eBOOK

Skillz to Master Your Virtual Universe: SOAR Framework

by Kong Yang

4 New Skills to Become the Master of Your Virtual Universe

INTRODUCTION

SECURE

OPTIMIZE

AUTOMATE

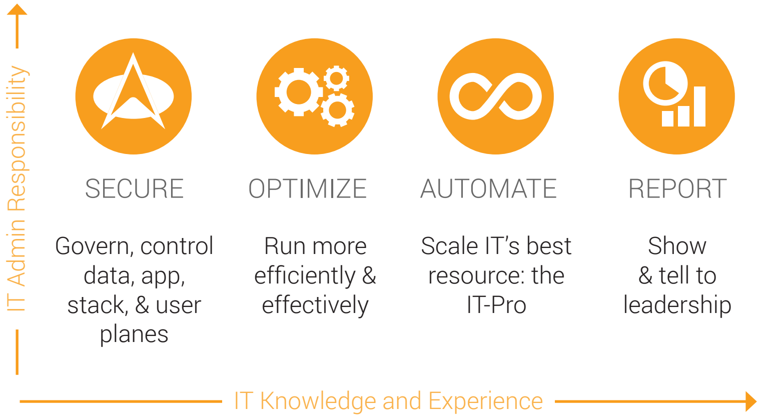
REPORT

CONCLUSION

Take IT Flight with the SOAR Framework

In a previous eBook, I introduced the DART Framework as a series of foundational skills that virtualization administrators can leverage to master their virtual universe. In this eBook, it's time to take your IT career flight beyond the final frontiers of your virtual universe. Do it with the SOAR Framework:

> *"It's time to take your IT career flight beyond the final frontiers of your virtual universe."*


IT Admin Responsibility
SECURE
Govern, control data, app, stack, & user planes
OPTIMIZE
Run more efficiently & effectively
AUTOMATE
Scale IT's best resource: the IT-Pro
REPORT
Show & tell to leadership
IT Knowledge and Experience

SOAR Framework

SOAR-ING SKILL SET

Security should be top of mind with every IT professional — we are all responsible for security operations whether directly or indirectly. Securing IT delves into governance, compliance and control of data, applications, stacks, and user planes.

Optimization boils down to maximizing the return on investment (ROI) of IT. We all get that IT budgets are getting squeezed or being diverted into new investment areas. Optimizing allows IT professionals to do more with less in their data center environment. If done well, it highlights command and control over any given data center ecosystem and opens the door to many new career opportunities.

Automation is the skill that allows IT professionals to scale both their data center and their career aspirations. Whether it's through scripts, workflows, templates, or blueprints, automation is a skill that reclaims the most important resource for any IT pro—time.

Reporting is the least glamorous IT skill, but it's the one that will most likely get you promoted. Essentially, it revolves around communicating how great of a job you are doing managing your data center efficiency or making your case to get the necessary tools to deliver what the business needs.

> *"Reporting is the least glamorous IT skill, but it's the one that will most likely get you promoted."*

TIME FOR IT PROFESSIONALS TO SOAR

Each SOAR skill aids IT professionals in dealing with change management in the era of continuous service integration and continuous service delivery. SOAR skills are apropos for virtualized environments as they can be applied to any tech construct and tech domain. Time to shatter the shackles of silos!

In the following chapters, I will cover secure, optimize, automate, and report as advanced skills that IT administrators need to exceed the boundaries of their current IT universe.

REFERENCES:

1. IT's a MAAD World

2. DART Framework

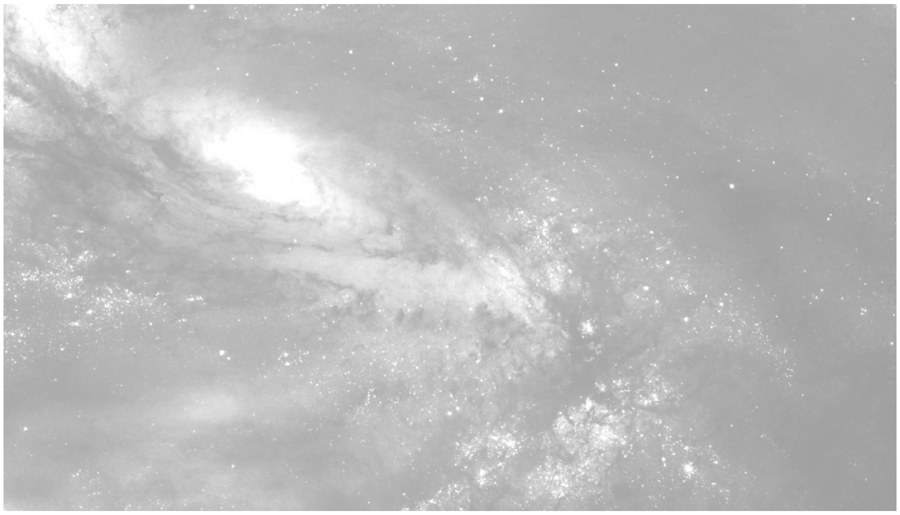
Secure Your Virtual Environments

In the intro chapter, I discussed how to extend your mastery of your virtual environment beyond its current domain. I listed a set of skills that will allow any virtualization administrator to take flight in their IT career: Security, Optimization, Automation, and Reporting. In this chapter, I'll cover what it means to secure the virtual environment

SECURITY: CONTROL AND GOVERNANCE ACROSS THE DATA, APPLICATION, AND USER PLANES.

The principle of security guides you around governance and control as 1s and 0s traverse across the IT planes. Security is a loaded term that can encompass all manners of sin committed against the IT domain. In the virtual environment, just because the resources are abstracted doesn't mean that you're immune to security breaches. Ultimately, the end-goal of breaches is to gain access and control of the data, application, and user planes. Accordingly, IT needs to defend multiple planes across multiple domains.

The figure below highlights the many vendors who operate in the security space and all the different entities that require securing, from infrastructure to SIEM to cyber to IAM to application.



Momentum Partners' Security Sector Strategic Landscape (Q2 2015)

WHY IS SECURITY IMPORTANT?

The end goal of security is to prevent your environment—which includes your data, applications, and users—from being breached. If you understand the threats to your security, then you'll also understand the protocols needed to stop them.

FOUR COMMON SECURITY THREATS THAT IT ADMINISTRATORS DEAL WITH ARE:

» **DDOS Attacks**

- An attack designed to overwhelm servers with bogus traffc that causes websites and spplications to slow down and eventually become unavailable.

» **Phishing Schemes**

- An attack that sends fraudulent email disguised as a legitimate communication that lures recipients into clicking a malware link

» **Poor Patch Management**

- Leaving operating systems, browsers, applications, and databases unpatched allow hackers to access your organization's IT assets.

» **User Error**

- Human error can lead to IT nightmares such as losing a work device with unencrypted, sensitive data, falling for phishing schemes, or surfing to malware-infested websites.

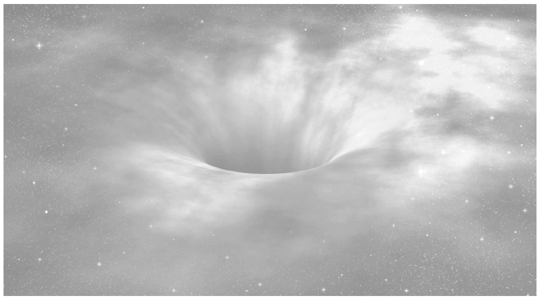
> *"The end goal of security is to prevent your environment from being breached."*

SCARCITY OF SECURITY OPS PROFESSIONALS

Security presents a tremendous challenge and career opportunity for IT professionals. The topic is much too vast to properly cover in a single chapter, so consider this an appetizer for future eBooks.

As the digital transformation expands, the gap in security ops personnel is growing as well. For example, this 2016 Cybersecurity infographic from the ISACA shows the shortage of security ops professionals.

> *"Security starts with being aware of potential security threats and developing countermeasures."*



http://www.isaca.org/cyber/PublishingImages/Cybersecurity-Skills-Gap-1500.jpg

NIST CYBERSECURITY FRAMEWORK

Security starts with being aware of potential security threats and developing countermeasures. IT professionals looking to get a start in security should leverage the NIST Cybersecurity Framework, which covers the following risk management functions in detail. The next page outlines the functions along with their definitions from the NIST Cybersecurity Framework pages 10-11 and Appendix A.

NIST Cyberscurity Framework

IDENTIFY

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

PROTECT

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

The NIST cybersecurity framework is one that is drilled into security operations professionals and provides great context into creating security ops protocol for its environments. These functions are intended to work concurrently.

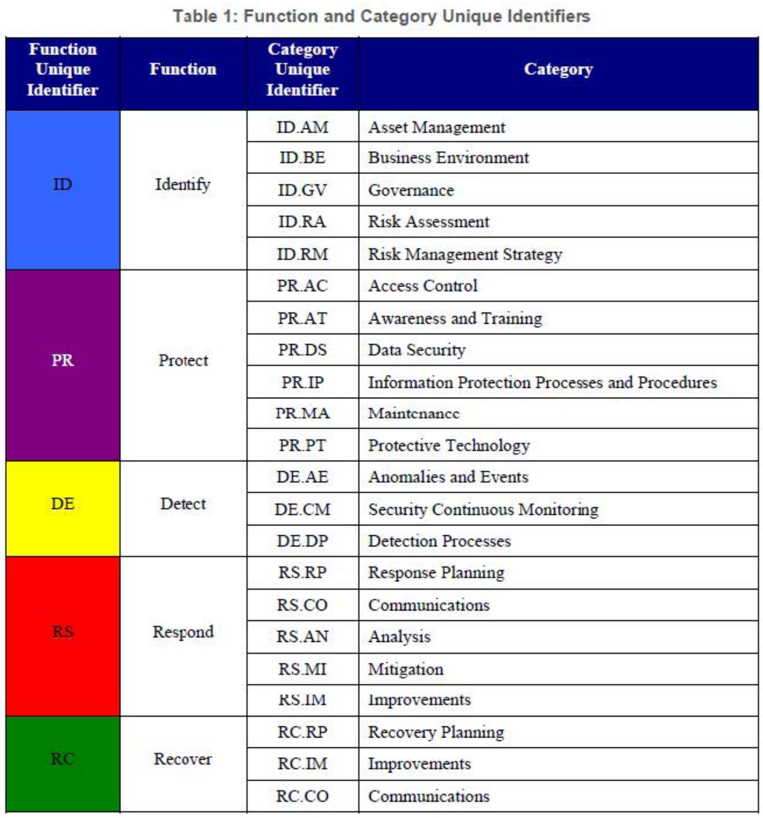


Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

From Appendix A of the NIST Cybersecurity framework
© 2014 National Institute of Standards and Technology. All rights reserved.

> *“Security instills trust throughout your IT planes and ensures that your business can continue to close deals with confidence.”*

SECURE YOUR IT OPERATIONS AND ANOTHER CAREER PATH

Security is a skill that can propel a virtualization administrator’s career into the final frontier. It instills trust throughout your IT planes and ensures that your business can continue to close deals with confidence.

In the next chapter, I’ll talk about Optimization, the next critical skill any virtualization master needs to soar.

ADDITIONAL REFERENCES FOR SECURITY OPS:

» How to solve today’s top three virtual environment challenges by Kong Yang on Network Computing, November 13, 2015

» SolarWinds Lab™ Episode 27

» thwackCamp 2015: Crossing the Great Divide: Conversations between IT, Networking,and Security Ops

Optimize Your Virtual Environments

Previously, I covered security as a skill to take your IT career to the next level. In this chapter, I'll walk through optimization as another high-value skill in the virtual environment. To truly appreciate the importance of optimization, you have to understand the blood, sweat, and tears that comes with gaining optimization wisdom.

> "Optimization is a skill forged from tuning your focus on achieving an end goal."

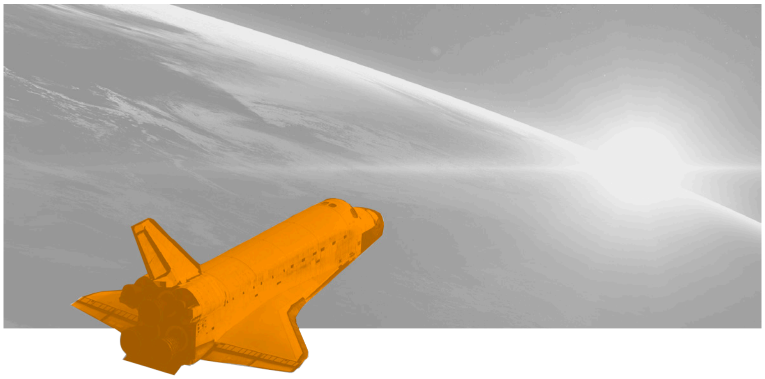
OPTIMIZATION: MORE THAN MEETS THE I→T

Optimization is a skill that requires a clear end goal in mind. Optimization focuses on understanding the interactions of the IT ecosystem, the behavior of the application stack, and the interdependencies of systems inside and outside their sphere of influence in order to deliver success in business objectives.

If one were to look at optimization from a theoretical perspective, each instantiation of optimization would be a mathematical equation with multiple variables. Think multivariate calculus where an IT pro tries to find the maxima as other variables change with respect to one another.

I'm positive that Professor Thomas LaRock could lead us through a database optimization course leveraging multivariate calculus to analyze the deterministic SQL systems with N degrees of freedom. Meanwhile, I could leverage my ECE background and lead a discussion on applied control systems theory and how its application can optimize performance in your dynamic, virtual data centers.

This begs the question: is calculus and control systems theory knowledge required to optimize your virtual environment? The answer is no. While it may help to formulate theories to visualize and formulate the overall concepts, IT is all about keeping IT stupid simple. That should be the IT ideal after all.



Focus on achieving an end goal.

How to Avoid Optimization Pitfalls

1. Have a simple optimization plan

2. Prioritize your most deliverable as defined by all the stakeholders

3. Optimize with that deliverable as the focal point

4. Understand the behavior and relationship of change as it pertains to your optimization goal

5. If additional optimization tasks are appended to the original task, communicate the risks clearly and concisely

- *Sometimes there is no hope for an IT executive looking to make their mark even at the expense of their direct reports.*

OPTIMIZING FOR EVERYTHING IS REALLY OPTIMIZING FOR NOTHING

Optimization is a skill forged from tuning your focus on achieving an end goal. As such, the one trap that all IT pros should avoid is trying to do too much. Optimizing for everything and everyone usually ends in disappointment because it can make the Quality of Service worse for everyone involved.

> *"To successfully optimize is to carefully balance change management of the infrastructure and the application service with respect to the needs of the business and end users."*

CLOSING

Optimization is a perfect skill for the continuous service delivery and continuous service integration era. Its simple premise does not allow an IT professional to stop and settle. To successfully optimize is to carefully balance change management of the infrastructure and the application service with respect to the needs of the business and end users. Optimization is an exercise in balancing an equation that is dynamic in nature and requires constant monitoring and feedback in order to deliver the most optimal experience.

Optimization is an exercise in balancing an equation that is dynamic in nature.

Optimization is a high-reward skill that builds upon the DART skills framework. It seeks to maximize the utility of IT resources as it delivers the best-in-class Quality of Service to end users. In the following chapter, I'll discuss the Automation skill, the next SOAR skill that virtualization admins need to take flight in their careers.

Automate Your Virtual Environment Processes

In the last chapter, I covered optimization as a skill to keep your IT environment in tip-top shape by constantly delivering the most optimal Quality of Service (QoS). In this section, I'll walk you through automation as another value-added skill for the virtual environment.

AUTOMATION IS:

» One part best practice

» One part policy

» And one part execution

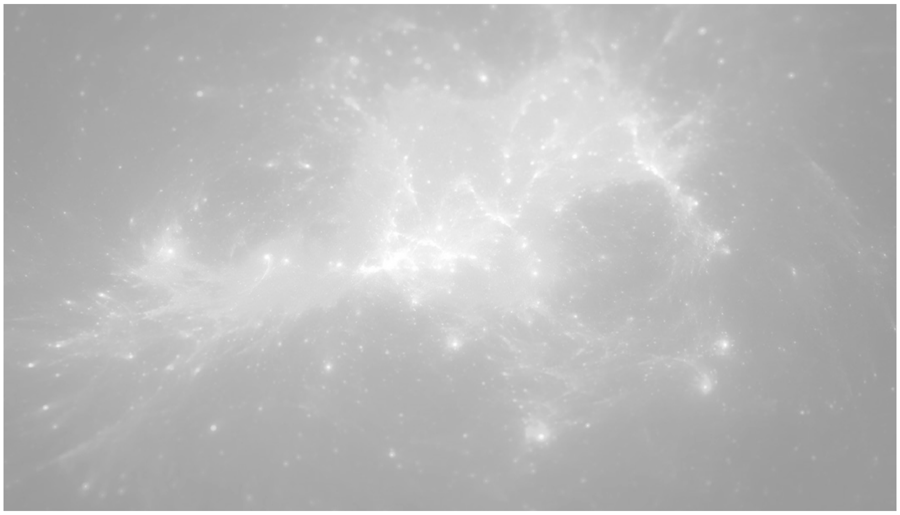
AUTOMATION IS THE ONLY WAY TO SCALE IT'S MOST VALUABLE RESOURCE ➛THE IT PROFESSIONAL

Automation is a skill that requires detailed knowledge and comprehensive experience with a specific task. That's because a task needs to be fully encapsulated in a workflow script, template, or blueprint. Automation, much like optimization, focuses on understanding the interactions of the IT ecosystem, the behavior of the application stack, and the interdependencies of systems to deliver the benefits of economies of scale and efficiency to the overall business objectives. And it embraces the do-more-with-less edict that IT professionals have to abide by.

> *“Unfortunately, automation cannot differentiate between good and bad practices.”*

AUTOMATE AWAY

Automation is the culmination of a series of brain dumps covering the steps that an IT professional takes to complete a single task. These are steps that the IT pro is expected to complete multiple times with regularity and consistency. The singularity of regularity is a common thread in deciding whether to automate an IT process. The chart below, entitled “Geeks and Repetitive Tasks,” gives you a good perspective on an IT professional's decision to automate.



Geeks and Repetitive Tasks: http://i.imgur.com/ONoeM.jpg

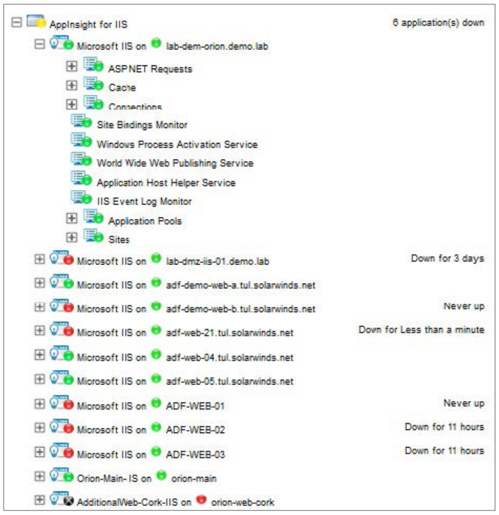
AUTOMATE THE IT WAY: SCRIPTS, TEMPLATES, AND BLUEPRINTS

Scripts, templates, and blueprints embody IT automation. They create the foundation of an IT professional's practice and methods. Ideally, automation is based upon best practices and tried-and-true IT methods. Unfortunately, automation cannot differentiate between good and bad practices. Therefore, automating bad IT practices will lead to unbelievable pain that scales across your data centers. With this in mind, keep automation stupid simple. First, automate at a controlled scale and follow the mantra, "Do no harm to your production data center environment." Next, monitor the automation process to make sure that every step executes as expected. Finally, analyze the results and use your findings to make necessary adjustments to the automation process.

AUTOMATION BY TEMPLATE EXAMPLE

Automation can take many forms since its purpose is to minimize repetitive actions. The example below shows how to set up application performance monitoring (APM) for applications that spin up and down over time. This is where leveraging an APM template can make your job as an IT professional easier. You'll get the benefits of consistency across all monitored applications as well as embedded best practices and key performance metrics at a quick glance.

> *"Automation is the skill that allows an IT professional to scale beyond what they can do solo."*



```
⊟ AppInsight for IIS                                                  6 application(s) down
   ⊟ Microsoft IIS on ● lab-dem-orion.demo.lab
        ⊞ ASP.NET Requests
        ⊞ Cache
        ⊞ Connections
          Site Bindings Monitor
          Windows Process Activation Service
          World Wide Web Publishing Service
          Application Host Helper Service
          IIS Event Log Monitor
        ⊞ Application Pools
        ⊞ Sites
   ⊞ Microsoft IIS on ● lab-dmz-iis-01.demo.lab                      Down for 3 days
   ⊞ Microsoft IIS on ● adf-demo-web-a.tul.solarwinds.net
   ⊞ Microsoft IIS on ● adf-demo-web-b.tul.solarwinds.net                  Never up
   ⊞ Microsoft IIS on ● adf-web-21.tul.solarwinds.net       Down for Less than a minute
   ⊞ Microsoft IIS on ● adf-web-04.tul.solarwinds.net
   ⊞ Microsoft IIS on ● adf-web-05.tul.solarwinds.net
   ⊞ Microsoft IIS on ● ADF-WEB-01                                         Never up
   ⊞ Microsoft IIS on ● ADF-WEB-02                                Down for 11 hours
   ⊞ Microsoft IIS on ● ADF-WEB-03                                Down for 11 hours
   ⊞ Orion-Main- IS on ● orion-main
   ⊞ AdditionalWeb-Cork-IIS on ● orion-web-cork
```

AppInsight™ for IIS™ template from SolarWinds® Server and Application Monitor.

CLOSING

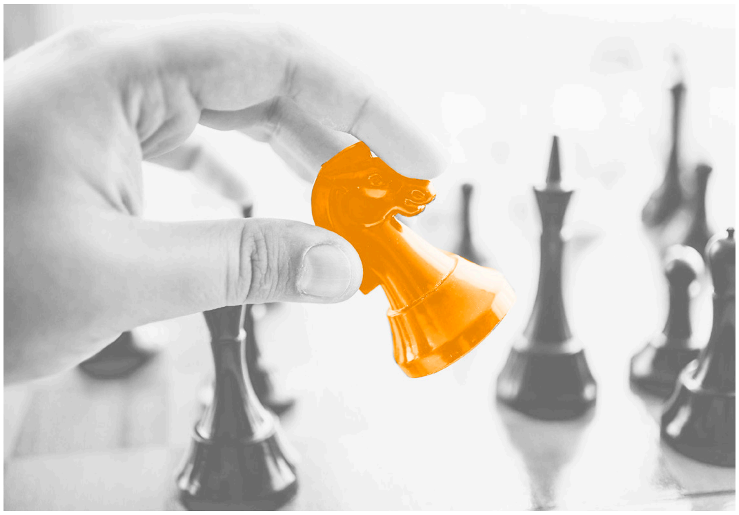
Automation is the skill that allows an IT professional to scale beyond what they can do solo. It is also a skill that builds upon the DART and optimization skills, maximizing an IT professional's productivity by freeing up time to perform other tasks. In the final chapter, I'll talk about reporting, the last SOAR skill that virtualization admins need to soar in their professional careers

Report on Your Virtual Environment

In this final chapter, I conclude with reporting as the final value-add SOAR skill needed to master the virtual environment. Reporting is all about supplying the intended audience with what they need to make a decision.

REPORTING: THE DECISION-MAKER'S AMMO

Reporting molds data and logged events into a summary that highlights key facts to help the end user make a quick, yet sound decision. Reporting is neither glamorous nor adrenaline-pumping, like the experience you get with the other SOAR skills, but utilizing it will help you get on the promotion fast track.



Reporting highlights key facts to help the end user make a quick, yet sound decision.

REPORTING IS BETTER THAN SLIDEWARE

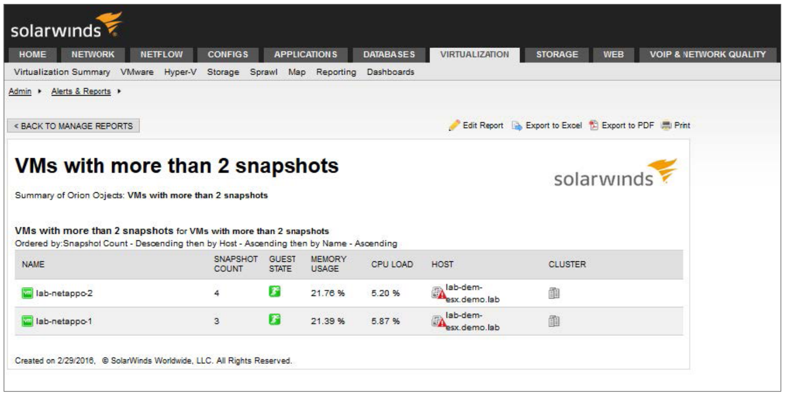
IT reporting at its best is pure art backed by pure science and logic. It is storytelling with charts, figures, and infographics. The intended audience should be able to grasp key information quickly. In other words, keep it stupid simple.

Those of you following this eBook series and my IT resolution for 2016 know that I've been beating the "keep it stupid simple" theme pretty hard. This is because endless decision-making across complex systems can lead to second-guessing, and we don't want that. Successful reporting takes the guesswork out of the equation by framing the problem and solution in a simple, easily consumable way.

The most important aspect of reporting is knowing your target audience and creating the report just for them. Next, define the decision that needs to be made. Make the report pivot on that focal point, because a decision will be made based on your report. Finally, construct the reporting process in a way that will be consistent and repeatable.

REPORTING EXAMPLE

Monitoring reports can cover IT operation statuses such as 'what virtual machines (VMs) are being monitored' to specific situations such as 'what VMs have multiple snapshots.' The latter situation would indicate a VM that undergoes quite a bit of change. Reports can also cover aspects that span both IT operations and business operations. For instance, creating an inventory of Windows® VMs may help you plan for and justify an upgrade.



VMs with more than 2 snapshots

Summary of Orion Objects: **VMs with more than 2 snapshots**

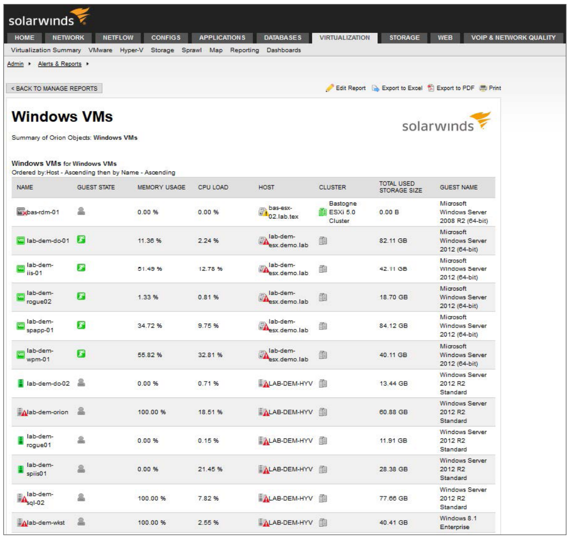
VMs with more than 2 snapshots for VMs with more than 2 snapshots
Ordered by:Snapshot Count - Descending then by Host - Ascending then by Name - Ascending

NAME	SNAPSHOT COUNT	GUEST STATE	MEMORY USAGE	CPU LOAD	HOST	CLUSTER
lab-netappo-2	4		21.76 %	5.20 %	lab-dem-esx.demo.lab	
lab-netappo-1	3		21.39 %	5.87 %	lab-dem-esx.demo.lab	

Created on 2/29/2016, © SolarWinds Worldwide, LLC. All Rights Reserved.

Report showing VMs with more than two snapshots

Reports can also cover aspects that span both IT operations and business operations. For instance, creating an inventory of Windows© VMs may help you plan for and justify an upgrade.



Windows VMs

Summary of Orion Objects: **Windows VMs**

Windows VMs for Windows VMs
Ordered by:Host - Ascending then by Name - Ascending

NAME	GUEST STATE	MEMORY USAGE	CPU LOAD	HOST	CLUSTER	TOTAL USED STORAGE SIZE	GUEST NAME
bas-rdm-01		0.00 %	0.00 %	bas-esx-02.lab.tex	Bastogne ESXi 5.0 Cluster	0.00 B	Microsoft Windows Server 2008 R2 (64-bit)
lab-dem-dc-01		11.36 %	2.24 %	lab-dem-esx.demo.lab		82.11 GB	Microsoft Windows Server 2012 (64-bit)
lab-dem-iis-01		51.49 %	12.78 %	lab-dem-esx.demo.lab		42.11 GB	Microsoft Windows Server 2012 (64-bit)
lab-dem-rogue02		1.33 %	0.81 %	lab-dem-esx.demo.lab		18.70 GB	Microsoft Windows Server 2012 (64-bit)
lab-dem-spapp-01		34.72 %	9.75 %	lab-dem-esx.demo.lab		84.12 GB	Microsoft Windows Server 2012 (64-bit)
lab-dem-wpm-01		55.82 %	32.81 %	lab-dem-esx.demo.lab		40.11 GB	Microsoft Windows Server 2012 (64-bit)
lab-dem-dc-02		0.00 %	0.71 %	LAB-DEM-HYV		13.44 GB	Windows Server 2012 R2 Standard
lab-dem-orion		100.00 %	18.51 %	LAB-DEM-HYV		60.88 GB	Windows Server 2012 R2 Standard
lab-dem-rogue01		0.00 %	0.15 %	LAB-DEM-HYV		11.91 GB	Windows Server 2012 R2 Standard
lab-dem-spiis01		0.00 %	21.45 %	LAB-DEM-HYV		28.38 GB	Windows Server 2012 R2 Standard
lab-dem-sql-02		100.00 %	7.82 %	LAB-DEM-HYV		77.66 GB	Windows Server 2012 R2 Standard
lab-dem-wkst		100.00 %	2.55 %	LAB-DEM-HYV		40.41 GB	Windows 8.1 Enterprise

Report for Windows VMs

CLOSING

Reporting is a necessary skill for IT professionals. It helps you provide decision-makers with the evidence they need to make a determination. Reporting needs to leverage the other DART and SOAR skills so that reports become a valuable asset instead of merely a check mark on someone's to-do list. When utilized effectively, reporting can propel IT pros to new career paths and to new IT frontiers.

Conclusion

SECURE, OPTIMIZE, AUTOMATE, REPORT YOUR WAY TO THE TOP

The SOAR skills framework is about realizing value-add skills and quickly surfacing them for immediate consumption. The benefits start with instilling trust, exceeding Quality-of-Service expectations, extending scale and agility, and providing just-in-time justification. These four SOAR skills—Secure, Optimize, Automate, and Report—are definitely in demand in the '–as-a-Service' era. The cool thing is that these skills have been in demand for as long as IT has been around—just like the DART skills. Escape your IT career silo with the SOAR skills.

REFERENCE MATERIALS

DART eBook

Monitoring eBook

Geek Speak Blog

thwack Community

SolarWinds Lab

ABOUT THE AUTHOR

Kong Yang is a Head Geek at SolarWinds with over 20 years of IT experience specializing in virtualization and Cloud management. He is a VMware® vExpert™, Cisco® Champion, and active contributing thought leader within the virtualization and Cloud communities.