

Lab Validation Report

EMC VNX Total Protection Pack

Continuous Local, Remote, and Application Protection with Unified Management

By Vinny Choinski with Brian Garrett

September 2011

Contents

Introduction	3
Background	3
EMC VNX Total Protection Pack	4
ESG Lab Validation	6
Test Bed	6
Ease of Management	7
Continuous Protection	10
Application Protection and Replication with Replication Manager	13
Solution and Application Analysis with Data Protection Advisor	15
ESG Lab Validation Highlights	17
Issues to Consider	17
The Bigger Truth	18
Appendix	19

ESG Lab Reports

The goal of ESG Lab reports is to educate IT professionals about emerging technologies and products in the storage, data management and information security industries. 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. This ESG Lab report was sponsored by EMC.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. Copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482.0188.

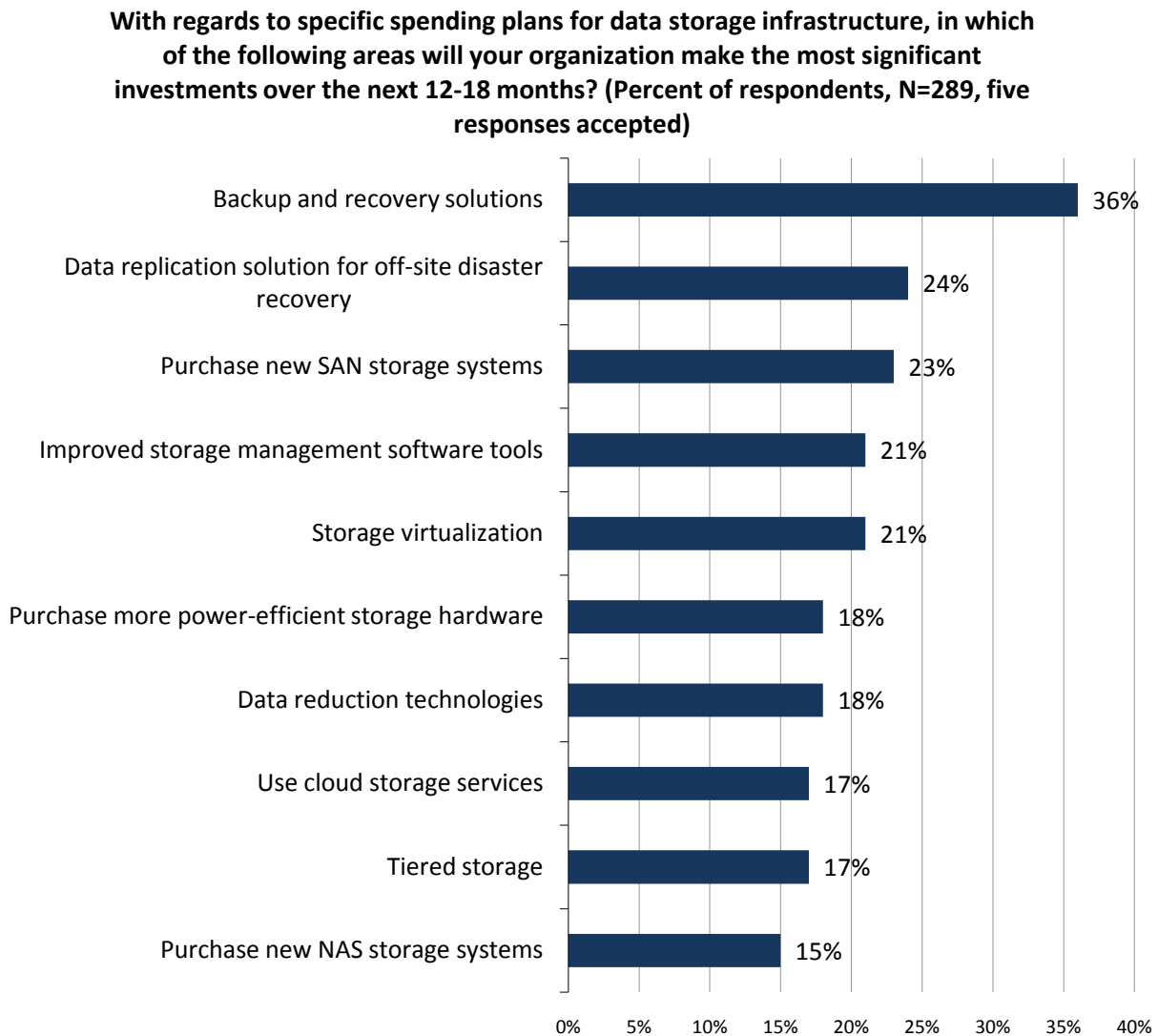
Introduction

This ESG Lab Validation report documents the results of hands-on testing of local, remote, and application protection components of the [EMC VNX Total Protection Pack](#), which consists of RecoverPoint/SE, Replication Manager, and Data Protection Advisor for Replication Analysis. ESG Lab evaluated both replication and consolidated management capabilities at an EMC lab facility in Hopkinton, MA.

Background

ESG recently asked IT professionals in North America and Western Europe about their top storage spending priorities over the next 12-18 months. Their responses make clear the importance of data protection: the top two priorities were backup and recovery solutions (36%) and data replication for off-site disaster recovery (24%). Also high on the list was improving storage management software tools (21%). Given the financial damage that can occur in a data loss event, the focus on data protection makes sense.¹

Figure 1. Top Ten Data Storage Infrastructure Spending Plans



Source: Enterprise Strategy Group, 2011.

¹ Source: ESG Research Brief, [2011 Storage Infrastructure Spending Trends](#), January 2011.

EMC VNX Total Protection Pack

The EMC VNX Total Protection Pack provides local, remote, and application data protection for EMC VNX arrays. With EMC RecoverPoint/SE serving as the core replication engine, this data protection suite integrates continuous data protection (CDP) and continuous remote replication (CRR) with compression, bandwidth reduction, and support for both physical and virtual servers. Block-based data and file system remote replication are currently supported with RecoverPoint/SE on VNX Series arrays. Integration with EMC Unisphere and VMware vCenter enable unified management from a single location. The Total Protection Pack's key capabilities include:

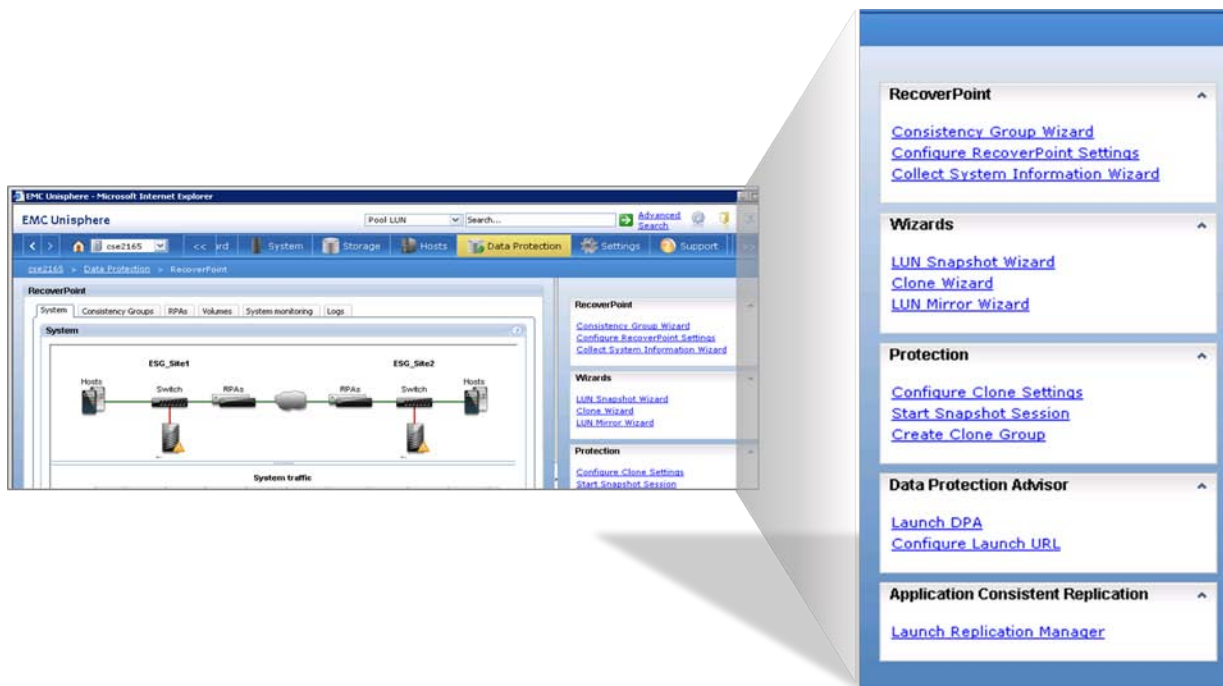
- Continuous local and remote data protection and recovery with DVR-like rollback
- Point-in-time recovery of individual or multiple virtual machines with a single click
- The ability to define and manage recovery point objectives and SLAs across the infrastructure
- Automated failover and failback through integration with VMware Site Recovery Manager

The VNX Total Protection Pack consists of:

- **Local Protection Suite:** RecoverPoint/SE CDP, SnapView, and SnapSure for local protection and data re-purposing
- **Remote Protection Suite:** RecoverPoint/SE CRR, Celerra Replicator, and MirrorView A/S for remote protection against failures and disasters
- **Application Protection Suite:** EMC Replication Manager and Data Protection Advisor for Replication Analysis for application protection and automated replication management

ESG Lab tested RecoverPoint/SE CDP and CRR, Replication Manager, and Data Protection Advisor for Replication Analysis. Figure 2 shows the RecoverPoint/SE GUI within the EMC Unisphere management interface, with the System tab displaying the replication topology. Note that RecoverPoint/SE, Data Protection Advisor, and Replication Manager (as well as other management wizards) can be launched directly from the Unisphere management screen (right side navigation).

Figure 2. Unisphere Management View



RecoverPoint/SE

As part of the RecoverPoint product family, RecoverPoint/SE is replication software that runs on SAN-attached RecoverPoint Appliances (RPAs) that protect physical and virtual hosts, providing unified SAN/NAS replication for EMC VNX arrays. Also in the RecoverPoint family are RecoverPoint/EX for replication within VMAXe and VNX arrays and RecoverPoint/CL which adds support for EMC VMAX and also non-EMC storage environments. They provide synchronous local replication with CDP and synchronous and asynchronous CRR, as well as concurrent local and remote replication. RecoverPoint tracks changes to data at the block level and journals those changes using CDP technology; this journal-based architecture enables rollback to any point in time and simultaneously reduces storage costs. WAN deduplication and compression features reduce TCO by reducing overall WAN bandwidth requirements. Management is integrated with both EMC Unisphere and VMware vCenter; in addition, RecoverPoint/SE supports all features of VMware vSphere 5.0 including Site Recovery Manager (SRM) automated failover and failback. The easy-to-manage RecoverPoint/SE product can be used to replace multiple application-specific point solutions.

Replication Manager

Replication Manager (RM) automates the creation and management of application-consistent replicas without impacting production performance for tasks such as instant restore, backup, and creating test/dev data sets in physical and virtual server environments. It integrates with the EMC RecoverPoint family as well as with EMC TimeFinder, SnapView, SnapSure, SAN Copy, and Celerra Replicator. It automates discovery of the environment at initial implementation and when changes occur. The point-and-click interface, pull-down menus, and wizards replace complex scripting and manual mapping between replication technologies, storage, and applications/file systems. Built-in intelligence places applications in the proper state to create application-consistent replicas, which can then be mounted to any host. RM's simplicity, policy-based management, and definable user roles make it usable by most IT staff, not just storage or replication experts.

Data Protection Advisor

Data Protection Advisor (DPA) provides unified monitoring, analysis, alerting, and reporting across the data protection environment. It collects information about data protection automatically to inform IT decisions and help administrators correct problems and meet SLAs; the single, integrated view brings simplicity to a complex environment and helps IT work more effectively. DPA takes volumes of disparate data and turns it into actionable knowledge, enabling organizations to reduce costs by more efficiently managing people, processes, and equipment. Improved visibility helps to reduce risk and ensure compliance by alerting IT about bottlenecks that can impact replication, recoverability exposure, policy enforcement status, and more. The bottom line? Problems can be resolved with less effort and cost.

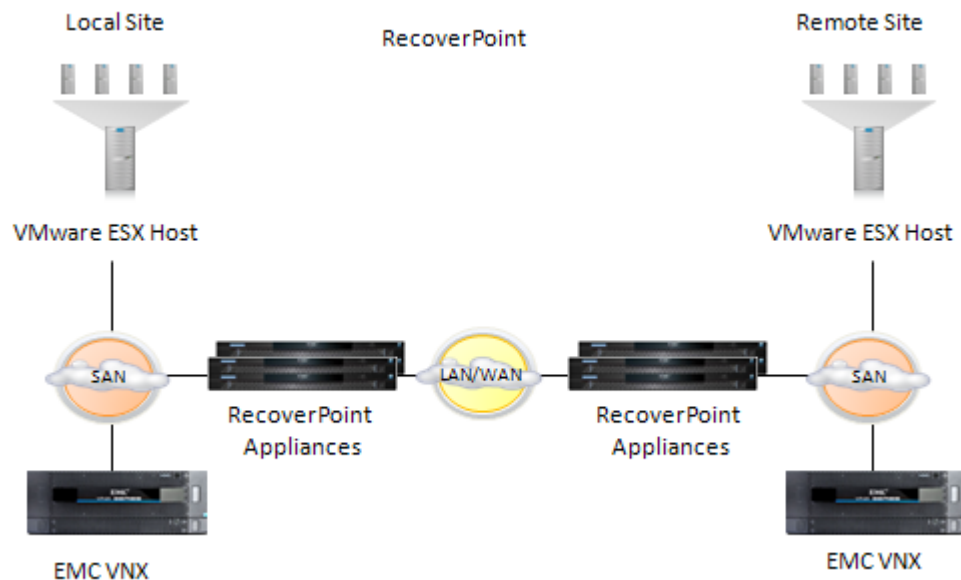
ESG Lab Validation

ESG Lab performed hands-on evaluation and testing of components of the VNX Total Protection Pack at EMC's lab in Hopkinton, MA. Testing of the VNX Total Protection Pack was focused around RecoverPoint/SE, Replication Manager, and Data Protection Advisor for Replication, designed to demonstrate the integration of local, remote, and application protection along with consolidated management through Unisphere.

Test Bed

Figure 3 illustrates the test configuration. Local and remote servers were configured with VMware ESX 4.1. Both environments were connected with 4 Gb iSCSI SANs to EMC VNX 5500 arrays. The RecoverPoint/SE configuration consisted of two Dell R610 servers at the local and remote sites with RecoverPoint/SE software version 3.4.1.1. These were connected via SAN and 1 Gb LAN. At the remote site, RM and DPA were run on VMs.

Figure 3. ESG Lab Test Bed



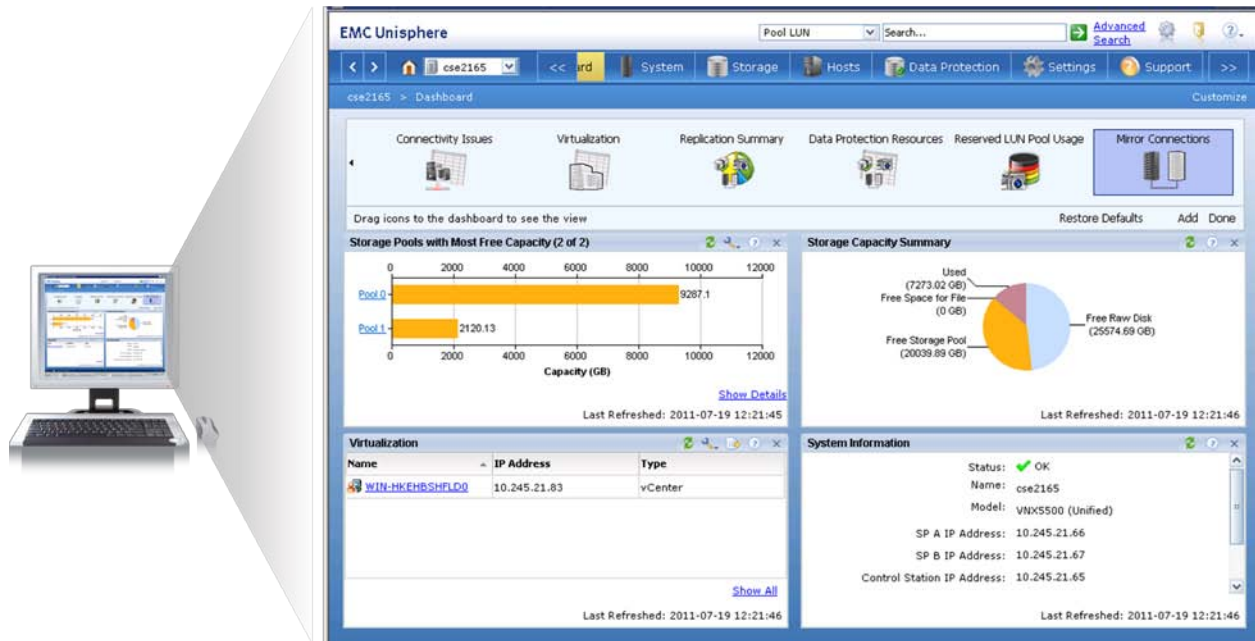
Ease of Management

ESG Lab tested the ability to execute replication configuration and management from within EMC Unisphere, the VNX array management interface.

ESG Lab Testing

ESG Lab was able to view and manage replication from a consolidated EMC Unisphere GUI. Figure 4 shows the dashboard view. Graphical summaries of storage capacity for the local and remote VNX arrays are shown, as are array status and details. Alerts would be displayed here and a link to the virtual server is available in the lower left window. To add other types of information to the dashboard, the administrator simply drags icons from the dashboard options. Different systems can be viewed by selecting them from the top navigation.

Figure 4. Unisphere Dashboard View



Management tasks are menu- and wizard-driven. Figure 5 shows the RecoverPoint wizard for configuring and creating replication consistency groups to a RecoverPoint Appliance. Settings such as bandwidth reduction, protection policy, resource allocation, clustering, and VMware SRM support are defined here. At least one journal LUN must be created for each consistency group copy; during testing, journal LUNs were created for the production data, local copy, and remote copy to ensure transactional consistency for recovery. Consolidated management makes this simple: because the RecoverPoint GUI is available within Unisphere, ESG Lab was able switch easily to the Unisphere GUI to create the new LUNs instead of having to exit one application/management station and start another.

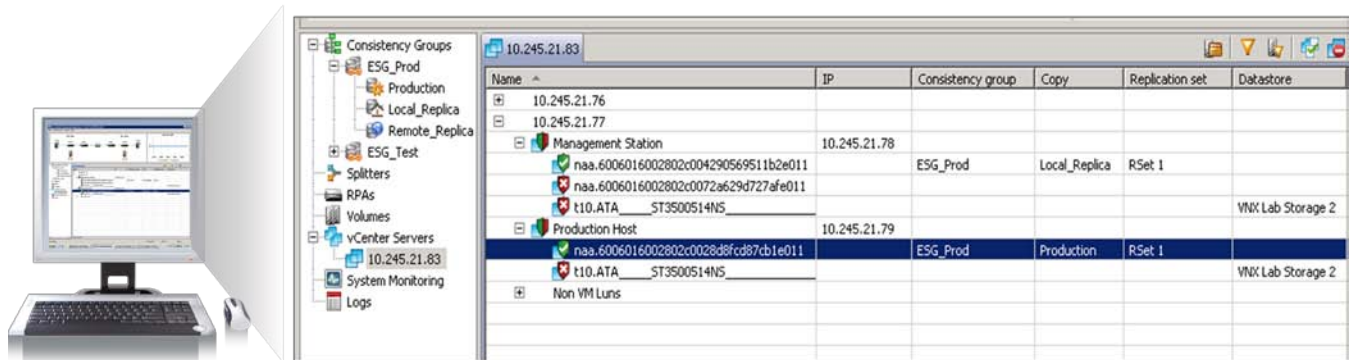
Figure 5. Unisphere Consistency Group Wizard



ESG Lab was able to view the status of different portions of the environment through the RecoverPoint GUI. Figure 6 shows the view from the VMware vCenter API integration, including IP address, consistency group protection status, and replication set details. RecoverPoint's integration with VMware vCenter provides management visibility into the virtual servers being managed within a replicated environment, allowing for real-time management of the production, local, and remote replicas within a single management interface. This allows administrators to manage the protection of their virtual server environment from a single console.

VMware 5.0 SRM integration is also part of the package; in the RecoverPoint tab, the administrator can choose to let SRM manage recovery or allow the administrator to manage failover within the RecoverPoint GUI.

Figure 6. RecoverPoint Manager VMware View



Name	IP	Consistency group	Copy	Replication set	Datastore
10.245.21.76					
10.245.21.77					
Management Station	10.245.21.78				
naa.6006016002802c004290569511b2e011		ESG_Prod	Local_Replica	RSet 1	
naa.6006016002802c0072a629d727afe011					
t10.ATA__ST3500514NS					VNX Lab Storage 2
Production Host	10.245.21.79				
naa.6006016002802c0028d8fcd87cb1e011		ESG_Prod	Production	RSet 1	
t10.ATA__ST3500514NS					VNX Lab Storage 2
Non VM Luns					

Why This Matters

Separate management stations make multiple data protection activities complex, time-consuming, and expensive while limiting visibility. As administrative roles begin to converge in virtual environments, consolidation of management tasks will become imperative.

ESG Lab testing confirmed that key RecoverPoint/SE, RM, and DPA features can be centrally managed within EMC Unisphere or VMware vCenter, and that each application can be fully launched from the central console. Dashboards deliver expanded infrastructure visibility, while menus and wizards simplify management tasks. Array-based tasks required for replication were quickly accessible just by selecting another tab.

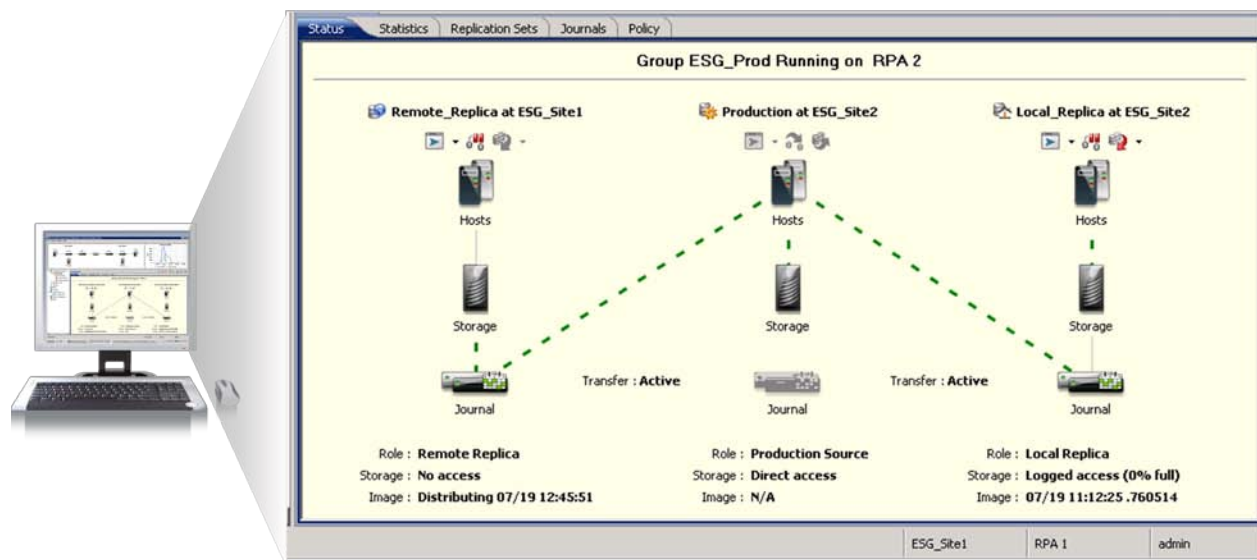
Continuous Protection

The VNX Total Protection Pack includes RecoverPoint/SE, which provides simultaneous local and remote replication and disaster recovery for physical and virtual environments. Continuous protection is provided by the creation of sub-second snapshot copies that provide a set of time-stamped images that can be restored if needed.

ESG Lab Testing

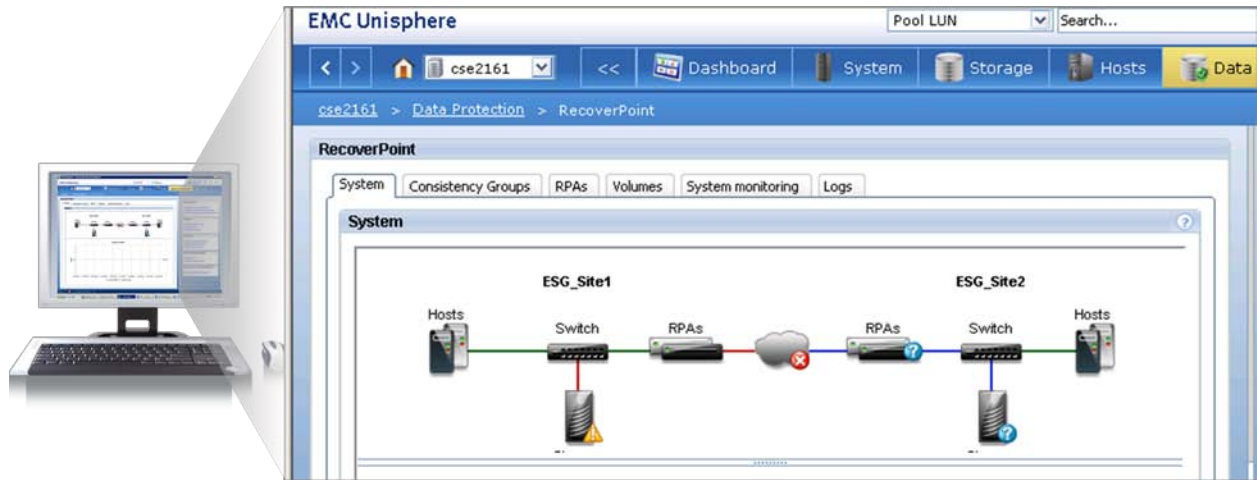
ESG Lab launched the RecoverPoint/SE GUI from within Unisphere. After creating a consistency group, both local and remote replication processes were started. Figure 7 shows the RecoverPoint/SE GUI; the large graphic shows the view from the defined consistency group. The production site is creating local and remote copies simultaneously (represented by the dotted green lines). Local and site-to-site system traffic is charted in the upper right corner, while the upper left graphic shows the replication topology.

Figure 7. RecoverPoint Manager Status View



Next, ESG Lab created a failure by disconnecting the LAN. Figure 8 shows the topology view indicating a failure in the continuous protection process. The system traffic chart shows no local or remote replication traffic.

Figure 8. Unisphere View with Replication Failure



Next, ESG Lab tested remote recovery. After creating a bookmark to identify a replica at a particular point in time, ESG Lab deleted one file and edited another. The target site view (see Figure 9) shows the time-stamped CDP images available for recovery to another VM.

Figure 9. Remote Recovery Bookmark Details

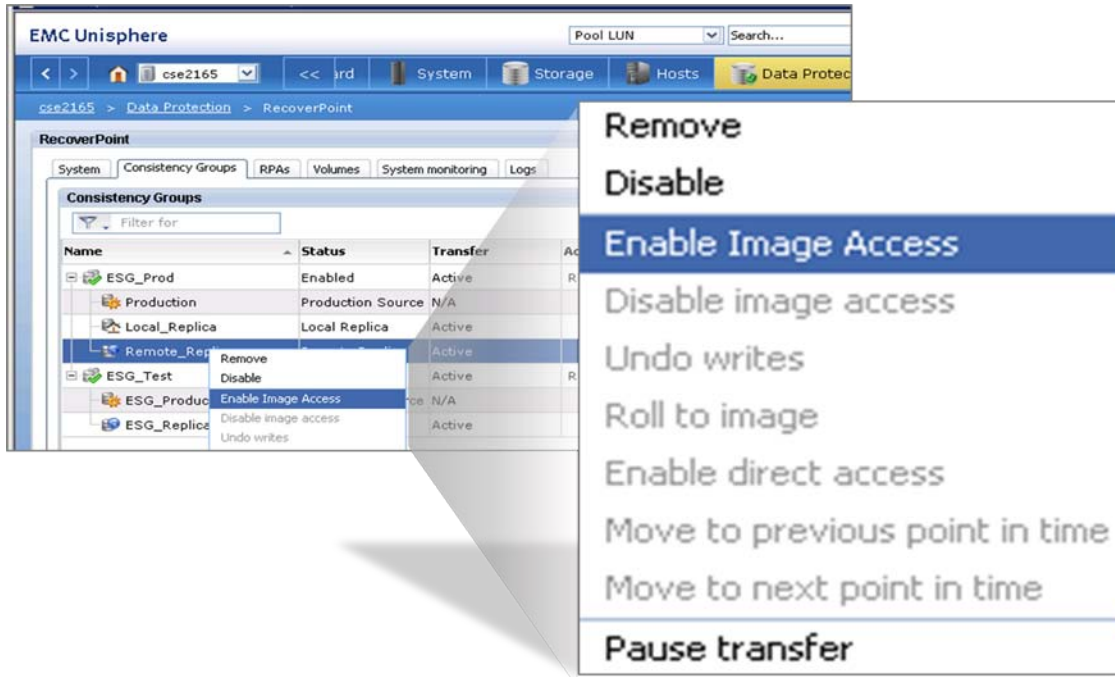
The screenshot shows the 'Policy Journal' view in EMC Unisphere. The 'Image' section shows 'Current: Distributed Pre-replication ima...' and 'Storage: No access'. The 'Journal' section lists: 'Journal Lag: 925KB', 'Compression Ratio: N/A', 'Required Protection Window: N/A', 'Current Protection Window: 2 hours and 10 mins', 'Predicted Protection Window: N/A', and 'Space Saved By Consolidation: N/A'. The 'Sample Images' table is as follows:

Time	Size	Bookmark Details
07/19 11:12:30	180 bytes	
07/19 11:12:30	36.6KB	Synchronization co...
07/19 11:12:37	1.23KB	
07/19 11:16:29	4.13KB	
07/19 11:16:33	12.8KB	
07/19 11:16:37	8.73KB	
07/19 11:16:40	39.2KB	
07/19 11:16:48	16.8KB	
07/19 11:16:51	12.8KB	
07/19 11:16:55	19.0KB	
07/19 11:16:58	4.63KB	
07/19 12:26:09	12.8KB	
07/19 12:26:13	4.63KB	
07/19 12:26:20	12.8KB	
07/19 12:26:24	12.8KB	
07/19 12:34:18	392 bytes	before upgrade
07/19 12:36:47	540 bytes	

0 Selected

ESG Lab then selected “Enable Image Access” to confirm the viability of remote copies and journals to ensure proper restore (see Figure 10). Once the image was selected, a simple right click restored it to production; the journal was used to restore changes that occurred after the snapshot was created. Because replication is continuous, the local copy continues to journal changes during the recovery activity. Production resumed, completing the full failover and failback process.

Figure 10. Remote Copy Image Access



Why This Matters

Realities of time and budget require many organizations to implement different data protection strategies to handle disaster recovery, instant restore, backup, data migrations, and firmware upgrades. This can result in protection gaps that leave organizations vulnerable.

ESG Lab confirmed RecoverPoint/SE’s ability to conduct continuous local and remote replication of a consistency group, and to quickly roll back to transaction-consistent, point-in-time snapshot using both bookmarked replicas and journals of changes. Testing confirmed that remote replicas can be verified non-disruptively, and that replication malfunction alerts appear in the Unisphere management view.

Application Protection and Replication with Replication Manager

Replication Manager provides a single interface for automating all EMC replication applications, and is tightly integrated with RecoverPoint. Automation of scheduling, application-consistent replication creation, and workflow can reduce administrative effort and ensure that protection policies are enforced. In addition, Replication Manager enables self-service replication with its selectable user roles and privileges.

ESG Lab Testing

ESG Lab launched RM directly from the Unisphere management window. Figure 11 shows the view of replication jobs by application set. RM Server, storage pool, and storage service views are also available. The “Getting Started” pane lists the four steps required to launch RM: registering agents on servers to be protected and on hosts on which replicas will be mounted, adding replication storage, creating an application set to be protected, and creating a policy-based replication job.

Figure 11. Replication Manager

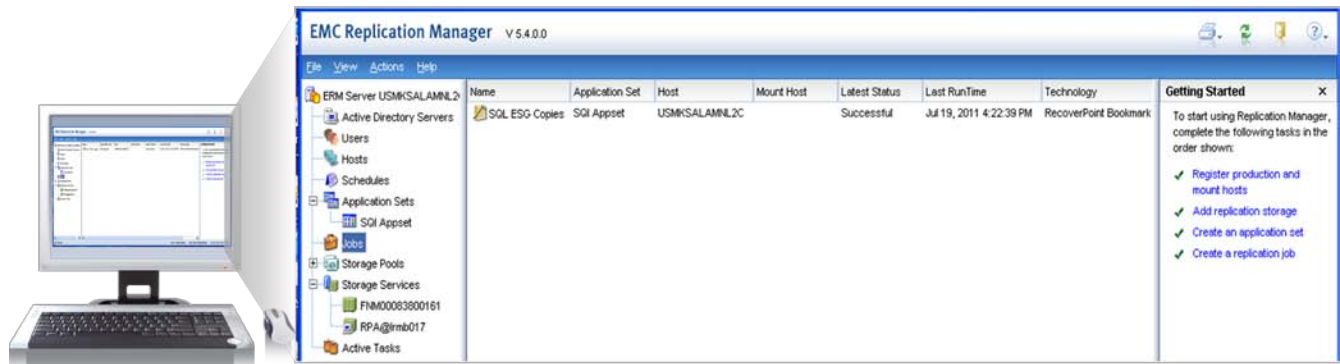
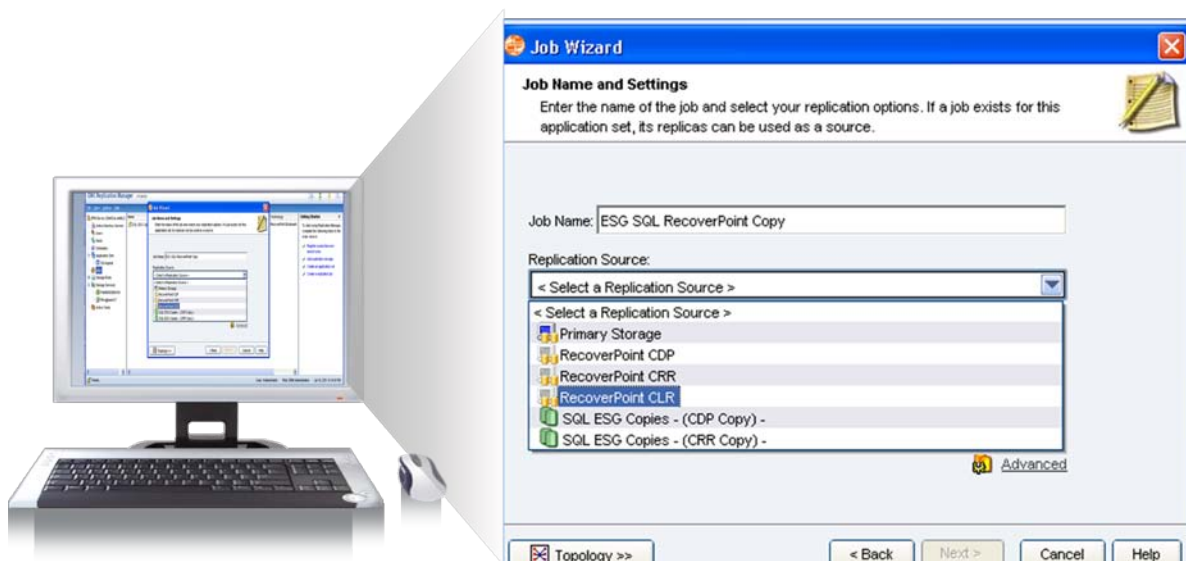


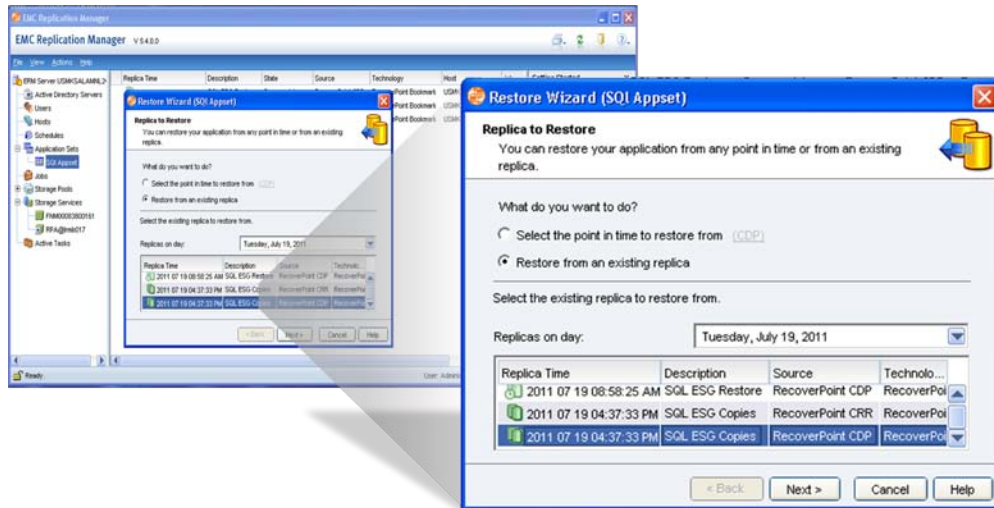
Figure 12 shows the RM Job Wizard. From this window, ESG Lab selected RecoverPoint Concurrent Local and Remote (CLR) Replication. Other RecoverPoint/SE options are available, as would be any installed EMC replication software. Workflow can also be automated; for example, RM can be configured to launch another replication task immediately following completion of the current task to eliminate complex scripting.

Figure 12. Replication Manager Job Wizard



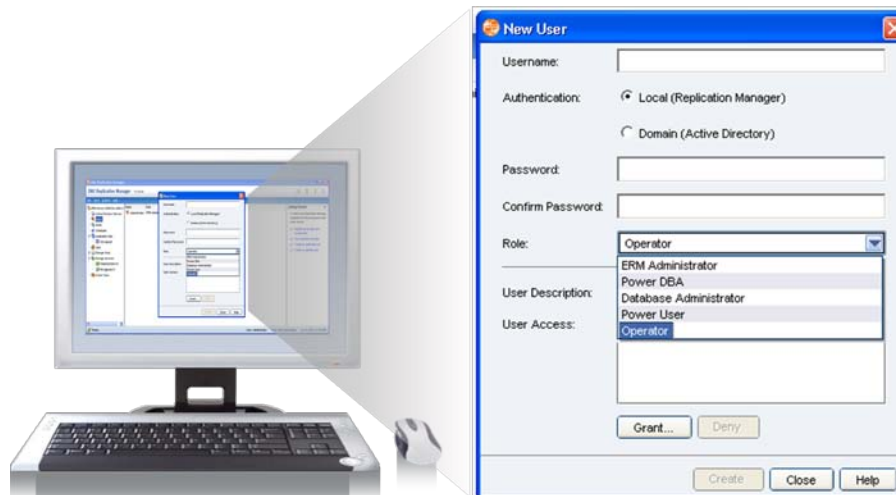
Next, ESG Lab selected and restored the point-in-time replica from the Restore Wizard.

Figure 13. Replication Manager Restore Wizard



RM offers five levels of user-defined, role-based management (see Figure 14). This enables administrators to offer different levels of management according to user type, including self-service. Certain roles may be able to manage only particular storage pools or hosts, which can reduce IT’s administrative burden while ensuring that the infrastructure is managed properly.

Figure 14. Replication Manager User Management



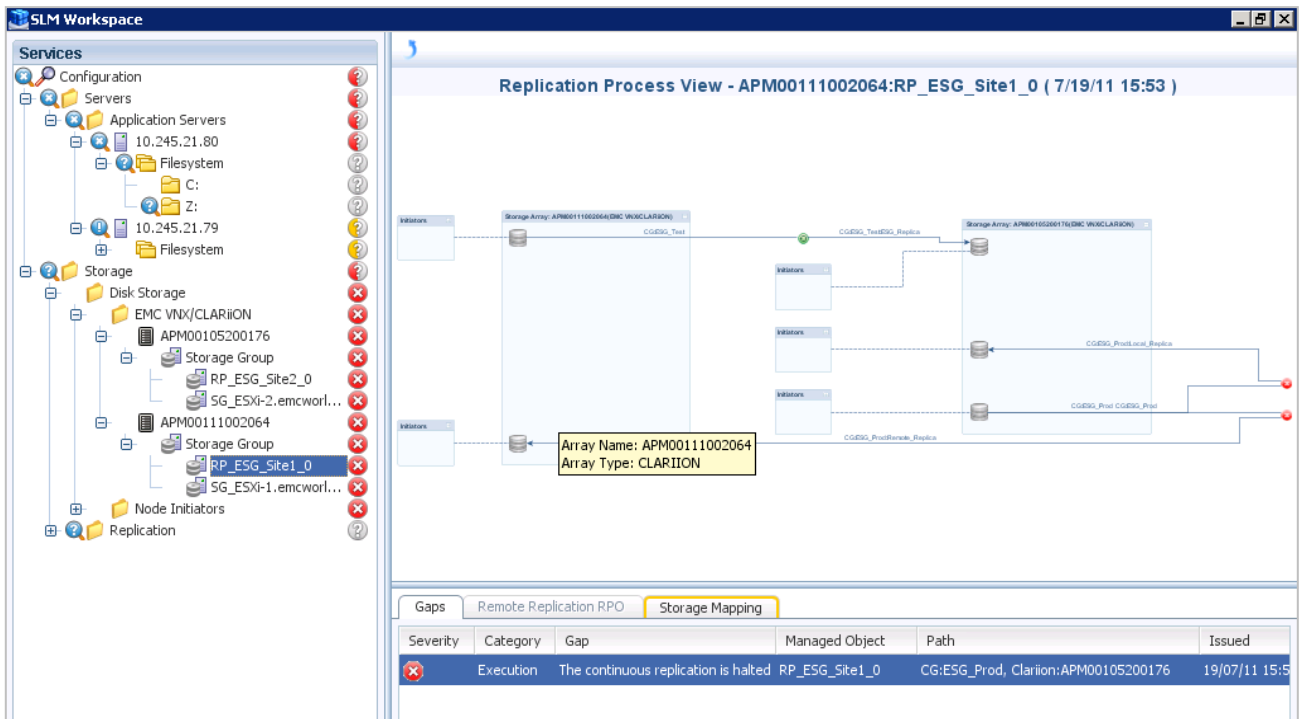
Why This Matters

Most replication solutions require manual application-to-storage mapping as well as constant monitoring to ensure compliance with company policies. Many solutions only generate crash-consistent replicas that are difficult, time-consuming, and unreliable when it comes to restore.

ESG Lab confirmed that Replication Manager automates replication activities and workflows. Testing also confirmed RM’s ability to support multiple replication applications, to restore quickly and easily from point-in-time snapshots, and to define role-based activities that enable user self-service functions.

DPA also reports on and provides visibility to successful and unsuccessful replications. As shown in Figure 16, DPA generated a replication gap alert, as well as alert icons when ESG Lab disabled the simulated WAN connection. The alert icons are displayed in the navigation and topology views with gap alert details shown at the bottom of the view.

Figure 16. Replication Process View with Gap Alert



Why This Matters

In large environments with many virtual and physical servers, it can be difficult to know what servers are protected, how they are protected, and whether replication is operating properly. Also, because it is easy to create new virtual machines, some can inadvertently be left out of the protection scheme.

ESG Lab confirmed that Data Protection Advisor for Replication Analysis provides enterprise-wide visualization from the host, storage, or replication view, including server-to-storage topology, array replication technology, analysis, and reporting. DPA automatically generated and sent an alert via e-mail in response to a gap in protection that enabled IT to intervene.

ESG Lab Validation Highlights

- ☑ ESG Lab confirmed that VNX Total Protection Pack applications can be launched and easily managed from the EMC Unisphere and VMware vCenter management interfaces for visibility across the replication environment.
- ☑ ESG Lab validated the VNX Total Protection Pack's ability to provide simultaneous local and remote replication, including application-consistent replicas, for virtual and physical servers.
- ☑ The DVR-like rollback to any point in time, combined with journal-based architecture, enables fast and easy recovery with no data loss.
- ☑ ESG Lab confirmed the benefits of RM's task and workflow automation and DPA's enhanced visibility, trending, and analysis for managing large scale virtual environments.

Issues to Consider

- ☑ It should be noted that RecoverPoint volumes at two sites do not have to be the same size. However, if this approach is used, RecoverPoint will not be able to utilize the extra capacity of the larger volume.
- ☑ Once the Total Protection Pack solution is in production, best practices should be followed when creating application sets. Initialization of protection may cause unacceptable performance degradation in the production environment until the process completes. Consider creating application sets during off-peak hours.
- ☑ Analysis jobs that are shipped as part of Data Protection Advisor cannot be edited. Selecting edit grants access only to a view of the job's properties. To modify these jobs, a user must create a copy and edit that version.

The Bigger Truth

Traditional disaster recovery solutions often come up short when dealing with both physical and virtual infrastructures. Some require multiple, application-focused point solutions that must be individually managed and are difficult (if not impossible) to integrate with other tools. Others create challenges in virtual server environments as their recovery processes are manual, complex, and hard to execute—the kiss of death for dynamic virtual environments management.

WAN improvements have made replication and data protection much more viable for mid-range organizations. Still, these IT shops are often short-staffed and operate on limited budgets. Complex protection environments with multiple disparate applications and management stations are not conducive to improving their levels of protection.

ESG Lab tested EMC VNX Total Protection Pack components including RecoverPoint/SE, Replication Manager, and Data Protection Advisor in a virtual server environment connected to an EMC VNX SAN and validated the ability to perform CDP and CRR, and to restore quickly from point-in-time snapshots and application-consistent bookmarks. ESG Lab also validated RM's automation of replica creation and management, and DPA's visualization, analysis, and gap alerting capabilities. All of this was easily viewed and managed centrally via EMC Unisphere, which provided link and launch capability for the individual applications.

ESG Lab commends EMC for its commitment to simplifying its data protection portfolio for the mid-range customer. While the process is in transition, ultimately the functionality of several current products (such as MirrorView and Celerra Replicator) will be folded into RecoverPoint. Other products such as Replication Manager and Data Protection Advisor are already significantly integrated despite remaining discrete products. At its end state, this consolidation will make deploying, managing, and licensing data protection simpler for users—and selling it simpler for EMC.

Appendix

Table 1. ESG Lab Test Bed Detail

Storage	
EMC VNX	Model – VNX5500 Block Version – 5.31.000.5.008 File Version – 7.0.14.0
Replication	
EMC RecoverPoint	Version – 3.4.1.1
RecoverPoint Appliances	Generation 4 8 Gb Capable
Servers	
Cisco Servers	Model – UCS C200 M2 Operating System – ESX 4.1
Network	
Network Switch	Make – Dell Model – PowerConnect 2824 Speed – 1 Gb
SAN Switch 1	Make – Brocade Model – DS-300B Version – 6.3.1a
SAN Switch 2	Make – Brocade Model – DS-5100B Version – 6.3.1a



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