ESG
Enterprise Strategy Group | Getting **to the bigger truth.** ™

ESG Lab Review

Protecting Virtual Environments with Spectrum Protect Plus from IBM

Date: November 2017 **Author:** Vinny Choinski, Senior Validation Analyst

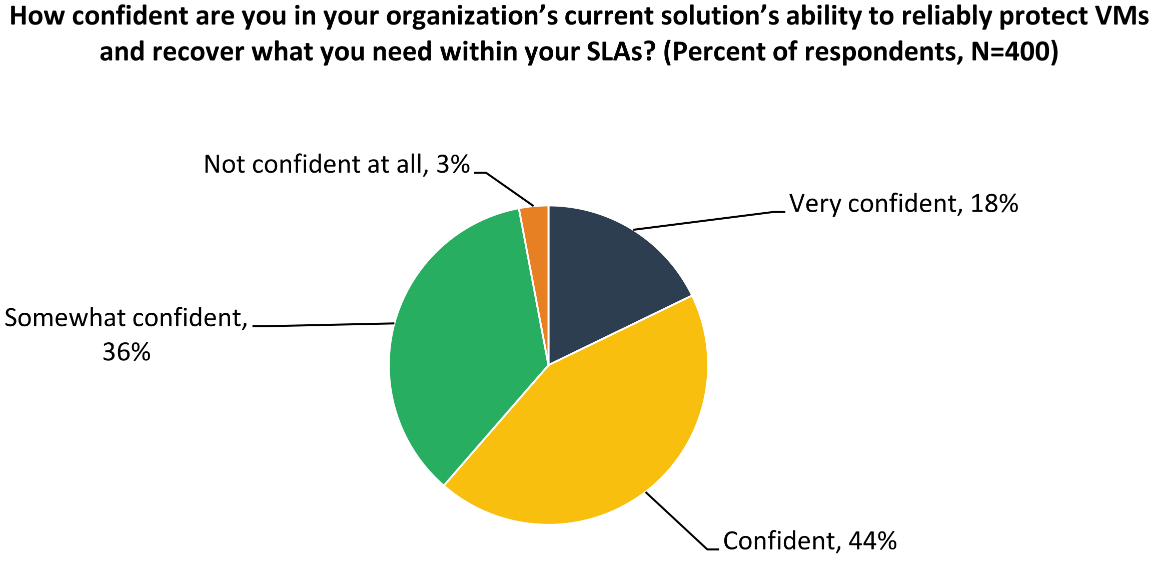
Abstract

This ESG Lab Review documents hands-on validation of the IBM Spectrum Protect Plus solution with a focus on how IBM makes deployment and management easy, while delivering multi-workflow recovery agility.

The Challenges

Even today, the reliable protection and recovery of virtual environments continues to be a daunting task for many IT organizations. That said, backup and recovery software does not always make VM protection and recovery easy. As an example, and perhaps most alarmingly, one in nine VM recoveries fails because the data was never backed up.[1] When looking into why VM recoveries fail, one finds a startling range of causes. With so many challenges—the less-than-perfect track records of IT organizations when it comes to VM protection, coupled with failures to meet modern-day SLAs—it is not surprising that some respondents report they continue to lack complete confidence in their VM protection and recovery solution.[2]

Figure 1. Confidence Level of Current Backup Solution's Ability to Protect VMs and Meet Recovery SLAs



Source: Enterprise Strategy Group, 2017

It's apparent through the introduction of the Spectrum Protect Plus solution that these challenges have not been ignored by IBM. Now IBM customers can quickly and easily deploy a solution specifically designed to meet the challenges of virtual machine data protection and administration.

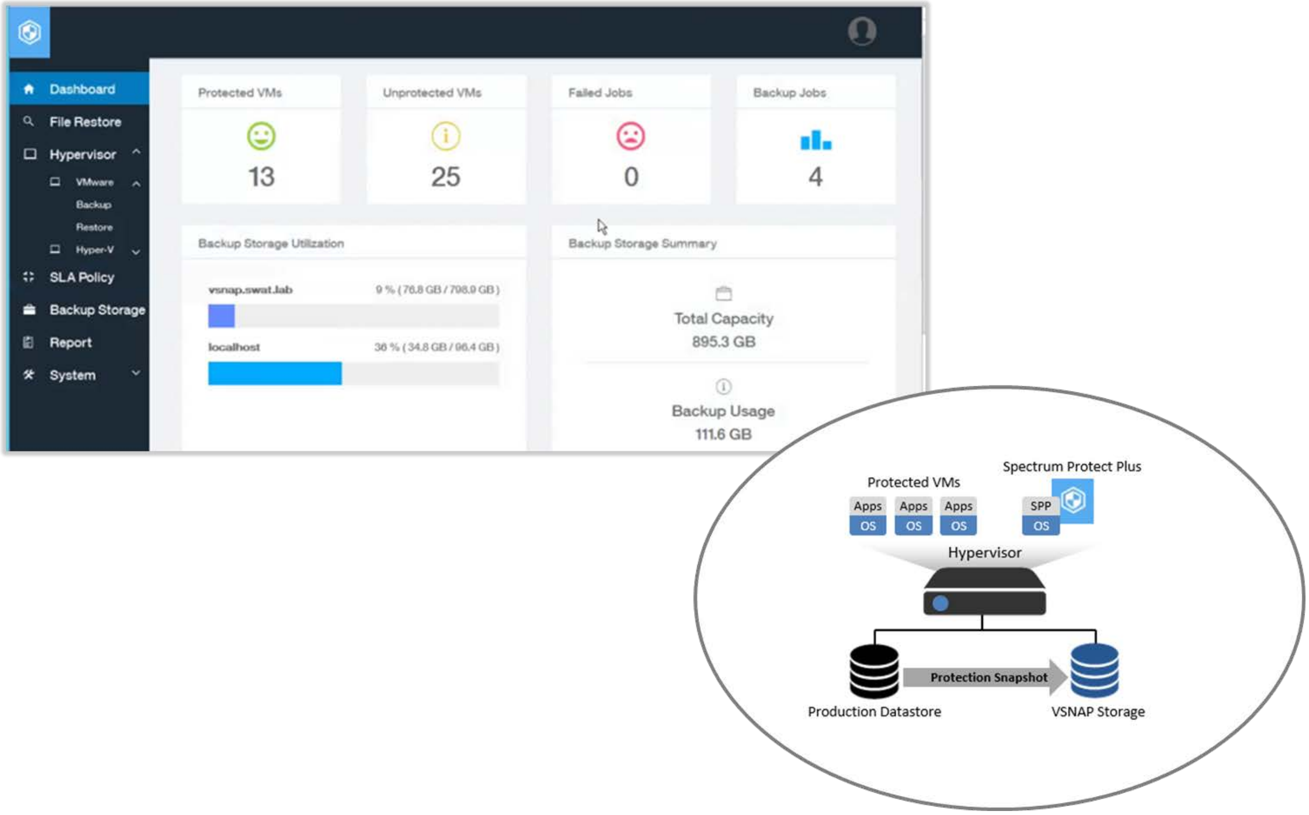
[1] Source: ESG Brief, *Reliable Virtualization Protection Continues to Elude Many Organizations*, October 2017.
[2] ibid.

The Solution: IBM Spectrum Protect Plus

IBM Spectrum Protect Plus is a data protection and availability solution for virtual environments that provides data availability using snapshot technology for rapid backup, recovery, and data management. Spectrum Protect Plus leverages its snap technology to support and automate multiple workflows including data protection, development, analytics/reporting, test, and operations. It can be deployed as a standalone solution or integrate with your IBM Spectrum Protect environment to offload copies for long-term storage and data governance with scale and efficiency.

Spectrum Protect Plus was specifically designed with virtual machine data protection and administration in mind. It can be deployed, without the need for backup agents, in minutes and be protecting virtual environments in as little as an hour. The service level agreement (SLA) policy-based user interface makes data protection management easy with intuitive global search for fast recovery.

Figure 2. Solution Overview



Source: Enterprise Strategy Group, 2017

Key features include:

Quick to Deploy: The use of open virtual machine (OVF) templates and the agentless architecture make deployment fast and enables data protection within an hour.

Easy to Use: The SLA policy-based management interface makes configuring backup jobs quick and easy. It also provides an at-a-glance dashboard view of backup compliance and storage utilization.

Fast Recovery: The global file catalog features enable instant file-level search and restore across many recovery points.

Advanced Data Governance: The integration with IBM Spectrum Protect for efficient long-term storage enables archive across flexible media—including tape, disk, and cloud—to meet data governance requirements.

ESG Lab Validated

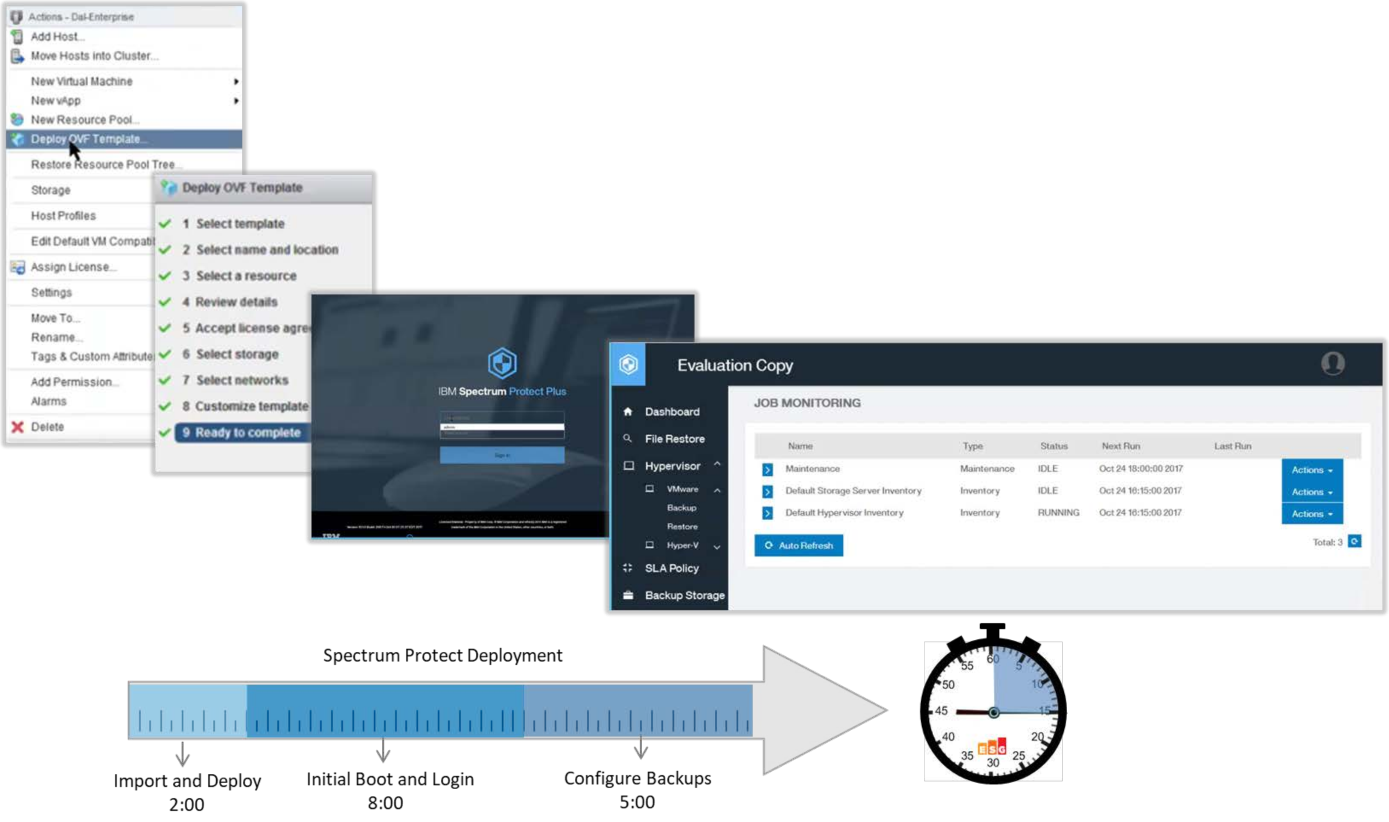
ESG Lab performed hands-on evaluation of the IBM Spectrum Protect Plus solution from our corporate office in Milford, MA by leveraging a remote IBM demo environment. Validation was focused on how IBM makes deployment and management easy, while delivering multi-workflow recovery agility.

Easy Deployment and Management

ESG Lab began its validation of the Spectrum Protect Plus solution with an exploration of the base deployment process. The solution can be deployed as a virtual machine in VMware and Microsoft Hyper-V environments and can protect both VMware and Hyper-V virtual machines from either type of deployment. For this project, we conducted the Spectrum Protect Plus deployment in a VMware test environment. To help make the VMware implementation process easy, IBM has packaged the Spectrum Protect Plus solution in an open virtual machine format template. The template contains the Spectrum Protect Plus application and OS configured with 100 GB of disk space to be used as a data protection repository, and the IBM VSNAP storage components. IBM VSNAP is a storage service or process specifically designed as a data repository for the Spectrum Protect Plus application to write to. VSNAP comes packaged with Spectrum Protect Plus but can also be deployed and run on its own VM or physical host as an independent storage service.

As shown in Figure 3, ESG was able to walk through a basic Spectrum Protect Plus deployment in approximately 15 minutes, including the kickoff of an initial backup job for a virtual machine in the test environment. We deployed from a previously downloaded OVF template stored in a directory on a vSphere Client in the test environment.

Figure 3. Spectrum Protect Plus VMware Deployment Process



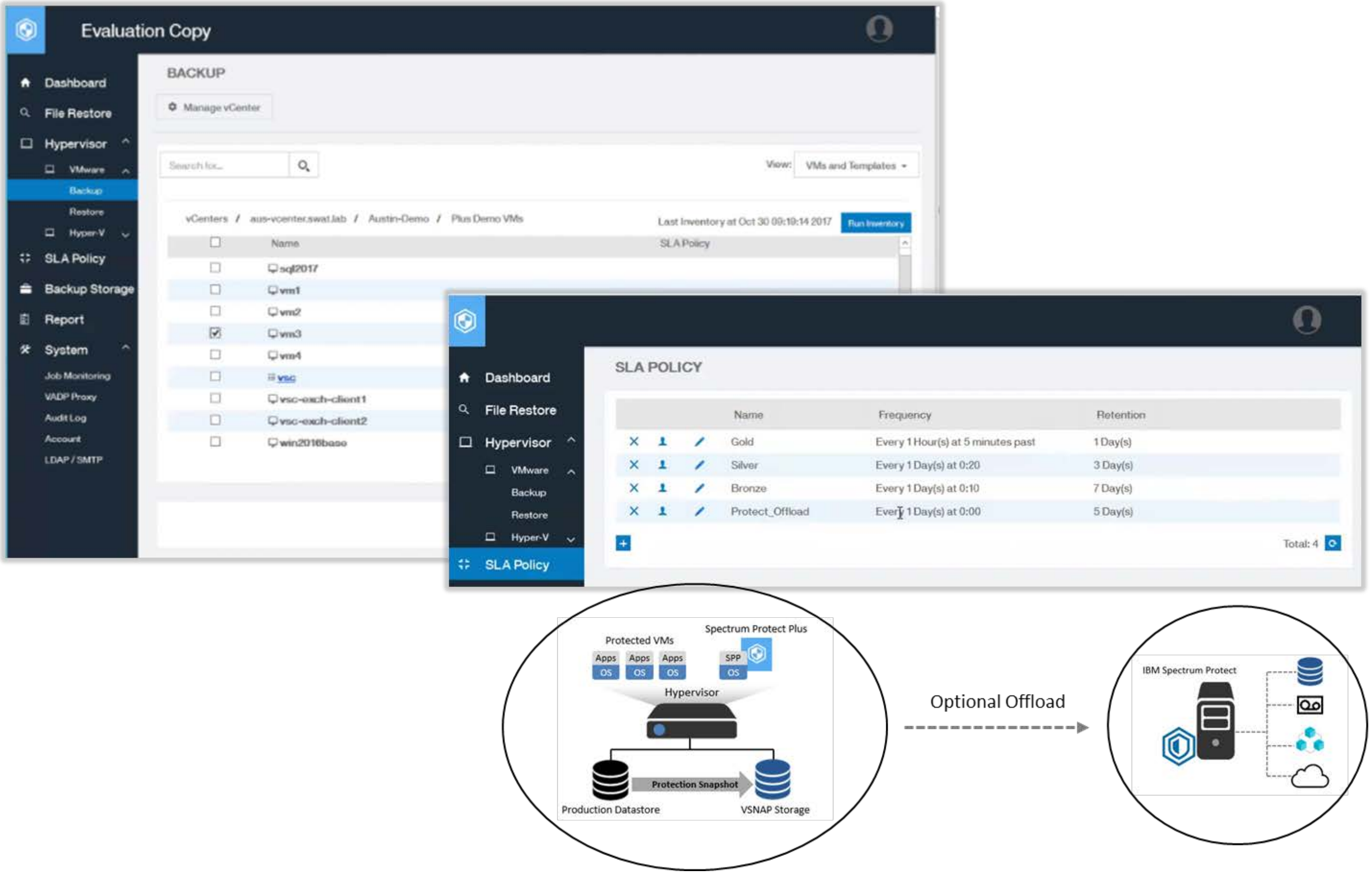
Name	Type	Status	Next Run	Last Run	
Maintenance	Maintenance	IDLE	Oct 24 18:00:00 2017		Actions
Default Storage Server Inventory	Inventory	IDLE	Oct 24 16:15:00 2017		Actions
Default Hypervisor Inventory	Inventory	RUNNING	Oct 24 16:15:00 2017		Actions

Source: Enterprise Strategy Group, 2017

From the vSphere Client, as shown in Figure 3, ESG selected the ***Deploy OVF Template*** option, which launched the OVF template configuration wizard. With the network address settings and naming convention documented, it took approximately two minutes to configure, import, and deploy the template. We also used thin provisioning for the storage and did not select any custom settings. Once the new Spectrum Protect Plus VM appeared on the VMware host, it took about eight additional minutes to run through the initial boot/configuration process, which then allowed us to access the Spectrum Protect Plus login screen. After logging into the management interface, it took ESG another five minutes to configure a backup policy with default settings and initiate a backup job for one of the VMs in the new configuration.

Next, ESG conducted a detailed review of the Spectrum Protect Plus backup configuration process. We started by adding a VMware vCenter Server to the Spectrum Protect Plus configuration. The process was straightforward: We entered the hostname and login credentials of the vCenter Server into the Spectrum Protect Plus management interface. Once the vCenter Server was added, an inventory of all its associated resources automatically started. The inventoried resources included all the host servers, VMs, datastores, and network configurations. When the vCenter Server Inventory completed, and the virtual machines associated with the vCenter Server displayed in the Spectrum Protect Plus dashboard view as unprotected VMs.

Figure 4. Backup Configuration Process



BACKUP

vCenters / aus-vcenter.swat.lab / Austin-Demo / Plus Demo VMs

Last Inventory at Oct 30 09:19:14 2017

□	Name	SLA Policy
□	sql2017	
□	vm1	
□	vm2	
☑	vm3	
□	vm4	
□	vsc	
□	vsc-exch-client1	
□	vsc-exch-client2	
□	win2016base	

SLA POLICY

Name	Frequency	Retention
Gold	Every 1 Hour(s) at 5 minutes past	1 Day(s)
Silver	Every 1 Day(s) at 0:20	3 Day(s)
Bronze	Every 1 Day(s) at 0:10	7 Day(s)
Protect_Offload	Every 1 Day(s) at 0:00	5 Day(s)

Total: 4

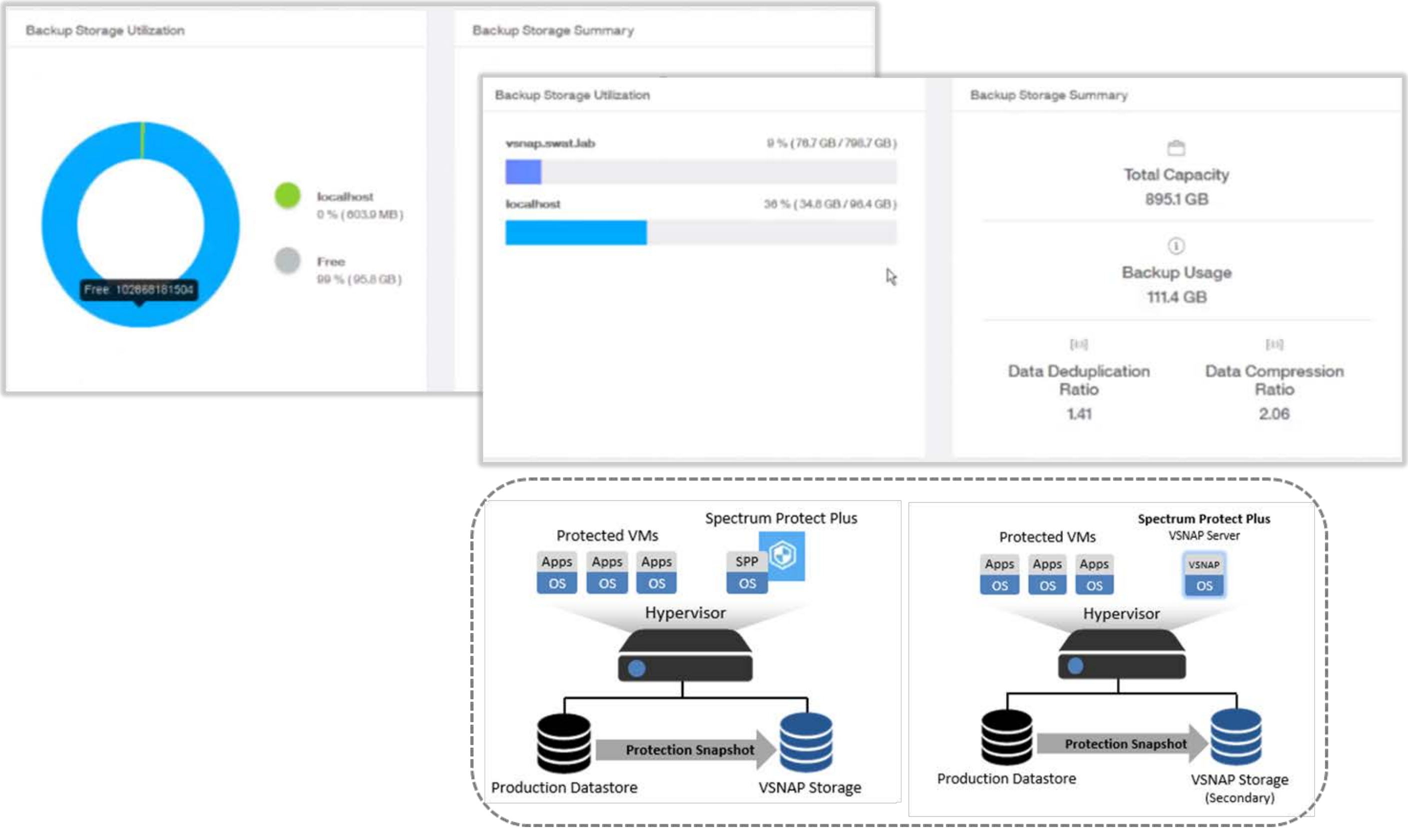
Source: Enterprise Strategy Group, 2017

Next, from within the Spectrum Protect Plus management interface, ESG navigated the vCenter Server resource structure to the *Plus Demo VMs* VMware host. We then assigned the VMs associated with the host to the preconfigured Gold SLA policy and started a backup job. The SLA policies define how the backup data will be managed. SLA policy options include backup frequency, retention, and the desired VSNAP storage repository. The three preconfigured SLA policies are Gold, Silver, and Bronze and they are set up during deployment. Gold is the most aggressive policy, with more frequent backups to the most localized VSNAP storage to facilitate the quickest restore of the most recent copy.

The Bronze policy is the least aggressive. ESG noted that each policy can be easily modified and custom policies can be added to tailor backup management for any business environment. As shown in Figure 4, ESG added the custom policy *Protect_Offload* to send data to an IBM Spectrum Protect environment for long-term data retention.

Finally, as shown in Figure 5, ESG added storage to the test environment to expand the size of the backup repository. The upper left side of the figure shows the base 100 GB of VSNAP storage included with the initial deployment of Spectrum Protect Plus. As shown at the bottom of Figure 5, we added 100 GB of storage by deploying a VSNAP virtual machine on a second hypervisor in the test environment. The VSNAP service dynamically provides storage to Spectrum Protect Plus during backup and recovery operations. VSNAP can be deployed on a virtual machine or even on a physical Linux server in the protection environment.

Figure 5. VSNAP Storage Overview


Backup Storage Utilization

localhost
0 % (603.9 MB)

Free
99 % (95.8 GB)

Free 102868181504

Backup Storage Summary

Backup Storage Utilization

vsnap.swat.lab 9 % (78.7 GB / 798.7 GB)

localhost 36 % (34.8 GB / 96.4 GB)

Backup Storage Summary

Total Capacity
895.1 GB

Backup Usage
111.4 GB

Data Deduplication Ratio
1.41

Data Compression Ratio
2.06

Source: Enterprise Strategy Group, 2017

Why This Matters

Organizations are constantly looking for ways to simplify and automate data protection operations for their virtual environments. Continually growing and evolving production workloads demand that today's data protection solutions be agile, easy to use, and easy to deploy.

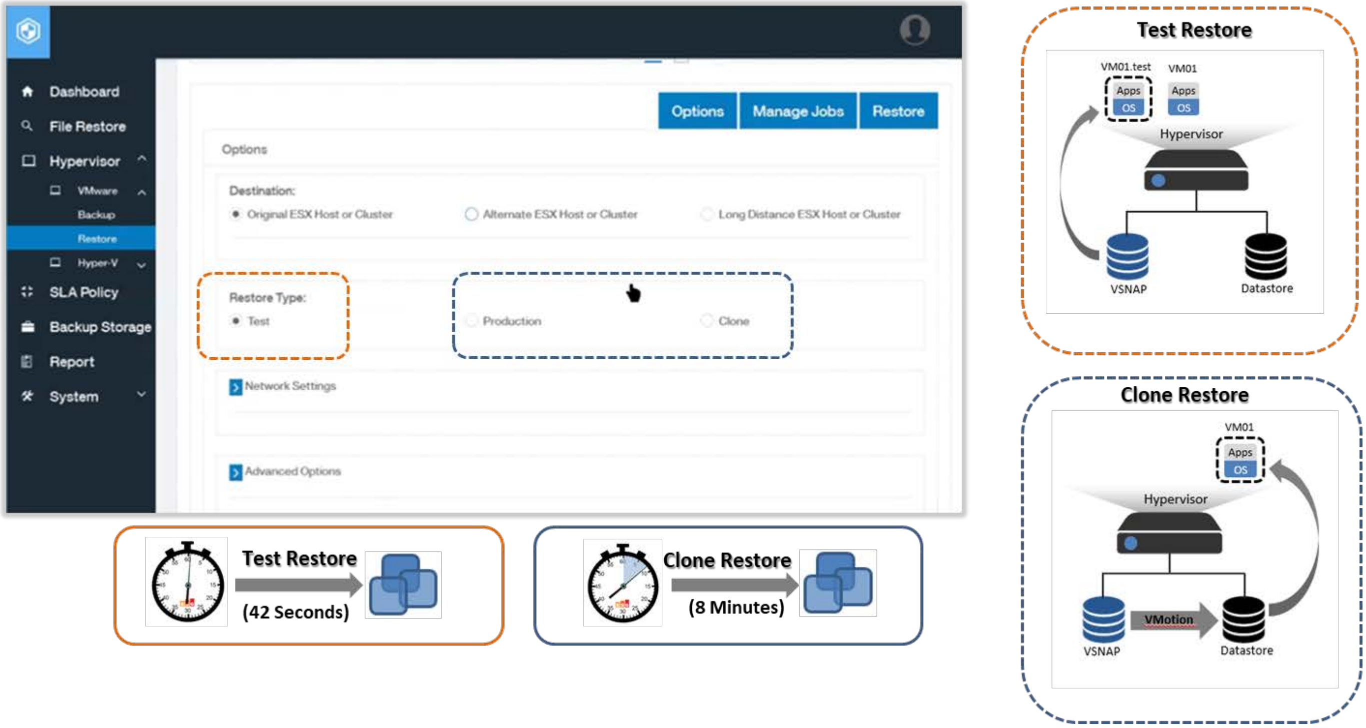
ESG validated that Spectrum Protect Plus from IBM is extremely flexible, easy to use, and easy to deploy. The solution is specifically designed for virtual environments and is tightly integrated with the infrastructure it is protecting. It leverages native APIs for data protection, SLA policies for easy management, and storage components that easily integrate with virtual environments where you need them.

Recovery Agility

Recovery is undeniably the most important aspect of any data protection solution. After all, it's why backups are created in the first place. In today's highly virtualized environments, the requirements of data protection solutions go far beyond the successful recovery of a chunk of data. Today, easy file-level recovery, instant system-level recovery, and the ability to leverage backup images to run multiple workflows directly from the backup repository are expected.

ESG began its validation of the recovery capabilities of the Spectrum Protect Plus solution from IBM by exploring the process and options for restoring a full virtual machine. After successfully completing a number of backup jobs with different SLA policies, we were able to use the Spectrum Protect Plus management interface to browse a list of recovery points. We then selected a recovery point for a VM that best matched the restore outcome we wanted. As shown in Figure 6, Spectrum Protect Plus offers a number of options for virtual machine recovery. A user can select the recovery destination and the type of restore, choose to modify network settings, and select the target datastore under the advanced tab.

Figure 6. VM Recovery



Options

Destination:
● Original ESX Host or Cluster ○ Alternate ESX Host or Cluster ○ Long Distance ESX Host or Cluster

Restore Type:
● Test ○ Production ○ Clone

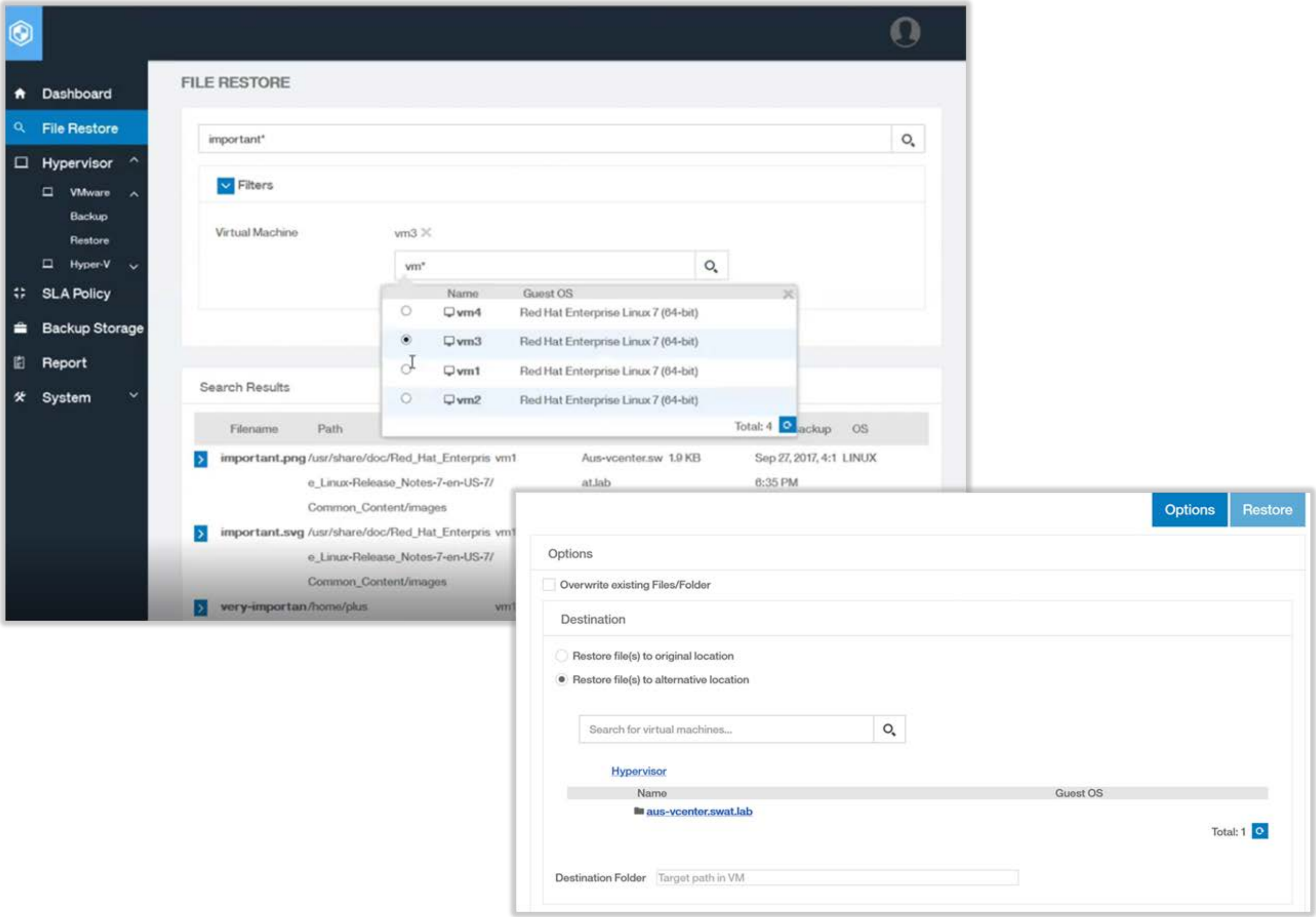
Source: Enterprise Strategy Group, 2017

As shown in Figure 6, the destination option allows a VM to be restored to its original host or cluster, an alternate host or cluster, and a long-distance host or cluster. ESG successfully tested a VM restore to an original host and a restore to an alternate host.[3] We did not test a long-distance restore because our demo environment was not configured to support that option. For the recovery to the original host, we chose a restore type of *Test*. As shown in Figure 6, ESG first conducted a test restore of *VM01* to the original host. This type of restore runs the VM directly from the VSNAP repository and appends *.test* to the end of the VM's name. It took approximately *42 seconds* to recover the VM in test mode. The restore job will remain active and the VM will continue running from the VSNAP repository as long as the VM is needed. We then conducted a restore to an alternate host. For this job, we used a restore type of *Clone*. With this type of restore, the VM initially runs from the VSNAP repository while a background process restores data to a production datastore using VMware vMotion. It took approximately *eight minutes* to recover the VM in clone mode.

[3] The test recovery VM had a 40 GB disk drive, eight GB of RAM, one CPU, a one Gb ethernet connection, and a Windows Server 2016 OS.

Finally, ESG explored the solution’s file-level restore capabilities. To deliver this feature, Spectrum Protect Plus implemented a dedicated catalog for file indexing and search. Any VM in the environment can be added to or excluded from the file catalog. If a VM does not contain user type file data, it may not need to be cataloged. As shown in Figure 7, this file catalog approach allows file-level search and restore of all cataloged files directly from the Spectrum Protect Plus management interface. Searches can be conducted with wild cards and filters, such as a specific VM, to speed the search. Once a file for recovery has been identified, it can be easily restored to the original or alternate location.

Figure 7. File-level Recovery



FILE RESTORE

important*

Filters

Virtual Machine: vm3

vm*

	Name	Guest OS
○	vm4	Red Hat Enterprise Linux 7 (64-bit)
●	vm3	Red Hat Enterprise Linux 7 (64-bit)
○	vm1	Red Hat Enterprise Linux 7 (64-bit)
○	vm2	Red Hat Enterprise Linux 7 (64-bit)

Total: 4

Search Results

Filename	Path				ackup	OS
important.png	/usr/share/doc/Red_Hat_Enterprise_Linux-Release_Notes-7-en-US-7/Common_Content/images	vm1	Aus-vcenter.swat.lab	1.9 KB	Sep 27, 2017, 4:16:35 PM	LINUX
important.svg	/usr/share/doc/Red_Hat_Enterprise_Linux-Release_Notes-7-en-US-7/Common_Content/images	vm1				
very-importan	/home/plus	vm1				

Options

□ Overwrite existing Files/Folder

Destination

○ Restore file(s) to original location

● Restore file(s) to alternative location

Search for virtual machines...

Hypervisor

Name	Guest OS
aus-vcenter.swat.lab	

Total: 1

Destination Folder: Target path in VM

Source: Enterprise Strategy Group, 2017

Why This Matters

There is a lot of pressure on data protection professionals these days, especially in highly virtualized environments, to keep pace with new business initiatives and the new production infrastructure that supports them. IT organizations are constantly being asked to do more with less, and they don’t have the time or money to deploy new infrastructure for every business initiative—not to mention the staff to manage it.

ESG confirmed that when it comes to business resiliency, Spectrum Protect Plus from IBM can help IT organizations meet these challenges. From a single, easy-to-use interface, IT can manage data protection, disaster recovery, test and development, and business continuance all from a single solution specifically designed for virtual environments.

The Bigger Truth

We all know IBM is not new to the data protection market. The company has a long history of delivering enterprise-class data protection applications, with Spectrum Protect as its flagship product. IBM also knows that developing anything more than a niche point solution with rudimentary features in the backup and recovery space, especially for highly virtualized infrastructure, can be a demanding task. Even today, the reliable protection and recovery of virtual environments continues to be a daunting task for many IT organizations. It's apparent through the introduction of the Spectrum Protect Plus solution that these challenges have not been ignored by IBM.

During our review, ESG confirmed that Spectrum Protect Plus was in fact quick and easy to deploy, and easy to manage. We were happy to see the solution packaged in OVF template format. ESG was able to do a basic deployment of Spectrum Protect Plus in approximately 15 minutes. We also liked the SLA policy-based management schema. The preconfigured policies make it easy to get started and can be easily customized and adjusted as the data protection environment grows and changes. ESG found the recovery features quite agile; it was just as easy to recover a full virtual machine as it was to do a file-level restore. Many data protection solutions for virtualized environments sacrifice file-level recovery functionality for robust full VM recovery, but Spectrum Protect Plus does both well.

ESG was pleased with how the SLA policy schema and the VSNAP storage components aligned. The VSNAP storage repository can be decoupled from the application and deployed on a host at an appropriated location. This means that a backup policy can be configured for recovery from the most local storage repository. In fact, even with the one Gb ethernet small test environment used for this report, ESG was able to do a test type recovery of a 20 GB virtual machine in approximately 42 seconds, and a clone type recovery for that same VM in approximately eight minutes.

Overall, ESG was impressed with Spectrum Protect Plus from IBM. It should be a pretty easy choice for existing IBM customers with growing virtual environments, especially with the integration into IBM Spectrum Protect. However, for new customers, the correct packaging and pricing could prove critical. ESG believes that integration with other major backup applications or a built-in cloud connector for long-term storage management could help attract new customers.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.