Executive Briefing:

Paragon StarWind iSCSI SANs Maximize Performance and Functionality for Virtualized Storage Systems

Driving Enterprise Performance with Hypervisor Neutrality for Cloud Computing
In this analysis, openBench Labs examines the storage virtualization features and performance of the Paragon StarWind iSCSI SAN storage hypervisor software. Using Paragon StarWind iSCSI SAN, IT is free to use a wide array of common server hardware and Windows Server operating systems to implement a highly functional iSCSI SAN infrastructure servicing both physical and virtual systems in a private cloud.

Virtual Machines (VMs) in particular have become closely associated with an iSCSI SAN. For IT, the key features of a private cloud based on a Virtual Infrastructure (VI), include the non-disruptive movement of VMs among VI hosts and the rapid cloning of VMs for simplified provisioning, which are dependent on storage sharing on a SAN fabric. More importantly, a VI private cloud is often cited by CIOs as a critical factor in assuaging the down-time fears of corporate executives.

With a rich portfolio of performance software for storage resources, Paragon Software is well positioned to provide an evolving feature-rich iSCSI SAN that is grounded on solid performance. Specifically, Paragon has developed an enterprise service architecture, which it uses to deploy and manage critical IT storage services for physical and virtual systems across an entire site. Under this architecture, each IT service is characterized by
three elements: an administration server, an ESX bridge, and service agents.

The administration server distributes agents and resources to client systems, manages a central database, resolves conflicts between agents, and provides IT administrators with a single centralized management GUI. The ESX Bridge is a special agent that interacts with a VMware VI through a vCenter server in order to present IT administrators with the same VI topology views in the Paragon GUI as those provided by vCenter.

Two IT services distributed in this manner by Paragon are particularly synergistic with their iSCSI SAN storage hypervisor. These services are targeted for tight integration into the iSCSI SAN in order to provide enhanced scalability and availability of storage devices and to offer more powerful and flexible options for protecting mission-critical systems. These services are the Paragon Alignment Tool (PAT), which ensures the alignment of disk blocks across multiple storage architectures to optimize I/O traffic and Paragon Protect & Restore (PPR), which complements the replication and recovery features of a Paragon StarWind iSCSI SAN storage hypervisor with a sophisticated image-based backup and disaster recovery (DR) service for virtual and physical systems.

**HIGH THROUGHPUT & HIGH AVAILABILITY TESTING**

With infrastructure virtualization a major driver for adoption of an iSCSI SAN, openBench Labs set up a Paragon StarWind iSCSI SAN storage hypervisor with both 10Gb and 1Gb Ethernet support. We then set up key value-added features in the Paragon StarWind iSCSI SAN including data deduplication and high availability (HA) for iSCSI volumes.

To test the Paragon iSCSI storage hypervisor in a VI, we utilized vSphere and Hyper-V environments that were hosted on Dell PowerEdge R710 servers, each provisioned with dual 6-core processors and 48 GB of RAM. To simplify our iSCSI SAN fabric, we used copper 10GbE cables.
to make direct server-to-server connections without using a 10GbE switch. We set up a
direct connection to each VI host from each server running the Paragon iSCSI storage
hypervisor. We needed two Paragon StarWind iSCSI SAN server nodes to support and
test the HA iSCSI configuration. For this task, we utilized older generation Dell
PowerEdge 1950 Servers configured with a quad-core CPU, 8GB of RAM, four 1GbE
ports, and 1TB of DAS storage. These servers are typical of the systems IT typically has
available to retask.

With respect to added-value
synergies for an iSCSI SAN, the
Paragon Alignment Tool provides
IT administrators with the ability to
examine all virtual and physical
systems that are running Windows
at a site for misaligned disk blocks.
Data block alignment is an oft
overlooked problem that can result
in significant I/O overhead that
impacts an entire SAN fabric.
When IO requests traverse logical
block layers that are not aligned,
the I/O subsystem has to generate
extra I/O requests to handle any
blocks that extend beyond the
boundaries of the top layer, which
is the only layer known by the OS
of the requesting system.

Misaligned blocks can be a
significant problem in a VI, where
multiple hidden file systems will be
layered beneath the native NTFS
layer created by a Windows-based
VM. In particular, the devices on a Paragon StarWind iSCSI SAN start as NTFS files.
Next, the system that imports the device—often an ESX host—will format the device
with a new logical layer of blocks. Finally a Windows VM creates yet another virtual
layer of NTFS blocks. As a result, I/O requests in a VI will likely cross four boundary
layers of logical blocks.

Paragon Protect & Restore also uses the new Paragon distributed architecture to
provide efficient central management of potentially thousands of systems, including VMs
via Paragon’s special ESX bridge connector. Unlike PAT, which addresses the needs of IT
operations for optimizing SAN I/O performance, PPR addresses the critical Recovery
Point and Recovery Time Objectives (RPO and RTO) that CIOs must promise Line of
Business executives that IT will meet within the context of a Service Level Agreement
(SLA) for data protection and business continuity.
For fast and reliable agent-less backup and replication using disk-imaging for Windows and Linux VMs, PPR uses the Paragon Image Transfer Engine (ITE) and VMware Changed Block Tracking (CBT) to run full and incremental backups quickly, create replicas, and generate minimal impact on an ESX host. To test advanced VM data protection features, in our iSCSI SAN environment, we installed PPR on a VM server configured with a virtual quad-core processor and 4GB of RAM.

To provide our VM server running PPR with data deduplication on storage to be used for backup files and VM replicas, we created two identical 512GB data deduplication devices on a Paragon iSCSI storage hypervisor. Paragon’s ability to deliver centralized global data deduplication at a device-level is especially important for simplifying IT administration in a VI environment. By moving memory-intensive data deduplication off of backup servers, a Paragon StarWind iSCSI SAN makes it much easier for IT to adopt an increasingly popular strategy for backup scalability that distributes light-weight VM servers running backup and recovery processes across the hosts in a VI.

To store backup files, PPR is able to utilize local or NAS-based logical disks. On the other hand, PPR needs to create a VM replica on an ESX datastore to make it available to
an ESX/ESXi host to publish into a VI. As a result, we needed one target to connect our
ESXi host to the data-deduplication device intended for storing VM replicas. For
connecting the device for backup files, we had the option to utilize the same iSCSI target
to mount the device on our PPR VM server as a raw device mapped (RDM) VMware
volume. Instead, we chose to bypass the ESXi host and create another target that
connected directly to the iSCSI initiator on the PPR VM server.

When we examined the impact of
data deduplication on the two devices, we
discovered that the device used for
backup files exhibited very little storage
reduction. The data processing methods
employed by Paragon’s ITE produced
minimal duplicate data within the backup
storage.

After running one full and three
incremental backups for each of eight
VMs, we had transferred 309GB of
backup data to the local logical disk and
the three files used to create a data-
deduplication device were consuming
273 GB of storage on our iSCSI SAN
server. On the other hand, the data
deduplication device that we were using
to support a datastore with VM replicas,
exhibited a 30% reduction in the amount
of storage being consumed without
impacting on the ability to use a PPR
replica to meet a very aggressive RTO.
Specifically, we were able to deploy
replicas in a DR scenario from a
datastore backed by a data-deduplication
device in a matter of seconds.

More importantly, Paragon StarWind iSCSI SAN devices with global deduplication
significantly enhances CapEx savings for data protection packages that do not support
global deduplication—many provide data deduplication at a job level—or that only
offer global deduplication as an extra-cost option. While many packages, such as
Paragon Protect & Restore default to an incremental backup scheme utilizing the
vStorage APIs for Data Protection—in particular Changed Block Tracking (CBT)—
this does not diminish the possibility to extract additional storage savings for
deduplication when performing periodic full backups or more importantly, replicating
VM for fast recovery. In our tests of Paragon Protect & Restore, we reduced storage
requirements for a VM replica by 30%. 

CLOUD-SCALE DATA PROTECTION

Paragon Protect & Restore complements the replication and
recovery features that come included in the iSCSI SAN storage
hyervisor with powerful and flexible options to efficiently protect
mission-critical systems for virtual environments as well as standalone
servers and workstations.

The product offers fast and reliable agent-less disk-imaging backup
and replication of both online and offline Windows or Linux virtual
machines. Flexible retention policies, enhanced data processing
methods, and the automatic exclusion of irrelevant data (page files,
etc.) allow the optimal utilization of backup storage destinations.
Employment of MS VSS (Volume Shadow Copy Service) when taking
snapshots of Windows machines guarantees data consistency. The
introduction of Paragon’s ProTran®, a unique data transport protocol
and a two-tier backup storage infrastructure (available in the next
release), allow you to further optimize backup windows and network
traffic for simultaneously generated backups.

On the recovery side, Paragon Protect & Restore meets even the
most aggressive RTOs (Recovery Time Objectives). The user has the
option to restore a backup to either its original location or a new
location, based on available restore points. When restored to a new
location, the target virtual machine will be appropriately reconfigured
during the process. For replicas, the entire disaster recovery procedure
may take only a few seconds, ensuring maximum business continuity.
**Mastering IT CapEx and OpEx**

Starting with no limits on the storage capacity exported to clients or on the number of client connections, the Paragon StarWind iSCSI SAN storage hypervisor can help IT control capital expense (CapEx) costs associated with rapidly expanding storage resources. At the heart of every Paragon StarWind iSCSI SAN, the light-weight Paragon storage hypervisor allows IT to utilize any 32-bit or 64-bit server running a Windows operating system to provide iSCSI target devices capable of being shared among multiple hosts. Shared storage is an essential component of VI environments and the Paragon storage hypervisor lowers CapEx for shared storage by allowing IT to use a wide array of existing hardware and OS options to implement an iSCSI SAN with high-availability and instant fail-over features.

Nonetheless, it costs much more per GB to manage storage than acquire it. For IT, the bottom line for controlling budgets rests on controlling operating expense (OpEx). For storage resources, OpEx dominates the Total Cost of Ownership (TCO) by an order of magnitude. As a result, OpEx issues pressure IT to minimize management time and maximize utilization of storage resources. That’s why CIOs are focused on eliminating the constraints that physical limitations put on devices, as a way to lower IT OpEx costs.

The Paragon StarWind iSCSI SAN storage hypervisor simplifies virtualization by allowing IT administrators to decouple storage devices easily from published iSCSI targets. More importantly, Paragon compounds the traditional iSCSI SAN value proposition by integrating automated storage management functions, including data deduplication, data protection, and HA for critical applications. Working within the Paragon Management Console, IT administrators can easily configure an independent hierarchy of storage targets based on functionality, such as mirroring, replication, data deduplication, fully synchronized HA failover with no single point of failure, and snapshots compatible with Microsoft’s Volume Shadow Copy Services (VSS).

At the same time, administrators can also use the Paragon Management Console to provision and manage an equally broad hierarchy of devices based on hardware performance metrics with respect to throughput (MB per second), access (IOPS), or capacity (price per GB). As a result, IT administrators are able to group and manage storage targets as pools characterized by device functionality and storage devices as pools characterized by performance metrics using one tool set, which simplifies the task of providing a network of servers with cost-effective, thin-provisioned, flexible storage.

More importantly, the Paragon StarWind iSCSI SAN storage hypervisor extends the benefits of storage virtualization well beyond oft-cited operational benefits, such as higher utilization of storage devices and higher productivity for IT administrators. CIOs are able to leverage Paragon’s operational support of advanced features, including a distributed iSCSI server cache, automated HA failover, and unlimited snapshot fall back points, to address strategic business-application issues within service level agreements (SLAs) that address issues such as data availability, business continuity, and disaster recovery (DR).
It is the virtualization of systems in a VI, however, that garners the lion’s share of attention from CIOs. More importantly, to maximize the benefits of a VI, such as vSphere, a shared SAN-based storage is a prerequisite to provide a virtual machine (VM) with mobility. VM mobility is essential to leverage critical VI features, such as load balancing and disaster recovery. That explains why strong growth in server virtualization is spurring strong iSCSI adoption as the least complicated way to migrate from DAS to a SAN and harness holistic system and storage virtualization synergies.

vSphere Datastore Snap Back

While IT overhead is the primary factor in OpEx reduction, CIOs also have to worry about meeting SLAs made with Line of Business executives in association with key business initiatives. These executives think in terms of business process parameters, so SLA objectives focus on the notions of process availability and process performance. For IT sites struggling with implementing critical business-driven initiatives, a Paragon iSCSI storage hypervisor provides an environment that satisfies a wide range of I/O metrics with respect to access (IOPS), throughput (MB per second), and capacity (price per GB), while simultaneously supporting multiple levels of resource availability and security.

The lynch pin for supporting advanced VMware features, such as vMotion and DRS, is disk sharing. VMware simplifies host volume sharing by treating the logical drives on a host datastore analogously to CDROM images. As a result, there is no need for a complex distributed lock manager scheme and a Paragon storage hypervisor can easily allow hosts to share storage volumes—dubbed device “clustering” in the Paragon GUI. More importantly, simplified sharing frees Paragon to meet a value proposition touting optimal resource utilization, minimal administration, and maximal performance, by packaging and virtualizing pools of disk blocks in multiple ways.

The most basic level of virtualization and simplest management task for IT involves exporting a raw physical device. If a device uses the SCSI command set, then all Paragon needs to do is route the command and data streams. All extended functionality is provided by the device. This device choice is dubbed a SCSI pass-through interface (SPTI). If the device does not utilize the SCSI command set, such as a SATA drive, Paragon offers a Disk Bridge device that virtualizes the command set so that a non-SCSI drive or array can be employed.

Paragon adds functionality to iSCSI devices by representing the devices as disk image files created by the iSCSI storage hypervisor. The Paragon’s hierarchy of device functions includes thin storage provisioning, automatic snapshot creation, and automatic HA failover. To support that feature hierarchy, Paragon uses several schemes that virtualize disk blocks by leveraging a local disk image file to represent the iSCSI device. Using multiple virtualization schemes, the Paragon iSCSI storage hypervisor is able to balance low overhead and high I/O performance with more sophisticated device functionality.

Using a basic image file, we were able to support a vSphere datastore with a VM running an 800-user Exchange 2010 configuration that could sustain a heavy processing load of 800 email transactions per second (TPS) generated using the
Jetstress benchmark. Moreover, this device configuration is the technology used as a foundation for RAID-1 mirror devices and synchronous HA support.

Paragon utilizes a more sophisticated image-based virtual disk (IBV) scheme to provide thin provisioning, device snapshots—both manual and automated for continuous data protection—and disk cloning. For an IBV-based device, Paragon virtualizes disk blocks using separate files for disk headers (.ibvm), block data (.ibvd), and disk snapshots (.ibvss), which means a Paragon IBV device represents a virtualized iSCSI target that is entirely independent of the underlying storage hardware and the server running the Paragon StarWind iSCSI SAN storage hypervisor.

**Snapshot Datastore Recovery**

Starting with a target to provide vSphere with a datastore backed by device-based snapshots, we created an image-based virtual disk (IBV) device with automated snapshots. After adding several VM servers to the device, we used the Paragon Management Console, to pick a device snapshot, generate an image file device corresponding to the restore point, and assign the device a new LUN on the original target. We were then able to import the new iSCI storage device on our vSphere host and recover each VM on the datastore.

We used an IBV device to underpin a vSphere datastore supporting VM servers
running SQL Server. Paragon device snapshots provided additional data protection that was independent of the PPR data protection software. With the vSphere datastore resident on a Paragon IBV device, we encountered no issues in either performance or functionality, when leveraging any advanced IBV-based device feature, including thin provisioning and automated snapshots. The central issue for IT administrators with respect to the automated snapshot scheme is the rate at which snapshots grow and consume resources. If a limit is placed on the number of snapshots, Paragon will overwrite the oldest snapshot when the limit is reached.

The most independent way to mount and leverage a Paragon snapshot is through the creation of a full device-image created as a linked clone representing the restore point. To minimize the storage required to virtualize the restore point—especially useful if the device is intended to be temporary. In seconds, the linked clone process utilizes pointers to the data associated with a snapshot restore point. Once the new device is created, any changes to either the new device or the original are independent. As a result, snapshots and linked-clone replication provide IT with a powerful means to provide an aggressive Recovery Point Option (RPO) and a Recovery Time Option (RTO) for an entire vSphere datastore and all of the VMs located on that datastore.

**iSCSI HA**

When we ran Jetstress on our 800-user configuration of Exchange on a VM server resident on a Paragon HA device, we comfortably sustained 400 email TPS, after relaxing the average access time for a transaction to be under 35ms rather than 20ms. During this test, Paragon CPU overhead associated with keeping the two iSCSI HA devices in synch was typically about 15% of a single core on each Paragon quad-core server.

Setting up an HA environment was a very simple configuration exercise with Paragon. We created a target on each Paragon server. Each target was assigned an image
file device on a local disk and network interfaces were assigned to handle synchronization and heartbeat data traffic. We then exported each iSCSI target over a 10GbE link to the vSphere host server. The host treated the two synchronized devices as a single device with multiple iSCSI paths. As a result, Paragon leveraged iSCSI path failover to provide HA failover for two physically different devices.

**HA Failover Scenarios**

We ran failure tests of the 10GbE network and the HA device. With a simple 10GbE failure, Paragon handled the entire recovery without intervention. When a 10GbE to one of the servers failed, vSphere immediately failed the iSCSI connection to the remaining server. At the same time, Paragon maximized its utilization of the 1GbE synchronization channels to keep the isolated device synchronized. As a result, when the 10GbE connection was restored, the device immediately came back on line as an available alternate path.

When we failed a complete HA device, the effect was the same as failing an entire server. Once again the remaining server took over all processing. We then had to configure a new partner device manually on any available Paragon server. Once we established a new partner device, Paragon immediately made full use of the synchronization channels to prepare the new device with current data. In both cases, the active Paragon server continued processing the Exchange application data with no impact on users.
To test the performance and functionality of our HA device on the vSphere host, we configured the LUN as a datastore and installed a VM running Windows Server 2008 R2 and Exchange Server 2010. We set up an email server configuration with six dedicated virtual disks to service 800 email accounts. In particular, we dedicated a pair of disks to store the mailbox database and the transaction logs for every group of 400 email users.

To establish a performance baseline for our email server’s configuration, we used the Jetstress benchmark, which distributes email transactions in four groups: 35% reads, 20% deletes, 5% replaces, and 40% inserts and requires an average transaction response time to be under 20ms. Within this framework, normal processing is defined as one transaction per second (TPS) for half the server’s mailboxes, which translates to 400 email TPS for our scenario.

For our unoptimized 10GbE network configuration, we relaxed the average transaction response time to 35ms. With this change in place, we were able to sustain email transaction loads of about 450 TPS. Nonetheless, the key issue for HA is performance at a point of failure.

The most important take away from all of our failover tests, was that Paragon was able to maintain user processing at least at the level prior to the point of failure. The key to this amazing statistic is the I/O processing capability of a image-file device, which underpins all HA devices. As a result of this device choice, HA failover in our tests raised user I/O capabilities by up to 200%. What’s more, it allows Paragon to implement very robust synchronization repair techniques and automated HA restoration.

**CUSTOMER VALUE**

For CIOs, the top-of-mind issue is how to reduce the cost of IT operations. With storage volume the biggest cost driver for IT, storage management is directly in the spotlight.

At most SMB sites today, IT has multiple vendor storage arrays that all have similar functions that must be managed in different ways. From an IT operations perspective, multiple arrays with multiple management systems forces IT administrators to develop many sets of skills. Worse yet, if IT attempts to automate based on one of these proprietary functions, they may be unable to move data from one system to another. By tying data to the functions on one box, purchase options and
vendor choice is greatly reduced.

There are also substantial capital costs to be paid when the same critical management functions are repeatedly licensed for every storage array. By building on multiple virtualization constructs, including the notion of a space of virtual disk blocks from which logical volumes are built, a Paragon StarWind iSCSI SAN is able to take full control over physical storage devices. In doing so, Paragon provides storage administrators with all of the tools needed to automate such critical functions as thin provisioning, creating disk snapshots, disk replication and cloning, as well as local and remote disk mirroring for High-Availability (HA) and Disaster-Recovery (DR) capabilities. With an iSCSI SAN anchored by Paragon, IT buyers can plan for new storage devices not with an eye to the bottom line, but with laser-like precision.

What’s more, Paragon helps IT utilize storage assets more efficiently and avoid vendor lock-in. By leveraging the storage capacity of many disk arrays, IT administrators no longer need to keep spare space available for each individual storage array. This is a particularly important advantage when pushing an iSCSI SAN out to desktop systems, which are notoriously underutilized and over provisioned.

Paragon can also play a very important role in supporting business continuity. With two servers included in a Paragon StarWind iSCSI SAN & NAS Enterprise license, the ability to replicate and mirror devices eliminates single points of failure and all of the disk-related interruptions that get in the way of mission-critical business processing.

Jack Fegreus is Managing Director of openBench Labs; consults through Ridgetop Research; and contributes to InfoStor and Open Magazine. Previously he was Editor in Chief of Open Magazine, Data Storage, BackOffice CTO, Client/Server Today, and Digital Review. Jack also served as CTO of Strategic Communications, a consultant to Demax Software, and IT Director at Riley Stoker Corp. Jack holds a Ph.D. in Mathematics and worked on the application of computers to symbolic logic.