifying these known bad conditions before they cause a problem led to the creation of the Runecast product. IT operations teams need software that can identify known issues before they cause an outage.

The Problem with Small Business Virtualization

Small businesses have many of the same issues as their larger counterparts, simply at a smaller scale. Their virtualization infrastructure is still a collection of complex technologies that are interdependent. They still have reactive fault resolution and can have delays in that resolution. In a small business environment, it can be even harder to achieve consistency as there is less IT management process in place. An enterprise vSphere deployment may use Host Profiles for point-in-time consistency across their ESXi servers, a small business is unlikely to have the vSphere license with Host Profiles. They will be dependent on consistent manual configuration, and manual adherence to best practices. Manual processes are renowned for their inconsistency, leading to inconsistency in SMB vSphere deployments.

Small business, small team

The additional challenge for smaller businesses is that they have fewer staff and less opportunity for those staff to specialize. IT staff in smaller businesses are usually responsible for far more than the vSphere environment. Often one person looks after the Windows infrastructure and applications with only a limited amount of time to focus on the vSphere platform. These staff must be broadly skilled, without a deep specialization. Often specialists are hired in from consulting companies for specific projects. These specialists are expensive and are only available for the duration of the project. After the project responsibility reverts to the generalist IT staff.

It is impossible for SMB IT staff to keep up-to-date on all the technologies that are in their data centers. An automated system that brings in outside expertise, without consulting costs is the only way to ensure that small business virtualization is up to the task at minimal cost.

A New Approach to Fault and Problem Management

Addressing these issues requires a different approach to managing an enterprise virtualization platform. One element is to use automated scanning of the environment, ideally multiple times per day. Another element is centralization of system logs for analysis. The results need to be compared to a set of known issues and best practices. The entire objective is to identify any known problematic conditions before they impact availability.

1. Expert system maintained by a trusted third party

There is a wealth of troubleshooting information in the VMware Support Knowledge Base. Most often this is where engineers Googling vSphere problems will end up. This Knowledge Base does not lend itself to automated scanning; it is written and formatted to be read by humans. VMware does not provide a way to check whether there are any Knowledge Base articles that are relevant to your environment.

Runecast provides this ability, a programmatically accessible repository being the core of the product. Runecast analyzed all the VMware Knowledge Base articles and added the actionable results to the Runecast central repository. Every Runecast appliance has a local copy of the repository as the reference for all analysis. As VMware publishes new Knowledge Base articles, these are added to the central repository. These updates are delivered online to Runecast appliances running on-premises. The latest Knowledge Base articles are then included in the on-premises analysis.

2. Identify best practice

The VMware Knowledge Base identifies configurations for stability and performance. It does not necessarily include guidance for creating a vSphere deployment that is secure and easy to operate and upgrade. This is why best practice guidance is part of the Runecast repository: simple guidance like having the same shared datastores accessible to all ESXi servers in a cluster, or having the same servers providing coordinated time for the cluster.

3. Security scanning

Security compliance is not simply about passing audit; security breaches have significant financial cost to businesses. A study by the Ponemon Institute [5] found the average cost of a security breach is around $4 million. In addition to the financial cost there can be a huge cost in lost consumer confidence when a breach is disclosed. Business names like Target, Sony, and Ashley Madison have become synonymous with their security breaches. A strong security stance throughout the infrastructure is essential to support secure applications and practices.

VMware publishes guidance on security configuration in its Security Hardening Guides. These hardening guides also feed into the Runecast repository. The repository combines the VMware Knowledge Base, VMware Security Hardening Guide and expert best practice to create a curated repository of everything that can go right or wrong with a vSphere deployment.

4. Automated scanning

Misconfigurations can happen at any time and become a risk to service. An automated scanning system can rapidly identify the risk conditions. Waiting for the weekly or monthly checks leaves the service at risk for far longer than is necessary. The performance impact of system scanning on the virtualization platform is weighed against the risk of leaving conditions undiscovered.

A lightweight scanning method allows Runecast to scan the entire vSphere environment in minutes. Scanning can occur multiple times each day without a performance impact. Frequent scanning will minimize the amount of time a fault condition is in place, reducing the risk of an outage. Frequent updates to the Runecast repository ensure that new issues added to the VMware Knowledge Base are immediately identified on the next scan.

[5] http://fortune.com/2016/06/15/data-breach-cost-study-ibm/

5. Log monitoring

Not all faults are about ESXi server configurations. Many faults are caused by the interaction of the ESXi servers with external components, such as switches and storage networks. Runecast uses an automated Syslog configuration to receive all the logs from ESXi servers and VMs, including any error messages such as storage timeouts or VMkernel error messages. As the Syslog messages are received by the Runecast appliance, they are compared in real time to the known issues in the Runecast repository.

6. Identify known faults

By combining scanning and log collection with the repository and we have a mechanism for identifying potential faults before they manifest major symptoms. Any events that correlate to a known fault will trigger a warning in the Runecast console. Similarly, combinations of software and configurations that are known to cause issues will be identified. For example, Runecast can identify when a combination of ESXi versions and drivers requires a specific advanced setting to be stable. When an issue is identified, the Runecast console includes the steps for remediation and links to the source of the information.

7. Simplified compliance

For many regulated industries, security compliance is a continuous practice. To avoid vulnerabilities it is important to have secure configurations and robust procedures. Runecast will check for compliance with the VMware Security Hardening guide's recommendations. Naturally, this compliance checking can be tailored to the specific combination of security configurations that your organization requires.

Periodic security scanning is an important procedure for security compliance, ensuring that systems remain compliant over time. This is a better solution than simply being compliant at a single point in time, and more reliable than manually checking for compliance. Having continuous scanning against a baseline makes security audits much simpler.

8. Secure deployment

Runecast deploys as a virtual appliance inside your on-premises vSphere environment. All scanning and analysis are conducted locally on the appliance. The appliance contains a full copy of the Runecast repository. None of your data or metadata is transmitted to the Internet; in fact, no Internet connection is required for the Runecast appliance to operate. Updates to the repository are delivered as appliance updates, using the VAMI interface directly over the Internet. Alternatively, updates can be downloaded and transferred to non-Internet connected deployments.

Conclusion

Runecast provides a way to identify issues in your vSphere deployment that may impact it in the future. Proactively resolving these issues will reduce the risk of outages and downtime, with the associated reduction in cost to the business. Runecast provides a repository of VMware Knowledge Base documents, security hardening guidance and expert best practices. Your vSphere configuration and logs are compared to this repository to identify possible issues before the issue causes a fault in your environment. Correcting the identified issues prevents faults and provides better uptime and lower risk. The result is a vSphere infrastructure that is more valuable to and more trusted by the business.

Visit www.runecast.biz to start making your infrastructure rock solid.

How to deploy Runecast Analyzer

Register at http://runecast.biz/register to activate your evaluation copy of Runecast Analyzer.

Contact Runecast

innovate@runecast.biz

Chat with the Runecast team live at www.runecast.biz